

Debdeep Mukhopadhyay

Associate Professor of Computer Science and Engineering
Indian Institute of Technology, Kharagpur, India 721302

<http://cse.iitkgp.ac.in/~debdeep>

email: debdeep@cse.iitkgp.ernet.in.

telephone: +91-3222-282352; fax: +91-3222-278985

Academic Degrees:

Ph.D. in Computer Science and Engineering, Indian Institute of Technology, Kharagpur, 2007

M.S. in Computer Science and Engineering, Indian Institute of Technology, Kharagpur, 2004

B.Tech in Electrical Engineering, Indian Institute of Technology, Kharagpur, 2001

Research Interests:

Cryptography, Hardware Security, Fault Attacks, Side-channel attacks and side channel resistant architectures; Interaction between security and reliability, micro-architectural threats.

Professional Experience:

2/13-Present: Associate Professor, Dept of Computer Science & Engg., IIT Kharagpur

8/14-12/14: Visiting Associate Professor in the Department of Computer Science, NYU-Shanghai, China

6/12-8/12: Visiting Researcher at Polytechnic Institute of New York University, Brooklyn.

6/08-present: Assistant Professor of CSE, Indian Institute of Technology, Kharagpur, India

4/07-6/08: Assistant Professor of CSE, Indian Institute of Technology, Madras, India

10/06-4/07: Visiting Professor, CSE, Indian Institute of Technology, Madras, India

5/05-9/06: Senior Project Officer, CSE, Indian Institute of Technology, Kharagpur, India

5/02-5/05: Graduate Research Assistant, Advanced VLSI Design Laboratory, IIT Kharagpur, India

5/01-5/02: Graduate Research Assistant, CSE, Indian Institute of Technology, Kharagpur, India

Awards/Invitations:

2012: Recipient of Indo-USSTF Fellowship

2012, Associate for the Indian Academy of Sciences

2012, Best student paper award at VLSID 11 for “Design for Security of Block Cipher S-Boxes to Resist Differential Power Attacks”.

2011, Outstanding Young Faculty Fellowship, IIT Kharagpur

2010, Indian National Academy of Engineers (INAE) Young Engineer Award, 2010

2010, Indian National Science Academy (INSA) Young Scientist Award, 2010

2009, Second Place in VLSI Design Contest, VLSID

2008, Indian Semiconductors Association (ISA) Techno-Inventor Award, Best PhD Award

Synergistic Activities:

Tutorial talk on Embedded Security, to be delivered in VLSID 2016

Tutorial talk on “Fault Analysis of Cryptosystems: Attacks, Countermeasures and Metrics”, CHES 2015.

Tutorial talk on “Physically Unclonable Function: a Promising Security Primitive for Internet of Things”, VLSID 2015.

Invited talk on “Cryptographic Pairings: Theory to Implementations”, Canon R&D India, June 2015.

Invited talk on “Hardware Security”, Shanghai JiaoTong University, 2014.

Co-organized a Special session on Hardware Security, at WESS 2014.

Invited talk on “Side Channel Analysis”, Texas Instruments, 2014.

Invited talk on Hardware Security, in Stanford University, Columbia University, July 2012.

Lunch talk on “Hardware Security: A Snap-Shot”, at NYU-Poly July 2012

Full day Tutorial talk on “*Information Security from a Hardware Perspective: Challenges and Solutions*” at IEEE International Workshop on Information Forensics and Security (WIFS), November 2011

Embedded Tutorial talk on “*Testability of Cryptographic Hardware and Detection of Hardware Trojans*” at IEEE Asian Test Symposium, (ATS), November 2011

EC-Spride Colloquium, “*Cache Attacks on Symmetric Key Crypto-systems and their Formal Analysis*”, CASED, T.U.Darmstadt, Germany, September 2011

Full day Tutorial talk on “*Hardware Security: a 21st Century Perspective*” at IEEE VLSI Design Conference (VLSID), 2011

Full day talk on “*Side Channels in Cryptography*”, National Knowledge Center, Abu Dhabi, UAE

Delivered a one-week talk-series on “*Crypto-Boolean Functions, Fault Attacks, Side Channel Analysis and Hardware Design of Elliptic Curve Cryptosystems*”, NTT-Labs, Japan, June 2010.
Tutorial talk on “*Side Channels in Cryptography*”, ICISS 2009
Organized “*Cryptographic Hardware and Embedded Workshop*”, 2012, IIT Kharagpur
Co-founded “*Security, Privacy and Applied Cryptographic Engineering*” (SPACE) conference in India, with association with International Association of Cryptologic Research (conference editions from 2011-Present)

Professional Activities:

Established SEAL IIT Kharagpur (<http://cse.iitkgp.ac.in/resgrp/seal/>) to initiate work on Hardware and Embedded Security (2008-Present).

Program Chair Indocrypt 2014, Co-founded SPACE in India (2011-2015), Organized CHEW 11 (Cryptographic Hardware and Embedded Workshop) at IIT Kharagpur, Tutorial Chair of Indocrypt 2008, Reviewer of IEEE Transactions of Circuits and Systems-I, IEEE Transactions on Computers, ACM Computing Surveys, IEEE Transactions on Information Forensics and Security, IEEE Transactions on VLSI, Journal of Systems and Software (Elsevier), CT-RSA 2012, 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, Journal of Multimedia Tools and Applications, Springer, American Mathematical Reviews.

Selected Program Committees: CHES 2016, DATE 2014, Indocrypt 2014 (PC Chair), COSADE 2013-15, ICCD 2015, 2012, PROOFS 2012, FDTC 2012, 2011, SPACE 12, Indocrypt 11, 07 and 08, ICISS 2009, 2010, VLSI Design 2010, 2011, VDAT 2012

Editorial Activities (for journals): Journal of Cyber Security and Mobility, Journal on Hardware Security (Springer)

Selected Publications:

1. Sarani Bhattacharya, Debdeep Mukhopadhyay: Curious case of Rowhammer: Flipping Secret Exponent Bits using Timing Analysis (to Appear in CHES 2016)
2. Debdeep Mukhopadhyay: PUFs as Promising Tools for Security in Internet of Things. IEEE Design & Test 33(3): 103-115(2016)
3. Sarani Bhattacharya, Debdeep Mukhopadhyay: Who Watches the Watchmen?: Utilizing Performance Monitors for Compromising Keys of RSA on Intel Platforms. CHES 2015: 248-266
4. Harshal Tupsamudre, Shikha Bisht, Debdeep Mukhopadhyay: Destroying Fault Invariant with Randomization - A Countermeasure for AES Against Differential Fault Attacks. CHES 2014: 93-111
5. Debapriya Basu Roy, Debdeep Mukhopadhyay, Masami Izumi, Junko Takahashi: Tile Before Multiplication: An Efficient Strategy to Optimize DSP Multiplier for Accelerating Prime Field ECC for NIST Curves. DAC 2014: 177:1-177:6
6. Suvadeep Hajra, Debdeep Mukhopadhyay: Reaching the Limit of Nonprofiling DPA. IEEE Trans. on CAD of Integrated Circuits and Systems 34(6): 915-927 (2015)
7. Durga Prasad Sahoo, Sayandeep Saha, Debdeep Mukhopadhyay, Rajat Subhra Chakraborty, Hitesh Kapoor: Composite PUF: A new design paradigm for Physically Unclonable Functions on FPGA. HOST 2014: 50-55
8. Sujoy Sinha Roy, Chester Rebeiro, Debdeep Mukhopadhyay: Theoretical Modeling of Elliptic Curve Scalar Multiplier on LUT-Based FPGAs for Area and Speed. IEEE Trans. VLSI Syst. 21(5): 901-909 (2013)
9. Chester Rebeiro, Sujoy Sinha Roy, and Debdeep Mukhopadhyay, Pushing the Limits of High-Speed GF(2^m) Elliptic Curve Scalar Multiplication on FPGAs," CHES 2012: 494-511.
10. Subidh Ali, Debdeep Mukhopadhyay: Differential Fault Analysis of AES-128 Key Schedule Using a Single Multi-byte Fault. CARDIS 2011: 50-64
11. Debdeep Mukhopadhyay: An Improved Fault Based Attack of the Advanced Encryption Standard. AFRICACRYPT 2009: 421-434
12. Chester Rebeiro, Debdeep Mukhopadhyay: Cryptanalysis of CLEFIA Using Differential Methods with Cache Trace Patterns. CT-RSA 2011: 89-103

13. Chester Rebeiro, Debdeep Mukhopadhyay, Junko Takahashi, Toshinori Fukunaga: Cache Timing Attacks on Clefia. INDOCRYPT 2009: 104-118
14. Subidh Ali, Debdeep Mukhopadhyay: An Improved Differential Fault Analysis on AES-256. AFRICACRYPT 2011: 332-347
15. Bodhisatwa Mazumdar, Debdeep Mukhopadhyay, Indranil Sengupta: Design for Security of Block Cipher S-Boxes to Resist Differential Power Attacks. VLSI Design 2012: 113-118 (best student paper)
16. Debdeep Mukhopadhyay, Rajat Subhra Chakraborty: Testability of Cryptographic Hardware and Detection of Hardware Trojans. Asian Test Symposium 2011: 517-524 (Invited Tutorial)
17. Sujoy Sinha Roy, Chester Rebeiro, Debdeep Mukhopadhyay: Theoretical modeling of the Itoh-Tsujii Inversion algorithm for enhanced performance on k-LUT based FPGAs. DATE 2011: 1231-1236
18. Dhiman Saha, Debdeep Mukhopadhyay, Dipanwita Roy Chowdhury: A Diagonal Fault Attack on the Advanced Encryption Standard. IACR Cryptology ePrint Archive 2009: 581 (2009)
19. Debdeep Mukhopadhyay, Dipanwita Roy Chowdhury: A Parallel Efficient Architecture for Large Cryptographically Robust $n \times k$ ($k > n/2$) Mappings. IEEE Trans. Computers 60(3): 375-385 (2011)
20. Dhiman Saha, Debdeep Mukhopadhyay, Dipanwita Roy Chowdhury: PKDPA: An Enhanced Probabilistic Differential Power Attack Methodology. INDOCRYPT 2011: 3-21
21. Santosh Ghosh, Debdeep Mukhopadhyay, Dipanwita Roy Chowdhury: High Speed Flexible Pairing Cryptoprocessor on FPGA Platform. Pairing 2010: 450-466
22. Debdeep Mukhopadhyay, Gaurav Sengar, Dipanwita Roy Chowdhury: Hierarchical Verification of Galois Field Circuits. IEEE Trans. on CAD of Integrated Circuits and Systems 26(10): 1893-1898 (2007)

Books/Edited Volumes/Online Courses Related to Cryptography and Security:

1. B. Forouzan, D. Mukhopadhyay, "Cryptography and Network Security e/2", Tata-McGraw Hill
2. Marc Joye, Debdeep Mukhopadhyay, and Michael Tunstall, "Security Aspects in Information Technology", Lecture Notes in Computer Science, Springer, 2011.
3. Invited Book Chapter on "Fault Attacks and Countermeasures", Editor Chip-Hong Chan and Miodrag Potkonjak, Springer
4. Debdeep Mukhopadhyay and Rajat Subhra Chakraborty, "Hardware Security: Design, Threats, and Safeguards", CRC Press. (among 20 best sellers of CS books, ref. <http://reviews.libraryjournal.com/2015/05/best-sellers/computer-science-may-2015-best-sellers/>)
5. Chester Rebeiro, Debdeep Mukhopadhyay, Sarani Bhattacharya, Timing Channels in Cryptography: A Micro-architectural Perspective, Springer.
6. Video Course on Cryptography and Network Security, National Programme on Technology Enhanced Learning, <http://nptel.iitm.ac.in/courses/106105031/>

Collaborators: Santosh Ghosh (Intel US), Junko Takahashi (NTT-Labs, Japan), Toshinori Fukunaga (NTT-Labs, Japan), Srivaths Ravi (Texas Instruments, India), V. Kamakoti (IIT Madras, India), C. Pandurangan (IIT Madras, India), Somitra Sanadhya (IIIT, Delhi), Kallol Biswas (Neucleodyne, USA), Sanjay Burman (DRDO, CAIR, India), Ramesh Karri (NYU-Poly, USA), Swarup Bhunia (Case Western Reserve, USA), Rajat Subhra Chakraborty (IIT KGP, India), Michael Tunstall (University of Bristol, UK), Marc Joye (Technicolor, France), Ingrid Verbauwhede (K.U.Leuven, Belgium), Bendikt Gierlichs (K.U Leuven, Belgium), Santosh Ghosh (K.U.Leuven, Belgium), Sylvain Guilley (TelecomParis, France), Shivam Bhasin (TelecomParis, France)