Resume for Debdeep Mukhopadhyay

Permanent Address
C/o Mr. N. Mukhopadhyay
71/2 College Road,
Howrah 711103
West Bengal, India
+91-033-26687665

Present Address
Dept of Computer Science and Engg,
Indian Institute of Technology
Kharagpur 721302
West Bengal, India
+91-3222-282352
debdeep@cse.iitkgp.ernet.in
Website:http://cse.iitkgp.ac.in/∼debdeep

Education

Indian Institute of Technology, Kharagpur
Ph.D., Computer Science and Engineering
Master of Science, Computer Science and Engineering
Bachelor of Technology (Hons), Electrical Engineering

- Summary of Masters and PhD Thesis
  - Title of MS Thesis: *Hardware for Cryptography*

    The work proposes a novel architecture for AES-Rijndael, which is the worldwide standard for block ciphers. A complete ASIC design of the cryptosystem is presented. The designed ASIC was found to be more efficient (parameterized as throughput/area) than all reported works. The thesis also deals with the design of a special purpose hardware for cryptanalysis of AES Rijndael.
  - Title of PhD Thesis: *Design and Analysis of Cellular Automata Based Cryptographic Algorithms*

    The work investigates the application of Cellular Automata (CA) in the world of cipher design. The fact that the simple rules of the CA can be used to develop complex dynamics have often inspired cryptographers to develop ciphers based on them. However, the adventures have not been successful, mainly because of its affine nature. Hence, my line of attack to the problem was first to develop crypto-primitives using CA and then to develop techniques to assemble them for developing ciphers (both block ciphers and key agreement protocols). Finally the proposals have to be evaluated (cryptanalyzed) to estimate their security margin. The novelty of the schemes lies in the simplicity of the underlying rules, thus leading to efficient implementations. In my work I have also developed a fault based side-channel attack on AES Rijndael, which outperforms all the existing attacks in this class. Further, the Cellular Message Encryption Algorithm (CMEA) has been customized against its existing weakness. It has been theoretically and practically demonstrated that the customized CMEA has a higher security margin than the original algorithm.

- Details of employment :
  - Working as **Assistant Professor** in the Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur (from June 2008-present).
  - Worked as **Assistant Professor** in the Department of Computer Science and Engineering, Indian Institute of Technology Madras (from April, 2007-June, 2008).
  - Worked as **visiting Professor** in the Department of Computer Science and Engineering, Indian Institute of Technology Madras (from October, 2006-April, 2007).

- Worked as a **Senior Project Officer** in the Department of Computer Science and Engineering, IIT Kharagpur in the following projects (from May 2005-September 2006):
  1. Department of Information Technology, India (DIT) Sponsored Project: Design of Side-channel resistant crypto-hardware
  2. Indian Space Research Organization (ISRO) Sponsored Project: FPGA Design of AES Rijndael and a Cellular Automata based Encompression Architecture.
- Worked as **Graduate Research Assistant** in the Advanced VLSI Design Laboratory, IIT Kharagpur. The project work was on the design and test of digital chips. During this period I had the oppurtunity of being aware of the complete flow in the design industry (from May 2002-May 2005).
- Worked as an **Graduate Research Assistant** in the Department of Computer Science and Engineering, in the project ”Testing of Embedded Core Based System-On-Chip”. This project was sponsored by Lucent Technologies Inc., USA from May 2001 to May 2002.

Technical Skills

Use of Synopsys, Design Analyzer for front end of Digital Design.
Use of Cadence, Silicon Ensemble for backend of Digital Design.
Use of Synopsys, Apollo for backend of Digital Design.
Use of Specman Elite, Verification of Digital Design.
Use of Hercules for physical verification.
Worked as the System Administrator of Advanced VLSI Laboratory. The laboratory has one ULTRAENT-450 Sun machine (main server) and 10 Ultra-60 Sun machines (clients), working as servers to 50 thin clients. The machines are all connected in a Network File System. The laboratory is a central research facility in IIT Kharagpur, catering to a large number of students, research fellows and faculties. The laboratory has numerous CAD tools supported by Synopsys, Cadence, Mentor and Magma.

Updated List of Publications

- **Journal Papers:**
  - **Published Journal Papers:**

    J1. Santosh Ghosh, Debdeep Mukhopadhyay, Dipanwita RoyChowdhury, ”Petrel: Power and Timing Attack Resistant Elliptic Curve Scalar Multiplier Based on Programmable $GF(p)$ Arithmetic Unit”’, To Appear in IEEE Transactions on Circuits and Systems-I (IEEE TCAS-I).

    J2. Chester Rebeiro, Sujoy Sinha Roy, Sankara Reddy and Debdeep Mukhopadhyay, ”Revisiting the Itoh-Tsujii Inversion Algorithm for FPGA Platforms”’, To Appear in IEEE Transactions on VLSI Systems (IEEE TVLSI).

    J3. Debdeep Mukhopadhyay and Dipanwita RoyChowdhury, ”A Parallel Efficient Architecture for Large Cryptographically Robust $n \times k$ ($k > n/2$) Mappings”, To Appear in IEEE Transactions on Computers (IEEE TC).

    J4. Santosh Ghosh, Debdeep Mukhopadhyay, Dipanwita Roy Chowdhury, ”Fault Attack and Countermeasures on Pairing Based Cryptography”, To Appear in International Journal of Network Security.

    J5. Debdeep Mukhopadhyay, ”Group Properties of Non-linear Cellular Automata”, Journal of Cellular Automata (JCA), October, Vol. 5 issue 1, 2009, pp 139-155.

J6. M. Alam, S. Ghosh, M.J. Mohan, D. Mukhopadhyay, D.R. Chowdhury, and I.S. Gupta, ”Effect of glitches against masked AES S-box implementation and countermeasure”, IET Information Security, 2009, Volume 3, Issue 1, pp 34-44

J7. Debdeep Mukhopadhyay, Pallavi Joshi, Dipanwita Roy Chowdhury: VLSI Architecture of a Cellular Automata based One-Way Function. Journal of Computers, 2008, Volume 3, Issue: 5, pp 46-53.

J8. G. Sengar, D. Mukhopadhyay and D.RoyChowdhury, ”Secured Flipped Scan Chain Model for Crypto-architecture”, IEEE Transactions on CAD, Nov 2007, Volume 26, Issue: 11 pp 2080-2084.

J9. D. Mukhopadhyay, G. Sengar and D.RoyChowdhury, ”Hierarchical Verification of Galois Field Circuits”, IEEE Transactions on CAD, Oct 2007, Volume 26, Issue 10, pp 1893-1898.

J10. D. Mukhopadhyay and D. RoyChowdhury, ”Fault Based Attack on the Rijndael Cryptosystem”, Journal of Discrete Mathematical Sciences & Cryptography, April 2007, Volume 10, Number 2, pp 267-290.

J11. D. Mukhopadhyay and D. RoyChowdhury, ”Theory of a Class of Complemented Group Cellular Automata and its Application to Cryptography”, Journal of Cellular Automata, Volume 2, Number 3, 2007, pp 243-271.

J12. D. Mukhopadhyay and D. RoyChowdhury, ”Key Mixing through Addition Modulo 2^n”, In International Journal of Computer, Mathematical Sciences and Applications, Cryptology ePrint Archive, Report 2005/383, http://eprint.iacr.org/, 2005.

J13. S. Banerjee, D. Mukhopadhyay and D. RoyChowdhury, ”A DFT Solution for Mixed Signal SOCs”, IEEE Transactions on CAD, Volume 25, Issue 7, pp: 1368-1377, July 2006.

J14. D. Mukhopadhyay and D. RoyChowdhury, ”Customizing Cellular Message Encryption Algorithm”, International Journal of Network Security, Volume 7, No. 2, 2008, pp. 194-202.

– **Papers under Review:**

J15. Debdeep Mukhopadhyay, ”Generating Expander Graphs using Cellular Automata” submitted to Journal of Graphs and Combinatorics, Springer.

J16. Michael Tunstall and Debdeep Mukhopadhyay, ”Differential Fault Analysis of the Advanced Encryption Standard using a Single Fault”, Cryptology ePrint Archive, Report 2009/575, http://eprint.iacr.org/, 2009.

- **Conference Papers:**

C1. Sujoy Roy, Chester Rebeiro and Debdeep Mukhopadhyay, ”Theoretical Modeling of the Itoh-Tsujii Inversion Algorithm for Enhanced Performance on k-LUT based FPGAs”, To Appear in the Proceedings of DATE 2011.

C2. Subidh Ali, Rajat Subhra Chakraborty, Debdeep Mukhopadhyay and Swarup Bhunia, ”Multi-level Attack: an Emerging Threat Model for Cryptographic Hardware”, To Appear in the Proceedings of DATE 2011.

C3. Chester Rebeiro and Debdeep Mukhopadhyay, ”Cryptanalysis of CLEFIA using Differential Methods with Cache Trace Patterns”, To appear in the Proceedings of CT-RSA 2011.

C4. Mainack Mondal, Avik Chakraborti, Nilanjan Datta and Debdeep Mukhopadhyay, ”TweLEX: A Tweaked Version of the LEX Stream Cipher”, Accepted for 5th Benelux Workshop on Information and System Security (Wissec), November 29-30, 2010, Nijmegen, the Netherlands.

C5. Santosh Ghosh, Debdeep Mukhopadhyay and Dipanwita Roy Chowdhury, ”High Speed Flexible Pairing Cryptoprocessor on FPGA Platform”, To Appear in the 4^{th} International Conference on Pairing, 2010, Japan.

C6. Santosh Ghosh, Debdeep Mukhopadhyay, and Dipanwita Roy Chowdhury. High Speed Fp Multipliers and Adders on FPGA Platform. DASIP 2010, Edinburgh, Scotland, October 2010.

C7. Sandip Karmakar, Debdeep Mukhopadhyay and Dipanwita Roy Chowdhury, ”d-Monomial Tests of Nonlinear Cellular Automata for Cryptographic Design”’, To Appear in the 9th International Conference on Cellular Automata for Research and Industry (ACRI), Italy, 2010.

C8. Sandip Karmakar, Debdeep Mukhopadhyay and Dipanwita Roy Chowdhury ”CAvium - Strengthening Trivium Stream Cipher Using Cellular Automata”, To Appear in Automata, France, 2010.

C9. Dibyendu Mallik and Debdeep Mukhopadhyay, ”New Pseudo Near Collision on Tiger”, To appear in the International Conference on Security and Cryptography, Secrypt 2010, Athens, Greece.

C10. Chester Rebeiro, Debdeep Mukhopadhyay, Junko Takahashi and Toshinori Fukunaga, ”Cache Timing Attacks on CLEFIA”, In the Proceedings of 10th International Conference on Cryptology in India, INDOCRYPT 2009, pp. 104-118, Lecture Notes in Computer Science, 5922 Springer 2009.

C11. Chester Rebeiro, Mainack Mondal, Debdeep Mukhopadhyay, ”Pinpointing Cache Timing Attacks on AES”, In the Proceedings of 23rd International Conference on VLSI Design, VLSID 2010, pp. 306-311, Bangalore.

C12. Debdeep Mukhopadhyay, ”A New Fault Attack on the Advanced Encryption Standard Hardware”, Invited Paper in the Proceedings of IEEE 19th European Conference on Circuit Theory and Design, pp. 387-390, Antalya, Turkey, 2009.

C13. Ankur Sharma, Debdeep Mukhopadhyay, ”Performance Evaluation of an Efficient Boolean Function Generator for Cryptographic Applications”, In the Proceedings of 13th IEEE VLSI Design And Test Symposium, VDAT 2009, Bangalore, India.

C14. Debdeep Mukhopadhyay, ”An Improved Fault Based Attack of the Advanced Encryption Standard”, In the Proceedings of 2nd African International Conference on Cryptology, AFRICACRYPT 2009, Gammarth-Tunisia, 412-434, Lecture Notes in Computer Science, 5580 Springer 2009.

C15. Chester Rebeiro, Debdeep Mukhopadhyay, ”High Speed Compact Elliptic Curve Cryptoprocessor for FPGA Platforms”, In the Proceedings of 9th International Conference on Cryptology in India, INDOCRYPT 2008, Kharagpur, 376-388, Lecture Notes in Computer Science, 5365 Springer 2008.

C16. Mukesh Agrawal, Sandip Karmakar, Dhiman Saha, Debdeep Mukhopadhyay, ”Scan Based Side Channel Attacks on Stream Ciphers and Their Counter-Measures”, In the Proceedings of 9th International Conference on Cryptology in India, INDOCRYPT 2008, Kharagpur, 226-238, Lecture Notes in Computer Science, 5365 Springer 2008.

C17. Debdeep Mukhopadhyay, Dipanwita Roy Chowdhury, Chester Rebeiro, ”Theory of Composing Non-linear Machines with Predictable Cyclic Structures”, In the Proceedings of 8th International Conference on Cellular Automata for Research and Industry (ACRI), Japan, 210-219, Springer, Lecture Notes in Computer Science, 5191 Springer 2008.

C18. Chester Rebeiro and Debdeep Mukhopadhyay, ”High Performance Elliptic Curve Cryptoprocessor for FPGA Platforms”, In the Proceedings of 12th IEEE VLSI Design And Test Symposium, VDAT 2008, Bangalore, India

C19. Chester Rebeiro and Debdeep Mukhopadhyay, ”Power Attack Resistant Efficient FPGA Architecture for Karatsuba Multiplier”, In the Proceedings of 21st IEEE Conference on VLSI Design 2008, pp 706-711, India.

C20. Sanjay Burman, Debdeep Mukhopadhyay and V. Kamakoti, ”LFSR Based Stream Ciphers are vulnerable to Power Attacks”, In the Proceedings of 8th International Conference on Cryptology in India, INDOCRYPT 2007, Lecture Notes in Computer Science, 4859, pp 384-392.

C21. Kundan Kumar, Debdeep Mukhopadhyay and Dipanwita RoyChowdhury, ”Design of a Differential Power Analysis Resistant AES S-Box”, In the Proceedings of 8th International Conference on Cryptology in India, INDOCRYPT 2007, Lecture Notes in Computer Science, 4859, pp 373-383, India.

C22. Gaurav Sengar,Debdeep Mukhopadhyay, D. Roy Chowdhury, ”An Efficient Approach to Develop Secure Scan Tree for Crypto-Hardware”, In the Proceedings of 15th International Conference on Advanced Computing & Communication, ADCOM 2007, pp 21-26, 18 - 21 December, 2007, IIT Guwahati, India.

C23. Santosh Ghosh, Monjur Alam, Kundan Kumar, Debdeep Mukhopadhyay, Dipanwita Roy Chowdhury, ”Preventing the Side-Channel Leakage of Masked AES S-Box”, In the Proceedings of 15th International Conference on Advanced Computing & Communication, ADCOM 2007, pp 15-20 ,18 - 21 December, 2007, IIT Guwahati, India.

C24. Chester Rebeiro and Debdeep Mukhopadhyay, ”Hybrid Masked Karatsuba Multiplier for $GF(2^{233})$”, In the Proceedings of the 11th IEEE VLSI Design And Test Symposium, pp 379-387, August 8-11, 2007, Calcutta, India.

C25. Monjur Alam, Santosh Ghosh, Debdeep Mukhopadhyay, Dipanwita Roy Chowdhury, Indranil Sen Gupta, ”Latency Optimized AES-Rijndael with Flexible Mode of Operation”, In the Proceedings of 11th IEEE VLSI Design And Test Symposium, pp 268-280, August 8-11, 2007, Calcutta, India.

C26. Debojyoti Bhattacharya, Debdeep Mukhopadhyay, Dhiman Saha and Dipanwita RoyChowdhury, ”Strengthening NLS against Crossword Puzzle Attack”, Published in 12th Australasian Conference on Information Security and Privacy (ACISP), Lecture Notes in Computer Science, 4586, pp 29-44,James Cook University, Townsville, Queensland, Australia, July 2-4, 2007, ACISP 07.

C27. Monjur Alam, Sonai Ray, Debdeep Mukhopadhyay, Dipanwita RoyChoudhury and Indranil Sengupta, ”An Area optimized Reconfigurable Encryptor for AES-Rijndael”, Design, Automation and Test in Europe, DATE 2007, 16-20 April, Acropolis, Nice, France, DATE 07.

C28. Monjur Alam, Sonai Ray, Debdeep Mukhopadhyay, Dipanwita RoyChoudhury and Indranil Sengupta, ”An Efficient Reconfigurable Encryptor for AES-Rijndael with S-box Optimization”, Fifteenth ACM/SIGDA International Symposium on Field-Programmable Gate Arrays, Monterey Beach Resort Monterey, California, February 18-20, 2007, FPGA 07.

C29. Debdeep Mukhopadhyay, P.Joshi and D.RoyChowdhury, ”An Efficient Design of Cellular Automata based Cryptographically Robust One-Way Function”, Proceedings of 20th IEEE International Conference on VLSI Design, VLSID 07, pp 842-853, India.

C30. Kundan Kumar, Debdeep Mukhopadhyay and D. RoyChowdhury, ”A Programmable Parallel Structure to perform Galois Field Exponentiation”, Proceedings of International Conference on Information Technology, ICIT 2006, pp 277-280, India.

C31. Debdeep Mukhopadhyay and D. RoyChowdhury, ”Key Mixing in Block Ciphers through Addition Modulo 2^n, Published in the Proceedings of National Workshop in Cryptology, 2006, India.

C32. Debdeep Mukhopadhyay and D. RoyChowdhury, ”Generation of Expander Graphs Using Cellular Automata and its Applications to Cryptography”, Proceedings of the 7th International Conference on Cellular Automata for Research and Industry (ACRI 2006), Lecture Notes in Computer Science 4173, pp 636-645, 20-23 September 2006, Perpignan, France.

C33. D. Bhattacharya, Debdeep Mukhopadhyay and D. RoyChowdhury, "A Cellular Automata Based Approach for Generation of Large Primitive Polynomial and its Application to RS-coded MPSK Modulation", Proceedings of the 7th International Conference on Cellular Automata for Research and Industry (ACRI 2006), Lecture Notes in Computer Science 4173, pp 204-214, 20-23 September 2006, Perpignan, France.

C34. D. Mukhopadhyay and D. RoyChowdhury, "R6Crypt: A New Cryptosystem for Handheld Devices", Proceedings of International Conference on Computer & Communication Engineering, (ICCCE'06) May 2006, Kuala Lumpur, 9-11 May 2006.

C35. P. Joshi, D. Mukhopadhyay and D. RoyChowdhury, "Design and Analysis of a Robust and Efficient Block Cipher Using Cellular Automata", In the Proceedings of the 20th International Conference on Advanced Networking and Applications (AINA'06), volume 2, pp 67-71, April 18-20, Vienna, Austria.

C36. D. Mukhopadhyay, A. Chaudhury, A. Nebhnani and D. RoyChowdhury, "CCMEA : Customized Cellular Message Encryption Algorithm for Wireless Networks", In the Proceedings of International Conference on Information Systems Security (ICISS 2005), Lecture Notes in Computer Science 3803, pp 217-227, December 19-21, Kolkata, India.

C37. D. Mukhopadhyay, S. Banerjee, D. RoyChowdhury and B. Bhattacharya, "CryptoScan: A Secured Scan Chain Architecture", in the Proceedings of Asian Test Symposium 2005, pp 348-353, December 18-21, Kolkata, India.

C38. D. Mukhopadhyay and D. RoyChowdhury, "Cellular Automata Based Key Agreement", 2nd International Conference on E-Business and Telecommunication Networks", Microsoft Convention Centre at Reading U.K. (ICETE 2005), pp 262-267, October 3-7, 2005.

C39. D. Mukhopadhyay, S. Banerjee and D. RoyChowdhury, "Performing Scan Based Attack On a Stream Cipher Hardware", In the Proceedings of National Workshop on Cryptology, 12-14 August, pp 1-8, Shimoga, India.

C40. D. Mukhopadhyay and D. RoyChowdhury, "Secured Key Agreement Using Cellular Automata", In the Proceedings of National Workshop on Cryptology, 12-14 August, 2005, pp 85-94, Shimoga, India.

C41. D. Mukhopadhyay and D. RoyChowdhury, "Programmable Galois Multiplier Using Cellular Automaton", In the Proceedings of 9th VLSI Design and Test Symposium (VDAT 2005), pp 169-176, Bangalore, India.

C42. Debdeep Mukhopadhyay and D. RoyChowdhury, "An Efficient End to End Design of Rijndael Cryptosystem in 0.18 μ CMOS", In the Proceedings of the 18th International Conference on VLSI Design 2005 jointly held with 4th International Conference on Embedded Systems Design, pp 405-410, Kolkata, India.

C43. S. Banerjee, D. Mukhopadhyay and D. RoyChowdhury, "Computer Aided Test (CAT) Tool for Mixed Siganal SOCs", In the Proceedings of the 18th International Conference on VLSI Design 2005, pp 787-790, Kolkata, India.

C44. D. Mukhopadhyay and D. RoyChowdhury, "New Observations on the Security of the Rijndael Cryptosystem", In the Proceedings of National Workshop on Cryptology 2004, pp 292-312, Kollam, India

C45. D. Mukhopadhyay and D. RoyChowdhury, "An Efficient Galois Multiplier Using Cellular Automata", International Conference on Number Theory and Fourier Techniques-ICNFT 2004, Srinivas Ramanujam Centre, SASTRA Deemed University, Kumbakonam, India

C46. D. Mukhopadhyay and D. RoyChowdhury, "Cellular Automata : An Ideal Candidate for a Block Cipher", 1st International Conference on Distributed Computing and Internet Technology (ICDCIT 2004), Lecture Notes in Computer Science, 3347, pp 452-457, Bhuvaneshwar, India.

C47. D. Mukhopadhyay and D. RoyChowdhury, ”Characterization of a Class of Complemented Group Cellular Automata”, 6th International Conference on Cellular Automata for Research and Industry, ACRI’04, Lecture Notes in Computer Science, 3305, pp 775-784, Amsterdam, The Netherlands.

C48. D. Mukhopadhyay and D. RoyChowdhury, ”Design of a coprocessor for Galois Field Computation”, In the Proceedings of the International Conference on Communication, Devices and Intelligent Systems, CODIS04, Kolkata, India.

C49. S. Banerjee, D. Mukhopadhyay, and D. RoyChowdhury, ”Testing of ADC Embedded in Mixed-Signal SOC”, In the Proceedings of the International Conference on Communication, Devices and Intelligent Systems, CODIS04, Kolkata.

C50. S. Banerjee, D. Mukhopadhyay and D. RoyChowdhury, ” Automatic Generated Built-In-Self-Test for Embedded Memory”, in the Proceedings of the IEEE Indicon 2004, pp 377-380, Kharagpur, India.

C51. S. Banerjee, D. Mukhopadhyay and D. RoyChowdhury, ”Best Repair: An Efficient Reconfiguration for RRAM”, in the Proceedings of the IEEE Indicon 2004, pp 423-426, Kharagpur, India.

C52. D. Mukhopadhyay and D. RoyChowdhury, ”Design and Implementation of Cryptoattack on Secured Embedded Systems”, In the Proceedings of the 6th International Conference on Information Technology, CIT03, Bhubaneshwar, India.

C53. C. V. Guru Rao and D. Mukhopadhyay and D. Roy Chowdhury, ”A New Strategy and Design For Mixed signal SOC Testing”, In the digest of the papers of 4th International Workshop on RTL and High Level Testing (WRTLT’03) in conjunction with ATS’03 at Xi’an, P.R.China, November 20-21, 2003.

C54. D. Mukhopadhyay and D. RoyChowdhury, ”Smart Medical Service to the Rural World”, In the Proceedings of the International Conference on Information Technology: Prospects and Challenges in the 21st century, ITPC03, Kathmandu Nepal.

C55. S.Basu, D. Mukhopadhyay, Dipanwita Roychoudhury, Indranil Sengupta, Sudipta Bhawmik, ”Reformatting Test Patterns for Embedded Core Based Systems Using Test Access Mechanism (TAM) Switch”, Proceedings of International Conference on ASP-DAC and VLSI Design 2002, pp 598-603, Bangalore, India.

C56. C. V. Guru Rao, D. Mukhopadhyay, D. Roy Chowdhury, ”A Design for test Technique for mixed mode SOC Design”, 11th Annual IEEE Symposium on System On a Chip, Bangalore, India, November 22-23, 2002.

C57. D. Mukhopadhyay and D. RoyChowdhury, ”Cellular Automata Based Cryptosystem Employing Galois Field (2^p) algebra”, International Symposium on Cellular Automata, Yokohama, Japan, 2001, pp 114-119.

- **Books:** B. A. Forouzan and D. Mukhopadhyay, ”‘Cryptography and Network Security”, Tata Mc-GrawHills, 2nd Edition, 2010.

Invited Talks Delivered

1. *Cryptographically Robust Large Boolean Functions* (NTT Labs, Japan, June 2010)
2. *Side Channel Attacks* (NTT Labs, Japan, June 2010)
3. *High Performance Elliptic Curve Crypto-processor for FPGA platforms* (NTT Labs, Japan, June 2010)
4. *Recent Works on Fault and Cache Attacks* (NTT Labs, Japan, June 2010)
5. *Cryptographically Robust Large Boolean Functions*, Seminar in Computer Sc and Engg, IIT Kharagpur, 2010 (to appear in IEEE TC 2010)

6. Tutorial Talk on *Side Channels in Cryptography*, Fifth International Conference on Information Systems Security (ICISS 2009)
7. Invited Paper on *A New Fault Attack on the Advanced Encryption Standard Hardware*, Published in the Proceedings of IEEE 19^{th} European Conference on Circuit Theory and Design, 387-390, Antalya, Turkey, 2009.
8. Invited Talk on *Fault Attack on AES Cryptosystem*, at National Wokshop on Cryptology, SVNIT Surat, India.
9. Presentations at PragaTI Course in Texas Instruments, Bangalore, Feb 2007.
   - Elliptic Curve Cryptosystems
   - Side Channels in Cryptography
10. Design of Efficient Cryptographically Robust Substitution Boxes, National Conference on Information Security-Issues and Challenges (NCISIC-08), Orissa, India
11. Testing of Cryptographic Hardware, CAIR Workshop, IIT Madras, December 2006.
12. Physical Design Automation, National Workshop on Cryptology, RIT, Behrampur, Orissa, November 2006.
13. Cellular Automata and Galois Field Architectures, Synopsys Inc, India.
14. Workshop in Cryptology, IEEE Chapter, IIT Kharagpur, 2005:
    - Cryptanalysis of Block Ciphers
    - Notions of Security and Random Oracles
15. Instructor in the Annual Summer Training Course in the Advanced VLSI Design Laboratory, IIT Kharagpur (2002-2005).
    - How to write hardware friendly Verilog code?
    - Low Power Architectures
    - Backend of IC Design

Courses Offered at IIT Kharagpur

1. Cryptography and Network Security (CS60041) [Autumn Semester, 2008, 2009, 2010 (on Going)] Present Course getting recorded for National Program for Technology Enhancement Learning, sponsored by Ministry of Human Resource Development, Govt of India.
2. Foundations of Cryptography (CS60084) [Spring Semester, 2009, 2010]
3. Programming and Data Structures Laboratory (CS11001) [Autumn Semester, 2010]
4. Computing System Laboratory (CS69004) [Spring Semester, 2009]
5. Computer Organization Laboratory (CS39001) [Autumn Semester, 2008]
6. Programming and Data Structures Laboratory (CS19001) [Autumn Semester, 2008]
7. Switching Laboratory (CS29002) [Spring Semester, 2009]

Courses Offered at IIT Madras

1. CAD for VLSI (Spring Semester 2008), M Tech Elective, Dept of Comp. Sc and Engg, IIT Madras

2. Digital Design Verification (Spring Semester, 2007 and 2008), M. Tech Elective, Dept of Comp. Sc and Engg, IIT Madras
3. Foundations of Computer Science (Autumn Semester, 2007), B. Tech Second Year Core Course, Dept of Comp. Sc and Engg, IIT Madras
4. Computer Programming Laboratory (Autumn Semester, 2007), B. Tech Second Year Laboratory, Dept of Comp. Sc and Engg, IIT Madras
5. Introduction to Computer Science (Autumn Semester, 2007), B. Tech First Year Core Course, Dept of Comp. Sc and Engg, IIT Madras
6. Computational Engineering Laboratory (Spring Semester, 2008), B. Tech First Year Core Course

Students under Guidance

1. PhD : 5
2. Masters : 4 (Present), 6 (Graduated)

Industry Partners/ Collaborators

1. 2010-2013: Design of a Side Channel Attack Resistant Family of Block Ciphers
2. 2009-2012: Design and Analysis of Side Channel Attack Resistant Symmetric Key Cryptosystems, Department of Science and Technology, India
3. 2009-2012: Design of Indigenous Encryption Algorithms for SDH-16, Indian Telephonic Industry (completed)
4. 2009-2011: Development of Elliptic Curve Cryptosystem on Reconfigurable Platform, Centre for Artificial Intelligence and Robotics (CAIR), Bangalore.
5. Evaluation of image compression algorithm (EICA), National Semiconductors Ltd. (completed)
6. 2008-2009: Studies on Fault Based Cryptanalysis on AES, NTT Labs, Japan (completed)
7. 2009-2010: Cache Timing Attacks on Clefia Cipher, Designed by Sony Corporations Ltd, NTT Labs, Japan (completed)
8. Side Channel Laboratory Setup, Collaborating with DIT India, DST India, National Institute of Advanced Industrial Science and Technology, Japan.

Awards Received

1. Selected for Indian National Science Academy (INSA) Young Scientist Award (2010)
2. Selected for Indian National Academy of Engineers (INAE) Young Engineer Award (2010)
3. Second Place in VLSI Design Contest of 22nd International Conference on VLSI Design, New Delhi, 2009
4. Indian Semiconductors Association (ISA) Techno-Inventor Award, Best PhD Award

Professional Activities

1. Served as Program Committee Member of various International Conferences, like Indocrypt 07 and 08, ICISS 2009, 2010, VLSI Design 2010, 2011.
2. Tutorial Chair of Indocrypt 2008

3. Reviewer of IEEE Transactions on VLSI, International Journal of Network Security, Journal of Systems and Software (Elsevier), VLSI Design Conference, International Conference on Language and Automata Theory 2009, Symposium on VLSI Design and Test 2009, International Conference on Networked Digital Technologies (NDT-2009), Cryptographic Hardware and Embedded System (CHES) 2009, Indicon, Journal of Multimedia Tools and Applications Springer.