A CHAOTIC PSEUDORANDOM BIT GENERATOR FOR CRYPTOGRAPHY

Rashidah Kadir, Prof. Dr. Mohd Aizaini Maarof
Faculty of Computer Science and Information Systems,
Universiti Teknologi Malaysia
rashidah@utm.my, aizaini@utm.my

ABSTRACT
Pseudo-random number generation (PRBG) has become a critical requirement in cryptography field. However, the randomness of generated pseudorandom numbers is under questioned whether it can support reliable security in secure communication. Inadequate source of randomness can compromise the strongest cryptographic protocol and application. In this study, cryptographic pseudorandom bit sequences (PRBS) based on two-dimensional compound chaotic map are produced. Due to some interesting characteristics of chaos, such as sensitivity to initial conditions, ergodicity, unstable periodic orbits with long periods and random-like behavior, chaotic systems may appear to be good sources of randomness. The randomness of the PRBS has been statistically tested using FIPS140-2 and SP800-22. Comparison is made for different length of PRBS and different type of chaotic map. It shows a promising result that benefit in secure communication.

KEYWORD
Chaotic Pseudorandom Bit Generator, Chaotic Cryptography, Randomness Test