International Journal of Engineering & Technology, 7 (3) (2018) 1783-1785

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i3.16586
Research paper

Efficient design of chaos based 4 bit true random number generator on FPGA

Ramji Gupta [1] *, Alpana Pandey [1], R. K. Baghel [1]

[1] Department of Electronics and Communication MANIT, Bhopal, India
**Corresponding author E-mail: ramjigupta38@yahoo.com*

Abstract

True random number generator is a basic building block of any modern secure communication and cryptography system. FPGA implementation of any system has a flexible architecture and low-cost test cycle. In this paper, we present an FPGA implementation of a high speed true random number generator based on chaos oscillator which gives optimize ratio of bit rate to area. The proposed generator is faster and more compact than the existing chaotic oscillator based TRNGs. The Experimental result shows that the proposed TRNG gives 1439 Mbps with optimizing the use of LUTs and registers. It is verified that the generator passes all the NIST SP 800-22 tests. The proposed TRNG is implemented in two FPGA families Nexus 4 (Artix 7) DDR XC7A100TCSG-1 and Basys 3 XC7A35T1CPG236C (Artix 7) using Xilinx Vivado v.2017.3 design suite.

Keywords: *Field Programmable Gate Array (FPGA); Chaotic Oscillator; True Random Number Generator (TRNG).*

1. Introduction

True random number generators (TRNG), is an integral part of any security system. With high entropy, true random number generator find applications in software security via password generation, protocols to validate aforesaid parties and vector initialization. TRNG overcomes the limitation of pseudo random generators using microscopic or macroscopic phenomenon such as electrical noise, as a sources of randomness which may produce predictable outcomes [1-2]. TRNG based on analogue circuits requires larger area, high power consumption and having low speed. On the other hand digital logic and FPGA based TRNG have good flexibility, high speed, reduced size and less complexity. Digital TRNGs has mainly three components: Entropy source such as ring oscillator or chaotic oscillator, Entropy harvester such as sampler and post processor such as linear feedback shift register (LFSR) [3-6]. The speed of the TRNGs depends upon the used entropy sources such as accumulated jitter [3], [4], [7] and transition effect [6]. Chaotic oscillator can be used as an entropy source and the achieved output bit rate are in the range of 125 Mbit/s [3]. Self-time ring based TRNG (STRNG) gives a high bit rate with larger area [8]. TRNG based on critical sampling requires fast oscillator with manual placement [8]. TNRG based on two metastable flip-flops uses adaptive feedback loop to control the randomness [2], [9], 10].
Our aim is to design TRNG containing digital components to make design simple and suited for FPGA implementation. We proposes a FPGA implementation of TRNG using chaotic oscillator as a source of randomness in addition to meta-stability state of flip flop stage which provide a high bit rate with small area in terms of LUT's and registers compare to previous designs.

2. Chaos based TRNG

The proposed chaos based TRNG with multiple sampling uses chaotic oscillator (CO) as a source of randomness and output of ring oscillator (RO) to provide clock signal. The schematic diagram of proposed 4 bit TRNG is presented in fig.1 consisting of [4] chaos based TRNGs in parallel. The chaos based TRNG consist of a chaotic oscillator, a ring oscillator and a D flip flop. The schematic diagram of chaos based TRNG is presented in fig.2.

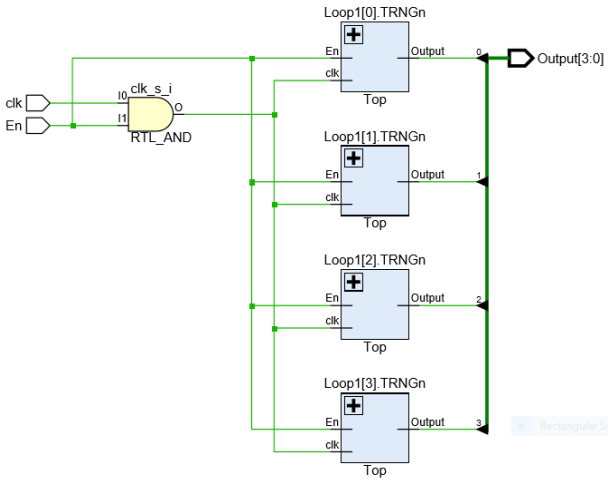


Fig. 1: Schematic of Proposed [4] Bit TRNG.

Copyright © 2018 Ramji Gupta et. al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

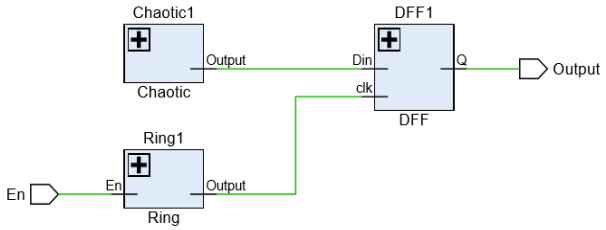


Fig. 2: Schematic of TRNG.

Chaotic oscillator consists of 16 inverters in series presented in fig.3. The schematic diagram of ring oscillator is presented in fig.4 which also consist of 16 inverter in series.

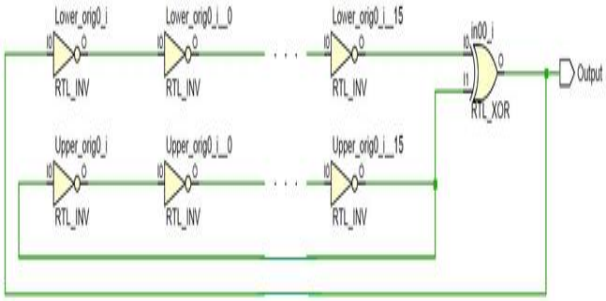


Fig. 3: Schematic of Chaotic Oscillator.

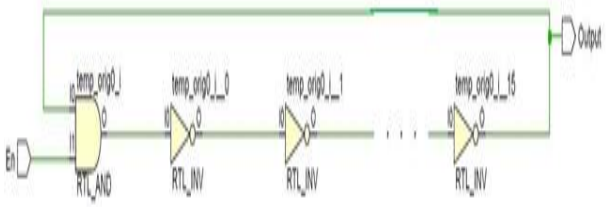


Fig. 4: Schematic of Ring Oscillator.

The output bit rate can be easily increases either by increasing the global clock frequency or by adding identical TRNGs in parallel. The Proposed design of TRNG consist of chaos based [4] identical TRNGs in parallel to increase the bit rate. The output signal of CO is sampled into the positive edge triggered D Flip Flop (FF) which works as a sampler. The clock pulse is provided by RO. Chaotic oscillator and ring oscillator starts oscillation at enable high. CO and RO does not oscillates at enable low and FFs retain the previous value. The output of CO is sampled to the D flip flop at the intervals of T_{clk}, and it generates 4-bit random string. The proposed design shows randomness of chaotic oscillator at different clock pulses of duration 2.78 ns, 8ns and 10 ns which corresponds to maximum achieved clock frequency of RO 359.71 MHz. So under the design frame work the proposed TRNG is capable to generate 4 bit in 2.78 ns at the output which corresponds to bit rate of 1439 Mbps. Further to increase randomness, post processing unit (PPU) is added to the circuit as presented in fig.5. The PPU consist of 4 bit linear feedback shift resister (LFSR) connected to the TRNG which remove the raw numbers from generated bit strings and improve the randomness. The schematic diagram of PPU unit implemented in FPGA is shown in fig.6

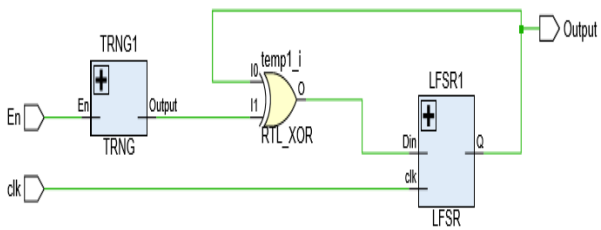


Fig. 5: Structure of Proposed TRNG with PPU.

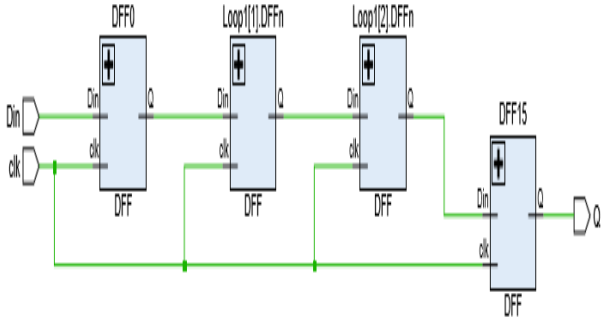


Fig. 6: Structure of 4 Bit LFSR.

3. Implementation and test results

The proposed TRNG is implemented with Nexys 4 DDR XC7A100TCSG-1 (Artix 7) and Basys 3 XC7A35T1CPG236C (Artix 7) FPGA families. Nexys 4 and Basys 3 gives high performance with Vivado Design Suite of Xilinx is which includes several new tools and design flows that expedite and improve the latest design methods. It runs faster; make better use of FPGA resources. For the NIST test 10^6-bit streams were generated from TRNG and the bit streams at the output of PPU were transmitted from FPGA board to the PC using USB port of the Nexys 4 DDR and Basys 3 evaluation board with the help of interface unit. The interface unit is implemented by a FIFO-UART (Universal Asynchronous Receive Transmit) combination. For NIST test results the level of significance is set to P = 0.01[11]. Result shows that all P-value are greater than 0.01 for T_{clk} of duration 2.78 ns, 8 ns and 10 ns which confirms that the generated bit strings are random. The NIST SP 800-22 test results for T_{clk} of duration 2.78 ns is presented in table 1.

Table 1: NIST Test Results of Proposed TRNG for Tclk = 2.78 Ns

Test	Artix7 Nexus-4		Artix7 Basys-3	
	P-value	Result	P-value	Result
Frequency (monobit)	0.579	Successful	0.783	Successful
Block Frequency	0.288	Successful	0.433	Successful
Cumulative sums(forward)	0.097	Successful	0.387	Successful
Cumulative sums (inverse)	0.453	Successful	0.613	Successful
Runs	0.288	Successful	0.783	Successful
Longest run	0.539	Successful	0.563	Successful
Rank	0.349	Successful	0.231	Successful
FFT	0.999	Successful	0.342	Successful
Non-overlapping	0.734	Successful	0.672	Successful
Overlapping	0.342	Successful	0.876	Successful
Universal	0.394	Successful	0.453	Successful
Approximate entropy	0.743	Successful	0.821	Successful
Random excursions (x=+1)	0.384	Successful	0.781	Successful
Random excur.variant(x=-1)	0.832	Successful	0.912	Successful
Serial (m=16)	0.403	Successful	0.994	Successful
Linear complexity	0.754	Successful	0.834	Successful

The area (LUT and register) and throughput of the proposed TRNG are given in table 2.

Table 2: Implementation Results of Proposed TRNG

FPGA family	Area (LUT+Reg.)		Bit rate (Mbit/s)	BPA ($\frac{Mbit/s}{LUT+Reg.}$)
	TRNG	TRNG with PPU		
Nexus 4 DDR Artix7	44+4	53+8	1439	29.87
Basys 3 Artix7	44+4	53+8	1439	29.87

The statistics of the TRNGs implemented previously is given in Table 3. It can be observed from Tables 2 and 3 that the presented TRNG is optimized in terms of bit rate and area. At very high bit rate of 1439 Mbps the proposed TRNG occupy relatively low area. The parameter bit rate to area ratio (BPA) of proposed TRNG is better than other all TRNGs.

Table 3: Implementation Results of Previous Trngs

	[7]	[8]	[9]	[10]	Proposed TRNG
Area(LUT+REG)	525+130	352+256	298	511	53+8
Bit rate (Mbps)	2.2	245	150	133	1439
BPA	0.0033	0.402	0.5033	0.260	29.87
FPGA family	Cyclone V	Cyclone V	Cyclone IV	Cyclone III	Artix-7

4. Conclusion

We presented a chaos based TRNG using chaotic oscillator at 359.71 MHz using multiple sampling implemented in two FPGA family: Nexus 4 DDR XC7A100TCSG-1 (Artix 7) and Basys 3 (Artix 7) Xilinx Vivado v.2017.3 design suite passed the entire NIST test. At clock, timing of 2.78 ns and 4 TRNGs which were added in parallel proposed 4 bit TRNG produces maximum bit rate of 1439 Mbps. The experimental results showed that the proposed TRNG is faster and more compact than previously implemented TRNGs.

References

[1] V. Fischer, "A closer look at security in TRNGs design," in Proceedings of Constructive Side-Channel Analysis and Secure Design COSADE'12, ser. LNCS, vol. 7275. Springer Verlag Berlin Heidelberg, 2012, pp. 167–182. https://doi.org/10.1007/978-3-642-29912-4_13.

[2] R. Brown, "Dieharder: A Random Number Test Suite," [online] Available from http://www.phy.duke.edu/rgb/General/dieharder.php, 2015.

[3] Y. Yang, S. Jia, Y. Wang, S. Zhang, C. Liu, "A Reliable True Random Number Generator Based on Novel Chaotic Ring Oscillator", *IEEE conference*, 978-1-4673-6853-7/17/$31.00 2017.

[4] NIST, "FIPS 140-1: Security Requirements for Cryptographic Modules," [online] Available from http://csrc.nist.gov/publications/fips/fips140- 1/fips1401.pdf, 1994.

[5] M. Baudet, D. Lubicz, J. Micolod, and A. Tassiaux, "On the security of oscillator-based random number generators," Journal of Cryptology, vol. 24, no. 2, pp. 398–425, 2011. https://doi.org/10.1007/s00145-010-9089-3.

[6] P. Kohlbrenner and K. Gaj, "An embedded true random number generator for FPGAs," in Proceedings of the 2004 ACM/SIGDA 12th international symposium on Field programmable gate arrays. ACM, 2004, pp. 71–78. https://doi.org/10.1145/968280.968292.

[7] B. Sunar, W. Martin, and D. Stinson, "A Provably Secure True Random Number Generator with Built-In Tolerance to Active Attacks," IEEE Transactions on Computers, pp. 109–119, 2007. https://doi.org/10.1109/TC.2007.250627.

[8] A. Cherkaoui, V. Fischer, A. Aubert, and L. Fesquet, "A self-timed ring based true random number generator," in IEEE International Symposium on Asynchronous Circuits and Systems (ASYNC 2013), 2013, pp. 99–106. https://doi.org/10.1109/ASYNC.2013.15.

[9] Xufan Wu and Shuguo Li; "A New Digital True Random Number Generator Based on Delay Chain Feedback Loop", IEEE conference 978-1-4673-6853-7/17/$31.00, 2017.

[10] A. Cherkaoui, V. Fischer, L. Fesquet, and A. Aubert, "A very high speed true random number generator with entropy assessment," in International Conference on Cryptographic Hardware and Embedded Systems. https://doi.org/10.1007/978-3-642-40349-1_11.

[11] Bassham, L.E. III, Rukhin, A.L., Soto, J., et al.: "SP 800-22 rev. 1a. A statistical test suite for random and pseudorandom number generators for cryptographic applications", National Institute of Standards and Technology (NIST), 2010.