A New Trend of Pseudorandom Number Generator using Multiple Chaotic Systems

Saba M. Ismail[1], Muamer N. Mohammed[1,2], Mohammed A. Ameedeen[1,2], Hussam Alddin S. Ahmed[1]

[1]Faculty of Computer Systems & Software Engineering, Universiti Malaysia Pahnag, 26300, Kuantan, Pahang, Malaysia

[2]IBM Center of excellence University Malaysia Pahang, 26300, Kuantan, Pahang, Malaysia

Corresponding author Email: saba.ismael@outlook.com

Received: 10 July 2017 Accepted: 29 August 2017

The information transmission domain had well been extended by the recent and fast developments in the telecommunication technologies specifically, the mobile networks and internet services. These new developments in turn, had come up with cutting-edge resolutions to secure information from being wiretapped. Countless in-depth studies in the field of cryptography had been carried out with the intent to propose a revolutionary solution for data protection of cryptographic techniques. This paper had proposed a new pseudo-random number generator (PRNG) design that had employed two chaotic systems which were logistics and tent maps, both of which had various operational and initialization values, which had subsequently contributed to the sequential distinction of the statistical properties. A compilation of a well- formulated assessment that had been provided by the National Institute of Standard Technology (NIST) was the foundation to ascertain the accuracy and exclusivity of the generated sequence and features with regards to this area of study. Moreover, a security analysis on key space and key sensitivity had been performed and it was concluded that the proposed PRNG was relevant for the implementation of cryptography.

Keywords: PRNG, Logistic map, Tent map, Cryptograph.