An Improved DCM-based Tunable True Random Number Generator for Xilinx FPGA

RACHURI VENKATESH[1]

[1]M.Tech , Dept. Electronics and communication Engineering, Siddhartha Institute of Technology and Sciences(Approved by AICTE & Affiliated to JNTU, HYDERABAD) Telangana – 501 301, India

---***---

Abstract:- True Random Number Generators (TRNGs) assume a critical job in present day cryptographic frameworks. Field Programmable Gate Arrays (FPGAs) shape a perfect stage for equipment usage of huge numbers of these security calculations. In this paper we present an exceptionally effective and tunable TRNG dependent on the rule of Beat Frequency Detection (BFD), specifically for Xilinx FPGA based applications. The fundamental focal points of the proposed TRNG are its on-the-fly tunability through Dynamic Partial Reconfiguration (DPR) to enhance haphazardness characteristics. We depict the scientific model of the TRNG activities, and trial results for the circuit actualized on a Xilinx Virtex-V FPGA. The proposed TRNG has low equipment impression and in-fabricated inclination disposal capacities. The irregular bit streams produced from it breezes through all tests in the NIST factual test suite.

Keywords:- Digital Clock Manager, Dynamic Partial Reconfiguration, Field Programmable Gate Arrays, True Random Number Generator.

1. INTRODUCTION

Genuine Random Number Generators (TRNGs) have turned out to be vital part in numerous cryptographic frameworks, including PIN/secret word age, validation conventions, key age, arbitrary cushioning and nonce age. TRNG circuits use a non-deterministic arbitrary process, for the most part as electrical commotion, as an essential wellspring of arbitrariness. Alongside the commotion source, a clamor reaping instrument to remove the clamor, and a post-handling stage to give a uniform measurable appropriation are other critical parts of the TRNG. Our center is to outline an enhanced FPGA based TRNGs, utilizing absolutely advanced parts. Utilizing computerized fabricating hinders for TRNGs has the favorable position that the plans are moderately basic and appropriate to the FPGA configuration stream, as they can reasonably use the CAD programming devices accessible for FPGA outline. Notwithstanding, computerized circuits show nearly predetermined number of wellsprings of irregular clamor, e.g. metastability of circuit components, recurrence of free running oscillators and butterflies
(arbitrary stage shifts) in clock signals. As would be apparent, our proposed TRNG circuit uses the recurrence distinction of two oscillators and oscillator jitter as wellsprings of haphazardness.

Reconfigurable devices have become an integral part of many embedded digital systems, and predicted to become the platform of choice for general computing in near future. From being for the most part prototyping gadgets, reconfigurable frameworks including FPGAs are as a rule broadly utilized in cryptographic applications, as they can give satisfactory to high preparing rate at much lower cost and quicker plan process duration. Henceforth, many installed frameworks in the space of security require a top notch TRNG implementable on FPGA as a part. We present a TRNG for Xilinx FPGA based applications, which has tunable jitter control ability dependent on DPR capacities accessible on Xilinx FPGAs. The significant commitment of this paper is the advancement of an engineering which permits on– the– fly tunabilty of measurable characteristics of a TRNG by using DPR abilities of present day FPGAs for differing the DCM displaying parameters. To the best of our insight this is the principal revealed work which joins tenability in a TRNG. This methodology is relevant for Xilinx FPGAs which give programmable clock age component, and capacity of DPR.

DPR is a generally new improvement in FPGA innovation, whereby adjustments to predefined bits of the FPGA rationale texture is conceivable on– the– fly, without influencing the typical usefulness of the FPGA. Xilinx Clock Management Tiles (CMTs) contain Dynamic Reconfiguration Port (DRP) which enable DPR to be performed through significantly easier means [1]. Utilizing DPR, the clock frequencies produced can be changed on– the– fly by modifying the comparing DCM parameters. DPR by means of DRP is an additional preferred standpoint in FPGAs as it enables the client to tune the clock recurrence according to the need. Plan strategies exist to keep any pernicious controls by means of DPR which in different ways may adversely influence the security of the framework [2].

The goal of this paper is the design, analysis and implementation of an easy-to-design, improved, low-overhead, tunable TRNG for the FPGA platform. The following are our major contributions:

We examine the impediments of the BFD– TRNG [3] when executed on a FPGA outline stage. To settle the inadequacies, we propose an enhanced BFD– TRNG design reasonable for FPGA based applications. To the best of our insight this is the main revealed work which fuses tunability in a completely advanced TRNG. We dissect the changed proposed design mathematically and tentatively.

The rest of the paper is organized as follows: Section II discusses the preliminaries, followed by the proposed TRNG design in Section III. The mathematical model of the proposed design is discussed in Section IV. Section V describes the implementation and experimental results. We conclude in Section VI.

2. BACKGROUND AND MOTIVATION

This section briefly describes the basic BFD–TRNG model and the DPR methodology utilizing DRP ports available in Xilinx CMTs.

A. Single Phase BFD-TRNG Model

The BFD-TRNG circuit [3] is a fully-digital TRNG, which relies on jitter extraction by the Beat Frequency Detection (BFD) mechanism, originally implemented as a 65-nm CMOS ASIC. The structure and working of the (single phase) BFD-TRNG can be summarized as follows, in conjunction with Fig. 1:

1) The circuit comprises of two semi indistinguishable ring oscillators (let us term them as ROSCA and ROSCB), with comparative development and position. Because of innate physical irregularity starting from process variety impacts related with profound sub-micron CMOS fabricating, one of the oscillators (say, ROSCA) sways marginally quicker than the other oscillator (ROSCB). What's more, the creators [3] proposed to utilize trimming capacitors to additionally tune the oscillator yield frequencies.

2) The output of one of the ROs is used to sample the output of the other, using a D flip-flop (DFF). Without loss of generality, assume the output of ROSCA is fed to the D-input of the DFF, while the output of ROSCB is connected to the clock input of the DFF.

3) At certain time interims (controlled by the recurrence distinction of the two ROCs), the quicker oscillator flag passes, gets up to speed, and overwhelms the slower motion in stage. Because of irregular jitter, these catching occasions occur indiscriminately interims, called "Beat Frequency Intervals". Subsequently, the DFF yields a rationale 1 at various arbitrary examples.

4) A counter controlled by the DFF increments during the beat frequency intervals, and gets reset due to the logic-1 output of the DFF. Due to the random jitter, the free-running counter output ramps up to different peak values in each of the count-up intervals before getting reset.

5) The output of the counter is sampled by a sampling clock before it reaches its maximum value.

6) The sampled response is then serialized to obtain the random bit stream.

B. Shortcoming of the BFD-TRNG

One shortcoming of the previous BFD-TRNG circuit is that its statistical randomness is dependent on the design quality of the ring oscillators. Any design bias in the ring oscillators might adversely affect the statistical randomness of the bit-stream generated by the TRNG. Designs with same number of inverters but different placements resulted in varying counter maximas. Additionally the same ring-oscillator based BFD-TRNG implemented on different FPGAs of the same family shows distinct counter maxima

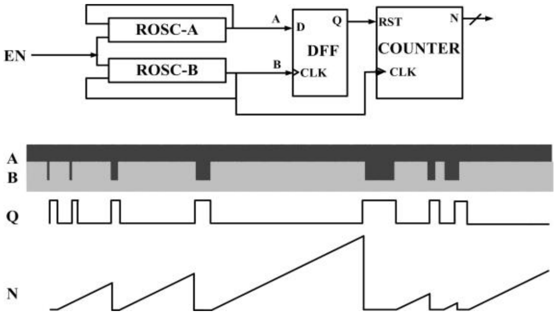


Fig. 1: Architecture of single phase BFD–TRNG [3].

Unfortunately, since the ring oscillators are free-running, it is difficult to control them to eliminate any design bias. The problem is exacerbated in FPGAs where it is often difficult to control design bias because of the lack of fine-grained designer control on routing in the FPGA design fabric. A relatively simple way of tuning clock generator hardware primitives on Xilinx FPGAs, particularly the Phase Locked Loop (P LL) or the Digital Clock Manager (DCM) as used in this work, is by enabling dynamic reconfiguration via the Dynamic Reconfiguration Ports (DRPs). Once enabled, the clock generators can be tuned to generate clock signals of different frequencies by modifying values at the DRPs [1] on–the–fly, without needing to bring the device off– line.

We next describe the proposed tunable BFD-TRNG suitable for FPGA platforms.

3. TUNABLE BFD–TRNG FOR FPGA BASED APPLICATIONS

A. Design Overview

Fig. 2 demonstrates the general design of the proposed TRNG. Instead of two ring oscillators, two DCM modules create the swaying waveforms. The DCM natives are parameterized to produce somewhat extraordinary frequencies, by changing two plan parameters M (Multiplication Factor) and D (Division Factor). In the proposed plan, the wellspring of irregularity is the jitter displayed in the DCM hardware. The DCM modules permit more noteworthy architect power over the clock waveforms, and their use disposes of the requirement for introductory adjustment [3]. Tun-capacity is built up by setting the DCM parameters on– the– fly utilizing DPR abilities utilizing DRP ports. This ability gives the plan more noteworthy adaptability than the ring oscillator based BFD-TRNG. The distinction in the frequencies of the two produced clock signals is caught utilizing a DFF. The DFF sets when the quicker oscillator finishes one cycle more than the slower one (at the beat recurrence interim). A counter is driven by one of the produced clock flags, and is reset when the DFF is set. Adequately, the counter expands the throughput of the created arbitrary numbers. The last three LSBs of the greatest check esteems come to by the tally were found to demonstrate great arbitrariness properties

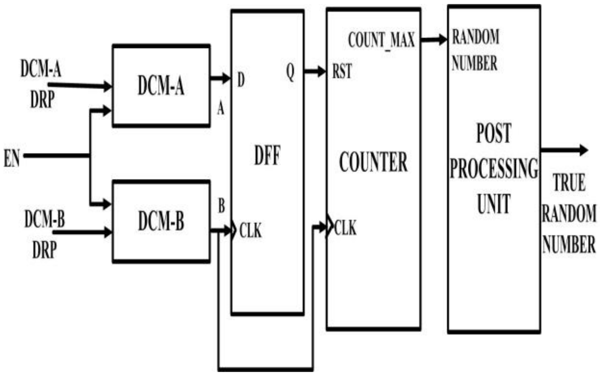


Fig. 2: Overall architecture of proposed Digital Clock Manager based tunable BFD–TRNG.

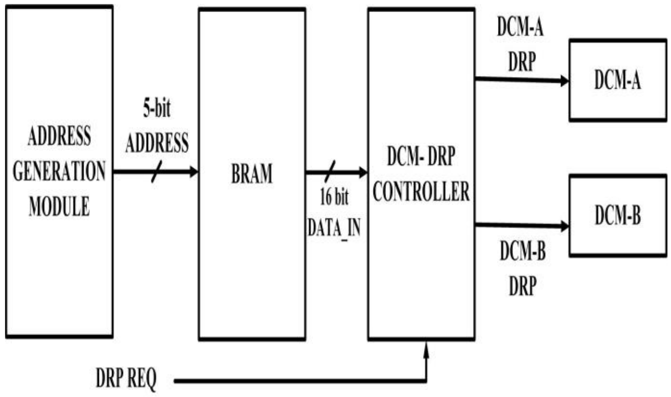


Fig. 3: Architecture of tuning circuit.

Additionally, we have a simple post-processing unit using a Von Neumann Corrector (VNC) [5] to eliminate any biasing in the generated random bits. VNC is a well-known low-overhead scheme to eliminate bias from a random bit stream. In this scheme, any input bit "00" or "11" pattern is eliminated; otherwise, if the input bit pattern is "01" or "10", only the first bit is retained. The last three LSBs of the generated random number is passed through the VNC. The VNC improves the statistical qualities at the cost of slight decrease in throughput.

B. Tuning Circuitry

The design of the tuning hardware is appeared in Fig. 3. The objective clock recurrence is dictated by the arrangement of dad rameter values really chose. The arbitrary qualities come to by the counter, and the jitter are identified with the picked parameters M and D (points of interest are examined in Section IV). This makes it conceivable to tune the proposed TRNG utilizing the foreordained put away M and D esteems. As unlimited DPR has been appeared to be a potential risk to the circuit [6], the safe operational esteem mixes of the D and M parameters for each DCM are foreordained amid the plan time, and put away on an on-chip Block RAM (BRAM) memory obstruct in the FPGA.

There are really two distinct choices for the clock generators – one can utilize the Phase Locked Loop (PLL) hard macros accessible on Xilinx FPGAs, or the DCMs. We next portray expository and exploratory outcomes which constrained us to pick DCM for the PLL modules for clock waveform age.

4. MATHEMATICAL MODEL OF PROPOSED TRNG

A. Circuit Behavior with PLL as Clock Generator

We first consider the operational principle for the PLL, and its feasibility as a component of the proposed TRNG. The Xilinx PLL synthesizes a clock signal whose frequency is given by:

$$ {}^{F}CLKF\ X = {}^{F}CLKIN \quad \frac{M}{D} \quad (1) $$

Where FCLKIN is the frequency of input clock signal, and M and D are the multiplication and division factors previously mentioned. Values of M and D can be varied to generate the required clock frequency. The two PLLs can be parameterized with the necessary set of (M; D) values to generate two slightly different clock frequencies. Without loss of generality, assume P LLA is set up to be slightly faster than P LLB, i.e. the time periods are related by TA < TB. On reaching the beat frequency interval (say, n clock cycles), by definition, P LLA completes one cycle more than the slower one. The following equation depicts this simple model:

$$ \frac{{}^{T}A}{} = \frac{N}{} \quad (2) $$

$$T_B \qquad N + 1$$

N = 2:n, where n is the estimated maximum counter value. For the first n clock cycles, the counter does not increment, and then increments by one for each of the next n clock cycles. Hence, the maximum counter values reached is n. Then, Eqn. (2) leads to:

$$n = \; 2(T_B \quad T_A) \qquad\qquad (3)$$
$$\underline{T_B \qquad}$$

Utilizing outline arrangement parameters (M and D) one of the oscillators is made to run quicker than the other. This is done with the end goal to confine the scope of counter qualities delivered. In the event that both the oscillators were designed to keep running at a similar recurrence we may get arbitrary numbers, however the most extreme counter esteem created will be high (hypothetically unbounded) according to Eqn. (3). As it were, the idleness of the circuit will be high, since the counter sets and resets simply in the wake of achieving a huge check esteem. At the point when the Xilinx PLLs are utilized as clock generators, the anticipated and watched counter qualities for all blends of (M; D) values continue as before. This affirms the Xilinx PLL cases show near perfect conduct and are semi indistinguishable, and have irrelevant jitter between the waveforms produced by them. Since the BFD-TRNG is basically subject to the nearness of jitter between the two created clock waveforms, PLLs appear to be inadmissible as segments of the proposed TRNG. Subsequently, next we analyze the DCM as clock generators.

B. Circuit Behavior with DCM as Clock Generator

Without loss of generality, the clock signals produced by one of the DCM (say, DCMA) is slightly faster than the other (DCMB), implying TA < TB. This is ensured by assigning the design parameters M and D as in Eqn. (7). More details are discussed in Section IV-C. Timing diagrams of the DCM clock outputs and the resultant DFF response is shown in Fig. 4. Let N be the number of clock cycles of the slower clock signal in which the faster clock signal completes exactly one cycle more. Then,

$$t_A[N + 1] = (N + 1)T_A + {}_A \qquad\qquad (4)$$

and

$$t_B[N] = N\,T_B + {}_B \qquad\qquad (5)$$

Where A and B are the uncertainties due to jitter in DCMA and DCMB respectively. The uncertainties due to jitter in

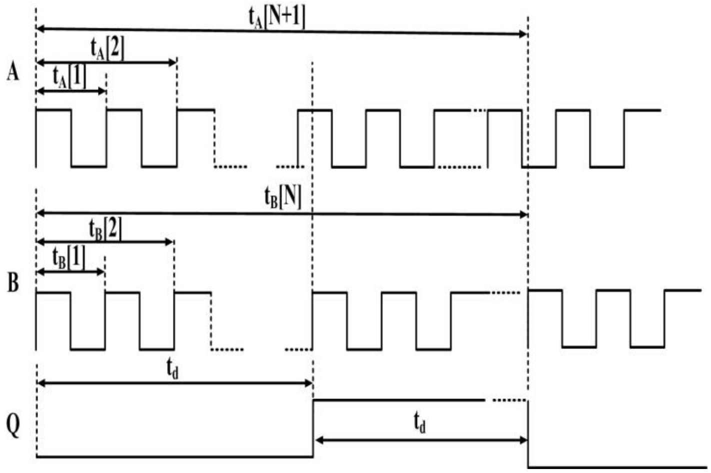
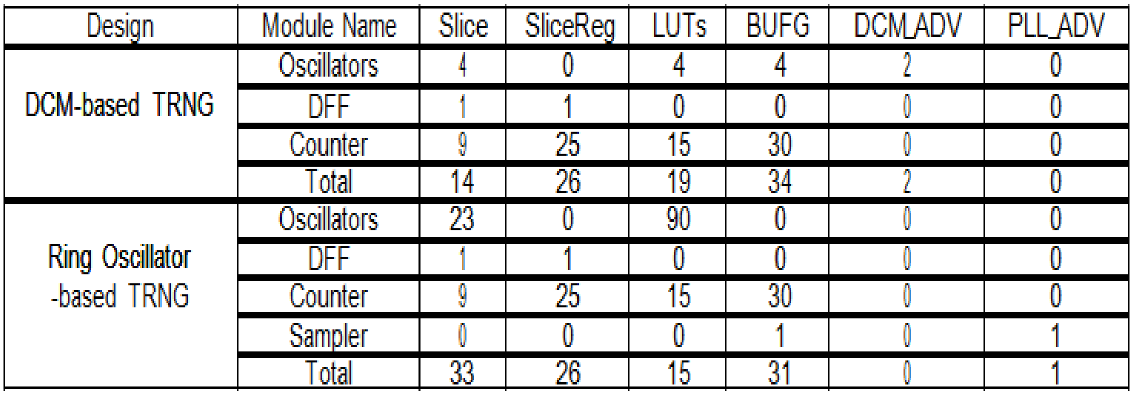


Fig. 4: Timing diagram of DCM output waveforms and the corresponding and DFF response.

TABLE I: Hardware Footprint of the Proposed TRNG^z and the Ring Oscillator based TRNG^Z

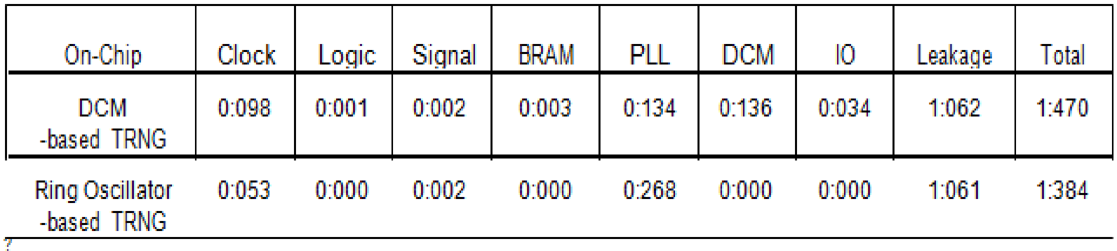


Design	Module Name	Slice	SliceReg	LUTs	BUFG	DCM_ADV	PLL_ADV
DCM-based TRNG	Oscillators	4	0	4	4	2	0
	DFF	1	1	0	0	0	0
	Counter	9	25	15	30	0	0
	Total	14	26	19	34	2	0
Ring Oscillator -based TRNG	Oscillators	23	0	90	0	0	0
	DFF	1	1	0	0	0	0
	Counter	9	25	15	30	0	0
	Sampler	0	0	0	1	0	1
	Total	33	26	15	31	0	1

z

The hardware footprint excludes the Micro Blaze 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.

TABLE II: On-Chip Power Dissipation$^?$ of the Proposed TRNG and the Ring Oscillator based TRNG^z



On-Chip	Clock	Logic	Signal	BRAM	PLL	DCM	IO	Leakage	Total
DCM -based TRNG	0:098	0:001	0:002	0:003	0:134	0:136	0:034	1:062	1:470
Ring Oscillator -based TRNG	0:053	0:000	0:002	0:000	0:268	0:000	0:000	1:061	1:384

?

Power dissipation in watt.

Sampling clock frequency is 103:1992 kHz.

DCMA and DCMB are different, this is because the DCMs are designed with distinct modeling parameters M and D. The corresponding jitter for each of the DCMs used in the proposed design is presented in Table III. For example, consider the configuration presented in Sl.No. 1. In this case, DCMA is configured with M=15 and D=31 and DCMB is configured with M=14 and D=29. This results in peak-to-peak jitter of 0:600 ns and 0:568 ns for DCMA and DCMB respectively. Of course, we also have: tA[N + 1] = tB[N]. Assuming there is no metastability for the DFF if signal transitions occur in the setup-hold timing window around its driving clock edge (the metastability issue can be avoided by cascaded DFF combination), the transition time (td) of the DFF, the time interval after which it sets (i.e. the counter driven by the DFF resets), is estimated by:

$$td = \frac{t_A[N+1] + t_B[N]}{2} = \frac{(N+1)T_A + N\,T_B + A + B}{2} \qquad (6)$$

From Eqn. (6), the transition time of DFF is a random process.

The output of the DFF, i.e. the time interval (t_d) after which the counter resets, is thus a random function. As a result, the count value obtained when the counter resets is also a rando quantity. The counter resets automatically when the DFF sets, and the operation continues. The DFF resets approximately n cycles after it sets, and the counter starts counting again.

C. Tuning Parameter Value Ranges

Eqns.(1)–(2) also holds true for DCM based beat frequency detection also. Hence, we have the following relationships:

$$\frac{D_1 \quad M_2}{D_2 \quad M_1} = \frac{N}{N+1} \qquad 81 \; D_i \; 32; \quad >2 \; M_i \; 33; \qquad (7)$$

Where, M and D esteems are according to the Xilinx DCM specification [1]. The tally an incentive to be examined was set to be somewhere in the range of 200 and 500, subsequently the estimations of N are according to Eqn. (7). Higher estimation of check isn't wanted, as it prompts higher power dissemination. According to Eqn. (7), there are 23 sets of (M; D) esteem mixes for the two DCMs, which fulfill the required tally go. These qualities are put away in a BRAM, and for 23 particular sets we require 5 bit address line for choosing one of the mixes of M and D esteems, and if the BRAM is con-figured to hold 16-bit words, we require 46 bytes of memory. The deliver additions to the required BRAM area where the comparing estimations of the DCMB is put away on interest, utilizing a basic location age module. Along these lines, utilizing a confined DPR technique, the originator has authority over the DCM arrangement to pick the best blend creating arbitrary numbers with the best factual quality. With the end goal to keep away from vindictive changes through DPR, we have empowered DPR prohibitively by putting away the reasonable displaying parameters. With the end goal to actualize this protected tunable plan marginally higher equipment overhead and power dissemination is required. The DCM-DRP controller starts DPR in DCMA and DCMB utilizing standard Xilinx plan strategy [1].

5. EXPERIMENTAL RESULTS

The proposed circuit was outlined utilizing Verilog HDL, and executed utilizing Xilinx ISE (v 14.5) CAD programming stage focusing on the Xilinx Virtex-V FPGA stage. The DCM-DRP controller was executed utilizing the Micro Blaze delicate processor specifically center straightforwardly instantiable in a Xilinx FPGA. Table-I demonstrates the equipment asset prerequisites aftereffects of the proposed TRNG, barring the delicate processor and the BRAM memory. This table likewise analyzes the equipment asset caused in the plan of ring oscillator-based BFD-TRNG which arranged with target (ostensible) day and age of 38:00 ns (89 inverters). The clock signals created by the DCMs are sets of estimations of the plan parameters M and D according to Eq.(1). DCM is more controllable in light of the fact that there is authority over the two parameters M and D which is set by the architect, no such parameters exist for the RO based conventional BFD-TRNG. Also, it was seen that equivalent hard full scale constructed traditional BFD-TRNG actualized in light of various FPGAs demonstrate distinctive counter maximas. In ASIC-based plans, trimming capacitors are utilized to change the frequencies of the clock generator hardware; notwithstanding, it is hard to have such a component on FPGA executions. Because of the procedure variety impacts, a recurrence distinction of 0:1959%

TABLE III: Experimental and Estimated Results of Counter Value Distribution

Sl.No.	DCM-1					DCM-2					Counter		
	M	D	Output Freq. (MHz)	Period Jitter (unit interval) (ns)	Period Jitter (pk-to-pk) (ns)	M	D	Output Freq. (MHz)	Period Jitter (unit interval) (ns)	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	0:7683
2	21	22	95:4545	0:043	0:453	20	21	95:2381	0:042	0:436	220	218	1:1735
3	17	21	80:9534	0:035	0:436	21	26	80:7692	0:042	0:518	220	217	3:0310
4	20	27	74:0741	0:040	0:535	17	23	73:9130	0:035	0:469	229	224	6:3010

5	15	29	51:7241	0:029	0:568	16	31	51:6129	0:031	0:600	232	225	5:4424
6	17	25	68:0000	0:034	0:502	19	28	67:8571	0:037	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	3:3484
8	19	29	65:5172	0:037	0:568	17	26	65:3846	0:034	0:518	246	241	5:0744
9	19	32	59:3750	0:037	0:617	16	27	59:2593	0:032	0:535	256	254	1:0534
10	22	31	70:9677	0:043	0:600	17	24	70:8333	0:034	0:486	268	263	0:8939
11	23	24	95:8333	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	24	25	96:0000	0:048	0:502	23	24	95:8333	0:047	0:486	287	283	1:9877
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	1:2826
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	1:8000
19	27	28	96:4286	0:053	0:551	26	27	96:2963	0:052	0:535	364	387	1:5485
20	28	29	96:5517	0:055	0:568	27	28	96:4286	0:053	0:551	391	388	1:7102
21	29	30	96:6667	0:056	0:584	28	29	96:5517	:055	0:568	420	398	14:3593
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

was seen between the two ring oscillators. Also, equipment asset and power utilization fluctuates with contrast end clock recurrence of the ring oscillator. Likewise, this plan is helpless against Hardware Trojan Horse (HTH) inclusions forced on examining tickers [7]. Table-II demonstrates the power investigation report of the proposed TRNG and the Ring Oscillator based BFD-TRNG, the proposed configuration has around 6% control overhead contrasted with BFD-TRNG. Expecting a normal TRNG tally of 271 (relating to memory area 12), counter working at 75.8621 MHz (comparing to DCMB), half bits dismissed by the Von Neumann Corrector, and 3 bits for every arbitrary number held, the Power-defer Product (PDP) of the proposed TRNG is 3.50 mJ per kilobit.

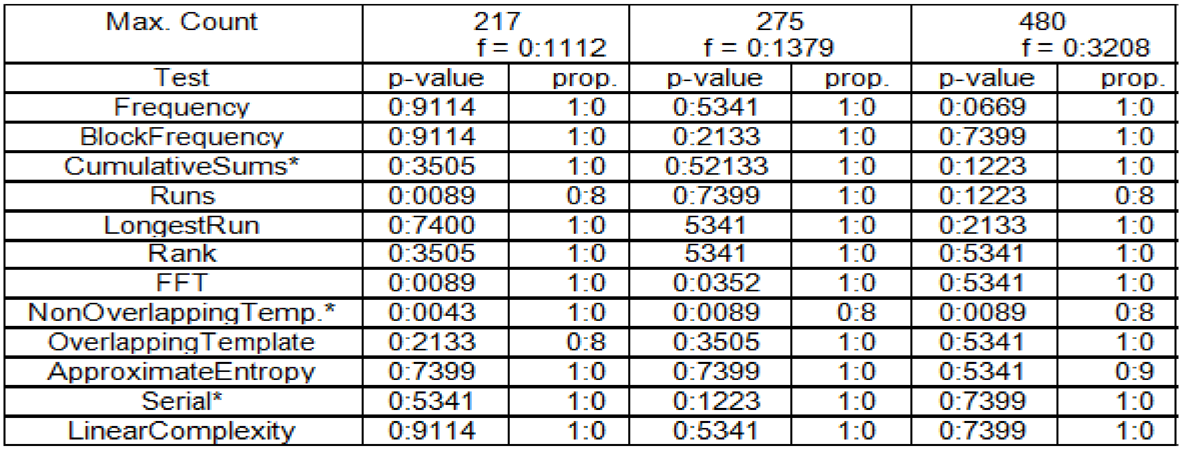
The tunable arrangements of DCM parameters, and the resultant hypothetical and exploratory irregular numbers are appeared in Table-III. To comprehend the outcomes, consider the arrangement introduced in Sl.No. (1) In the table. For this situation, DCMA is designed with M = 15 and D = 31, and DCMB is arranged with M = 14 and D = 29. This outcomes in top to-top jitter of 0:600 ns and 0:568 ns for DCMA and DCMB individually. The subsequent clock frequencies blended are 48:3871 MHz and 48:2759 MHz separately. The assessed counter qualities according to Eqn. (3) is 217, and the relating mean of the counter esteem conveyance acquired tentatively is 215. Thus, there is a relative deviation of 0:7683.

The factual execution of the outline is appeared in Table-IV. This table introduces the p-qualities and extents corresponding for the individual NIST tests on the produced ran-dom numbers with mean 217, 275 and 480 individually (corresponding to results for three separate cases: (Sl. No. 1,12, and 23 considered in Table III). From the outcomes, it is clear that the proposed TRNG shows fantastic irregularity properties at low equipment impression and low power dispersal.

6. CONCLUSION

We have displayed an enhanced completely advanced tunable TRNG for FPGA based applications, in view of the rule of Beat Frequency Detection and clock jitter, and with in-manufactured mistake adjustment abilities. The TRNG uses this tunability feature for deciding the level of haphazardness, subsequently giving a high degree of flexibility for various applications. The proposed design successfully passes all NIST statistical tests

TABLE IV: NIST Statistical Test Results^{z}



Max. Count	217 f = 0:1112		275 f = 0:1379		480 f = 0:3208	
Test	p-value	prop.	p-value	prop.	p-value	prop.
Frequency	0:9114	1:0	0:5341	1:0	0:0669	1:0
BlockFrequency	0:9114	1:0	0:2133	1:0	0:7399	1:0
CumulativeSums*	0:3505	1:0	0:52133	1:0	0:1223	1:0
Runs	0:0089	0:8	0:7399	1:0	0:1223	0:8
LongestRun	0:7400	1:0	5341	1:0	0:2133	1:0
Rank	0:3505	1:0	5341	1:0	0:5341	1:0
FFT	0:0089	1:0	0:0352	1:0	0:5341	1:0
NonOverlappingTemp.*	0:0043	1:0	0:0089	0:8	0:0089	0:8
OverlappingTemplate	0:2133	0:8	0:3505	1:0	0:5341	1:0
ApproximateEntropy	0:7399	1:0	0:7399	1:0	0:5341	0:9
Serial*	0:5341	1:0	0:1223	1:0	0:7399	1:0
LinearComplexity	0:9114	1:0	0:5341	1:0	0:7399	1:0

For tests with more than one subtest, the p-value and proportion shown are the smaller values.

REFERENCES

[1] Xilinx, Inc., “Virtex-5 FPGA Configuration User Guide UG 191 (v3.11)”, [Online]. Available: www.xilinx.com/support/documentation/ user guides/ug191.pdf, Accessed: May 2016.

[2] A. P. Johnson, R. S. Chakraborty and D. Mukhopadhyay, “A PUF-Enabled Secure Architecture for FPGA-Based IoT Applications,” in IEEE Transactions on Multi-Scale Computing Systems, vol. 1, no. 2, pp. 110-122, April-June 1 2015.

[3] Q. Tang, B. Kim, Y. Lao, K. K. Parhi and C. H. Kim, “True Random Number Generator circuits based on single- and multi-phase beat fre-quency detection,” Proceedings of the IEEE 2014 Custom Integrated Circuits Conference, pp. 1-4, September 2014.

[4] A. Rukhin, J. Soto, J. Nechvatal, M. Smid and E. Barker, “A Statistical Test Suite for Random and Pseudorandom

[5] Number Generators for Cryptographic Applications”, DTIC Document, Tech. Rep., 2001.

[6] J. Von Neumann, “Various Techniques used in Connection with Random Digits.”, National Bureau of Standards Applied Mathematics Series, vol. 12, pp. 36-38, 1951.

[7] A. P. Johnson, S. Saha, R. S. Chakraborty, D. Mukhopadyay and Sezer Goren¨ ,“Fault Attack on AES via Hardware Trojan Insertion by Dynamic Partial Reconfiguration of FPGA over Ethernet”, 9th Workshop on Embedded Systems Security (WESS 2014), October 2014.

[8] A. P. Johnson, R. S. Chakraborty and D. Mukhopadhyay, “A Novel Attack on a FPGA based True Random Number Generator”, 10th Workshop on Embedded Systems Security (WESS 2015), October 2015.