Curriculum Vitæ

Bimal Kumar Roy

Professor, Applied Statistics Unit, Indian Statistical Institute
Head, R C Bose Centre for Cryptology and Security, ISI Kolkata

bimal@isical.ac.in | www.isical.ac.in/~bimal

Contents

1 Personal Details

Full Name	:	Bimal Kumar Roy
Citizenship	:	India
Present Position	:	Professor, Applied Statistics Unit, ISI Kolkata Head, R C Bose Centre for Cryptology and Security
Office Address	:	Indian Statistical Institute, 203 B. T. Road, Kolkata 700108, India. Phone: +91 (33) 2575 3301 Fax: +91 (33) 2577 6925 Email: bimal@isical.ac.in Web: www.isical.ac.in/~bimal
Residence	:	T7/F12/1, Eastern High, Rajarhat – New Town, Kolkata 700156.

2 Professional Details

2.1 Educational Qualifications

1982 **Ph.D. in Combinatorics**, University of Waterloo, Canada

1979 **Master of Statistics – M.Stat.**, Indian Statistical Institute, Kolkata

1978 **Bachelor of Statistics – B.Stat. (Hons)**, Indian Statistical Institute, Kolkata

2.2 Academic Positions

Since 2015 **Head**, R C Bose Centre for Cryptology and Security, ISI Kolkata.

Since 1997 **Professor**, Applied Statistics Unit, Indian Statistical Institute.

2010–2015 **Director**, Indian Statistical Institute.

1990–1991 **Associate Professor**, Department of Computer Science, State University of New York at Utica, USA (on leave from the Indian Statistical Institute).

1989–1997 **Associate Professor**, Computer Science Unit, Indian Statistical Institute.

1984–1989 **Lecturer**, Computer Science Unit, Indian Statistical Institute.

1982–1984 **Assistant Professor**, Department of Computer Science, State University of New York at Utica, USA (position offered immediately after PhD).

3 Awards and Honors

- **Padma Shri Award**, Government of India, 2015.
- **Teacher's Award**, Indian National Science Academy, 2014.
- **Fellow**, Indian Society for Probability and Statistics, since 2014.
- **Fellow**, National Academy of Sciences, India, since 2010.
- **Reliance Platinum Jubilee Award**, National Academy of Science, India, 2007.
- **IBM Faculty Award** for research, teaching and initiative in Cryptology, 2007.

4 Memberships and Professional Services

1. Chairman, Steering Board, Indo-French Centre for Applied Mathematics (IFCAM), **Department of Science and Technology, Government of India** and **The National Center for Scientific Research, Government of France**, since 2013.
2. Member, Scientific Council, Indo-French Centre for the Promotion of Advanced Research (CEFIPRA), **Department of Science and Technology, Government of India** and **Ministry of Foreign Affairs, Government of France**, since 2013.
3. Member, India-Japan Science Council, **Department of Science and Technology (DST), Government of India**, since 2013.
4. Board Member, **National Board for Higher Mathematics (NBHM)**, since 2012.
5. Member, **UNESCO Technical Advisory Committee**, Asia-Pacific, since 2009.

   Involvement in statistical assessment of literacy of the developing nations in the Asia-Pacific region, in order to advice concerned nations on infrastructural requirements for literacy improvement. Active involvement with Palestine and Laos.
6. Member, Program Advisory Committee for Mathematical Sciences, **Department of Science and Technology (DST), Government of India**, 2007–2012.

   Involvement in the study and recommendation for approval of nation-wide research and/or project proposals in pure and applied mathematics, statistics, operations research and theoretical computer science.
7. Adviser for Secure Wireless Communication, **Special Protection Group (SPG), Government of India**, 2006–2007.

   Involvement in the security assessment of the entire wireless communication systems, including the main network, mobile devices and key management issues.

8. Member, Technical Advisory Committee for Surveys, **Reserve Bank of India (RBI), Government of India**, 2007–2015.

   Instrumental in streamlining the inflation expectation survey, significantly impacting RBI's monetary policy. Involvement in building housing price indices for different segments such as big metropolis, small towns, villages, etc.

9. Member, Governing Council, **National Sample Survey Organization (NSSO), Government of India**, 2002–2006.

   Instrumental in designing national level surveys for all rounds in the said period. Advice on data validation, compilation and analysis. Chairman of a working group to study potential under-estimation of population total via NSSO surveys, as compared to census.

10. Member, Board for Security and Assurance, **National Association of Software and Service Companies (NASSCOM)**, since 2004.

    Instrumental in advising all software companies to formulate policies on information security. Involvement in the formulation of the Information Technology Act, 2006.

11. Founder-Secretary, **Cryptology Research Society of India**, since inception in 2001.

    Pioneering role in the development of cryptology research in India, and in the promotion of the science of modern cryptology in Indian academia and government agencies.

    Instrumental in initiating and organizing Indocrypt (since 2000), one of the leading international conferences dedicated to cryptology. Invited doyens of cryptology, such as Professors Adi Shamir, Claus P. Schnorr, Vincent Rijmen, Bart Preneel, Neal Koblitz, to India for talks and interactions with the Indian cryptology community.

12. Member, **International Association for Cryptologic Research**, since 2000.

5 Services to the Nation

1. Pioneered cryptology education and research in India. Instrumental in organizing national-level research and instructional workshops for students, young faculty members and researchers, to disseminate the state-of-the-art knowledge in cryptology.

2. Conceptualized and initiated the R.C. Bose Centre for Cryptology and Security at the Institute, aimed at marshaling of human and infrastructure resources for the purpose of inventing and developing avant-garde technologies that will address the cryptographic needs of our Nation. The Centre aims to act as a hub for all cryptographic requirements, cutting-edge research and relevant technology development in relevant fields, and will create a critical mass of researchers and experts in the country.

3. Conceived and created the Sampling and Official Statistics Unit (SOSU) at Indian Statistical Institute to serve the Nation in these niche domain. The unit supports the Government by taking up projects of national importance, and trains relevant manpower from the government sectors in the target areas of statistics.

4. Initiated the North-East centre of the Institute at Tezpur to bring advanced training in Statistics and allied disciplines within reach of the students from the north eastern states. Created a sustainable solution for employment of students from these parts of the country through collaborative ventures with relevant industries.

5. Developed indigenous cryptographic algorithms for different government agencies such as Defence Research Development Organization (DRDO), Department of Information Technology (DIT), Indian Navy, Indian Space Research Organization (ISRO), Bhabha Atomic Research Center (BARC), etc. Served as an adviser to the Special Protection Group (SPG) and Police Wireless Communications for secure wireless communications.

6. Provided knowhow on methodology and applications of Statistics to National Sample Survey Organization (NSSO), Reserve Bank of India, Ministry of Labour etc. in conducting nationwide surveys, data analysis and inference.

7. Created sustainable avenues for the Institute to serve the country towards economic and security policy decisions, in collaboration with eminent Government of India bodies like DRDO, Cabinet Secretariat, DIT, DST, DAE, and the Reserve Bank of India.

8. Acted as a liaison between prominent corporate sectors and underprivileged graduates from sub-urban and rural areas, resulting in placements of around fifty such candidates from remote areas of the Sundarbans and Giridih.

6 International Recognition

6.1 International Academic Liaison

1. Advisor for setting a centre for cryptography and information security at **Khalifa University, Abu Dhabi** for the **Government of the United Arab Emirates**.

2. International faculty for supervising Master's degree cadets of **École Spéciale Militaire de Saint-Cyr, France**, since 2001.

3. Member of **International Scientific Advisory Committee** of the **Centre for Applied Cryptography Research, University of Waterloo, Canada**, since 2001.

6.2 International Research Collaboration

– Amiya Nayak, Univ. of Ottawa, **Canada**

– Jennifer Seberry, Univ. of Wollongong, **Australia**

– Anne Canteaut, INRIA, **France**

– Nicolas Sendrier, INRIA, **France**

– Thomas Johansson, Lund Univ., **Sweden**

6.3 Invited International Visits

- French Military Academy, Rennes and INRIA-Paris, **France**
- University of Waterloo, Carleton University, and University of Ottawa, **Canada**
- George Washington University, Purdue University, Johns Hopkins University, **USA**
- Chinese Academy of Sciences, **PR of China**
- University of Science and Technology, **Hong Kong**
- Kyushu University, Tokyo University, **Japan**
- Lund University, **Sweden**
- National University of Singapore, **Singapore**
- Katholieke Universiteit, **Belgium**

Invited Talks at International Conferences

- IEEE International Workshop in Information Theory, Gdansk, Poland, 2008.
- Special invited talks at the Chinese Academy of Science, Beijing, 2007.
- Australasian Conference on Information Security and Privacy, Melbourne, 2002.

6.4 Editorial Work

1. Associate Editor, **Journal of Ad Hoc & Sensor Wireless Networks**.
2. Associate Editor, **Journal of Wireless Sensor Networks**.
3. Associate Editor, **Research & Reviews: Journal of Statistics**.

Edited Volumes

1. Bimal K. Roy and Nicolas Sendrier (editors). *Progress in Cryptology – INDOCRYPT 2009*. **Lecture Notes in Computer Science**, Volume 5922, Springer 2009.
2. D.K. Ray-Chaudhuri, A.R. Rao, and Bimal K. Roy (editors). *R. C. Bose Centennial Symposium on Discrete Mathematics and Applications*. **Discrete Mathematics** (Special Edition), Volume 306, Issue 14, Elsevier 2006.

   Note: Discrete Mathematics very selectively publishes special issues and it is a great international honor to be an editor for such issues.
3. Bimal K. Roy (editor). *Advances in Cryptology – ASIACRYPT 2005*. **Lecture Notes in Computer Science**, Volume 3788, Springer 2005.

4. Bimal K. Roy and Willi Meier (editors). *Fast Software Encryption – FSE 2004*. **Lecture Notes in Computer Science**, Volume 3017, Springer 2004.

   Note: ASIACRYPT and FSE are flagship conferences of the International Association for Cryptologic Research (IACR) and a cryptologist is invited to chair such conference only once in a lifetime. Chairing two such conferences is a rare honor shared only by a handful of international researchers.

5. Bimal K. Roy and Eiji Okamoto (editors). *Progress in Cryptology – INDOCRYPT 2000*. **Lecture Notes in Computer Science**, Volume 1977, Springer 2000.

   Note: This was the first international conference on cryptology organized in India.

6. Bimal K. Roy (editor). *Special Issue on Cryptology* **Journal of the Indian Statistical Association**, Volume 42, 2004.

   Note: This was the first such initiative to motivate the statistics research community about the multifarious applications of statistics in cryptology.

Program Committee: Served as a Member of the Technical Program Committees of numerous top-tier International conferences in Cryptology and allied disciplines.

7 Academic Administration

1. **Director**, Indian Statistical Institute, 2010 to date.

   Growth of the Institute

   - Initiated the North-East centre of the Institute at Tezpur to bring advanced training in Statistics and allied disciplines within reach of the students from NE states.
   - Revived the Chennai and Giridih centres of the Institute, by offering appropriate courses in Statistics and applications at both the centres.
   - Initiated new academic programs at every Centre of the Institute, focussing on human welfare and national development, in addition to the academic goals.

   Academic Liaison

   - Signed MoUs and initiated academic collaborations with London School of Economics (UK); Johns Hopkins University, Columbia University, Purdue University (USA); NUS (Singapore); Kyushu University (Japan); and INRIA (France).
   - Created new channels for sustained academic collaborations with national institutes of importance like IMSc (Chennai), CMI (Chennai) and TIFR (Mumbai).

   Service to the Nation

   - Created sustainable avenues for the Institute to serve the country in collaboration with eminent Government of India bodies like DRDO, Cabinet Secretariat, DIT, DST, DAE, and the Reserve Bank of India.

- Conceptualized and initiated the R.C. Bose Centre for Cryptology and Security at the Institute, aimed to address the cryptographic needs of our Nation.
- Conceived and created the Sampling and Official Statistics Unit (SOSU) at Indian Statistical Institute to serve the Nation in these niche domain.

Ergonomic Administration

- Decentralized the administrative responsibilities of the Institute by providing reasonable financial power to the Centre Heads, Professors-in-Charge and Unit Heads. This helped in a smooth functioning of day-to-day activities without burden on or interference from the other levels of the administrative hierarchy.
- Encouraged Institute workers, both academic and non-academic, at every level, to realize and take charge of their administrative duties and powers. This resulted in a flatter, and more ergonomic, structure of administration at the Institute.

Carried out the role of a regular faculty member of the Institute in spite of the aforesaid administrative workload. Regularly taught courses offered at various levels, and continued research supervision of PhD and Masters students during the tenure.

2. **Dean of Studies**, Indian Statistical Institute, 2006–2008.
   - Initiated the introduction of special quotas for the underprivileged section of the society (as per the Government of India policies).
   - Initiated pro-active measures leading to an increased intake in the number of students and research scholars.
   - Initiated cultural and sports program for the students including a drama festival and a football competition.
   - Initiated interaction of the students with captains of the industry such as the CEO of Infosys and Vice President & General Manager of IBM Global Services in India.
   - Initiated funding from Microsoft Research India for awards to bright young faculty of the institute and for providing international travel support to both PhD students and faculty members.
   - Initiated measures to modernize the dean's office operations including the starting of OCR based processing of admission test answer scripts.
3. **Professor-in-Charge**, Applied Statistics Division, ISI, 2000–2002 and 2008–2010.
4. **Head**, Applied Statistics Unit, ISI Kolkata, 2005–2006.
5. **Warden**, Students' Hostels (all), ISI Kolkata, 1987–1998.
6. **Founder of the Placement Committee**, Indian Statistical Institute, 1985.
   - Served as the convener of the committee for the period 1985–1992.
   - Created liaisons and carried out negotiations with different industries resulting in making '*ISI Graduate*' a sought-after brand-name in the relevant sectors.

8 Teaching Experience

- Taught at Indian Statistical Institute for over 30 years, since 1984.
- Taught at almost all degree courses offered at the Institute – B.Stat., M.Stat., M.Math., M.Tech.(CS), M.Tech.(QR&OR) and M.S.(QE) – at almost every possible level.
- Taught more than 60 courses, including almost all courses related to Statistics and Computer Science offered at all undergraduate and postgraduate levels of the Institute.
- Pioneered Cryptology education in India. Taught the subject through numerous courses, lectures, popular talks, seminars and workshops, and promoted this niche subject area.

9 Sponsored Projects

9.1 Projects on Cryptology

Served as the **Principal Investigator** for all the projects in Cryptology mentioned in this section. Each project mentioned in this section has led to significant cryptographic solutions and services meant to be used by the concerned agencies.

High-Budget Projects

1. **Centre of Excellence in Cryptology**, funded by **Defence Research and Development Organization**, 2011–2016.

   Meant to support basic research and development in Cryptology and related disciplines. Conceived and operated as an umbrella project to host multiple associated projects in Cryptology that serve multifarious pertinent issues of National importance.

2. Strategic Japanese-Indian Co-operative Program on **Multidisciplinary Research Field which combines Information and Communications Technology with Other Fields**, 2009–2012.

   Joint research on network security and key management solutions meant for potential adoption by the Indian and Japanese governments.

3. **Research and development of Cryptographic Primitives**, funded by **Department of Information Technology**, 2006–2011.

   Meant for development of indigenous crypto-systems involving encryption and hash function for use by different government agencies. Supported new research in the areas of Boolean functions, identity-based encryption, signcryption, visual cryptography, and sensor networks, with potential for development as commercial products.

4. **Evaluation of a stream cipher designed by KDDI, Tokyo, Japan**, 2006–2007.

   Assess and validate an LFSR based stream cipher to be used for mobile communication.

5. **Development of pairing based cryptographic protocols**, funded by **Department of Information Technology**, 2003–2006.

   Development of new protocols using bilinear maps realized through Tate pairings.

6. **Cryptanalysis of complex LFSR based stream ciphers**, funded by **Scientific Analysis Group, Defence Research and Development Org.**, 2000–2002.

   Complete cryptanalysis of very general LFSR based combiner models where the combining function has low correlation immunity which is the case in reality.

7. **Cryptanalysis of LFSR based stream ciphers**, funded by **Defence Research and Development Organization**, 1998–2000.

   Cryptanalysis of specified combiner models and related stream ciphers.

Other Projects of National Importance

1. *Construction of Universal One-Way Hash Functions*, funded by **WESEE, Indian Navy**, 2005–2006.

2. *Study of connection polynomials over* $GF(2^k)$, funded by **CAIR, Defence Research and Development Organization**, 2005–2006.

3. *Development of visual cryptographic schemes*, funded by **WESEE, Indian Navy**, 2005–2006.

4. *Development of visual cryptographic schemes*, funded by **ADRIN, Indian Space Research Organization**, 2002–2004.

5. *Study of connection polynomials over* $GF(2)$, funded by **CAIR, Defence Research and Development Organization**, 2001–2002.

6. *Development of indigenous stream cipher for Indian Navy*, funded by **WESEE, Indian Navy**, 2001–2002.

7. *Construction of Boolean functions with cryptographic properties*, funded by **CAIR, Defence Research and Development Organization**, 2000–2001.

8. *Design of new stream cipher*, funded by **SHOGHI**.

9. *Design of self-synchronizing stream cipher*, funded by **Sutech**.

9.2 Projects on Statistics

1. Member of a project on **Methods for Estimating Tiger Population in the Sunderbans**, funded by the **Government of West Bengal**, 2006–2007.

2. Member of a project on **Methods for Estimating Elephant Population in Jaldapara** funded by the **Government of West Bengal**, 2006–2007.

3. Member of a project on **Life Distribution of Currency Notes**, funded by the **Reserve Bank of India**, 2002–2003.

4. Principal investigator of a project on **Tracer Study of ITI Trainees**, funded by **Directorate General (Education and Training)**, 1994–1996.

   Survey and analysis of employability of ITI trainees in government and private industries as skilled labors with emphasis on region and trade-wise variations. Provided inputs for improvement of ITI training program for better employability of the trainees.

5. Principal investigator of a project on **Rural Indebtedness**, funded by the **Reserve Bank of India**, 1993–1995.

   Resolved a dispute that arose from contradictions between NSSO's All-India Debt and Investment Surveys and RBI bulletin on rural credit disbursements.

6. Principal investigator of a project on **Garbage Management of Calcutta Municipal Corporation**, funded by **Calcutta Municipal Corporation**, 1989–1990.

   Solved the challenging problem of estimation of garbage accumulation in the Calcutta Municipal Corporation area with seasonal variations. Suggested optimal routing of vehicles for garbage clearance within a given time-frame with the available resources, including vehicles and manpower.

10 Thesis Supervision

10.1 PhD Thesis Supervision

Supervised thirteen (13) PhD theses in four different technical areas – 3 in Statistics, 7 in Computer Science, 1 in Mathematics and 2 in Statistical Applications.

Statistics

1. On **some contemporary issues in software reliability**, 2014.

2. On **application of combinatorics in fault tolerant VLSI designs**, 2001.

3. On **repeated measurement designs and symmetric balanced squares**, 1992.

Computer Science

4. On **application of combinatorial structures in wireless communication**, 2014.

5. On **the problem of coverage and event detection in sensor networks**, 2014.

6. On **black-box reduction of cryptographic algorithms**, 2011.

7. On **application of combinatorial structures to key predistribution in sensor networks and traitor tracing**, 2009.

8. On **key pre-distribution in sensor networks**, 2008.

9. On **construction of visual cryptographic schemes**, 2004.

10. On **construction of Boolean functions with cryptographic properties**, 2000.

Mathematics

11. On **designs of iteration on hash functions and its cryptanalysis**, 2005.

Statistical Applications (degrees awarded by Jadavpur University)

12. On **environmental sciences** (co-supervisor), 2008.

13. On **statistical methods in analytical chemistry** (co-supervisor), 1991.

10.2 Masters Thesis Supervision

Supervised over fifty (50) Masters dissertations in four different technical areas – Master of Statistics, Master of Mathematics, Master of Technology in Computer Science, and Master of Technology in Quality, Reliability and Operations Research.

11 List of Publications

Published around forty (40) papers in refereed Journals; around twenty (20) book chapters, including proceedings for International Conferences; with over twenty (20) papers in Cryptology and Information Security, in reputed International Conferences and Journals.

11.1 Refereed Journals

1. Vignesh T. Subrahmaniam, Anup Dewanji, and Bimal K. Roy. *A Semiparametric Software Reliability Model for Analysis of a Bug-Database with Multiple Defect Types.* **Technometrics**, 2014.

2. Mrinal Nandi, Anup Dewanji, Bimal K. Roy, and Santanu Sarkar. *Model Selection Approach for Distributed Fault Detection in Wireless Sensor Networks.* **IJDSN**, 2014.

3. Samiran Bag and Bimal K. Roy: *A new key predistribution scheme for general and grid-group deployment of wireless sensor networks.* **EURASIP Journal on Wireless Communication and Networking**, 2013.

4. Srimanta Bhattacharya, Sushmita Ruj and Bimal K. Roy. *Combinatorial Batch Codes: Lower Bound and Optimal Constructions.* **Advances in Mathematics of Communications**, Volume 6, Number 2, Pages 165–174, 2012.

5. Sushmita Ruj and Bimal K. Roy. *Key Predistribution using Partially Balanced Designs in Wireless Sensor Networks.* **IJHPCN**, Volume 7, Number 1, Pages 19–28, 2011.

6. Subba Rao V. Yengisetty and Bimal K. Roy. *Applications of visual cryptography.* **IJPEDS**, Volume 26, Number 5, Pages 429–442, 2011.

7. Sushmita Ruj and Bimal K. Roy. *Key Predistribution Using Combinatorial Designs for Grid-group Deployment Scheme in Wireless Sensor Networks.* **ACM Transaction on Sensor Networks**, Volume 6, Number 1, 2009.

8. Sushmita Ruj and Bimal K. Roy. *Revisiting Key Predistribution using Transversal Designs for a Grid-based Deployment Scheme.* **IJDSN**, Volume 5, Number 6, Pages 660–674, 2009.

9. Sushmita Ruj and Bimal K. Roy. *Key Distribution Schemes Using Combinatorial Designs to Identify all Traitors.* **Congressus Numerantium**, Volume 193, Pages 195–214, 2008.

10. Sushmita Ruj, Subhamoy Maitra, and Bimal K. Roy. *Key Predistribution using Transversal Design on a Grid of Wireless Sensor Network.* **Ad Hoc & Sensor Wireless Networks**, Volume 5, Number 3–4, pp 247–264, 2008.

11. Avishek Adhikari Mausumi Bose, Dewesh Kumar, and Bimal K. Roy. *Applications of Partially Balanced Incomplete Block Designs in Developing* $(2, n)$ *Visual Cryptographic Schemes.* **IEICE Transactions**, Volume 90-A, Number 5, Pages 949–951, 2007.

12. Dibyendu Chakrabarti, Subhamoy Maitra, and Bimal K. Roy. *A key pre-distribution scheme for wireless sensor networks: merging blocks in combinatorial design.* **IJIS**, Volume 5, Number 2, Pages 105–114, 2006.

13. M. Amir Hossain, Mrinal Kumar Sengupta, Sad Ahamed, Mohammad Mahmudur Rahman, Debapriya Mondal, Dilip Lodh, Bhaskar Das, Bishwajit Nayak, Bimal K. Roy, Amitava Mukherjee, and Dipankar Chakraborti. *Ineffectiveness and Poor Reliability of Arsenic Removal Plants in West Bengal, India.* **Environmental Science & Technology**, Volume39, Number 11, Pages 4300–4306, 2005.

    Highlighted in News Section of Nature Magazine. *Arsenic-free water still a pipedream.* **NATURE**, Volume 436, Page 313, 21st July 2005.

14. Dibyendu Chakrabarti, Subhamoy Maitra, Bimal K. Roy. *Clique Size in Sensor Networks with Key Pre-distribution Based on Transversal Design.* **IJDSN**, Volume 1, Number 3–4, Pages 345–354, 2005.

15. Soumen Maity, Amiya Nayak, and Bimal K. Roy. *Characterization of catastrophic faults in two-dimensional reconfigurable systolic arrays with unidirectional links.* **Information Processing Letters**, Volume 92, Number 4, Pages 189–197, 2004.

16. Soumen Maity, Amiya Nayak, and Bimal K. Roy. *On characterization of catastrophic faults in two-dimensional VLSI arrays.* **Integration**, Volume 38, Number 2, Pages 267–281, 2004.

17. Bimal K. Roy and Sarbani Palit. *Some statistical attacks on stream cipher cryptosystems.* **Journal of Indian Statistical Association**, Volume 42, Number 1, Pages 1–34, 2004.

18. Bimal K. Roy and Sourav Mukhopadhyay. *Statistical Cryptanalysis on Block Cipher.* **Journal of the Indian Society for Probability and Statistics**, Volume 7, 2003.

19. Soumen Maity, Bimal K. Roy, and Amiya Nayak. *On enumeration of catastrophic fault patterns.* **Information Processing Letters**, Volume 81, Number 4, Pages 209–212, 2002.

20. Soumen Maity, Bimal K. Roy and Amiya Nayak. *Identification of optimal link redundancy for which a given fault pattern is catastrophic in VLSI linear arrays.* **Congressus Numerantium**, Volume 151, Pages 41–52, 2001.

21. Tridib K. Dutta and Bimal K. Roy. *Construction of some repeated measurements designs.* **Journal of Statistical Planning and Inference**, Volume 95, Issues 1–2, Pages 283–291, 2001.

22. Soumen Maity, Tridib K. Dutta, and Bimal K. Roy. *Construction and efficiency of some repeated measurements designs.* **Journal of the Indian Statistical Association**, Volume 39, Number 2, Pages 137–160, 2001.

23. Soumen Maity, Bimal K. Roy, and Amiya Nayak. *Enumerating catastrophic fault patterns in VLSI arrays with both uni- and bidirectional links.* **Integration**, Volume 30, Number 2, Pages 157–168, 2001.

24. Soumen Maity and Bimal K. Roy. *Construction of some classes of optimal repeated measurements designs.* **Calcutta Statistical Association Bulletin**, Volume 50, Number 197–198, Pages 33–42, 2000.

25. Subhamoy Maitra, Bimal K. Roy and Palash Sarkar. *Ciphertext only attack on LFSR based encryption scheme.* **Calcutta Statistical Association Bulletin**, Volume 49, Number 195–196, Pages 239–254, 1999.

26. Dipankar Basu, Kumar K. Mahalanabis and Bimal K. Roy. *Application of least squares method in matrix form: simultaneous determination of ibuprofen and paracetamol in tablets.* **Journal of Pharmaceutical and Biomedical Analysis**, Volume 16, Issue 5, Pages 809–812, 1998.

27. Tridib K. Dutta and Bimal K. Roy. *Construction of symmetric balanced squares.* **Ars Combinatoria**, Volume 47, Pages 49–64, 1997.

28. Palash Sarkar, Bimal K. Roy, and Pabitra Pal Choudhury. *Polynomial division using left shift register.* **Computers & Mathematics with Applications**, Volume 35, Number 6, Pages 27–31, 1998.

29. Palash Sarkar and Bimal K. Roy. *Construction of nearly balanced uniform repeated measurement designs.* **Calcutta Statistical Association Bulletin**, Volume 45, Number 179–180, Pages 235–243, 1995.

30. Indranil Ojha and Bimal K. Roy. *Optimal routing of vehicles for garbage clearance in a city.* **Opsearch**, Volume 31, Number 4, Pages 279–295, 1994.

31. Tridib K. Dutta and Bimal K. Roy. *Construction of strongly balanced uniform repeated measurements designs: a new approach.* **Sankhya**, Volume 54, Pages 147–153, 1992.

32. Dipankar Basu Kumar K. Mahalanabis and Bimal K. Roy. *Simultaneous spectrophotometric determination of metronidazole and furazolidone with multi standard addition and a least-squares method.* **Analytica Chimica Acta**, Volume 249, Issue 2, Pages 349–352, 1991.

33. Anup K. De and Bimal K. Roy. *Computer construction of some group divisible designs.* **Sankhya, Series-B**, Volume 52, Part 1, Pages 82–92, 1990.

34. Kumar K. Mahalanabis, Dipankar Basu, and Bimal K. Roy. *Application of the least-squares method in the matrix form: simultaneous spectrophotometric determination of rifampicin and isoniazid in binary pharmaceutical formulations.* **Analyst**, Volume 114, Number 10, Pages 1311–1314, 1989.

35. Bimal K. Roy. *Construction of strongly balanced uniform repeated measurements designs.* **Journal of Statistical Planning and Inference**, Volume 19, Number 3, Pages 341–348, 1988.

36. Joseph D. Horton, Bimal K. Roy, Paul J. Schellenberg, and Douglas R. Stinson. *On decomposing graphs into isomorphic uniform* $2-$*factors.* **Annals of Discrete Mathematics**, Volume 27, Pages 297–320, 1985.

37. Bimal K. Roy and Kirti R. Shah. *On the optimality of a class of minimal covering designs.* **Journal of Statistical Planning and Inference**, Volume 10, Number 2, Pages 189–194, 1984.

38. Ronald C. Mullin, Bimal K. Roy, Paul J. Schellenberg. *Isomorphic subgraphs having minimal intersections.* **Journal of the Australian Mathematical Society**, Series A-Pure Mathematics and Statistics, Volume 35, Issue DEC, Pages 287–306, 1983.

39. Bimal K. Roy. *Construction of* (M, S)*-optimal design for block size* 3. **Journal of Statistical Planning and Inference**, Volume 7, Issue 1, Pages 35–37, 1982.

11.2 Book Chapters

1. Samiran Bag, Sushmita Ruj, and Bimal K. Roy. *Jamming Resistant Schemes for Wireless Communication: A Combinatorial Approach.* ICISS 2013, **Lecture Notes in Computer Science**, Volume 8303, Pages 43–62, Springer 2013.

2. Samiran Bag and Bimal K. Roy. *Two channel hopping schemes for jamming resistant wireless communication.* WiMob 2013, **IEEE Computer Society**, Pages 659–666, IEEE 2013.

3. Sushmita Ruj, Jennifer Seberry, and Bimal K. Roy. *Key Predistribution Schemes Using Block Designs in Wireless Sensor Networks.* CSE 2009, **IEEE Computer Society**, Pages 873–878, IEEE 2009.

4. Sushmita Ruj and Bimal K. Roy. *Key Predistribution Schemes Using Codes in Wireless Sensor Networks.* INSCRYPT 2008, **Lecture Notes in Computer Science**, Volume 5487, Pages 275–288, Springer 2008.

5. Abhijit Das and Bimal K. Roy. *A New Key-Predistribution Scheme for Highly Mobile Sensor Networks.* ICDCN 2008, **Lecture Notes in Computer Science**, Volume 4904, Pages 298–303, Springer 2008.

6. Sushmita Ruj and Bimal K. Roy. *Key Establishment Algorithms for some Deterministic Key Predistribution Schemes.* WOSIS 2008, Pages 68–77, INSTICC 2008.

7. Sushmita Ruj and Bimal K. Roy. *Key Predistribution using Partially Balanced Designs in Wireless Sensor Networks.* ISPA 2007, **Lecture Notes in Computer Science**, Volume 4742, Pages 431–445, Springer 2007.

8. Bimal K. Roy. *Book Review On Branch-and-Bound Applications in Combinatorial Data Analysis.* **Sankhya**, Volume 68, Part 1, Pages 174–175, 2006.

9. Dibyendu Chakrabarti, Subhamoy Maitra, and Bimal K. Roy. *A Hybrid Design of Key Pre-distribution Scheme for Wireless Sensor Networks.* ICISS 2005, **Lecture Notes in Computer Science**, Volume 3803, Pages 228–238, Springer 2005.

10. Dibyendu Chakrabarti, Subhamoy Maitra, and Bimal K. Roy. *A Key Pre-distribution Scheme for Wireless Sensor Networks: Merging Blocks in Combinatorial Design.* ISC 2005, **Lecture Notes in Computer Science**, Volume 3650, Pages 89–103, Springer 2005.

11. Dibyendu Chakrabarti, Subhamoy Maitra, and Bimal K. Roy. *Clique Size in Sensor Networks with Key Pre-distribution Based on Transversal Design.* IWDC 2005, **Lecture Notes in Computer Science**, Volume 3741, Pages 329–337, Springer 2005.

12. Avishek Adhikari, Tridib Kumar Dutta, and Bimal K. Roy. *A New Black and White Visual Cryptographic Scheme for General Access Structures.* INDOCRYPT 2004, **Lecture Notes in Computer Science**, Volume 3348, Pages 399–413, Springer 2004.

13. Soumen Maity, Amiya Nayak, and Bimal K. Roy. *Reliability of VLSI Linear Arrays with Redundant Links.* IWDC 2004, **Lecture Notes in Computer Science**, Volume 3326, Pages 326–337, Springer 2004.

14. Sarbani Palit, Bimal K. Roy, and Arindom De. *A Fast Correlation Attack for LFSR-Based Stream Ciphers.* ACNS 2003, **Lecture Notes in Computer Science**, Volume 2846, Pages 331–342, Springer 2003.

15. Bimal K. Roy. *Summarizing Recent Results on Finding Multiples of Primitive Polynomials over $GF(2)$.* Information Theory Workshop, 2002.

16. Bimal K. Roy. *A brief outline of Research on Correlation Immune Functions.* ACISP 2002, **Lecture Notes in Computer Science**, Volume 2384, Pages 379–394, Springer 2002.

17. Sarbani Palit and Bimal K. Roy. *Cryptanalysis of LFSR-Encrypted Codes with Unknown Combining Function.* ASIACRYPT 1999, **Lecture Notes in Computer Science**, Volume 1716, Pages 306–320, Springer 1999.

18. Palash Sarkar, Bimal K. Roy, and Pabitra Pal Choudhury. *VLSI Implementation of Modulo Multiplication Using Carry Free Addition.* VLSI Design 1997, **IEEE Computer Society**, Pages 457–460, IEEE 1997.