References

[1] Rivest; Ronald L. (Belmont, MA), Shamir; Adi (Cambridge, MA), Adleman; Leonard M. (Arlington, MA), “RSA - Cryptographic communications system and method” U.S. Patent 4,405,829, December 14, 1977.

[2] National Bureau of Standards, “Data Encryption Standard”, FIPS-Pub.46. National Bureau of Standards, U.S. Department of Commerce, Washington D.C., January 1977.

[3] Baptista M.S, “Cryptography with chaos”, *Phys. Lett. A 240, pp.50,* 1998.

[4] Ivan B.R., Dhodapkar S.D. and Lawande Q.V., “Cryptography using Lorenz dynamics”, *National Workshop on Cryptology*-2004, pp.10-12, Sept. 2004.

[5] Lorenz E.N., “Deterministic non periodic flow”, *J. Atmos. Sci. 20*, pp.130, 1963.

[6] Shanon, C., “Communication theory of secrecy systems,” *Bell Sys. Tech. J.* 28, pp. 656–715, 1949.

[7] Devaney, R. L., “An Introduction to Chaotic Dynamical Systems”, Redwood City, California, USA: Addison-Wesley, 1989.

[8] Hasler, M. “Synchronization of chaotic systems and transmission of information,” *Int. J. Bifurc. Chaos* 8, pp.647–659, 1998.

[9] Alvarez, G., Montoya, F., Romera, M. & Pastor, G. “Chaotic cryptosystems,” in L. D. Sanson, ed., *Proc. 33rd Annual 1999 International Carnahan Conference on Security Technology*, pp.332–338, 1999.

[10] Silva, C. P. & Young, A. M. "Introduction to chaos-based communications and signal processing," *in Proc. IEEE Aerospace Conference,* pp.279–299, 2000.

[11] Kocarev, L. "Chaos-based cryptography: A brief overview," *IEEE Circuits and Systems Magazine* 1, pp.6–21, 2001.

[12] Li, C., Li, S., Zhang, D. & Chen, G. "Cryptanalysis of a chaotic neural network based multimedia encryption scheme," *in Advances in Multimedia Information Processing – PCM 2004 Proceedings, Part III, Lecture Notes in Computer Science*, vol. 3333, pp. 418–425, 2004.

[13] Yang, T. "A survey of chaotic secure communication systems," *Int. J. Comp. Cognition 2,* pp.81–130, 2004.

[14] R.M. May, "Simple mathematical model with very complicated dynamics", *Nature 261*, pp.459, 1976.

[15] Boccaletti S., Kurths J., Osipov G., Valladares D., and Zhou C., "The synchronization of chaotic systems," *Phys. Rep*., vol. 366, no. 1-2, pp.1–101, 2002.

[16] Li S., Gonzalo G., Li Z., and Wolfgang A. Halang "Analog Chaos-based Secure Communications and Cryptanalysis: A Brief Survey"

[17] Wolfram, S. "Cryptography with cellular automata," *in Advances in Cryptology CRYPTO'85, Lecture Notes in Computer Science*, vol. 218, pp.429–432, 1985.

[18] Matthews, R. A. J. "On the derivation of a 'chaotic' encryption algorithm," *Cryptologia* XIII, pp.29–42, 1989.

[19] Berstein, G. M. & Lieberman, M. A. "Method and apparatus for generating secure random numbers using chaos," US Patent No. 5007087, 1991.

[20] Zhou, H. & Ling, X. "Generating chaotic secure sequences with desired statistical properties and high security," *Int. J. Bifurc. Chaos* 7, pp.205–213, 1997.

[21] Lee, P.-H., Pei, S.-C. & Chen, Y.-Y. “Generating chaotic stream ciphers using chaotic systems,” *Chinese J. Phys*. 41, pp. 559–581, 2003.

[22] Frey, D. R. “Chaotic digital encoding: An approach to secure communication,” *IEEE Trans. Circuits Syst. II* 40, pp. 660–666, 1993.

[23] Zhou, H. & Ling, X. “Problems with the chaotic inverse system encryption approach,” *IEEE Trans. Circuits Syst. I* 44, pp.268–271, 1997.

[24] Zhou, L.-H. & Feng, Z.-J. “A new idea of using one-dimensional PWL map in digital secure communications–dual-resolution approach,” IEEE *Trans. Circuits Syst. II* 47, pp.1107–1111, 2000.

[25] Kocarev, L., Jakimoski, G., Stojanovski, T. & Parlitz, U. “From chaotic maps to encryption schemes,” *in Proc. IEEE Int. Symposium Circuits and Systems* (ISCAS’98), vol. 4, pp.514–517, 1998.

[26] Guo, D., Cheng, L. M. & Cheng, L. L. “A new symmetric probabilistic encryption scheme based on chaotic attractors of neural networks,” *Applied Intelligence* 10, pp.71–84, 1999.

[27] Jakimoski, G. & Kocarev, L. “Chaos and cryptography: Block encryption ciphers based on chaotic maps,” *IEEE Trans. Circuits Syst. I* 48, pp.163–169, 2001.

[28] Papadimitriou, S., Bountis, T., Mavaroudi, S. & Bezerianos, A. “A probabilistic symmetric encryption scheme for very fast secure communications based on chaotic systems of difference equations,” *Int. J. Bifurc. Chaos* 11, pp.3107–3115, 2001.

[29] Tang, G., Liao, X. & Chen, Y. “A novel method for designing S-boxes based on chaotic maps,” *Chaos Solitons Fractals* 23, pp.413–419, 2005.

[30] Habutsu, T., Nishio, Y., Sasase, I. & Mori, S. “A secret key cryptosystem by iterating a chaotic map,” *in Advances in Cryptology – EUROCRYPT’91, Lecture Notes in Computer Science*, vol. 547, pp.127–140, 1991.

[31] Fridrich, J. “Symmetric ciphers based on two-dimensional chaotic maps,” *Int. J. Bifurc. Chaos* 8, pp.1259–1284, 1998.

[32] U´ıs, J., Ugalde, E. & Salazar, G. “A cryptosystem based on cellular automata,” *Chaos 8*, pp.819–822, 1998.

[33] Masuda, N. & Aihara, K. “Cryptosystems with discretized chaotic maps,” *IEEE Trans. Circuits Syst.I* 49, pp.28–40, 2002.

[34] Wen J., Severa M., Zeng W., Maximilian H. Luttrell, and Jin W., “A format compliant configurable encryption framework for access control of multimedia.” In *Proc. IEEE 4th Workshop on Multimedia Signal Processing (MMSP’2001),* pp 435–440, 2001.

[35] David S. Taubman and Michael W.M., “JPEG2000: Standard for interactive imaging.” *Proceedings of the IEEE*, 90(8), pp.1336–1357, 2002.

[36] Benoıt M. Macq and Jean-Jacques Q., “Cryptology for digital TV broadcasting.” *Proceedings of the IEEE*, 83(6), pp.944–957, 1995.

[37] Ali S.¸ Tosun A., and Wu-chi Feng. “Lightweight security mechanisms for wireless video transmission.” In *Proc. IEEE Int. Conference on Information Technology: Coding and Computing*, pp 157–161, 2001.

[38] Pareek N.K, Patidar V, Sud K.K. “Discrete chaotic cryptography using external key.” *Phys Lett A* 2003;309, pp.75-82, 2003.

[39] Chen G, Mao YB, Chui CK. “A symmetric image encryption scheme based on 3D chaotic cat maps.” *Chaos, Solutions & Fractals* 2004;12, pp.749-761, 2004.

[40] Mao Y.B, Chen G, Lian S.G, “A novel fast image encryption scheme based on the 3D chaotic baker map.” *Int. J. Bifurcat Chaos* 2004;14(10), pp.3613-24, 2004.

[41] Guan ZH, Huang FJ, Guan WJ. “Chaos-based image encryption algorithm,” *Phys Lett A* 2005;346, pp.153-7, 2005.

[42] Lian SG, Sun J, Wang Z. “A block cipher based on a suitable use of chaotic standard map.” Chaos, Solitons and Fractals 2005;26(1), pp.117-29, 2005.

[43] Li, S., Mou, X., Yang, B. L., Ji, Z. & Zhang, J. “Problems with a probabilistic encryption scheme based on chaotic systems,” *Int. J. Bifurc. Chaos* 13, pp.3063–3077, 2003.

[44] Alvarez, G., Hern´andez, L., Montoya, F. & Mu˜noz, J. “Cryptanalysis of a novel cryptosystem based on chaotic oscillators and feedback inversion,” *J. Sound Vibrat, pp.*275, 423–430, 2004.

[45] Cerm´ak, J. “Digital generators of chaos,” *Phys. Lett. A* 214, pp.151–160, 1996.

[46] Sang, T., Wang, R. & Yan, Y. “Perturbance-based algorithm to expand cycle length of chaotic key stream,” *Electron. Lett*. 34, pp.873–874, 1998.

[47] Fog, A. “How to optimize for the Pentium family of microprocessors”, 2000 [Online], Available: http://www.codingnow.com/2000/download/pentopt.htm. [Accessed: Sept. 13, 2008].

[48] Li, S. “Analyse and New Designs of Digital Chaotic Ciphers”, PhD thesis, School of Electronics and Information Engineering, Xi’an Jiaotong University, Xi’an, China, 2003, [online], available: http://www.hooklee.com/pub.html, [Accessed: June. 11, 2008].

[49] Menezes, A. J., van Oorschot, P. C. & Vanstone, S. A. *Handbook of Applied Cryptography*, CRC Press, 1997.

[50] Wang, X., Zhan, M., Lai, C.-H. & Gang, H. “Error function attack of chaos synchronization based encryption schemes,” *Chaos* 14, pp.128–137, 2004.

[51] ´Alvarez, G., Montoya, F., Romera, M. & Pastor, G. “Breaking parameter modulated chaotic secure communication system,” *Chaos Solitons Fractals* 21, pp.783–787, 2004.

[52] Stinson, D. R. “Cryptography: Theory and Practice”, CRC Press, 1995.

[53] Beth, T., Lazic, D. E. & Mathias, A. “Cryptanalysis of cryptosystems based on remote chaos replication,” in Y. G. Desmedt, ed., *Advances in Cryptology – CRYPTO’94, Lecture Notes in Computer Science*, vol. 839, pp.318–331, 1994.

[54] Sinha A., Singh K., “A technique for image encryption using digital signature”, *Optics Communications*, pp.1-6, 2003.

[55] Maniccam S.S., Bourbakis N.G., “Lossless image compression and encryption using SCAN”, *Pattern Recognition* 34, pp.1229-1245, 2001.

[56] Chin-Chen C., Min-Shian H., Tung-Shou C., “A new encryption algorithm for image cryptosystems”, *The Journal of Systems and Software 58*, pp.83-91, 2001.

[57] Jiun-In G., Jui-Cheng Y., “A new mirror-like image encryption algorithm and its VLSI architecture”, Department of Electronics Engineering National Lien-Ho College of Technology and Commerce.

[58] Zhang S. and Mohammed A.K., “Color image encryption using double random phase encoding”, MICROWAVE AND OPTICAL TECHNOLOGY LETTERS / Vol. 21, No. 5, pp. 318-322, June 5 1999.

[59] Young-Chang H., “Visual cryptography for colour images”, Pattern Recognition 36, 2003, [online], Available: www.elsevier.com/locate/patcog, pp.1619-1629, [Accessed: Jan. 20, 2008].

[60] Kuo C.J. , “Novel image encryption technique and its application in progressive transmission.” *J. Electron. Imaging* 24, pp. 345–351, 1993.

[61] Chang, H.K., Liou, J.L., “An image encryption scheme based on quad-tree compression scheme.” In: Proceedings of *the International Computer Symposium, Taiwan*, pp. 230–237, 1994.

[62] Scharinger J., “Fast encryption of image data using chaotic Kolmogrov flow”, J. *Electronic Eng 7* (2), pp. 318–325, 1998.

[63] Hossam El-din H.A., Hamdy M. K., and Osama S. F.A, “Encryption Efficiency Analysis and Security Evaluation of RC6 Block Cipher for Digital Images”

[64] Hossam El-din H. A, Hamdy M. K., and Osama S. F.A., “Encryption Quality Analysis of RC5 Block Cipher Algorithm for Digital Images.” *Journal of Optical Engineering*, vol. 45, 2006.

[65] ElGamal T., "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", *IEEE Transactions on Information Theory*, vol. IT-31, no.4, pp.469–472, 1985.

[66] Schneier B., “Description of a New Variable-Length Key, 64-bit Block Cipher (Blowfish)”, *Fast Software Encryption*, pp. 191-204, 1993

[67] Courtois N., Pieprzyk J., "Cryptanalysis of Block Ciphers with over defined Systems of Equations". pp267–287, ASIACRYPT 2002.

[68] Rivest, R. L. "The RC5 Encryption Algorithm" Proceedings of the *Second International Workshop on Fast Software Encryption (FSE)* 1994e: 86–96.