IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710


# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 9, September 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 9, September 2023 ||

| DOI:10.15680/IJIRSET.2023.1209073 |

# A Fast True Random Number Generator of 64 bit Based on FPGA by using Digital Clock Managers and Metastability

**Ch. Sai kishore[1], K. Hari krishna[2], Dr. A.M. Prasad[3]**

M.Tech Student, I&CE, Dept. of ECE, UCEK (A), JNTUK, Kakinada, Andhra Pradesh, India[1]

Assistant Professor, Dept. of ECE, UCEK (A), JNTUK, Kakinada, Andhra Pradesh, India[2]

Professor, Dept. of ECE, UCEK (A), JNTUK, Kakinada, Andhra Pradesh, India[3]

**ABSTRACT:** Public key generation, nonce generation in authentication protocols, and initialization vector generation in cryptographic systems all make use of true random numbers, and this work proposes an efficient technique to produce such random numbers in altera quartus. The proposed technique employs a randomness source based on the metastability condition of flip-flops. In order to coerce the flip-flop into the metastability area, the plan exploits the hardware primitives given by Digital Clock Manager and changes the phase shift between the two clock signals. A 64-bit shift register is used to store the created random bit, since it consecutively stores 64 bits. On-chip post-processing, including the accumulation approach and the bit-flipping method, is used to boost randomness and decrease the occurrence of patterns.

**KEYWORDS:** FPGA, True Random Number Generator (TRNG), Metastability, Digital Clock Manager (DCM),

## I. INTRODUCTION

The data security is utmost important in communication systems and computer applications. For many cryptographic and security-related purposes—including the production of secret or public keys, challenges for protocol authentication, and nonces—it is necessary to have access to a True random number generator. Games, lottery draws, and gambling all make use of true random numbers. The generated random number should be unexpected and non-repeatable. In communication systems information transferred by means of either wired or wireless and it is necessary to protect the information from hacker attacks. Random numbers are necessary for encryption as they are used to generate the codes that scrambles messages such that the selected receiver can receive the message because of this scrambling. Key lengths in contemporary cryptography are sometimes rather large, but if such keys were generated from a much smaller seed, they would lose much of their entropy.

Various TRNGs have been proposed and executed so far, each utilizing a one of a kind arrangement of strategies for separating this randomness or haphazardness from some fundamental actual process showing uncertainity; this incorporates things like thermal and shot noise, as well as optional impacts like clock jitter and metastability in circuits, and, surprisingly, environmental noise. Be that as it may, in considering the fact that to their notoriety, a ton of late work has been committed to the production of completely computerized TRNGs for execution on Field Programmable Gate Arrays (FPGAs).

To remove the haphazardness, prior frameworks frequently utilize free-running Ring Oscillators (ROs) and Programmable Delay Lines (PDLs) in light of Look-up Tables (LUTs). As indicated by [2], an Data Flip-Flop (FF) may have its clock and data inputs driven by two PDLs. There, the PDLs are carried out as series-associated LUTs also use a inverter. The delay of each LUT is adjusted independently of the underlying logic by assigning appropriate values to their unused inputs.

Notwithstanding, in [11] and [14], creators take an alternate tack by utilizing a XOR gate where its result is samled by a FF to deal with the information from a few ROs. The FF may generate a random bit due to sampling glitches of non-deterministic length due to the existence of phase jitter.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 9, September 2023 ||

| DOI:10.15680/IJIRSET.2023.1209073 |

## II. LITERATURE REVIEW

This section provides a literature survey to examine important points from recent studies. In the first part, the idea of metastability in bistable circuit components like flip-flops is explained; this metastability is achieved by utilizing specific programmable delaye lines to impeccably balance the signal appearance timings to goes back and forth, as depicted in [2]. Here, the PDLs' accuracy for changing signal spread delays is bigger than parts of a picosecond. Elevated degrees of irregularity in the created bits, flexibility against changes in the environment, and strength against dynamic contentious attacks are guaranteed with the assistance of a constant observing framework. In [11] and [14], which use the substitute methodologies, the result of a few ROs is given to a XOR gate, the result of which is tested by a FF. Within the sight of phase jitter, the FF might test errors of non-deterministic term, yielding an irregular piece. New security key age strategy for SRAM PUF in light of Fourier examination is shown by W. Liu, Z. Lu, H. Liu, R. Min, Z. Zeng, and Z. Liu in [10]. The SRAM PUF Boolean capability and the SRAM device Fourier spectra together describe the device's power-on conduct. Key organization and capacity answers for sensor networks and RFID frameworks have been shown by J. Guajardo et al. in [6], in view of the utilization of physically-unclonable functions (PUFs). As well as giving a synopsis of the numerous PUF acknowledge now being used, this article likewise offered a PUF acknowledgment focused on for incredibly minimal expense applications. The time-to-digital converter in the [8] design is constructed from 32 series-connected 8-bit fast carry chains and a LUT-based programmable delay chain. The actual implementation of such systems requires the requisite number of ROs and inverters inside each RO, in addition to the exact tuning of the PDL delays, which may be substantially effected by the routing. In order to provide enough variability, the greater part of the previously mentioned geographies need a post-processing block and an feedback control. Clock managers have recently been studied as a practical means of making TRNG design on FPGA devices easier [12], [13]. These equipment natives are for the most part tracked down in current FPGAs and are utilized to make at least one result clock signals at client selectable frequencies. The Digital Clock Manager (DCM) is accessible on Xilinx gadgets, though the Clock Manager (CM) is accessible on Intel processors.

### TRUE RANDOM NUMBER GENERATOR ARCHITECTURE:

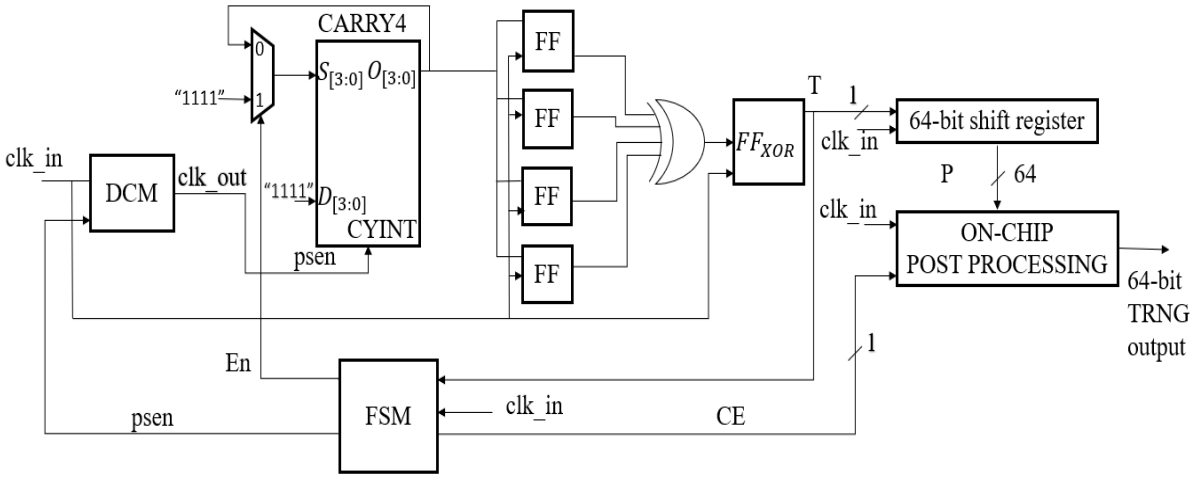


Fig. 1. TRNG architecture

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 9, September 2023 ||

| DOI:10.15680/IJIRSET.2023.1209073 |

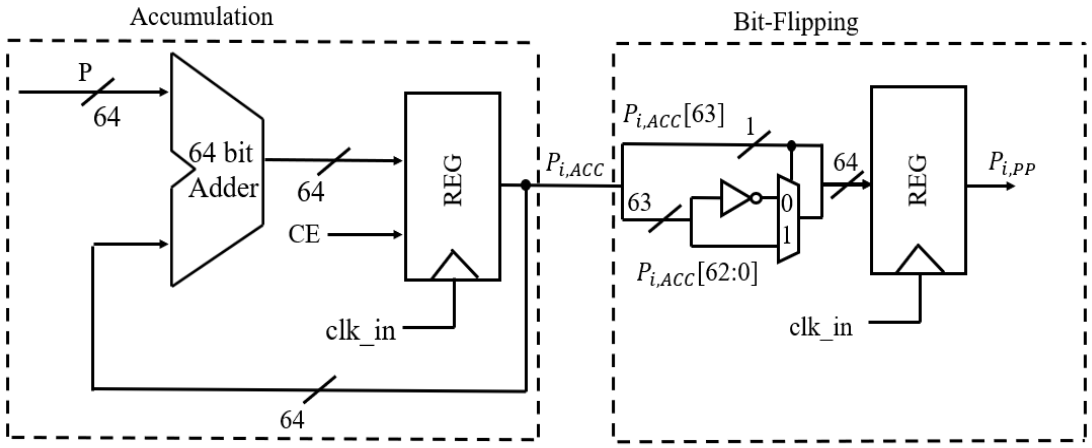


Fig. 2. Post Processing Circuit

Fig.1 displays the True Random Number Generator design as it is planned. The architecture consists of Digital Clock Manager and its output clk out is given to the carry4 adder and the sum outputs ($O_{[3:0]}$) is fed as data input to the four flip-flops. The DCMs clk_out drives the input $C_{YINIT}$ of the carry4 adder. The XOR gate merges the four flip-flops output. Therefore, it makes no difference which of them evolved into a metastable state. The flip-flop $FF_{XOR}$ clocked by the system clk_in samples the output of XOR. The FFXOR yield T is 0 since each of the four FFs samples a similar stable number, perhaps in light of the underlying DCM state or some unanticipated variation in the signals routing. The setup signals of the DCM are controlled in a feedback structure by a signal T, which is a contribution to the finite state machine. Assuming T is zero, the FSM will state psen to 1 for one clock cycle, starting a phase shift with the DCM. Then, while monitoring out for the condition of the signal T, the FSM hangs tight for up to N clock cycles. Another phase shifting exchange is begun each N clock cycles assuming T stays at 0. When T = 1, in the FFs one have arrived at their metastable region, and the phase contrast among clk_in and clk_out will no longer auto-align. At the point when a signal called En is set to 0, the FSM quits changing the period of clk_out and then obtaining the irregular bit stream might start. As should be visible in Fig.1, the selectors S[3:0] of the carry-4 chain multiplexers are being driven in a feedback by the signals O[3:0]. S[3:0] = "1111" implies that the auto-alignment stage is as yet running when the signal En = 1. Whenever metastability has been delivered, En is reset to 0 and S[3:0] becomes O[3:0]. To go with this decision, En controls a group of four of multiplexers whose logic might be imposed by a group of four of Lookup Tables (LUTs) in a verysame CARRY4 slice. The proposed procedure endeavors to set off a race order at the XOR gate of the CARRY4. Then, a shift register gets the random number bit T and unions the accompanying 64 pieces into a 64-bit bundle (P). To dispose of any possible bias in the produced random order, the on-chip post-processing module, as displayed in Fig. 2, is utilized. The 64-bit accumulator receives the packet P as input. The sum is calculated as $P_{i,ACC} = (P_i + P_{i-1,ACC}).(\text{mod } 2^{32})$, where Pi is the i-th 64-bit packet. Modern FPGAs also have Digital Signal Processing (DSP) slices, into which this logic may be easily incorporated. The FSM then uses the CE signal to activate the accumulator register once the shift register has recieved 64 consecutive random bits. To reduce the prevalence of repetition, bits are flipped dynamically. The final 64-bit packet $P_{i,PP}$ is produced after post-processing.

## III. RESULTS

The simulation results shown in fig.3 illustrates the 64 bit random number generated using the proposed 64 bit shift register along with 64 bit accumulation and bit flipping mechanism in post processing method, in altera quartus ii. The area consumption and power dissipation results are shown in fig 4 and 5. In simulation, the input signal ‘clk’ is clocked with rising edge as ‘1’ and a falling edge as ‘0’.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 9, September 2023 ||

| DOI:10.15680/IJIRSET.2023.1209073 |

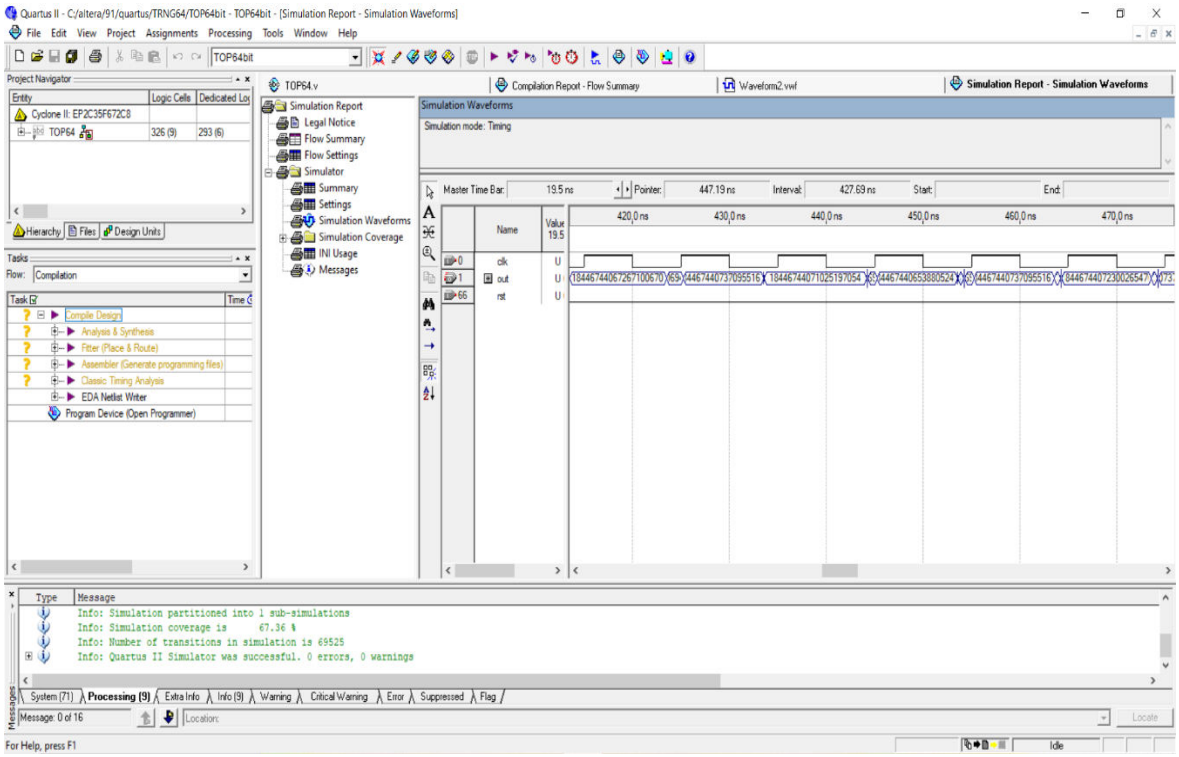


Fig.3 Simulation Results

| | |
|---|---|
| Quartus II Version | 9.1 Build 222 10/21/2009 SJ Web Edition |
| Revision Name | TOP64bit |
| Top-level Entity Name | TOP64 |
| Family | Cyclone II |
| Device | EP2C35F672C8 |
| Timing Models | Final |
| Met timing requirements | Yes |
| Total logic elements | 326 / 33,216 ( < 1 % ) |
| Total combinational functions | 261 / 33,216 ( < 1 % ) |
| Dedicated logic registers | 293 / 33,216 ( < 1 % ) |
| Total registers | 293 |
| Total pins | 66 / 475 ( 14 % ) |
| Total virtual pins | 0 |
| Total memory bits | 0 / 483,840 ( 0 % ) |
| Embedded Multiplier 9-bit elements | 0 / 70 ( 0 % ) |
| Total PLLs | 0 / 4 ( 0 % ) |

Fig.4 Area result

| | |
|---|---|
| Quartus II Version | 9.1 Build 222 10/21/2009 SJ Web Edition |
| Revision Name | TOP64bit |
| Top-level Entity Name | TOP64 |
| Family | Cyclone II |
| Device | EP2C35F672C8 |
| Power Models | Final |
| Total Thermal Power Dissipation | 117.81 mW |
| Core Dynamic Thermal Power Dissipation | 0.00 mW |
| Core Static Thermal Power Dissipation | 79.95 mW |
| I/O Thermal Power Dissipation | 37.87 mW |
| Power Estimation Confidence | Low: user provided insufficient toggle rate data |

Fig.5 Power dissipation result

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 9, September 2023 ||

| DOI:10.15680/IJIRSET.2023.1209073 |

## IV. CONCLUSION AND FUTURE SCOPE

It is simple to create this True random number generator based on DCM using FPGA device. It makes benefit of the tuning capability of DCM's primitives to change the phase shift between the two clock signals. As a source of unpredictability, the produced metastability is used. The phase difference is determined automatically by the finite state machine. The produced bits will be even more unpredictable using the fast carry chain primitive CARRY4. This work was done in altera quartus ii. All the characteristics like area, delay, and power consumptions were evaluated. TRNGs will have far-reaching impact in the future. Its data width may be extended in the future.

## REFERENCES

[1] H. Hata, and S. Ichikawa, "FPGA Implementation of Metastability-Based True Random Number Generator," IEICE Trans. Inf. & Syst., vol.E95-D, no. 2, pp. 426-436, Feb 2012.
[2] M. Majzoobi, F. Koushanfar, and S. Devadas, "FPGA-based true random number generation using circuit metastability with adaptive feedback control," in Proc. Crypt. Hard. Embedded Syst. (CHES), 2011, pp. 17–32.
[3] V. Fischer and M. Drutarovsky, "True random number generator embedded in reconfigurable hardware," Proc. Cryptographic Hardware and Embedded Systems - CHES 2002, LNCS 2523, pp.415–430, Springer, 2002
[4] R. Della Sala, D. Bellizia and G. Scotti, "A Novel Ultra-Compact FPGA compatible TRNG Architecture Exploiting Latched Ring Oscillators," in IEEE Trans. Circuits Syst. II, Exp. Briefs, vol. 69, no. 3, pp. 1672-1676, March 2022.
[5] M. Drutarovsky, and P. Galajda, "A Robust Chaos-Based True Random Number Generator Embedded in Reconfigurable Switched-Capacitor Hardware," in Proc. of 17th International Conference Radioelektronika, pp. 1-6, Apr. 2007.
[6] J.Guajardoetal.,"Anti-counterfeiting, key distribution, and key storage in an ambient world via physical unclonable functions," Inf. Syst. Frontiers, vol. 11, no. 1, pp. 19–41, Mar. 2009
[7] W. Liu, Z. Lu, H. Liu, R. Min, Z. Zeng, and Z. Liu, "A novel security key generation method for SRAM PUF based on Fourier analysis," IEEE Access, vol. 6, pp. 49576–49587, 2018.
[8] X. Li, P. Stanwicks, G. Provelengios, R. Tessier, and D. Holcomb, "Jitter-based adaptive true random number generation for FPGAs in the cloud," in Proc. Int. Conf. Field-Programmable Technol. (ICFPT), 2020, pp. 112–119.
[9] A. Cherkaoui, V. Fischer, L. Fesquet, A. Aubert, A, "A Very High Speed True Random Number Generator with Entropy Assessment. Cryptographic Hardware and Embedded Systems," in Proc. Crypt. Hard. Embedded Syst. (CHES), 2013, pp. 1–18.
[10] W. Liu, Z. Lu, H. Liu, R. Min, Z. Zeng, and Z. Liu, "A novel security key generation method for SRAM PUF based on Fourier analysis," IEEE Access, vol. 6, pp. 49576–49587, 2018
[11] N. N. Anandakumar, S. K. Sanadhya, and M. S. Hasmi, "FPGA-based True Random Number Generation Using Programmable Delays in Oscillator rings," IEEE Trans. Circuits Syst. II, Exp. Briefs, vol. 67, no. 3, pp. 570- 574, March 2020.
[12] A. P. Johnson, R. S. Chakraborty, and D. Mukhopadyay, "An improved DCM-based tunable true random number generator for Xilinx FPGA," IEEE Trans. Circuits Syst. II, Exp. Briefs, vol. 64, no. 4, pp. 452–456, Apr. 2017.
[13] N. Fujieda, M. Takeda, and S. Ichikawa, "An Analysis of DCM-Based True Random Number Generator," IEEE Trans. Circuits Syst. II, Exp. Briefs, vol. 67, no. 6, pp. 1109–1113, Apr. 2020.
[14] D. Schellekens, B. Preneel, and I. Verbauwhede, "FPGA Vendor Agnostic True Random Number Generator," in Proc. Int. Conf. Field Program. Logic Appl. (FPL), pp 1-6, Aug. 2006
[15] L. Santiago et al., "Realizing strong PUF from weak PUF via neural computing," in Proc. IEEE Int. Symp. Defect Fault Tolerance VLSI Nanotechnology. Syst. (DFT), Cambridge, MA, USA, Oct. 2017, pp. 1–6.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details