True Random Number Generator using Avalanche noise

Pratik Dhane, Dhanraj Shelke, Prashant Dheple

Abstract- **In this study, we explore the development and implementation of a True Random Number Generator based on avalanche noise in a reversed-biased p-n junction, leveraging the 2N3904 transistor as a noise source. The circuitry is meticulously designed, encompassing several crucial components, each contributing to the noise generation and amplification process. A White Noise Generator produces symmetrical, zero-average noise from the reverse-biased p-n junction, ensuring that the generated noise is of high quality. To accommodate a single-supply voltage, a Virtual Ground is created, enabling biasing of subsequent op-amp stages. A Buffer stage is strategically positioned to prevent loading of the noise generator, while an Amplifier stage linearly amplifies the initial noise signal. Finally, a Current Switch (Comparator) determines the instantaneous noise polarity, yielding a digital signal that encapsulates the inherent randomness of the noise. This True Random Number Generator exhibits remarkable characteristics, including a high breakdown voltage, ensuring robust operation, and a substantial noise amplitude for discernibility. The output of this TRNG promises to enhance the security of cryptographic protocols, improve the fairness of gaming applications, and contribute to the accuracy of statistical simulations.**

Keywords- Random generator, Avalanche noise,TRNG.

I. Introduction

In the digital age, the quest for randomness has become increasingly vital. From cryptographic applications to secure data transmission, random numbers serve as the foundational building blocks for numerous facets of modern technology. However, achieving true randomness, a concept as elusive as it is fundamental, remains a significant challenge. This paper embarks on a journey into the world of True Random Number Generators (TRNGs), aiming to dissect their essence, discuss their significance, and explore their real-world applications.

The reliance on randomness in technology is ubiquitous. From securing sensitive data to generating cryptographic keys, random numbers are an essential component of numerous processes. In the realm of cryptography, pseudorandom numbers, which are generated using algorithms, have been the norm for decades. However, the inherent predictability of pseudorandom numbers leaves them vulnerable to attacks, undermining the security of the systems they protect. The demand for absolute randomness, therefore, has never been greater.Pseudorandom Number Generators (PRNGs), though efficient and widely used, exhibit predictable patterns due to their deterministic nature. They begin with a seed value and generate a sequence of numbers based on complex mathematical algorithms. While this approach suffices for many applications, it is not immune to predictability. Given a sufficient amount of data, an adversary may deduce the seed value, thereby compromising the security of the entire system.

A True Random Number Generator, in contrast, does not rely on predetermined algorithms or mathematical formulas to generate numbers. Instead, TRNGs exploit physical processes in the environment to produce numbers that are inherently random. These processes could involve various sources of entropy, such as electronic noise, radioactive decay, or even unpredictable user behaviors, like mouse movements. The outcome is a sequence of numbers that is theoretically unpredictable and therefore considered truly random.

The pursuit of true randomness is not merely a technological endeavor; it is a fundamental philosophical quest. In a world governed by deterministic laws, the idea of generating absolute randomness challenges our understanding of reality. Scientists and engineers strive to harness the inherent unpredictability of quantum mechanics, the chaotic nature of natural processes, or the minute details of human actions to create TRNGs that can withstand even the most advanced attacks.

The significance of TRNGs extends beyond cybersecurity. In fields such as statistical analysis, scientific research, and even entertainment, true randomness is invaluable. For example, in Monte Carlo simulations used in scientific research and engineering, the quality of random numbers directly influences the accuracy of the results. Poorly generated random numbers can lead to skewed or misleading conclusions.

TRNGs have found their place in a variety of real-world applications. One notable example is in the world of cryptography, where TRNGs are utilized to create truly secure encryption keys. Additionally, TRNGs are employed in secure communication systems, online gambling platforms, and lottery machines, where fairness and unpredictability are paramount. Moreover, they play a crucial role in randomized experiments in social sciences, ensuring the unbiased selection of subjects and eliminating potential biases.

In the following sections, we will dive deeper into the principles behind True Random Number Generators, exploring the various sources of entropy and the techniques employed to extract random data from them. We will also discuss the challenges associated with TRNGs, including issues related to bias, quality, and speed. Additionally, we will review notable TRNG designs and their real-world applications. Finally, we will contemplate the future of TRNGs in an ever-evolving technological landscape. In the quest for absolute randomness, True Random Number Generators represent a remarkable achievement, pushing the boundaries of what is possible in the world of data security and unpredictability. This paper aims to illuminate the intricacies of TRNGs and the pivotal role they play in the realm of modern technology and science.

II. Literature Review

The paper [1] presents a True Random Number Generator (TRNG) based on thermal noise that exploits the random fluctuations in the thermal energy of a resistor. The proposed TRNG uses a comparator to compare the voltage across the resistor with a reference voltage, and the comparator output is sampled and digitized to generate random numbers. The generated numbers are evaluated for randomness using statistical tests, and the results demonstrate that the proposed TRNG produces high-quality random numbers with good statistical properties. The proposed TRNG has potential applications in various cryptographic systems that require high-quality random numbers. The researchers [2] aimed to develop a True Random Number Generator (TRNG) based on a Boolean chaotic oscillator. They sought to model, implement, and evaluate the TRNG's performance, with a focus on generating high-quality random numbers for cryptographic applications. What they achieved was the successful modeling, construction, and CMOS implementation of the TRNG. They demonstrated that the TRNG could produce random numbers with strong statistical properties, as confirmed by the NIST statistical tests. The study showcased the TRNG's potential as a reliable source of randomness for cryptographic systems. The study [3] aimed to develop a True Random Number Generator (TRNG) using FPGA-based ring oscillators (ROs) with programmable delay lines (PDLs) to enhance randomness and reduce correlation. Results indicated that the proposed TRNG achieved competitive area-throughput trade-offs, outperforming previous FPGA-based TRNG designs in terms of area utilization. Tests demonstrated that the 32 ROs within the TRNG were uncorrelated. The TRNG exhibited an entropy rate of 7.9946 bits per byte, exceeding minimum requirements, and maintained distinct output sequences across multiple restarts. Rigorous NIST statistical testing confirmed its suitability for secure applications. This paper [4] introduces a chaos-based True Random Number Generator (TRNG) and a Sliding Mode Controller (SMC) for synchronization, suitable for FPGA implementation. A discrete SMC is used to synchronize master-slave chaotic systems. The TRNG design incorporates a hybrid function with the El-Gamal algorithm, ensuring randomness through Shannon's entropy and NIST tests. Implementation on an FPGA is demonstrated, and TRNG sequences are evaluated using NIST-800-22 standards. However, the paper lacks discussion on designing real random numbers and chaos-based synchronization control. This paper [5] introduces an optical random number generator circuit based on single-photon avalanche diodes (SPADs) in 180 nm CMOS technology. It generates two-bit random numbers by detecting photon populations in a fixed time interval using three SPADs. To reduce dark count rate and after-pulsing, one SPAD is biased in Geiger mode, while the other two are in the hold-off phase. The circuit is validated using a SPAD circuit model, achieving 16 pj/bit energy consumption and an 80 MHz generation rate. NIST statistical tests confirm its randomness, and the paper includes circuit operation principles, timing, and schematic diagrams. This paper [6] introduces a novel true random number generator (TRNG) concept based on FPGA flip-flop resolve times, distinct from deep-metastability-based TRNGs. It discusses design considerations, including flip-flop operating point adjustment, randomness extraction, and circuit fitting. The TRNG offers stable statistical quality despite process, voltage, and temperature variations and employs an adaptive feedback loop for robustness. The paper also mentions enhancing another metastability-based TRNG with a proportional-integral (PI) controller and programmable delay lines (PDLs) for precision.

Mouse movement [7] is a cost-effective and practical source for generating random numbers in PC applications. Analog-to-digital transformation is used to convert mouse movement data into usable digital form. However, inherent patterns and similarities in mouse movements must be addressed to ensure true randomness. Chaos-based methods are employed to introduce unpredictability and sensitivity to input variations. The size of the input space is kept large to resist brute-force attacks. Three chaos-based approaches are proposed: discretized 2D chaos maps, spatiotemporal chaotic systems, and the 'MASK' image encryption algorithm. Experiments reveal that the 'MASK' algorithm outperforms other methods, offering enhanced randomness, though with a slightly longer processing time. Mouse movement remains a

practical and secure source of random numbers for PC applications. The paper [8] discusses a novel design method for discrete time chaos-based true random number generators (TRNGs) using the skew tent map as a case study. The authors calculate optimum parameter values for maximum randomness in the TRNG using a mathematical model. The paper explores the statistical characteristics and randomness performance of the generated bitstream in terms of a practical information measure called T-entropy. It also presents a minimalist circuit implementing the skew tent map and provides simulation results. The paper mentions that previous variants of TRNGs utilize arrays of high power-consuming ring oscillators, but they are not suitable for mobile applications due to various limitations. This paper [9] presents Galois and Fibonacci ring oscillators for high-speed true random number generation using logic gates exclusively. True randomness can be assessed by examining the standard deviation's time evolution. The restart approach greatly enhances entropy rates compared to classical ring oscillators. It introduces restart and continuous modes and a novel sampling method to boost entropy. These oscillators are touted as more effective for logic-based random number generation. The paper also explores the oscillating nature of standard deviation curves and potential randomness extraction near signal edges, acknowledging the impact of internal metastability events on entropy. The research paper[10] employs architecture and circuit design techniques to minimize data-dependent noise in random bit streams. The proposed model has combined thermal noise with chaotic True Random Number Generators (TRNGs) to enhance randomness. Results show a 2 Mbit/s random bit rate, passing various tests. Limitations include a lack of data on TRNG efficiency and a failure to compare the TRNGs with existing designs.The paper [11] introduces a pseudo-random number generator employing wavelet theory. The scaling function produces real number sequences, with specific binary values extracted. The generated sequences pass statistical tests, but these tests lack detailed descriptions. The paper doesn't address potential cryptographic vulnerabilities and lacks justification for recommended sequence lengths. The proposed model [12] focuses on evaluating a True Random Number Generator (TRNG) using statistical tests and de-skewing to enhance randomness. The TRNG was synthesized using Xilinx tools but initially showed bias and correlation. The paper lacks information regarding scalability, performance under varying FPGA conditions, and comparative analysis with existing TRNGs. The paper [13] introduces a pseudo-chaotic number generator (PCNG) utilizing entropy from the Linux kernel, employing recursive filters with non-linear functions. The PCNG passes various statistical tests, indicating strong performance. The paper lacks discussion on computational efficiency, time complexity, and potential vulnerabilities or biases in the generated random numbers. The proposed model [14] introduces a Parallel-True Random Number Generator (P-TRNG) by combining two TRNGs on a Raspberry Pi platform, significantly increasing the bit generation rate. The P-TRNG surpasses expectations, offering applications in sensitive transactions. It lacks a comprehensive scalability analysis and doesn't delve into potential challenges associated with parallel TRNG implementation. The study [15] introduces a True Random Number Generator (TRNG) circuit using programming sequences applied to a memory array. It converts resistance values into a bit stream, which successfully passes eleven NIST tests. It details the TRNG implementation and performance, but it lacks a comprehensive discussion of potential limitations or drawbacks, leaving room for further analysis and scrutiny. The paper [16] introduces a Polynomial Modulator (PM) to enhance the unpredictability and extend the sequence length of linear-feedback shift registers (LFSRs) in random number generation. By dynamically altering the LFSR polynomials, this approach generates sequences over 4,000 times longer before repetition. While the paper demonstrates improved performance, it lacks a comprehensive computational analysis, comparisons with alternative methods, and discussions on potential security vulnerabilities. The study[17] explores an FPGA-based true random number generator (TRNG) using oscillator rings and spectral analysis. The FPGA implementation achieves a high bit rate of 300 Mbit/s, demonstrating genuine randomness, not pseudorandomness. However, the paper lacks discussion regarding optimization challenges, constraints, and comparative analysis with other TRNG methods, leaving room for a more comprehensive evaluation of the proposed approach.

The paper [18] proposes a high-speed reconfigurable True Random Number Generator (TRNG) design based on a Current Starved Ring Oscillator (CSRO) using Resistive RAM (RRAM) as the source of randomness. The paper discusses the utilization of intra-device stochastic variations in RRAM switching parameters and Random Telegraph Noise (RTN) to generate random numbers in the TRNG. The effect of RTN on the jitter of CSRO oscillations is demonstrated in the paper. The paper also presents a methodology to reconfigure the TRNG for generating new random numbers. The proposed 10-bit TRNG is validated using the NIST test suite for randomness in the data stream. The energy/bit for random number generation is reported as 22.8fJ, and the speed of random data generation is 6MHz.The paper also investigates the security vulnerabilities and countermeasures of the proposed TRNG.The paper [19] discusses the use of phase jitter in oscillator rings to generate random bits, which are then processed using post-processing techniques to improve their quality and randomness. Another approach mentioned is the use of arbiter-based Physical Unclonable Function (PUF) structure to generate random bits by driving the arbiter into the metastable state.Various post-processing techniques, such as

resilient functions and extractor functions, are used to improve the quality and randomness of the generated random bits. The TRNG system proposed in this paper provides randomness, robustness, low area overhead, and high throughput. The paper [20] proposes a scheme for a high-efficiency quantum random number generator (RNG) using avalanche photodiodes (APDs). The scheme utilizes an effective extractor with a simple time bin encoding method to convert avalanche pulses of APDs into high-quality random numbers (RNs) that are robust to slow varying noise. The proposed system does not require a light source, enhancing its robustness. The proof-of-principle system achieves a random bits generation rate of 0.69 Mbps with double APDs and 0.34 Mbps with single APD. The results suggest the potential availability of a high-speed RNG chip based on the proposed scheme with an integrable APD array.The paper [21] presents a new physical random number generator based on the dark pulses thermally generated in single photon avalanche photodiodes operating in the Geiger mode. The proposed random number generator produced nearly 50% zeros and 50% ones, making it suitable for quantum cryptography systems. The generator uses one single-photon avalanche photodiode without the need for an optical source, resulting in lower cost compared to other random number generators. The method used and electronic parts of this generator are simpler compared to other random number generators. The generator utilizes active quenching and passive quenching techniques to reduce the dead time and improve efficiency. Overall, the paper presents a novel random number generator based on single-photon avalanche photodiodes, which offers simplicity, lower cost, and suitable performance for quantum cryptography systems. The paper [22] discusses the development of a true random number generator (RNG) based on set variability in a resistive switching memory (RRAM). The RNG relies on a single RRAM device, which is repeatedly programmed at a constant voltage close to the nominal set voltage, resulting in a bimodal distribution of resistance. The randomness of the RNG in the RRAM circuit is demonstrated by verifying that there is no correlation between successive RRAM states in a sequence of generated bits. The resistance value after a random set displays a bimodal distribution with high resistance state (HRS) and low resistance state (LRS) sub-distributions, and careful adjustment of the applied voltage allows for fine balancing of these sub-distribution. The paper also proposes a regeneration circuit to allow for ideal digital RNG and discusses the optimization of the RNG process by choosing the parameters in the pulse sequence. Overall, the paper presents a novel approach to achieving true randomness in RNG using RRAM and demonstrates its effectiveness through experimental results.The paper [23] discusses different methods to harvest electrical noise in True Random Number Generators (TRNGs), including early amplify noise based on amplifier, phase jitter based on oscillator, the effect of electrical noise on metastable behavior, and amplify noise based on chaos circuits. The paper also mentions the importance of post-processing technologies in TRNGs to reduce statistical flaws and provide prediction resistance. Additionally, the paper highlights the need for TRNGs evaluation, including entropy estimations and statistical tests, to ensure the reliability of the generated random bits. The spectral density of thermal noise, which is an ideal entropy source for TRNGs, is discussed, and its independence with frequency is emphasized. The paper concludes by summarizing the current state of TRNGs using electrical noise and pointing out possible future directions.

The paper [24] evaluates the relationship between the sampling rate and the autocorrelation function of temporal waveforms generated from a superluminescent diode (SLD) and a semiconductor laser. It investigates two types of random number generators: noise-based and chaos-based generators, using the SLD as a noise source and unidirectionally coupled semiconductor lasers for chaos generation. The paper mentions that the randomness in SLDs originates from amplified spontaneous emission and in chaotic lasers from nonlinear amplification of intrinsic noise by chaotic dynamics. The entropy rate can be evaluated from the maximum Lyapunov exponent. The paper discusses the difficulty in passing certain tests of randomness, such as the "block frequency," "runs," "non overlapping-template," and "random-excursions" tests, for both single-bit and multibit generation schemes. The paper acknowledges the importance of theoretical works in guaranteeing the randomness of these optical random number generators. Paper [25] says, Random number generators can be divided into two categories: pseudo-random number generators (PRNGs) and true random number generators (TRNGs). PRNGs are deterministic processes designed to generate sequences that appear random, while TRNGs generate sequences from physical phenomena such as nuclear decay, thermal noise, cosmic radiation, or keyboard strokes. PRNGs are widely used due to their excellent statistical properties and easy digital implementations, but they require a TRNG as a source of entropy. Most integrated TRNGs use one of three basic methods for generating random numbers from a thermal noise source.

III. Methodology

Avalanche noise occurs in semiconductor devices, such as diodes or transistors, when they are operated in a reverse-biased state and experience a sudden and unpredictable increase in current due to the generation of electron-hole pairs within the device's depletion region.

Here we are using transistor 2N3904(NPN bipolar junction transistor) for the generation of avalanche noise because of factors such as, the breakdown voltage of 2N3904 at 10μA is

measured as 10.80V which is a crucial parameter as it signifies the voltage at which the avalanche effect occurs, leading to noise generation. At a current level of 10μA, the 2N3904 exhibits a noise amplitude of 400mVpp (millivolts peak-to-peak). A 2N3904 is the preferred choice for avalanche noise generation due to its combination of a high breakdown voltage and consistent noise performance. The higher breakdown voltage of the 2N3904 suggests that it can operate at a relatively higher voltage, making it robust for avalanche noise generation. A higher noise amplitude indicates that the 2N3904 can produce a more significant and discernible noise signal.

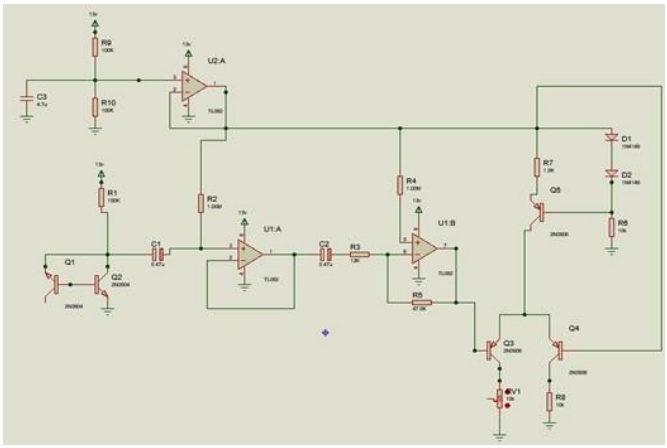

Fig. 1: Avalanche Noise Generator and Digital output generator

The circuit designed for generating true random numbers using avalanche noise in a reversed-biased p-n junction, primarily utilizing the 2N3904 transistor, can be divided into several distinct blocks, each serving a specific purpose in the noise generation and amplification process.

White Noise Generator: This is the initial stage of the circuit responsible for generating symmetrical, zero-average noise from the reverse-biased p-n junction of the 2N3904 transistor. It comprises two 2N3904 transistors, Q1 and Q2, along with resistor R1.Transistor Q1's collector is not connected to any source, making Q1 to work as a diode in reverse bias. The key to achieving symmetrical noise is to bias the 2N3904 with a very low reverse current, approximately 50nA. The emitter current of Q2 (Ie2) is determined by R1, creating a base current (Ib2) that flows into the reverse-biased emitter-base junction of Q1. The result is a symmetrical noise voltage, with a small signal gain close to unity, served at the collector of Q2

Virtual Ground: Since the circuit operates with a single supply voltage, a virtual ground (labeled Vref) at Vcc/2 is required to bias subsequent op-amp stages. This virtual ground is created using a voltage divider consisting of equal resistors R9 and R10 of 100k ohm, followed by a unity-gain buffer realized with op-amp U2: A.

Buffer: Positioned between the noise generator and the amplifier, this buffer comprises half of the U1: A op-amp, resistor R2, and capacitor C1. It serves to prevent loading of the noise generator by the subsequent amplifier stage, ensuring minimal current draw from the noise source. Resistor R2 biases the amplifier around the virtual ground, and capacitor C1 removes any DC components from the signal.

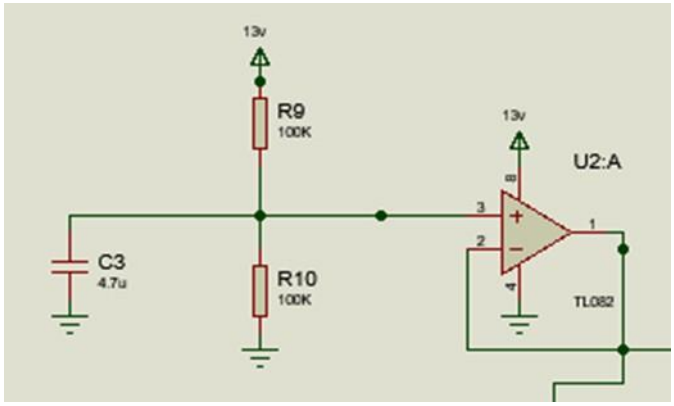

Fig. 2: Vref Circuit

Amplifier: Following the buffer, the amplifier stage amplifies the noise signal. It employs the other half of op-amp U1: A, capacitors C2, and resistors R3, R4, and R5. The gain of this stage is set by the ratio of R5 to R3 and provides linear amplification of the noise signal. This amplification brings the initial noise signal from 250mVpp to approximately 1Vpp around the virtual ground.

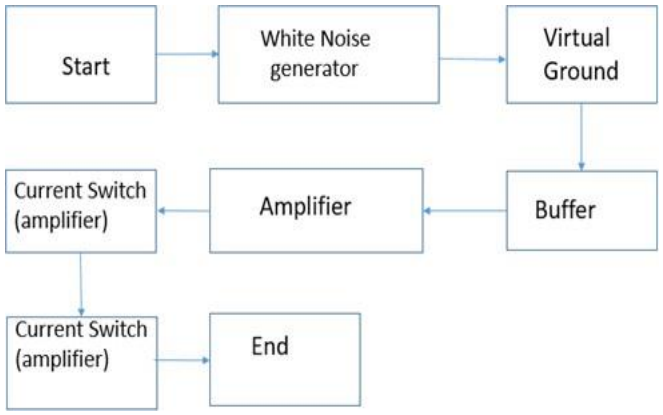

Fig.3: Components of the TRANG circuit

Current Switch (Comparator): The final stage of the circuit is the current switch, which serves as a comparator. It determines whether the instantaneous noise voltage is positive or negative with respect to the virtual ground (Vref). This block comprises a constant current generator (D1, D2, Q5, R6, and R7) and a differential pair (Q3 and Q4) with resistive loads (R8 and R9). The constant current generator ensures a stable reference current (Ig) is available. The differential pair functions as a current switch, steering the constant current between R8 and RV1 based on the voltage at the base of Q3.

When the voltage exceeds a threshold, Q3 or Q4 turns off, creating a digital signal that represents the randomness of the noise signal.

IV. Analysis

The noise characteristics of a circuit were investigated using ngspice simulations. The circuit design went through an initial conceptual phase followed by iterative refinement through simulation. Each node in the schematic diagram was labeled with progressive numbers for reference in the netlist. The simulations were conducted using ngspice, and the simulation output graphs can be seen in Fig. 4.

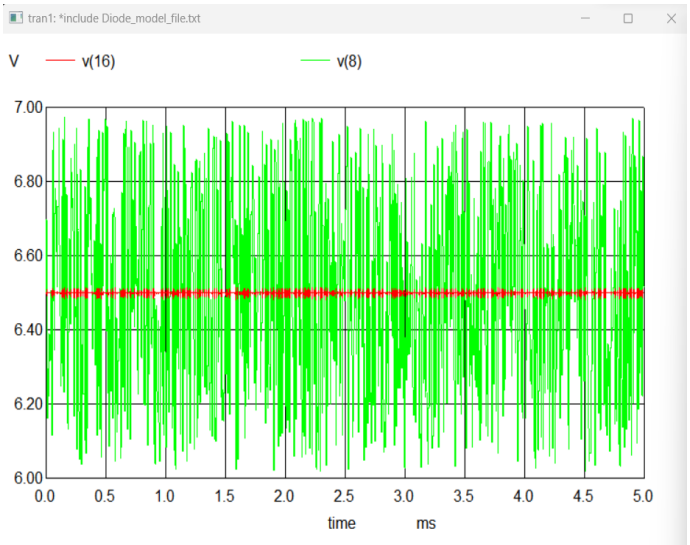

Fig. 4: Analog Noise output

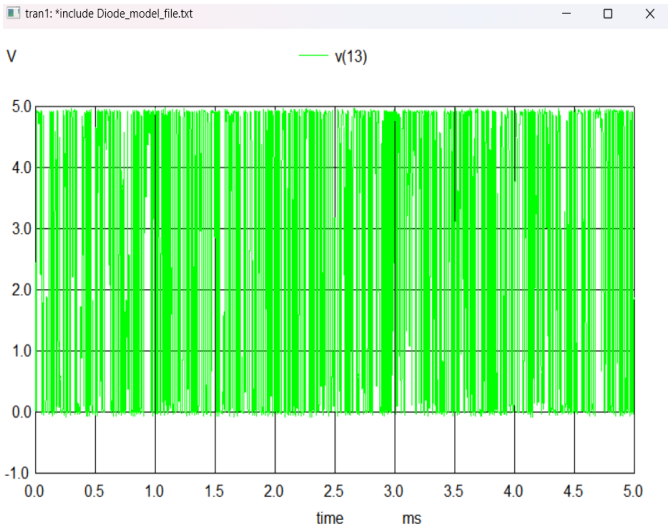

Fig. 5: Digital Output (ngspice simulated)

In Fig.4 and Fig.5, time-domain signals were investigated, including v(8) representing the output noise of the amplifier and v(13) indicating the collector of Q3, associated with digital signal processing. These simulations aimed to provide insights into the noise characteristics that the Avalanche noise generated is truly random in nature.

The Arduino code reads analog voltage levels from a connected analog pin. It does so by repeatedly reading the voltage and comparing it to a set threshold (0.06 V). When the voltage surpasses the threshold, it is considered a received "1," otherwise, it's treated as a "0." The code stores these received bits in an array. This process repeats for a fixed number of times as per our random digit requirement. The bits stored in the array are accessed in a loop and are multiplied with the 8421-weights format to get digital value. The 8421 can give random numbers from 0 to 15 decimal form.

V. Novelty

The novelty of this research lies in the development and implementation of a True Random Number Generator (TRNG) that leverages the phenomenon of avalanche noise in a reversed-biased p-n junction, with a specific focus on using the 2N3904 transistor as a noise source. Several key aspects of this TRNG set it apart from existing methods:

1) **Avalanche Noise Source:** Unlike many other TRNGs that rely on various physical processes, this TRNG harnesses avalanche noise generated in the 2N3904 transistor. This unique source of entropy is crucial in ensuring the generated numbers are inherently random.

2)**High Breakdown Voltage and Noise Amplitude:** The 2N3904 transistor's characteristics, such as a high breakdown voltage and substantial noise amplitude, set it apart as an ideal choice for avalanche noise generation. These features are essential for the robust operation of the TRNG.

3)**White Noise Generation:** The use of a White Noise Generator as the initial stage ensures that the generated noise is symmetrical, zero-average, and of high quality. This is a novel approach to ensuring the quality of the random numbers produced.

One of the major uniqueness of this TRNG is that we are using an arduino for reading the output. This makes the operation of reading and converting the output to a decimal value easy .We are reading output in 4-bit loops, which have 16 lengths and 16 random values from 0 to 15. Here we can change the range of random numbers by changing the length of the loop in arduino code.

VI. Result and Discussion

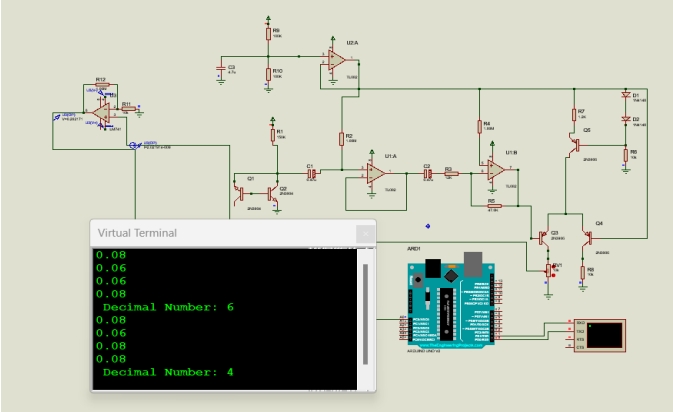

Fig. 6: True random number generated

The analog voltage levels read by the arduino are 0.08, 0.06, 0.06, 0.08. The code compares these values with the said threshold i.e.0.06, we get the sequence as 0, 1, 1 ,0. Therefore by using the binary to decimal conversion by multiplying each bit by its weights i.e.8421, [(8*1) + (4*1) + (2*1) + (1*0)], we get 6 as our random number.

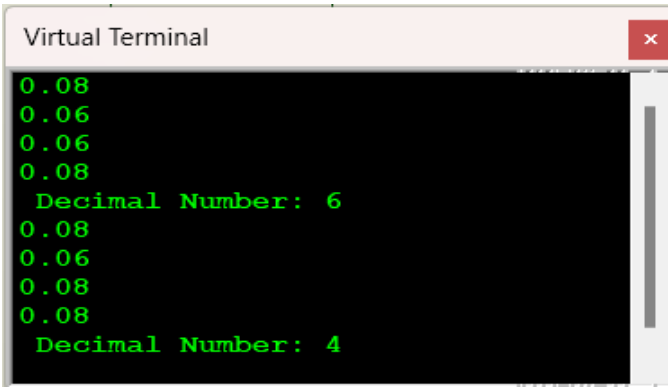

Fig. 7: Output of Arduino on virtual terminal

Similarly, if the values are 0.08, 0.06, 0.08, 0.08 we get the sequence 0, 1, 0, 0. Therefore the random number generated is 4.

VII. Conclusion

The development and implementation of a true random number generator (TRNG) based on avalanche noise has been an effective approach for generating unpredictable and unbiased random numbers. Avalanche noise, which occurs in semiconductor junctions, provides a source of inherent randomness that is highly suitable for cryptographic applications

References :

1) Zhun, Huang, and Chen Hongyi. "A truly random number generator based on thermal noise." *In ASICON 2001. 2001 4th International Conference on ASIC Proceedings (Cat. No. 01TH8549), pp. 862-864. IEEE, 2001.*
2) Myunghwan Park, John C.Rodgers, Daniel P.Lathrop "True random number generation using CMOS Boolean chaotic oscillator" *Publish in Research gate MicroelectronicsJournal46(2015)1364–1370*
3) N. Nalla Anandakumar; Somitra Kumar Sanadhya; and Mohammad S. Hashmi "FPGA-Based True Random Number Generation Using Programmable Delays in Oscillator-Rings" *DOI 10.1109/TCSII.2019.2919891, IEEE Transactions on Circuits and Systems II: Express Briefs.*
4) T.L.LIAO, P.Y.WAN, AND JUN-JUH YAN "Design and Synchronization of Chaos-Based True Random Number Generators and Its FPGA Implementation"*Digital Object Identifier 10.1109/ACCESS.2022.3142536 publish in IEEE Access.*
5) Soghra Ejdehakosh, Misagh Ansarian, Mohammad Azim Karami, "A new optical random number generator circuit design using single-photon avalanche diodes" *Published in Optik - International Journal for Light and Electron Optics 224 (2020) 165698.*
6) Piotr Zbigniew Wieczorek "An FPGA Implementation of the Resolve Time-Based True Random Number Generator With Quality Control" *IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—I: REGULAR PAPERS.*
7) Qing Zhou, Xiaofeng Liao, Kwok-wo Wong, Yue Hu "A True Random Number Generator Based on Mouse Movement and Chaotic Cryptography" *ResearchGate June2009.*
8) Ihsan Cicek, Ali Emre Pusane, Gunhan Dundar, "A novel design method for discrete time chaos based true random number generators" *INTEGRATION, the VLSI journal June 2013.*
9) Markus Dichtl1 and Jovan Dj. Goli´, "High-Speed True Random Number Generation with Logic Gates Only" *P. Paillier and I. Verbauwhede (Eds.): CHES 2007, LNCS 4727, pp. 45–62, 2007.*
10) Vincent von Kaenel, Toshinari Takayanagi "Dual True Random Number Generators for Cryptographic Applications Embedded on a 200 Million Device Dual CPU SoC" *IEEE 2007 Custom Integrated Circuits Conference (CICC)*
11) Jengnan Tzeng, I-Te Chen*, Jer-Min Tsai "Random Number Generator designed by the divergence of scaling functions" *2009 Fifth International*

Conference on Intelligent Information Hiding and Multimedia Signal Processing

12) Sammy H. M. Kwok, Edmund Y. Lam "FPGA-based High-speed True Random Number Generator for Cryptographic Applications" *IEEE 2017.*
13) Mohammed Abutaha, Safwan El Assad, Ons Jallouli, Audrey Queudet, Olivier Deforges , "Design of a Pseudo-Chaotic Number Generator as a Random Number Generator" *IEEE 2016.*
14) Thomas Arciuolo and Khaled M. Elleithy "Parallel, True Random Number Generator (P-TRNG): Using Parallelism for Fast True Random Number Generation in Hardware " *2021 IEEE 11th Annual Computing and Communication Workshop and Conference*
15) Jeremy Postel-Pellerin, Hussein Bazzi, Hassen Aziza, Pierre Canet, Mathieu Moreau, Vincenzo Della Marca, Adnan Harb "True Random Number Generation Exploiting SET Voltage Variability in Resistive RAM Memory Arrays" *IEEE 2015*
16) Mangi Han and Youngmin Kim"Unpredictable 16 bits LFSR-based True Random Number Generator" *ISOCC 2017 IEEE*
17) Knut Wold, Slobodan Petrovic, "Optimizing Speed of a True Random Number Generator in FPGA by Spectral Analysis" *2009 Fourth International Conference on Computer Sciences and Convergence Information Technology*
18) Rekha Govindaraj, Swaroop Ghosh, and Srinivas Katkoori "CSRO based Reconfigurable True Random Number Generator using RRAM" *2018 IEEE IEEE Transactions on Very Large Scale Integration (VLSI) Systems*.
19) Majzoobi, Mehrdad, Farinaz Koushanfar, and Srinivas Devadas. "FPGA-Based True Random Number Generation Using Circuit Metastability with Adaptive Feedback Control." *Cryptographic Hardware and Embedded Systems – CHES 2011. Ed. Bart Preneel & Tsuyoshi Takagi. LNCS Vol. 6917. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011. 17–32.*
20) Fang-Xiang Wang,Chao Wang, Wei Chen,Shuang Wang,Fu-Sheng Lv, De-Yong He, Zhen-Qiang Yin, Hong-Wei Li,Guang-Can Guo,and Zheng-Fu Han, "Robust quantum random number generator based on avalanche photodiodes" *February 2015 Journal of Lightwave Technology 33(15).*
21) Shelan Khasro Tawfeeq "A Random Number Generator Based on Single-Photon Avalanche Photodiode Dark Counts"*JOURNAL OF LIGHTWAVE TECHNOLOGY, VOL. 27, NO. 24, DECEMBER 15, 2009*
22) S. Balatti, Student Member, IEEE, S. Ambrogio, Student Member, IEEE,Z.-Q. Wang, and D. Ielmini, Senior Member, IEEE "True random number generation by variability of resistive switching in oxide-based devices" *published in IEEE xplore 2015*
23) LISHUANG GONG1 , JIANGUO ZHANG1 , HAIFANG LIU1 , LUXIAO SANG1 , AND YUNCAI WANG 1,2 "True Random Number Generators Using Electrical Noise" *Digital Object Identifier 10.1109/ACCESS.2019.2939027*
24) Taiki Yamazaki and Atsushi Uchida, Member, IEEE "Performance of Random Number Generators Using Noise-Based Superluminescent Diode and Chaos-Based Semiconductor Lasers" IEEE JOURNAL OF SELECTED TOPICS IN QUANTUM ELECTRONICS, VOL. 19, NO. 4, JULY/AUGUST 2013
25) Jeremy Holleman, Student Member, IEEE, Seth Bridges, Member, IEEE, Brian P. Otis, Member, IEEE, and Chris Diorio, Member, IEEE "A 3micro W CMOS True Random Number Generator With Adaptive Floating-Gate Offset Cancellation" *IEEE JOURNAL OF SOLID-STATE CIRCUITS, VOL. 43, NO. 5, MAY 2008*