Resume for Debdeep Mukhopadhyay

Permanent Address
C/o Mr. N. Mukhopadhyay
71/2 College Road,
Howrah 711103
West Bengal, India
+91-033-26686081

Present Address
Dept of Computer Science and Engg,
Indian Institute of Technology
Madras 600036
Tamil Nadu, India
+91-044-2257-4375
debdeep@cse.iitm.ernet.in
Website:www.cs.iitm.ernet.in/∼debdeep

Education

Indian Institute of Technology, Kharagpur
Ph.D., Computer Science and Engineering, 2007
Master of Science, Computer Science and Engineering, 2004
Bachelor of Technology (Hons), Electrical Engineering, 2001

- 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 Madras.
  - 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.

Current Projects

Since joining IIT Madras as an Assistant Professor, I am involved with the following projects:

1. Design of a Fault Based Attack on AES for Nippon Telegraph and Telephone (NTT) Corporation, Japan.
2. Design of extremely fast block ciphers using Cellular Automata for Indian Telephonic Industry (ITI), jointly with Prof D. RoyChowdhury, IIT Kharagpur.

Projects Undertaken

During my PhD I was associated with the Advanced VLSI Design Laboratory, IIT Kharagpur. The Laboratory has fabrication facilities from National Semiconductors, in 0.25 and 0.18 μ CMOS technology. The name of my research guide was Prof. Dipanwita Roy Chowdhury, Professor, Department of CSE, IIT Kharagpur.
I worked in the following projects as a part of my research work.

1. Projects Related to Cryptography and System Security

   - Design of ASIC and FPGA for Advanced Encryption Standard(AES), Rijndael (sponsored by Indian Space Research Organisation (ISRO))
   - Development of Key Agreement Protocol using Cellular Automata
   - Design of a low cost, reduced round Block Cipher using Cellular Automata
   - Customizing Cellular Message Encryption algorithm (used in CDMA networks)
   - Design and Implementation of a Hardware for Square Attack on 5 rounds of AES-Rijndael
   - Design of an Encompression Scheme for Text Data (sponsored by ISRO)
   - Performing Fault Based Algebraic Attacks on AES Rijndael
   - Preforming Scan Based attacks on Stream Ciphers
   - Analyzing Side-Channel Cryptanalysis and developing secured architectures resistant to them (sponsored by Department of Information Technology, DIT India)

2. Projects Related to VLSI Design and Test

   - Design of a Computer-Aided-Test (CAT) Tool for System on Chip (sponsored by Lucent Technology)

- Design of a Testing scheme for system on chip having mixed signal components.

- Design of a Secured DFT solution for Cryptographic Chips

Apart from the above projects I was also involved in the following projects during my BTech:

- Reformatting Test Patterns for Testing Embedded Core Based System using Test Access Mechanism (TAM) switch, under the guidance of Prof. Dipanwita Roy Chowdhury and Prof. Indranil Sengupta. The project was sponsored by Lucent Technology, USA.

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.

Publications

- **Conference Papers:**

1. C. Rebeiro and D. Mukhopadhyay, "Power Attack Resistant Efficient FPGA Architecture for Karatsuba Multiplier", To appear in the Proceedings of 21^{st} IEEE Conference on VLSI Design 2008.
2. S. Burman, D. Mukhopadhyay and V. Kamakoti, "LFSR Based Stream Ciphers are vulnerable to Power Attacks", In the Proceedings of 8^{th} International Conference on Cryptology in India, Indocrypt 2007, pp 384-392.
3. K. Kumar, D. Mukhopadhyay and D. RoyChowdhury, "Design of a Differential Power Analysis Resistant AES S-Box", In the Proceedings of 8^{th} International Conference on Cryptology in India, Indocrypt 2007, pp 373-383.
4. Gaurav Sengar,Debdeep Mukhopadhyay,D. Roy Chowdhury, "An Efficient Approach to Develop Secure Scan Tree for Crypto-Hardware", In the Proceedings of 15^{th} International Conference on Advanced Computing & Communication, ADCOM 2007, pp 21-26, 18 - 21 December, 2007, IIT Guwahati, India.
5. 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 15^{th} International Conference on Advanced Computing & Communication, ADCOM 2007, pp 15-20 ,18 - 21 December, 2007, IIT Guwahati, India.
6. C. Rebeiro and D.Mukhopadhyay, "Hybrid Masked Karatsuba Multiplier for $GF(2^{233})$", In the Proceedings of the 11^{th} IEEE VLSI Design And Test Symposium, pp 379-387, August 8-11, 2007, Calcutta, India.
7. Monjur Alam, Santosh Ghosh, Debdeep Mukhopadhay, Dipanwita Roy Chowdhury, Indranil Sen Gupta, "Latency Optimized AES-Rijndael with Flexible Mode of Operation", In the Proceedings of 11^{th} IEEE VLSI Design And Test Symposium, pp 268-280, August 8-11, 2007, Calcutta, India.
8. D.Bhattacharya, D.Mukhopadhyay, D.Saha and D.RoyChowdhury, "Strengthening NLS against Crossword Puzzle Attack", Published in 12^{th} 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.
9. 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.
10. 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.
11. D.Mukhopadhyay, P.Joshi and D.RoyChowdhury, "An Efficient Design of Cellular Automata based Cryptographically Robust One-Way Function", Proceedings of 20^{th} International Conference on VLSI Design, VLSID 07.
12. K. Kumar, D. 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.
13. D. Mukhopadhyay and D. RoyChowdhury, "Key Mixing in Block Ciphers through Addition Modulo 2^n, to be published in the Proceedings of National Workshop in Cryptology, 2006, India.

14. D. Mukhopadhyay and D. RoyChowdhury, "Generation of Expander Graphs Using Cellular Automata and its Applications to Cryptography", Proceedings of the 7^{th} International Conference on Cellular Automata for Research and Industry (ACRI 2006), 20-23 September 2006, Perpignan, France
15. D. Bhattacharya, D. 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 7^{th} International Conference on Cellular Automata for Research and Industry (ACRI 2006), 20-23 September 2006, Perpignan, France
16. 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.
17. 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 20^{th} International Conference on Advanced Networking and Applications (AINA'06), volume 2, pp 67-71, April 18-20, Vienna, Austria.
18. 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), LNCS 3803 pp 217-227, December 19-21, Kolkata, India.
19. 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.
20. D. Mukhopadhyay and D. RoyChowdhury, "Cellular Automata Based Key Agreement", 2^{nd} International Conference on E-Business and Telecommunication Networks", Microsoft Convention Centre at Reading U.K. (ICETE 2005), October 3-7, 2005.
21. 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.
22. 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.
23. D. Mukhopadhyay and D. RoyChowdhury, "Programmable Galois Multiplier Using Cellular Automaton", 9^{th} VLSI Design and Test Symposium (VDAT 2005), pp 169-176, Bangalore, India.
24. Debdeep Mukhopadhyay and D. RoyChowdhury, "An Efficient End to End Design of Rijndael Cryptosystem in 0.18 μ CMOS", in the Proceedings of the 18^{th} International Conference on VLSI Design 2005 jointly held with 4^{th} International Conference on Embedded Systems Design, pp 405-410, Kolkata, India.
25. S. Banerjee, D. Mukhopadhyay and D. RoyChowdhury, "Computer Aided Test (CAT) Tool for Mixed Siganal SOCs", in the Proceedings of the comming 18^{th} International Conference on VLSI Design 2005, pp 787-790, Kolkata, India.
26. 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
27. 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
28. D. Mukhopadhyay and D. RoyChowdhury, "Cellular Automata : An Ideal Candidate for a Block Cipher", 1^{st} International Conference on Distributed Computing and Internet Technology (ICDCIT 2004), Lecture Notes in Computer Science, 3347, pp 452-457, Bhuvaneshwar, India.

29. D. Mukhopadhyay and D. RoyChowdhury, "Characterization of a Class of Complemented Group Cellular Automata", 6^{th} International Conference on Cellular Automata for Research and Industry, ACRI'04, Lecture Notes in Computer Science, 3305, pp 775-784, Amsterdam, The Netherlands.
30. 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.
31. 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.
32. 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.
33. 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.
34. D. Mukhopadhyay and D. RoyChowdhury, "Design and Implementation of Cryptoattack on Secured Embedded Systems", In the Proceedings of the 6^{th} International Conference on Information Technology, CIT03, Bhubaneshwar, India.
35. 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 4^{th} 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.
36. 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 21^{st} century, ITPC03, Kathmandu Nepal.
37. 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.
38. C. V. Guru Rao, D. Mukhopadhyay, D. Roy Chowdhury, "A Design for test Technique for mixed mode SOC Design", 11^{th} Annual IEEE Symposium on System On a Chip, Bangalore, India, November 22-23, 2002.
39. D. Mukhopadhyay and D. RoyChowdhury, "Cellular Automata Based Cryptosystem Employing Galois Field (2^p) algebra", International Symposium on Cellular Automata, Yokohama, Japan, 2001.

- **Journal Papers**

1. D. Mukhopadhyay, P. Joshi and D.RoyChowdhury, "VLSI Architecture of a Cellular Automata based One-Way Function", Accepted in Journal of Computers, Academy Publishers.
2. 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.
3. 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.
4. 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.

5. 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.
6. 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.
7. D. Mukhopadhyay and D. RoyChowdhury, "Customizing Cellular Message Encryption Algorithm", International Journal of Network Security, Volume 7, No. 2, 2008, pp. 194-202.

Invited Talks Delivered

1. Presentations at PragaTI Course in Texas Instruments, Bangalore, Feb 2007.
   - Elliptic Curve Cryptosystems
   - Side Channels in Cryptography
2. Testing of Cryptographic Hardware, CAIR Workshop, IIT Madras, December 2006.
3. Physical Design Automation, National Workshop on Cryptology, RIT, Behrampur, Orissa, November 2006.
4. Cellular Automata and Galois Field Architectures, Synopsys Inc, India.
5. Workshop in Cryptology, IEEE Chapter, IIT Kharagpur, 2005:
   - Cryptanalysis of Block Ciphers
   - Notions of Security and Random Oracles
6. 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 or On-going Courses

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

Students Under Guidance

1. Master of Science : 1
2. MTech : 2
3. Dual Degree MTech : 2
4. BTech : 1

Extracurricular Activities

Won the first prize in Microsoft sponsored IDEON'2000 at IIT Kharagpur (Explored the possibility of storing equal number of bits using lesser components than the existing 3 transistor DRAM cell)
Won the second prize in IDEON'2001, IIT Kharagpur (analog and digital design competition)
Took active participation in elocution and chess in school. Was awarded the best all-rounder (boys) in school.

Professional Activities

- Programme Committee Member of Indocrypt 2007

References

Prof D. RoyChowdhury, Professor, Dept of Computer Sc and Engg, IIT Kharagpur, India,
Email: drc@cse.iitkgp.ernet.in, drc@iitkgp.ac.in
Prof Bimal Roy, Professor, Applied Statistics Unit, Indian Statistical Institute,
Email: bimal@isical.ac.in
Prof T. K. Basu, Professor, Electrical Engineering Head of the Department, Center for Educational Technology, IIT Kharagpur,
Email: tkb@ee.iitkgp.ernet.in