Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, April : 2024

FPGA-BASED TRUE RANDOM NUMBER GENERATION USING CIRCUIT EXPLOITING LATCHED RING OSCILLATORS

K.NARESH, M.TECH[1]

P.VENKAT[2], P.UDAY KUMAR[3], PRADEEP JAIKAR[4], B.TEJAVANTH[5]

[1]Assistant Professor, Department of ECE,ELURU COLLEGE OF ENGINEERING AND TECHNOLOGY, A.P., India.

[2, 3,4, 5]Student,Department of ECE, ELURU COLLEGE OF ENGINEERING AND TECHNOLOGY, A.P., India.

ABSTRACT: 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. This paper proposes a new and efficient method to generate true random numbers in XILINX by utilizing . 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 FPGAbased 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.

INTRODUCTION

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.

PROPOSEDSYSTEM

Existing system Drawbacks

- While using ring oscillator the propogationdelay of each inverter is difficultto accurately predict.
- clockskew sensitivity

Proposed System:

- Secure communications
- Cryptography systems
- Sensor data encryption
- Gaming and gambling
- Hardware security modules(HSMs)
- Quality assurance and testing

Advantages

- Low power
- Low accessing time
- Efficiency

LITERATURE SURVEY

This section highlights the literature survey which has been done to review the critical points of the related works in recent days. In an irreversible circuit, if one bit informationislostthenatleastKTln2joulesofe nergyisdissipated.WhereKisBoltzmann's constant and T is absolute temperature. This was stated by Landauer R in 1961.

In 1973, Bennett proved that, KTln2 joules of energy dissipated due to information loss in irreversible circuit can be controlled by reversible logic where the reversible circuit allowstoreproducetheinputsfromoutputresu ltinginnoinformationloss.Healsoshowed thatreversiblesystemscandothesamecomput ationsastheclassicalorirreversiblesystems at same efficiency. This leads to the evolution of reversible logic based systems. Any reversible gate should have equal number of inputs and outputs such that, inputs can be recovered uniquely from outputs at any point of time.

D. Muthih and A.Arockia Bazil Raj [1] have presented a parallel architecture for designing high speed LFSR and explained that, BCH encoders and CRC operations are normally carried out by using LFSR. A

novel approach for high speed BCH encoder is proposed. This paper presents two key points. First, it presents a linear transformation algorithm for converting a serial LFSR into parallel architecture, which can be used for generating polynomials in CRC and BCH encoders. Secondly, anew approach is proposed to amend parallel LFSR into pipelining and retiming algorithm.

Inpaper[2],authorshavepresentedtwodesign approachesfordesigningreversible DFF with asynchronous set/reset which are optimized in terms of quantum cost, delay and garbageoutputs.Italsoincludesthedesignof3 bitLFSRusingtwodesignapproaches.The application of these FF's as LFSR is designed and discussed.

RELATED WORK

Cryptography: True random generators are crucial for generating encryption keys, ensuring the security of sensitive data and communication channels.

Simulation and Modeling: In scientific research and engineering, true random numbers are used to simulate complex systems, model probabilistic events, and conduct Monte Carlo simulations.

Gaming and Gambling: True random generators are employed in gaming and gamblingindustriestoensurefairgameplay,r andomoutcomes,andunbiasedresults in games and lotteries.

Statistical Sampling: True random numbers are utilized in statistical sampling techniques for selecting random samples from populations, ensuring representative data collection and accurate analysis.

Art and Creativity: True random generators are sometimes used as creative tools in art and music to generate random patterns, melodies, or visual compositions, fostering experimentation and innovation.

Randomized Testing: In software development and quality assurance, true random numbers are used to perform randomized testing, helping to identify bugs, vulnerabilities, and performance issues in software applications.

Randomized Algorithms: True random generators are integral components of randomized algorithms used in various computational tasks, such as sorting, searching, and optimization, to improve efficiency and accuracy.

Lottery and Gaming Systems: True random generators areused in lottery machines

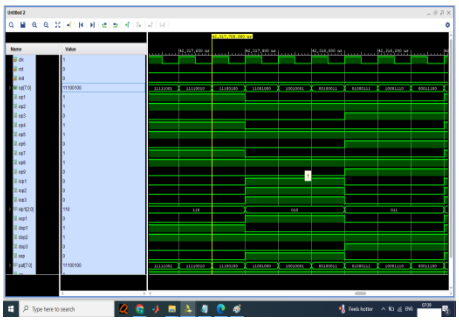
Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, April : 2024

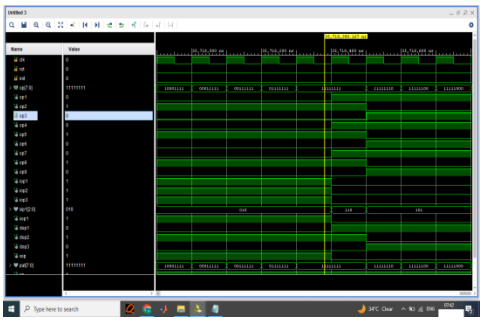
andgamingsystemstoensurefairnessandrandomnessinselectingwinningnumbers and outcomes.

Cryptocurrency and Blockchain: True random generators play a crucial role in generating random seeds and private keys in cryptocurrency systems, ensuring the security and integrity of transactions and blockchain networks.

Secure Authentication: True random numbers are utilized in secure authentication systemstogeneraterandomtokens,passwords,andauthenticationcodes,enhancing security and preventing unauthorized access.

SAMPLE RESULTS





CONCLUSION

A novel TRNG architecture that leverages the benefits of both the jitter of ring oscillators and the D-Latches' metastability has been proposed. A feedback strategy to randomly set the 4 LSBs of the control word defining the excitation time has been exploited to enhance the randomness and increase the entropy. The randomness of the raw response, showsthatalsowhensupplyvoltagevariationsareconsideredtheTRNGisabletoful-fillthe test requirements

Anew design of RO-based multiple clock generator is described and its implementation on Xilinx is presented in this project. The programmable delay LUTs has been used to achieve random jitter and to enhance the randomness. It has been demonstrated that the proposed implementation provides a very good area-throughput trade-off

REFERENCES

[1] C. Böhm and M. Hofer, Physical Unclonable Functions in Theory and Practice. NewYork, NY, USA: Springer, 2012.

[2] M.A. Qureshi andA. Munir, "PUF-rake:APUF- based robust and lightweight authentication and key establishment

protocol," IEEE Trans. DependableSecureComput.,earlyaccess,Feb.16,2021,doi:10.1109/TDSC.2021.3059454.

[3]S.Larimian,M.R.Mahmoodi,andD.B.Strukov,"LightweightintegrateddesignofPUF and TRNG security primitives based on EFLASH memory in 55-nm CMOS," IEEE Trans. Electron Devices, vol. 67, no. 4, pp. 1586–1592, Apr. 2020. [4] B. Yang, N. Mentens, M. Grujic, N. Mentens, and I. Verbauwhede, "ES-TRNG: A high-throughput, low-area true random number generator based on edge sampling," IACR Trans. Cryptograph. Hardw. Embedded Syst., vol. 2018, no. 3, pp. 267–292, 2018.

[5] C. Tokunaga, D. Blaauw, and T. Mudge,"Truerandomnumbergeneratorwith ametastability-basedqualitycontrol,"IEEEJ. Solid-State Circuits, vol. 43, no. 1, pp. 78–85, Jan. 2008.

[6] B. Dang et al., "Physically transient true random number generators based on paired threshold switches enabling Monte Carlo method applications," IEEE Electron Device Lett., vol. 40, no.

7, pp. 1096–1099, Jul. 2019.[7]O.Petura,U. Mureddu,N.Bochard,V. Fischer,andL.Bossuet,"AsurveyofAIS-20/31 compliant TRNG cores suitable for FPGA devices," in Proc. 26th Int. Conf. Field Program.LogicAppl.(FPL),Lausanne,Switzerland,2016,pp.1–10.

[8]B.JunandP.Kocher, "TheIntelrandom numbergenerator,"San Francisco, CA, USA, Cryptogr. Res. Inc.,White Paper, 1999, pp. 1–8.