REFERENCES

1. PGP, Version 6. 0, "An Introduction to Cryptography," Copyright © 1990-1998 Network Associates, Inc. and its Affiliated Companies, USA, August 1998
2. David Kahn, "The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet," The New American Library, Inc., USA, February 1973
3. Bruce Schneier, "Applied Cryptography," Second Edition, Wiley Computer Publishing, 1996
4. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "HANDBOOK of APPLIED CRYPTOGRAPHY," Fourth Printing, CRC Press, July 1999.
5. Nik Goots, Boris Izotov, Alex Moldovyan, Nik Moldovyan, "Modern Cryptography: Protect Your Data with Fast Block Ciphers," A-LIST Publishing, 2003
6. Thomas W. Korner, "Coding and Cryptography," Lecture Notes of a IIA course on Codes and Cryptography at the Department of Mathematics at University of Cambridge, UK, July 1998.
7. Toshinobu Kaneko, "Report on Present State of Symmetric-Key Cipher evaluations," CRYPTREC 2001, January 2002
8. Robshaw, M. J. B., "Stream ciphers," RSA Laboratories Technical Report TR-701, Version 2. 0, July 1995
9. James L. Massey, "Design and Analysis of Block Ciphers,"EIDMA Minicourse, Eindhoven University of Technology, May 2000
10. Alex Biryukov, "Block Ciphers and Stream Ciphers: The State of the Art," Cryptology ePrint Archive 2004/094, 2004
11. Richard J. De Moliner, "On the Statistical Testing of Block Ciphers," PhD Thesis, SWISS FEDERAL INSTITUTE OF TECHNOLOGY ZURICH, 1999
12. Jean-Sebastien Coron, "Evaluation of Cryptographic Techniques," CRYPTREC, FY2002 (Overseas), 2002
13. Toshinobu Kaneko, "Report on Evaluation of Symmetric-Key Cryptographic Techniques," CRYPTREC 2002-2003, Information-

Technology Promotion Agency, Japan Telecommunications Advancement Organization of Japan, May 2003

14. Thomas Jakobsen, "Correlation Attacks on Block Ciphers," Master's Thesis, Department of Mathematics, Technical University of Denmark, January 1996
15. E. Filiol, "Decimation attack of stream ciphers," In E. Okamoto B. Roy, editor, Progress in Cryptology - INDOCRYPT 2000, number 1977 in Lecture Notes in Computer Science, pp. 31-42, Springer-Verlag, 2000.
16. S. Petrović, Amparo Fster-Sabater, "Cryptanalysis of the A5/2 algorithm," in Cryptology ePrint Archive, Report 2000/52, 2000
17. National Institute of Standards and Technology. FIPS PUB 46-3: Data Encryption Standard (DES). National Institute for Standards and Technology, Gaithersburg, MD, USA, October 1999.
18. National Institute of Standards and Technology. FIPS Standard "Announcing the ADVANCED ENCRYPTION STANDARD (AES)," in Federal Information Processing Standards Publication, No. 197, November 2001
19. J. Daemen, V. Rijmen, "AES proposal: Rijndael," Technical report, National Institute of Standards and Technology (NIST), March 2000
20. Ed Dawson, Helen Gustafson, Matt Henricksen, Bill Millan, "Evaluation of RC4 Stream Cipher," CRYPTREC, FY2002 (Overseas), 2002
21. R. L. Rivest, M. J. B. Robshaw, R. Sidney and Y. L. Yin, "The RC6 Block Cipher", v1. 1, August 1998
22. J. Jonsson, J. -O. Larsson, and M. Robshaw, "On the Statistical Testing of RC6," AES Round 2 public comment, April 2000
23. J. L. Massey, G. H. Khachatrian, and M. K. Kuregian, "Nomination of SAFER+ as Candidate Algorithm for the Advance Encryption Standard," Proceeding of the first Advanced Encryption Standard Candidate Conference, 1998
24. Bruce Schneier, "Risks of Relying on Cryptography," COMMUNICATIONS OF THE ACM, Vol. 42, No. 10, October 1999
25. Alireza Nemaney Pour, "Number Theory and related Algorithms in Cryptography," Master's thesis, School of Information Science, Japan Advanced Institute of Science and Technology, September 2002

26. X. M. Zhang, Y. Zheng, Hideki Imai, "Relating differential distribution tables to other properties of substitution boxes," Designs, Codes and Cryptography, Vol. 19, pp. 45-63, 2000
27. Daniel Olejar, Martin Stanek, "On Cryptographic Properties of Random Boolean Functions," Journal of Universal Computer Science, Vol. 4, Issue 8, pp. 705-717, 1998
28. C. Carlet, P. Sarkar, "Spectral domain analysis of correlation immune and resilient Boolean functions," Finite fields Appl., Vol. 8, pp. 120-130, 2002
29. E. Pasalic, T. Johansson, S. Maitra, P. Sarkar, "New construction of resilient and correlation immune Boolean functions achieving upper bounds on nonlinearity," ePrint archive 2000/048, 2000
30. K. Gopalakrishnan, D. R. Stinson, "A Short Proof of the Non-Existence of Certain Cryptographic Functions," Journal of Combinatorial Mathematics and Combinatorial Computing, Vol. 20, pp. 129-137, 1996
31. Masashi Mitomo, Kaoru Kurosawa, "How to Encrypt Long Messages without Large Size Symmetric/Asymmetric Encryption Schemes," Cryptology ePrint Archive, Report 2000/065, 2000
32. National Institute of Standards and Technology. FIPS PUB 140-2: "SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES." National Institute for Standards and Technology, MD, USA, 2002
33. S. Brands, R. D. Gill, "Cryptography, statistics and pseudo-randomness, I," Prob. Math. Statist. Vol. 15, pp. 101-114, 1995
34. S. Brands, R. D. Gill, "Cryptography, statistics and pseudo-randomness, II," Prob. Math. Statist. Vol. 16, pp. 1-17, 1996
35. Soumen Maity, Thomas Johansson, "Construction of Cryptographically Important Boolean Functions," INDOCRYPT 2002, pp. 234-245, 2002
36. Subhamoy Maitra, "Highly Nonlinear Balanced Boolean Functions with very good Autocorrelation Property," Cryptology ePrint Archive, Report 2000/047, 2000
37. E. Filiol, C. Fontaine, "Highly nonlinear balanced Boolean functions with a good correlation-immunity," Advances in Cryptology - EUROCRYPT'98, LNCS 1403, pp. 475-488, Springer-Verlag, 1998
38. Palash Sarkar, Subhamoy Maitra, "Balancedness and Correlation Immunity of Symmetric Boolean Functions," Proceedings of the R. C.

Bose Centenary Symposium, Electronics Notes in Discrete Mathematics, Vol. 15, pp. 178-183, May 2003

39. Subhamoy Maitra, "Correlation Immune Boolean Functions with Very High Nonlinearity," Cryptology ePrint Archive, Report 2000/054, 2000
40. Subhamoy Maitra, "On Nonlinearity and Autocorrelation Properties of Correlation Immune Boolean Functions," J. Inf. Sci. Eng. Vol. 20, No. 2, pp. 305-323, 2004
41. T. Johansson, E. Pasalic. "A construction of resilient functions with high nonlinearity," IEEE Tran. on Info. Theory, Vol. 49, No. 2, pp. 494-501, 2003
42. Yuriy Tarannikov, "On Resilient Boolean Functions with Maximal Possible Nonlinearity," INDOCRYPT 2000, pp. 19-30, 2000
43. Y. Tarannikov, "New constructions of resilient Boolean functions with maximal nonlinearity," ePrint archive 2000/069 and in Fast Software Encryption FSE'2001
44. Yu. Tarannikov, D. Kirienko, "Spectral analysis of high order correlation immune functions," Proceedings of 2001 IEEE International Symposium on Information Theory ISIT-2001, pp. 69, Washington, DC, USA, June 2001
45. Yuliang Zheng, Xian-Mo Zhang, "Connections among nonlinearity, avalanche and correlation immunity," Theoretical Computer Science, Vol. 292, No. 3, pp. 697-710, January 2003
46. National Institute of Standards and Technology. NIST Special Publication 800-22: "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," USA, May 2001
47. Web Sites:
48. http://www.wikipedia.org
49. http://www.nist.org
50. http://www.nist.gov
51. Angelo P. E. Rosiello, "Design of a Synchronous Stream Cipher from Hash Functions", IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.8, August 2007

52. Souradyuti Paulz, Bart Preneelz, and Gautham Sekarzy, "Distinguishing Attacks on the Stream Cipher Py", In the proceedings of FSE 2006 (Matt Robshaw, ed.), LNCS, Springer, 2006, pp.405-421.
53. D. Chang, K. C. Gupta amd M. Nandi, "RC4-Hash : A New Hash Function based on RC4", In Proceedings of Indocrypt 2006, pp 80-94, Lecture Notes in Computer Science 4329, Springer Verlag, 2006.
54. Guang Gong, Kishan Chand Gupta, Martin Hell, Yassir Nawaz, "Towards a General RC4-Like Keystream Generator", CISC 2005, 162-174
55. Serge Vaudenay, Martin Vuagnoux, "Passive-Only Key Recovery Attacks on RC4", Selected Areas in Cryptography 2007, pp 344-359