IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

FPGA BASED 64-BIT TRUE RANDOM NUMBER GENERATOR

Bonala Purushotham[1], Karee Manish[2], Vankala Bhanu Prakash[3]

Sudhir Dakey[4](Assistant Professor)

[1,2,3,4]Department of Electronics and Communication Engineering

Maturi Venkata Subba Rao (MVSR), Engineering College, Nadergul, Telangana

ABSTRACT

True random number generators, often known as TRNGs, are essential components of a wide variety of critical security applications. Despite the fact that digital-based solutions take use of randomness sources that are often found in the analogue domain, digital-based solutions are highly needed, particularly when they need to be implemented on Field Programmable Gate Array (FPGA)-based digital systems. In this research, a unique technique that makes the design of a TRNG on FPGA devices more straightforward is described. In order to adjust the phase shift between two clock signals, it takes use of the runtime capabilities of the hardware primitives provided by the Digital Clock Manager (DCM). The auto-tuning approach that is being given automatically adjusts the phase difference between two clock signals to compel one or more flip-flops (FFs) to enter the metastability zone. This region is used as a source of unpredictability in the system. In addition, a unique use of the fast carry-chain hardware primitive is offered as a means of further increasing the level of randomness present in the bits that are created. In final, a powerful on-chip post-processing strategy that does not inhibit the TRNG throughput is outlined here. This work was built in 32 and 64 data width, in verilog HDL, and synthesized in QUARTUS II. All of the characteristics were evaluated with regard to area, latency, and power consumption.

Keywords: Metastability, FPGA, Phase Shift, Auto Tuning, Flip Flops, Carry Chain, Post-Processing, Verilog HDL, QuartusII.

1. INTRODUCTION

Random number generators are indispensable components of any modern security system. With physically unclonable functions (PUFs), true random number generators (TRNGs) are the only cryptographic primitives producing truly unpredictable bits for generating secrets in symmetric and public-key cryptography. Random number generators are also extensively used in various randomization-based countermeasures for protecting cryptographic implementations against side-channel attacks (SCA). Among others, the low-latency masking schemes for countering the SCA incur a high area penalty, leaving only limited resources for random number generation. These schemes also require many random bits per execution cycle that a TRNG often cannot provide. Therefore, they resort to faster pseudo-random number generators (PRNGs) to generate random masks. Although producing statistically perfect random bits, the output of a cryptographically secure PRNG becomes entirely predictable once its inner state is leaked or guessed due to its deterministic nature. In the world of information security, we often see statements such as 'secured by 128-bit AES' or 'protected by 2048-bit authentication'. We are used to people asking about the strength of the cryptographic algorithms deployed in a security solution. Algorithms such as the AES, RSA and ECC have a proven track record of being difficult to break. They are successfully deployed in protocols that protect our identity and the integrity and confidentiality of our data, what we see very rarely, unfortunately, are statements about the strength of the random number generator used by a security system. System designers are typically more concerned with the power consumption and bit generation speed, than with the actual randomness of the bits generated.

2. LITERATURE SURVEY

[1] M. Drutarovsky, and P. Galajda

A Robust Chaos-Based True Random Number Generator Embedded in Reconfigurable Switched-Capacitor Hardware.

This paper reviews, design is optimized for reduction of influence of **supply voltage** to the quality of generated random bit stream. The ultimate output **bit rate** of proposed TRNG is 60 kbit/s and quality of generated bit-streams is confirmed.

[2] M. Majzoobi, F. Koushanfar, and S. Devadas

FPGA-based true random number generation using circuit metastability with adaptive feedback control.

This paper reviews, the monitoring system employs a **feedback loop** that actively monitors the probability of output bits; as soon as any bias is observed in probabilities, it adjusts the delay through PDLs to return to the **metastable** operation region.

[3] R. Della Sala, D. Bellizia and G. Scotti

A Novel Ultra-Compact FPGACompatible TRNG Architecture Exploiting Latched Ring Oscillators

This paper reviews, architecture has been implemented on Xilinx Spartan-6 devices and the TRNG performances have been extensively validated under **supply voltage** and **temperature variations**. An estimated **entropy** of about 7.99834 per bit, **throughput** of 0.76 Mbits/s with a 50MHz clock.

[4] M. Grujić and I. VerbauwhedeTROT: A Three-Edge Ring Oscillator Based True Random Number Generator with Time-to-Digital Conversion. This paper reviews, TRNG exquisitely balances low design effort and resource consumption with **high throughput** and a **high min-entropy rate**, making it more suitable for randomness. TRNG digital noise source and the **post-**

processing occupies 33 slices and achieves a throughput of 12.5 Mbps.

3. SCOPE AND AIM OF THE PROJECT

SCOPE OF THE PROJECT

FPGA-based true random number generators (TRNGs) have a wide range of applications in areas that require high-quality and unbiased random numbers, such as cryptography, simulation, and scientific computing.

AIM OF THE PROJECT

To generate a stream of random numbers to operate at high speeds, making it suitable for use in high-speed applications. The use of a clock manager allows generation of random numbers. The FPGA-based design allows for flexibility and customization, making it possible to tailor the generator to specific requirements and characteristics were evaluated with regard to area, latency, and power consumption.

4. PROPOSED METHOD

The system clock, i.e., the DCM input clock clk_in, drives the clock input of a FF. The DCM produces the output clock clk_out with the same frequency that drives the data input of the FF. To force the FF entering the metastable region, clk_in and clk_out should arrive almost simultaneously at the FF inputs, thus violating the FF setup/hold timing constraints. the proposed design exploits its dynamic phase shifting (DPS) capability to force one or more FFs to enter the metastability region. The DCM phase shift is exploited to compensate this difference in routing delays. Alternative use of the clock manager hardware primitive to design a high-speed TRNG. In place of tuning the frequency of the output clocks,

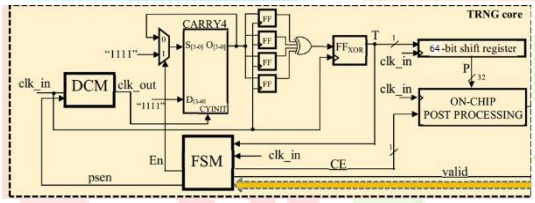

Fig.1: TRNG Core

the proposed design exploits its dynamic phase shifting (DPS) capability to force one or more FFs to enter the metastability region. The proposed solution has the ability to automatically tune the phase shifting of the DCM so that the random sequence generation automatically starts when this condition occurs.

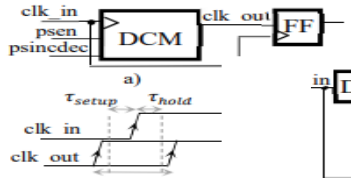

Fig.2: T-shift

To enhance the randomness, we also propose an unconventional utilization of the carry-chain primitive included in the FPGAs slice with a configurable feedback scheme.

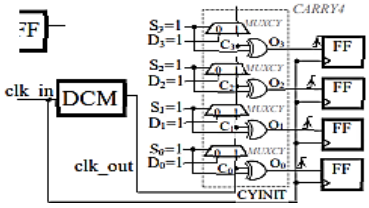

Fig.3: Carry4

Four FFs receive as data input the sum outputs (O[3:0]) of a CARRY4 chain. The signal clk_out drives the CARRY4 input signal CYINIT. The generic signal Oi+1 is delayed with respect to Oi by the propagation delay τ of the multiplexer in-between the output positions i and i+1, with i=0…2. In the event that T-shift is too large to ingenerate metastability, it is reasonable to assume that τ shift > T mux hence a finer phase shifting of the FF data inputs is obtained. The four FFs of the randomness generator sample the same stable value and the output T of FFXOR is 0.

The signals O[3:0] are in a feedback loop to drive the selectors S[3:0] of the multiplexers of the carry chain. When the signal En is 1, the auto-calibration phase is still running and S[3:0] is set to "1111", the signal T is the input of a Finite State Machine (FSM) that controls the configuration signals of the DCM in a feedback fashion. The purpose of the proposed scheme is to force the XOR gates of the CARRY4 in a race condition. On different placement sites, demonstrated that after the auto-calibration which takes 160 clock cycles on average, at least one of the fours FFs actually enters the metastable region.

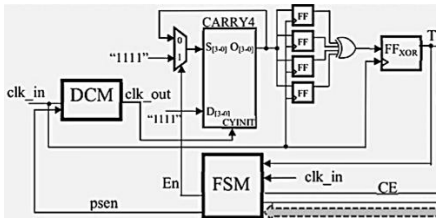

Fig.4: Auto calibration & Feedback Loop

Indeed, over a 10Mb sequence outputted by the XOR gate, the percentage of 0's and 1's is close to 50%. In the proposed scheme, **the signal T represents the raw random bit** that is generated with a throughput equal to the system clock frequency. With the goal of increasing the randomness of the signal T, a further technique is here adopted in conjunction with the use of the DCM. Finally, a simple

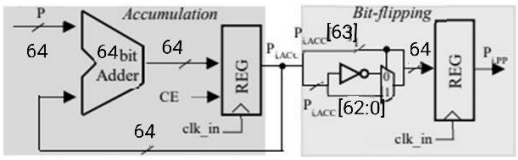

Fig.5: On chip Post-Processing

on-chip post processing scheme is proposed that exploits only one Digital Processing Signal (DSP) slice without reducing the bit production rate.

5. SOFTWARE USED

QUARTUS II

The Altera Quartus II design software provides a complete, multiplatform design environment that easily adapts to your specific design needs. It is a comprehensive environment for system-on-a-programmable-chip (SOPC) design. The Quartus II software includes solutions for all phases of FPGA and CPLD design.

Steps involved:

- Creating a Project
- Project Navigator
- Creating a Design
- RTL Viewer
- Technology Map viewer
- Simulation
- Waveform Editor
- Simulator Tool

VERILOG HDL

Hardware Description Language (HDL). Any digital system can be represented in a Register Transfer Level (RTL) and HDLs are used to describe this RTL. The idea is to specify how the data flows between registers and how the design processes the data.

Steps involved:

- Architectural Design
- Behavioural or Functional Design:
- Logic Design:
- Circuit Design:
- Physical design:
- Layout verification:
- Fabrication and Testing:
- MODULE:
- Syntax:

7. RESULTS

Random numbers are generated with regarded to,

High Speed

Area

Power Dissipation

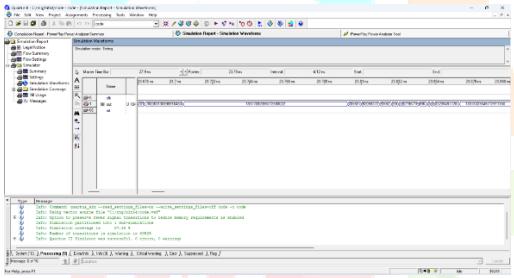

Fig.6: Simulation Results

PowerPlay Power Analyzer Status	Successful - Thu May 04 18:37:37 2023
Quartus II Version	9.1 Build 222 10/21/2009 SJ Web Edition
Revision Name	code
Top-level Entity Name	TOP64
Family	Cyclone II
Device	EP2C35F672C8
Power Models	Final
Total Thermal Power Dissipation	117.80 mW
Core Dynamic Thermal Power Dissipation	0.00 mW
Core Static Thermal Power Dissipation	79.95 mW
I/O Thermal Power Dissipation	37.85 mW
Power Estimation Confidence	Low: user provided insufficient toggle rate data

Fig.7: Power Dissipation

Flow Status	Successful - Thu May 04 14:19:57 2023
Quartus II Version	9.1 Build 222 10/21/2009 SJ Web Edition
Revision Name	code
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.8: Area Cnsumption

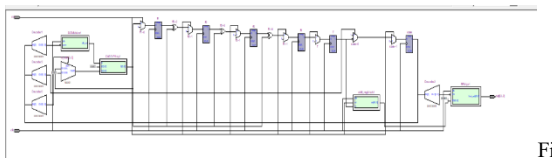

Fig.9: RTL Schematic

8. ADVANTAGES & APPLICATIONS

ADVANTAGES:

- Security Enhanced.
- Randomness Increased.

APPLICATIONS:

- Low-Cost authentication applications.
- Key generation applications.
- OTP applications.

9. CONCLUSION

A new design of a DCM-based TRNG for an easy implementation on FPGA devices has been presented. It exploits the dynamic capability of the DCMs hardware primitives to fine tune the phase difference between two clock signals. The metastability ingenerated by the latter signals is used as a randomness source. The required phase difference is automatically set by a simple FSM. A smart use of the CARRY4 hardware primitive further increases the randomness of the generated bits. Finally, a low-latency on-chip postprocessing scheme is also presented.

10. FUTURE SCOPE

FPGA-based TRNGs can have a significant impact in the future:

Cybersecurity: With the increase in cyber-attacks and data breaches, there is a growing demand for secure cryptographic systems. FPGA-based TRNGs can provide a high level of randomness, which is essential for generating secure encryption keys.

Internet of Things (IoT): With the proliferation of IoT devices, there is a growing need for secure and reliable communication channels. FPGA-based TRNGs can help provide secure and random keys that can be used for secure communication between IoT devices.

Blockchain: Blockchain technology relies on the generation of random numbers for the creation of new blocks. FPGA-based TRNGs can provide a reliable source of random numbers that can be used for block generation in blockchain systems.

REFERENCES

[1] 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.

[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] 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.

[4] R. Della Sala, D. Bellizia and G. Scotti, "A Novel Ultra-Compact FPGACompatible TRNG Architecture Exploiting Latched Ring Oscillators," in IEEE Trans. Circuits Syst. II, Exp. Briefs, vol. 69, no. 3, pp. 1672-1676, March 2022.

[5] N. N. Anandakumar, S. K. Sanadhya, and M. S. Hasmi, "FPGA-based True Random Number Generation Using Programmable Delays in Oscillatorrings," IEEE Trans. Circuits Syst. II, Exp. Briefs, vol. 67, no. 3, pp. 570- 574, March 2020.

[6] H. Martin, P. Peris-Lopez, J. E. Tapiador, and E. San Millan, "A New TRNG Based on Coherent Sampling With Self-Timed Rings," IEEE Trans.

BIOGRAPHIES

DAKEY SUDHIR

Assistant Professor, B.E. in Electronics & Communication Engineering. MVSREC.

BONALA PURUSHOTHAM

B.E. in Electronics & Communication Engineering

KAREE MANISH

B.E. in E Electronics & Communication Engineering

VANKALA BHANU PRAKASH

B.E. in E Electronics & Communication Engineering