Reference Papers

[S1] Biryukov, Shamir, “Wagner: Real Time Cryptanalysis of A5/1 on a PC,” FSE2000

[S2] Canteaut, Filiol, “Ciphertext Only Reconstruction of Stream Ciphers based on Combination Generator,” FSE2000

[S3] Chepyzhov, Johansson, Smeets, “A simple algorithm for fast correlation attacks on stream ciphers,” FSE2000

[S4] Ding, “The Differential Cryptanalysis and Design of Natural Stream Ciphers,” Fast Software Encryption, Cambridge Security Workshop, December 1993, LNCS 809

[S5] Ding, Xiao, Sham, “The Stability Theory of Stream Ciphers,” LNCS 561

[S6] Johansson, Jonsson, “Fast correlation attacks based on Turbo code techniques,” CRYPTO’99, August 99, 19th Annual International Cryptology Conference, LNCS 1666

[S7] Fossorier, Mihaljevic, Imai, “Critical Noise for Convergence of Iterative Probabilistic Decoding with Belief Propagation in Cryptographic Applications,” LNCS 1719.

[S8] Golic, “Linear Cryptanalysis of Stream Ciphers,” Fast Software Encryption, Second International Workshop, December 1994, LNCS 1008.

[S9] Johansson, Jonsson, “Improved Fast Correlation Attacks in Stream Ciphers via Convolutional codes,” EUROCRYPT’99, International Conference on the Theory and Application of Cryptographic Techniques, May 1999, LNCS 1592

[S10] Meier, Staffelbach, “Correlation Properties of Comniners with Memory in Stream Ciphers,” Journal of Cryptology 5(1992)

[S11] Palit, Roy, “Cryptanalysis of LFSR-Encrypted Codes with Unknown Combining,” LNCS 1716

[S12] Ruppel, “Correlation Immunity and Summation Generator,” CRYPTO’85 Proceedings, August 85, LNCS 218.

[S13] Sigenthalar, “Decrypting a class of Ciphers using Ciphertext only,” IEEE C-34.

[S14] Tanaka, Ohishi, Kaneko, “An Optimized Linear Attack on Pseudorandom Generators using a Non-Linear Combiner, Information Security,” First International Workshop, ISW’97 Proceedings, September 1997, LNCS 1396

[S15] Zeng, Huang, “On the Linear Syndrome Method in Cryptanalysis,” CRYPTO’88 Proceedings, August 1988, LNCS 403.

[S16] Zeng, Yang, Rao, “On the Linear Consistency Test in cryptanalysis and its applications,” CRYPTO’89 Proceedings, August 89, LNCS 435.

[S17] Zeng, Yang, Rao, “An improved Linear Syndrome Algorithm in Cryptanalysis with Applications,” CRYPTO’90 Proceedings, August 90, LNCS 537.

[S18] Zeng, Yang, Wei, Rao, “Pseudorandom Bit Generators in Stream-Cipher

Cryptography," IEEE Computer Feb-1991

[B1] L.R. Knudsen, "Practically Secure Fesitel Ciphers," 1st Fast Software Encryption(1993), LNCS 809, pp.211-221, Springer-Verlag, 1994.

[B2] M.E. Hellman, "A Cryptanalytic Time-Memory Trade-Off," IEEE Trans. On Information Theory,26(4), pp.401-406,1980.

[B3] E. Biham, A. Shamir, "Differential Cryptanalysis of DES-Like Cryptosystems," Journal of Cryptology, 4(1), pp.3-72, 1991.

[B4] L.R. Knudsen, T.A. Berson, "Truncated Differentials of SAFER," 3rd Fast Software Encryption(1996), LNCS 1039, pp.15-25, Springer-Verlag, 1996.

[B5] S. Lucks, "On the Security of the 128-Bit Block Cipher DEAL," 6th Fast Software Encryption(1999), LNCS 1636pp.60-69, Springer-Verlag, 1999

[B6] D. Wagner, "The Boomerang Attack," 6th Fast Software Encryption(1999), LNCS 1636pp.156-170, Springer-Verlag, 1999

[B7] M. Matsui, "Linear Cryptanalysis Method for DES Cipher," EUROCRYPT'93, LNCS 765, pp.386-397, Springer-Verlag, 1994.

[B8] P. Hawkes, "Differential-Linear Week Key Class of IDEA," EUROCRYPT'98, LNCS 1403, pp.112-126, Springer-Verlag, 1994.

[B9] M. Tanaka, T. Hamaide, K. Hisamatsu and T. Kaneko, "Linear cryptanalysis by Linear Sieve Method," IECE Transactions on Fundamentals of Electronics, Communications and Computer Science, E81-A(1), pp.82-87, 1998.

[B10] L.R. Knudsen, "Truncated and Higher Order Differentials," 2nd Fast Software Encryption(1996), LNCS 1008, pp.196-211, Springer-Verlag, 1995.

[B11] T. Jakobsen and L.R. Knudsen, " The Interpolation Attack on Block Ciphers," 4th Fast Software Encryption(1997), LNCS 1267, pp.28-40, Springer-Verlag, 1997.

[B12] E. Biham, A. Biryukov, N. Ferguson, L.R. Knudsen, B. Schneier, A. Shamir, "Cryptanalysis of Magenta," 2nd AES Conference, pp. 182-183, 1999.

[B13] A. Biryukov, D. Wanger, "Slide Attacks," 6th Fast Software Encryption(1999), LNCS 1636, pp.245-259, Springer-Verlag, 1999.

[B14] E. Biham, "New Type of Cryptanalytic Attacks Using Related Keys," EUROCRYPTO'93 LNCS 765, pp.398-409, Springer-Verlag, 1993.

[B15] C. Harpes, J.L. Massey, "Partitioning Cryptanalysis," FSE'97, LNCS 1267, pp.13-27, Springer-Verlag, 1997.

[B16] J. Kelsey, B. Schneier, and D. Wagner, "Mod n Cryptanalysis, with Applications against RC5P and M6," FSE'99, LNCS1636, pp.139-155, Springer-Verlag, 1999.

[B17] V. Rijmen, B. Preneel and E.D. Win, "On Weaknesses of Non-surjective Round

Functions," Designs, Codes and Cryptography, 12, pp.253-266, 1997.
[B18] J.Daemen and V. Rijmen, "Resistance against Implementaion Attacks: A Comparative Study of the AES Proposals," 2nd AES Conference, pp.122-133, 1999.
[B19] P. Kocher, "Timing Attackes on Implementations of Diffe-Hellman, RSA, DSS, and Other systems," CRYPTO'96, LNCS 1109, pp.104-113, Springer-Verlag, 1996.
[B20] TAO Research Project on Info-communication Security, "Technical Report on Design, Analysis and Use of Block Ciphers," Telecommunications Advancements Organization of Japan, 2000 (in Japanese).

[H1] H.Dobbertin, "Crypanalyasis of MD4," Fast software encryption,Springer-Verlag, 1996, pp.53-69
[H2] H.Dobbertin, "The status of MD5 after recent attack," CryptoBytes, 2(2), Sep., 1996, pp.1.-6
[H3] F. Chabaud and A. Joux, "Differential Collisions in SHA-0," Advances in Cryptology-Crypto'94, Springer-Verlag,pp.56-71
[H4] B.den Boer and A, Bosselaersm " An attack on the last two rounds of MD4," Advances in Cryptology-Crypto'91, Springer-Verlag, pp.194-203
[H5] E.Biham, and A.Shamir, Differential cryptanalysis of the Data encryption Standard, Springer-Verlag, 1993
[H6] M. Bellare, J.Kilian, and P.Rogaway, " The security of cipher blocks chaining," Advances in Cryptology-Crypto'94, Springer-Verlag, pp.341-358
[H7] Preneel and Knudsen, Hash Functions Based on Block Ciphers and Quaternary Codes, Advances in Cryptology - Proc. AsiaCrypt'96, LNCS 1163, pp. 77-90, Springer Verlag, 1996.
[H8] B. Preneel and P.C. van Oorschot and Knudsen, "MDx-MAC and building fast MACs from hash functions," Advances in Cryptology, Proceedings Crypto'95, LNCS 963, D. Coppersmith, Ed., Springer-Verlag, 1995, pp. 1-14.

[R1] Ruppel: Analysis and Design of stream ciphers, Springer-Verlag, Berlin,1986
[R2] Niederreiter: "The probabilistic theory of liner complexity", Advances in Cryptology-EUROCRYPTO '88 (LNCS 330), 191-209, 1988
[R3] Niederreiter: "A combinatorial approach to probabilistic results on the liner-complexity profile of random sequences", Journal of Cryptology, 2(1990), 105-112
[R4] Niederreiter: "Keystream sequences with a good linear complexity profile for every starting point", Advances in Cryptology-EUROCRYPTO '89 (LNCS 433), 523-532,1990
[R5] Niederreiter: "The linear complexity profile and the jump complexity of keystream

sequences", Advances in Cryptology-EUROCRYPTO '90 (LNCS 473), 174-188, 1991
[R6] Jansen and Boekee: "On the significance of the directed asyclic word graph in cryptology", Advances in Cryptology-AUSCRYPTO '90 (LNCS 453), 318-326,1990
[R7] Jansen and Boekee: "The shortest feedback shift register that can generate a given sequence", Advances in cryptology-CRYPTO '89 (LNCS 435), 90-99, 1990
[R8] Ziv and Lempel: "On the complexity of finite sequences", IEEE Transactions on Information Theory, 22(1976), 75-81
[R9] Erdmann: "Empirical tests of binary keystreams", Master's thesis, Department of Mathematics, Royal Holloway and Bedford New College, University of London, 1992
[R10] Kolmogorov: "Three approaches to the definition of the concept 'quantity of information'", Problemy Peredachi Informatsii, 1(1965), 3-11
[R11] Chaitin: "On the length of programs for computing finite binary sequences", Journal of the association for Computing Machinery, 13(1996), 547-569
[R12] Meier and Staffelbach: "Fast atacks on certin stream ciphers", Journal of Cryptography, 1(1989), 159-176
[R13] Chepyzhov and Smeets, "On a fast correlation attack on certain stream ciphers", Advances in Cryptography-EUROCRYPTO '91 (LNCS 547), 176-185,1991
[R14] Coppersmith, Krawczyk, and Mansour, "The shrinking generator", Advances in Cryptography-CRYPTO '93 (LNCS 773), 22,39,1994
[R15] Rubin, "Decrypting a stream cipher based on J-K flip-flops", IEEE Transaction on computers, 28(1979), 483-487
[R16] Zeng, Yang, and Rao, "On the linearsyndrome algorithm in cryptanalysis with applications", Advanves in Cryptology-CRYPTO '90 (LNCS 537), 34-37,1991
[R17] Siegenthaler, "Decrypting a class of stream cipher using ciphertext only", IEEE Transactions on Computers, 34(1985), 81-85
[R18] Golic, "Correlation via linear sequential circuit approximation of combiners with memory", Advances in Cryptology-EUROCRYPT '92 (LNCS 658), 113-123, 1993
[R19] Siegenthaler, "Cryptanalysts representation of nonlinear filtered ML-sequences", Advances in Cryptology-EUROCRYPTO '85 (LNCS 219), 103-110, 1986
[R20] Ding, "The differential cryptanalysis and design of natural stream ciphers", R. Anderson, editor, Fast Software Encryption, Cambridge Security Workshop (LNCS 809), 101-115, Springer-Verlag
[R21] Zeng, Yang, and Rao, "On the linear consistency test (LCT) in cryptanalysis with applications", Advances in Cryptology-CRYPTO '89 (LNCS 435), 164-174,1990
[R22] Massey and Rueppel, "Linear ciphers and random sequence generators with multiple clocks", Advances in Cryptology-Preceedings of EUROCRYPT 84 (LNCS 209),

74-87, 1985
[R23] Gunther, "Alternating step generators controlled by de Bruijn sequence", Adnances in Cryptology-EUROCRYPT '87 (LNCS 304), 5-14, 1988
[R24] Zivkovic, "An algorithm for the initial state reconstruction of the clock-contorolled shift register", IEEE Transactions on information Theory, 37(1991), 1488-1490