References

[1] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Advances in Cryptology EUROCRYPT 93*, pp. 386–397, Springer, 1994.

[2] M. Hell, A. Maximov, and S. Maitra, "On efficient implementation of a search strategy for rotation symmetric Boolean functions," in *9th International Workshop on Algebraic and Combinatorial Coding Theory-ACCT 2004*, pp. 214–222, 2004.

[3] P. Stănică, S. Maitra, and J. A. Clark, "Results on rotation symmetric bent and correlation immune Boolean functions," in *Fast Software Encryption*, pp. 161–177, Springer, 2004.

[4] P. Stănică and S. Maitra, "Rotation symmetric Boolean functions count and cryptographic properties," *Discrete Applied Mathematics*, vol. 156, no. 10, pp. 1567–1580, 2008.

[5] J. Pieprzyk and C. X. Qu, "Fast hashing and rotation-symmetric functions," *Journal of Universal Computer Science*, vol. 5, no. 1, pp. 20–31, 1999.

[6] T. W. Cusick, "Affine equivalence of cubic homogeneous rotation symmetric functions," *Information Sciences*, vol. 181, no. 22, pp. 5067–5083, 2011.

[7] T. W. Cusick and P. Stănică, "Fast evaluation, weights and nonlinearity of rotation-symmetric functions," *Discrete Mathematics*, vol. 258, no. 1, pp. 289–301, 2002.

[8] S. Kavut, S. Maitra, S. Sarkar, and M. D. Yücel, "Enumeration of 9-variable rotation symmetric Boolean functions having nonlinearity > 240," in *Progress in Cryptology-INDOCRYPT 2006*, pp. 266–279, Springer, 2006.

[9] A. Maximov, M. Hell, and S. Maitra, "Plateaued rotation symmetric Boolean functions on odd number of variables," in *Proc. of First Workshop on Boolean Functions: Cryptography and Applications (BFCA 05)*, pp. 83–104, 2005.

[10] O. S. Rothaus, "On bent functions," *Journal of Combinatorial Theory, Series A*, vol. 20, no. 3, pp. 300–305, 1976.

[11] N. Patterson and D. Wiedemann, "The covering radius of the Reed-Muller code is at least 16276," *IEEE Transactions on Information Theory*, vol. 29, no. 3, pp. 354–356, 1983.

[12] S. Kavut, S. Maitra, and M. D. Yucel, "Search for Boolean functions with excellent profiles in the rotation symmetric class," *IEEE Transactions on Information Theory*, vol. 53, no. 5, pp. 1743–1751, 2007.

[13] Y. Li, "Results on rotation symmetric polynomials over GF(p)," *Information Sciences*, vol. 178, no. 1, pp. 280–286, 2008.

[14] S. Fu, C. Li, and B. Sun, "Enumeration of homogeneous rotation symmetric functions over F_p," in *Cryptology and Network Security*, pp. 278–284, Springer, 2008.

[15] S. Fu, C. Li, L. Qu, and D. Dong, "On the number of rotation symmetric functions over GF(p)," *Mathematical and Computer Modelling*, vol. 55, no. 1, pp. 142–150, 2012.

[16] T. W. Cusick and P. Stănică, *Cryptographic Boolean functions and applications*. Academic Press, 2009.

[17] S. Fu, C. Li, and L. Qu, "On the number of rotation symmetric Boolean functions," *Science China Information Sciences*, vol. 53, no. 3, pp. 537–545, 2010.

[18] H. Kim, S.-M. Park, and S. G. Hahn, "On the weight and nonlinearity of homogeneous rotation symmetric Boolean functions of degree 2," *Discrete Applied Mathematics*, vol. 157, no. 2, pp. 428–432, 2009.

[19] A. Brown and T. W. Cusick, "Equivalence classes for cubic rotation symmetric functions," *Cryptography and Communications*, vol. 5, no. 2, pp. 85–118, 2013.

[20] T. W. Cusick and Y. Cheon, "Affine equivalence of quartic homogeneous rotation symmetric Boolean functions," *Information Sciences*, vol. 259, pp. 192–211, 2014.

[21] P. Stănică, "Affine equivalence of quartic monomial rotation symmetric boolean functions in prime power dimension," *Information Sciences*, vol. 314, pp. 212–224, 2015.

[22] T. W. Cusick and P. Stănică, "Counting equivalence classes for monomial rotation symmetric boolean functions with prime dimension," *Cryptography and Communications*, pp. 1–15, 2015.

[23] J. H. Redfield, "The theory of group-reduced distributions," *American Journal of Mathematics*, pp. 433–455, 1927.

[24] G. Pólya, "Combinatorial number rules for groups, graphs and chemical compounds," *Acta mathematica*, vol. 68, no. 1, pp. 145–254, 1937.

[25] S. Golomb, "On the classification of Boolean functions," *IRE Transactions on Circuit Theory*, vol. 6, no. 5, pp. 176–186, 1959.

[26] R. Forré, "The strict avalanche criterion: spectral properties of Boolean functions and an extended definition," in *Proceedings on Advances in cryptology*, pp. 450–468, Springer-Verlag New York, Inc., 1990.

[27] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, vol. 16. Elsevier, 1977.

[28] H. Dobbertin, "Construction of bent functions and balanced Boolean functions with high nonlinearity," in *Fast Software Encryption*, pp. 61–74, Springer, 1995.

[29] J. F. Dillon, *Elementary Hadamard difference sets*. PhD thesis, University of Maryland, College Park., 1974.

[30] C. Carlet, "Two new classes of bent functions," in *Advances in cryptology-EUROCRYPT'93*, pp. 77–101, Springer, 1994.

[31] C. Adams and S. Tavares, "The structured design of cryptographically good S-boxes," *journal of Cryptology*, vol. 3, no. 1, pp. 27–41, 1990.

[32] J. Maiorana, "A class of bent functions," *R41 Technical Paper*, 1971.

[33] C. Carlet and S. Mesnager, "Improving the upper bounds on the covering radii of binary reed–muller codes," *IEEE Transactions on Information Theory*, vol. 53, no. 1, pp. 162–173, 2007.

[34] C. Carlet, "On bent and highly nonlinear balanced / resilient functions and their algebraic immunities," in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, pp. 1–28, Springer, 2006.

[35] T. Siegenthaler, "Correlation-immunity of nonlinear combining functions for cryptographic applications," *IEEE Transactions on Information Theory*, vol. 30, no. 5, pp. 776–780, 1984.

[36] G. Z. Xiao and J. L. Massey, "A spectral characterization of correlation-immune combining functions," *IEEE Transactions on Information Theory*, pp. 569–569, 1988.

[37] A. Webster and S. E. Tavares, "On the design of S-boxes," in *Advances in Cryptology-CRYPTO'85 Proceedings*, pp. 523–534, Springer, 1986.

[38] S. Lloyd, "Counting functions satisfying a higher order strict avalanche criterion," in *Advances in Cryptology—EUROCRYPT'89*, pp. 63–74, Springer, 1990.

[39] L. O'Connor, "An upper bound on the number of functions satisfying the strict avalanche criterion," *Information Processing Letters*, vol. 52, no. 6, pp. 325–327, 1994.

[40] T. W. Cusick, "Boolean functions satisfying a higher order strict avalanche criterion," in *Advances in Cryptology—EUROCRYPT'93*, pp. 102–117, Springer, 1994.

[41] T. W. Cusick, "Bounds on the number of functions satisfying the strict avalanche criterion," *Information processing letters*, vol. 57, no. 5, pp. 261–263, 1996.

[42] B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts, and J. Vandewalle, "Propagation characteristics of Boolean functions," in *Advances in Cryptology—EUROCRYPT'90*, pp. 161–173, Springer, 1991.

[43] X.-M. Zhang and Y. Zheng, "GAC-the criterion for global avalanche characteristics of cryptographic functions," in *Journal of Universal Computer Science*, pp. 320–337, Springer, 1996.

[44] N. T. Courtois and W. Meier, "Algebraic attacks on stream ciphers with linear feedback," in *Advances in Cryptology—EUROCRYPT 2003*, pp. 345–359, Springer, 2003.

[45] W. Meier, E. Pasalic, and C. Carlet, "Algebraic attacks and decomposition of Boolean functions," in *Advances in Cryptology-EUROCRYPT 2004*, pp. 474–491, Springer, 2004.

[46] C. Carlet, "Boolean functions for cryptography and error correcting codes," *Chapter of the monography Boolean Methods and Models, Y. Crama and P. Hammer eds*, 2006.

[47] J. Seberry, X.-M. Zhang, and Y. Zheng, "Nonlinearly balanced Boolean functions and their propagation characteristics," in *Advances in Cryptology-CRYPTO'93*, pp. 49–60, Springer, 1994.

[48] D. K. Dalai, K. C. Gupta, and S. Maitra, "Results on algebraic immunity for cryptographically significant Boolean functions," in *Progress in Cryptology-Indocrypt 2004*, pp. 92–106, Springer, 2005.

[49] M. Lobanov, "Tight bound between nonlinearity and algebraic immunity.," *IACR Cryptology ePrint Archive*, vol. 2005, p. 441, 2005.

[50] J. Seberry, X.-M. Zhang, and Y. Zheng, "On constructions and nonlinearity of correlation immune functions," in *Advances in Cryptology-EUROCRYPT'93*, pp. 181–199, Springer, 1994.

[51] S. Chee, S. Lee, D. Lee, and S. H. Sung, "On the correlation immune functions and their nonlinearity," in *Advances in Cryptology—ASIACRYPT'96*, pp. 232–243, Springer, 1996.

[52] P. Sarkar and S. Maitra, "Nonlinearity bounds and constructions of resilient Boolean functions," in *Advances in Cryptology-CRYPTO 2000*, pp. 515–532, Springer, 2000.

[53] Y. Zheng and X.-M. Zhang, "Improved upper bound on the nonlinearity of high order correlation immune functions," in *Selected Areas in Cryptography*, pp. 262–274, Springer, 2001.

[54] C. Carlet, "On the coset weight divisibility and nonlinearity of resilient and correlation-immune functions," in *Sequences and their Applications*, pp. 131–144, Springer, 2002.

[55] D. K. Dalai, S. Maitra, and S. Sarkar, "Results on rotation symmetric bent functions," *Discrete Mathematics*, vol. 309, no. 8, pp. 2398 – 2409, 2009.

[56] Q. Meng, L. Chen, and F.-W. Fu, "On homogeneous rotation symmetric bent functions," *Discrete Applied Mathematics*, vol. 158, no. 10, pp. 1111–1117, 2010.

[57] P. Stanica, "On the nonexistence of homogeneous rotation symmetric bent boolean functions of degree greater than two," *Proceedings of the NATO Advanced Study Institute on Boolean functions in Cryptology and Information Security,(IOS Press, Amsterdam, 2008)*, pp. 214–218, 2008.

[58] E. Filiol and C. Fontaine, "Highly nonlinear balanced boolean functions with a good correlation-immunity," in *Advances in Cryptology—EUROCRYPT'98*, pp. 475–488, Springer, 1998.

[59] Q. Li, G.-P. Gao, and W.-F. Liu, "Analysis of properties and counting of orbits for k-rotation symmetric Boolean functions," *Tongxin Xuebao/Journal on Communications*, vol. 33, no. 1, pp. 114–119, 2012.

[60] S. Fu, C. Li, L. Qu, and D. Dong, "On the number of rotation symmetric functions over GF(p)," *Mathematical and Computer Modelling*, vol. 55, no. 1–2, pp. 142 – 150, 2012.

[61] H. Kim, S.-M. Park, and S. G. Hahn, "On the weight and nonlinearity of homogeneous rotation symmetric Boolean functions of degree 2," *Discrete Applied Mathematics*, vol. 157, no. 2, pp. 428–432, 2009.

[62] M. L. Bileschi, T. W. Cusick, and D. Padgett, "Weights of Boolean cubic monomial rotation symmetric functions," *Cryptography and Communications*, vol. 4, no. 2, pp. 105–130, 2012.

[63] X. Zhang, H. Guo, R. Feng, and Y. Li, "Proof of a conjecture about rotation symmetric functions," *Discrete Mathematics*, vol. 311, no. 14, pp. 1281–1289, 2011.

[64] L. Yang, R. Wu, and S. Hong, "Nonlinearity of quartic rotation symmetric boolean functions.," *Southeast Asian Bulletin of Mathematics*, vol. 37, no. 6, 2013.

[65] T. W. Cusick and D. Padgett, "A recursive formula for weights of Boolean rotation symmetric functions," *Discrete Applied Mathematics*, vol. 160, no. 4-5, pp. 391–397, 2012.

[66] A. Maximov, "Classes of plateaued rotation symmetric boolean functions under transformation of walsh spectra.," *IACR Cryptology ePrint Archive*, vol. 2004, p. 354, 2004.

[67] M. A. Harrison, "On the classification of Boolean functions by the general linear and affine groups," *Journal of the Society for Industrial & Applied Mathematics*, vol. 12, no. 2, pp. 285–299, 1964.

[68] E. Berlekamp and L. Welch, "Weight distributions of the cosets of the (32, 6) reed-muller code," *IEEE Transactions on Information Theory*, vol. 18, no. 1, pp. 203–207, 1972.

[69] J. A. Maiorana, "A classification of the cosets of the reed-muller code R(1, 6)," *Mathematics of Computation*, vol. 57, no. 195, pp. 403–414, 1991.

[70] L. E. Dickson and J. Gillis, "Linear groups with an exposition of the galois field theory," *Physics Today*, vol. 12, p. 52, 1959.

[71] T. W. Cusick, "Permutation equivalence of cubic rotation symmetric Boolean functions," *International Journal of Computer Mathematics*, pp. 1–6, 2014.

[72] D. Wiedemann and M. Zieve, "Equivalence of sparse circulants: the bipartite adam problem," *arXiv preprint arXiv:0706.1567*, 2007.

[73] W.-D. Wei and J.-Y. Xu, "Cycle index of direct product of permutation groups and number of equivalence classes of subsets of Z_v," *Discrete Mathematics*, vol. 123, no. 1, pp. 179–188, 1993.

[74] G. Miller, "On the holomorph of a cyclic group," *Transactions of the American Mathematical Society*, vol. 4, no. 2, pp. 153–160, 1903.

[75] S. Kavut and M. Yücel, "Generalized Rotation Symmetric and Dihedral Symmetric Boolean Functions - 9 Variable Boolean Functions with Nonlinearity 242," *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, vol. 2, pp. 1–8, 2007.

[76] S. Kavut and M. D. Yücel, "9-variable Boolean functions with nonlinearity 242 in the generalized rotation symmetric class," *Information and Computation*, vol. 208, no. 4, pp. 341–350, 2010.

[77] S. Kavut, "Results on rotation-symmetric S-boxes," *Information Sciences*, vol. 201, pp. 93–113, 2012.

[78] T. W. Cusick and B. Johns, "Theory of 2-rotation symmetric cubic Boolean functions," *Designs, Codes and Cryptography*, pp. 1–21, 2014.

[79] V. Rijmen, P. S. Barreto, and D. L. G. Filho, "Rotation symmetry in algebraically generated cryptographic substitution tables," *Information Processing Letters*, vol. 106, no. 6, pp. 246 – 250, 2008.