Bibliographie

[ABM..] G.B. Agnew, T. Beth, R.C. Mullin and S.A. Vanstone, "Arithmetic Operations in $\mathbb{F}_{2^m}$", Journal of Cryptology, n. 6, 1993, pp. 3-13.

[Bec] B. Beckett, *Introduction aux méthodes de la cryptologie*, Masson, 1990.

[Ber1] E.R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill Book Company, 1968.

[Ber2] E.R. Berlekamp, "Bit-Serial Reed-Solomon Encoders", IEEE Trans. Inform. Theory, vol IT-28, n. 6, 1982, pp. 869-874.

[BeRo] M. Bellare and P. Rogaway, "Random oracles are practical : a paradigm for designing efficient protocols", Proceedings of the 1st ACM Conference on Computer and Communications Security 1993, pp. 62-73.

[Bet] T. Beth, "Efficient Zero-Knowledge Identification Scheme for Smart Cards", Advances in Cryptology, Eurocrypt'88 Proceedings, Berlin, Springer Verlag, 1988, pp. 77-84.

[BGG..] M. Ben-Or, O. Godreich., S Goldwasser, J. Hastad, J. Kilian, S. Micali and P. Rogaway, "Everything Provable is Provable in Zero-Knowledge", Advances in Cryptology, Crypto'88 Proceedings, Berlin, Springer Verlag, 1990, pp. 37-56.

[BGV] A. Bosselaers, R. Govaerts, J. Vandewalle, "Comparison of three modular reduction functions", Crypto'93, Lecture Notes in Computer Science 773, Springer-Verlag, 1994, pp. 13-21.

[Bla] F. Blanchet, "Codes classiques de Goppa binaires", Rapport Inria, en préparation.

[BMT] E.R. Berlekamp, R.J. Mc Eliece & H.C.A. Van Tilborg, "On the inherent intractability of certain coding problems", IEEE Trans. Inform. Theory, 1978, pp. 384-386.

[Blu] M. Blum, "How to Prove a Theorem So No One Else Can Claim It", Proceedings of the International Congress of Mathematicians, Berkeley, CA 1986, pp. 1444-1451.

[Bom] G. Bommier, "Un logiciel dédié aux codes de Goppa", Rapport de DEA, Septembre 1994.

[BoPe] J. Boyar and R. Peralta, "On the Concrete Complexity of Zero-Knowledge Proofs", Advances in Cryptology, Crypto'89 Proceedings, Berlin : Springer-Verlag, vol 435, 1989, pp. 507-525.

[Bou] L. Bournon, "Applications de la réduction de réseaux et nouvelle cryptanalyse d'une fonction de hachage", Thèse de Doctorat, Université de Toulon et du Var, Février 1995.

[Bra] G. Brassard, *Cryptologie Contemporaine*, Masson, 1993.

[BrCr] G. Brassard and C. Crepeau, "Sorting Out Zero-Knowledge", Advances in Cryptology, Eurocrypt'89 Proceedings, Berlin : Springer-Verlag, 1990, pp. 181-191.

[BrMc] E.F. Brickell and K.S. McCurley, "An interactive identification scheme based on discrete logarithms and factoring", Journal of Cryptology, 5, 1992, pp. 29-39.

[CaCh1] A. Canteaut & H. Chabanne, “A further improvement of the work factor in an attempt at breaking Mc Eliece’s cryptosystem”, Proceedings of Eurocode’94, Inria, pp. 163-167.

[CaCh2] A. Canteaut & F. Chabaud, “Improvements of the attacks on cryptosystems based on error-correcting codes”, soumis à Journal of Cryptology.

[CDG] G. Cohen, J.L. Dornstetter, P. Godlewski, *Codes Correcteurs d’Erreurs*, Masson, 1992.

[Cha1] F. Chabaud, “Asymptotic analysis of probabilistic algorithms for finding short codewords”, Eurocode’92, CISM Courses and Lectures, 339, Springer Verlag 1993, pp. 175-183.

[Cha2] F. Chabaud, “On the Security Of Some Cryptosystems Based On Error-Correcting Codes”, Pre-proceedings of Eurocrypt’94, pp. 127-135.

[Chau] D. Chaum, “Demonstrating that a Public Predicate can be Satisfied Without Revealing Any Information About How”, Advances in Cryptology, Eurocrypt’86, Lecture Notes in Computer Science 263, pp. 195-199, Berlin.

[Che] K. Chen, “Improved Girault Identification scheme”, Electronic Letters, 15th September 1994, Vol. 30, No. 19, pp. 1590- 1591.

[CJL..] M.J. Coster, A. Joux, B.A. LaMacchia, A.M. Odlyzko, C.P. Schnorr and J. Stern, “Improved low-density subset algorithms”, Computational Complexity, 2, 1992, pp. 11-28.

[CLR] T. Cormen, C. Leiserson, R. Rivest, *Introduction à l’algorithmique*, Dunod, 1995.

[Dur] R. Durstenfeld, “Algorithm 235 : Random Permutation”, Communications of the ACM, v. 7, n. 7, Jul 1964.

[EvYa] S. Even and Y. Yacobi, “Cryptocomplexity and NP-Completeness”, Proceedings of the 7th International Colloquium on Automata, Languages, and Programming, Berlin : Springer-Verlag, 1980, pp. 195- 207.

[FFS] U. Feige, A. Fiat & A. Shamir, “Zero-knowledge proofs of identity”, Proc. 19th ACM Symp. Theory of Computing, 1987, pp. 210-217.

[FiSh] A. Fiat, A. Shamir, “How To Prove Yourself : Practical Solutions to Identification and Signatures Problems”, Advances in Cryptology, Crypto’86, Lecture Notes in Computer Science 263, pp. 186-194.

[Gab] E.M. Gabidulin, “Theory of codes with maximum rank distance”, Problems of Information Transmission, 1985, 21, pp. 1-12.

[GaJo] M.R. Garey, D. Johnson, *Computers and Intractability, A guide to the theory of NP-Completeness*, W.H. Freeman and Company, New-York, 1978.

[Gir] M. Girault, “A (non-practical) three-pass identification protocol using coding theory”, Advances in Cryptology, Auscrypt’90, Lecture Notes in Computer Science 453, pp. 265-272.

[GiSt] M. Girault, J. Stern, “On the length of cryptographic hash-values used in identification schemes”, Crypto’94, Lecture Notes in Computer Science 839, Springer-Verlag, 1994, pp. 202-215.

[GMR] S. Goldwasser, S. Micali and C. Rackoff, “The knowledge complexity of interactive proof systems”, Proc. 17th ACM Symp. Theory of Computing, 1985, pp. 291-304.

[GMW] O. Goldreich, S. Micali, A. Wigderson, "How to Prove All NP Statements in Zero-Knowledge and a Methodology of Cryptographic Protocol Design", Advances in Cryptology, Crypto'86, Lecture Notes in Computer Science 263, pp. 171-185.

[GoKr] O. Goldreich, H. Krawczyk, "On the Composition of Zero-Knowledge Proof-Systems", Dimacs Technical Report 91-60, August 1991.

[Gol1] O. Goldreich, *Foundations of Cryptography*, Class Notes, Spring 1989.

[Gol2] O. Goldreich, "On Defining Proof of Knowledge", Technical Report 710, Technion, Israel Institute of Technology, December 1991.

[Gop] V.D. Goppa, "A new class of linear error correcting codes", Prob. Pered. Inform., vol. 6, Sept. 1970, pp. 24-30.

[GuQu] L.C. Guillou and J.-J. Quisquater, "A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory", Advances in Cryptology, Eurocrypt'88, 330, 1988, pp. 123-128.

[Har] S. Harari, "A New Authentication Algorithm", Proceedings of Coding Theory and Applications, Lecture Notes in Computer Science 388, 1988, pp. 91-105.

[Hei] R. Heiman, *On The Security Of Cryptosystems Based On Linear Error Correcting Codes*, Thesis, Feinberg Graduate School, August 1987.

[KLP] T. Kasami, S. Lin & W.W. Peterson, "New generalisations of the Reed-Muller codes", IEEE Trans. on Info. Theory, vol. IT-14, 1968, pp. 189-199.

[LeBr] P.J. Lee and E.F. Brickell, "An Observation on the Security of Mc Eliece's Public-Key Cryptosystem", Lecture notes in Computer Science, Advances in Cryptology, Eurocrypt'88, 1989, pp. 275-280.

[Leo] J.S. Leon, "A probabilistic algorithm for computing minimum weights of large error-correcting codes", IEEE Trans. Inform. Theory, IT-34(5), 1988, pp. 1354-1359.

[LiNi] Lidl R., Niederreiter H., *Finite Fields*, Encyclopedia of Mathematics and its Applications, vol. 20, Addison-Wesley, 1983.

[LobCo] A. Lobstein, G. Cohen, "Sur la Complexité d'un Problème de Codage", Informatique Théorique et Applications, vol. 21, n. 1, 1987, pp. 25-32.

[LoCo1] M. LoeLoeian, J. Conan, "A [55, 16, 19] Binary Goppa Code", IEEE Trans. on Inf. Theo., vol IT-30, No. 5, September 1984, pp. 773.

[LoCo2] M. LoeLoeian, J. Conan, "A Transform Approach to Goppa Codes", IEEE Trans. on Inf. Theo., vol IT-33, No. 1, January 1987, pp. 105-115.

[LuRa] M. Luby, CH. Rackoff, "How to construct pseudorandom permutations from pseudorandom functions", SIAM Journal and Computing, 17(2), 1988, 373-386.

[MaSl] F.J. MacWilliams & N.J.A. Sloane, *The Theory of error-correcting codes*, North-Holland, Amsterdam-New-York-Oxford, 1977.

[McE] R.J. McEliece, "A public key cryptosystem based on algebraic coding theory", DSN Progress Report 42-44, Jet Propulsion Laboratory, 1978, pp. 114-116.

[MKI] T. Matsumoto, K. Kato, H. Imai, "Speeding up Secret Computation with Insecure Auxiliary Devices", Proceedings of Crypto'88, Lecture Notes in Computer Science 403, pp. 497-506.

[Mon] P.L. Montgomery, "Modular multiplication without trial division", Mathematics of Computation, vol. 44, 1985, pp. 519-512.

[NIE] H. NIEDERREITER, "Knapsack-Type Cryptosystems and Algebraic Coding Theory", Problems of Control and Information Theory, v. 15, n. 2, 1986, pp. 159-166.

[NTHA] S.C. NTAFOS, S.L. HAKIMI, "On the Complexity of Some Coding Problems", IEEE Trans. on Inf. Theo., vol IT-27, No. 6, November 1981, pp. 794-796.

[OKA] T. OKAMOTO, "Provably secure and practical identification schemes and corresponding signature schemes", Advances in Cryptology, Crypto'92, Lecture Notes in Computer Science, 740, 1993, pp. 31-53.

[PACH] J. PATARIN, P. CHAUVAUD, "Improved algorithms for the permuted kernel problem", Proceeedings of Crypto'93, Lecture Note in Computer Science 435, 606-609.

[PAT] J. PATARIN, *Etude des générateurs de permutations pseudo-aléatoires basés sur le schéma du DES*, Thèse, Université de Paris VII, Novembre 1991.

[PATT1] N.J. PATTERSON, "The Algebraic Decoding of Goppa Codes", IEEE Trans. on Info Theory, vol 21, 1975, pp. 203-207.

[PATT2] W. PATTERSON, *Mathematical Cryptology for computer scientists and mathematicians*, Rowman & Littlefield, 1987.

[POI] D. POINTCHEVAL, "A New Identification Scheme Based on the Percerptrons Problem", Advances in Cryptology, Eurocrypt'95, Lecture Notes in Computer Science, 921, pp. 319-328.

[QUGU] J.J. QUISQUATER, L. GUILLOU, "How to Explain Zero-Knowledge Protocols to Your Children", Advances in Cryptology, Crypto'89, Lecture Notes in Computer Science, 435, 1990, pp. 628-631.

[RIV] R. L. RIVEST, "The MD5 Message Digest Algorithm", Proceedings of Crypto'90, Lecture Notes in Computer Science 537, 303-311.

[ROB] G. ROBIN, *Algorithmique et Cryptographie*, Mathématiques et Applications, Ellipses, 1991.

[ROS] A.M. ROSEIRO, *The Trace Operator and Generalized Goppa Codes*, Ph.D. Dissert., Dept. of Elect. Eng., Michigan State Univ., East Lansing, MI 48823, July 1989.

[RHHS] A.M. ROSEIRO, J.I. HALL, J.E. HADNEY, M. SIEGEL, "The Trace Operator and Redundancy of Goppa Codes", IEEE Trans. Info. Theory, vol. 38, n. 3, May 1992, pp. 1130-1133.

[SBM] N.A. SHEKHUNOVA, S.V. BEZZATEEV AND E.T. MIRONCHIKOV, "A subclass of binary Goppa codes", Problemy Peredachi Informatsii, vol. 25, n. 3, July-September 1989, pp. 98-102.

[SCH] B. SCHNEIER, *Applied Cryptography*, John Wiley & Sons, 1994.

[SCHN] C.P. SCHNORR, "Efficient signature generation by smart cards", Journal of Cryptology, 4, 1991, 161-174.

[SHA] A. SHAMIR, "An efficient identification scheme based on permuted kernels", Proceedings of Crypto'89, Lecture Notes in Computer Science 435, pp. 606-609.

[SHVU] M. SHAND AND J. VUILLEMIN, "Fast Implementations of RSA cryptography", Proceedings of the 11th IEEE Symposium on Computer Arithmetic, IEEE Computer Society Press, Los Alamitos, CA, 1993, pp. 252-259.

[STE1] J. STERN, "A method for finding codewords of small weight", Coding Theory and Applications, Lecture Notes in Computer Science 434, pp. 173-180.

[STE2] J. STERN, "An alternative to the Fiat-Shamir protocol", Proc. Eurocrypt'89, Lecture Notes in Computer Science 434, Springer-Verlag, 1990, pp. 173-180.

[STE3] J. STERN, "A new identification scheme based on syndrome decoding", Crypto'93, Lecture Notes in Computer Science 773, Springer-Verlag, 1994, pp. 13-21.

[STE4] J. STERN, "Designing identification schemes with keys of short size", Crypto'94, Lecture Notes in Computer Science 839, Springer-Verlag, 1994, pp. 164-173.

[STI] D.R. STINSON, *Cryptography, Theory and Practice*, CRC Press, 1995.

[VER1] P. VÉRON, "Syndrome decoding problem and Identification scheme", Proceedins of Eurocode'94, Inria, pp. 175-181.

[VER2] P. VÉRON, "A Fast Identification Scheme", IEEE Symp. on Inform. Theory, Canada, 1995, à paraitre.

[VER3] P. VÉRON, "Goppa Codes defined from a trace polynomial", Abstracts of the Third International Conference on Finite Fields and Applications, Glasgow, 1995, pp. 36-37.

[VER4] P. VÉRON, "Cryptanalysis of Harari's Identification Scheme", Fifth IMA Conference on Cryptography and Coding, Lecture Note in Computer Science, Springer-Verlag, Décembre 1995, à paraitre.

[VER5] P. VÉRON, "An identification scheme based on error correcting codes", soumis à publication.

[WAL] C.D. WALTER, "Faster modular multiplication by operand scaling", Proceedings of Crypto'91, Lecture Note in Computer Science 576, Springer-Verlag, 1992, pp. 252-259.

[WEL] D. WELSH, *Codes and Cryptography*, Oxford Science Publications, 1989.

[WIR] M. WIRTZ, "On the Parameters of Goppa Codes", IEEE Trans. Inform. Theory, Sept. 1988, pp. 1341-1342.

[ZIE] N. ZIERLER, "On the Theorem of Gleason and Marsh", Proc. Am. Math. Soc., 9, 236-237, Math. Rev., 20 : 851, 1958.