Analog Integr Circ Sig Process
DOI 10.1007/s10470-015-0498-y

A new Chua's circuit with monolithic Chua's diode and its use for efficient true random number generation in CMOS 180 nm

H. Moqadasi · M. B. Ghaznavi-Ghoushchi

Received: 3 October 2014 / Revised: 9 January 2015 / Accepted: 19 January 2015

Abstract In this work we have proposed a new Chua's circuit which its negative resistor is a monolithic CMOS based circuit with 12 transistors, and then a true random number generator (TRNG) is proposed based on this new Chua's circuit which works. This proposed system also consists of a sample and hold block, an analog to digital converter (ADC) block and a linear feedback shift register (LFSR) block which scrambles generated bit stream and increases randomness. We changed the number of LFSR bits from 6 to 32, Experiments confirmed that the 6 bits length is optimum for LFSR which was better than previous works. In order to confirm correctness of the proposed TRNG, we applied four levels of FIPS140-1 statistical tests of National Institute of Standards and Technology then by varying the ADC resolution; we determined the allowable range which these tests were passed with and without using LFSR. Experiments confirmed that using LFSR lets us have smaller ADC and tests are passed better. Simulations were performed in system level and circuit level; also the system level simulation was used as golden model and was performed with MATLAB and circuit level was performed with SPICE and CMOS TECH 180 nm.

Keywords True random number generator · Chaos · Chua's circuit · CMOS technology · Nonlinear resistor · FIPS140-1

H. Moqadasi · M. B. Ghaznavi-Ghoushchi (✉)
Department of Electrical Engineering, School of Engineering, Shahed University, Tehran, Iran
e-mail: ghaznavi@shahed.ac.ir

H. Moqadasi
e-mail: hamidehmoghadasi@gmail.com

1 Introduction

Nowadays true random number generators (TRNGs) and pseudo random number generators (PRNGs) are needed in many important and applicable issues like cryptography, computer games and computer simulation programs [1]. Pseudo random numbers are generated in a deterministic manner [2] usually generated by predictable methods and mathematical formulas [3]. They have periodicity and are reproducible [4] so they cannot be random enough in some applications [3] whereas true random numbers are independent and unbiased and are generated by a nondeterministic and irreproducible process [5] with some post-processing functions [6] and usually are extracted from the natural world and intrinsic behavior of phenomena so they are better than pseudo random numbers in many cases [7]. Basically there are four ways for true random number generation which include: (1) Amplification of a noise source. (2) Jittered oscillator sampling. (3) Discrete-time chaotic map. (4) Continuous-time chaotic oscillators [8]. Generally there are three well known methods for randomness confirmation of a random bit stream, they include of: (1) Bitmap image. (2) Monte Carlo analysis of π. (3) statistical tests [9]. Federal information processing standard (FIPS) statistical tests include FIPS140-1 and FIPS140-2 [10] are used in many previous works like [11–18] in order to randomness confirmation.

Up to now many attempts have been conducted to generate true and pseudo random numbers and many of them are based on chaos. A lot of PRNGs are proposed based on linear feedback shift registers (LFSR). In [19] a parallel structured/-shifting LFSR (PS-LFSR) is proposed which has appropriate speed but could not pass simple statistical tests. In [20] this structure is reformed so that it has better randomness performance with maintaining the

Published online: 05 February 2015