Chaotic pseudorandom sequences and the security of cryptosystems

ABSTRACT

The generation of pseudo-random numbers (bits) plays a critical role in a large number of applications such as statistical mechanics, numerical simulations, gaming industry, communication or cryptography. The choice of secret keys for cryptographic primitives largely depends on the quality of random numbers used. These random numbers are fundamental tools in the generation of secret keys and initialization variables of encryption for cryptographic application, masking protocols, or for internet gambling. Chaotic Pseudorandom numbers were found to be very efficient in this aspect. The relevance of chaotic pseudorandom sequences in ensuring security in cryptosystems is considered, at the same time reviewing statistical tests required to make such sequences cryptographically secure. This paper intends to review the development of chaotic pseudorandom number generators through the years and the statistical tests they are required to pass as a measure of their randomness.

Keywords: Chaos; Deterministic algorithm; Non-linear map; Pseudorandom; Statistical test