Computers and Electrical Engineering 000 (2016) 1–12

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

The design and realization of a new high speed FPGA-based chaotic true random number generator

İsmail Koyuncu[a,*], Ahmet Turan Özcerit[b]

[a] Department of Electronic and Automation, Duzce University, Uzunmustafa Mah., Duzce 81010, Turkey
[b] Department of Computer Engineering, Sakarya University, Serdivan, Sakarya 54187, Turkey

ARTICLE INFO

Article history:
Received 12 August 2015
Revised 7 May 2016
Accepted 5 July 2016
Available online xxx

Keywords:
Chaos
Chaotic oscillators
Field programmable gate array
RK4 algorithm
True random number generator
NIST-800-22 statistical tests

ABSTRACT

Chaotic systems and chaos-based applications have been commonly used in the fields of engineering recently. The most essential part of them is the chaotic oscillator that has very critical role in some applications such as chaotic communications and cryptography. In this study, Sundarapandian–Pehlivan chaotic system has been modeled and simulated in three distinct platforms to show the advantages of FPGA-based chaotic oscillator with respect to alternative solutions. In the first stage, the chaotic system has been modeled numerically by the help of fourth order of Runge–Kutta (RK4) method. Additionally, phase portraits of the system have been obtained and Lyapunov exponents have been examined. Secondly, the system has been modeled by using PSpice for the implementation of the chaotic system with analog circuit elements. Then, Pspice simulation results have been compared with the numerical outcome to justify the designed model. Furthermore, the chaotic system has been physically confirmed with real analog circuit elements. Signals obtained from the physical system have been verified with both numerical and PSpice results. It has been also modeled by the help of method of RK4 in a hardware description language (VHDL) and the model further has been synthesized and tested for Xilinx Virtex-6 FPGA chip. Finally, the chaotic oscillator designed has been tested for True Random Number Generators (TRNG) and the maximum operating frequency has been achieved as 293 MHz with a speed of 58.76 Mbit/s. Besides, the random bit sets produced by TRNG have been further verified by FIPS-140-1 and NIST-800-22 statistical standards and it has been proved that the proposed design can be used in embedded cryptologic applications.

1. Introduction

Significant studies have been carried out in scientific and industrial fields for research and implementation of chaos and chaotic systems. Proving the existence of chaos in almost all fields of engineering, intensive studies and simultaneous developments lead to form many areas of implementation related to the chaotic systems. Following examples given below are some of their implementations: Control [1,2], optimization [3], cryptography [4], artificial neural network [5], communication [6], random number generator [7,8], and image processing [8].

One of the most fundamental structures required to use in chaotic-based engineering applications is the chaos generator. Chaos generators can be implemented in two fashions: analog or digital. Chaotic generators based on digital circuits have

[*] Corresponding author. Fax: +90 0380 524 00 97.
E-mail address: ismailkoyuncu@duzce.edu.tr (İ. Koyuncu).

http://dx.doi.org/10.1016/j.compeleceng.2016.07.005
0045-7906/© 2016 Elsevier Ltd. All rights reserved.

comparative advantages over analog ones [9]. Digital chaotic generators have been implemented by varied structures such as Digital Signal Processor (DSP) [10,11], Application Specific Integrated Circuit (ASIC) [12], and Field Programmable Gate Array (FPGA) [13-21].

Considering technologies mentioned above, the highest performance could be obtained from ASIC-based chaotic generators. However, ASIC-based implementations do not promise a flexible use, additionally; the cost of prototyping and testing of the system is very high. The system cost can be reduced substantially only if mass production is an option. A mistake made in mass production cycles could cause particularly high cost and waste of time.

DSP chips, which are optimized for realizing complex mathematical operations, implement operations sequentially. Constant-time chaotic systems characteristically constitute at least three differential equations and have at least three outputs. Being calculating sequentially values of output signal by systems based microprocessor or DSP takes a long time. On the other hand, FPGA chips are able to run concurrently and have relatively flexible architecture. Therefore, the cost of design and test cycles of FPGA chips is particularly low [22]. To increase and proliferate chaos-based engineering applications, current chaotic systems should be diversified and supported by flexible architectures. By means of digital and reconfigurable nature of FPGAs, chaotic systems and their applications can be more flexible. Thus, the chaotic systems can easily generate signals in different form as to their parameter changes. Besides, related chaotic system can be alternatively implemented by various nonlinear functions.

In the second section, Sundarapandian–Pehlivan Chaotic System (SPCS) is presented. In addition to numerical model, electronic circuit model and oscilloscope screen image obtained from physical circuits of SPCS are given. In the third section, the FPGA-based model of SPCS is introduced and simulation results of FPGA-based model are presented. In fourth section, SPCS is employed for TRNG purposes and related tests for randomness standards are verified. In the last section, obtained statistics and data have been interpreted.

2. Numerical solutions of SPCS and model of electronic circuit

In this section, SPCS [2] has been introduced by using differential equations (1) along with its numerical model. Additionally, oscilloscope outputs obtained from circuit model have been given.

$$\begin{aligned} dx/dt &= \alpha.y - x \\ dy/dt &= -\beta.x - z \\ dz/dt &= \gamma.z + x.y^2 - x \end{aligned} \tag{1}$$

To obtain a chaotic behavior, SPCS parameters are chosen as $\alpha = 1.5$, $\beta = 0.4$, and $\gamma = 0.4$ and the initial conditions are determined as $x_0 = 0$, $y_0 = 0$, and $z_0 = 0.1$. To perform an analysis on whether the system is chaotic, some available methods exist such as phase portraits, time series, Poincare mappings, power spectrums, bifurcation diagrams, spectrum of Lyapunov exponents. A Lyapunov exponent is one of the chaotic analysis methods that indicate whether the time series of the system has chaotic behaviors. Lyapunov methods can be used in the stability analysis of linear and non-linear systems.

In Lyapunov stability method, let $\dot{x} = f(x)$, $x \varepsilon \Re^n$ and consider a non-linear system function $f(x)$ having continuous and derivative characteristics when variables of x_1, x_2.....x_n are concerned and $f(x_e) = 0$ at equilibrium point. Having obtained Taylor series near the equilibrium point x_e and by the help of $y = x - x_e$ transformation, the equilibrium point can be shifted to the origin. In $\dot{y} = Ay + xG(y)y$ expression, Ay denotes linear and $G(y)y$ denotes non-linear terms. The value of each element of $G(y)y$, *which* is formed by the high degree derivatives of Taylor expansion, is regarded as zero. Thus, it can be defined as $\dot{y} = Ay$. Lyapunov method shows that if the reel part of each characteristic value of matrix A are different from zero, the stability of non-linear system ($\dot{x} = f(x)$) equals the stability of the system. As a result, if the reel part of one of the characteristic value is in the right pane, the system is regarded as unstable; if each characteristic value is in left pane, the system is regarded as asymptotic stable.

In three-dimensional phase space when Lyapunov method is used to analyze the system, the exponents (λ_1, λ_2, λ_3) have signs as (-, -, -) respectively if the system is at equilibrium point; (0, 0, -) if the system is in two torus state; (0, -, -) if the system is in limited cycle state; and (+, 0, -) if the system is in chaotic state. In other words, if the sign of the biggest exponent is positive, the system is regarded as chaotic.

In order to find the equilibrium point of the SPCS and to calculate the Lyapunov exponents, we have used a Matlab-based tool, and obtained results are presented in Fig. 1. As shown in Fig. 1, since the biggest exponent of Lyapunov has a positive sign, the system is chaotic.

There are many methods exist in the literature to solve differential equations such as Euler, Heun and 4th degree Runge–Kutta (RK4). RK4 is a derivative of the Runge–Kutta basic model and mostly has proved itself as superior to alternatives solutions. The equations of RK4 algorithm are given in Eq. (2) [23]. In order to calculate term $y_{\lambda+1}$, initially the value of parameter k_1, k_2, k_3 and k_4 must be computed. Each parameter k_x is computed iteratively and respectively by facilitating the previous parameter and regarding Δh distance. Thus, the next $y_{\lambda+1}$ value of the system is calculated using the values of y_λ and Δh distance.

$$\begin{aligned} y_{\lambda+1} &= y_\lambda + \frac{1}{6}(k_1 + 2k_2 + 2k_3 + k_4)\Delta h \\ k_1 &= f(y_\lambda) \end{aligned}$$

Please cite this article as: İ. Koyuncu, A. Turan Özcerit, The design and realization of a new high speed FPGA-based chaotic true random number generator, Computers and Electrical Engineering (2016), http://dx.doi.org/10.1016/j.compeleceng.2016.07.005