Nonlinear dynamics, applications to chaos-based cryptography

Abstract

Chaotic systems are known to exhibit complex dynamic behavior. Their attractive characteristics render chaos-based cryptography very promising for the design of secure cryptosystems. Chaos-based cryptosystems can be classified into stream ciphers and block ciphers. A well designed pseudo-chaotic number generator (PCNG) with enhanced chaotic features and pseudo-randomness plays a crucial role in the security of a chaos-based cryptosystem. However, insufficient confusion and diffusion levels in the encryption algorithm, and unreliable PCNGs can lead to a security breach. In addition, the use of chaotic maps based on real numbers may jeopardize the reliability of the whole chaos-based cryptosystem.

For these reasons, in this thesis the proposed chaotic maps have been reformulated and designed over an N-bit (N=32) integer finite field, which overcomes the quantification problems and reduces the resource utilization. In addition, a new stream cipher based on an efficient PCNG, and a robust block cipher based on chaotic components and the S-box of Advanced Encryption Standard (AES) with excellent confusion and diffusion properties have been proposed. Both have been verified to be secure and reliable. Furthermore, a universal pseudo-random number generator (PRNG) framework based on a newly designed smart coupling of chaotic maps has been explored. It has good flexibility and can be used in cryptographic or other PRNG required applications.

Mots-clés : nonlinear dynamics, chaos-based cryptosystem, encryption algorithm, stream cipher, block cipher, pseudo-random number generator (PRNG)