Pseudo random bits' generator based on Tent chaotic map and linear feedback shift register

Hussam Alddin S. Ahmed[1], Mohamad F. Zolkipli[1], Saba M. Ismail1, Yazan A. Alsariera[1]
[1]Faculty of Computer Systems & Software Engineering, University Malaysia Pahang, 26300, Kuantan, Pahang, Malaysia
Corresponding author Email: hussam.alddin@outlook.com
Received: 16 Jun 2017 Accepted: 15 September 2017

The unforeseeable demand for secure paradigm cannot be fulfilled by the arbitrary sequence generated by the linear feedback shift register, which means the generated sequence can't meet satisfy the unpredictable demand for secure paradigm. Tent chaotic equation combined with the linear property of Linear Feedback Shift Register (LFSR) has resulted in a novel arbitrary sequence generator having a lengthier and composite structure. An analysis of the LFSR output sequence's architecture when combined with Tent map has revealed similar conformity compared to the homologous set of the individual linear constituents. Furthermore, to ensure the reliability of using the proposed Pseudo Random Number Generator (PRNG) in secure algorithms, the generated output bits sequence has been subjected to statistical analysis by NIST test suite and the result of the generated sequence confirm the efficiency of the proposed generator. The speed of the proposed generator and the security in terms of key space has been evaluated which give a robustness against different attacks.

Keywords: PRNG, Chaotic map, Cryptography, NIST 800-22.