A Very Efficient Pseudo-Random Number Generator Based On Chaotic Maps and S-Box Tables

Authors : M. Hamdi, R. Rhouma, S. Belghith

Abstract : Generating random numbers are mainly used to create secret keys or random sequences. It can be carried out by various techniques. In this paper we present a very simple and efficient pseudo-random number generator (PRNG) based on chaotic maps and S-Box tables. This technique adopted two main operations one to generate chaotic values using two logistic maps and the second to transform them into binary words using random S-Box tables. The simulation analysis indicates that our PRNG possessing excellent statistical and cryptographic properties.

Keywords : Random Numbers, Chaotic map, S-box, cryptography, statistical tests

Conference Title : ICICE 2015 : International Conference on Information and Communication Engineering

Conference Location : Istanbul, Türkiye

Conference Dates : January 26-27, 2015