A HIGH SPEED TRUE RANDOM NUMBER GENERATOR WITH NOVEL ALGORITHM OF DIGITAL CLOCK MANAGER

[1]A. Naga Jyothi, [2]Dr. P. Krishna Murthy

[1]M.Tech Student, [2]Associate Professor & Head
[1, 2]Department of ECE,
[1,2] Chadalawada Ramanamma Engineering College, Tirupati, A.P. India.

Abstract: The Random number (bit) generators are vital to protected communications, data transmit and storage space and electronic communication to bring out stochastic replications and a lot of other applications. Our theory has be that random numbers cannot be compute; since computers activate in deterministic approach, they cannot construct random numbers. As an alternative, random numbers are finest obtain using physical (True) Random Number Generators (TRNG), which function by measure a well-controlled and particularly equipped physical progression. Randomness of a TRNG be able to be accurately, scientifically characterize and calculated. True Random Numbers correspond to a understanding investigate area intended for cryptographic algorithms and application They are frequently worn in generate non-reproducible and non-deterministic pattern use in unusual cryptographic protocol, present some novel practical approach on True Random Number Generation by using DCM blocks of a Xilinx FPGA. Moreover, It describes the whole generation process, comparison of proposed method with previous methods shown in the thesis where the proposed method have better speed or delay over conventional design. The total design were done and implemented in Xilinx ISE 14.7 with HDL coding.

***IndexTerms* - True Random Number Generators (TRNG), FPGA, Digital Clock Manager (DCM), Edge Detection.**

I. INTRODUCTION

Random Number Generation (RNG) is a process all the way through a device, generates a series of numbers or symbols that cannot be sensibly predict well than by a random possibility. Random number generators can be true hardware random number generators (HRNGS), which generate random numbers as a purpose of current value of some physical surroundings attribute that is constantly changing in a manner that is practically impossible to model, or pseudorandom number generator (PRNGS), which generate numbers that look random, but are actually deterministic, and can be reproduced if the state of the PRNG is known. A variety of applications of randomness have led to the growth of several different methods for generate random data, of which some have existed since ancient times, among whose ranks are famous "classic" example together with the rolling of dice, coin flip, the shuffle of playing cards, the use of yarrow stalks (for divination) in the I Ching, as well as countless other techniques. Due to the mechanical nature of this technique, generating large quantities of suitably random numbers (important in statistics) required much work and time. Thus, outcome would from time to time be collected and distributed as random number tables.

In cryptographic systems, a true random number generator (TRNG) is an vital component used in key production and confirmation protocols. It extracts physical uncertainty as unpredictable random numbers. Since it is preferred that the amount of additional hardware for a TRNG is as small as possible, many TRNGs that utilize existing hardware elements have been proposed. For example, in FPGA systems, metastability of latches or flip-flops can be used as a source of entropy. Uncertainty in an external chip, such as the read noise of NAND flash, is also utilized to produce random numbers.

Block Diagram and Timing Diagram of DCM based TRNG

For Xilinx FPGAs, Johnson et al proposed a TRNG using two DCM (Digital Clock Manager) blocks. Its operating principle is called Beat Frequency Detection (BFD). There, two DCMs generate clock signals that have slightly different clock frequencies. They are connected to the data and clock inputs of a D flip-flop (DFF). The output of the DFF becomes a repetition of consecutive logic-zeros and logic-ones. Since the least significant bits (LSBs) of the number of consecutive logic-ones have randomness because of jitter and metastability, they are collected as a source of entropy. An improvement of this DCM-based TRNG is to facilitate the number of required logic elements is small.

Although two additional DCMs are required, there are very few applications that use up all of the DCMs on an FPGA. Also, since a pair of frequencies can be dynamically reconfigured, the TRNG can be tuned by looking for a pair that shows good randomness. However, the previous work did not show the systematic information to find a good frequency pair, which prevents this type of TRNG from practical applications.

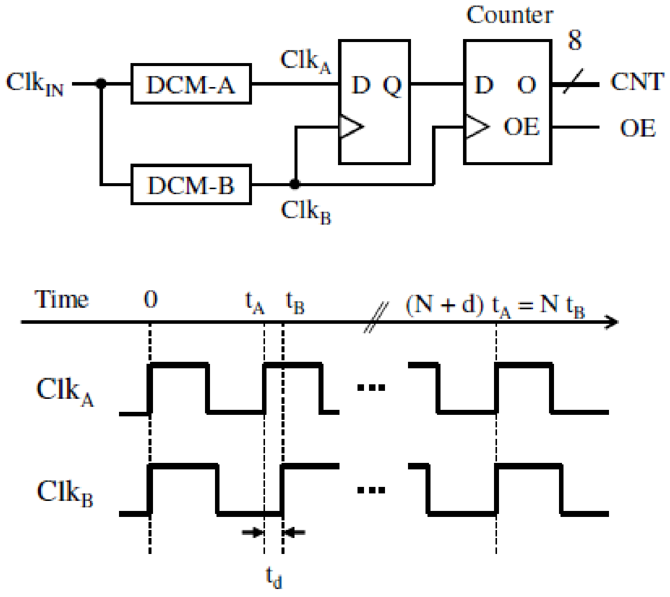


Figure 1: Block diagram and Timing Diagram of the DCM-based TRNG

This thesis represents a quick way to find a good frequency pair for the DCM-based TRNG. To this end, we evaluate a DCM-based TRNG with 100 pairs of frequencies. The previous work presented 23 pairs and the results of statistical tests were shown only for three pairs of them. This thesis quantitatively shows the effect of selection of a pair of frequencies on the quality of random numbers and the generation rate of the TRNG by passing random bit strings for all the pairs to the diehard statistical tests. This gives designers a guideline on which pair of frequencies should be tried at first.

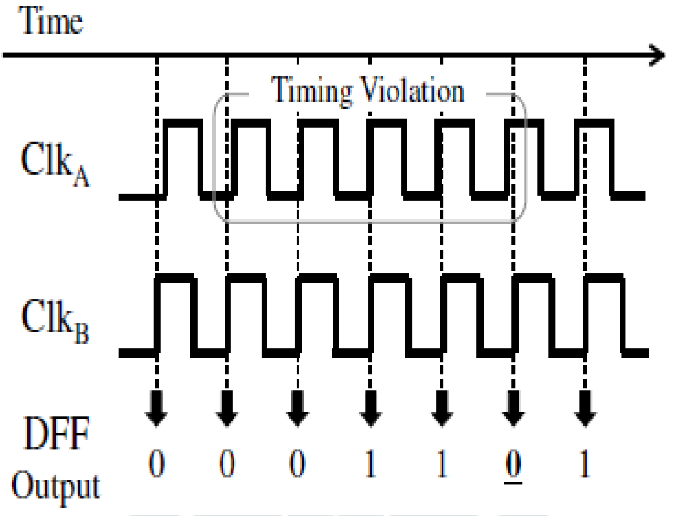


Figure 2: Effect of Timing Violation in the DCM-Based TRNG.

In this propose method, to make a finer trade-off between the quality of random numbers and the generation rate, using the fact that the distribution of the number of consecutive logic-ones in the DFF exhibits biphasic histograms. Through the evaluation, The proposed method can greatly increase the number of pairs that give good random numbers with a small penalty on the generation rate.

II. Literature Review

A.P. Johnson, R. S. Chakraborty, and D. Mukhopadyay, "An Improved DCM-Based Tunable True Random Number Generator for Xilinx FPGA," IEEE Transaction on Circuits and Systems II: Express Briefs, vol. 64, no. 4, pp. 452–456, 2017.

True Random Number Generators (TRNGs) play a extremely significant role in up to date cryptographic system. Field Programmable Gate Arrays (FPGAs) appearance an perfect stage for hardware executions of a lot of these safety algorithms. In this thesis, a highly efficient and tunable TRNG based on the principle of Beat Frequency Detection (BFD), specifically for Xilinx FPGA based applications are presented. The major advantages of the proposed TRNG are its on-the-fly tunability from side to side Dynamic Partial Reconfiguration (DPR) to improve randomness character. The mathematical model of the TRNG operations, and experimental results for the circuit implemented on a Xilinx Virtex-V FPGA are described. The proposed TRNG has low hardware footprint and in-built bias elimination capabilities. The random bit streams generated from it passes all tests in the NIST statistical test suite.

True Random Number Generators (TRNGs) have become indispensable component in many cryptographic systems, including PIN/password generation, authentication protocols, key generation, random padding and nonce generation. TRNG circuits utilize a non-deterministic random process, usually in the form of electrical noise, as a basic source of randomness. Along with the noise source, a noise harvesting mechanism to extract the noise, and a post-processing stage to provide a uniform statistical distribution are other important components of the TRNG. Our focus is to design an improved FPGA based TRNGs, using purely digital components.

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 frequency detection," in Proc. IEEE 2014 Custom Integrated Circuits Conference, 2014, pp. 1–4.

A novel technique for true random number generation using commercial off-the-shelf Flash memory. Flash memory cells are known to exhibit thermal noise and random telegraph noise during sensing of their threshold voltage. In order to extract this inherent noise properties of the Flash memory bits through a standard digital Flash memory interface, utilize the program disturb and read noise characteristics, which are fundamental properties of all NAND Flash memory arrays. The proposed technique is experimentally demonstrated and evaluated using state-of-art Flash memory chips. The experimental evaluation shows that the proposed technique enables extraction of high quality, high throughput, controllable (or tunable), and temperature- and aging-tolerant random bits.

Random numbers are the cornerstone of many cryptographic primitives and secure communication protocols. Pseudorandom number generators, typically used in modern systems due to their high throughput and ease of implementation, cannot provide true randomness and hence are vulnerable to cyber-attacks. True random number generators (TRNGs) can provide true randomness, but their speed is typically low and their implementation remains too complex for many practical applications. Over the last few years, there have been several proposals of TRNGs that rely on some physical processes, such as radioactive decay, single photon optical processes, Brownian motion, clock jitters, noise in electronics devices, and others. However, the complexity involved in randomness extraction from such sources often makes the proposed TRNGs impractical for many emerging applications that rely on resource-constrained systems (e.g., Internet-of-Things and sensor networks). Such systems would greatly benefit from low-cost, easily implementable, robust, high-speed TRNGs.

E.J.Pankratz and E.Sánchez-Sinencio, "Multiloop high power supply rejection quadrature ring oscillator," IEEE J. Solid-State Circuits, vol. 47, no. 9, pp. 2033–2048, Sep. 2012.

This presents a source-follower-delay-cell, multiloop ring oscillator that provides power-supply isolation. The main contributions of this work are a source-follower-based delay cell with a multiloop ring structure achieving improved supply rejection, a design-oriented analysis of the proposed structure to facilitate its use, and a layout technique allowing straightforward mask design for the multiloop oscillator. The oscillator also features differential control voltages to allow rejection of common-mode control and supply noise. The oscillator was fabricated in a UMC CMOS pure logic process with no analog components (regular VT), and the minimum measured incremental supply sensitivity, which is more than better than that of a conventional CMOS-delay-cell quadrature oscillator fabricated on the same test chip. The oscillator's measured tuning range. Over the tuning range, the phase noise varies offset, and the power consumption. The measured mean quadrature accuracy performance is within to error including board parasitics without any trimming/tuning across the oscillator's frequency range.

III. Existing Method

Edge Detection Circuit

A DCM in Xilinx FPGAs has a dynamic reconfiguration port (DRP), which enables modification of its output frequency without reconfiguration of the entire circuit. This functionality makes the DCM-based TRNG tunable: although the use of a single pair of frequencies might result in generation of random numbers of poor quality, the TRNG can find a desirable pair of frequencies that shows good randomness by trying multiple pairs of frequencies while testing the generated random numbers. The counter of the TRNG primitive is designed so that only its MSB can be saturated (i.e. the next value to 0xff can be 0x80). The number of successive logic-ones may exceed 28, or even 29, yet its 27 or higher bits can be easily recovered by calculation in this design. While the DFF and the counter in the TRNG primitive are synchronized with ClkB, the other circuits are synchronized with the 100-MHz input clock ClkIN. To connect the output of the TRNG primitive to the subsequent circuits, synchronizer and edge detection circuits are required to prevent malfunction of the subsequent circuits.

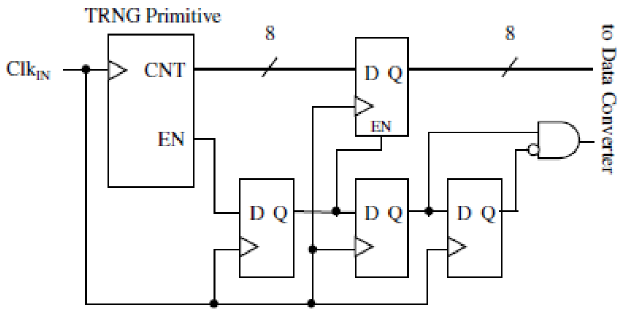


Figure 3: Block Diagram of Synchronization and Edge Detection Circuit

Table 1: A PART OF FREQUENCY PAIRS SELECTED

ID	M_A	D_A	M_B	D_B	t_j	Δt(ps)	η
1	31	32	30	31	609	10.8	480.0
2	30	31	29	30	592	11.5	449.5
3	29	30	28	29	576	12.3	420.0
68	31	32	28	29	593	34.6	149.3
98	17	23	14	19	437	42.0	161.0
99	9	10	26	29	412	42.7	130.0
100	18	20	26	29	412	42.7	130.0

The block diagram of the additional circuits is shown in Figure 3.1. In the evaluation shown in a data converter circuit that compresses an 8-bit counter value to 4 bits is also added, which will be described to Obtained counter values are sent to a PC via a UART connection of 460800 bps using a controller with a 4-KB buffer. When the output of the counter is written to the end of the buffer, subsequent counter values will be discarded until all data in the buffer is sent out. The DCMs are not dynamically reconfigured. An individual bit stream to the whole FPGA is generated for each set of parameters of the DCMs board, respectively.

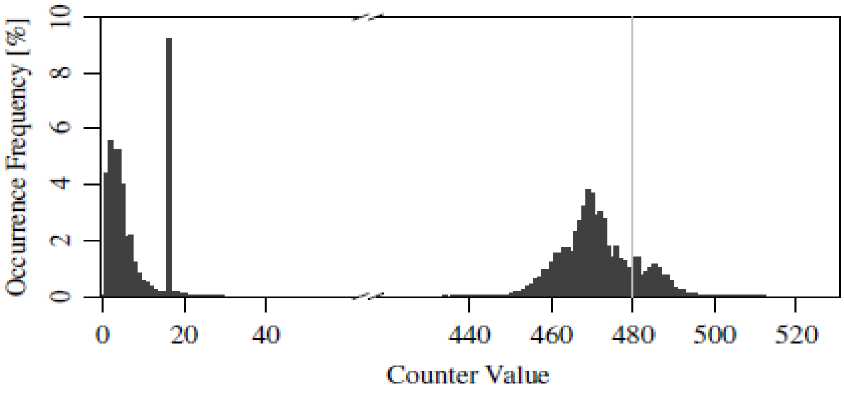


Figure 4: Distribution of counter value (1st pair).

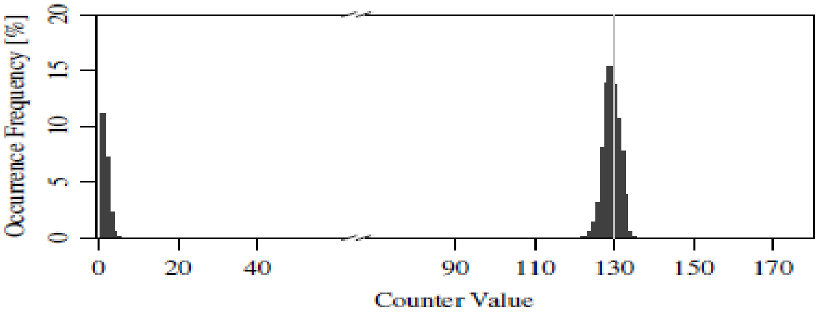


Figure 5: Distribution of counter value (100th pair).

To make the bit width of LSBs of the small counter values to be extracted smaller than that of the large counter values. From the preliminary experiment shown in counter values can be clearly divided into large ones and small ones.

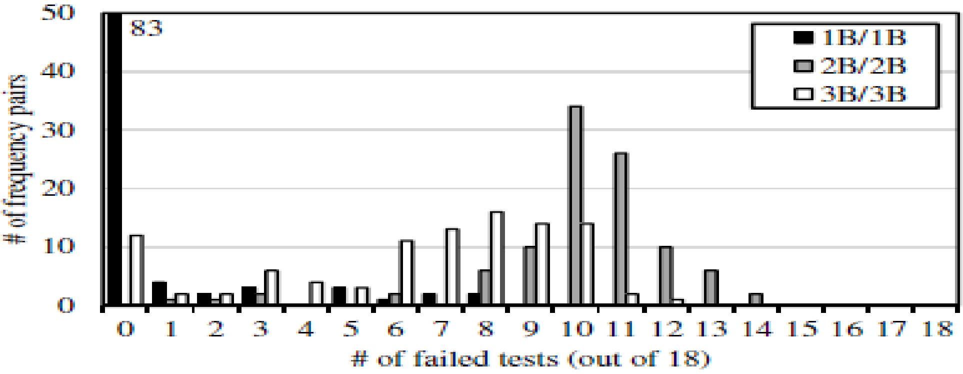


Figure 6: Distribution of the number of failed tests (same width of LSBs).

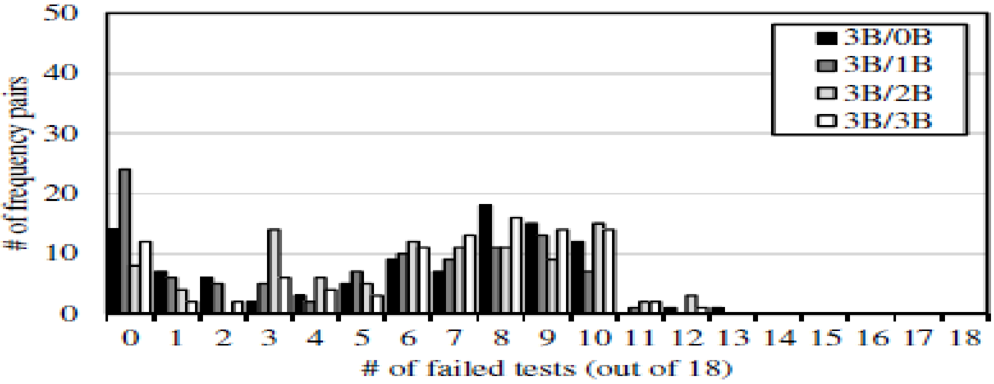


Figure 7: Distribution of the number of failed tests (different widths of LSBs).

A TRNG with these parameters is expressed as wlB/wsB. A comparison of their standard deviation implies that small counter values have less uncertainty than large ones. Therefore, it is expected that our proposal can improve the quality of generated random numbers with a minimal reduction of the generation rate of the TRNG.

IV. Proposed Method

Hardware True Random Number Generators

Hardware True Random Number Generators (TRNGs) are worn in all campaign that necessitate protected communiqué, device certification or data encryption. Applications include smartcards, RFID tags and IoT devices TRNGs used in cryptography are subject to strict certification procedure. In the past, the security of TRNG designs was evaluated by running a set of statistical tests Motivated by the current lack of mathematically-secure post-processing modules in the TRNG state-of-the-art, and suggest three hardware-well-organized post-processing architectures appropriate for condensed implementations. Which provide theoretically proved guarantees for the statistical quality and unpredictability of the output.

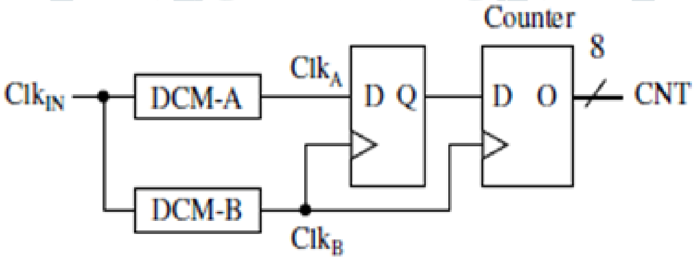


Figure 8: Basic Building Block of DCM

The only requirement imposed on the digital noise source is that it produces sufficient amount of min-entropy, which makes these post-processing methods compatible with all physical sources of randomness. For all three architectures, this thesis provide a method for selecting design parameters given the min-entropy of the digital noise source.

Our goal is to develop a digital post-processing method that provides theoretical guarantees for the quality of the output bits. This thesis provides a necessitate this unit to be worldwide in the intelligence that the guarantee is provide for whichever digital noise basis with enough level of min-entropy. Since there is no known mathematical method which guarantees uniformity(full-entropy) for all such sources. In the Existing method, preprocessing stage at the end of the circuitry where have to make a logic of random number generation. For that, removed the unnecessary section which takes more area, where the purpose of the circuitry is to frame the patters according to edge triggering.

Digital Clock Manager

DCMs merge advanced clocking potential into the Spartan-3 worldwide clock distribution arrangement. As a result, Spartan-3 DCMs determine a range of general clocking concern predominantly in high-concert immense frequency relevance expand or come apart an expected Clock Frequency or bring into being a entirely new frequency by a fusion of clock replica and partition. Condition a Clock, ensure a unsoiled output clock with a 50% duty cycle. Phase Shift a clock signal, moreover by a set of fraction of a clock period or by exact increment. Remove Clock Skew, moreover inside the device or to exterior apparatus, to get better in general structure recital and to get rid of clock allocation delays. Mirror, ahead or Rebuffer a Clock Signal, frequently to deskew and translate the arriving clock signal to a dissimilar I/O standard—for example, forward and convert an arriving LVTTL clock to LVDS.

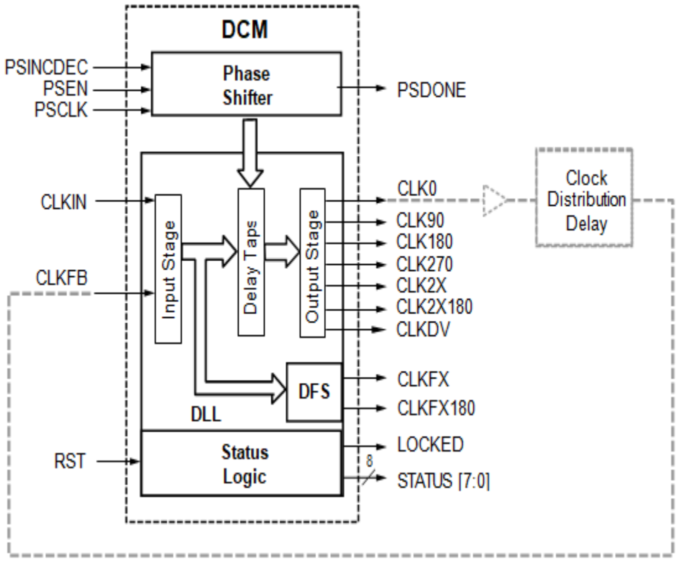


Figure 9: DCM Functional Block Diagram

The Delay-Locked Loop (DLL) entity make available an on-chip digital deskew pathway so as to generate zero-propagation-interruption clock output signal. The deskew path compensate intended for the delay on the direction-finding set of connections by monitor an output clock, furthermore the CLK0 or the CLK2X. The DLL unit efficiently eliminate the delay as of the exterior clock input port to the personage clock load surrounded by the mechanism. The well-buffer global arrangement minimize the clock skew on the system cause by load differences .The input signals in the direction of the DLL entity are CLKIN and CLKFB. The output signals as of the DLL are CLK0, CLK90, CLK180, CLK270, CLK2X, CLK2X180, and CLKDV .The DLL part generate the output designed for the Clock Doubler (CLK2X, CLK2X180), the Clock Divider (CLKDV) and the Quadrant Phase Shifted Outputs function.

Architecture of the Proposed TRNG

The Proposed TRNG architecture is similar to the Existing DCM based Architecture but there is no circuitry before Pre-Processing stage and thus the area of the circuit will get reduced and the count values are directly feed to post processing circuit can map 2 bits from each segment where actually it is 1-bit in the existing DCM based network. The algorithm for post processing method is briefly explained as below.

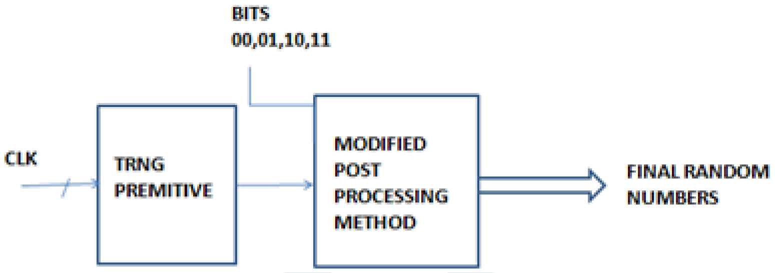


Figure 10: Architecture of the Proposed TRNG

The Above block diagram shows the clk is given as input and the combination of counter and enable is known as TRNG Primitive and the output is passed to the modified post processing method. That means, this method have Two-Bit Edge Detection is nothing but directly giving two inputs at a time and two bit edge detection process have been done with a novel Algorithm in generation of True Random Numbers And then the output has more and better random numbers with less circuit area and delay will be greatly reduces and power consumption is also greatly reduces.

Novel Algorithm of the proposed method:

```
Algorithm 1 Proposed Algorithm for Random number generation
Input: CNT, Output: q
Generating the 2 bit counter for splitting CNT values and assign to a value mem[d].
If there is d value with ‘00’ then
    Assign values for q as mem of 1,2,0,3
Else if there is d value with ‘01 then
    Assign values for q as mem of 0,3,2,1
Else if there is d value with ‘10’ then
```

```
        Assign values for **q** as **mem** of 0,3,1,2
    **Else if** there is d value with ‘11 **then**
        Assign values for **q** as **mem** of 0,2,1,3
```

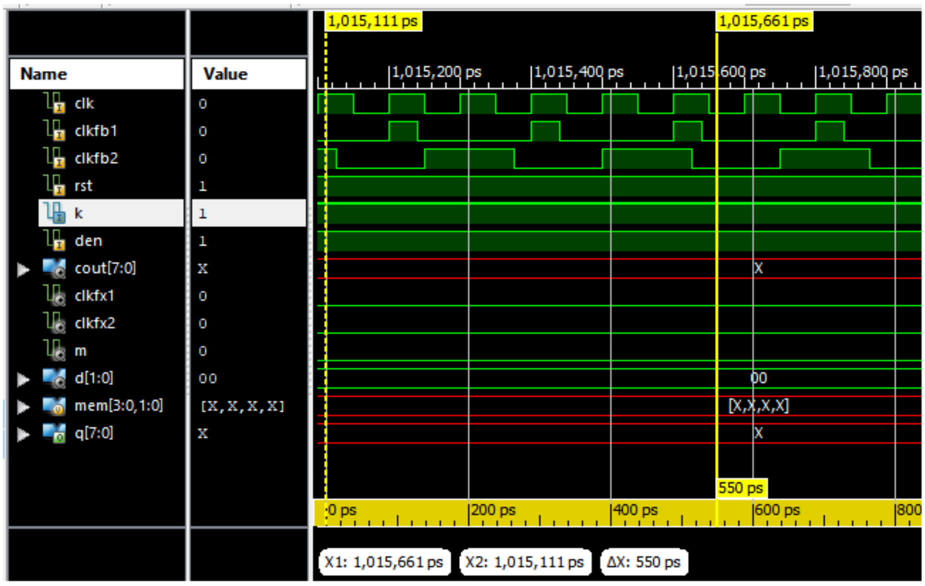
As per the above Algorithm, taking Input as CNT is nothing but a counter with 2 bits known as 2 bit Counter and Output is taken as q. and then split the counter values and assigning them to a mem[d] is nothing but random numbers.

And here inputs as with two bit binary digits nothing but “00,01,10,11”. At first can take input d as “00” means the generated random numbers are assigned to the output q as mem of “1,2,0,3” are four random numbers else with the condition input is given as “01” then the generated output is assigned to the q as mem of “0,3,2,1” . And giving input d as “10” then the output is assigned to the value as mem of “0,3,1,2”and the fourth condition as “11”is given as input and the generated output is as mem of “0,2,1,3”. At a time four Random Numbers generated with lees Power Reduction, requiring less Area and delay ia also reduced.

V. Results

Approximate circuits are used where the computation speed, area, energy and power are of more priority outcome to be accurate i.e., By Using ISE DESIGN SUITE Project Navigator, Xilinx 14.7 version in the simulation procedure the better outputs are achieved with Less Circuit Area with low power consumption.

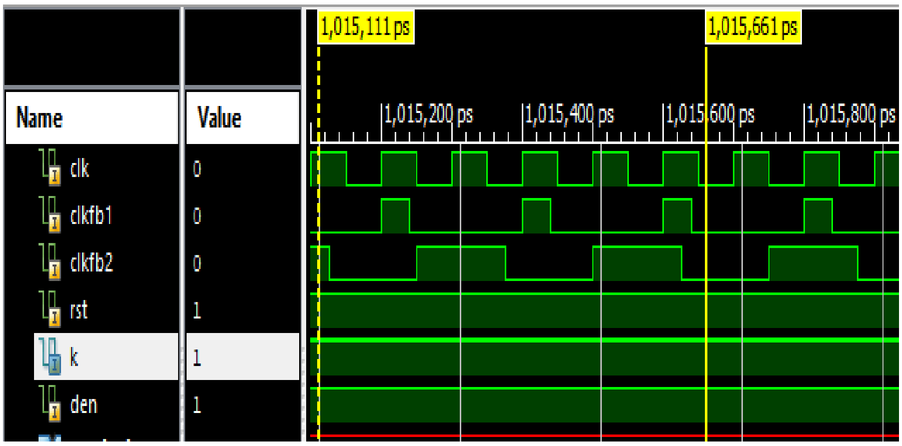
Generating Clock Pulses For Clk, Clk fb1and Clk fb2 :



Name	Value
clk	0
clkfb1	0
clkfb2	0
rst	1
k	1
den	1
cout[7:0]	X
clkfx1	0
clkfx2	0
m	0
d[1:0]	00
mem[3:0,1:0]	[X,X,X,X]
q[7:0]	X

X1: 1,015,661 ps X2: 1,015,111 ps ΔX: 550 ps

Figure 11: Clock Pulses



Name	Value
clk	0
clkfb1	0
clkfb2	0
rst	1
k	1
den	1

Figure 12: Clock Pulses For Clk, Clk fb1 and Clk fb2

Table 2: Comparison for Existing Method and the Proposed Method

Parameters	Existing Method	Proposed Method
LUT	22	22
Slice Registers	35	23
Delay (ns)	11.222	9.603

By comparing the Slice Registers has been reduced and improved the efficiency by using the proposed method compared to Existing method. The Delay (ns) has been reduced and increase the execution speed in the proposed method compared to Existing method.

CONCLUSION

This thesis analyzed and described the method on how one can generate True Random Numbers using a FPGA Based on the partitions of the counter values, random numbers are generated. The proposed design can greatly increase the number of pairs that give good random numbers and speed also increases in the generation of random numbers when compared to the previous method.

The randomness improved by combining independent random numbers into single one. The system gives high randomness and also consumes low power compare to the previous system. The important contribution of this thesis is Linear Feedback Shift Register based processor produces unpredictable codes, enhances the randomness of output binary sequences and the bit rate produced.

FUTURE SCOPE

In Future, it can be implemented by increasing number of bits in TRNG improve the security in Cryptography and Communication of Authentication in Key generation.

REFERENCES

[1] N. Fujieda and S. Ichikawa, “A latch-latch composition of metastability based true random number generator for Xilinx FPGAs,” IEICE Electronics Express, vol. 15, no. 10, pp. 20 180 386:1–20 180 386:12, 2018.

[2] A. P. Johnson, R. S. Chakraborty, and D. Mukhopadyay, “An Improved DCM-Based Tunable True Random Number Generator for Xilinx FPGA,” IEEE Transaction on Circuits and Systems II: Express Briefs, vol. 64, no. 4, pp. 452–456, 2017.

[3] M. Majzoobi, F. Koushanfar, and S. Devadas, “FPGA-Based True Random Number Generation Using Circuit Metastability with Adaptive Feedback Control,” in Proc. International Workshop on Cryptographic Hardware and Embedded Systems 2011, pp. 17–32.

[4] G. Marsaglia. Diehard battery of tests of randomness (mirror). [Online]. Available: https://github.com/reubenhwk/diehard

[5] B. Ray and A. Milenkovi´c, “True Random Number Generation Using Read Noise of Flash Memory Cells,” IEEE Transactions on Electron Devices, vol. 65, no. 3, pp. 963–969, 2018.

[6] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, A statistical test suite for random and pseudorandom number generators for cryptographic applications, NIST Special Publication 800–22, Rev. 1a, 2010.

[7] 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 frequency detection,” in Proc. IEEE 2014 Custom Integrated Circuits Conference, 2014, pp. 1–4.

[8] J. von Neumann, “Various techniques used in connection with random digits,” Monte Carlo Method, National Bureau of Standards Applied Mathematics Series 12, pp. 36–38, 1951.

[9] Xilinx Inc., Virtex-5 FPGA Data Sheet: DC and Switching Characterisics, Product Specification DS202 (v5.5), 2016.

[10] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. Varanonuovo, “A high-speed oscillator-based truly random number source for cryptographic applications on a smart card IC,” IEEE Trans. Comput., vol. 52, no. 4, pp. 403–409, Apr. 2003.

[11] W. Chen et al., “A 1.04 µW truly random number generator for Gen2 RFID tags,” in Proc. IEEE A-SSCC, Nov. 2009,pp. 117–120.

[12] M. Jessa and L. Matuszewski, “Enhancing the randomness of a combined true random number generator based on the ring oscillator sampling method,” in Proc. Int. Conf. ReConFig Comput. FPGAs, Cancun, Mexico, Nov. 30–Dec. 2, 2011, pp. 274–279.

[13] E.J.Pankratz and E.Sánchez-Sinencio, “Multiloop high power supply rejection quadrature ring oscillator,” IEEE J. Solid-State Circuits, vol. 47, no. 9, pp. 2033–2048, Sep. 2012.

[14] L. Dai and R. Harjani, “Design of low phase noise CMOS ring oscillators,” IEEE Trans. Circuits Syst. II, Analog Digit. Signal Process., vol. 49, no. 5, pp. 328–338, May 2002.

[15] Dongsheng Liu, Zilong Liu, Lun Li, and Xuecheng Zou”.A low cost low power ring oscillator based truly random number generator for encryption on smart cards”, IEEE Trans IEEE Transactions on circuits and systems vol. 63, no. 6, june 2016.

[16] P. Choi, M.-K. Lee and D.K. Kim,” Fast compact true random number generator based on multiple sampling”’, ELECTRONICS LETTERS 22nd June 2017 Vol. 53 No. 13 pp. 841–843.