Curriculum Vitae

1. Name: Subhamoy Maitra
2. Designation: Professor
3. Address: Applied Statistics Unit, Indian Statistical Institute, 203 B T Road, Kolkata 700 108, India.

   (including e-mail & Ph. No.) subho@isical.ac.in, +91-33-2575-2805

4. Details of Educational Qualification:

- Secondary Examination (Std. X) in the year 1986 from West Bengal Board of Secondary Education with marks 80.6% and rank 63rd.
- Higher Secondary Examination (Std. XII) in the year 1988 from West Bengal Council of Higher Secondary Education with marks 87.7% and **rank 5th**.
- Bachelor of Engineering in Electronics & TeleCommunication from Jadavpur University, Calcutta (1988-1992) with marks 85.6% and rank 7th.
- Master of Technology in Computer Science from Indian Statistical Institute, Calcutta (1994-1996) with marks 90.7% and **rank 1st**. **Awarded the "Indian Statistical Institute Alumni Association Medal" for outstanding performance in M. Tech. (CS).**
- PhD from Indian Statistical Institute, thesis entitled "Boolean Functions with Important Cryptographic Properties", 2001.

Contents

1 Complete List of Publications/Projects

1.1 Refereed Journals

Accepted papers

1. S. Sarkar and S. Maitra. Cryptanalysis of RSA with more than one Decryption Exponent. accepted in **Information Processing Letters**, acceptance date: 25 February, 2010.

2. S. Maity and S. Maitra. Minimum Distance between Bent and 1-resilient Boolean Functions. Accepted in **Ars Combinatoria** (acceptance date: 8 September, 2006).

3. S. Maitra, G. Paul, S. Raizada, S. Sen, R. Sengupta. Some Observations on HC-128. Accepted in **Designs, Codes and Cryptography**, (acceptance date: 12 February, 2010).

Published papers

2010

4. S. Sarkar and S. Maitra. Cryptanalysis of RSA with Two Decryption Exponents. **Information Processing Letters**, 110:178–181, 2010,
DOI information: 10.1016/j.ipl.2009.11.016

2009

5. S. Sarkar and S. Maitra. Further results on implicit factoring in polynomial time. **Advances in Mathematics of Communications**, Volume: 3, Number: 2, Pages : 205 - 217, May 2009.

6. S. Gangopadhyay, D. Sharma, S. Sarkar and S. Maitra. On affine (non)equivalence of Boolean functions. **Computing**, 85(1-2): 37-55 (2009).

7. G. Paul and S. Maitra. On Biases of Permutation and Keystream Bytes of RC4 towards the Secret Key. **Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences**, Volume 1, Number 2, August 2009, Pages 225-268, DOI 10.1007/s12095-008-0009-4.

8. D. K. Dalai, S. Maitra and S. Sarkar. Results on Rotation Symmetric Bent Functions. **Discrete Mathematics**, Volume 309, Issue 8, 28 April 2009, Pages 2398-2409.

9. S. Sarkar and S. Maitra. Partial Key Exposure Attacks on RSA and Its Variant by Guessing a few Bits of one of the Prime Factors. **Bulletin of the Korean Mathematical Society (B-KMS)**, Volume 46, Number 4, Pages 721-741, 2009.

10. S. Sarkar and S. Maitra. Efficient search for symmetric Boolean functions under constraints on Walsh spectra values. **Journal of Combinatorial Mathematics and Combinatorial Computing**, Volume 68, pages 163-191, 2009.

11. S. Sarkar and S. Maitra. Construction of rotation symmetric Boolean functions with optimal algebraic immunity. Special Issue on Applied Cryptography & Data Security, **Journal of Computacion y Sistemas**, Mexico, volume 12, no. 3, pages 267-284, 2009.

12. D. K. Dalai and S. Maitra. Algebraic Immunity of Boolean Functions – Analysis and Construction. Accepted in the Special Issue on Applied Cryptography & Data Security, **Journal of Computacion y Sistemas**, Mexico, volume 12, no. 3, pages 297-321, 2009.

13. S. Maitra, Y. V. Subba Rao, P. Stanica and S. Gangopadhyay. Nontrivial solutions to the cubic sieve congruence problem: $x^3 \equiv y^2 z \bmod p$. Accepted in the Special Issue on Applied Cryptography & Data Security, **Journal of Computacion y Sistemas**, Mexico, volume 12, no. 3, pages 253-266, 2009.

2008

14. G. Paul, S. Rathi and S. Maitra. On Non-negligible Bias of the First Output Byte of RC4 towards the First Three Bytes of the Secret Key. **Designs, Codes and Cryptography**, special issue of in memory of Hans Dobbertin, 49(1-3): 123-134 (2008).

15. S. Sarkar and S. Maitra. Idempotents in the Neighbourhood of Patterson-Wiedemann Functions having Walsh Spectra Zeros. **Designs, Codes and Cryptography**, special issue of in memory of Hans Dobbertin, 49(1-3): 95-103 (2008).

16. P. Stănică and S. Maitra. Rotation Symmetric Boolean Functions – Count and Cryptographic Properties. **Discrete Applied mathematics**, 156(10): 1567-1580 (2008). Available at http://dx.doi.org/10.1016/j.dam.2007.04.029

17. R. Basu, S. Ganguly, S. Maitra, G. Paul. A Complete Characterization of the Evolution of RC4 Pseudo Random Generation Algorithm. **Journal of Mathematical Cryptology**, Pages 257–289, Volume 2, Issue 3, October 2008.

18. S. Ruj, S. Maitra and B. Roy. Key predistribution using transversal design on a grid of wireless sensor network. **Ad Hoc & Sensor Wireless Networks**, Volume 5, Number 3-4, Pages 247–264, 2008.

2007

19. P. Sarkar and S. Maitra. Balancedness and Correlation Immunity of Symmetric Boolean Functions. **Discrete Mathematics**, Volume 307, Issues 19-20, 28 September

2007, Pages 2351-2358.
Available at http://dx.doi.org/10.1016/j.disc.2006.08.008

20. S. L. Braunstein, B.-S. Choi, S. Ghosh and S. Maitra. Exact quantum algorithm to distinguish Boolean functions of different weights. In **Journal of Physics A: Mathematical and Theoretical**, Volume: 40, Pages 8441-8454, doi:10.1088/1751-8113/40/29/017, published: 3 July 2007.

21. S. Kavut, S. Maitra, M. D. Yucel. Search for Boolean Functions with Excellent Profiles in the Rotation Symmetric Class. In **IEEE Transactions on Information Theory**, 53(5): 1743-1751, May 2007.

2006

22. S. Maitra and E. Pasalic. A Maiorana-McFarland type Construction for Resilient Boolean Functions on n Variables (n Even) with Nonlinearity $> 2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2}$. **Discrete Applied Mathematics**, Volume 154, Issue 2, February 2006, Pages 357-369, Special issue on Coding and Cryptography.

23. S. Gangopadhyay, P. H. Keskar and S. Maitra. Patterson-Wiedemann Construction Revisited. In **Discrete Mathematics**, Volume 306, Issue 14, Pages 1540–1556, 2006. A special issue containing selected papers from "R.C. Bose Centennial Symposium on discrete mathematics and Applications" December 2002.

24. T. K. Das, S. Maitra and J. Zhou. Cryptanalysis of Chu's DCT Based Watermarking Scheme. In **IEEE Transactions on Multimedia**, Volume 8, Number 3, Pages 629–632, June 2006.

25. D. Chakrabarti, S. Maitra and B. Roy. A Key Pre-distribution Scheme for Wireless Sensor Networks: Merging Blocks in Combinatorial Design. In **International Journal of Information Security**, Pages 105–114, Volume 5, Number 2, April 2006.

26. D. K. Dalai, S. Maitra and S. Sarkar. Basic Theory in Construction of Boolean Functions with Maximum Possible Annihilator Immunity. In **Designs, Codes and Cryptography**, Volume 40, Number 1, Pages 41–58, July 2006.

27. C. Carlet, D. K. Dalai, K. C. Gupta and S. Maitra. Algebraic Immunity for Cryptographically Significant Boolean Functions: Analysis and Construction. **IEEE Transactions on Information Theory**, Pages 3105–3121, Volume 52, Number 7, July 2006.

28. T. K. Das and S. Maitra. Analysis of the "Wavelet Tree Quantization" Watermarking Strategy and a Modified Robust Scheme. **Multimedia System Journal**, 12(2): 151-163 (2006).

2005

29. T. K. Das, S. Maitra and J. Mitra. Cryptanalysis of Optimal Differential Energy Watermarking (DEW) and a Modified Robust Scheme. **IEEE Transactions on Signal Processing**, PART II, 53(2):768–775, February 2005.

30. S. Maitra and P. Mukhopadhyay. Deutsch-Jozsa Algorithm Revisited in the Domain of Cryptographically Significant Boolean Functions. In **International Journal on Quantum Information**, Pages 359–370, Volume 3, Number 2, June 2005.

31. S. Maitra, K. C. Gupta and A. Venkateswarlu. Results on Multiples of Primitive Polynomials and Their Products over GF(2). **Theoretical Computer Science**, 341 (2005) 311-343, September 2005.

32. D. Chakrabarti, S. Maitra and B. Roy. Clique Size in Sensor Networks with Key Predistribution based on Transversal Design. In **International Journal of Distributed Sensor Networks**, Volume 1, No. 3-4, Pages 345–354, 2005.

2004

33. D. P. Mukherjee, S. Maitra and S. T. Acton. Spatial domain digital watermarking of multimedia objects for buyer authentication. **IEEE Transactions on Multimedia**, 6(1):1–15, February 2004.

34. T. K. Das and S. Maitra. Cryptanalysis of Correlation Based Watermarking Schemes using Single Watermarked Copy. **IEEE Signal Processing Letters**, 446–449, 11(4), April 2004.

35. S. Maitra. On Nonlinearity and Autocorrelation Properties of Correlation Immune Boolean Functions. **Journal of Information Science and Engineering**, 20:305–323, 2004.

36. P. Sarkar and S. Maitra. Construction of nonlinear resilient Boolean functions using "small" affine functions. **IEEE Transactions on Information Theory**, September 2004, 50(9), Pages 2185–2193.

37. S. Maitra. Autocorrelation Values of Highly Nonlinear Balanced Boolean Functions on Even Number of Variables. In **Journal of the Indian Statistical Association**, Vol 42, No. 2, Pages 219–229, 2004. Special Issue on Statistics in Cryptology.

38. E. Pasalic, S. Maitra, T. Johansson, and P. Sarkar. New Constructions of Resilient and Correlation Immune Boolean Functions Achieving the Upper Bound on Nonlinearity. In **Journal of the Indian Statistical Association**, Vol 42, No. 2, Pages 287–307, 2004. Special Issue on Statistics in Cryptology.

39. J. A. Clark, J. L. Jacob, S. Maitra and P. Stanica. Almost Boolean Functions: The Design of Boolean Functions by Spectral Inversion. **Computational Intelligence**, Pages 450–462, Volume 20, Number 3, 2004.

2003

40. P. Stănică and S. Maitra. A constructive count of Rotation Symmetric functions. **Information Processing Letters**, 88:299–304, December 2003.

41. P. Sarkar and S. Maitra. Efficient Implementation of Cryptographically Useful "Large" Boolean Functions. **IEEE Transactions on Computers**, special issue on Cryptographic Hardware and Embedded Systems, 52(4):410–417, April 2003.

2002

42. S. Maitra and P. Sarkar. Modifications of Patterson-Wiedemann functions for cryptographic applications. **IEEE Transactions on Information Theory**, 48(1):278–284, January 2002.

43. S. Maitra and P. Sarkar. Characterization of symmetric bent functions – An elementary proof. **Journal of Combinatorial Mathematics and Combinatorial Computing**, Volume 43, Pages 227–230, 2002.

44. S. Maitra and P. Sarkar. Cryptographically significant Boolean functions with five valued Walsh spectra. **Theoretical Computer Science**, Volume 276, Number 1–2, pages 133-146, 2002.

45. S. Maitra and P. Sarkar. Maximum Nonlinearity of Symmetric Boolean Functions on Odd Number of Variables. **IEEE Transactions on Information Theory**, 48(9):2626–2630, September 2002.

46. E. Pasalic and S. Maitra. Linear codes in generalized construction of resilient functions with very high nonlinearity. **IEEE Transactions on Information Theory**, 48(8):2182–2191, August 2002.

47. S. Maitra and E. Pasalic. Further constructions of resilient Boolean functions with very high nonlinearity. **IEEE Transactions on Information Theory**, 48(7):1825–1834, July 2002.

48. S. Maitra. Highly nonlinear balanced Boolean functions with good local and global avalanche characteristics. **Information Processing Letters**, July 2002, 83(5), Pages 281–286.

49. P. Sarkar and S. Maitra. Cross-correlation analysis of cryptographically useful Boolean functions and S-boxes. **Theory of Computing Systems**, 35(1):39–57, 2002.

1999

50. S. Maitra and P. Sarkar. Hamming weights of correlation immune Boolean functions. **Information Processing Letters**, 71(3-4):149–153, 1999.

51. S. Maitra, B. K. Roy, and P. Sarkar. Ciphertext only attack on LFSR based encryption scheme. **Calcutta Statistical Association Bulletin**, 49(195-196):239–254, 1999.

1.2 Refereed Conferences

Papers marked * have been accepted in refereed journals later and they are included in the previous list of journal papers.

2010

52. S. Maitra, S. Sarkar and S. Sen Gupta. Factoring RSA Modulus using Prime Reconstruction from Random Known Bits. In *Africacrypt 2010*, May 3–6, 2010, Stellenbosch, South Africa. To be published in Lecture Notes in Computer Science, Springer Verlag, 2010.

53. S. Maitra and S. Sarkar. Efficient CRT-RSA Decryption for Small Encryption Exponents. In *CT-RSA 2010*, March 1-5, 2010, San Francisco, CA, USA. Pages 26–40, volume 5985, Lecture Notes in Computer Science, Springer Verlag, 2010.

2009

54. S. Sarkar and S. Maitra. Partial Key Exposure Attack on CRT-RSA. In *ACNS 2009*, Paris-Rocquencourt, France, June 2-5, 2009, Pages 473–484, volume 5536, Lecture Notes in Computer Science, Springer Verlag, 2009.

55. R. Basu, S. Maitra, G. Paul and T. Talukdar. On Some Sequences of the Secret Pseudo-Random Index j in RC4 Key Scheduling. Accepted in *18th Symposium on Applied algebra, Algebraic algorithms, and Error Correcting Codes (AAECC 2009)*, Catalonia, Spain, June 8-12, 2009, to be published in Lecture Notes in Computer Science, Springer Verlag.

56. * S. Maitra, G. Paul and S. Raizada. Some Observations on HC-128. In *WCC 2009, International Workshop on Coding and Cryptography*, May 10-15, 2009, Ullensvang, Norway.

57. S. Maitra and S. Sarkar. Deterministic Polynomial-Time Equivalence of Computing the CRT-RSA Secret Keys and Factoring. In *WCC 2009, International Workshop on Coding and Cryptography*, May 10-15, 2009, Ullensvang, Norway.

2008

58. S. Maitra and G. Paul. Analysis of RC4 and Proposal of Additional Layers for Better Security Margin. In *INDOCRYPT 2008*. Pages 27–39, volume 5365, Lecture Notes in Computer Science, Springer Verlag, 2008.

59. S. Maitra, S. Sarkar. A New Class of Weak Encryption Exponents in RSA. In *INDOCRYPT 2008*. Pages 337–349, volume 5365, Lecture Notes in Computer Science, Springer Verlag, 2008.

60. * S. Sarkar and S. Maitra. Improved Partial Key Exposure Attacks on RSA by Guessing a few Bits of one of the Prime Factors. In *ICISC 2008*, December 3–5, 2008, Seoul, Korea. Pages 37–51, volume 5461, Lecture Notes in Computer Science, Springer Verlag, 2009.

61. S. Maitra and S. Sarkar. Revisiting Wiener's Attack – New Weak Keys in RSA. In *ISC 2008, 11th Information Security Conference,* September 15-18, 2008, Taipei, Taiwan. Pages 228–243, volume 5222, Lecture Notes in Computer Science, Springer Verlag, 2008.

62. * S. Gangopadhyay, D. Sharma, S. Sarkar and S. Maitra. On Affine (Non) Equivalence of Bent Functions. In *CECC 2008, 8th Central European Conference on Cryptography*, July 2-4, 2008, Graz, Austria.

63. S. Maitra, S. Kavut, M. D. Yucel. Balanced Boolean function on 13-variables having nonlinearity greater than the bent concatenation bound. In *Fourth International Workshop on Boolean Functions: Cryptography and Applications, BFCA 08*, May 19–21, 2008, Copenhagen, Denmark.

64. S. Maitra and G. Paul. Recovering RC4 Permutation from 2048 Keystream Bytes if j is Stuck. In *13th Australiasian Conference on Information Security and Privacy, ACISP 2008.* Pages 306–320, volume 5107, Lecture Notes in Computer Science, Springer Verlag, 2008.

65. * R. Basu, S. Ganguly, S. Maitra, G. Paul. RC4 Keystream Always Leaks Information about the Hidden Index j. In *SASC 2008 - The State of the Art of Stream Ciphers*, Special Workshop hosted by the ECRYPT Network of Excellence, Lausanne, Switzerland, February 13-14, 2008.

66. * S. Maitra and G. Paul. New Form of Permutation Bias and Secret Key Leakage in Keystream Bytes of RC4. In *Workshop on Fast Software Encryption, FSE 2008.* Pages 253–269, volume 5086, Lecture Notes in Computer Science, Springer Verlag, 2008.

2007

67. G. Paul, S. Maitra and R. Srivastava. On Non-Randomness of the Permutation after RC4 Key Scheduling. In *Applied Algebra, Algebraic Algorithms, and Error Correcting Codes (AAECC-17)*, Indian Institute of Science, Bangalore, December 16-20, 2007, pages 100–109, volume 4851, Lecture Notes in Computer Science, Springer Verlag, 2007.

68. * S. Sarkar and S. Maitra. Construction of Rotation Symmetric Boolean Functions on Odd Number of Variables with Maximum Algebraic Immunity. In *Applied Algebra, Algebraic Algorithms, and Error Correcting Codes (AAECC-17)*, Indian Institute of

Science, Bangalore, December 16-20, 2007, pages 271–280, volume 4851, Lecture Notes in Computer Science, Springer Verlag, 2007.

69. * G. Paul and S. Maitra. Permutation after RC4 Key Scheduling Reveals the Secret Key. In *Selected Areas in Cryptography, 14th International Workshop, SAC 2007*, August 16-17, Ottawa, Canada, pages 360–377, volume 4876, Lecture Notes in Computer Science, Springer Verlag, 2007.

70. * S. Sarkar and S. Maitra. Idempotents in the Neighbourhood of Patterson-Wiedemann Functions having Walsh Spectra Zeros. In *WCC 2007, International Workshop on Coding and Cryptography*, Pages 351–360, April 16-20, 2007, Versailles (France).

71. * G. Paul, S. Rathi and S. Maitra. On Non-negligible Bias of the First Output Byte of RC4 towards the First Three Bytes of the Secret Key. In *WCC 2007, International Workshop on Coding and Cryptography*, Pages 285–294, April 16-20, 2007, Versailles (France).

72. * D. K. Dalai and S. Maitra. Balanced Boolean Functions with (more than) Maximum Algebraic Immunity. In *WCC 2007, International Workshop on Coding and Cryptography*, Pages 99–108, April 16-20, 2007, Versailles (France).

73. S. Kavut, M. Yucel and S. Maitra. Construction of Resilient Functions by the Concatenation of Boolean Functions Having nonintersecting Walsh Spectra. In *Third International Workshop on Boolean Functions: Cryptography and Applications, BFCA 07*, May 2–3, 2007, Paris, France.

74. S. Maitra, S. Sarkar and D. K. Dalai. On Dihedral Group Invariant Boolean Functions. In *Third International Workshop on Boolean Functions: Cryptography and Applications, BFCA 07*, May 2–3, 2007, Paris, France.

2006

75. * C. Carlet, D. K. Dalai, and S. Maitra. Cryptographic Properties and Structure of Boolean Functions with Full Algebraic Immunity. In *IEEE International Symposium on Information Theory, ISIT 2006.*

76. * S. Sarkar and S. Maitra. Efficient search for symmetric Boolean functions under constraints on Walsh spectra values. In *Second International Workshop on Boolean Functions: Cryptography and Applications, BFCA 06*, Pages 29–50, March 13–15, 2006, LIFAR, University of Rouen, France.

77. * D. K. Dalai, S. Maitra and S. Sarkar. Results on rotation symmetric Bent functions. In *Second International Workshop on Boolean Functions: Cryptography and Applications, BFCA 06*, Pages 137–156, March 13–15, 2006, LIFAR, University of Rouen, France.

78. D. K. Dalai, K. C. Gupta and S. Maitra. Notion of algebraic immunity and its evaluation related to fast algebraic attacks. In *Second International Workshop on Boolean Functions: Cryptography and Applications, BFCA 06*, Pages 107–124, March 13–15, 2006, LIFAR, University of Rouen, France.

79. * S. Kavut, S. Maitra, M. D. Yucel. Autocorrelation spectra of balanced boolean functions on odd number input variables with maximum absolute value $< 2^{\frac{n+1}{2}}$. In *Second International Workshop on Boolean Functions: Cryptography and Applications, BFCA 06*, Pages 73–86, March 13–15, 2006, LIFAR, University of Rouen, France.

80. * D. K. Dalai and S. Maitra. Reducing the Number of Homogeneous Linear Equations in Finding Annihilators. *Sequences and Their Applications, SETA'06*, 4th International Conference, Beijing, China, September 24-28, 2006, pages 376–390, volume 4086, Lecture Notes in Computer Science, Springer Verlag, 2006.

2005

81. * D. K. Dalai, K. C. Gupta and S. Maitra. Cryptographically Significant Boolean functions: Construction and Analysis in terms of Algebraic Immunity. In *Workshop on Fast Software Encryption, FSE 2005*, pages 98–111, number 3557, Lecture Notes in Computer Science, Springer-Verlag.

82. A. Maximov, M. Hell, S. Maitra. Plateaued Rotation Symmetric Boolean Functions on Odd Number of Variables. In *First Workshop on Boolean Functions: Cryptography and Applications, BFCA 05*, Pages 83–104, March 7–9, 2005, LIFAR, University of Rouen, France.

83. * D. Chakrabarti, S. Maitra and B. Roy. A Key Pre-distribution Scheme for Wireless Sensor Networks: Merging Blocks in Combinatorial Design. In *8th Information Security Conference, ISC'05*, Page 89–103, Lecture Notes in Computer Science, volume 3650, Springer Verlag.

84. T. K. Das, H. J. Kim and S. Maitra. Security Evaluation of Generalized Patchwork Algorithm from Cryptanalytic Viewpoint. In *Knowledge-Based Intelligent Information and Engineering Systems, 9th International Conference, KES 2005, Melbourne, Australia, September 14-16, 2005, Proceedings, Part I*, Pages 1240–1247, volume 3681 in Lecture Notes in Computer Science.

85. S. Maitra, T. K. Das and J. Zhou. An Information Hiding Framework for Lightweight Mobile Devices with Digital Camera. In *Pattern Recognition and Machine Intelligence, First International Conference, PReMI 2005*, Pages 491–496, volume 3776 in Lecture Notes in Computer Science.

86. * B. -S. Choi, S. L. Braunstein, S. Maitra, D. Chakrabarti, S. Ghosh and P. Mukhopadhyay. Quantum Weight Decision Algorithm of a Boolean Function. In *ERATO*

conference on Quantum Information Science 2005, EQIS 2005, National Museum of Emerging Science and Innovation, JST, Tokyo, JAPAN, August 26-30, 2005.

87. D. Chakrabarti, S. Maitra and B. Roy. A Hybrid Design of Key Pre-distribution Scheme for Wireless Sensor Networks. In *1st International Conference on Information Systems Security, ICISS 2005*, pages 228–238, volume 3803, Lecture Notes in Computer Science, Springer Verlag, 2005.

88. C. Carlet, S. Gangopadhyay and S. Maitra. Crosscorrelation spectra of Dillon type functions. In *IWSDA 2005, the 2nd international workshop on sequence design and its application in communication*, October 10–14, 2005, Japan.

89. * D. Chakrabarti, S. Maitra and B. Roy. Clique Size in Sensor Networks with Key Pre-distribution based on Transversal Design. In *7th International Workshop on Distributed Computing, IWDC 2005*, pages 329–337, number 3741, Lecture Notes in Computer Science, Springer Verlag, December 2005.

2004

90. * S. Maity and S. Maitra. Minimum Distance between Bent and 1-resilient Boolean Functions. In *Workshop on Fast Software Encryption, FSE 2004*, New Delhi, India, February 5–7, 2004, number 3017 in Lecture Notes in Computer Science. Pages 143–160. Springer Verlag, 2004.

91. P. Stanica, S. Maitra and J. A. Clark. Results on Rotation Symmetric Bent and Correlation Immune Boolean Functions. In *Workshop on Fast Software Encryption, FSE 2004*, New Delhi, India, February 5–7, 2004, number 3017 in Lecture Notes in Computer Science. Pages 161–177. Springer Verlag, 2004.

92. M. Hell, A. Maximov, S. Maitra. On efficient implementation of search strategy for rotation symmetric Boolean functions. In *Ninth International Workshop on Algebraic and Combinatorial Coding Theory, ACCT 2004*, June 19–25, 2004, Black Sea Coast, Bulgaria.

93. T. K. Das, J. Zhou and S. Maitra. Cryptanalysis of a Wavelet Based Watermarking Scheme. In *International Workshop on Digital Watermarking, IWDW 2004*, number 3304 in Lecture Notes in Computer Science. Pages 192–203. Springer Verlag, 2005.

94. * D. K. Dalai, K. C. Gupta and S. Maitra. Results on Algebraic Immunity for Cryptographically Significant Boolean Functions. In *INDOCRYPT 2004*, number 3348 in Lecture Notes in Computer Science, Page 92–106, Springer Verlag, December 2004.

95. * T. K. Das and S. Maitra. Cryptanalysis of "Wavelet Tree Quantization" Watermarking Scheme. In *International Workshop on Distributed Computing, IWDC 2004*,

number 3326 in Lecture Notes in Computer Science. Pages 219–230. Springer Verlag, 2004.

2003

96. * J. A. Clark, J. L. Jacob, S. Maitra and P. Stanica. Almost Boolean Functions: The Design of Boolean Functions by Spectral Inversion. In *CEC 2003, the 2003 Congress on Evolutionary Computation*, Volume 3 in the proceedings, page 2173–2180, IEEE Press, December 8–12, 2003, Canberra, Australia.

97. S. Chowdhury and S. Maitra. Efficient Software Implementation of LFSR and Boolean Function and Its Application in Nonlinear Combiner Model. In *ACNS 2003*, number 2846 in Lecture Notes in Computer Science. Pages 387–402. Springer Verlag, October 16–19, 2003.

98. D. P. Mukherjee and S. Maitra. Robust Buyer Authentication Scheme for Multimedia Object. In 2003 IEEE International Conference on Multimedia & Expo. Baltimore, M. D., USA, July 6–9, 2003.

99. * E. Pasalic and S. Maitra. A Maiorana-McFarland type Construction for Resilient Boolean Functions on n Variables (n Even) with Nonlinearity $> 2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2}$. In *Workshop on Coding and Cryptography - WCC 2003*, France, March 2003, Page 365–374.

2002

100. * S. Maitra, K. C. Gupta and A. Venkateswarlu. Multiples of Primitive Polynomials and Their Products over GF(2). In *Selected Areas in Cryptography, SAC 2002, August 2002*, Pages 214–231, number 2595 in Lecture Notes in Computer Science, Springer Verlag, 2003.

101. * T. K. Das and S. Maitra. Cryptanalysis of Correlation Based Watermark using Single Copy. In *IEEE Information Theory Workshop, ITW 2002*, Page 204, Bangalore, India, October 2002.

102. * P. Stănică and S. Maitra. Rotation Symmetric Boolean Functions – Count and Cryptographic Properties. In *R. C. Bose Centenary Symposium on Discrete Mathematics and Applications*, Electronic Notes in Discrete Mathematics, Elsevier, December 2002.

103. * S. Gangopadhyay, P. H. Keskar and S. Maitra. Patterson-Wiedemann Construction Revisited. In *R. C. Bose Centenary Symposium on Discrete Mathematics and Applications*, Electronic Notes in Discrete Mathematics, Elsevier, December 2002.

104. * P. Sarkar and S. Maitra. Balancedness and Correlation Immunity of Symmetric Boolean Functions. In *R. C. Bose Centenary Symposium on Discrete Mathematics and Applications*, Electronic Notes in Discrete Mathematics, Elsevier, December 2002.

105. T. K. Das and S. Maitra. A Robust Block Oriented Watermarking Scheme in Spatial Domain. In *ICICS 2002*, number 2513 in Lecture Notes in Computer Science, page 184–196, Springer Verlag, December 2002.

106. * A. Venkateswarlu and S. Maitra. Further Results on Multiples of Primitive Polynomials and Their Products over GF(2). In *ICICS 2002*, number 2513 in Lecture Notes in Computer Science, page 231–242, Springer Verlag, December 2002.

107. * T. K. Das and S. Maitra. Cryptanalysis of Optimal Differential Energy Watermarking (DEW) and a Modified Robust Scheme. In *INDOCRYPT 2002*, number 2551 in Lecture Notes in Computer Science, Page 135–148, Springer Verlag, December 2002.

108. S. Gangopadhyay and S. Maitra. Further results related to Generalized Nonlinearity. In *INDOCRYPT 2002*, number 2551 in Lecture Notes in Computer Science, Page 260–274, Springer Verlag, December 2002.

109. J. Clark, J. Jacob, S. Stepney, S. Maitra and W. Millan. Evolving Boolean Functions Satisfying Multiple Criteria. In *INDOCRYPT 2002*, number 2551 in Lecture Notes in Computer Science, Page 246–259, Springer Verlag, December 2002.

2001

110. * S. Maitra. Highly nonlinear balanced Boolean functions with very good autocorrelation property. In *Workshop on Coding and Cryptography - WCC 2001*, Electronic Notes in Discrete Mathematics, Volume 6. Elsevier, January 2001.

111. * E. Pasalic, S. Maitra, T. Johansson, and P. Sarkar. New constructions of resilient and correlation immune Boolean functions achieving upper bounds on nonlinearity. In *Workshop on Coding and Cryptography - WCC 2001*, Electronic Notes in Discrete Mathematics, Volume 6. Elsevier, January 2001.

112. * S. Maitra and E. Pasalic. Further constructions of resilient Boolean functions with very high nonlinearity. *Sequences and Their Applications, SETA'01*, Bergen, Norway, May 13–17, 2001. The proceedings is published in the series Discrete Mathematics and Theoretical Computer Science, pages 265–280. Springer-Verlag, May 2001.

113. * P. Sarkar and S. Maitra. Efficient implementation of Large stream cipher systems. In *Workshop on Cryptographic Hardware and Embedded Systems, CHES 2001*, number 2162 in Lecture Notes in Computer Science, Pages 319–332, Springer Verlag, May 2001.

114. * E. Pasalic and S. Maitra. Linear codes in constructing resilient functions with high nonlinearity. In *Selected Areas in Cryptography - SAC 2001*, number 2259 in Lecture Notes in Computer Science. Pages 60–74, Springer Verlag, August 2001.

115. * K. C. Gupta and S. Maitra. Primitive polynomials over GF(2) – A cryptologic approach. In *ICICS 2001*, number 2229 in Lecture Notes in Computer Science, Pages 23–34, Springer Verlag, November 2001.

116. * K. C. Gupta and S. Maitra. Multiples of primitive polynomials over GF(2). INDOCRYPT 2001, number 2247 in Lecture Notes in Computer Science. Pages 62–72. Springer Verlag, December 2001.

117. * S. Maitra. Autocorrelation Properties of correlation immune Boolean function, INDOCRYPT 2001, number 2247, Lecture Notes in Computer Science, pages 242–253, Springer Verlag, December 2001.

118. S. Chowdhury and S. Maitra. Efficient software implementation of Linear Feedback Shift Registers. INDOCRYPT 2001, number 2247 in Lecture Notes in Computer Science. Pages 297–307. Springer Verlag, December 2001.

119. * S. Maitra and D. P. Mukherjee. Spatial domain digital watermarking with buyer authentication. INDOCRYPT 2001, number 2247 in Lecture Notes in Computer Science. Pages 149–161. Springer Verlag, December 2001.

2000

120. * P. Sarkar and S. Maitra. Construction of nonlinear Boolean functions with important cryptographic properties. In *Advances in Cryptology - EUROCRYPT 2000*, number 1807 in Lecture Notes in Computer Science, pages 485–506. Springer Verlag, May 2000.

121. P. Sarkar and S. Maitra. Nonlinearity bounds and constructions of resilient Boolean functions. In *Advances in Cryptology - CRYPTO 2000*, number 1880 in Lecture Notes in Computer Science, pages 515–532. Springer Verlag, August 2000.

1999

122. S. Maitra and P. Sarkar. Enumeration of correlation immune Boolean functions. In *4th Australasian Conference on Information, Security and Privacy*, number 1587 in Lecture Notes in Computer Science, pages 12–25. Springer Verlag, April 1999.

123. S. Maitra and P. Sarkar. Highly nonlinear resilient functions optimizing Siegenthaler's inequality. In *Advances in Cryptology - CRYPTO'99*, number 1666 in Lecture Notes in Computer Science, pages 198–215. Springer Verlag, August 1999.

1998

124. S. Maitra and A. Bagchi. Dynamic restructuring of classification hierarchy towards data mining. In *9th International Conference on Management of Data*, COMAD 1998, pages 143–160, Tata McGraw Hill.

1.3 Edited Conference Proceedings

1. Subhamoy Maitra, C. E. Veni Madhavan, Ramarathnam Venkatesan (Eds.): Progress in Cryptology - INDOCRYPT 2005, 6th International Conference on Cryptology in India, Bangalore, India, December 10-12, 2005, Proceedings. Lecture Notes in Computer Science 3797, Springer, 2005, ISBN 3-540-30805-9.

2. Thomas Johansson, Subhamoy Maitra (Eds.): Progress in Cryptology - INDOCRYPT 2003, 4th International Conference on Cryptology in India, New Delhi, India, December 8-10, 2003, Proceedings. Lecture Notes in Computer Science 2904, Springer, 2003, ISBN 3-540-20609-4.

1.4 Book Chapters

1. H. -J. Kim, S. Xiang, I.-K. Yeo, and S. Maitra.
   Chapter VIII: Robustness Analysis of Patchwork Watermarking Schemes.
   Book Title: Digital Audio Watermarking Techniques and Technologies: Applications and Benchmark.
   Editors: Nedeljko Cvejic, Tapio Seppanen.
   Publisher: Igi Global. July 2007. ISBN: 978-1-59904-513-9

2. S. Maitra and B. Roy.
   Chapter: Secure communication in Distributed Sensor Networks (DSN).
   Book Title: Handbook of Applied Algorithms: Solving Scientific, Engineering and Practical Problems.
   Editors: Amiya Nayak and Ivan Stojmenovic.
   Publisher: Wiley-IEEE Press. December 2007. ISBN: 978-0-470-04492-6

1.5 Externally Funded Projects

Served in Governmental and Industry sponsored projects worth 2 million US$ in last 10 years.

2 Other Academic Information

2.1 Teaching Activities

2.1.1 Thesis Supervision

1. Dr. Deepak Kumar Dalai received his PhD degree (Title: On Some Necessary Conditions of Boolean Functions to Resist Algebraic Attacks) in Computer Science from Indian Statistical Institute in 2006.

2. Dr. Tanmoy Kanti Das received his PhD degree (Title: Analysis and Design of Digital Watermarking Schemes) in Computer Science in the year 2006 from Jadavpur University (co-supervisor: Prof. Debesh Das).

3. Dr. Sumanta Sarkar received his PhD degree (Title: Combinatorial Aspects in Construction of Cryptographically Significant Boolean Functions under different Symmetry Conditions) in Mathematics in the year 2008 from Jadavpur University.

4. Dr. Goutam Paul received his PhD degree (Title: Analysis and Design of RC4 and its Variants) in Computer Science in the year 2009 from Jadavpur University.

5. Supervised more than 10 students for M. Tech. (CS) dissertation at Indian Statistical Institute.

2.1.2 Courses taught at Indian Statistical Institute, Kolkata

20 courses in last 10 years at B. Stat, M. Stat and M. Tech. level in the area of Computer Science. Each course is of approximately 50 hours per semester.

2.1.3 Teaching outside Indian Statistical Institute

1. Invited to present some lectures in the area of Stream Ciphers in a week long International workshop in September, 2006 at the Information Security Group, Deakin University, Australia.

2. Invited to present some lectures on Cryptanalysis of Digital Watermarking Schemes at Institute of Infocomm Research, National University of Singapore, November, 2004.

3. Invited to present a half day long lecture on Cryptology as a Tutorial Speaker at the Second International Conference on Information Systems Security (ICISS 2006), December, 2006, Kolkata.

4. Invited to present some lectures in the area of Programming and Data Structure as a part of Quality Improvement Program at IIT, Guahati, November, 2004.

2.2 Important Professional and Editorial Works

1. Editorial Board Member of the International Journal "Cryptography and Communications: Discrete Structures, Boolean Functions and Sequences", published by Springer.

2. Program co-chair of Indocrypt 2003 and 2005.

3. Served as program committee member for

   - Indocrypt 2002;
   - Information Security, 8th International Conference, Singapore, ISC 2005;
   - 11th Australasian Conference on Information Security and Privacy, ACISP 2006;
   - The Third International Workshop on Signal Design and Its Applications in Communications, China, IWSDA 2007;
   - Information Security, 11th International Conference, Taiwan, ISC 2008.

4. Reviewed papers for many other leading cryptology conferences like Crypto, Eurocrypt, Asiacrypt, SAC, FSE etc.

5. Journal paper review:
   IEEE Transactions on Information Theory,
   Journal of Cryptology,
   IEEE Transactions on Multimedia,
   Designs Codes and Cryptography,
   Theoretical Computer Science,
   Discrete Applied Mathematics,
   Discrete Mathematics,
   Information Processing Letters,
   Applicable Algebra in Engineering Communication and Computing,
   and many other journals.

2.3 Design and Development of Computer Software

1. A library of functions to study the cryptographic and combinatorial properties of Boolean functions.

2. Tools for analysis and design of watermarking and steganographic schemes.

3. Tools for cryptanalysis of different stream ciphers.

   These softwares were developed as part of different external projects.

2.4 Professional awards/honours received

1. **Invited Speaker** in the **First National Cryptology Symposium in Turkey**, at Middle East Technical University (METU), Ankara, Turkey, during November 18-20, 2005.
2. **Nominated from Japanese Ministry of Foreign Affairs (MOFA)** as one of the Indian experts to discuss co-operation possibilities between India and Japan in the areas of Biotechnology, Nanotechnology and Information and Communication Technology during October 16–17, 2006 at Tokyo, Japan.

2.5 Other Relevant Information

2.5.1 Short Academic Visits

1. Information Security Group, Deakin University, Australia, September, 2006.
2. Department of Mathematics, Middle East Technical University, Ankara, Turkey, November, 2005.
3. Institute of Infocomm Reserach, National University of Singapore, November, 2004.

2.5.2 Sports

Nominated as the **Best Footballer** in the Football Tournament Organized by Indian Statistical Institute Club in the year 2006.

3 Earlier Experiences as Computer Professional

Cumulative experience: 3 years.

3.1 At DAIS Infotech

Organization	Dais Infotech Pvt. Ltd.
Address	SDF Building, Module 223-226, Salt Lake, Calcutta, Pin: 700 091
Designation	Software Engineer
Duration	1st August, 1996 to 3rd April, 1997

Software Projects :

1. Communication Software for handshaking PCs (OS: WINDOWS'95) with back end Mainframe Systems using Windows Programming with VC++.

2. Internet based Shipping Management Software using CGI (in C) with INFORMIX as back end database.

3. Development of Web Tools (mainly search engine) using JAVA.

3.2 At CMC Limited

Organization	CMC Limited
Address	28, Camac Street, Calcutta, Pin: 700 016
Designation	Information Technology Engineer
Duration	1st June, 1992 to 31st July, 1994

Software and Hardware Maintenance and Installation at

1. Railway Reservation System, Calcutta.

2. Indian Statistical Institute, Calcutta.

3. Gun and Shell Factory, Cossipore.

4. Calcutta State Transport Corporation, Belghoria.

Software Projects

1. Maintenance of Railway Reservation System. This is the nationwide railway reservation system in India. The software was developed in FORTRAN using VAX FORMS for screens. The operating system is VMS.

2. Communication Software for connecting VAX 8650 and VAXSTATION 2000 using C on VMS operating system.

3. Transport Management Software using COBOL on UNIX platform.