MATRIX ROM

C.P. 16 – 162, 062510 – BUCUREŞTI
tel. 021.4113617, fax 021.4114280
e-mail: office@matrixrom.ro, www.matrixrom.ro

Pseudo-random signal processing for cryptology. A chaos-teory based perspective

Contents

1 A pseudo-random perspective on chaos theory.
- 1.1 The logistic map, a model for chaos-based cryptography
- 1.2 A simple map exhibiting hyperchaotic behavior
- 1.3 Continuous-time chaotic algebraically simple jerks
- 1.4 Synchronization receiver - transmitter

2 Discrete-time chaos-based ciphers
- 2.1 A generalized 3D Hénon map cryptosystem
- 2.2 An algebraic cryptanalytic attack
- 2.3 A Matlab-Simulink application
- 2.4 Cryptographic security evaluation

3 Continuous-time chaos-based ciphers
- 3.1 The transmitter - a chaotic system embedding the private message
- 3.2 The receiving end - a high-order sliding mode estimator
- 3.3 A statistical method to determine the parameters of the observer
- 3.4 The cryptanalyst's perspective on the cryptosystem
- 3.5 Yet another chaotic flow as transmitter of the private message

4 A digital receiver for an analog transmitter
- 4.1 The transmitter - a Simulink analog model
- 4.2 A digital observer for the analog Simulink model
- 4.3 A glance into the future