

Bibliografia

- [1] W.C. Brown. *Matrices and Vector Spaces*. Marcel Dekker Inc., 1991.
- [2] D. Coppersmith. The Data Encryption Standard (DES) and its strength against attacks. *IBM Journal of Research and Development*, 38:243–250, 1994.
- [3] W. Beyer ed. *CRC Standard Mathematical Tables*. CRC Press, Boca Raton FL, 1981.
- [4] H.M. Heys. A tutorial on linear and differential cryptanalysis. *Cryptologia*, 26:189–221, 2002.
- [5] F.J. MacWilliams. A theorem on the distribution of weights in a systematic code. *Bell System Technical Journal*, 42:79–94, 1963.
- [6] R. Lidl, H. Niederreiter. *Introduction to Finite Fields and Their Applications*. Cambridge University Press, revised edition, 1994.
- [7] V. Pless. Power moment identities on weight distributions in error correcting codes. *Information and Control*, 6:147–152, 1963.
- [8] D.R. Hankerson, D.G. Hoffman, D.A. Leonard, C.C. Lindner, K.T. Phelps, C.A. Rodger, J.R. Wall. *CODING THEORY AND CRYPTOGRAPHY: the essentials*. Marcel Decker Inc. New York Basel, Second edition, 2000.
- [9] P. Roelse. Differential and linear distributions of substitution boxes for symmetric-key cryptosystems. In Mullen GL, Stichtenoth H, Tapia-Recillas H, editor, *Finite fields with applications to coding theory, cryptography and related areas*, pages 270–285. Springer-Verlag, Berlin, 2002.
- [10] P. Roelse. The design of composite permutation with applications to DES-like S-boxes. *Design, Codes and Cryptography*, 42:21–42, 2007.
- [11] C.E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423, 1948.
- [12] C.E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28:656–715, 1949.
- [13] D.R. Stinson. *CRYPTOGRAPHY: Theory and Praticce*. Chapman and Hall/CRC, Third edition, 2006.

- [14] A.J. Menezes, P.C. van Oorschot, S.A. Vanstone. *Handbook of Applied Cryptography*. CRC Press New York, 1996.
- [15] W. W. Peterson, E. J. Weldon, Jr. *Error Correcting Codes*. The Colonial Press, Inc., Second edition, 1972.