Abkürzungen

AAECC =

ACCT = International Workshop on Algebraic and Combinatorial Coding Theory

ACS =

ACSIP = Australian Conference on Security and Information Privacy

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

DCC = Designs, Codes and Cryptography

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

ICISC = International Conference on Information Security and Cryptography

IEEE =

IEICE =

INDOCRYPT

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] Carlisle Adams, Stafford 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] E. R. Berlekamp, L. R. Welch: Weight distributions of the cosets of the (32,6) Reed-Muller code. IEEE Transactions on Information Theory 18 (1972), 203–207.

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

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

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

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

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

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

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

[12] Yuri Borissov, Nickolay Manev, Svetla Nikova: On the non-minimal codewords in the binary Reed-Muller code. ISIT 2001, Washington DC Ju´ne 24–29, 2001.

[13] Brouwer, Verhoeff: An updated table of minimum distance bounds for binary linear codes. IEEE Transactions on Information Theory 39 (1993), 662–677. [Online: `http://www.win.tue.nl/math/dw/voorlincod.html`]

[14] 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.

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

[16] Paul Camion, Claude Carlet, Pascale Charpin, N. Sendrier: On correlation immune functions. Crypto 91, 86–100.

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

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

[19] Anne Canteaut, Pascale Charpin, Hans Dobbertin: A new characterization of almost bent functions. FSE 99, 186–200.

[20] Anne Canteaut, Pascale Charpin, Hans Dobbertin: Weight divisibility of cyclic codes, highly nonlinear functions on $\mathbf{F}_{2^m}$, and crosscorrelation of maximum-length sequences. SIAM J. Discrete Math. 13 (2000), 105–138.

[21] Anne Canteaut, Claude Carlet, Pascale Charpin, Caroline Fontaine: Propagation characteristics and correlation-immunity of highly nonlinear Boolean functions. Eurocrypt 2000, 507–522.

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

[23] Claude Carlet: Partially-bent functions. Crypto 92, 280–291.

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

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

[26] Claude Carlet: Hyperbent functions. Pragocrypt 96, 145–155.

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

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

[29] Claude Carlet: Recent results on bent functions. ICC 97.

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

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

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

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

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

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

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

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

[38] Claude Carlet, Palash Sarkar: Spectral domain analysis of correlation immune and resilient Boolean functions. Finite Fields Appl. 8 (2002), 120–130.

[39] Claude Carlet, Jennifer Seberry, Xian-Mo Zhang: Comments on „Generating and counting binary bent sequences“. IEEE Trans. Inform. Th. 40 (1994), 600.

[40] Claude Carlet, Yurij Tarannikov: Covering sequences of Boolean functions and their cryptographic significance. DCC 25 (2002), 263–279.

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

[42] Chris Charnes, Martin Rötteler, Thomas Beth: Homogeneous bent functions, invariants, and designs. DCC 26 (2002), 139–154.

[43] 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.

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

[45] John A. Clark, Jeremy L. Jacob: Two-stage optimisation in the design of Boolean functions. ACSIP 2000.

[46] John A. Clark, Jeremy L. Jacob, Susan Stepney, Subhamoy Maitra, William Millan: Evolving Boolean functions satisfying multiple criteria. INDOCRYPT 2002.

[47] Jung Hee Cheon, Seongtaek Chee, Choonsik Park: S-boxes with controllable nonlinearity. EUROCRYPT 99, 286–294.

[48] Jung Hee Cheon, Seongtaek Chee: Nonlinearity of Boolean functions and hyperelliptic curves. SIAM J. Discrete Math. 16 (2003), 354–365.

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

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

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

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

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

[54] Hans Dobbertin: Almost perfect nonlinear power functions on GF(2^n): the Niho case. Information and Computation 151 (1999), 57–72.

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

[56] Eric Filiol, Caroline Fontaine: Highly nonlinear balanced boolean functions with a good correlation-immunity. EUROCRYPT 98, 475–488.

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

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

[59] K. Gopalakrishnan, D. R. Stinson: Three characterizations of non-binary correlation-immune and resilient functions. Designs, Codes and Cryptography 5 (1995), 241–251.

[60] 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.

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

[62] Howard M. Heys: Modelling avalanche in DES-like ciphers. SAC 96.

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

[64] Xiang-Dong Hou: GL(m,2) acting on R(r,m)/R(r-1,m). Discrete Mathematics 149 (1996), 99–122.

[65] Xiang-Dong Hou: Cubic bent functions. Discrete Mathematics 189 (1998), 149–161.

[66] T. Jakobsen: Cryptanalysis of block ciphers with probabilistic nonlinear relations of low degree. Crypto 98, 212–222.

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

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

[69] Tadao Kasami, Nobuki Tokura: On the weight structure of Reed-Muller codes. IEEE Transactions on Information Theory 16 (1970), 752–759.

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

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

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

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

[74] 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.

[75] Lai Xuejia: Higher order derivatives and differential cryptanalysis. Proc. Symp. on Communication, Coding and Cryptography in Honour of J. L. Massey, 1994.

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

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

[78] R. J. Lechner: A correspondence between equivalence classes of switching functions and group codes. IEEE Transactions on Computers 16 (1967), 621–624.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[107] N. J. Patterson, D. H. Wiedemann: The covering radius of the $[2^{15}, 16]$ Reed-Muller code is at least 16276. IEEE Transactions on Information Theory 29 (1983), 354–356. Correction. IEEE Transactions on Information Theory 36 (1990), 443.

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

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

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

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

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

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

[114] Qing Xiang: Maximally nonlinear functions and bent functions. DCC 17 (1999), 211–218.

[115] Qu Chengxin, Jennifer Seberry, Josef Pieprzyk: On the symmetric property of homogeneous Boolean functions. ACISP 99. Lecture Notes in Computer Science 1587 (1999), 26–35.

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

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

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

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

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

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

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

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

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

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

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

[127] Jennifer Seberry, Xian-Mo Zhang, Yuliang Zheng: GAC — the criterion for global avalanche characteristics of cryptographic functions. Preprint 1994.

[128] Jennifer Seberry, Xian-Mo Zhang, Yuliang Zheng: The relationship between propagation characteristic and nonlinearity of cryptographic functions. Preprint 1994.

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

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

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

[132] D. R. Stinson, J. L. Massey: An infinite class of counterexamples to a conjecture concerning nonlinear resilient functions. J. Cryptology 8 (1995), 167–173.

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

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

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

[136] Tadashi Wadayama, Toru Hada, Koichiro Wakasugi, Masao Kasahara: Upper and lower bounds on maximum nonlinearity of n-input and m-output Boolean functions. DCC 23 (2001), 23–33.

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

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

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

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

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

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

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

[144] Xian-Mo Zhang, Yuliang Zheng: Difference distribution table of a regular substitution box. SAC 96, 57–60.

[145] Xian-Mo Zhang, Yuliang Zheng: New lower bounds on nonlinearity and a class of highly nonlinear functions. ACISP 97, 147–158.

[146] Xian-Mo Zhang, Yuliang Zheng: The nonhomomorphicity of Boolean functions. SAC98, 280–295.

[147] 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, 27–39.

[148] Xian-Mo Zhang, Yuliang Zheng, Hideki Imai: Duality of Boolean functions and its cryptographic significance. ICICS 97, 159–169.

[149] Yuliang Zheng, Xian-Mo Zhang: The nonhomomorphicity of S-boxes. ICISC 98, 92–105.

[150] Yuliang Zheng, Xian-Mo Zhang: Strong linear dependence and unbiased distributions of non-propagative vecotrs. SAC 99, 92–105.

[151] Yuliang Zheng, Xian-Mo Zhang: Relationships between bent functions and complimentary plateaued functions. ICISC 99, 60–75.

[152] Yuliang Zheng, Xian-Mo Zhang: Plateaued functions. ICICS 99, 284–300.

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

[154] Yuliang Zheng, Xian-Mo Zhang: Non-separable cryptographic functions. Int. Symp. Information Theory and its Applications, Honolulu 2000, 51–58.

[155] Yuliang Zheng, Xian-Mo Zhang: On k-th order nonhomomorphicity of S-Boxes. J. Unic. Comp. Sci. 6 (2000), 830–848.

[156] Yuliang Zheng, Xian-Mo Zhang: Improved upper bound on the nonlinearity of high order correlation immune functions. SAC 2000, 262–274.

[157] Yuliang Zheng, Xian-Mo Zhang: A new property of Maiorana-McFarland functions. Bull. Inst. Comb. Appl. 33 (2001), 13–22.

[158] Yuliang Zheng, Xian-Mo Zhang, Hideki Imai: Connections between nonlinearity and restrictions, terms and hypergraphs of Boolean functions. IEEE Int. Symp. IT 1998, 439.

[159] Yuliang Zheng, Xian-Mo Zhang, Hideki Imai: Restrictions, terms and nonlinearity of Boolean functions. Theor. Comp. Sc. 226 (1999), 207–223.

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