GENERATING TRUE RANDOM NUMBERS BASED ON CHUA'S CIRCUIT

G.D. Illeperuma

Department of Physics, Open University of Sri Lanka, Sri Lanka
Corresponding author: gdill@ou.ac.lk

A sequence of numbers that cannot be predicted is defined as a random number sequence. Random numbers have wide range of applications including cryptography, entertainment, lottery tickets and scientific simulations. Since a computer algorithm always follows a pre-determined path, it cannot be used to generate true random numbers, but can only generate pseudo random numbers. To generate true random numbers it is required to use an external non predictable trigger such as the electromagnetic noise or radioactive decay. In this research a novel approach of generating true random number is presented. Chua's circuit is a simple electronic circuit that exhibits chaotic behaviour. Standard Chua's circuit is deterministically chaotic, making it less suitable for random number generation. Therefore, it was modified to include a LDR coupled with a resistor to vary the initial conditions. Due to the butterfly effect, a small change in the initial condition would be magnified and effect the output. Since the initial parameters cannot be measured to an infinite accuracy, output would be non-predictable. Output voltage of the Chua's circuit was sampled at 0.1mV accuracy with a 10 mS period. Sample contained over 40,000 data points. It was hypothesized that it was impossible to determine the output of the circuit when the time difference between two consecutive readings is large. To test the hypothesis, data was re-sampled to have 0.5 S periods in between. Second digit of the decimal representation of the voltage level was converted to binary and the least significant bit was used as the random bit. The hypothesis was tested using the revised test suit published by National Institute of Standards and Technology (NIST), U.S, in 2010. Test suit was designed to test the feasibility of random number generators for cryptographic applications. Four of the standard tests were completed and further tests are to be conducted. Resulting P-values for the completed statistical tests are, Mono bit test: 0.69, Block test: 0.69, Runs test: 0.42, Longest run test: 0.99. Since all tests have a p-value > 0.1, it was concluded the sequence was random and the circuit can be used as a true random number generator.

Keywords: Chaos, Chua's circuit, NIS, Random number generation, True random numbers