Abkürzungen

AAECC =

ACCT = International Workshop on Algebraic and Combinatorial Coding Theory

ACS =

ASIACRYPT = Advances in Cryptology Proceedings, Springer Lecture Notes in Computer Science

AUSCRYPT = Advances in Cryptology Proceedings, Springer Lecture Notes in Computer Science

CRYPTO = Advances in Cryptology Proceedings, Springer Lecture Notes in Computer Science

EUROCRYPT = Advances in Cryptology Proceedings, Springer Lecture Notes in Computer Science

FSE = Fast Software Encryption Proceedings, Springer Lecture Notes in Computer Science

ICC = International Conference on Combinatorics, Information Theory and Statistics

IEEE =

IEICE =

ISIT = IEEE International Symposium on Information Theory

LIENS = Laboratoire d'informatique de l'Ecole Normale Supérieure Paris

LMS = London Mathematical Society

SAC = Selected Areas on Cryptography

Literatur

[1] C. Adams, S. Tavares: The structured design of cryptographically good S-boxes. Journal of Crytology 3 (1990), 27–41.

[2] Carlisle Adams: Designing DES-like ciphers with guaranteed resistance to differential and linear attacks. SAC 95.

[3] K. G. Beauchamp: *Applications of Walsh and Related Functions.* Academic Press, London 1984.

[4] T. Beth, C. Ding: On almost perfect nonlinear permutations. EUROCRYPT 93, 65–76.

[5] Eli Biham, Adi Shamir: Differential cryptanalysis of DES-like cryptosystems. CRYPTO 90, 2–21.

[6] Eli Biham, Adi Shamir: Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology 4 (1991), 3–72.

[7] Eli Biham, Adi Shamir: Differential cryptanalysis of FEAL and N-Hash. EUROCRYPT 91, 1–16.

[8] Eli Biham, Adi Shamir: Differential cryptanalysis of the full 16-round DES. CRYPTO 92, 487–496.

[9] Eli Biham, Adi Shamir: *Differential cryptanalysis of the Data Encryption Standard.* Springer-Verlag 1993.

[10] Eli Biham: On Matsui's linear cryptanalysis. EUROCRYPT 94, 341–355.

[11] Lawrence Brown, Matthew Kwan, Josef Pieprzyk, Jennifer Seberry: Improving resistance to differential cryptanalysis and the redesign of LOKI. Technical Report CS38/91, Dep.of Computer Science, Canberra.

[12] P. Camion, A. Canteaut: Correlation-immune and resilient functions over a finite alphabet and their applications in cryptography. Designs, Codes, and Cryptography 16 (1999), 121–149.

[13] P. Camion, C. Carlet, P. Charpin, N. Sendrier: On correlation immune functions. CRYPTO 91, 86–100.

[14] Anne Canteaut: Differential cryptanalysis of Feistel ciphers and differentially δ-uniform mappings. SAC 97, 172–184.

[15] Anne Canteaut: Cryptographic functions and design criteria for block ciphers. INDOCRYPT 2001, 1–16.

[16] A. Canteaut, P. Charpin, H. Dobbertin: A new characterization of almost bent functions. FSE 99, 186–200.

[17] A. Canteaut, C. Carlet, P. Charpin, C. Fontaine: Propagation characteristics and correlation-immunity of highly nonlinear Boolean functions. EUROCRYPT 2000, 507–522.

[18] Anne Canteaut, Marion Videau: Degree of composition of highly nonlinear functions and applications to higher order differential cryptanalysis. EUROCRYPT 2002, 518–533.

[19] C. Carlet: Partially-bent functions. Crypto 92, 280–291.

[20] C. Carlet: Partially-bent functions. Designs, Codes, and Cryptography 3 (1993), 135–145.

[21] C. Carlet: Two new classes of bent functions. Eurocrypt 93, 77–101.

[22] C. Carlet: Hyperbent functions. Pragocrypt 96, 145–155.

[23] C. Carlet: A construction of bent functions. In: *Finite Fields and their Applications.* LMS Lecture Series 233.

[24] C. Carlet: A characterization of binary bent functions. ACCT-5/1996.

[25] C. Carlet: Recent results on bent functions. ICC 97.

[26] C. Carlet: More correlation immune und resilient functions over Galois fields and Galois rings. Eurocrypt 97, 422–433.

[27] C. Carlet: On cryptographic propagation criteria for Boolean functions. Information and Computation 151 (1999), 32–56.

[28] C. Carlet, P. Charpin, V. Zinoviev: Codes, bent functions and permutations suitable for DES-like cryptosystems. Designs, Codes, and Cryptography 15 (1998), 125–156.

[29] C. Carlet, P. Guillot: Une caractérisation des fonctions courbes. C. R. Acad. Sci. Paris (1995).

[30] C. Carlet, P. Guillot: A characterization of binary bent functions. J. Combinatorial Theory A 76 (1996), 328–335.

[31] C. Carlet, P. Guillot: A characterization of binary bent functions. ISIT 97, 451–.

[32] C. Carlet, P. Guillot: An alternate characterization of the bentness of binary functions, with uniqueness. Designs, Codes, and Cryptography 14 (1998), 133–140.

[33] C. Carlet, P. Guillot: A representation of Boolean functions. AAECC 13/1999.

[34] Florent Chabaud, Serge Vaudenay: Links between differential and linear cryptanalysis. Eurocrypt 94, 356–365.

[35] David Chaum, Jan-Hendrik Evertse: Cryptanalysis of DES with a reduced number of rounds Sequences of linear factors in block ciphers. Crypto 85, 192–211.

[36] Jung Hee Cheon: Nonlinear vector resilient functions. CRYPTO 2001, 458–469.

[37] J. H. Cheon, S. Chee, C. Park: S-boxes with controllable nonlinearity. EUROCRYPT 99, 286–294.

[38] Joan Daemen: *Cipher and hash function design strategies based on linear and differential cryptanalysis.* Dissertation, KU Leuven 1995.

[39] Joan Daemen, Vincent Rijmen: *The Design of Rijndael.* Springer-Verlag, Berlin usw. 2002.

[40] Donald W. Davies: Some regular properties of the DES. CRYPTO 81, 41–41.

[41] Donald W. Davies: Some regular properties of the 'Data Encryption Standard' algorithm. CRYPTO 82, 89–96.

[42] J. F. Dillon: A survey of bent functions. The NSA technical journal 1972, 191–215.

[43] Jan-Hendrik Evertse: Linear structures in block ciphers. EUROCRYPT 87, 249–266.

[44] E. Filiol, C. Fontaine: Highly nonlinear balanced boolean functions with a good correlation-immunity. EUROCRYPT 98, 475–488.

[45] Réjane Forré: The strict avalanche criterion: Spectral properties of Boolean functions and an extended definition. CRYPTO 88, 450–468.

[46] Joanne Fuller, William Millan: On linear redundancy in the AES S-box. Preprint Brisbane 2002.

[47] Carlo Harpes, Gerhard G. Kramer, James L. Massey: A generalization of linear cryptanalysis and the applicability of Matsui's piling-up lemma. EUROCRYPT 95, 24–38.

[48] H. M. Heys, S. E. Tavares: Substitution-permutation networks resistant to differential and linear cryptanalysis. Journal of Cryptology 9 (1996), 1–19.

[49] H. Heys: Modelling avalanche in DES-like ciphers. SAC 96.

[50] Howard M. Heys: A Tutorial on Linear and Differential Cryptanalysis. Memorial University of Newfoundland.

[51] T. Jakobsen: Cryptanalysis of block ciphers with probabilistic non-linear relations of low degree. CRYPTO 98, 212–222.

[52] Burton S. Kaliski Jr., Matt J. B. Robshaw: Linear cryptanalysis using multiple approximations. CRYPTO 94, 26–39.

[53] Yasuyoshi Kaneko, Fumihiko Sano, Kouichi Sakurai: On provable security against differential and linear cryptanalysis in generalized Feistel ciphers with multiple random functions. SAC 97.

[54] Liam Keliher, Henk Meijer, Stafford Tavares: New method for upper bounding the maximum average linear hull probability for SPNs. EUROCRYPT 2001, 420–436:

[55] Lars R. Knudsen: *Block Ciphers – Analysis, Design and Applications.* Aarhus University 1994.

[56] Lars R. Knudsen: Truncated and higher order differentials. FSE 94, 196–211.

[57] Lars R. Knudsen, Matt J. B. Robshaw: Non-linear approximations in linear cryptanalysis. EUROCRYPT 96, 224–236.

[58] Gilles Lachaud, Jacques Wolfmann: The weights of the orthogonals of the extended quadratic binary Goppa codes. IEEE Transactions on Information Theory 36 (1990), 686–692S.

[59] Xuejia Lai, James L. Massey: Markov ciphers and differential cryptanalysis. EUROCRYPT 91, 17–38.

[60] Susan K. Langford, Martin E. Hellman: Differential-linear cryptanalysis. CRYPTO 94, 17–25.

[61] Rudolf Lidl, Harald Niederreiter: *Finite Fields.* Encyclopedia of Mathematics and its Applications. Addison-Wesley, Reading 1983.

[62] Helger Lipmaa, Shiho Moriai: Efficient algorithms for computing differential properties of addition. FSE 2001.

[63] Sheelagh Lloyd: Counting functions satisfying a higher order strict avalanche criterion. EUROCRYPT 89, 63–74.

[64] Sheelagh Lloyd: Properties of binary functions. EUROCRYPT 90, 124-139.

[65] F. J. MacWilliams, N. J. A. Sloane: *The Theory of Error Correcting Codes.* North-Holland, Amsterdam 1977.

[66] Subhamoy Maitra: Autocorrelation Properties of correlation immune Boolean functions. INDOCRYPT 2001, 242–253.

[67] Subhamoy Maitra: Highly nonlinear balanced Boolean functions with very good autocorrelation property. Elsevier Preprint 2001.

[68] Mitsuru Matsui, Atsuhiro Yamagishi: A new method for known plaintext attack of FEAL cipher. EUROCRYPT 92, 81–91.

[69] Mitsuru Matsui: Linear cryptanalysis method for DES cipher. EUROCRYPT 93, 386–397.

[70] Mitsuru Matsui: The first experimental cryptanalysis of the Data Encryption Standard. CRYPTO 94, 1–11.

[71] Mitsuro Matsui: New structure of block cipos with provable security against differential and linear cryptanalysis. FSE 96, 205–218.

[72] Mitsuro Matsui: On a structure of block ciphers with provable security against differential and linear cryptanalysis: IEICE Trans. Fundamentals E82-A (1999), 117–122.

[73] Willi Meier, Othmar Staffelbach: Fast correlation attacks on stream ciphers. EUROCRYPT 88, 301–314.

[74] Willi Meier, Othmar Staffelbach: Nonlinearity criteria for cryptographic functions. EUROCRYPT 89, 549–562.

[75] William Millan, Andrew Clark, Ed Dawson: Smart hill climbing finds better Boolean functions. SAC 97.

[76] Serge Mister, Carlisle Adams: Practical S-box design. SAC 96.

[77] Pat Morin: Provably secure and efficient block ciphers. SAC 96.

[78] Kaisa Nyberg: Constructions of bent functions and difference sets. EUROCRYPT 90, 151–160.

[79] Kaisa Nyberg: Perfect nonlinear S-boxes. EUROCRYPT 91, 378–386.

[80] Kaisa Nyberg: On the construction of highly nonlinear permutations. EUROCRYPT 92, 92–98.

[81] Kaisa Nyberg: Differentially uniform mappings for cryptography. EUROCRYPT 93, 55–64.

[82] Kaisa Nyberg: Linear approximation of block ciphers. EUROCRYPT 94, 439–444.

[83] Kaisa Nyberg, Lars R. Knudsen: Provable security against differential cryptanalysis. CRYPTO 92, 566–574.

[84] Kaisa Nyberg, Lars R. Knudsen: Provable security against differential cryptanalysis. Journal of Cryptology 8 (1995), 27–37.

[85] Luke O'Connor: On the distribution of characteristics in bijective mappings. Journal of Cryptology 8 (1995), 67–86.

[86] Luke O'Connor: Convergence in differential distributions. EUROCRYPT 95, 13–23.

[87] Katsuo Ohta, Shiho Moriai, Katsumaro Aoki: Improving the search algorithm for the best linear expression. CRYPTO 95, 157–170.

[88] J. D. Olsen, R. A. Scholtz, L. R. Welch: Bent function sequences. IEEE Transactions on Information Theory IT-28 (1982), 858–864.

[89] Franz Pichler: On the Walsh-Fourier analysis of correlation immune switching functions. EUROCRYPT 86, 43–44.

[90] J. P. Pieprzyk, G. Finkelstein: Towards an effective non-linear crypto design. IEEE Proceedings 135 (1988), 325–335.

[91] Josef P. Pieprzyk: Non-linearity of exponent permutations. EUROCRYPT 89, 80–92.

[92] Josef P. Pieprzyk, C. Charnes, J. Seberry: Linear approximation versus nonlinearity. SAC 94.

[93] Bart Preneel, Werner van Leekwijck, Luc van Linden, René Govaerts, Joos Vandevalle: Propagation characteristics of Boolean functions. EUROCRYPT 90, 161–173.

[94] Bart Preneel, René Govaerts, Joos Vandevalle: Boolean functions satisfying higher order propagation criteria. EUROCRYPT 91, 141–152.

[95] J. A. Reeds, J. L. Manferdelli: DES has no per round linear factors. CRYPTO 84, 377–394.

[96] Vincent Rijmen: *Cryptanalysis and Design of Iterated Block Ciphers.* Dissertation, KU Leuven 1997.

[97] O. S. Rothaus: On „bent" functions. J. Combinatorial Theory A 20 (1976),´300–305.

[98] Palash Sarkar, Subhamoy Maitra: Nonlinearity bounds and constructions of resilient Boolean functions. CRYPTO 2000, 515–532.

[99] Palash Sarkar, Subhamoy Maitra: Construction of nonlinear Boolean functions with important cryptographic properties. EUROCRYPT 2000, 485–506.

[100] Jennifer Seberry, Xian-Mo Zhang, Yuliang Zheng: Highly nonlinear 0-1-balanced functions satisfying strict avalanche criterion. AUSCRYPT 92, 145–155.

[101] Jennifer Seberry, Xian-Mo Zhang, Yuliang Zheng: On constructions and nonlinearity of correlation immune functions. EUROCRYPT 93, 181–199.

[102] Jennifer Seberry, Xian-Mo Zhang, Yuliang Zheng: Nonlinearly balanced Boolean functions and their propagation characteristics. CRYPTO 93, 49–60.

[103] Jennifer Seberry, Xian-Mo Zhang, Yuliang Zheng: Relationships among nonlinearity criteria. EUROCRYPT 94, 376–388.

[104] Jennifer Seberry, Xian-Mo Zhang, Yuliang Zheng: Pitfalls in designing substitution boxes. CRYPTO 94, 383–396.

[105] Jennifer Seberry, Xian-Mo Zhang, Yuliang Zheng: Nonlinearity characteristics of quadratic substitution boxes. SAC 94.

[106] Adi Shamir: On the security of DES. CRYPTO 85, 280–281.

[107] Thomas Siegenthaler: Correlation immune polynomials over finite fields. EUROCRYPT 86, 42–42.

[108] J. Silverman: *The Arithmetic of Elliptic Curves.* Springer-Verlag, New York 1986.

[109] Yurij Tarannikov: New constructions of resilient Boolean functions with maximal nonlinearity. FSE 2001.

[110] Yurij Tarannikov, Peter Korolev, Anton Botev: Autocorrelation coefficients and correlation immunity of Boolean functions. ASIACRYPT 2001, 460–479.

[111] Serge Vaudenay: Provable security for block ciphers by decorrelation. LIENS–98–8.

[112] W. C. Waterhouse: Abelian varieties over finite fields. Ann. Sc. ENS 4 (1969), 521–560.

[113] A. F. Webster, S. E. Tavares: On the design of S-Boxes. CRYPTO 85, 523–534.

[114] Xiao Guo-Chen, J. Massey: A spectral characterization of correlation immune combining functions. IEEE Transactions on Information Theory 34 (1988), 569-571.

[115] A. M. Youssef, T. W. Cusick, P. Stănică, S. E. Tavares: New bounds on the number of functions satisfying the strict avalanche criterion. SAC 96.

[116] Amr M. Youssef, Guang Gong: Hyper-bent functions. EUROCRYPT 2001, 406–419.

[117] Muxiang Zhang, Agnes Chan: Maximum correlation analysis of nonlinear S-Boxes in stream ciphers. CRYPTO 2000, 501–514.

[118] Xian-Mo Zhang, Yuliang Zheng: Auto-correlations and new bounds on the non-linearity of Boolean functions. EUROCRYPT 96, 294–306.

[119] Xian-Mo Zhang, Yuliang Zheng: Difference distribution table of a regular substitution box. SAC 96.

[120] Xian-Mo Zhang, Yuliang Zheng, Hideki Imai: Non-existence of certain quadratic S-boxes and two bounds on nonlinear characteristics of general S-boxes. SAC 97.

[121] Xian-Mo Zhang, Yuliang Zheng: New lower bounds on nonlinearity and a class of highly nonlinear functions. Preprint.

[122] Yuliang Zheng, Xian-Mo Zhang: On relationships among avalanche, nonlinearity, and correlation immunity. ASIACRYPT 2000, 470–482.

[123] Yuliang Zheng, Xian-Mo Zhang: Improved upper bound on the nonlinearity of high order correlation immune functions. Preprint.

[124] Anna Zugaj, Karol Górski, Zbigniew Kotulski, Andrzej Paszkiewicz, Janusz Szczepański: New constructions in linear cryptanalysis of block ciphers. ACS 2000, 523–530.