Goutam Kumar Paul

goutam.k.paul@gmail.com http://www.goutampaul.com +91 94333 21887

Current Affiliation

Assistant Professor, R. C. Bose Centre for Cryptology and Security, Indian Statistical Institute, Kolkata 700 108, India. [Aug 8, 2013 – to date]

Education

Ph.D. in the area of Cryptology [2006 – 2008]

Thesis submitted: December 12, 2008; Thesis Defense: May 20, 2009.
Dissertation: Analysis and Design of RC4 and Its Variants.
Advisor: Prof. Subhamoy Maitra, ASU, ISI, Kolkata.
Note: doctoral work done at ISI, degree obtained from JU
(secured **Junior Research Fellowship at ISI Kolkata** in 2006, but could not join as I was already an Assistant Professor at Jadavpur University).

M.S. in Computer Science [2001 – 2003]

Department of Computer Science, University at Albany, State University of New York (SUNY), U.S.A. GPA: 3.97/4.
Ranked 1st in the Master's Comprehensive Examination.

B.E. in Computer Engineering [1997 – 2001]

Department of Computer Science & Technology, Bengal Engineering College, now Bengal Engineering and Science University (BESU).
Division: First. Marks: 84.36%.
Ranked 1st in the Department (**Ranked 2nd in the University across all Departments**).

Higher Secondary Examination (10+2 Board Examination) [1997]

St. Xavier's College, Kolkata, India, under West Bengal Council of Higher Secondary Education (WBCHSE). Division: First. Marks: 85.10%.
Ranked 42nd (out of over 3,50,000 examinees) **in the Board**.

Secondary Examination (10 Board Examination) [1995]

New Alipore Multipurpose School, Kolkata, India, under West Bengal Board of Secondary Education (WBBSE). Division: First. Marks: 92.56%.
Ranked 2nd (out of over 5,00,000 examinees) **in the Board**.

Awards and Achievements

(Selected list)

1. **Young Scientist** Platinum Jubilee Award, National Academy of Sciences, India (**NASI**). [2013]
2. **Humboldt Fellow**, Alexander von Humboldt-Stiftung, Germany. [2012]
3. **DAAD Fellow**, Deutscher Akademischer Austausch Dienst (German Academic Exchange Service), Germany. [2012]
4. **Qualified the Junior Research Fellowship (JRF) selection test and interview for Ph.D. admission** in Computer and Communication Sciences, Indian Statistical Institute (ISI), Kolkata, India (did not join). [2006]
5. **Ranked 1st in the interview for Ph.D. admission**, Department of Computer Science & Automation, Indian Institute of Science (IISc), Bangalore, India (did not join). [2006]
6. **Ranked 1st in the selection test and interview for Ph.D. (Institute Scholar) admission**, Department of Computer Science & Engineering, Indian Institute of Technology (IIT), Kharagpur, India (did not join). [2006]
7. **Qualified** the University Grants Commission (India) National Eligibility Test (**UGC-NET**) for Junior Research Fellowship (JRF) and Lectureship in Computer Science & Applications. [2005]
8. **Leadership Award from Graduate Student Organization** (GSO), SUNY Albany, U.S.A. [2005]
9. **Ranked 1st in the Master's Comprehensive Examination**, SUNY Albany, U.S.A. [2002]
10. **Full scholarship offers for doctoral study** from four Universities in U.S.A.: (i) University of Arizona, Tucson, (ii) University of California, Irvine, (iii) University of Memphis, Tennessee, and (iv) State University of New York, Albany. [2001]
11. **Ranked 174th in the Country** (India) in Graduate Aptitude Test in Engineering, Computer Science (**GATE CS**). [2001]
12. **Ranked 1st in B.E. in the Department** of Computer Science & Technology of Bengal Engineering College, Howrah, India. [2001]
13. **Ranked 133rd in the State** (West Bengal, India) **in Joint Entrance Examination (Engg.)**. [1997]
14. **Ranked 42nd** (*out of over 3,50,000 examinees*) **in the State** (West Bengal, India) **in Higher Secondary Examination** (Board: WBCHSE). [1997]
15. **Ranked 2nd** (*out of over 5,00,000 examinees*) **in the State** (West Bengal, India) **in Secondary Examination** (Board: WBBSE). [1995]

Publications

∗ : *Conference publications that were subsequently extended to journal papers.*
\# : *Post-Ph.D. works.*
I : *Independent works in which the Ph.D. advisor is not a co-author; amongst these, the works with my students are marked* **I**.

Book

1. (#) Goutam Paul and Subhamoy Maitra. RC4 Stream Cipher and Its Variants. CRC Press, 1st Edition, November 16, 2011.

Publications in Refereed International Journals

2. (**I**#) Tamaghna Acharya and Goutam Paul. Maximum Lifetime Broadcast Communications in Cooperative Multihop Wireless Ad Hoc Networks: Centralized and Distributed Approaches. In *Ad Hoc Networks* (Elsevier), pages 1667–1682, vol. 11, issue 6, August 2013.
3. (**I**#) Arpita Maitra and Goutam Paul. Eavesdropping in Semiquantum Key Distribution Protocol. In *Information Processing Letters* (Elsevier), pages 418–422, vol. 113, issue 12, June 30, 2013.
4. (#) Sourav Sen Gupta, Subhamoy Maitra, Goutam Paul and Santanu Sarkar. (Non-)Random Sequences from (Non-)Random Permutations - Analysis of RC4 stream cipher. To appear in *Journal of Cryptology* (Springer), accepted November 3, 2012.
5. (**I**#) Miodrag Mihaljevic, Sugata Gangopadhyay, Goutam Paul, Hideki Imai. Generic Cryptographic Weakness of k-normal Boolean Functions in Certain Stream Ciphers and Cryptanalysis of Grain-128. In *Periodica Mathematica Hungarica* (Springer), pages 205–227, vol. 65, issue 2, December, 2012.
6. (**I**#) Miodrag Mihaljevic, Sugata Gangopadhyay, Goutam Paul and Hideki Imai. Internal State Recovery of Keystream Generator LILI-128 Based on a Novel Weakness of the Employed Boolean Function. In *Information Processing Letters* (Elsevier), pages 805–810, vol. 112, no. 21, November 15, 2012.
7. (**I**#) Miodrag Mihaljevic, Sugata Gangopadhyay, Goutam Paul and Hideki Imai. Internal State Recovery of Grain-v1 Using Normality Order of the Filter Function. In *IET Information Security*, pages 55–64, vol. 6, no. 2, June, 2012.
8. (#) Subhamoy Maitra, Goutam Paul, Shashwat Raizada, Subhabrata Sen and Rudradev Sengupta. Some Observations on HC-128. In *Designs, Codes and Cryptography* (Springer), pages 231–245, vol. 59, no. 1–3, April, 2011.
9. (**I**#) Sayan Bhattacharya, Goutam Paul and Swagato Sanyal. A Cops and Robber Game in Multidimensional Grids. In *Discrete Applied Mathematics* (Elsevier), pages 1745–1751, vol. 158, no. 16, August, 2010.
10. Goutam Paul and Subhamoy Maitra. On Biases of Permutation and Keystream Bytes of RC4 towards the Secret Key. In *Cryptography and Communications* (Springer), pages 225–268, vol. 1, no. 2, September, 2009.

11. Goutam Paul, Siddheshwar Rathi and Subhamoy Maitra. On Non-negligible Bias of the First Output Byte of RC4 towards the First Three Bytes of the Secret Key. In *Designs, Codes and Cryptography* (Springer), pages 123–134, vol. 49, no. 1–3, December, 2008.
12. Riddhipratim Basu, Shirshendu Ganguly, Subhamoy Maitra, Goutam Paul. A Complete Characterization of the Evolution of RC4 Pseudo Random Generation Algorithm. In *Journal of Mathematical Cryptology* (de Gruyter), pages 257–289, vol. 2, no. 3, October, 2008.

Publications in Refereed International Conferences

13. (I#) Imon Mukherjee and Goutam Paul. Efficient Multi-bit Image Steganography in Spatial Domain. In Proceedings of the 9th International Conference on Information Systems Security (ICISS), Dec 16-20, 2013, Kolkata, India, pages 270–284, vol. 8303, Lecture Notes in Computer Science (LNCS), Springer.
14. (**I#**) Ayesha Khalid, Muhammad Hassan, Anupam Chattopadhyay and Goutam Paul. RAPID-FeinSPN: A Rapid Prototyping Framework for Feistel and SPN-Based Block Ciphers. In Proceedings of the 9th International Conference on Information Systems Security (ICISS), Dec 16-20, 2013, Kolkata, India, pages 169–190, vol. 8303, LNCS, Springer.
15. (I#) Shubhajit Saha and Goutam Paul. On Effective Sharing of User Generated Content. To appear in Proceedings of the 11th Asia Pacific Conference on Computer Human Interaction (APCHI), September 24-27, 2013, Bangalore, India.
16. (**I#**) Goutam Paul and Soumi Paul. Proposal for a Novel Computerized Menu-Presentation Interface for Restaurants. To appear in Proceedings of the 11th Asia Pacific Conference on Computer Human Interaction (APCHI), September 24-27, 2013, Bangalore, India.
17. (**I#**) Ayesha Khalid, Goutam Paul and Anupam Chattopadhyay. New Speed Records for Salsa20 Stream Cipher using an Autotuning Framework on GPUs. In Proceedings of the 6th International Conference on Cryptology in Africa (AFRICACRYPT), June 22-24, 2013, Cairo, Egypt, pages 189–207, vol. 7918, LNCS, Springer.
18. (#) Subhamoy Maitra, Goutam Paul, Santanu Sarkar, Michael Lehmann and Willi Meier. New Results on Generalization of Roos-type Biases and Related Keystream of RC4. In Proceedings of the 6th International Conference on Cryptology in Africa (AFRICACRYPT), June 22-24, 2013, Cairo, Egypt, pages 222–239, vol. 7918, LNCS, Springer.
19. (**I#**) Khawar Shahzad, Ayesha Khalid, Zoltán Endre Rákossy, Goutam Paul and Anupam Chattopadhyay. CoARX: A Coprocessor for ARX-based Cryptographic Algorithms. In Proceedings of the 50th ACM/IEEE Design Automation Conference (DAC), June 2-6, 2013, Austin, U.S.A., Article No. 133, ACM.
20. (I#) Arpita Maitra and Goutam Paul. Symmetric Incoherent Eavesdropping against MDI QKD. In Proceedings of the International Workshop on Coding and Cryptography (WCC), April 15-19, 2013, Bergen, Norway, pages 413–426.
21. (I#) Ayesha Khalid, Deblin Bagchi, Goutam Paul and Anupam Chattopadhyay. Optimized GPU Implementation and Performance Analysis of HC Series of Stream Ciphers. In Proceedings of the 15th International Conference on Information Security and Cryptology (ICISC), November 28-30, 2012, Seoul, Korea, pages 293–308, vol. 7839, LNCS, Springer.
22. (I#) Goutam Paul, Ian Davidson, Imon Mukherjee and S. S. Ravi. Keyless Steganography in Spatial Domain using Energetic Pixels. In Proceedings of the 8th International Conference on Information Systems Security (ICISS), Dec 15-19, 2012, Guwahati, India, pages 134–148, vol. 7671, LNCS, Springer.

23. (I#) Arpita Maitra and Goutam Paul. Another Look at Symmetric Incoherent Optimal Eavesdropping against BB84. In Proceedings of the 13th International Conference on Cryptology in India (INDOCRYPT), December 9-12, 2012, Kolkata, India, pages 80–99, vol. 7668, LNCS, Springer.
24. (**I#**) Goutam Paul and Shashwat Raizada. Impact of Extending Side Channel Attack on Cipher Variants: A Case Study with the HC Series of Stream Ciphers. In Proceedings of International Conference on Security, Privacy and Applied Cryptography Engineering (SPACE), November 2-3, 2012, Chennai, India, pages 32–44, vol. 7644, LNCS, Springer.
25. (**I#**) Anupam Chattopadhyay and Goutam Paul. Exploring Security-Performance Tradeoffs during Hardware Accelerator Design of Stream Cipher RC4. In Proceedings of the 20th IFIP/IEEE International Conference on Very Large Scale Integration and System-on-Chip (VLSI-SoC), October 7-10, 2012, Santa Cruz, U.S.A., pages 251–254.
26. (I#) Goutam Paul and Imon Mukherjee. Sterilization of Stego-images through Histogram Normalization. In Proceedings of the 11th International Conference on Security and Management (SAM), July 16-19, 2012, Las Vegas, U.S.A., pages 448–454.
27. (#) Apurba Das, Subhamoy Maitra, Goutam Paul and Santanu Sarkar. Some Combinatorial Results Towards State Recovery Attack on RC4. In Proceedings of the 7th International Conference on Information Systems Security (ICISS), Dec 15-19, 2011, Kolkata, India, pages 204–214, vol. 7093, LNCS, Springer.
28. (#) Goutam Paul, Subhamoy Maitra and Shashwat Raizada. A Theoretical Analysis of the Structure of HC-128. In Proceedings of the 6th International Workshop on Security (IWSEC), November 8-10, 2011, Tokyo, Japan, pages 161–177, vol. 7038, LNCS, Springer.
29. (#∗) Sourav Sen Gupta, Subhamoy Maitra, Goutam Paul and Santanu Sarkar. Proof of Empirical RC4 Biases and New Key Correlations. In Proceedings of the 18th Workshop on Selected Areas in Cryptography (SAC), August 11-12, 2011, Toronto, Canada, pages 151–168, vol. 7118, LNCS, Springer.
30. (I#) Imon Mukherjee and Goutam Paul. Double Bit Sterilization of Stego-images. In Proceedings of the 10th International Conference on Security and Management (SAM), July 18-21, 2011, Las Vegas, U.S.A., pages 743–746.
31. (**I#**∗) Miodrag Mihaljevic, Sugata Gangopadhyay, Goutam Paul, Hideki Imai. An Algorithm for the Internal State Recovery of Grain-v1. In 11th Central European Conference on Cryptology (CECC), June 30-July 2, 2011, Debrecen, Hungary.
32. (#∗) Subhamoy Maitra, Goutam Paul and Sourav Sen Gupta. Attack on Broadcast RC4 Revisited. In Proceedings of the 18th Fast Software Encryption (FSE) Workshop, February 13-16, 2011, Lyngby, Denmark, pages 199–217, vol. 6733, LNCS, Springer.
33. (**I#**) Miodrag Mihaljevic, Sugata Gangopadhyay, Goutam Paul, Hideki Imai. A Generic Weakness of the k-normal Boolean Functions Exposed to Dedicated Algebraic Attack. In Proceedings of the 11th International Symposium on Information Theory and its Applications (ISITA), October 17-20, 2010, Taichung, Taiwan, pages 911–916.
34. (**I#**) Shashwat Raizada, Goutam Paul and Vineet Pandey. Nearby-Friend Discovery Protocol for Multiple Users. In Proceedings of the 2009 IEEE International Conference on Computational Science and Engineering (CSE), vol. 3, Track: International Symposium on Secure Computing (SecureCom 2009), August 29-31, 2009, Vancouver, Canada, pages 238–243, IEEE Computer Society Press.

35. (#) Riddhipratim Basu, Subhamoy Maitra, Goutam Paul and Tanmoy Talukdar. On Some Sequences of the Secret Pseudo-random Index j in RC4 Key Scheduling. In Proceedings of the 18th International Symposium on Applied Algebra, Algebraic Algorithms and Error Correcting Codes (AAECC), June 8-12, 2009, Tarragona, Spain, pages 137–148, vol. 5527, LNCS, Springer.
36. (#∗) Subhamoy Maitra, Goutam Paul and Shashwat Raizada. Some Observations on HC-128. In Proceedings of the International Workshop on Coding and Cryptography (WCC), May 10-15, 2009, Ullensvang, Norway, pages 527–539.
37. Subhamoy Maitra and Goutam Paul. Analysis of RC4 and Proposal of Additional Layers for Better Security Margin. In Proceedings of the 9th International Conference on Cryptology in India (INDOCRYPT), December 14-17, 2008, Indian Institute of Technology, Kharagpur, India, pages 27–39, vol. 5365, LNCS, Springer.
38. Subhamoy Maitra and Goutam Paul. Recovering RC4 Permutation from 2048 Keystream Bytes if j is Stuck. In Proceedings of the 13th Australasian Conference on Information Security and Privacy (ACISP), July 7-9, 2008, Wollongong, Australia, pages 306–320, vol. 5107, LNCS, Springer.
39. (∗) Riddhipratim Basu, Shirshendu Ganguly, Subhamoy Maitra, Goutam Paul. RC4 Keystream Always Leaks Information about the Hidden Index j. In Proceedings of the State of the Art of Stream Ciphers (SASC), special Workshop hosted by ECRYPT, the European Network of Excellence in Cryptography, February 13-14, 2008, Lausanne, Switzerland, pages 233–247.
40. (∗) Subhamoy Maitra and Goutam Paul. New Form of Permutation Bias and Secret Key Leakage in Keystream Bytes of RC4. In Proceedings of the 15th Fast Software Encryption (FSE) Workshop, February 10-13, 2008, Lausanne, Switzerland, pages 253–269, vol. 5086, LNCS, Springer.
41. Goutam Paul, Subhamoy Maitra and Rohit Srivastava. On Non-Randomness of the Permutation after RC4 Key Scheduling. In Proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error Correcting Codes (AAECC), December 16-20, 2007, Bangalore, India, pages 100–109, vol. 4851, LNCS, Springer.
42. (∗) Goutam Paul and Subhamoy Maitra. Permutation after RC4 Key Scheduling Reveals the Secret Key. In Proceedings of the 14th Workshop on Selected Areas in Cryptography (SAC), August 16-17, 2007, Ottawa, Canada, pages 360–377, vol. 4876, LNCS, Springer.
43. (I∗) Sayan Bhattacharya, Goutam Paul and Swagato Sanyal. On Necessary and Sufficient Number of Cops in the Game of Cops and Robber in Multidimensional Grids. In 8th Asian Symposium on Computer Mathematics (ASCM), December 15-17, 2007, Singapore.
44. (∗) Goutam Paul, Siddheshwar Rathi and Subhamoy Maitra. On Non-negligible Bias of the First Output Byte of RC4 towards the First Three Bytes of the Secret Key. In Proceedings of the International Workshop on Coding and Cryptography (WCC), April 16-20, 2007, Versailles, France, pages 285–294.
45. (**I**) Goutam Paul. Occam's Razor and a Non-syntactic Measure of Decision Tree Complexity. In Proceedings of the 19th National Conference on Artificial Intelligence (AAAI), July 25-29, 2004, San Jose, California, U.S.A., pages 962–963.
46. (**I**) Ian Davidson and Goutam Paul. Locating Secret Messages in Images. In Proceedings of the 10th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD), August 22-25, 2004, Seattle, Washington, U.S.A., pages 545–550.

47. (**I**) George Berg, Ian Davidson, Ming-Yuan Duan and Goutam Paul. Searching for Hidden Messages: Automatic Detection of Steganography. In Proceedings of the 15th Innovative Applications of Artificial Intelligence (IAAI) Conference, August 12-14, 2003, Acapulco, Mexico, pages 51–56.
48. (**I**) Somnath Pal, Tridib Kumar Saha, Goutam K. Paul, Chinmay Maiti and Ananda Mohan Ghosh. Multi-method Decision Tree Learning for Data Mining. In Proceedings of the 28th Annual Convention and Exhibition of IEEE India Council (IEEE-ACE), December 20-21, 2002, Science City, Kolkata, India, pages 238–242.

Pre-Prints / Other Publications (Selected list)

49. (**I#**) Goutam Paul, Anupam Chattopadhyay and Chander Chandak. Designing Parity Preserving Reversible Circuits. In arXiv.org e-Print Archive, arXiv:1308.0840v1 [cs.AR], August 4, 2013.
50. (**I#**) Goutam Paul and Anupam Chattopadhyay. Three Snakes in One Hole: A 67 Gbps Flexible Hardware for SOSEMANUK with Optional Serpent and SNOW 2.0 Modes. In IACR ePrint Archive, Report 2013/282, May 14, 2013.
51. (**I#**) Sounak Gupta and Goutam Paul. Revisiting Fermats Factorization for the RSA Modulus. In arXiv.org e-Print Archive, arXiv:0910.4179v1 [cs.CR], October 21, 2009.
52. (**I#**) Adway Mitra, Goutam Paul and Ushnish Sarkar. Some Conjectures on the Number of Primes in Certain Intervals. In arXiv.org e-Print Archive, arXiv:0906.0104v1 [math.NT], May 30, 2009.
53. (**I**) Goutam Paul. Artificial Intelligence and Consciousness. In 2nd Human-E-Tech Conference, April 23-25, 2004, SUNY Albany, U.S.A.

Research Experience

Research Positions

1. **Visiting Scientist**, Multi-Processor System-on-Chip (MPSoC) Architectures Research Group, Ultra High-Speed Mobile Information and Communication (UMIC) Research Centre, RWTH Aachen University, Aachen, Germany. [Jun 2012 – Jul 2013]
2. **Visiting Research Scientist**, Crypto and Security group, Department of Electrical and Information Technology, Lund University, Sweden. [Mar 2013]
3. **Visiting Research Scientist**, Security and Cryptography Laboratory (LASEC), School of Computer and Communication Sciences (I&C), Ecole Polytechnique Fédérale de Lausanne (EPFL), Switzerland. [Feb 2013]
4. **Visiting Research Scientist**, Fachhochschule Nordwestschweiz (FHNW), Windisch, Switzerland. [Oct 2012]
5. **Visiting Scientist**, Centre of Excellence in Cryptology, Indian Statistical Institute, Kolkata, India. [Sep 2011 – May 2012]

6. **Visiting Research Scientist**, Research Center for Information Security (RCIS), National Institute of Advanced Industrial Science and Technology (AIST), Tokyo & Tsukuba, Japan. [Jun – Jul 2009, Feb – Mar 2010, Feb & Nov 2011]
7. **Visiting Research Scientist**, Coding & Cryptography Research Group (CCRG), Division of Mathematical Sciences, School of Physical & Mathematical Sciences, Nanyang Technological University (NTU), Singapore. [Mar 2010]
8. **Visiting Research Scientist**, Information Technology and Security Laboratory (Sakurai Laboratory) of the Kyushu University and the Information Security Laboratory of the Institute of the Systems, Information Technologies and Nanotechnologies (ISIT), Fukuoka, Japan. [Jul 2009]
9. **Visiting Researcher**, Center of Applied Cryptographic Research (CACR), University of Waterloo, Ontario, Canada. [Jul – Aug 2007]
10. **Research Fellow**, Cryptology Research Group (CRG), Applied Statistics Unit (ASU), Indian Statistical Institute (ISI), Kolkata, India. [Sep 2006 – Dec 2008]
11. **Research Associate**, Brain-Computer Interface Lab, Wadsworth Center, New York State Department of Health, New York, U.S.A. [Jul – Dec 2004]
12. **Research Assistant**, Department of Computer Science, University at Albany, State University of New York, U.S.A. [Jul – Aug 2003, Jan – May 2004]
13. **Research Assistant**, Electronics and Communication Science Unit, Indian Statistical Institute (ISI), Kolkata, India. [Aug – Dec 2000]
14. **Summer Intern**, Applied Statistics Unit, Indian Statistical Institute (ISI), Kolkata, India. [Jun – Jul 2000]

Student Supervision

- No. of registered Ph.D. students: 3 (ongoing).
- No. of Master's Theses supervised: 4 (completed) + 1 (ongoing).

Sponsored Research Projects

1. *Threat and Attack Modeling of Heterogeneous Enterprise Networks.*
   Duration: 18 months (2011-2013).
   Funding Agency: Sceintific Analysis Group (SAG), Defence Research & Development Organisation (DRDO), Delhi, Ministry of Defence, Government of India.
   Role: **Consultant**.
2. *Development of Encryption Algorithm for BARC.*
   Duration: 24 months (2011-2013).
   Funding Agency: Bhabha Atomic Research Centre (BARC), Mumbai, India.
   Role: **Project Member**.
3. *Development of Tool and Design Aid for Developing Safe Guards against Related Key and IV Attacks and Proactive Key Scheduling Scheme for Packet Encryption.*
   Duration: 15 months (2010-2012).
   Funding Agency: Defence Research & Development Organisation (DRDO), Ministry of

Defence, Government of India.
Role: **Principal Investigator**.

4. *Security Evaluation and Design of Components and Cryptographic Primitives for RFID and Sensor Networks.*
   Duration: 3 years (2009-2012).
   Funding Agency: Department of Science and Technology (DST), Government of India and Japan Science and Technology (JST) Agency, the National Organization in Japan for implementing the Science and Technology Policies of the Government of Japan.
   Role: **Member of the Indian team of four scientists**.
5. *Steganography using Machine Learning.*
   Duration: 1 year (2006-2007).
   Funding Agency: Jadavpur University.
   Role: **Principal Investigator**.

Teaching Experience

Teaching Positions

1. **Assistant Professor**, Department of Computer Science & Engineering, Jadavpur University, Kolkata, India. [Jul 2006 – Aug 2013]
2. **Visiting Professor**, Computer & Communication Sciences Division, Indian Statistical Institute (ISI), Kolkata, India. [Jan – May 2010]
3. **Visiting Lecturer**, Department of Computer Science & Technology, Bengal Engineering & Science University, Howrah, India. [Jan – May, 2009 & 2010]
4. **Lecturer**, Department of Computer Science & Engineering, St. Thomas' College of Engineering & Technology, Kolkata, India. [Aug 2005 – Jul 2006]
5. **Adjunct Faculty**, Department of Computer Science, University at Albany, State University of New York (SUNY), U.S.A. [Summer 2003 & 2004]
6. **Teaching Assistant**, Department of Computer Science, University at Albany, State University of New York (SUNY), U.S.A. [Aug 2001 – Dec 2003, Aug 2004 – Jun 2005]

Subjects Taught

Master's Level	Bachelor's Level
Information Security	Cryptography & Computer Security
Information & Coding Theory	Formal Language & Automata Theory
Analysis & Design of Algorithms	Discrete Structures / Discrete Mathematics
Operating Systems	Data Structures
Computer Networks	Programming Languages
Application Software	Elements of Computing
Artificial Intelligence	Soft Computing
	System Analysis & Design / Software Engineering
	Computer Graphics
	Numerical Analysis
	Programming at the HW-SW Interface

Extended Academic Activities

Editorial Work

- **Contribution in preparing the International Edition** of the book "Computer Networking", 6th Edition, James F. Kurose and Keith W. Ross, Pearson International Edition. [May 2012]
- **Contribution in preparing the International Edition** of the book "Operating Systems: Internals and Design Principles", 7th Edition, William Stallings, Pearson International Edition. [May 2011]
- **Program Co-Chair**, 14th International Conference on Cryptology in India (INDOCRYPT), December 7-10, 2013, Mumbai, India. [2013]
- **Program Committee Member of refereed international conferences**: ACNS 2014, INDOCRYPT 2012, AFRICACRYPT 2012, ICISS 2011, InfoSecHiComNet 2011, IEEE INDICON 2010, INDOCRYPT 2010.
- Regular **reviewer of refereed international journals** like JOC, IEEE-IT, DCC, CCDS etc. and **refereed international conferences** like CRYPTO, EUROCRYPT, ASIACRYPT, FSE, SAC, WCC, INDOCRYPT etc.
- **Executive Editor**, *Computer Jagat* Magazine, Online Issue (English Version). [Dec 2008]

Organisational Activities

1. **Membership in Professional Bodies**:
   (a) Member, Institute of Electrical and Electronics Engineers (IEEE). [2009 – to date]
   (b) Member, Cryptology Research Society of India (CRSI). [2006 – to date]
2. **Session Chair**, 9th International Conference on Information Systems Security (ICISS, Dec 16-20, 2013), Session: Cryptography-1, December 19, 2013, Kolkata, India. [2013]

3. **Session Chair**, 6th International Conference on Cryptology in Africa (AFRICACRYPT, June 22-24, 2013), Session: Efficient Implementations for ECC, June 22, 2013, Cairo, Egypt. [2013]
4. **Program Coordinator**, Software Freedom with Google Summer of Code, a one-day awareness programme for the students of all disciplines of all colleges and Universities in Kolkata, May 22, 2012, Jadavpur University, Kolkata, India. [2012]
5. **Program Coordinator**, Workshop on Information and Security in Quantum World, organized by the Centre of Excellence in Cryptology, Indian Statistical Institute, March 28-30, 2012, Indian Statistical Institute, Kolkata, India. [2012]
6. Played **key role in preparing the draft proposal of the UGC XIIth Plan requirements** of the Department of Computer Science & Engineering, Jadavpur University, Kolkata, India. [2012]
7. **Convener & Program Coordinator**, Tutorial Workshop on Many Facets of Cryptology, jointly organized by the Department of Computer Science & Engineering, Jadavpur University and the Centre of Excellence in Cryptology, Indian Statistical Institute, October 14-15, 2011, Jadavpur University, Kolkata, India. [2011]
8. **Session Chair**, Indo-Japan Joint Workshop on Cryptography, December 12, 2009, Indian Statistical Institute, Delhi. [2009]
9. **Tutorial Chair**, 2nd National Conference on Recent Trends in Information Systems (ReTIS), February 7-9, 2008, Kolkata, India. [2008]
10. **Publicity Chair**, 9th International Conference on Distributed Computing and Networking (ICDCN), January 5-8, 2008, Kolkata, India. [2008]
11. **Local Organizer**, 7th International Conference on Cryptology in India (INDOCRYPT), December 11-13, 2006, Kolkata, India. [2006]
12. **Senator** at the University Senate (*one of the three student members nominated by the Graduate Student Organization*), SUNY Albany, U.S.A. [2004 – 2005]
13. **Council Member**, Resource Analysis and Planning Committee, University Planning and Policy Council (*the only student member nominated by the Graduate Student Organization*), SUNY Albany, U.S.A. [2004 – 2005]
14. **Department Representative / Mobilizer**, Graduate Student Employees Union, SUNY Albany, U.S.A. [2004 – 2005]

Curriculum Development

1. **Designed and Introduced** an elective course entitled **Cryptography and Computer Security** for B.E. 3rd year students of Dept. of Computer Science & Engineering, Jadavpur University, Kolkata, India. [2010]
2. **Designed and Introduced** an elective course entitled **Information Security** for M.E. 1st year students of Dept. of Computer Science & Engineering, Jadavpur University, Kolkata, India. [2009]
3. Played **key role in thorough revision of the syllabi for B.E., M.E. and M.C.A. courses**, while serving as an **active member of the Curriculum Development Subcommittee** under the Board of Studies of the Dept. of Computer Science & Engineering, Jadavpur University, Kolkata, India. [2009 – 2012]

External Expert Service

- **Selection Committee Member**
  1. Recruitment of Research Consultants and Personnels for the Centre of Excellence in Cryptology, Indian Statistical Institute, Kolkata. [April 19, 2012]
  2. Recruitment of Research Consultants and Personnels for the Centre of Excellence in Cryptology, Indian Statistical Institute, Kolkata. [July, 2011]
  3. Recruitment of Project Assistants for the project "Indexing, digital imaging and online hosting of photo images in ISI repository" in Reprography & Photography Unit, Indian Statistical Institute, Kolkata. [May 20, 2011]
  4. Recruitment of Computer faculty, West Bengal State Cooperative Union, Salt Lake, Kolkata. [Sep 16, 2010]
- **Moderator** for the paper "Information and Coding Theory" in M. Tech. (Computer Science), Indian Statistical Institute, Kolkata. [2011]
- **Paper Setter and Examiner** for the paper "Discrete Mathematical Structure" in M.Sc. (Mathematics), Visva-Bharati University. [2006 – 2010]
- **Master's Thesis Evaluation**
  1. Department of Computer Science & Technology, Bengal Engineering and Science University (BESU). [2007 – 2011]
  2. Department of Electronics & Telecommunication Engineering, Bengal Engineering and Science University (BESU). [2009 – 2011]

Invited Talks

(Excluding Paper Presentations at Conferences / Workshops)

On Quantum Information and Security

1. No Cloning Theorem and Quantum Key Distribution.
   Seminar at the Department of Mathematics, Birla Institute of Technology and Science (BITS) Pilani, K. K. Birla Goa campus, Goa, India, December 6, 2013.
2. Classical Cryptography in a Quantum World.
   Seminar at the Satellite Meeting on Quantum Correlation and Its Possible Application in Communication and Cryptography (Sep 2-3, 2013), Indian Statistical Institute (ISI), Kolkata, India, September 2, 2013.
3. Architectural and Implementation Issues of Robust Cryptosystems in the Quantum Era: A Case Study.
   Seminar at the Network Meeting of the Alexander von Humboldt Foundation (November 28-30, 2012), Institute of Theoretical Informatics, Karlsruher Institut für Technologie (KIT), Karlsruhe, Germany, November 29, 2012.

4. Pseudo-Random Generators: from Classical to Quantum Security.
   Seminar at the Ultra High-Speed Mobile Information and Communication (UMIC) Research Centre, Rheinisch-Westfaelische Technische Hochschule (RWTH) Aachen, Germany, July 11, 2012.
5. Protecting Privacy: from Stone-age to Quantum World.
   Seminar for the Faculty Members of the Department of Computer Science & Engineering, the Department of Information Technology and the Department of Master of Camputer Application, Siliguri Institute of Technology, Siliguri, India, January 20, 2012.
6. Four-State BB84 is as Secure as the Six-State Protocol.
   Security Fundamentals (SF) Meeting, Research Center for Information Security (RCIS), National Institute of Advanced Industrial Science and Technology (AIST), Tsukuba, Japan, November 15, 2011.

On Classical Cryptology

7. Introduction to Block Ciphers.
   Lecture at Staff Development Programme on Cryptography & Information Security (Sep 21-25, 2013), Govt. College of Engineering & Textile Technology - Berhampore, Murshidabad, India, Sep 22, 2013.
8. Introduction to Cryptology.
   Lecture at Staff Development Programme on Cryptography & Information Security (Sep 21-25, 2013), Govt. College of Engineering & Textile Technology - Berhampore, Murshidabad, India, Sep 21, 2013.
9. Biases and Distinguishers of the RC4 Stream Cipher. Seminar at Crypto and Security group, Department of Electrical and Information Technology, Lund University, Sweden, March 27, 2013.
10. A Look into (Non-)Randomness of RC4 Stream Cipher. Theory Seminar at Center for the Theory of Interactive Computation (CTIC), Aarhus University, Denmark, March 22, 2013.
11. The RC4 Landscape: Hills, Canyons and Plateaus.
    Seminar at Security and Cryptography Laboratory (LASEC), School of Computer and Communication Sciences (I&C), Ecole Polytechnique Fédérale de Lausanne (EPFL), Switzerland, February 8, 2013.
12. Connection between Information Theory and Security.
    Seminar at the Institute for Communication Technologies and Embedded Systems (ICE), Rheinisch-Westfaelische Technische Hochschule (RWTH) Aachen, Germany, June 26, 2012.
13. An Overview of Classical Information and Classical Cryptography.
    Workshop on Information and Security in Quantum World (March 28-30, 2012), Indian Statistical Institute, Kolkata, India, March 28, 2012.
14. Statistics in Cryptology.
    Seminar for one-week visit to Indian Statistical Institute, Kolkata, India, by the students of Post Graduate Diploma in Statistical Methods with Applications, Indian Statistical Institute North East Centre, Tezpur, Applied Statistics Unit (ASU), Indian Statistical Institute (ISI), Kolkata, India, December 7, 2011.
15. Distinguishing Attacks on Stream Ciphers.
    ASU Seminar Series, Applied Statistics Unit (ASU), Indian Statistical Institute (ISI), Kolkata, India, November 29, 2011.

16. Trivial and Non-trivial Issues of TRIVIUM.
    Workshop on eSTREAM Ciphers (Sep 30-Oct 1, 2011), Indian Statistical Institute, Delhi Centre, India, September 30, 2011.
17. Stream Ciphers: from One Time Pad to 4G.
    National Level Workshop on Cryptology (September 29-30, 2011) for College and University Teachers and Students, West Bengal State University, Barasat, India, September 29, 2011.
18. How to Send Secret Messages in Public.
    NAMSAA Popular Talk Series, New Alipore Multipurpose School, Kolkata, India, September 24, 2011.
19. Partial State Exposure of HC-128 and Its Consequences.
    Indo-Japan Joint Workshop on Cryptography, Indian Statistical Institute, Kolkata, India, September 15, 2011.
20. Random Number Generation and Stream Cipher.
    Tutorial Workshop on Cryptology, Rajabazar Science College Campus, University of Calcutta, India; jointly organized by the University of Calcutta & the Centre of Excellence in Cryptology, Indian Statistical Institute, July 16, 2011.
21. Wireless Encryption Algorithms.
    UGC Refresher Course on Security in Wired and Wireless Networks, School of Mobile Computing and Communication, Jadavpur University, Kolkata, India, July 14, 2011.
22. Randomness and Cryptography.
    Seminar organized by Computer Chapter, IEEE Calcutta Section, School of Mobile Computing and Communication, Jadavpur University, Kolkata, India, July 13, 2011.
23. Cryptology: the Art and Science of Secure Communication.
    Workshop on Emerging Technology in Computing, St. Thomas' College of Engineering & Technology, Kolkata, India, June 8, 2011.
24. Fundamentals of Stream Ciphers.
    National Level Instructional Workshop on Cryptology (May 9-13, 2011), May 11, 2011, Centre for Cyber Security, Amrita Vishya Vidyapeetham, Coimbatore, India.
25. Cryptosystems and Cryptanalytic Attacks.
    Training on Information and Network Security, Scientific Analysis Group (SAG), Defence Research & Development Organisation (DRDO), Delhi, Ministry of Defence, Govt. of India, February 4, 2011.
26. Symmetric Key Cryptography: Some Modern Stream Ciphers.
    BARC Lecture Series on Cryptology, Supercomputing Facility, Computer Division, Bhabha Atomic Research Centre (BARC), Mumbai, India, November 23, 2010.
27. State of the Art Software Stream Ciphers.
    National Level Instructional Workshop on Cryptology (for University and College Teachers of the North-East Region, May 5-7, 2010), Department of Mathematics, Manipur University, Imphal, India, May 6, 2010.
28. Construction of Full State from Half State of HC-128.
    Seminar at Coding & Cryptography Research Group (CCRG), Division of Mathematical Sciences, School of Physical & Mathematical Sciences, Nanyang Technological University (NTU), Singapore, March 10, 2010.
29. New Distinguishing Attacks on HC-128.
    Security Fundamentals (SF) Meeting, Research Center for Information Security (RCIS),

National Institute of Advanced Industrial Science and Technology (AIST), Akihabara Site, Tokyo, Japan, July 13, 2009.

30. Stream Cipher RC4: A Case Study.
    Workshop on Teaching Cryptology at Undergraduate Level, Indian Statistical Institute (ISI), Kolkata, India; jointly organized by the Cryptology Research Society of India (CRSI) and the Institute of Mathematical Sciences (IMSc), Chennai, India; partially sponsored by Department of Science and Technology (DST), Government of India, June 18, 2009.
31. Recent Advances in RC4 Cryptanalysis.
    Workshop on Cryptography, Institute of Mathematics and Applications (IMA), Bhubaneswar; co-organized by the National Institute of Science Education and Research (NISER), Bhubaneswar (an Autonomous Institution of Department of Atomic Energy, Government of India); sponsored by the Science and Technology Department, State Council on Science and Technology, Government of Orissa and Institute of Mathematical Sciences (IMSc), Chennai, India, December 6, 2008.
32. Cryptology: A Technical Overview.
    Seminar at TwoPiRadian Infotech Private Limited, Kolkata, India, February 2, 2008.
33. On New Weaknesses of the RC4 Stream Cipher.
    Centre for Applied Cryptographic Research (CACR) Seminar Series, University of Waterloo, Ontario, Canada, August 22, 2007.
34. Structural Weakness of the Key Scheduling of RC4.
    1st Indo-French Workshop on Cryptography and Related Topics (IFW), Paris, France; organized by the Indo-French Centre for the Promotion of Advanced Research under the Department of Science and Technology (DST), Government of India and the Ministry of Foreign Affairs, Government of France, June 11, 2007.
35. Basics of Public Key Cryptography.
    State Level Seminar on Application of Cryptology in Industry and Cryptanalysis (ACIC), Science City, Kolkata, India; organized by the Department of Information Technology of the RCC Institute of Information Technology and Partially Sponsored by Cognizant Technology Solutions (CTS), May 5, 2007.

On Mathematics

36. Theory of Metrics.
    Seminar, Centre for Distributed Computing, Jadavpur University, Kolkata, India, January 21, 2011.
37. Algebraic Inequalities.
    Training program for the Regional Mathematical Olympiad (RMO) 2008 qualified candidates (West Bengal Region), Indian Statistical Institute, Kolkata, India, December 29, 2008.

On Miscellaneous Topics in Computer Science

38. Automata Theory and Its Applications.
    Faculty Training Program at Bengal Institute of Technology (Techno-India Group of Colleges), Kolkata, India, December 20, 2013.
39. Introduction to Information and Coding Theory.
    UGC Refresher Course on Theoretical Aspects of Computer Science (Jan 21 - Feb 12,

2009), Department of Computer Science & Engineering, Jadavpur University, Kolkata, India, February 5, 2009.

40. On Analysis and Design of Algorithms.
    UGC Refresher Course on Theoretical Aspects of Computer Science (Jan 21 - Feb 12, 2009), Department of Computer Science & Engineering, Jadavpur University, Kolkata, India, February 6, 2009.
41. Propositional and Predicate Logic in Computer Science.
    UGC Refresher Course on Theoretical Aspects of Computer Science (Jan 21 - Feb 12, 2009), Department of Computer Science & Engineering, Jadavpur University, Kolkata, India, February 9, 2009.
42. Introduction to Artificial Intelligence and Its Applications in Robotics.
    Robotics Workshop, St. Thomas' College of Engineering & Technology, Kolkata, India, July 9, 2007.

On Education

43. Teaching as a Way of Learning.
    2nd Sharing Knowledge, Insights, and Lessons Learned (SKILL) Conference, SUNY Albany; organized by the Center for Excellence in Teaching and Learning (CETL), SUNY Albany, U.S.A., October 16, 2004.
44. Beyond Data and Digits : My Teaching Experiences in the CSI Department.
    1st Sharing Knowledge, Insights, and Lessons Learned (SKILL) Conference, SUNY Albany; organized by the Center for Excellence in Teaching and Learning (CETL), SUNY Albany, U.S.A., November 1, 2003.

Software Skills

Programming Languages: C, C++, Java, Prolog, Lisp, SQL.

Mathematical Computing: Sage, MATLAB.

Operating Systems: Windows, Linux, Unix, Mac OS, MS-DOS.

Personal Information

Date of Birth: December 22, 1978. **Nationality/Sex/Status:** Indian/Male/Married.

Father's Name: Mr. Nanda Dulal Paul.

Permanent Residential Address

21/5 Bankim Mukherjee Sarani (Sahapur Colony), Plot No. 65 & 66, 2nd Floor, New Alipore, Kolkata 700 053, West Bengal, India.

Languages Known

English (fluent), Bengali (fluent), Hindi (fair), Sanskrit (medium), German (a little).

Extra-Curricular Activities

(***Interests***: Puzzles, Triller movies, Hitchhiking, Photography, Poetry, Vedic Scriptures)

1. **Assistant Editor**, Bengali Little Magazine "Akhon Aahabkal". [2008 – to date]
2. Regular **Contributor** in "Computer Jagat", a monthly IT magazine in Bengali published from Jadavpur University. [2006 – to date]
3. **Author** of *Brishti Tomar Jonyo* ("For you, my raingirl"), a book of poems in Bengali, published by Ujjwal Sahitya Mandir. [2007]
4. **Speaker**, weekly discourses on *Science & Spirituality*:
   - Army Institute of Management, Kolkata, India. [2005 – 2006]
   - SUNY Albany. [2003 – 2005]
   - Albany Medical College. [2003 – 2005]
5. **Program Director**, Hindu Student Organization (HSO), SUNY Albany. [2003 – 2004]
6. **Cultural Secretary**, Hindu Student Organization (HSO), SUNY Albany. [2002 – 2003]

References

Doctoral Advisor

Prof. Subhamoy Maitra [subho@isical.ac.in], Applied Statistics Unit (ASU), Indian Statistical Institute (ISI), Kolkata, India.

Master's Advisor

Prof. S. S. Ravi [ravi@cs.albany.edu], Department of Computer Science, University at Albany, State University of New York (SUNY), U.S.A.

Research Collaborator

Prof. Miodrag Mihaljevic [miodragm@mi.sanu.ac.rs], Serbian Academy of Sciences and Arts, Belgrade, Serbia and Research Center for Information Security (RCIS), National Institute of Advanced Industrial Science and Technology (AIST), Tsukuba, Japan.