International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 14
November 2017

Providing High Degree of Flexibility for FPGA Applications by Enhancing Beat Frequency Detection based TRNGs

Sravanthi Pinninti, Vijay Kumar J, Dr R. Hemalatha (Associate Professor, OU)

ABSTRACT— ***A True Random Number Generator (TRNG) is a piece of electronics that plugs into a computer & produces true random numbers. True random number generators (TRNGs) have become an indispensable component in many cryptographic systems, including PIN or password generation, authentication protocols, key generation, random padding, & nonce generation. We investigate the limitations of the beat frequency detection (BFD)-TRNG when implemented on an FPGA design platform. To overcome the limitations of Beat Frequency Detection based TRNG, we are focusing in this paper is to design improved field-programmable gate array (FPGA) based TRNGs, using purely digital components.***

1. INTRODUCTION

Almost each cryptographic system contains a Random Number Generator (RNG) that produces random values for underlying algorithms. Random numbers are essential elements for secure transactions & therefore they should meet the highest strict requirements – they should be unpredictable, uniformly distributed on their range & independent. RNGs can be divided into two main subgroups: Pseudo RNG (PRNG) & True RNG (TRNG). The output of a PRNG is mathematically defined & all of its entropy is given by the random seed. On the other hand, entropy of a TRNG is increased by each generated bit. The TRNG operation is usually based on certain physical sources of entropy (e.g. thermal noise, timing jitter) that is present in modern electronic devices.

The increasing want for true random numbers is due to the emergence of many utility fields where those numbers are vital (e.g. Quantum Cryptography). Random numbers are useful for a variety of functions, along with generating statistics encryption keys, simulating & modeling complicated phenomena & for deciding on random samples from larger statistics sets. In many programs, a supplementary constraint at the random quantity generator is to provide numbers at a fairly excessive charge.

Cryptographic applications require random numbers to operate. There are many random quantity generation schemes, & Random Number Generators (RNGs) are actively used as IT safety merchandise. The random numbers generated must be simply random; else they could appreciably weaken the safety machine. They must no longer be predictable. They have to be uniformly allotted on a given range & impartial of each different. Thus there's a need for an excellent RNG that satisfies all these constraints, despite the fact that its development involves extra mathematical analysis.

Space applications have to rent notably sophisticated protection factors. Random range turbines are employed in satellite systems both at the base station

as well as at the satellites. Highly secured encryption & decryption is hired in all of the communications with the satellite television for pc from the base station. The cryptographic secret is generated and, once it is used, the generated key have to be destroyed to make sure it isn't used any extra. Random variety turbines can be evolved using Field Programmable Gate Arrays (FPGAs). The ported designs at the FPGAs can be hired as a part of the space programs. There are numerous necessities that have to be considered while the tool is to be located in area. These are radiation outcomes, as well as the existence cycle of the device as a way to have a redundant system which improves the reliability of the complete tool.

True random numbers also find applications in gaming, playing & lottery drawings. To date, numerous TRNG designs had been proposed & implemented. Each layout makes use of a different mechanism to extract randomness from a few underlying physical phenomena that showcase uncertainty or unpredictability. Examples of resources of randomness encompass thermal & shot noise in circuits, secondary outcomes including clock jitter & meta stability in circuits, Brownian movement, atmospheric noise, nuclear decay, & random photon behavior. Because of its flexibility & rapid time to marketplace, FPGA has grown to be a famous platform for enforcing many cryptographic systems that encompass TRNGs as a crucial block. It is important to develop new FPGA TRNG answers due to the fact: (i) no longer all hardware TRNG techniques to be had for ASICs or different systems are amenable to FPGA implementation; (ii) the prevailing FPGA TRNGs have boundaries in phrases of the throughput-in line with-unit-region & will be progressed; & (iii) lively adversarial assaults as well as variations in operational conditions along with fluctuations in temperature & voltage deliver may bias & disturb the randomness of TRNGs output bit circulate. Since most of the state-of-the-art TRNGs perform in an open-loop fashion, it's miles vital to include a mechanism to constantly provide a feedback sign to adaptively adjust the TRNG system parameters to growth its output bit randomness.

A. Field-Programmable Gate Arrays (FPGA)

Field Programmable Gate Arrays (FPGAs) are semiconductor devices that are based around a matrix of configurable logic blocks (CLBs) connected via programmable interconnects. FPGAs can be reprogrammed to desired application or functionality requirements after manufacturing. This feature distinguishes FPGAs from Application Specific Integrated Circuits (ASICs), which are custom manufactured for specific design tasks. Although one-time programmable (OTP) FPGAs are available, the dominant types are SRAM based which can be reprogrammed as the design evolves.

FPGA Architecture:

The general FPGA architecture consists of three types of modules. They are I/O blocks or Pads, Switch Matrix/ Interconnection Wires & Configurable logic blocks (CLB). The basic FPGA architecture has two dimensional arrays of logic blocks with a means for a user to arrange the interconnection between the logic blocks.

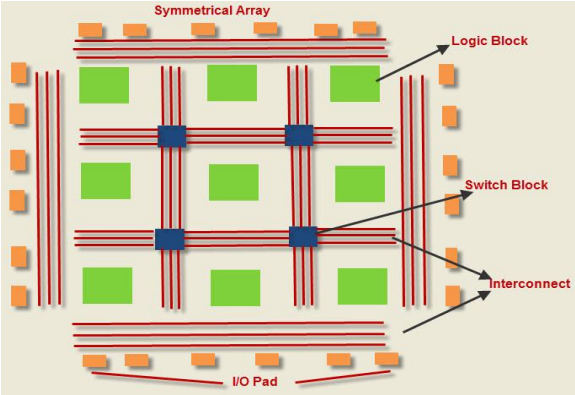

Fig1. FPGA Architecture

Applications of FPGA:

FPGAs have gained rapid growth over the past decade because they are useful for a wide range of applications. Specific application of an FPGA includes digital signal processing, bioinformatics, device controllers, software-defined radio, random logic, ASIC prototyping, medical imaging, computer hardware emulation, integrating multiple SPLDs, voice recognition, cryptography, filtering & communication encoding & many more. Usually, FPGAs are kept for particular vertical applications where the production volume is small. For these low-volume applications, the top companies pay in hardware costs per unit. Today, the new performance dynamics & cost have extended the range of viable applications.

2. RELATED WORK

Teng Xu & Miodrag Potkonjak have proposed a brand new form of digital PUF on an FPGA which leverages the conventional put off-based totally PUF & the DBF by means of deliberately choosing solid mission-response pairs from the delay-primarily based PUF & using them for DBF initialization. Their design inherited the security houses from both the delay primarily based PUF & the DBF concerning small energy, postpone, & region fees in addition to unclonability. Furthermore, the proposed FPGA-primarily based digital PUF enables complete removal of the usual PUF vulnerabilities, together with susceptibility to operational & environmental variations. They took benefit of the configurability of the FPGA & have proposed architecture for our layout. Their checks indicate that the proposed PUF is resilient to a huge spectrum of security assaults & its output circulate passes the NIST randomness check suite.

Hong Guo, Wenzhuo Tang, Yu Liu, & Wei Wei provided a simple technique to understand clearly random variety generation based totally on measurement of the segment noise of a single mode vertical cavity floor emitting laser (VCSEL). The authentic randomness of the quantum section noise originates from the spontaneous emission of photons & the random bit era rate is in the end confined handiest with the aid of the laser line width. With the very last bit era rate of 20 Mbit/s, the bodily assured simply random bit collection passes the 3 preferred random assessments. Moreover, for the primary time, a continuously generated random bit series up to 14 Gbit is tested with the aid of extra criteria for its true randomness.

Jiri Sobotík & Václav Plátěnka presented Statistical Tests Suite for Random & Pseudorandom Number Generators for Cryptographic Applications is a effective instrument for realistic verification of generators & algorithms in cryptography. It ought to

be implemented in the first steps of an assessment procedure of cryptographic primitives. It cannot absolutely substitute an in depth cryptanalysis, however if the generator or other primitives do not pass the take a look at suite then they're no longer appropriate for cryptographic software. It is possible & no longer so difficult to implement the take a look at suite in higher mathematically-orientated language. This gives upward thrust to the extra benefits of designated evaluation of sequences with other tests, operative manipulation of sequences, visualization of outcomes & interconnection with other packages.

3. FRAMEWORK

A. Beat Frequency Detection based TRNG (BFD-TRNG)

In the existing, we have BFD-TRNG circuit which is had drawback that is its statistical randomness is dependent on the design quality of the right oscillators. Any design bias in the ring oscillators might adversely affect the statistical randomness of the bitstream generated by the TRNG. Designs with the same number of inverters but different placements resulted in varying counter maximas.

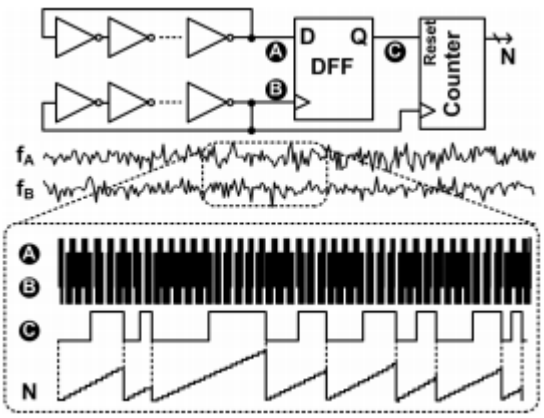

Fig2. Principle of BFD-TRNG

The faster signal A passes, catches up & overtakes the slower sign B repeatedly at periods decided with the aid of the frequency variations of the two ROSCs, particularly the beat frequency or Δf. This sample is recorded with the aid of a popular D-turn-flop in which the output of ROSC A is constantly sampled via that of ROSC B. The counter output (N in Fig. 2) increments each ROSC duration till it reaches the beat frequency interval & then the rely is sampled & reset. For higher example, allow's do not forget an instance in which the common frequency distinction between the ROSC pair is 1% & the maximum frequency distinction because of random jitter is 0.01%. Under this condition, the average counter output is 100 while the most & minimal counts are a hundred & one & ninety nine, respectively. In this situation, we can take the least large bit (LSB) of the output remember because the TRNG output. Now think the common frequency difference is reduced to 0.5% by means of adjusting the frequency difference, while the random jitter remains the identical at zero.01%. Then, the output rely will vary among 196 & 204, thereby offering up to 3 random bits (1st, second, & 3rd LSBs) in line with output matter & at the identical time growing the randomness of the decrease bits. By making the frequencies even closer using great grain trimming circuits, we ought to generate greater random bits from a bigger matter on the cost of an extended sampling time.

Additionally, the same ring-oscillator-based BFD-TRNG implemented on one of a kind FPGAs of the same family indicates awesome counter maxima. Unfortunately, since the ring oscillators are loose-

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 14
November 2017

walking, it is tough to control them to cast off any layout bias.

B. Proposed Tunable BFD-TRNG

To overcome this problem in this paper, we designed a tunable BFD-TRNG for FPGA-based applications.

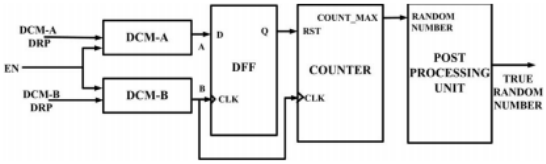

Fig3. Architecture of Proposed System

The proposed system is Digital Clock Manager (DCM)-based tunable BFD-TRNG. In the proposed layout, the supply of randomness is the jitter supplied inside the DCM circuitry. The DCM modules permit greater design manages over the clock waveforms, & their usage gets rid of the want for preliminary calibration. Tunability is established by using putting the DCM parameters on-the-fly using Dynamic Partial Reconfiguration (DPR) capabilities using DRP ports. This capability gives the design greater flexibility than the hoop-oscillator-based totally BFD-TRNG. The difference inside the frequencies of the two generated clock alerts is captured the usage of a D Flip-Flop (DFF). The DFF units when the faster oscillator completes one cycle more than the slower one (on the beat frequency interval). A counter is driven by way of one of the generated clock signals & is reset when the DFF is ready. Effectively, the counter will increase the throughput of the generated random numbers.

C. Tuning Circuit

Tuned circuit, any electrically conducting pathway containing each inductive & capacitive elements; if these factors are connected in collection, the circuit gives low impedance to alternating modern-day of the resonant frequency, which is decided via the values of the inductance & capacitance, & high impedance to current of different frequencies.

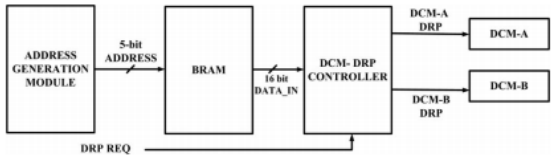

Fig4. Tuning Circuit Design

The target clock frequency is decided with the aid of the set of parameter values definitely decided on. The random values reached with the aid of the counter in addition to the jitter are related to the chosen parameters Multiplication element (M) & Division element (D). This makes it possible to track the proposed TRNG using the predetermined saved M & D values. As unrestricted DPR has been proven to be an ability chance to the circuit, the secure operational price combos of the D & M parameters for every DCM are predetermined throughout the layout time & saved on an on-chip block RAM (BRAM) reminiscence block inside the FPGA.

4. EXPERIMENTAL RESULTS

In this paper, we practical the DCM-DRP controller the use of the MicroBlaze soft processor without delay center at once instantiable in a Xilinx FPGA. Table I indicates the hardware aid requirement results of the proposed TRNG, except for the soft processor & the BRAM memory.

Design	Module Name	Slice	SliceReg	LUTs	BUFG	DCM_ADV	PLL_ADV
DCM-based TRNG	Oscillators	4	0	4	4	2	0
	DFF	1	1	0	0	0	0
	Counter	9	25	15	30	0	0
	Total	14	26	19	34	2	0
Ring Oscillator -based TRNG	Oscillators	23	0	90	0	0	0
	DFF	1	1	0	0	0	0
	Counter	9	25	15	30	0	0
	Sampler	0	0	0	1	0	1
	Total	33	26	15	31	0	1

‡ The hardware footprint excludes the *MicroBlaze* soft processor necessary for overall control and data acquisition from the TRNG, and 46 bytes of memory required in the BRAM module to store the 23 feasible (M, D) calculations.

This table additionally compares the hardware aid incurred in the design of ring-oscillator-based totally BFD-TRNG which configured with goal (nominal) term of 38.00 ns (89 inverters); the clock alerts produced by way of the DCMs are sets of values of the layout parameters M & D as in step with (1). DCM is greater controllable because there's manage over the two parameters M & D which is about through the designer; no such parameters exist for the RO-based conventional BFD-TRNG. A MicroBlaze processor is used in this design to acquire the generated random numbers returned to the computer.

The tunable units of DCM parameters & the resultant theoretical & experimental random numbers are proven in beneath table.

EXPERIMENTAL AND ESTIMATED RESULTS OF COUNTER VALUE DISTRIBUTION

SNo.	DCM-1					DCM-2					Counter		
	M	D	Output Freq. (MHz)	Period Jitter (unit interval) (ui)	Period Jitter (pk-to-pk) (ns)	M	D	Output Freq. (MHz)	Period Jitter (unit interval) (ui)	Period Jitter (pk-to-pk) (ns)	Estimated Max. Count	Experimental Mean	Relative Std. Dev. (%)
1	15	31	48.3871	0.029	0.600	14	29	48.2759	0.027	0.568	217	215	0.7883
2	21	22	95.4545	0.043	0.453	20	21	95.2381	0.042	0.436	220	218	1.1735
3	17	23	80.9534	0.035	0.436	21	26	80.7692	0.042	0.518	220	217	3.0310
4	30	37	74.0541	0.040	0.535	17	23	73.9130	0.035	0.469	229	224	6.3810
5	15	29	51.7241	0.029	0.568	16	31	51.6129	0.031	0.600	232	225	5.4321
6	17	25	68.0000	0.034	0.502	19	28	67.8571	0.032	0.551	237	236	1.2370
7	22	23	95.6522	0.045	0.469	21	22	95.9545	0.043	0.453	241	239	5.3184
8	19	29	65.5172	0.037	0.568	17	26	65.3846	0.034	0.518	246	241	5.9744
9	19	32	59.3750	0.037	0.617	16	27	59.2593	0.032	0.535	256	254	1.0531
10	22	31	70.9677	0.043	0.600	17	24	70.8333	0.034	0.486	268	263	0.4939
11	21	24	91.8333	0.047	0.486	22	23	95.6522	0.045	0.469	269	257	4.6929
12	19	25	76.0000	0.038	0.502	22	29	75.8621	0.043	0.568	275	271	1.0690
13	21	25	96.0000	0.048	0.502	23	24	95.8333	0.047	0.486	287	283	1.0977
14	21	32	65.6250	0.040	0.617	19	29	65.5172	0.037	0.568	304	302	0.9336
15	23	31	74.1936	0.045	0.060	20	27	74.0741	0.040	0.535	310	308	1.2926
16	25	26	96.1538	0.050	0.518	24	25	96.0000	0.048	0.502	312	300	5.3238
17	21	26	80.7692	0.042	0.518	25	31	80.6452	0.048	0.600	325	317	5.0382
18	26	27	96.2963	0.052	0.535	25	26	96.1538	0.050	0.518	337	333	1.8900
19	27	28	96.4286	0.053	0.551	26	27	96.2963	0.052	0.535	364	357	1.5485
20	28	29	96.5517	0.055	0.568	27	28	96.4286	0.053	0.551	391	388	1.7702
21	29	30	96.6667	0.056	0.584	28	29	96.5517	055	0.568	420	398	14.3583
22	30	31	96.7742	0.058	0.600	29	30	96.6667	0.056	0.584	449	446	3.8755
23	31	32	96.8750	0.060	0.6170	30	31	96.5542	0.058	0.600	480	468	3.6902

5. CONCLUSION

We conclude that in this paper we presented an enhanced fully digital tunable TRNG for FPGA-based applications, based on the theory of BFD & clock jitter, & with built-in error-correction potentials. The TRNG used this tunability feature for determining the degree of randomness, thus providing a high degree of flexibility for various applications.

REFERENCES

[1] Anju P. Johnson, Rajat Subhra Chakraborty & Debdeep Mukhopadyay, "An Improved DCM-Based Tunable True Random Number Generator for Xilinx FPGA", IEEE Transactions On Circuits & Systems—II: EXPRESS BRIEFS, VOL. 64, NO. 4, APRIL 2017

[2] Virtex-5 FPGA Configuration User Guide UG 191 (v3.11) Xilinx Inc., San Jose, CA, USA, Accessed: May 2016. [Online]. Available: www.xilinx.com/support/documentation/user_guides/ug191.pdf

[3] A. P. Johnson, R. S. Chakraborty, & D. Mukhopadhyay, "A PUF-enabled secure architecture for FPGA-based IoT applications," IEEE Trans. MultiScale Comput. Syst., vol. 1, no. 2, pp. 110–122, Apr.–Jun. 1, 2015.

[4] Q. Tang, B. Kim, Y. Lao, K. K. Parhi, & C. H. Kim, "True random number generator circuits based on single- & multi-phase beat frequency detection," in Proc. IEEE Custom Integr. Circuits Conf., Sep. 2014, pp. 1–4.

[5] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, & E. Barker, "A statistical test suite for random & pseudorandom number generators for cryptographic applications," Nat. Inst. Standards Technol. (NIST), Gaithersburg, MD, USA, DTIC Document, Tech. Rep., 2001.

[6] J. Von Neumann, "Various techniques used in connection with random digits," Nat. Bureau Standards Appl. Math. Ser., vol. 12, pp. 36–38, 1951.

[7] A. P. Johnson, S. Saha, R. S. Chakraborty, D. Mukhopadyay, & S. Gören, "Fault attack on AES via hardware Trojan insertion by dynamic partial reconfiguration of FPGA over Ethernet," in Proc. 9th WESS, Oct. 2014, pp. 1–8.

[8] P. Johnson, R. S. Chakraborty, & D. Mukhopadhyay, "A novel attack on a FPGA based true random number generator," in Proc. 10th WESS, Oct. 2015, pp. 1–6