

# Curriculum Vitae

## 1 Personal Details

1. Name: **Bimal Kumar Roy.**
2. Date of birth: **7<sup>th</sup> March, 1959.**
3. Citizenship : **India.**
4. Present position/designation:  
**Professor**  
**Applied Statistics Unit**  
**Indian Statistical Institute.**

5. Address.

(a) **Office:**

203, B. T. Road  
Kolkata 700108.  
Ph: 91 33 2575 2809  
FAX: 91 33 2577 6037  
email: bimal@isical.ac.in.

(b) **Residence:**

205, B. T. Road  
Kolkata 700108.  
Ph: 91 33 2575 5105, 91 33 2577 3593.

## 2 Academic and Professional Details

### 1. Qualifications.

Degree	Subject	Institution	Year	Remark
B.Stat	Statistics	Indian Statistical Institute	1978	<b>2nd rank</b>
M.Stat	Statistics	Indian Statistical Institute	1979	<b>1st rank</b>
PhD	Combinatorics	Univ. of Waterloo, Canada	1982	<b>completed in 2 years</b>

### 2. Positions Held.

- (a) **Assistant Professor, Department of Computer Science, State University of New York at Utica, 1982 – 1984.**
- (b) **Lecturer, Computer Science Unit, Indian Statistical Institute, 1984 – 1989.**
- (c) **Associate Professor, Computer Science Unit, Indian Statistical Institute, 1989 – 1997.**
- (d) **Associate Professor, Department of Computer Science, State University of New York at Utica, 1990 – 1991.** (on leave from the Indian Statistical Institute).
- (e) **Professor, Applied Statistics Unit, Indian Statistical Institute, 1997 till date.**

## 3 Awards

1. **National Academy of Science, India – Reliance Platinum Jubilee Award** for innovation in Physical Sciences, 2007.
2. **IBM Faculty Award 2007** for research, teaching and initiative in Cryptology and Security.

## 4 Thesis Supervision

### 4.1 PhD Supervision

The details of the supervision of research fellows in different areas are given below.

#### RF in Statistics.

1. On repeated measurement designs and symmetric balanced squares, 1992.
2. On application of combinatorics in fault tolerant VLSI designs, 2001.

#### RF in Computer Science.

3. On application of combinatorial structures to key predistribution in sensor networks and traitor tracing, 2009.
4. On key pre-distribution in sensor networks, 2008.
5. On construction and properties of cryptographic hash functions, expected 2010.
6. On construction of visual cryptographic schemes, 2004.
7. On construction of Boolean functions with cryptographic properties, 1999.

#### RF in Mathematics.

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

#### RF in Statistical Applications. The degrees were awarded by Jadavpur University.

9. On environmental sciences (co-supervisor), 2008.
10. On statistical methods in analytical chemistry (co-supervisor), 1991.

### 4.2 Master's Students

Supervised over fifty masters dissertation in different curricula such as **Master of Statistics**, **Master of Technology in Computer Science**, **Master of Technology in Quality, Reliability and Operations Research**.

## 5 Membership of Professional Bodies and Roles

1. Member of the **UNESCO Technical Advisory Committee** for Asia-Pacific region, since 2009.
  - Involved in statistical assessment of literacy of the developing nations in Asia-Pacific region and to advice concerned nations on infrastructural requirements for literacy improvement. Currently involved with Palestine and Laos.
2. Member of program advisory committee for mathematical sciences of the **Department of Science and Technology (DST)**, India, 2007 onwards.
  - Study and recommend for approval research/project nation-wide proposals in pure and applied mathematics, statistics, operations research and theoretical computer science.
  - Security assessment of the entire wireless communication systems, including main network, mobile devices and key management.
3. Member of Technical Advisory committee for surveys, **Reserve Bank of India** from 2007.
  - Streamlined inflation expectation survey that has impact on RBI's monetary policy.
  - To help in building housing price indices for different segments such as big metropolis, small towns, villages, etcetra.
4. Member of the Governing Council of the **National Sample Survey Organization (NSSO)**, 2002–2006.
  - Designing the national level surveys for all the rounds in the said period, advice on data validation, compilation and analysis.
  - Chairman of a working group to study possible under-estimation of population total via NSSO surveys as compared to census.
5. Member of the board for security and assurance, **National Association of Software and Service Companies (NASSCOM)**, from 2004.
  - Provided input to all software companies to formulate policies on information security.
  - Participated in the formulation of the Information Technology Act, 2006.
6. **Founder-Secretary** of the **Cryptology Research Society of India**, from its inception in 2001.
  - Leadership role in promoting the science of modern cryptology in academia and government agencies.
  - Organising an international conference series called Indocrypt since 2000 which has become one of the leading conferences dedicated to the science of cryptology.

- Inviting doyens of cryptology, such as Professors Adi Shamir, Claus P. Schnorr, Vincent Rijmen, Bart Preneel, to India for talks and interactions with the Indian cryptology community.
- Organising national-level workshops for young faculty and researchers to disseminate the state-of-the-art knowledge in the subject.
- Organising national-level instructional workshops for teachers of cryptology.

## 6 Sponsored Projects

### 6.1 Cryptology

Principal investigator for all the projects below.

#### 1. High-Budget Projects

- (a) **Strategic Japanese-Indian Co-operative Programme on “Multidisciplinary Research Field which combines Information and Communications Technology with Other Fields”**, 2009-2012.
  - Joint research on network security, key management for plausible adoption by the Indian and Japanese governments.
- (b) **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.
- (c) **Research and development of cryptographic primitives**, funded by **Department of Information Technology**, 2006-2011.
  - Develop indigenous cryptosystems involving encryption and hash function for use by different government agencies.
  - New research in the areas of Boolean functions, identity-based encryption, sign-cryption, visual cryptography, sensor networks with potential for development as commercial products.
- (d) **Development of pairing based cryptographic protocols**, funded by **Department of Information Technology**, 2003–2006.
  - Development of new protocols using bilinear maps realised through Tate pairings.
- (e) **Cryptanalysis of Complex LFSR based stream ciphers**, funded by **Scientific Analysis Group of the Defence Research and Development Organization**, 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.
- (f) **Cryptanalysis of LFSR based stream ciphers**, funded by **Defence Research and Development Organization**, 1998–2000.
  - Cryptanalysis of specified combiner models.

2. **Other Projects.** All the projects below have lead to products to be used by the concerned agencies.

- (a) **Construction of Boolean functions with cryptographic properties**, funded by **CAIR, Defence Research and Development Organization**, 2000-2001.
- (b) **Study of connection polynomials over  $GF(2)$** , funded by **CAIR, Defence Research and Development Organization**, 2001-2002.

- (c) **Study of connection polynomials over  $GF(2^k)$** , funded by **CAIR, Defence Research and Development Organization**, 2005-2006.
- (d) **Development of indigenous stream cipher for Indian Navy**, funded by **WESEE, Indian Navy**, 2001-2002.
- (e) **Development of visual cryptographic schemes**, funded by **WESEE, Indian Navy**, 2005-2006.
- (f) **Construction of UOWHF**, funded by **WESEE, Indian Navy**, 2005-2006.
- (g) **Development of visual cryptographic schemes**, funded by **ADRIN, Indian Space Research Organization**, 2002-2004.
- (h) **Design of new stream cipher**, funded by **SHOGHI**.
- (i) **Design of self-synchronizing stream cipher**, funded by **Sutech**,

## 6.2 Projects on Statistics

1. Principal investigator of a project on **“Tracer Study of ITI Trainees”** funded by **Directorate General (Education and Training)**, 1994–1996.
  - Employability of ITI trainees in government and private industries as skilled labours with emphasis on region and trade-wise variations.
  - Provide input for improvement of ITI training program for better employability of the trainees.
2. 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.
3. 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.
  - Optimal routing of vehicles for garbage clearance within a given time-frame with the available resources, including vehicles and manpower.
4. Team member of a project on **“Methods for Estimating Tiger Population in the Sunderbans”** funded by the **Government of West Bengal**, 2006-2007.
5. Team member of a project on **“Methods for Estimating Elephant Population in Jal-dapara”** funded by the **Government of West Bengal**, 2006–2007.
6. Team member of a project on **“Life Distribution of Currency Notes”** funded by the **Reserve Bank of India**, 2002–2003.

## 7 International Recognition

### 7.1 International Academic Liasion

1. Since 2001, international faculty for supervising master's degree cadets of **École spéciale militaire de Saint-Cyr, France**.
2. Currently an advisor for setting a centre for cryptography and information security at **Khalifa University, Abu Dhabi** for the government of the **United Arab Emirates**.
3. Since 2001, member of the **International Scientific Advisory Committee** of the **Centre for Applied Cryptography Research, University of Waterloo, Canada**.

### 7.2 Invited Talks in Major International Professional Conferences

1. At the Australasian Conference on Information Security and Privacy, Melbourne, 2002.
2. At the IEEE International Workshop in Information Theory, Bangalore, 2003.
3. At the IEEE International Workshop in Information Theory, Gdansk, Poland, 2008.
4. At Indocrypt, Chennai, 2004.
5. At Indocrypt, IIT-Kharagpur, 2008.
6. Special invited talks at the Chinese Academy of Science, Beijing, 2007.

### 7.3 Editorial Work

1. Associate Editor, **Journal of Ad Hoc & Sensor Wireless Networks**, 2009 onwards.
2. Associate Editor, **Journal of Wireless Sensor Networks**, 2009.
3. A.R. Rao, D.K. Ray-Chaudhuri and Bimal K. Roy (editors). **Special Issue of Discrete Mathematics in honour of R.C. Bose**, 2006.
  - Discrete Mathematics very selectively publishes special issues and it is a great international honour to be an editor for such issues.
4. Bimal K. Roy (editor). **Advances in Cryptology - ASIACRYPT 2005, Volume 3788 of Lecture Notes in Computer Science**, 11th International Conference on the Theory and Application of Cryptology and Information Security, Chennai, India, December 4-8, 2005, Proceedings Springer 2005.
5. Bimal K. Roy, Willi Meier (editors) **Volume 3017 of Lecture Notes in Computer Science**, Fast Software Encryption, 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004, Revised Papers Springer 2004.

- Both Asiacrypt and FSE are flagship conferences of the International Association for Cryptologic Research and a person is invited to chair such conference only once in a lifetime. Chairing two of these conferences is a rare honour shared only a handful of persons internationally.
6. Bimal K. Roy, Eiji Okamoto (editors). Progress in Cryptology - INDOCRYPT 2000, **Volume 1977 of Lecture Notes in Computer Science**, First International Conference in Cryptology in India, Calcutta, India, December 10-13, 2000, Proceedings Springer 2000.
    - This was the first international cryptology conference in India.
  7. Bimal K. Roy, Nicolas Sendrier (editors). Progress in Cryptology - INDOCRYPT 2009, **Volume 5922 of Lecture Notes in Computer Science**, Tenth International Conference in Cryptology in India, Proceedings Springer 2009.
  8. Bimal K. Roy (editor). **Special Issue on Cryptology of the Journal of the Indian Statistical Association**, Volume 42, 2004.
    - This was to motivate the statistics research community about applications of statistics in cryptology.

## 8 Invited International Visits

### 8.1 Regular visitors to the following places

1. French Military Academy, **Rennes, France.**
2. INRIA-Paris, **France.**
3. University of Waterloo, **Canada.**
4. Carleton University, **Canada.**
5. University of Ottawa, **Canada.**
6. Chinese Academy of Sciences, **P.R.C.**
7. University of Science and Technology, **Hong-Kong.**
8. Kyushu University, **Japan.**
9. Tokyo University, **Japan.**

### 8.2 Other visits

1. Lund University, **Sweden.**
2. National University of Singapore, **Singapore.**
3. Warshaw Polytechnic, **Poland.**
4. Gdansk Polytechnic, **Poland.**
5. North Carolina State University, **USA.**
6. Katholieke Universiteit, **Leuven, Belgium.**

## 9 Academic Administration at ISI

### 1. **Dean of Studies, 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 programme 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 modernise the dean's office operations including the starting of OCR based processing of admission test answerscripts.

### 2. **Professor-in-Charge, Applied Statistics Division, 2000-2002, 2008-2010.**

### 3. **Head, Applied Statistics Unit, 2005-2006.**

### 4. **Warden of all the students' hostels, 1987-1998.**

### 5. **Founder of the placement committee.**

- Served as the convenor for the period 1985-1992.
- Carried out negotiations with different industries resulting in making ISI graduates a sought-after brand-name in the relevant industries.

## 10 List of Publications

### 10.1 Journal Publications

1. Sushmita Ruj and Bimal 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.
2. Sushmita Ruj and Bimal Roy. Revisiting Key Predistribution using Transversal Designs for a Grid-based Deployment Scheme: **International Journal of Distributed Sensor Networks**. Volume 5, Number 6, pp 660-674, 2009.
3. Sushmita Ruj and Bimal Roy. Key Predistribution using Partially Balanced Designs in Wireless Sensor Networks: **International Journal of High Performance Computing and Networking (IJHPCN)**, 2009 (To appear).
4. Sushmita Ruj and Bimal Roy. Key Distribution Schemes Using Combinatorial Designs To Identify All Traitors. **Congressus Numerantium**, Volume 193, pp 195-214, 2008.
5. Sushmita Ruj, Subhamoy Maitra and Bimal 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.
6. 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 TRANS. FUNDAMENTALS**. Vol. E90-A, No. 5, May 2007.
7. Dibyendu Chakrabarti, Subhamoy Maitra, Bimal K. Roy. A key pre-distribution scheme for wireless sensor networks: merging blocks in combinatorial design. **International Journal of Information Security**, 5(2): 105-114 (2006).
8. 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**, 2005, 39,4300-4306. Highlighted in News Section of Nature Magazine: Arsenic - free water still a Pipe dream. **NATURE**, Vol. 436, page 313, 21st July 2005.
9. Dibyendu Chakrabarti, Subhamoy Maitra, Bimal K. Roy: Clique Size in Sensor Networks with Key Pre-distribution Based on Transversal Design. **International Journal of Distributed Sensor Networks**, Volume 1, No. 3-4, Pages 345–354, 2005.
10. Bimal K. Roy and Sarbani Palit. Some statistical attacks on stream cipher cryptosystems. **Journal of Indian Statistical Association**, 42 (2004), no. 1, 1–34.
11. Soumen Maity, Amiya Nayak, Bimal K. Roy: Characterization of catastrophic faults in two-dimensional reconfigurable systolic arrays with unidirectional links. **Information Processing Letters**, 92(4): 189-197 (2004).

12. Soumen Maity, Amiya Nayak, Bimal K. Roy: On characterization of catastrophic faults in two-dimensional VLSI arrays. **Integration**, 38(2): 267-281 (2004).
13. Bimal Roy and Sourav Mukhopadhyay. Statistical Cryptanalysis on Block Cipher. **Journal of the Indian Society for Probability and Statistics**, Vol. 7, 2003.
14. Soumen Maity, Bimal K. Roy, Amiya Nayak: On enumeration of catastrophic fault patterns. **Information Processing Letters**, 81(4): 209-212 (2002).
15. Tridib K. Dutta and Bimal K. Roy. Construction of some repeated measurements designs, **Journal of Statistical Planning and Inference**, 95 (2001) pp. 283–291.
16. Soumen Maity, Tridib K. Dutta, Bimal K. Roy. Construction and efficiency of some repeated measurements designs. **Journal of the Indian Statistical Association**, 39 (2001), no. 2, 137–160.
17. Soumen Maity, Bimal K. Roy, Amiya Nayak: Enumerating catastrophic fault patterns in VLSI arrays with both uni- and bidirectional links. **Integration**, 30(2): 157-168 (2001).
18. Soumen Maity, Bimal K. Roy. Construction of some classes of optimal repeated measurements designs. **Calcutta Statistical Association Bulletin**, 50 (2000), no. 197-198, 33–42.
19. Subhamoy Maitra, Bimal K. Roy and Palash Sarkar. Ciphertext only attack on LFSR based encryption scheme. **Calcutta Statistical Association Bulletin**, 49 (1999), no. 195-196, 239–254.
20. Dipankar Basu, Kumar K. Mahalanabis and Bimal 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, January 1998, Pages 809-812.
21. Tridib K. Dutta and Bimal K. Roy. Construction of symmetric balanced squares, **Ars Combinatoria**, Vol. 47 (1997) pp. 49-64.
22. Palash Sarkar, Bimal K. Roy, Pabitra Pal Choudhury. Polynomial division using left shift register **Computers & Mathematics with Applications**, 35 (6): 27-31 MAR 1998.
23. Palash Sarkar and Bimal K. Roy. Construction of nearly balanced uniform repeated measurement designs. **Calcutta Statistical Association Bulletin**, 45 (1995), no. 179-180, 235–243.
24. Indranil Ojha and Bimal K. Roy. **Opsearch**, Vol.31, no.4, 1994, pp 279–295.
25. Tridib K. Dutta, Bimal K. Roy. Construction of strongly balanced uniform repeated measurements designs: a new approach, **Sankhya**, 54, pp 147–153, 1992.
26. Dipankar Basu Kumar K. Mahalanabis and Bimal Roy. Simultaneous spectrophotometric determination of metronidazole and furazolidone with multi standard addition and a least-squares method, **Analytica Chimica Acta**, Volume 249, Issue 2, 1991, Pages 349-352.

27. Anup K. De and Bimal K. Roy. Computer construction of some group divisible designs. **Sankhya, Series-B**, Volume: 52, Part: 1, Page No.: 82–92 Year: 1990.
28. Kumar K. Mahalanabis, Dipankar Basu, Bimal Roy. Application of the least-squares method in the matrix form: simultaneous spectrophotometric determination of rifampicin and isoniazid in binary pharmaceutical formulations. **Analyst**, 1989, (10), 1311-1314.
29. Bimal K. Roy. Construction of strongly balanced uniform repeated measurements designs, **Journal of Statistical Planning and Inference**, 19 (3): 341-348, JUL 1988.
30. J. D. Horton, B. K. Roy, P. J. Schellenberg, and D. R. Stinson. On decomposing graphs into isomorphic uniform 2-factors. **Annals of Discrete Mathematics**, 27 (1985), 297-320.
31. Bimal K. Roy, Kirti R. Shah. On the optimality of a class of minimal covering designs, **Journal of Statistical Planning and Inference**, 10 (2): 189-194, 1984.
32. Ron 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, 35 (DEC): 287-306 1983.
33. Bimal K. Roy. Construction of (M,S)-optimal design for block size 3, **Journal of Statistical Planning and Inference**, Volume 7, Issue 1, October 1982, Pages 35-37.

## 10.2 List of Book Chapters

34. Sushmita Ruj, Jennifer Seberry and Bimal Roy. Key Predistribution using Block Designs. IEEE International Conference on Computational Science and Engineering, CSE '09, Volume 2, pp 873-878, 2009.
35. Sushmita Ruj and Bimal Roy. Key Predistribution Schemes Using Codes in Wireless Sensor Networks. In *Proceedings of the 4th International Conference on Security and Cryptology, INSCRYPT 2008*, Beijing, China, LNCS 5487, pp 275-288, 2008.
36. Sushmita Ruj and Bimal Roy. Key Establishment Algorithms for some Deterministic Key Predistribution Schemes. In *Proceedings of The Sixth Workshop on Security In Information Systems, WOSIS08*, Barcelona, Spain, INSTICC Press, pp 68-77, 2008.
37. Sushmita Ruj and Bimal Roy. Key Predistribution using Partially Balanced Designs in Wireless Sensor Networks. **Lecture Notes in Computer Science**, Springer, Volume 4742, ISPA 2007, 431–445. **Best Paper Award**.
38. Bimal Roy. Book Review On Branch-and-Bound Applications in Combinatorial Data Analysis. **Sankhya**, Volume 68, Part 1, pp 174–175, 2006.
39. Dibyendu Chakrabarti, Subhamoy Maitra, Bimal K. Roy: A Hybrid Design of Key Predistribution Scheme for Wireless Sensor Networks. Volume 3803 of **Lecture Notes in Computer Science**, Springer, ICISS 2005, 228–238.

40. Dibyendu Chakrabarti, Subhamoy Maitra, Bimal K. Roy: A Key Pre-distribution Scheme for Wireless Sensor Networks: Merging Blocks in Combinatorial Design. Volume 3650 of **Lecture Notes in Computer Science**, Springer, ISC 2005, pp 89–103.
41. Dibyendu Chakrabarti, Subhamoy Maitra, Bimal K. Roy: Clique Size in Sensor Networks with Key Pre-distribution Based on Transversal Design. Volume 3741 of **Lecture Notes in Computer Science**, Springer, IWDC 2005, pp 329–337.
42. Soumen Maity, Amiya Nayak, Bimal K. Roy: Reliability of VLSI Linear Arrays with Redundant Links. Volume 3326 of **Lecture Notes in Computer Science**, Springer, IWDC 2004, pp 326–337.
43. Avishek Adhikari, Tridib Kumar Dutta, Bimal K. Roy: A New Black and White Visual Cryptographic Scheme for General Access Structures. Volume 3348 of **Lecture Notes in Computer Science**, Springer, INDOCRYPT 2004, pp 399–413.
44. Sarbani Palit, Bimal K. Roy, Arindom De: A Fast Correlation Attack for LFSR-Based Stream Ciphers. Volume 2846 of **Lecture Notes in Computer Science**, Springer, ACNS 2003, pp 331–342.
45. Bimal K. Roy. Summarizing Recent Results on Finding Multiples of Primitive Polynomials over  $GF(2)$ . Information Theory Workshop, 2002.
46. Bimal K. Roy: A Brief Outline of Research on Correlation Immune Functions. Volume 2384 of **Lecture Notes in Computer Science**, Springer, ACISP 2002, pp 379–394.
47. 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. **Congr. Numer.**, 151 (2001), pp 41–52.
48. Sarbani Palit, Bimal K. Roy: Cryptanalysis of LFSR-Encrypted Codes with Unknown Combining Function. Volume 1716 of **Lecture Notes in Computer Science**, Springer, ASIACRYPT 1999, pp 306–320.
49. Palash Sarkar, Bimal K. Roy, Pabitra Pal Choudhury: VLSI Implementation of Modulo Multiplication Using Carry Free Addition. **VLSI Design 1997**, pp 457–460.