Bibliography

[1] *C. Asmuth and J. Bloom*: A Modular Approach to Key Safeguarding, IEEE Transactions on Information Theory, vol.IT-29, no.2, 1983, pp. 208-210.

[2] *G. Ateniese, C. Blundo, A.D. Santis, and D. Atinson*: Constructions and Bounds for Visual Cryptography, Proceedings 23rd International Colloquium on Automata, Languages, and Programming (ICALP '96), 1099, 1996, pp. 416-428.

[3] *G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson*: Visual Cryptography for General Access Structures, Information and Computation, vol. 129, no.2, 1996, pp. 86-106.

[4] *A. Beimel and B. Chor*: Universally Ideal Secret Sharing Schemes, Lecture Notes in Computer Science vol. 740, 1993, pp. 185-197.

[5] *J. C. Benaloh and J. Leichter*: Generalized Secret Sharing and Monotone Functions, Proceedings of Crypto '88, Advances in Cryptology, Lecture Notes in Computer Science, vol. 403, S. Goldwasser, Ed., Springer-Verlag, Berlin, 1990, pp. 27-35.

[6] *J. Benaloh*: Secret Sharing Homomorphisms - Keeping Shares of a Secret Secret, In Advances in Cryptology - CRYPTO '86, A. M. Odlyzko, Ed. 1987, vol. 263 of Lecture Notes in Computer Science, pp. 251-260, Springer-Verlag.

[7] *E. Bertinoro*: Secure and Selective Dissemination of XML Documents, ACM Transactions on Information System Security, vol. 5, No. 3, 2002, pp 290-331.

[8] *M. Bertilsson, I. Ingemarsson*: A Construction of Practical Secret Sharing Schemes using Linear Block Codes. In Proceedings AUSCRYPT '92, Springer Lecture Notes in Computer Science, vol. 718, pp. 67-79, 1993.

[9] *G. R. Blakley*: Safeguarding Cryptographic Keys, Proceeding of AFIPS 1979 National Computer Conference, vol. 48, New York, NY, June 1979, pp. 313-317.

[10] *B. Blakley, G. R. Blakley, A. H. Chan and J. L. Massey*: Threshold Schemes with Disenrollment. Lecture Notes in Computer Science 740, 1993, pp. 546-554.

[11] *G. R. Blakley and C. Meadows*: Security of Ramp Schemes, Proceeding of Crypto '84, Advances in Cryptology, Lecture notes in Computer Science, vol 196, 1985, G. R. Blakley and D. Chaum, Eds., Springer Verlag, pp 411-431.

[12] *C. Blundo, A. De Santis and U. Vaccaro*: Efficient Sharing of Many Secrets, Proceeding of STACS'93, Lecture Notes in Computer Science vol. 665, 1993, Springer Verlag, pp. 692-703.

[13] *C. Blundo, A. Cresti, A. De Santis and U. Vaccaro*: Fully Dynamic Secret Sharing Schemes. Theoretical Computer Science, vol. 165, no. 2, 1996, pp. 407-440.

[14] *C. Blundo, A. De Santis, L. Gargano and U. Vaccaro*: On the Information Rate of Secret Sharing Schemes, Lecture Notes in Computer Science vol. 740, 1993, pp. 149-169.

[15] *C. Blundo, A. De Santis, D. R. Stinson, and U. Vaccaro*: Graph Decomposition and Secret Sharing Schemes, Journal Cryptology. no. 8 1995, pp. 39-64.

[16] *C. Blundo and D. R. Stinson*: Anonymous Secret Sharing Schemes, Discrete Applied Mathematics, 77, 1997, pp 13-28.

[17] *E. F. Brickell*: Some ideal secret sharing schemes, Journal of Combin. Math. and Commbin. Comput. no. 9, 1989, pp 105-113.

[18] *E. F. Brickell and D. M. Davenport*: On Classification of Ideal Secret Sharing Schemes, Journal of Cryptology, vol 4, No. 2 1991, pp 123-134.

[19] *E. F. Brickell and D. R. Stinson*: Some Improved Bounds on the Information Rate Of Perfect Secret Sharing Schemes. Journal Cryptology vol. 5 no. 3, 1992, pp. 153-166.

[20] *E. F. Brickell and D. R. Stinson*: The Detection Of Cheaters In Threshold Schemes, SI AM J. on Discrete Math. no. 4, 1991, pp. 502-510.

[21] *R. Brinkman, J. M. Doumen and W. Jonker*: Using secret sharing for searching in encrypted data, In Workshop on Secure Data Management in a Connected World (SDM), 30 Aug 2004, Toronto, Canada. pp. 18-27. Lecture Notes in Computer Science 3178. Springer-Verlag. ISSN 0302-9743 ISBN 3-540-22983-3.

[22] *R. M. Capocelli, A. De Santis, L. Gargano and U. Vaccaro*: On the size of shares for secret sharing schemes. Journal Cryptology no. 6, 1993, pp. 157-168.

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

[24] *C. Chang, C. Tsait and T. Chen*: A New Scheme for Sharing Secret Colour Images in Computer Network, Proceeding of International Conference on Parallel and Distributed Systems, July 2000, pp 21-27.

[25] *Chin-Chen Chang and Tai-Xing Yu*: Sharing Secret Gray Image in Multiple Images, National Chung Cheng University, Taiwan, 2002.

[26] *D. Chen and D. R. Stinson*: Recent Results on Combinatorial Constructions for Threshold Schemes, Australasian Journal of Combinatorics, vol 1, 1990, pp. 29-48.

[27] *B. Chor, E. Kushilevitz*: Secret Sharing Over Infinite Domains, Journal of Cryptology, Vol 6, 1993, pp. 87-96

[28] *B. Chor, O. Goldreich, E. Kushilevitz and M. Sudan*: Private Information Retrieval, IN FOCS, 1995, pp 41-50.

[29] *Chwei-Shyong Tsai, Chin-Chen Chang and Tung-Shou Chen*: Sharing Multiple Secrets in Digital Images, The Journal of Systems and Software, vol 64, 2002, pp.163-170.

[30] *D. Denning*: Cryptography and Data Security, Addison-Wesley, Reading, MA, 1983.

[31] *Y. Desmedt, A. De Santis, Y. Frankel, and M. Yung*: How to Share a Function Securely. In: Proceedings STOC '94, ACM Press, 1994, pp. 22-33.

[32] *S. Droste*: New Results on Visual Cryptography, Advances in Cryptology-CRYPTO'96, Lecture Notes in Computer Science, vol. 1109, 1996, pp. 401-415.

[33] *O. Goldreich, S. Micali, and A. Wigderson*: How to Play Any Mental Game, Proceeding of the 19th Annual ACM Symposium on Theory of Computing, 1987, New York, pp. 218-229.

[34] *R. Hwang and C. Chang*: Some Secret Sharing Schemes and their Applications, Ph. D. dissertation of the Department of Computer Science and Information Engineering, National Chung Cheng University, Chiayi, Taiwan, 1998.

[35] *I. Ingemarsson and G. J. Simmons*: A Protocol to set up Shared Secret Schemes Without the Assistance of a Mutually Trusted Party. Lecture Notes in Computer Science vol. 473, 1991, pp. 266-282.

[36] *M. Ito, A. Saito, and T. Nishizeki*: Secret Sharing Schemes Realizing General Access Structure, Proceeding of IEEE Global Telecommunications Conference, Globecom 87, Tokyo, Japan, 1987, pp. 99-102, . Journal version: Multiple Assignment Scheme for Sharing Secret, Journal Cryptology, vol 6, no. 6, 1993, pp. 15-20.

[37] *W. A. Jackson and K M. Martin and C. M. O'Keefe*: On Sharing Many Secrets, Lecture Notes in Computer Science 917, Advances in Cryptology, Proceedings of Asiacrypt'94, Springer Verlag, 1994, pp. 42-54.

[38] *W.A. Jackson and K. M. Martin*: Combinatorial Models for Perfect Secret Sharing Schemes, J. Corn-bin. Math. Combin. Comput., Vol. 28, 1998 pp 249-265.

[39] *E. D. Karnin, J. W. Greene and M. E. Hellman*: On Secret Sharing Systems, IEEE Transactions on Information Theory, vol.IT-29, no. 1, Jan 1983, pp 35-41.

[40] *D. E. Knuth*: The Art of Computer Programming, Vol. 2, Seminumerical algorithms,2nd edition, Addison-Wesley Publishing Company, Reading, Massachusetts, 1981.

[41] *S. Kothari*: Generalized Linear Threshold Scheme, Proceedings Crypto '84, Santa Barbara, CA (Aug 1984), 231-241. Published as Advances in Cryptology, ed. by Blakley and D. Chaum in Lecture Notes in Computer Science, vol. 196, ed. by G. Goos and J. Hartmains. Springer-Verlag, New York 1985.

[42] *Lawrence C. Washington , Wade Trappe*: Introduction to Cryptography: With Coding Theory ,Prentice Hall PTR, Upper Saddle River, NJ, 2002.

[43] *C. L. Liu*: Introduction to Combinatorial Mathematics, McGraw-Hill, New York, 1968.

[44] *K. M. Martin*: Discrete Structures in the Theory of Secret Sharing. Ph. D. Thesis, University of London, 1991.

[45] *K. M. Martin*: New Secret Sharing Schemes fron Old, Journal of Combin. Math. and Combin. Comput. no. 14, 1993, pp 65-77.

[46] *R. J. McEliece and D. V. Sarwate.*: On Sharing Secrets and Reed-Solomon Codes. Commun. of the ACM no. 24, 1981, pp. 583-584.

[47] *M. Mignotte*: How to share a secret, Cryptography Proceedings of the Workshop on Cryptography, Burg Feuerstein, 1982, volume 149 of LNCS, pp 371-375 Springer-Verlag, 1983.

[48] *M. Naor and A. Shamir*: Visual Cryptography, Advances in cryptology- EUROCRYPT94, Lecture Notes in Computer Science, vol. 950, 1995, pp. 1-12.

[49] *S. J. Phillips and N. C. Phillips*: Strongly Ideal Secret Sharing Schemes, J. Cryptology, Vol. 5 (1992), pp. 185-191.

[50] *T. Rabin and M. Ben-Or*: Verifiable Secret Sharing and Multiparty Protocols with Honest Majority. Proceedings 21st ACM Symp. on Theory of Computing, 1989, pp. 73-85.

[51] *P. J. Schellenberg and D. R. Stinson*: Threshold Schemes from Combinatorial Designs, J. Combin. Math. Combin. Comput., vol. 5, 1989, pp. 143-160.

[52] *P. D. Seymour*: On Secret-Sharing Matroids, J. Combin. Theory B vol. 56, 1992, pp. 69-73.

[53] *A. Shamir*: How to Share a Secret, Communications of the ACM, vol. 22, no. 11, Nov. 1979, pp. 612-613.

[54] *G. J. Simmons*: Robust Shared Secret Schemes or "How to be Sure You Have the Right Answer even though You don't know the question", Congressus Numerantium, vol. 8, 1989, pp 215-248.

[55] *G. J. Simmons*: Shared Secret and/or Shared Control Schemes, Lecture Notes in Computer Science vol. 537, 1991, pp. 216-241.

[56] *G. J Simmons, W. Jacjson and K. Martin*: The Geometry of Shared Secret Schemes. Bulletin of ICA vol. 1, 1991, pp. 71-88.

[57] *Dawn Xiaodong Song, David Wagner and Adrian Perrig*: Practical techniques for searchs on encrypted data, In IEEE Symposium on Security and Privacy, pp 44-55, 2000. http://citeseer.nj.nec.com/song00practical.html.

[58] *D. R. Stinson*: An Explication of Secret Sharing Schemes, Designs, Codes and Cryptography, vol. 2, 1992, pp 357-390.

[59] *D. R. Stinson*: New General Lower Bounds on the Information Rate of Secret Sharing Schemes. Lecture Notes in Computer Science, vol. 740, 1993, pp. 170-184.

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

[61] *D. R. Stinson and S. A. Vanstone*: A combinatorial approach to threshold schemes. SIAMJ. on Discrete Mathematics, 1(2):230-236, 1988.

[62] *M. Tompa and H. Woll*: How to share a Secret with Cheaters, Journal of Cryptography, vol. 1, no.2, 1988,pp 133-138

[63] *E. Verheul and H.V. Tilborg*: Constructions and Propertics of k out of n Visual Secret Sharing Schemes, Designs, Codes and Cryptography, vol. 11 no.2, 1997, pp. 179-196.