Bibliografia

[1] L. Adleman, K. Manders i G. Miller. On taking roots in finite fields. Presentat a *18th IEEE Annual Symp. Foundations of Computer Science,* Providence, RI, 1977.

[2] G. Ateniese, C. Blundo, A. De Santis i D. R. Stinson. Visual Cryptography for General Access Structures. Apareixerà a *Information and Computation.*

[3] G. Ateniese, C. Blundo, A. De Santis i D. R. Stinson. Constructions and Bounds for Visual Cryptography. *"23rd International Colloquium on Automata, Languages and Programming" (ICALP '96)*, Ed. F. Meyer auf der Heide, Lecture Notes in Computer Science **1099**, Springer Verlag, 416–428.

[4] D. Baró. Raíces cúbicas en $\mathbb{Z}_m$. *Projecte Final de Carrera.* Escola Tècnica Superior d'Enginyeria de Telecomunicacions de Barcelona. Universitat Politècnica de Catalunya (1997).

[5] P. Béguin i A. Cresti. General Short Computational Secret Sharing Schemes. *EUROCRYPT'95* Lecture Notes in Computer Science **921** (1995), 194-208.

[6] A. Beimel i B. Chor. Universally Ideal Secret-Sharing Schemes. *IEEE Transactions on Information Theory* **40**, núm. 3 (1994) 786–794.

[7] J.C. Benaloh. Secret sharing homomorphisms: Keeping shares of a secret secret. *Advances in Cryptology, CRYPTO'86*, Lecture Notes in Computer Science **263** (1987) 251–260.

[8] J. Benaloh i J. Leichter. Generalized secret sharing and monotone functions. *Lecture Notes in Computer Science* **403** (1990) 27–35.

[9] M. Ben-Or and T. Rabin. Verifiable secret sharing and multiparty protocols with honest majority. *Proc. 21st ACM Symposium on Theory of Computing*, (1989) 73–85.

[10] A. Beutelspacher. How to say "No". *Advances in Cryptology, CRYPTO'89*, Lecture Notes in Computer Science, **434** (1990) 491–496.

[11] G.R. Blakley. Safeguarding criptographic keys. *AFIPS Conference Proceedings* **48** (1979) 313–317.

[12] B. Blakley, G.R. Blakley, A.H. Chan i J.L. Massey. Threshold schemes with disenrollment. *Lecture Notes in Computer Science* **740** (1993) 546—554.

[13] C. Blundo. Secret sharing schemes for access structures based on graphs. *Tesi di Laurea*. Universitat de Salerno (1991).

[14] C. Blundo, A. Cresti, A. De Santis i U. Vaccaro. Fully Dynamic Secret Sharing Schemes. *Advances in Cryptology CRYPTO'93*, Lecture Notes in Computer Science, 773, (1994) 126–135.

[15] C. Blundo, A. De Santis, L. Gargano i U. Vaccaro. On the information rate of secret sharing schemes. *Advances in Cryptology CRYPTO'92, Proc. of the 12th Annual International Cryptology Conference*, Lecture Notes in Computer Science, **740**, 149–169 (1993).

[16] C. Blundo i A. De Santis. Lower Bounds for Robust Secret Sharing Schemes. *Information Processing Letters* **63** (1997), núm. 6, 317–321.

[17] C. Blundo, A. De Santis, L. Gargano i U. Vaccaro. Secret sharing schemes with veto capabilities. *Proc. of French-Israely Workshop on Algebraic Coding*, Lecture notes in Computer Science, 781, (1994) 82–89.

[18] C. Blundo, A. De Santis, D.R. Stinson i U. Vaccaro. Graph decompositions and secret sharing schemes. *J. Cryptology* **8** (1995) 39–64.

[19] C. Blundo,A. De Santis, A.G. Gaggia i U. Vaccaro. New Bounds on the information Secret Sharing Schemes. *IEEE Transactions on Information Theory*, Vol. **41**, Núm. **2** (1995) 549–554.

[20] C. Blundo, A. De Santis, R. De Simone i U. Vaccaro. Tight bounds on the Information Rate of Secret Sharing Schemes. *Designs, Codes and Cryptography*, 11, 107–122 (1997).

[21] C. Blundo, A. De Santis i U. Vaccaro. Efficient Sharing of Many Secrets. *Proceedings of STACS'93 (10th. Symp. on Theoretical Aspects of Coputer Science*, Lecture Notes in Computer Science, **665**, 692–703 (1993).

[22] C. Blundo i D.R. Stinson. Anonymous secret sharing schemes. *Discrete Appl. Math.* **77** (1997), núm. 1, 13–28.

[23] J. Borrell. Estudi i desenvolupament d'un sistema criptogràfic per realitzar votacions segures sobre una xarxa local. Tesi doctoral, Universitat Autònoma de Barcelona (1996).

[24] E.F. Brickell. Some ideal secret sharing schemes. *J. Combin. Math. and Combin. Comput.*, **9** (1989) 105–113.

[25] E.F. Brickell i D.M. Davenport. On the classification of ideal secret sharing schemes. *J. Cryptology* **4** (1991) 123–134.

[26] E.F. Brickell i D.R. Stinson. The detection of cheaters in threshold schemes. *SIAM J. on Discrete Math.* **4** (1991) 502–510.

[27] E.F. Brickell i D.R. Stinson. Some Improved Bounds on the Information Rate of Perfect Secret Sharing Schemes. *J. Cryptology* **5** (1992) 153–166.

[28] J. Campos. Esquemas para compartir secretos robustos de tipo geométrico-vectorial. *Projecte Final de Carrera.* Escola Tècnica Superior d'Enginyeria de Telecomunicacions de Barcelona. Universitat Politècnica de Catalunya (prevista la lectura el setembre de 1998).

[29] R.M. Capocelli, A. De Santis, L. Gargano i U. Vaccaro. On the size of shares for secret sharing schemes. *J. Cryptology* **6** (1993) 157–168.

[30] M. Carpentieri. A Perfect Threshold Secret Sharing Scheme to Identify Cheaters. *Designs, Codes and Cryptography*, **5**, 183-187 (1995).

[31] M. Carpentieri, A. De Santis i U. Vaccaro. Size of shares and probability of cheating in threshold schemes. Presented at *EUROCRYPT'93.*

[32] C. Cachin i C. Boyd. On-line secret sharing. *Cryptography and Coding, IMA'96*, 190–198 (1995).

[33] B. Chor i E. Kushilevitz. Secret Sharing Over Infinite Domains. *J. of Cryptology,* **6**: 87–95 (1993).

[34] L.Csimarz. The size of a Share Must be Large. *Advances in Cryptology, CRYPTO'94*, Lecture Notes in Computer Science, **950**, 13–22 (1995).

[35] H. Cohen. A Course in Computational Algebraic Number Theory. *Springer Verlag, Graduate Texts in Mathematics 138*, Berlin 1995.

[36] T.M. Cover, J.A. Thomas. Elements of Information Theory. *Wiley Series in Telecommunications*, 1991.

[37] Y. Desmedt i Y. Frankel. Shared generation of authenticators and signatures. *Advances in Cryptology, CRYPTO'91.* Lecture Notes in Computer Science **576**, Springer-Verlag (1992), 457-469.

[38] M. van Dijk. On the Information Rate of Perfect Secret Sharing Schemes. *Designs, Codes and Cryptography*, Vol. **6** (1995) 143–169.

[39] A. Fiat, A. Shamir. How to prove yourself: practical solutions to identification and signature problems. *Lecture Notes in Computer Science, 263 (1987), 186-194*, Advances in Cryptology-CRYPTO'86.

[40] M.K. Franklin i M.K. Reiter. Verifiable signature sharing. *Advances in Cryptology, EUROCRYPT'95* Lecture Notes in Computer Science, (1995), 50-63.

[41] H. Ghodosi, J. Pieprzyk, G.R. Chaudhry i J. Seberry. How to prevent cheating in Pinch's scheme. *Electronics Letters* **33** (1997) 1453–1454.

[42] O. Goldreich, S. Micali i A. Wigderson. How to play any mental game. *Proc. 19th ACM Symp. on Theory of Computing* (1987) 218–229.

[43] J. He i E. Dawson. Multistage secret sharing based on one way function. *Electronics Letters*, Vol. **30**, Núm. **19**.

[44] M. Ito, A. Saito i T. Nishizeki. Secret sharing scheme realizing general acces structure. *Proc. IEEE GLOBECOM'87* (1987) 99–102.

[45] W.A. Jackson i K. Martin. Geometric Secret Sharing Schemes and Their Duals. *Designs, Codes and Cryptography*, **4**, 83-95 (1994).

[46] W.A. Jackson i K.M. Martin. Perfect Secret Sharing Schemes on Five Participants. *Designs, Codes and Cryptography*, **9**, 267-286 (1996).

[47] W.A. Jackson i K.M. Martin. An Algorithm for Efficient Geometric Secret Sharing Schemes. *Preprint*, (1996).

[48] W.A. Jackson, K.M. Martin i C.M. O'Keefe. Multisecret threshold schemes. Presented at *EUROCRYPT'93.*

[49] W.A. Jackson, K.M. Martin i C.M. O'Keefe. Efficient Secret Sharing Without a Mutually Trusted Authority. *EUROCRYPT'95* Lecture Notes in Computer Science **921** (1995), 183-193.

[50] W.A. Jackson, K.M. Martin i C.M. O'Keefe. Ideal Secret Sharing Schemes with Multiple Secrets. *J. Cryptology*, **9**, 233–250 (1996)

[51] E.D. Karnin, J.W. Greene i M.E. Hellman. On secret sharing systems. *IEEE Transactions on Information Theory* **29** (1982) 35–41.

[52] K. Kobara i H. Imai. Limiting the Visible Space Visual Secret Sharing Shemes and Their Application to Human Identification. Lecture Notes in Computer Science **1163** (1996).

[53] H. Krawczyk. Secret Sharing Made Short. *CRYPTO'93*, Montreal, Lecture Notes in Computer Science **773** (1993), 136-146.

[54] K. Kurosawa, K. Okada, K. Sakano, W. Ogata i S. Tsujii. Nonperfect Secret Sharing Schemes and Matroids. *Advances in Cryptology EUROCRYPT'93*, Lecture Notes In Computer Science, **765** (1994) 126–141.

[55] C. Laih, L. Harn, J. Lee i T. Hwang. Dynamic Threshold Scheme Based on the Definition of Cross Product in an $N-$Dimensional Linear Space. *Advances in Cryptology-CRYPTO'89*, Lecture Notes in Comput. Sci. 434: 20–24.

[56] S. Lang. Algebra. *Addison-Wesley Co. 1971.*

[57] D.H. Lehmer. Computer Technology Applied to the Theory of Numbers. *Studies in Number Theory (W.J. LeVeque, Ed.,)* Englewod Cliffs, N.J.: MAA, Prentice Hall, 1969.

[58] K.M. Martin. Discrete structures in the theory of secret sharing. *Ph. D. dissertation.* Univ. Londres, 1991.

[59] K.M. Martin. New secret sharing schemes from old. *Journal of Combin. Math. and Combin. Comput.* **14** (1993) 65–77.

[60] R.J. McEliece i D.V. Sarwate. On sharing secrets and Reed-Solomon codes. *Commun. of the ACM*, **24** (1981) 583–584.

[61] F.J. McWilliams i N.J.A. Sloane. The theory of error-correcting codes. *North-Holland*, (1981) 397–398.

[62] M. Naor i A. Shamir. Visual Cryptography. *Advances in Cryptology EUROCRYPT'94*, Lecture Notes in Computer Science **950** (1995), 1-12.

[63] I. Niven, H.S. Zuckerman. An Introduction to the Theory of Numbers. *John Wiley and Sons, Inc.*, New York, 1966.

[64] W. Ogata i K. Kurosawa. Optimum Secret Sharing Scheme Secure against Cheating. *Advances in Cryptology, EUROCRYPT'96*, Lecture Notes on Computer Sciences **1070**, Springer Verlag (1996) 200–211.

[65] L. Orós. Esquemas robustos para compartir secretos. *Projecte Final de Carrera.* Escola Tècnica Superior d'Enginyeria de Telecomunicacions de Barcelona. Universitat Politècnica de Catalunya (1996).

[66] C. Padró, G. Sáez i J.L. Villar. Detection of cheaters in vector space secret sharing schemes. *PRAGROCRYPT'96*, 359–369 (1996).

[67] C. Padró, G. Sáez i J.L. Villar. Detection of cheaters in vector space secret sharing schemes. En procés de referenciat a *Designs, Codes and Cryptography* (1996).

[68] C. Padró i G. Sáez. A secret sharing Scheme secure against cheaters for a general structure. En procés de referenciat a *IPL* (1998).

[69] C. Padró i G. Sáez. On taking cube roots in $\mathbb{Z}_m$. En procés de referenciat a *IPL* (1998).

[70] C. Padró i G. Sáez. Secret Sharing Schemes with Bipartite Access Structure. *Advances in Cryptology, EUROCRYPT'98*, Lecture Notes in Computer Sciences **1403**, Springer Verlag (1998) 500–511.

[71] C. Padró i G. Sáez. Lower Bounds on the Information Rate of Secret Sharing Schemes with Homogeneous Access Structure. Actes del *Workshop on Communications* del *The 23th International Symposium on Mathematical Foundations of Computer Science, MFCS'98.* Universitat de Aachen.

[72] R.C. Peralta. A Simple and Fast Probabilistic Algorithm for Computing Square Roots Modulo a Prime Number. *IEEE Transactions on Information Theory*, vol. it-32, no. 6, (846-847), November 1986.

[73] M.O. Rabin. Digitized signatures and public-key functions as intractible as factorization. *MIT Laboratory for Computer Science Technical Report,* LCS/TR-212, 1979.

[74] M.O. Rabin. Randomized Byzantine generals. *24th Symp. Found. Comp. Sci.*, 403–409 (1979).

[75] M. Rabin. Efficient dispersal of information for security, load balancing, and fault tolerance. *Journal of the ACM,* **22** 612–613, Abril de 1989.

[76] A. Renvall i C. Ding. The Access Structure of Some Secret-Shraing Schemes. *Proceedings of the First Australasian Conference ACISP'96* 67–78, 1996.

[77] J. Rifà-Coma. How to avoid cheaters succeeding in the key sharing scheme. *Designs, Codes and Cryptography*, **3** (1993) 221–228.

[78] G. Sáez, C. Padró, J.L. Villar i P. Morillo. Weighted threshold secret sharing schemes. En procés de revisió a *Information Processing Letters*.

[79] A. Salomaa. Public-key Cryptography. *Springer Verlag*(1990) 187–190.

[80] A. De Santis, Y. Desmedt, Y. Frankel i M. Yung. How to Share a Function Securely. *Proceedings of the twenty-sixth annual ACM Symposium on the theory of computing (STOC 94)*, Montreal (1994), 522-533.

[81] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod$p$. *Math. Comp.* **43** (1985), pp. 483-494.

[82] E.W. Selberg. How to Stop a Cheater : Secret Sharing with Dishonest Participation. *School of Computer Science*, Carnegie Mellon University, Pittsburgh, CMU-CS-93-182 (1994).

[83] A. Shamir. How to share a secret. *Commun. of the ACM* **22** (1979) 612–613.

[84] M. de Soete, J.J. Quisquater i K. Vedder. A signature with shared verification scheme. *Advances in Cryptology CRYPTO'89* Lecture Notes in Computer Sciences 434, (1990) 253–262.

[85] H.M. Sun, S.P. Shieh. Recursive Constructions for Perfect Secret Sharing Schemes. Preprint(1997).

[86] J. Torán. Esquemas para compartir secretos con participantes distribuidos en dos colectivos. *Projecte Final de Carrera.* Escola Tècnica Superior d'Enginyeria de Telecomunicacions de Barcelona. Universitat Politècnica de Catalunya(1997).

[87] D. Shanks. Five Number-Theoretical Algorithms. *Proc. Second Manitoba Conf. on Numerical Mathematics*, University of Manitoba, Winnipeg, Manitoba, Canada, 1972.

[88] G.J. Simmons. Prepositioned Shared Secret and/or Shared Control Schemes. *Advances in Cryptology-CRYPTO'89*, Lecture Notes in Comput. Sci. 434: 436–467 (1990).

[89] G.J. Simmons. How to (really) share a secret. *Advances in Cryptology-CRYPTO'88*, Lecture Notes in Comput. Sci. 403: 390–448.

[90] G.J. Simmons. An introduction to shared secret and/or shared control schemes and their application. En *Contemporary Cryptology. The science of information integrity* (G.J. Simmons Ed.) IEEE Press (1992) 441–497.

[91] G.J. Simmons, W. Jackson i K. Martin. The geometry of secret sharing schemes. *Bulletin of the ICA* **1** (1991) 71–88.

[92] D. R. Stinson. New General Lower Bounds on the Information Rate of Secret Sharing Schemes. *Advances in Cryptology CRYPTO'92, Proc. of the 12th Annual International Cryptology Conference* (1992) 168–182.

[93] D.R. Stinson. An explication of secret sharing schemes. *Designs, Codes and Cryptography*, **2** (1992) 357–390.

[94] D.R. Stinson. Cryptography: theory and practice. *Boca Raton* (Florida, USA), CRC Press Inc. (1995).

[95] D.R. Stinson. Decomposition Constructions for Secret Sharing-Schemes. *IEEE Transactions on Information Theory* **40** (1994), 118-125.

[96] D.R. Stinson i S.A. Vanstone. A combinatorial approach to threshold schemes. *SIAM J. on Discrete Math.* **1** (1988) 230–237.

[97] M.A. Tébar. Estructuras de acceso en esquemas para compartir secretos. *Projecte Final de Carrera.* Escola Tècnica Superior d'Enginyeria de Telecomunicacions de Barcelona. Universitat Politècnica de Catalunya (1996).

[98] M. Tompa i H. Woll. How to share a secret with cheaters. *J. of Cryptology*, **1** (1988) 133–139.