Deepak Kumar Dalai

Current Position

Assistant Professor
School of Mathematical Sciences
National Institute of Science Education and Research
(An autonomous Institution under Department of Atomic Energy,
Government of India.)
Bhubaneswar, India.

Educational Background

Ph.D.	Computer Science (Cryptology); Indian Statistical Institute, Kolkata, 2006. Thesis Title: On Some Necessary Conditions of Boolean Functions to Resist Algebraic Attacks. Supervisor: Prof. Subhamoy Maitra.
M. Tech	Computer Science; Indian Statistical Institute, Kolkata, 2003.
M.Sc.	Mathematics; Utkal University, Bhubaneswar, India, 2001.
B.Sc.	Mathematics (Hons.); Utkal University, Bhubaneswar, India, 1999.

Specialization

Theoretical Computer Sciences, Cryptology, Discrete Mathematics.

Present Research Interests

Symmetric ciphers, Algebraic Attacks, Boolean Functions, Combinatorics.

Research Experiences

1. Visiting Scientist (Feb 2008-Jun 2008) at Applied Statistics Unit in Indian Statistical Institute, Kolkata.
2. Post-doctoral fellow (Jan 2007 - Jan 2008) at Project Security in INRIA, Rocquencourt, France.

Teaching Experiences

1. MA401(Combinatorics and Graph theory) in 2009 and 2010 at NISER.
2. ML401(Computer Programming and Algorithm) in 2009 and 2010 at NISER.
3. MA301(Elementary Number Theory and Logic) in 2008 and 2009 at NISER.
4. ML301(Computer Programming and Algorithm) in 2008 and 2009 at NISER.
5. PDS(Programming and Data Structure) in 2009 at IIT, Bhubaneswar.
6. Math112(Introduction to Computation), in 2006 at IISER, Kolkata.

Workshop Organized

1. *Workshop on Cryptography* on 5th and 6th December 2008 at the Institute of Mathematics and Applications, Bhubaneswar.

Academical Visits

1. One month (4 April, 2006 - 5 May, 2006) visit to Tsukuba University, Tsukuba, Japan.
2. Three days (16 Aug. 2005 - 18 Aug, 2005) visit to the Center for Artificial Intelligence and Robotics (CAIR) lab of Defense Research & Development Organization (DRDO), Bangalore, India to discuss on algebraic attacks on stream ciphers and algebraic immunity of Boolean functions.
3. One month (24 Feb, 2005 - 23 Mar, 2005) visit to Project Codes in l'Institut National de Recherche en Informatique et en Automatique (INRIA), Rocquencourt, France.

Fellowships and Awards

- Selected for ISI (Indian Statistical Institute) fellowship for Ph.D. in Computer Science and Communication, 2003.
- Selected for ISI MTech (Computer Science) fellowship in 2001.
- Selected for NBHM (National Board for Higher Mathematics) fellowship for Ph.D. in Mathematical Sciences, 2001.
- Selected for CSIR (Council for Scientific and Industrial Research) fellowship for Ph.D. in Mathematical Sciences and SPMF test, 2001.
- Qualified JEST (Joint Entrance Screening Test) 2001 and 2003 for Ph.D. in Mathematics and Theoretical Computer Science respectively.
- Qualified GATE-2001 in Mathematics.
- Stood first in "Honours Mathematical Olympiad, Orissa", 1998.

Personal Details

Nick Name	Dipu
Sex	Male
Date of Birth	30.05.1979(DD/MM/YYYY)
Place of Birth	Bhadrak, Orissa, India
Nationality	Indian
Mother Tongue	Oriya
Other Languages	English, Hindi, Bengali
Sports and Games	Soccer, Cricket, Tennis, Ping Pong, Swimming, Jogging, ...
Working Address	School of Mathematical Sciences, National Institute of Science Education and Research, Institute of Physics Campus, P.O.: Sainik School, Bhubaneswar-751005, India.
Email Address	deepak@niser.ac.in, deepakkumardalai@gmail.com
Telephone Number	+91 (0674) 2304060 (office) +91 9777136302 (mobile)
Web page	http://www.niser.ac.in/∼deepak/

Publications

Refereed Journals

1. Deepak Kumar Dalai, Subhamoy Maitra and Sumanta Sarkar. Results on Rotation Symmetric Bent Functions. *Discrete Mathematics*, 309(8):2398–2409, April 2009.

2. Deepak Kumar Dalai and Subhamoy Maitra. Algebraic Immunity of Boolean Functions: Analysis and Constructions. Special Issue on Applied Cryptography and Data Security, *Journal of Computacion y Sistemas*, 12(3):297–321, 2009.

3. Deepak Kumar Dalai, Subhamoy Maitra and Sumanta Sarkar. Basic Theory in Construction of Boolean Functions with Maximum Possible Annihilator Immunity. *Design, Codes and Cryptography*, 40(1):41–58, July 2006.

4. Claude Carlet, Deepak Kumar Dalai, Kishan Chand Gupta and Subhamoy Maitra. Algebraic Immunity for Cryptographically Significant Boolean Functions: Analysis and Construction. *IEEE Transactions on Information Theory*, IT-52(7):3105–3121, 2006.

Refereed Conferences

(Papers marked * have been published in Lecture Notes in Computer Sciences (LNCS), Springer)

5. *Deepak Kumar Dalai. On 3-to-1 and Power APN S-boxes. In *Sequences and Their Applications, SETA 2008*, number 5203 in LNCS, pages 377–389, Springer-verlag 2008.

6. Deepak Kumar Dalai and Subhamoy Maitra. Balanced Boolean Functions with (more than) Maximum Algebraic Immunity. In *Workshop on Cryptography and Coding theory, 2007*, page 99-108, proceedings of WCC, 2007.

7. Subhamoy Maitra, Sumanta Sarkar and Deepak Kumar Dalai. On Dihedral Group Invariant Boolean Functions. In International Workshop on *Boolean Functions : Cryptography and Applications, BFCA 2007*.

8. Michael W. David, Deepak Kumar Dalai, Joydeep Mitra and Kouichi Sakurai. Statistically Based Intrusion Alert Point Detection. In *The 2nd Joint Workshop on Information Security, JWIS 2007*.

9. *Deepak Kumar Dalai and Subhamoy Maitra. Reducing the Number of Homogeneous Linear Equations in Finding Annihilators. In *Sequences and Their Applications, SETA 2006*, number 4086 in LNCS, pages 376–390, Springer-verlag 2006.

10. Claude Carlet, Deepak Kumar Dalai and Subhamoy Maitra. Cryptographic Properties and Structure of Boolean Functions with Full Algebraic Immunity, In *IEEE International Symposium on Information Theory, ISIT 2006*.

11. Deepak Kumar Dalai, Kishan Chand Gupta and Subhamoy Maitra. Notion of Algebraic Immunity and Its evaluation Related to Fast Algebraic Attacks. In International Workshop on *Boolean Functions : Cryptography and Applications, BFCA 2006*.

12. Deepak Kumar Dalai, Subhamoy Maitra and Sumanta Sarkar. Results on Rotation Symmetric Bent Functions. In International Workshop on *Boolean Functions : Cryptography and Applications, BFCA 2006*.

13. *Deepak Kumar Dalai, Kishan Chand Gupta and Subhamoy Maitra. Algebraic Immunity for Cryptographically Significant Boolean Functions: Construction and Analysis in terms of Algebraic Immunity. In *Fast Software Encryptions, FSE 2005*, number 3557 in LNCS, pages 98–111. Springer-Verlag 2005.

14. *Deepak Kumar Dalai, Kishan Chand Gupta and Subhamoy Maitra. Results on Algebraic Immunity for Cryptographically Significant Boolean Functions. In *Progress in Cryptology - Indocrypt 2004*, number 3348 in LNCS, pages 92–106. Springer Verlag, 2004.