Cryptanalysis of a family of 1D unimodal maps

ABSTRACT

In this paper, we proposed a topologically conjugate map,equivalent to the well known logistic map. This constructed map is defined on the integer domain [0, 2n) with a view to be used as a random number generator (RNG) based on an integer domain as is the required in classical cryptography. The maps were found to have a one to one correspondence between points in their respective defining intervals defined on an n-bits precision. The dynamics of the proposed map similar with that of the logistic map, in terms of the Lyapunov exponents with the control parameter. This similarity between the curves indicates topological conjugacy between the maps. With a view to be applied in cryptography as a Pseudo-Random number genera-tor (PRNG), the complexity of the constructed map as a source of randomness is determined using both the permutation entropy (PE)and the Lempel-Ziv (LZ-76) complexity measures, and the results are compared with numerical simulations.