FPGA Implementation of Chaotic Generator Using Numerical Algorithms

Subodh Kumar Pandey[1], Dr.Sanjeev Kumar Gupta[2]
[1,2]Dept. of ECE, Rabindranath Tagore University, Raisen (M.P.) India.

ABSTRACT
Now a day's chaotic systems have an important role in secure communication and cryptography. As FPGA implementation have certain advantages over analog one, different chaotic system like chaotic oscillator, True random number generators and chaotic systems used in image processing, optical circuits for secure communications were successfully realized in FPGA. This paper presents methodology of FPGA implementation of any chaotic system using different numerical algorithm. In study the Numerical solution of Differential equations given in Pandey-Baghel-Singh system were obtained and coded in Verilog and tested with XilinxVivado 17.3 design suites in Artix-7 Nexus 4 DDR and Basys3. Performance of the FPGA based chaotic generator using Heun and RK4 algorithmsare analyzed using 10^6 data sets with the maximum operating frequency achieved up to 359.71MHz.

Key Words - Chaotic Generators, Heun, RK4 algorithm, FPGA

I INTRODUCTION

Chaos generator is a fundamental block of any chaos based system. Basically chaos based system are used in secure communication and cryptography.Recently implementation of FPGA based real time chaotic systems were presented. Due to parallel processing capabilities the processing speed of FPGA is much higher. Analog based chaotic generatorsare sensitive to initial conditions and acquires a large chip area hence it may be interesting to see the performance of FPGA based chaotic generators to avoid these problems.Digital based design of chaotic generators using FPGA can be implemented as FPGA implementation is more flexible architecture and have low cost test cycle and found more useful in chaos based engineering applications [1-7].

In II section of the paper presented the Pandey-Baghel-Singh Chaos System (PBSCS) is described along with their x,y and z signals and their attractors [8]. In the III section the mathematical models of PBSCS is numerically obtained using Heun and RK4 algorithms and FPGA models of PBSCS is introduced. In sectionIV simulation results of different numerical algorithm based design has been presented and analyzed. In section V conclusion is given.

II INTRODUCTION TO PANDEY-BAGHEL-SINGH CHAOS SYSTEM

Pandey-Baghel-Singh Chaos System (PBSCS)is defined by the set of differential equation (1).

$$\begin{aligned} \dot{x} &= y \\ \dot{y} &= z \\ \dot{z} &= -ax - by - cz - x \end{aligned} \qquad (1)$$

In the system two equilibrium points as (0, 0, 0) and (-1, 0, 0)were shown forthe constants a = 1, b = 1.1, and c = 0.4.The equilibrium point (0, 0, 0) have the Eigen values -0.745, 0.162+j1.147and 0.162-j1.147. For the equilibrium point (-1, 0, 0) the Eigen values shown are 0.589, -0.504+j1.20, and -0.504-j1.20. The initial condition for the system is taken x = 0.1, y = 0 and z = 0.The time domain representation of x, y and z waveform are given in Fig.1 and attractors generated are given in Fig. 2 (a-c).

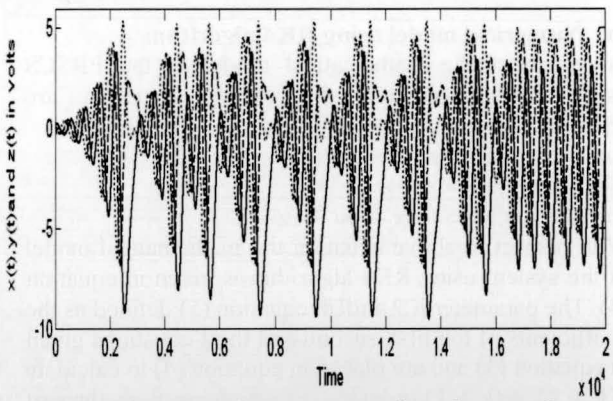
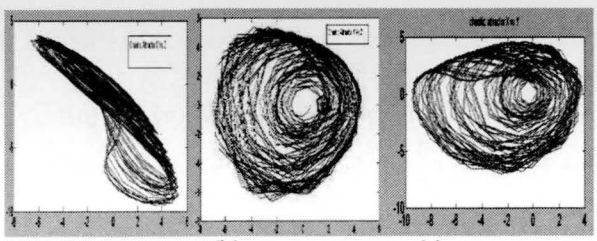


Fig 1: Time domain representation of x, y and z signals of PBSCS.



(a) (b) (c)

Fig 2: (a) x-y attractor, (b) y-z attractor, (c) x-z attractor

III NUMERICAL MODELS OF PBSCSAND THEIR FPGAIMPLEMENTATION USING DIFFERENT NUMERICAL ALGORITHMS

For FPGA implementation of the system the numerical model of PBSCSis obtained using Heun and RK4algorithm and coded in Verilog.

(a) Numerical model using Heun algorithm

For the numerical model using Heun algorithm initial value of x (n), y (n) and z (n) are taken as x (t_0) = x (n) = 0.1, y (t_0) = y (n) = 0 and z(t_0) = z(n) = 0, The Heun algorithm have two successive stages. In the first stage

$x(n+1)$ is calculated and $x(n+1)$ the value after steps h is calculated using previous values $x(n+1)$ and$x(n)$. The mathematical model of PBS chaotic system is described by the following Equation (2).

$$x(n+1) = x(n) + h.y(n)$$

$$x(n+1) = x(n) + h\{y(n) + x(n+1)\}/2 \quad (2)$$

$$y(n+1) = y(n) + h.z(n)$$

$$y(n+1) = y(n) + h\{z(n) + y(n+1)\}/2$$

$$z(n+1) = z(n) + h\{-a.x(n) - b.y(n) - c.z(n) - x(n)\}$$

$$z(n+1) = z(n) + h.[\{-a.x(n) - b.y(n) - c.z(n) - x(n)\} + z(n+1)]/2$$

(b) Numerical model using RK4 algorithm

To construct the mathematical model of the PBSCS using RK4 algorithm, the system equation are represented as a function of f, gandδ as equation (3)

$$\dot{x} = f(t,x,y,z) = y$$
$$\dot{y} = g(t,x,y,z) = z \quad (3)$$
$$\dot{z} = \delta(t,x,y,z) = -ax - by - cz - x$$

With respect to above equation the mathematical model of the system using RK4 algorithm is given in equation (4). The parameter K,λandξin equation (5) defined as the coefficients of the first, second and third equations given in equation (3) and are placed in equation (4) to calculate $x(k+1)$, $y(k+1)$and$z(k+1)$ which are the values of the system afterh steps.

The valuesx$(k+1)$,y$(k+1)$andz$(k+1)$are the output of the system after each interval which are used as initial conditions of the algorithm to calculate the values for the next cycle.

$$x(n+1) = x(n) + \frac{1}{6}h[k(n) + 2k(n) + 2k(n) + k(n)]$$

$$y(n+1) = y(n) + \frac{1}{6}h[\lambda(n) + 2\lambda(n) + 2\lambda(n) + \lambda(n)]$$

$$z(n+1) = z(n) + -h[\xi(n) + 2\xi(n) + 2\xi(n) + \xi(n)] \quad (4)$$

$$k = f[x(n), y(n), z(n)]$$
$$\lambda = g[x(n), y(n), z(n)]$$
$$\xi = \delta[x(n), y(n), z(n)]$$

$$k = f[x(n) + \frac{1}{2}hk.y(n) + \frac{1}{2}h\lambda.z(n) + \frac{1}{2}h\xi]$$
$$\lambda = g[x(n) + \frac{1}{2}hk.y(n) + \frac{1}{2}h\lambda.z(n) + \frac{1}{2}h\xi]$$
$$\xi = \delta[x(n) + \frac{1}{2}hk.y(n) + \frac{1}{2}h\lambda.z(n) + \frac{1}{2}h\xi]$$
$$k = f[x(n) + -hk.y(n) + -h\lambda.z(n) + -h\xi] \quad (5)$$
$$\lambda = g[x(n) + \frac{1}{2}hk.y(n) + \frac{1}{2}h\lambda.z(n) + \frac{1}{2}h\xi]$$
$$\xi = \delta[x(n) + \frac{1}{2}h.(\,) + \frac{1}{2}h.(n) + \frac{1}{2}h\xi]$$

$$k = f[x(n) + hk\ y(n) + h\lambda\ z(n) + h\xi]$$

$$\lambda = g[x(n) + hk\ y(n) + h\lambda\ z(n) + h\xi]$$

$$\xi = \delta[x(n) + hk\ y(n) + h\lambda\ z(n) + h\xi]$$

(c) FPGA Implementation of Autonomous Chaotic Generator

The PBSCS which have been modeled usingHeun andRK4 algorithm are implemented with 32- bit IEEE 754-1985 standard on FPGA. Mathematicalmodeling is done in VerilogusingVivado design suite. The Top-level diagramwhich is same for both models using Heun and RK4algorithm have been shown in Fig. 3. For the synchronization purpose one bit start, reset and clock signal is used. A 32-bit input has been used and initial conditions are set in the beginning phase. The 32-bit signal are used as input parameter. There is three 32-bit output signals (Xn_out), (Yn_out) and (Zn_out)and ready signal is taken as one bit control signals for the proposed chaotic generator.

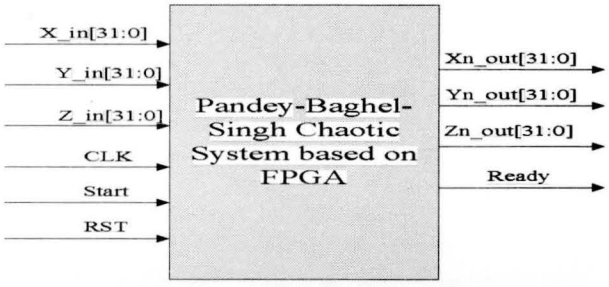


Fig.3 Top level diagram of PBS Chaotic System based on FPGA

The second level block diagram of the chaotic generator is presented in Fig. 4 It have one multiplexer and a chaotic generator unit whichis FPGA based. The multiplexer is used to provide initial condition signals. For successive operation it is provided by the output signals. When enable is at logic high, the output generates chaotic signal.

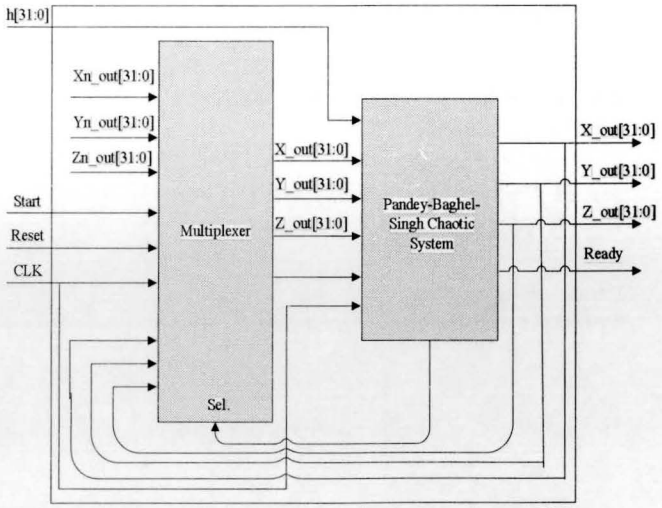


Fig.4 second level diagram of PBSCS based on FPGA

The third level block diagram of the Heun based chaotic generator is given in Fig.5. The proposed generator consist of multiplexer, function f^0, multiplier, adder, f, Divider and filter stages. The PBSCS equation are calculated by f stage with the help of MUX unit which provides control signal. After multiplication with h the

output is added with the previous generated signal x(n), y(n)andz(n) by the generator unit. The output of this adder stage is applied to f stage which calculate the equation of PBSCS. The output of this stage and output of f are adder-II stage. Further the output of the adder-II stage divided in the divider stage. In adder-III stage output of the chaotic generator from MUX stage and divider stage are added. The Heun based chaotic generator works in sequential order which generates the first value after 118 clock cycles.

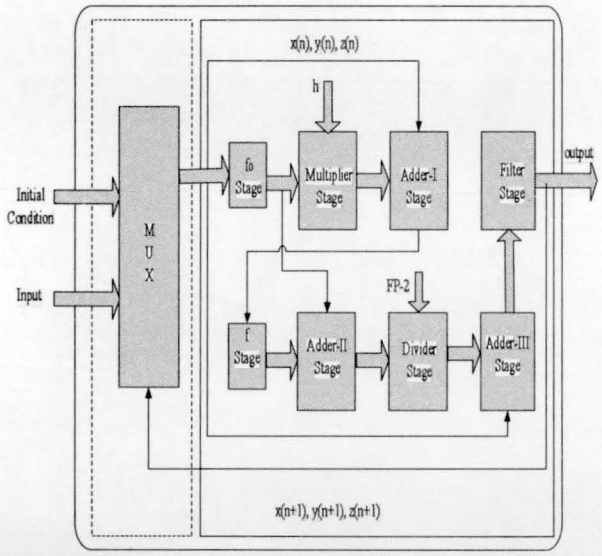


Fig. 5 Third Level diagram of Heun based PBSCS Generator Unit

The thirdlevel block diagram of the RK4 based chaotic generator is given in Fig. 6. The proposed chaotic generator consist of multiplexer, K_s units, Y_s block and filter stage.K_s units calculate k ,λ andξ where s varies between1 to 4.

The $x(k+1), y(k+1)$andz$(k+1)$given in equation (3) are Calculatedat Y_s block. The first value is generated after 142 clock pulses and a feedback system is to be employed so that output is feedback to MUX after 142 clock pulses to generate next cycle. Filter unit stops undesired signal to reach output if generator does not generate any result.

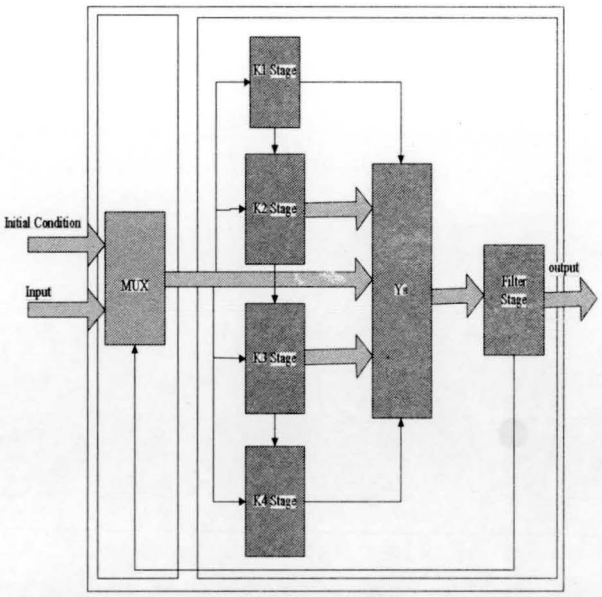


Fig. 6 Third Level diagram of RK4 based PBSCS Generator Unit

IV SIMULATION RESULTS OF PBS CHAOTIC GENERATOR

The numerically modelled (Heun and RK4) PBS Chaotic generator have been synthesized on Nexus-4 DDR XC7A100TCSG-1 (Artix7) and Basys-3 (Artix7) from the Xilinx Vivado v.2017.3 design suite. The simulation results of numerically modelled PBSCS andFPGA chip related Parameters and clock speed of the system is presented in the Fig. 7and Fig. 8. The summery of the FPGAchip speed and other statistics which are obtained for both the algorithm based system is given in table 1. Among the two numerically modelled system the RK4 based chaotic generator gives optimize result with the use of 2637 LUT's and 4692 registers with set clock period 2.78 ns which corresponds to maximum frequency achieved 359.71 MHz.The attracter of the system is generated by the data set are given in fig. 9 (a-c) which are similar to PBSCS designed on analog platform

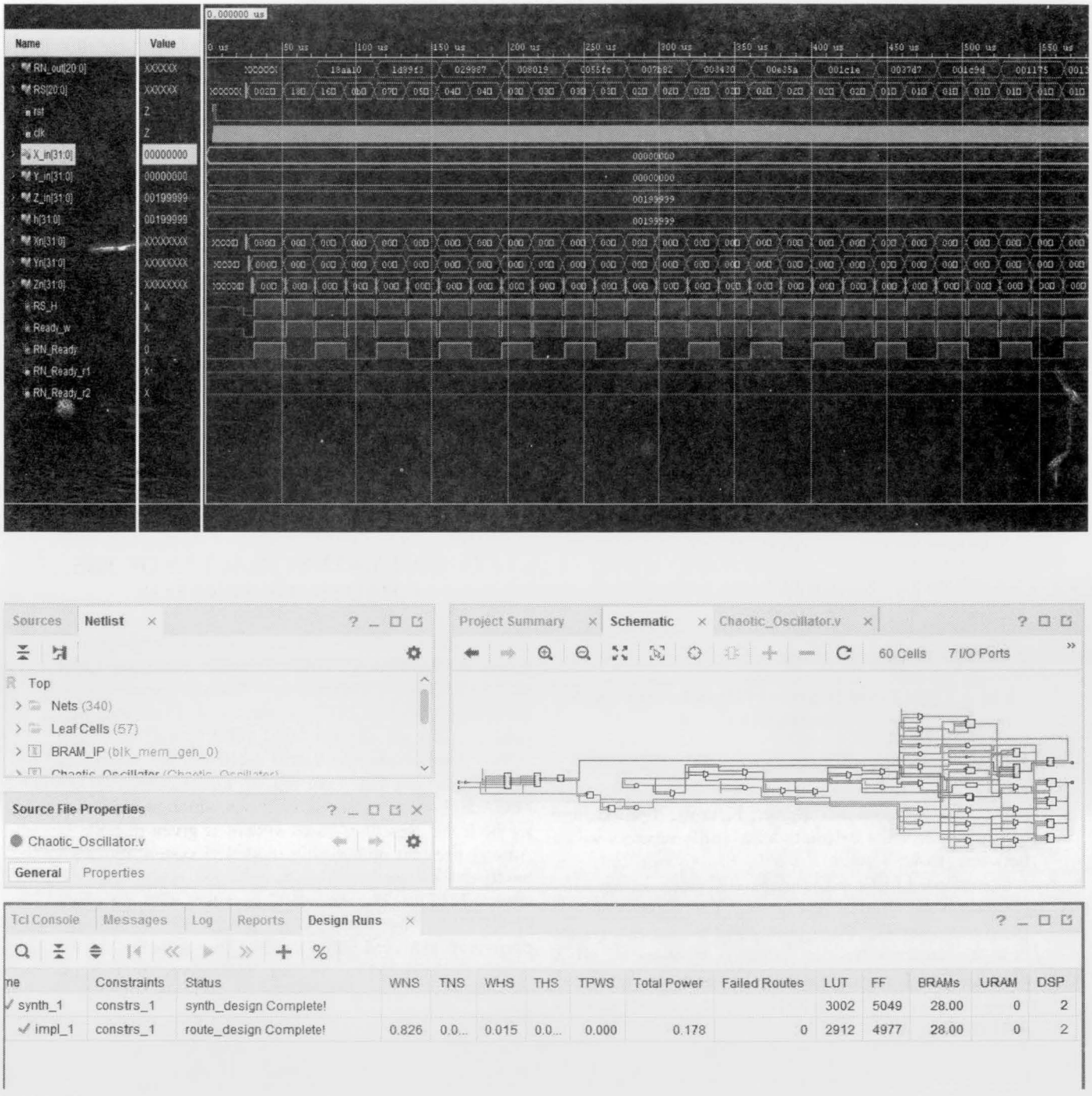


Fig.7 Simulation result of Heun based PBSCS on Vivado 17.3

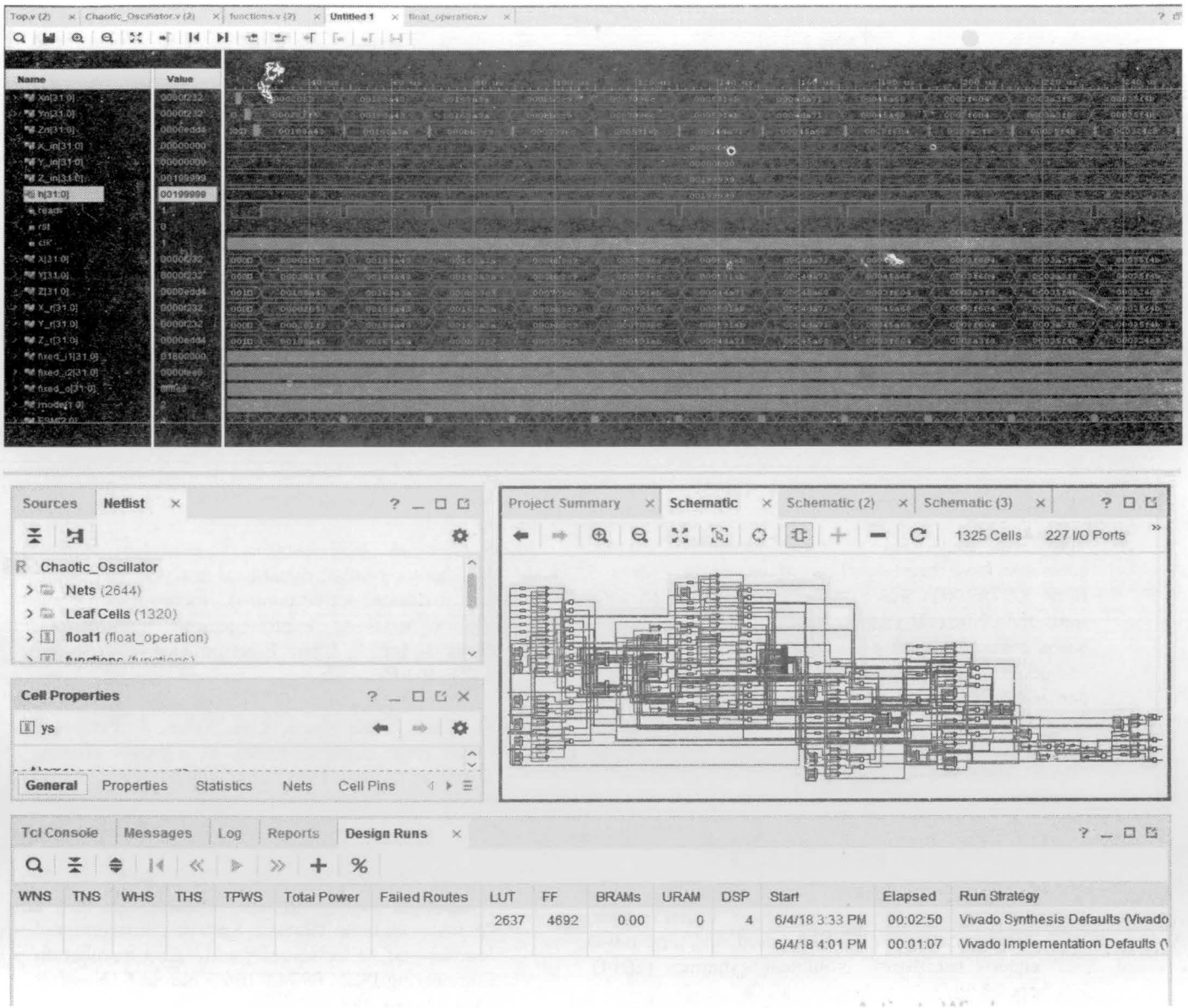
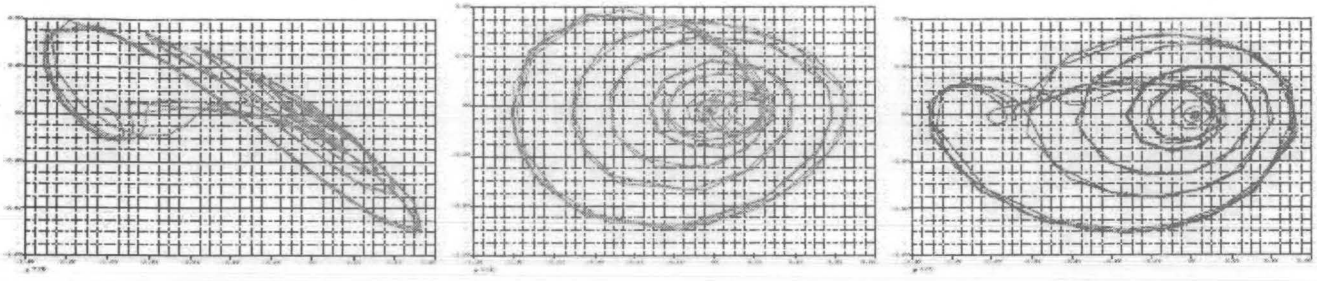


Fig.8 Simulation result of RK4 based PBSCS on Vivado 17.3



(a) (b) (c)

Fig. 9 (a) x-y attractor, (b) y-z attractor, (c) x-z attractor

Table 1
Final report of the resources consumption

Parameter	Heun-based	RK4-based
Maximum frequency (MHz)	359.71	359.71
No. of DSP	2	4
Number of 4 input LUTs	2912	2637
Number of bonded IOBs	32	32
Number of Slice Flip Flops	4977	4692
Total On-chip Power(W)	0.178	0.179

V CONCLUSION

The Heun and RK4 algorithm basedPBS Chaotic generator have been synthesized using the Nexus 4 DDR XC7A100TCSG-1 (Artix7) and Basys3 (Artix7) from the Xilinx Vivado v.2017.3 design suite. RK4 based chaotic generator gives optimize result with the use of 2637 LUT's and 4692 registers with set clock period 2.78 ns which corresponds to maximum frequency achieved 359.71 MHz.The attracter of the system is generated by the data setare given in fig. 10(a-c) which are similar to PBSCS designed on analog platform.

REFERENCES

[1] Ismail K., A. Tuaran O, IhsanPehlivan, "Implementation of FPGA-based real time novel chaotic oscillator", Nonlinear dynamics (2014); pp. 49-59.

[2] Murat Tunaa, Can BülentFidan, "Electronic circuit design, implementation and FPGA-basedrealization of a new 3D chaotic system with singleequilibrium point", Optic ElsevierOptik(2016) pp. 11786–11799.

[3] S. Banerjee, J. Kurths, "Chaos and cryptography: a new dimension in secure communications", Eur. Phys. J. Spec. Top. , (2014) pp. 1441–1445.

[4] I. Koyuncu, A.T. Ozcerit, I. Pehlivan, "An analog circuit design and FPGA-based implementation of the Burke-Shaw chaotic system", Optoelectron. Adv. Mater. Rapid Commun. (2013) pp. 635–638.

[5] L. Merah, A. Ali-pacha, N.H. Said, "A pseudo random number generator based on the chaotic system of Chua's circuit and its real time", FPGA Implementation (2013) pp. 2719–2734.

[6] S. C¸ ic¸ ek, A. Ferikog˘lu, I˙. Pehlivan, "A new 3D chaotic system: dynamical analysis, electronic circuit design, active control synchronization and chaotic masking communication application", Optik – Int. J. Light Electron Opt. (2016) pp. 4024–4030.

[7] M. Tuna, I. Koyuncu, C.B. Fidan, I. Pehlivan, "Real time implementation of a novel chaotic generator on FPGA", in: 2015 23rd Signal Processing andCommunications Applications Conference (SIU), IEEE, 2015, pp. 698–701.

[8] Alpana Pandey, R. K. Baghel, R.P. Singh, "Analysis and Circuit Realization of a NewAutonomous Chaotic System", International Journal of Electronics and Communication Engineering.ISSN 0974-2166 Volume 5, Number 4 (2012), pp. 487-495.