ISSN: 2395-1680 (ONLINE)
DOI: 10.21917/ijme.2026.0379

AN EFFICIENT AND LOW POWER SPAD BASED QUANTUM RANDOM NUMBER GENERATOR USING NLFSR FOR SECURE CRYPTOGRAPHIC APPLICATIONS

Vinod Babu Pusuluri, Shyam Perika, Bhanu Sri Venkata Vamsi Pandiri and Yamini Menda
Department of Electronics and Communication Engineering, Rajiv Gandhi University of Knowledge Technologies, India

Abstract

Random number generation is very useful and highly applicable in cryptographic applications, and also true randomness is highly advantage for secure and data protection. Actual pseudo random generators not having enough entropy and may get predictability. Quantum Random Number Generators (QRNGs), based on quantum phenomena like single photon detection and provides enhanced unpredictability and security. In this work, we present the design and hardware realization of a SPAD (Single Photon Avalanche Diode) based Quantum Random Number Generator using a complete RTL to GDS flow. A behavioural Verilog model of SPAD operation was designed, and launching photon pulse detection, dead time effects and dead time effects. The design was simulated using several EDA tools are used to validate functionality. Thereafter, the RTL was Synthesized, Placed, Routed and verified to generate a GDSII layout. The proposed implementation illustrates a implementable strategy for integrating quantum enhanced randomness into secure hardware systems. The RTL to GDSII affirmation of compatibility for Application Specific Integration Circuit (ASIC) fabrication, enabling cryptographic applications such as Quantum Key Distribution (QKD) and hardware security module for low power circuits. By using Non-linear feedback shift Register (NLFSR) to strengthen randomness extraction and output Bit rates. Resilient randomness statistics verified by NIST test, and a total power consumption of only 0.272 m Watts noticeably less than legacy CMOS random number generators. So our work presents a scalable architecture for next-generation quantum entropy generators in secure communication systems, and also achieved better timing performance, power consumption, and randomness characteristics.

Keywords:

SPAD (Single Photon Avalanche Diode), QRNG (Quantum Random Number Generator), ASIC Fabrication, NLFSR (Non-Linear Feedback Shift Register)

1. INTRODUCTION

We know cryptographic communication systems mainly depends on high standard random number sources to get secure key generation and better encryption and also data protection. Software generated pseudorandom numbers are inbuild predictable test patterns that can easily detected by hackers [1], [2]. This may weakens cryptographic security, mainly in sensitive applications such as embedded communication modules and quantum key distributions [3], [4]. So these quantum random number generators (QRNG) are highly used present days because of their proficiency to provide better randomness inferred from actual quantum phenomena. So this research explores SPAD (Single Photon Avalanche Diode)–based QRNG implemented using the osu035 process design kit (PDK) [5]. Due to lacks an actual alternative SPAD modelor component in the PDK, the system used the BPW21 silicon photodiode from the eSim toolset [6] to emulate photon detection. This replacement may introduces small amount of challenges related to device modelling accuracy,it slightly impacts photon detection efficiency and noise characterization. Previous QRNG designs takes frequently bulky optical setups or bulky off-chip photon detectors, complicating integration into CMOS technology [7] and also increasing power consumption. So in our SPAD implementation we had faced so many challenges to reduce dead time, power, and on chip area while maintaining high throughput. Post processing techniques such as Non Linear Feedback Shift Registers (NLFSRs) [8] have been used in work to increase random bit generation rates and improve randomness.

This work presents a behavioural Verilog model that includes pulse detection, dead time effects modelled at 50 micro seconds, and entropy monitoring using a 64-bit NLFSR (XOR of bits 63, 53, 1 and 0). The core frequency of operation is set at 0.5 GHZ, and our target bit rate is 10 Mbps. The SPAD operates at 10 V with a breakdown voltage around 20 V, for which to get efficiency of 89.9 %. The digital design took almost core area of 56,841 square microns and balanced the throughput.

The main contributions of this work include:

- Implementation of a SPAD based QRNG with detailed RTL to GDSII design flow in the osu035 PDK process [9], embedding real photodiode behaviour via eSim's BPW21 model.
- Use of a 64-bit NLFSR as a post processing block to boost randomness extraction and increase output bit rate.
- Manifestation of low power consumption measured at approximately 0.272 m W, superior to typical CMOS based RNGs.
- Comprehensive validation of timing efficiency with positive slack margins and robust randomness verified by NIST tests.
- Arrangement of a scalable frame work for embedding quantum randomness in secure hardware applications such as quantum key distribution and hardware security modules.

2. ARCHITECTURE OF QUANTUM RANDOM NUMBER GENERATOR

The proposed architecture illustrates that how our work interconnects the different components to generate efficient random numbers for secure cryptographic applications. Here the Fig.1 depicts proposed SPAD based quantum random number generator by detecting the single photon from the light source and then corresponding comparator compares the photon energy from the diode response with threshold energy which fed into as input signal to the RNG generator,so that RNG will generate the true random numbers by using RTL logic.Generally, if nothing was there before that RNG that random numbers might considered as pseudo random numbers but we have choosen quantum based diode to generate random numbers when only it detect photons.

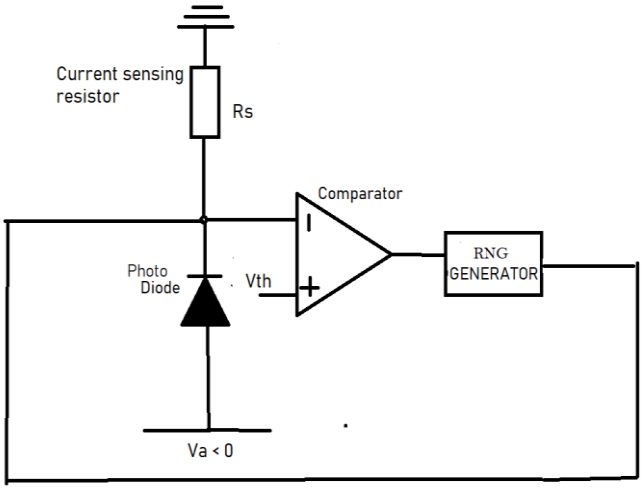

Fig.1. Architecture of active quenching circuit using SPAD

2.1 SPAD BASED DIODE OPERATION

A Single Photon Avalanche Diode (SPAD) is a semiconductor photodetector intended to detect single photons with high sensitivity and strict timing. It functions based on P N junction reverse biased beyond its breakdown voltage, a state known as Geiger mode. In this mode, the electric field within the diode is so strong that the ingestion of even a single photon generates a charge carrier that provokes a self-sustaining avalanche current. This yields in a sharp and easily detectable electrical pulse marking the photon's arrival [10]-[12].

This graph in Fig.2 clarifies the relationship between current and voltage for different types of photodiodes specifically SPAD & Si PM, avalanche photodiodes (APDs), and conventional photo diodes [13], [14] as the device is driven from forward bias into various reverse bias regimes.

SPAD & Si PM (Single Photon Avalanche Diode & Silicon Photomultiplier) Operates above the break down voltage in "Geiger mode". Here, a single photon can trigger a full avalanche breakdown, emanating in a sudden large current pulse. This region allows SPADs to detect single photons [15]-[17].

The Geiger mode is unique to SPADs and Si PM, where the bias voltage is set above the breakdown; the device evolves into digital and more meticulous to the Quantum technology, and is used to count arrival of individual photon instead of measuring light intensity.

However, in photon-based communication using SPAD (Single photon Avalanche Diode) technology, information is transferred as follows:

The sender encodes data into photons, that passes through an optical medium like fibre or free space to the receiver. When these photons reaches at the receiver, the SPAD detects single photons with extremely high sensitivity by generating an avalanche current from each detected photon. This Avalanche current creates a sharp electrical pulse corresponding to the photon's arrival, effectively converting the photon signal into electronic data pulses. These pulses are then processed to reconstruct the transmitted information.

The SPAD's has fast reflex and able to detect individual photons make it supreme for high speed, low light photon communication systems. Classical and quantum communication both utilize light, but they differ essentially in how they encode information.

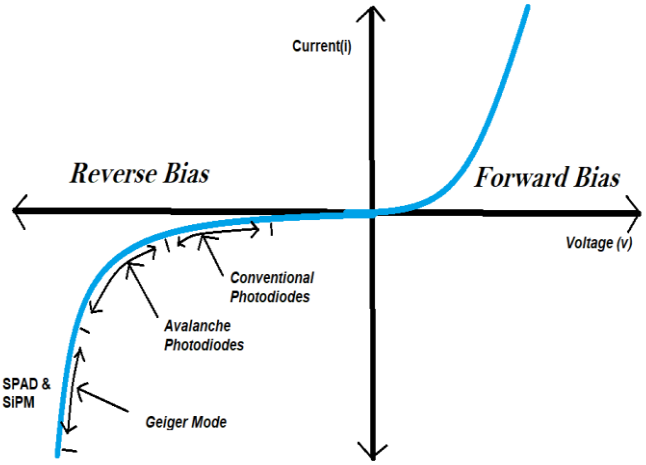

Fig.1. Diode characteristics

Classical communication, like the fibber optics powering the internet, uses strong pulses of light containing billions of photons, so that information is encoded in the light's intensity – a pulse being 'on' represents a 1, while 'off' represents a 0, with the main goal being high speed data transfer. Contrarily, quantum communication operates at maximum granular level, using single individual photons. Here the information is encoded in a photon's intrinsic quantum state, such as its polarization. This method employs the principles of quantum mechanics to attain its primary goal as forming primarily secure communication channels.

2.2 A NOVEL BASED 64BIT WIDTH NLFSR

In this work we used a novel based 64-bit Non-Linear Feedback Shift Register. It is a shift register in which the input bit is acquired from non-linear function of its previous state. NLFSRs provide strengthened security and randomness compared to Linear Feedback Shift Registers (LFSRs) due to their non-linear feedback function as shown in Fig.3. They are widely applicable in contemperorary stream of ciphers [18], particularly in RFID and standard applications, because of their defiance to cryptanalytic attacks. Constructing NLFSRs with assured long periods is very strenuous, though they can generate sophisticated pseudorandom sequences that refines cryptographic strength. Techniques such as adaptive algorithms have been evaluated to design effective NLFSRs for which to get the standard randomness criteria [19].

If spad_photon_pulse && ~detector_died:

$$Noise_{fb}=(((\sim s_{63}\&s_{57})\oplus\sim s_{33})\oplus(s_{40}\&s_{25}))\oplus(s_{10}\&s_0) \quad (1)$$

$$quantum_{noise}(new)=s_{62},\ldots\ldots s_2,s_1,s_0,noise_{fb} \quad (2)$$

We used these Eq.(1) and Eq.(2) in our logic at which the NLFSR work is to generate quantum_noises when the detector is enabled and the spad_photon_pulse is exists [20]. This defines only the quantum noise but not exactly expected output random bit. Mainly the output random bit will be generated based on the random photon noises. In these above equations "s" defined as state of the register and feedback function in NLFSR is defines by "noise_fb".

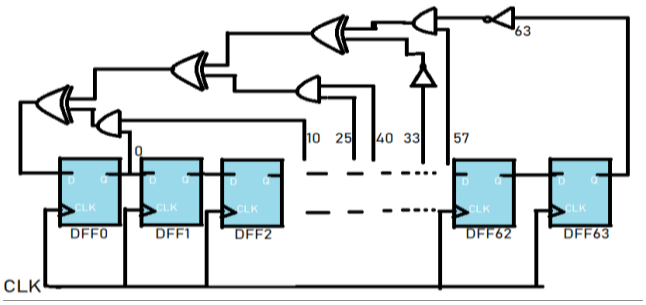

Fig.2. 64-BIT WDITH NLFSR

It is important to differentiate the roles of randomness generation and randomness extraction in our architecture. The true entropy source in this work is the quantum process of single photon detection via SPAD, delivering fundamentally unpredictable events. The NLFSR is implemented stringently as a randomness extractor [21] that operates on raw quantum data, removing technical bias and improving bit quality without introducing algorithmic pseudo randomness. Therefore, while the NLFSR is a classical circuit, it does not compromise the quantum nature of the final output, which remains appropriate way for cryptographic security applications and standard statistical tests are also passed.

The feedback function is composition of multiple AND, OR and NOT gate combinations among selected bits of the register, introducing strong non linearity into the sequence generation. So this approach increases randomness of the output sequence, as a part of proving it is more resistant to cryptanalytic attacks and suitable for cryptographic compared to traditional LFSRs. The shcematic in Fig.3 clearly described how selected bits (quantum_noise indices) are computated by various logic gates before giving feeding back to the first flip flop that is DFF0. This NLFSR structure and custom feedback function making it more ideal to use in secure stream ciphers and quantum random number generators, where this discourages predictability. Overall, the design showcases how implementing a non-linear feedback function in a shift register architecture via Verilog allows the synthesis of robust digital circuits, hardware efficient pseudo random generators for digital and cryptographic secure communication systems [22].

To design a 64-bit NLFSR, the process starts from the concepts of a actual basic LFSR, as shown in the Fig.4, where a series of flip flops are connected with XOR gates providing linear feedback. In a typical LFSR, the new input to the first register is generated by performing XOR logic between selected register bits(taps), resulting in a linear pseudorandom sequence that cycles through among all possible states. To upgrade to a 64-bit NLFSR from LFSR, we have to include multiple flip flops (usually 64) are cascaded with non linear feedback, but the feedback logic is swapped with non-linear Boolean expressions combining AND, OR and NOT gates to significantly increasing complexity and sequence unpredictability. Such a 64-bit NLFSR includes a feedback function not restricted to XOR gates but including multiple non-linear logic gates, performed to selected bits in the register. This non linearity confirmed the output sequence has higher entropy and sanctions more statistical randomness tests, making it more reliable for cryptography and random number generation applications.

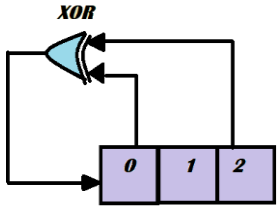

Fig.3. Architecture of Basic LFSR

2.3 ZERO AWARE CLOCK GATING

This work uses Clock Gating Technique to get low power consumption in our design. In the Fig.5 is an architecture called Integrated clock gated cell which using clock gating technique to reduce power consumption in the SPAD design

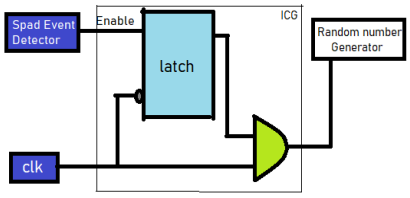

Fig.4. Integrated clock gated cell

So, this Integrated clock gated cell's output will be high when only spad event detects at active logic of clock signal in design. This will severly reduce power consumption in overall design because maximum clock network will consume power in entire network, then if we focus on clock gating then definitly more power consuption can be reduced. Hence, we have focussed on Clock gating Technique.

3. ARCHITECTURAL EVALUATION

3.1 MIXED SIGNAL SIMULATION USING ESIM

This mixed signal eSim schematic in Fig.6 implements a SPAD based quantum random number generator. Which having both photon detection and digital post processing logic [23].

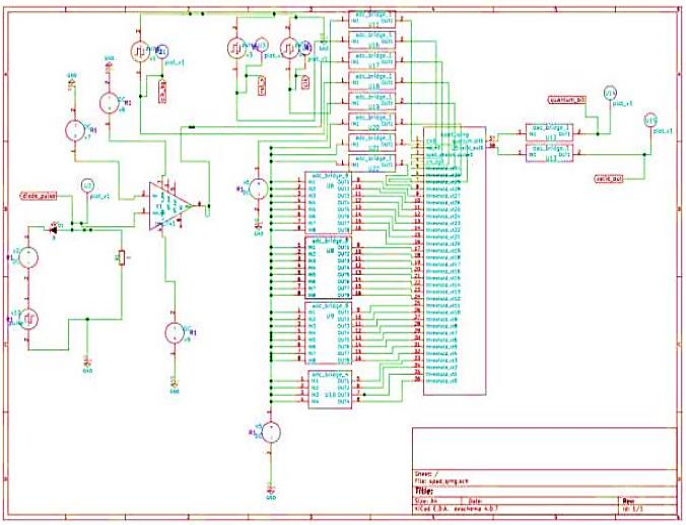

Fig.5. Mixed signal circuit for SPAD based QRNG

At the left of the schematic, the SPAD is reverse biased using alterable voltage source, allowing it to detect single photons and generate avalanche pulses upon a photon event. These quick, low level SPAD pulses are fed into a comparator conditionally, which takes each analog event and ensures reliable detection by rising up the pulse edges. These digital pulses then enter the core digital logic block, where the digital logic IC includes flip flops, logic gates, and counters to perform the events. The logic includes pulse regeneration, transition counting, and/or parallel digital extraction counting, and digital bit extraction, resulting in clean, unbiased random bits are the output. The careful partitioning of analog front end for quantum event captured and followed by digital post processing for randomness extraction and system level output, makes this as robust architecture perfectly suited for high quality, hardware quantum random number generation.

The presented waveforms in Fig.7 describing the simulation results of the SPAD based quantum random number generator's digital logic, obtained using GTKWave after simulation with Icarus Verilog [24], [25]. The diagram shows a exaclty DAC and ADC bridges for communication between digital and analog domains.

Counters like ones_count_tb and total_bits_tb, and transitions_count are included to continuously monitor randomness quality, with supplementary diagnostic lines such as entropy_monitor and last_quantum_bit providing real-time feedback for bias and entropy_monitor and last_quantum_bit providing real time feedback for entropy estimation. The signal transitions signifies robust operation verification counters, confirming correct behaviour and statistical monitoring throughout the digital post processing path. Overall, the simulation results validate the effectiveness of the digital design, assuring that the system reliably captures quantum events and produces high quality, unbiased binary random numbers for secure and cryptographic applications.

$$\text{Analog\_level} = \begin{cases} C_{\text{high}} + (\text{quantum\_noise} \square\ 0), & \text{if toggle = high} \\ C_{\text{low}} + (\text{quantum\_noise} \square\ 0), & \text{if toggle = low} \\ \text{Analog\_level} + \left(\text{quantum\_noise}_{[7:0]} \square\ 24\right)C, & \text{otherwise} \end{cases} \quad (3)$$

This Eq.(3) describes how the analog signal level is updated in the QRNG circuit. Constant value is described by "*C*" in the above equation. If the toggle state is high, the analog level is set to a high constant plus quantum noise; if the toggle state is low, it's set to a low constant plus quantum noise.

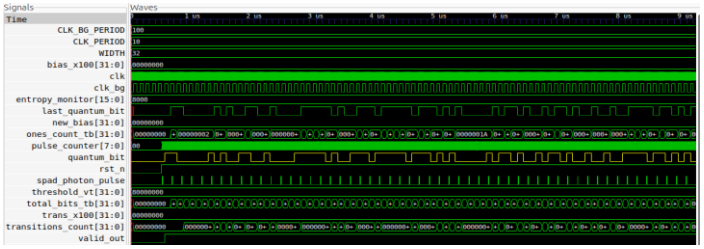

Fig.6. Simulation waveforms of our SPAD based QRNG Design

For all other circumstances, the analog level is adjusted by adding a shifted quantum noise fragment and subtracting a constant, giving continuous analog variation to support robust random bit generation.

$$\text{Quantum\_bit} = \begin{cases} 1, & \text{if Analog\_level} > \text{threshold} \\ 0, & \text{otherwise} \end{cases} \quad (4)$$

Quantum_bit is our output random bit. In Eq.(4) If Analog_level produced by quantum_noise evaluation is higher than threshold value, then output will be '1' or else it will be zero. So, the Analog _level is random in nature by the SPAD Based Diode at which the photonic noise is detected.

$$Pones = Nones/N \quad (5)$$

In the Eq.(5), *N* is defined as No. of samples in a window we are going to generate as random bits, here '*N*' value is 64 and Nones is No. of '1's are generated in total number of samples.

$$\text{Entropy\_monitor} = \begin{cases} C_{\text{high}}, & \text{if Nones} > 40 \\ C_{\text{low}}, & \text{if Nones} < 24 \\ C_{\text{mid}}, & \text{otherwise} \end{cases} \quad (6)$$

This Eq.(6) defines the entropy monitor value based on the count of ones in each block of output bits. If the number of ones exceeds 40, the monitor output will given as a high value; if less than 24, it gives output as a low value; and for values in between, it uses a mid-setting. This gave ongoing feedback about the statistical balance and quality of generated random bits in the system [26].

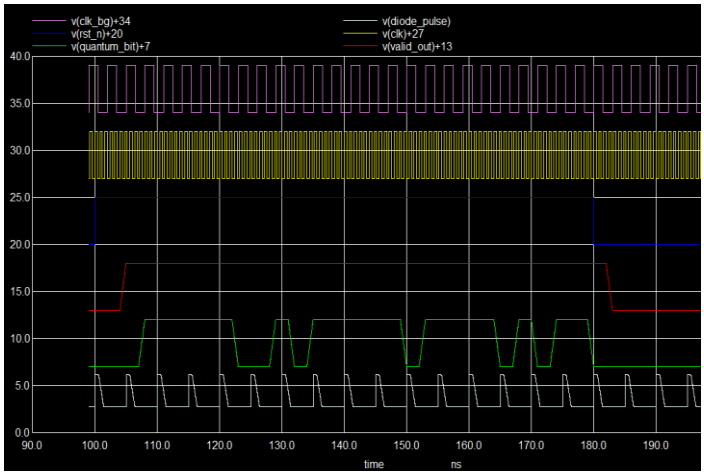

Fig.7. eSim Simulation results for SPAD_QRNG

In Fig.8 Simulation waveforms clearly describes the behavior of the proposed SPAD based quantum random number generator, as verified using the eSim analog/digital co-simulation. Each section of signals represents a key signal from the design, including the bit generation clock (clk_bg), main clock (clk), system reset(rst_n), photon detection pulses from the SPAD diode (diode_pulse), the validated quantum output bit (quantum_bit), and the valid output indicator (valid_out). The results in waveforms shows that how quantum bit values are generated and validated synchronously with photon arrival events and internal active clock edges.

During active period of clock signal, each photon detection pulse triggers the analog level and quantum noise logic to the new value, which will resulted as unpredictable quantum output bit. The valid output signal follows the generation of events. The simulation also highlights the actual execution of dead time intervals and synchronization between analog quantum sources and digital post processing. These results illustrate the perfect

achieved randomness quality and real time operability of the design and also verifying its appropriateness for hardware cryptographic communiation systems while also confirming the effectiveness of integrating quantum-derived physical entropy with a nonlinear digital extraction approach.

3.2 PERFORMED RTL TO GDSII FLOW FOR FUNCTIONAL EVALUATION

The presented simulation results validate the full implementation and verification flow of the proposed SPAD based quantum random number generator. Fig.9 shows the mixed signal analysis performed with the Verilog schematic design block, where the system's digital and analog constituents were simulated to ensure correct quantum bit generation and signal synchronization. This step affirmed the initial functional behaviour using schematic level design and eSim mixed signal simulation tools [27].

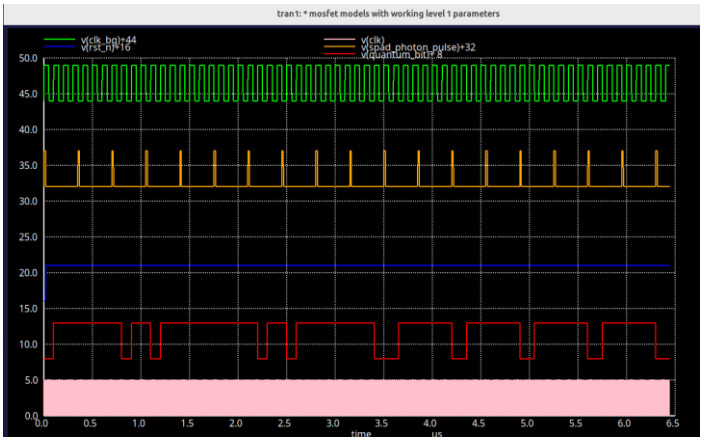

Fig.8. NGSPICE Simulation results for Magic generated SPAD_QRNG layout design

The Fig.9 Illustrates the results from the final layout, generated after completing the complete RTL TO GDSII flow, here, the design was implemented at the physical level, and post layout SPICE simulations were performed on the extracted netlist. The results from this layout level analysis exactly matched those of the schematic simulation, demonstrating that the physical implementation accurately preserves the intended circuit behaviour. Moreover, both the schematic and layout results were verified by running Layout results were verified by running Layout Versus Schematic (LVS) checks [28], ensuring layout corresponds exactly to the original design target.

The soundness of simulation outcomes before and after the RTL to GDS flow strongly verified the exactness of the design, the integrity of quantum randomness extraction, and the robustness of the ASIC implementation process. This verification from Schematic to Layout ensures the reliability of the proposed solution for secure hardware cryptographic applications. By performing RTL to GDS flow we can say our Verilog based designed RNG's can be possible to fabricate without DRC and LVS violations occurred. So we can happily that our design has that much intent as possible to fabricate undoubtedly.

In Fig.10 presents the final layout of the proposed quantum random number generator (QRNG), fully implemented using the 'osu035' stands for Oklahoma State University 0.35-micron standard cell technology. This physical layout was generated as part of the complete RTL to GDSII ASIC design flow, assuring every functional and verification step was intented at the silicon level.

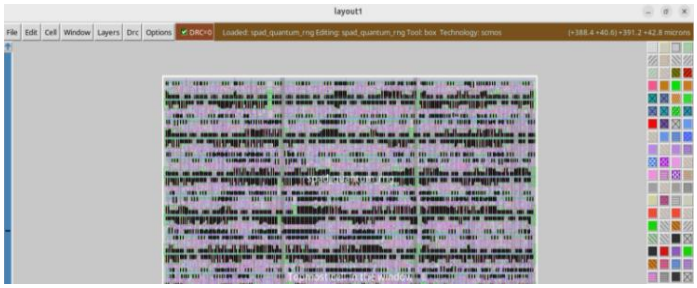

Fig.9. MAGIC Tool Generated Layout of our SPAD_QRNG Design

The layout reveals high density digital integration, with finely tuned placement and routing that exploits the compact feature set of the 0.35 um technology. Key benefits of our QRNG layout ensures maximum efficiency in silicon area usage critical for inclusion of secure entropy sources in resource constrained hardware modules and lessened power consumption due to improved netlist and cell selection. The physical design has stable clock operation, signal, and power distribution, confirming perfect operation even though having so much challenging environment and process variation scenarios. Merging a quantum entropy source together with advanced non-linear digital extraction in a physically secure layout substantiates the strength of our solution for cryptographic hardware applications. This generation and verification of both schematic and layout results confirm that the QRNG is fabricable and ready for practical deployment in modern secure systems without any DRC, LVS violations as described in the above Fig.10 Magic tool (DRC=0).

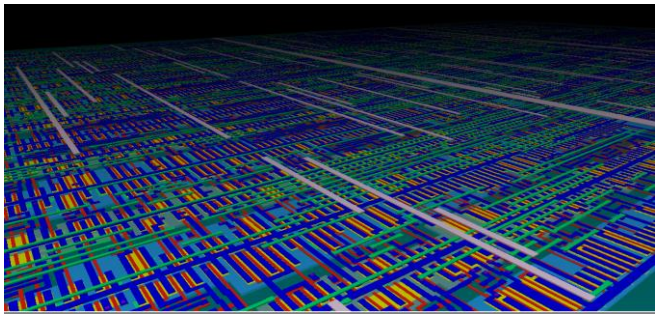

Fig.10. Graphic Data System (GDS) 3D View of SPAD based Design

The .gds file represents the final output in above Fig.11 of the RTL to GDSII flow, encoding the complete physical layout required for semiconductor fabrication. In industry, the .gds file is unavoidable, it translates digital design intent into a fabricable blueprint, serving as the universal format delivered to foundries for mask generation and chip production. It's ensure that advanced ICs meet better performance, power, and area requirements and also supporting large scale commercial utilization.

In academic and research institutions, the ability to generate and analysing .gds files signifies mastery over end-to-end VLSI implementation. It can assure of capable for fabrication ready

designs. Moreover, presenting a .gds file as part of research demonstrates that the investigation has progressed beyond theoretical modelling to practical realization, bridging the gap between scholarly exploration and industrial standards, and granting students and researches critical experience with professional EDA tool flows and tape out processes.

```
=== Test Results ===
Total bits generated:        249
Ones generated:         124
Zeros generated:         125
Bit transitions:         123
Entropy monitor: 8000
Bias percentage:          49%
Transition rate:          49%
BIAS TEST: PASSED
RANDOMNESS TEST: PASSED
```

Fig.11. Test Results of SPAD_QRNG Output Stream

This Fig.12 presents real time examine metrics for the generated quantum random bitstream produced by the proposed SPAD based QRNG.Total bits are 249, out of 249 bits generated, the results shows perfect statistical balance, with among 124 ones and 125 zeros, and a bit transition count of 123, which finalises as low bias and enhanced bit switching. The entropy monitors value and transition rate further confirm that the output randomness quality is stable. Importantly, the device passes both bias and randomness self-tests, which serves as additional evidence that the implemented system achieves high quality, and our design has very low biased random output perfectly suitable for secure cryptographic applications. These self-test results straightaway reflect the success of the foundational architectural steps for ensuring both physical and statistical integrity of quantum random bits. This hardware RTL to GDS Flow has done by an open-source tool Qflow [29], this Qflow tool chain includes several EDA tools like 'yosys' for synthesis, 'Graywolf' for placement and floor planning and 'qrouter' for routing, and LVS and DRC violation checks will be done for which our design can be sent to sign off (fabrication) due to not having any violations [30], [31]. 'magic' for layout and further 3D Graphic data system (GDSII).

Table.1. Power analysis results for SPAD Based Design

Parameter Description	Sequential	Combinational	Clock	Total
Internal Power (w)	0.11 m	19 µ	44 µ	1.76 m
Switching Power (w)	7.8 µ	12.6 µ	48.1 µ	68.6 µ
Leakage Power (w)	12.2 µ	13.8 µ	1.2µ	27.2 µ
Total Power (w)	0.13 m	45.8 µ	93 µ	0.2 m
Total Power (%)	48.7 %	16.8 %	34.5 %	100 %

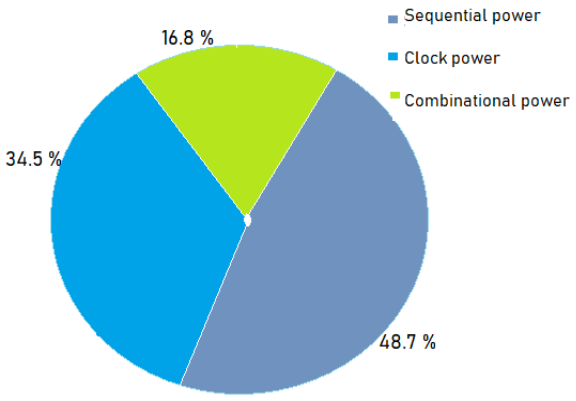

Fig.12. Power Analysis results for SPAD_QRNG

The power analysis in above Table.1 encapsulates the distribution and efficiency of power consumption in the implemented SPAD based QRNG ASIC design. Three main power components are reported Internal, switching, and leakage powers. The results reveal that the sequential logic leads the largest share of total power at 48.7%, followed by the clock network at 34.5%, and combinational logic at 16.8%. Internal power dominates, accounting for 64.8% of total consumption, while switching and leakage contribute 25.2% and 10%, respectively. The overall power measured for the complete IC design is 0.272 m W, validate the effectiveness of the proposed architecture in achieving ultra-low power operation. No significant power is spent on macros or I/O pads, indicating that the chip's energy is efficiently focused in computation and signal timing paths.

This breakdown demonstrates that the design is both power conscious and highly suitable for integration in energy constrained secure hardware cryptosystems, setting a strong benchmark compared to other SPAD based QRNG implementations. Due to having NLFSRs more registers are going have been used that's why we got more power consumption due to Sequential block.

Table.2. Total power consumed by all components

Component Type	Power (Watts)
Resistors	1.2 e-19
Capacitors	1.3 e-16
Op-amp	3.8 e-06
SPAD_QRNG	0.27 e-03
SPAD_Diode	1.5 e-12
TOTAL	0.273 e-03

The above Table.2 describes power consumed by the individual components respectively and the Total power consumed by the complete design is 0.273 mW.

4. COMPARATIVE ANALYSIS

The comparative analysis chart in Fig.14 is clearly demonstrates the performance differences between the Regazzoni, Tontini, and proposed designs [32] [33]. The proposed method achieves a high NIST pass percentage [34] [35], comparable to the established alter natives, suggesting strong randomness quality. However, it significantly outperforms the other designs by achieving a lower power consumption, as depicted by the reduced value in the power (m W) metric.

While the Tontini scheme excels in the maximum P value (10^2) compared to Regazzoni and the proposed method, the overall combination of low power and high NIST pass percentage in the proposed solution supports its effectiveness for quantum random number generation applications.

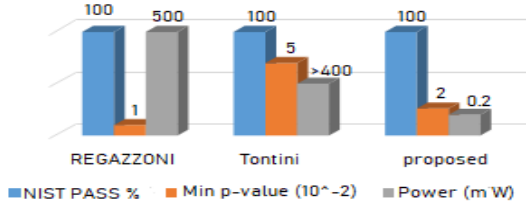

Fig.13. Comparative analysis on Power, NIST pass%, Min p value

The proposed architecture balances statistical robustness with significant energy efficiency advantages over previously reported approaches. And Key Strengths & Weaknesses of alternatives and proposed work has been detailed in the Table.3.

Table.3. Comparison of QRNG Design Implementations: Key Strengths and Weaknesses

Design	Key Strengths & Weaknesses
Regazzoni	High randomness (100% NIST Pass) but suffers from significantly high power consumption (500 mW).
Tontini	Highest Min p-value (5×10^{-2}) but has very high-power consumption (> 400 mW).
Proposed	Lowest power consumption (0.2 mW) while maintaining excellent randomness (100% NIST Pass). Implemented a complete RTL to GDSII ASIC flow.

5. CONCLUSION

The proposed SPAD based Quantum Random Number Generator (QRNG) successfully demonstrated an efficient hardware framework for realizing quantum entropy sources integrated with low power digital post processing. By using a Single Photon Avalanche Diode (SPAD) for true randomness extraction and a 64-bit Non-linear Feedback Shift Register (NLFSR) for enhanced randomness and bias removal, the design achieved superior statistical performance validated through NIST tests. The complete RTL to GDSII implementation using the osu035 PDK confirms the practical feasibility of ASIC fabrication with zero DRC/LVS violations. With a total power consumption of only 0.272 m W and reliable operation validated through mixed signal simulations, and also this work provides a energy efficient solution for secure cryptographic hardware, quantum key distribution systems, and embedded security modules. Future work can extend this architecture toward advanced technology nodes, higher bit rate optimization, and integration of multi SPAD arrays for improved throughput.

ACKNOWLEDGEMENT

We would like to thank the research facilities and laboratories that supported this work, especially the support from the eSim toolset for device emulation. We also gratefully acknowledge the guidance of our mentors and colleagues for their valuable insights and technical assistance throughout this project.

REFERENCES

[1] A.K. Singh, "Backflash Attack on Coherent One-Way Quantum Key Distribution Protocol", *Reviews of Modern Physics*, pp. 1-6, 2025.
[2] A. Meda, "Quantifying Back Flash Radiation to Prevent Zero Error Attacks in Quantum Key Distribution", *Light Science and Applications*, Vol. 6, pp. 1-5, 2017.
[3] V. Scarani, "The Security of Practical Quantum Key Distribution", *Reviews of Modern Physics*, Vol. 81, No. 3, pp. 1301-1350, 2009.
[4] "Quantum Key Distribution", Available at: https://en.wikipedia.org/wiki/Quantum key distribution, Accessed in 2025.
[5] W.E. Stanchina, "Oklahoma State University Standard Cell Library", Available at: https://-vlsiarch-.ecen.o kstate.edu, Accessed in 2007.
[6] OSRAM Opto-Semiconductors, "BPW21 Silicon Photodiode Data Sheet", Available at: https://look.ams-osram.com/m/2ce36b84bdf847e/original/BPW-21.pdf, Accessed in 2023.
[7] M. Kaeslin, "*Digital Integrated Circuit Design: From VLSI Architectures to CMOS Fabrication*", Cambridge University Press, 2008.
[8] N.D.K. AI-Shakarchy, "Randomly Steganography using LFSR and NLFSR Generation", *Journal Kerbala University*, Vol. 11, No.1, pp. 1-7, 2013.
[9] "Process Design Kit", Available at: https://en/wikipedia.org/wiki/process_design_kit, Accessed in 2025.
[10] I. Cusini, "Historical Perspectives, States of Art and Research Trends of Single Photon Avalanche Diodes", *Frontiers in Physics*, Vol. 10, pp. 1-12, 2022.
[11] "Single Photon Avalanche Diode", Available at: https://en.wikipedia.org-/wiki/Single_photon_ avalanche diode, Accessed in 2009.
[12] Y. Albeck, "Implementable Methods for Characterizing Single Photon Avalanche Diodes", *Results in Optics*, Vol. 15, pp. 1-6, 2024.
[13] E. Sarbazi, M. Safari and H. Haas, "Photon Detection Characteristics and Error Performance of SPAD Array Optical Receivers", *Proceedings of International Workshop on Optical Wireless Communications*, Vol. 63, No. 8, pp. 3043-3053, 2015.

[14] "Silicon Photomultiplier", Available at: https://en.wikipedia.org/wiki/silicon_photo-multiplier, Accessed in 2024.

[15] M. Rahmanpour, "Implementations Methods for Characterizing Single Photon Avalanche Diodes", *Results in Optics*, Vol. 15, pp. 1-7, 2024.

[16] F. Severini, "SPAD Pixel with Sub NS Dead Time for High Count Rate Applications*", IEEE Journal of Selected Topics in Quantum Electronics*, Vol. 28, No. 2, pp. 1 9, 2022.

[17] S. Cova, "Avalanche Photodiodes and Quenching Circuits for Single Photon Detection", *Applied Optics*, Vol. 35, No. 12, pp. 1956-1976, 1996.

[18] M. Hell, T. Johansson and W. Meier, "Grain: A Stream Cipher for Constrained Environments", *International Journal of Wireless Mobile Computing*, Vol. 2, No. 1, pp. 86-93, 2007.

[19] H. Nobach, "Pseudo Random Generators using Linear Feedback Shift Registers with Output Extraction", *Cryptography and Security*, pp. 1-18, 2024.

[20] X. Ma, F. Xu, X. Tan, B. Qi and H.K. Lo, "Post Processing for Quantum Random Number Generators: Entropy Evaluation and Randomness Extraction", *Physical Review A*, Vol. 87, pp. 1-13, 2013.

[21] R. Shaltiel, "An Introduction to Randomness Extractors", *Proceedings of International Colloquium on Automata, Languages, and Programming*, pp. 21 41, 2011.

[22] D.B. Thomas and W. Luk, "The LUT SR Family of Random Number Generators for FPGA Architectures", *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, Vol. 21, No. 4, pp. 761-770, 2021.

[23] P. Rahul, S. Bansode, N. Gloria, M.P. Desai and M. Kannan, "eSim: An Open Source EDA Tool for Mixed-Signal and Microcontroller Simulations", *Proceedings of International Conference on Circuits, Systems and Simulation*, pp. 1-11, 2021.

[24] "GTKWave Waveform Viewer", Available at: https://gtkwave.source-forge.net/, Accessed in 2024.

[25] "Icarus Verilog", Available at: https://iverilog.icarus.com/, Accessed in 2025.

[26] G. Gras, "Quantum Entropy Model of an Integrated Quantum Random Number Generator", *Physical Review Applied*, Vol. 15, pp. 1-9, 2021.

[27] "Ngspice: Open-Source Spice Simulator", Available at: http://ngspice.sourceforge.net/, Accessed in 2025.

[28] J.K. Ousterhout, "Magic: A VLSI Layout System", *Proceedings of International Conference on Design Automation*, pp. 152-159, 1984.

[29] T. Edwards, "Qflow 1.3: An Open-Source Digital Synthesis Flow", *Open Circuit Design*, pp. 1-6, 2010.

[30] C. Wolf, "Yosys Open Synthesis Suite", Available at: https://www.clifford.at/yosys/, Accessed in 2013.

[31] "Graywolf: VLSI Placement Tool", Available at: http://opencircuit-design.com, Accessed in 2025.

[32] A. Tontini, "SPAD based Quantum Random Number Generator with an Nth Order Rank Algorithm on FPGA", *IEEE Transactions on Circuits System*, Vol. 66, No. 12, pp. 2067-2071, 2019.

[33] F. Regazzoni, "A High-Speed Integrated Quantum Random Number Generator with on Chip Real Time Randomness Extraction", *Cryptography and Security*, pp. 1-9, 2021.

[34] A. Rukhin, S. Juan, N. James and M. Smid, "A Statistical Test Suite for Random and Pseudo Random Number Generators for Cryptographic Applications", Technical Report, National Institute of Standards and Technology, Department of Commerce, pp. 1-131, 2010.