Chaos Communication by Applying Spatiotemporal Chaos

Hu Gang

Beijing Normal University, Department of Physics
Beijing 100875, P.R. of China

Conventional and chaos-based cryptographies are briefly introduced. The principles of the chaotic encryption and cryptanalysis are discussed. A spatiotemporal chaotic system (chaotic one-way coupled map lattice) is suggested for secure communication among multiple users. The practical security, encryption speed and synchronization transient time of the spatiotemporal chaotic cryptosystem are investigated. It is shown that spatiotemporal chaos may have remarkable advantages in chaos applications.

[1] Pecora, L. M. and Carroll, T. L. Synchronization in chaotic systems. Phys. Rev. Lett. 64, 821-824 (1990).

[2] Cuomo, L. M., and Oppenheim, A. V. Circuit implementation of synchronized chaos with applications communications. Phys. Rev. Lett. 71, 65-68 (1993).

[3] Kocarev, L., Halle, K. S., Eckert, K., Chua, L. O., and Parlitz, U. Experimental demonstration of secure communications via chaotic synchronization. Int. J. Bif. and chaos 2(3), 709-713 (1992).

[4] Kocarev, L. and Parlitz, U. General approach for chaotic synchronization with applications to communication \ Phys. Rev. Lett. 74(25), 5028-5031 (1995).

[5] Xiao, J. H., Hu, G., and Qu, Zh. L. Synchronization of spatiotemporal chaos and its application to multichannel spread spectrum communication. Phys. Rev. Lett. 77, 4162-4165 (1996).

[6] Hu, G., Xiao, J. H. and Yang, J. Zh. Synchronization of spatiotemporal chaos and its applications. Phys. Rev. E 56, 2738-2746 (1997).

[7] Gotz, M., Kelber, K. and Schwarz, W. Discrete-time chaotic encryption systems-Part I: statistical design approach. IEEE trans. Circuits syst. I, 44(10) , 963-970 (1997).

[8] Van Wiggeren, D. G., andRoy, R. Communication with chaotic -- Lasers. Science 279(20), 1198-1200 (1998).

[9] Gauthier, D. J. Chaos has come again. Science 279(20), 1156-1157 (1998).

[10] Sundar, S. and Minai, A. A. Synchronization of randomly multiplexed chaotic systems with application to communication. Phys. Rev. Lett. 85(25), 5456-5459 (2000).

[11] Garcia-Ojalvo, J. and Roy, R. Parallel communication with optical spatiotemporal chaos. IEEE trans. Circuits syst. I, 48(12) , 1491-1497 (2001).

[12] Short, K. M. >Steps toward unmasking secure communications. Int. J. Bif and chaos. 4(4), 959-977 (1994).

[13] Perez, G, and Cerdeira, H. Extracting message masked by chaos. Phys. Rev. lett. 74(11), 1970-1973 (1995).

[14] Short, K. M. Unmasking a modulated chaotic communications scheme. Int. J. Bif and chaos. 6(2), 367-375 (1996).

[15] Short, K. M., and Parker, A. T. Unmasking a hyperchaotic communication scheme. Phys. Rev. E 58, 1159-1162 (1998).

[16] Zhou, Ch.-S., and Lai, C. H. Extracting messages masked by chaotic signals of time-delay systems. Phys. Rev. E 60(1), 320-323 (1999).

[17] Zhou, Ch.-S. and Lai, C.-H. Decoding information by following parameter modulation with parameter adaptive control. Phys. Rew. E 59(6), 6629-6636 (1999).

[18] Alvarez, G., Montoya, F., Romera, M. and Pastor, G. Cryptanalysis of a chaotic encryption system. Phys. Lett. A 276, 191-196 (2000).

[19] Parker, A. T., and Short, K. M. Reconstructing the keystream from a chaotic encryption scheme. IEEE. Trans. Circuits Syst I. 48(5), 624-630 (2001).

[20] Kocarev, L. Chaos-based cryptography: a brief overview. IEEE circuits syst magz., 1(3), 6-21 (2001).

[21] Dachselt, F. and Schwarz, W. Chaos and cryptography. IEEE trans. Circuits syst. I, 48(12) , 1498-1509 (2001).

[22] Biham, E. and Shamir, A. Differential cryptanalysis of DES-like cryptosystems. J. Crypt., 4(1), 3-72 (1991).

[23] Matsui, M. Linear cryptanalysis method for DES cipher. Advances in cryptology- EUROCRYPT'93, 765, 386-397 (1994).

[24] Ding, C. The differential cryptanalysis and design of natural stream ciphers. Fast Software Encryption. LNCS 809. Springer-Verlag. 101-115 (1994).

[25] Golic, J. D. Linear cryptanalysis of stream ciphers. Fast Software Encryption 1994. LNCS 1008. Springer-Verlag.154-169 (1995).

[26] Shannon, C. E. A mathematical theory of communication. Bell Syst. Tech. J. 27(3), 379-423, 623-656 (1948).

[27] Shannon, C. E. Communication theory of secrecy systems. Bell Syst. Tech. J. 28, 656-715 (1949).

[28] Nechvatal, J., Barber, E., Bassham, L., Burr, W., Dworkin, M., Foti, J. and Roback, E. Report on the development of the advanced encryption standard (AES). [online]. Available: http://csrc.nist.gov/encryption/aes.