Reliable TRNG and its Challenges

RajaAdhithan Radhakrishnan
r.rajaadhithan@gmail.com
Society For Electronic Transactions and Security(SETS)

***Abstract*—The objective of this work is to investigate methods for improving the self-tuning mechanism of ring oscillator (RO)-based True Random Number Generators (TRNGs). It also examines the challenges involved in achieving a reliable and stable design over long-term operation. Furthermore, this work analyzes potential approaches to address these challenges and validates their effectiveness using the NIST statistical test suite.**

***Index Terms*—TRNG - Reliable - Tuning - Delay -jitter.**

I. Introduction

In today's rapidly evolving technological landscape, advancements in technology are accompanied by the continuous evolution of security threats. Random number generators (RNGs) play a crucial role in addressing these security challenges and have evolved from Pseudo-Random Number Generators (PRNGs) to Quantum Random Number Generators (QRNGs). PRNGs are among the most widely standardized random number generation techniques; however, their deterministic nature requires an initial seed and periodic seed updates. This dependency makes them vulnerable to emerging threats, including side-channel attacks, artificial intelligence-based attacks, and future quantum computing attacks.

To overcome the limitations of deterministic randomness, researchers have shifted their focus toward True Random Number Generators (TRNGs), which exploit physical phenomena as sources of entropy. Further advancements in this field have led to the development of quantum-based random number generation techniques, such as QRNG and Quantum True Random Number Generators (QTRNGs), which utilize the inherent unpredictability of quantum mechanics. Although QRNGs provide strong theoretical security guarantees, their practical adoption in real-time systems remains challenging due to implementation and testing complexities.

For on-chip applications, hardware-based TRNGs remain more adaptable due to their compact design, integration capability, and compatibility with existing semiconductor technologies. However, achieving long-term reliability and stability in TRNGs, particularly Ring Oscillator (RO)-based TRNGs, remains a significant challenge due to process, voltage, and temperature (PVT) variations.

In this work, we discuss the advantages of QRNGs over conventional TRNGs and investigate the challenges associated with improving the reliability and stability of RO-based TRNGs. Furthermore, we explore potential approaches to enhance TRNG performance and validate their effectiveness using statistical randomness testing.

The rest of this paper is organized as follows.Section II discusses QRNG vs TRNG. Section III discusses ring oscillator and its challenge. Section IV approaches explored to improve the Ro's based TRNG and its significance. Finally, Section V concludes the paper.

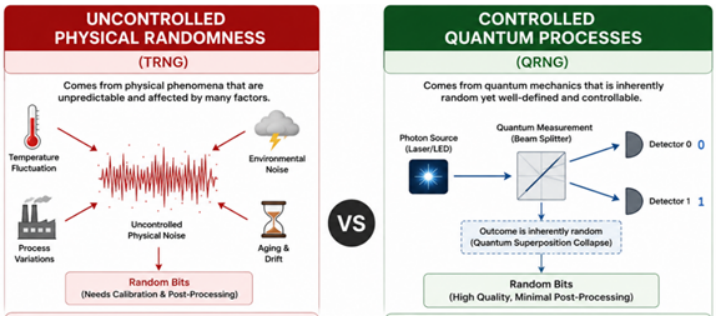

Fig. 1. Uncontrolled vs controlled random process

II. Motivation: QRNG vs. TRNG

TRNGs rely on uncontrolled physical randomness, such as thermal noise, jitter, or metastability, making them sensitive to manufacturing process variations, temperature changes, aging, and environmental noise. These factors can introduce bias and reduce the reliability of the generated random numbers. To maintain randomness, TRNGs often require calibration, compensation circuits, and post-processing, increasing design complexity and limiting scalability.

In contrast, QRNGs rely on controlled quantum processes, where randomness originates from the intrinsic unpredictability of quantum mechanics rather than hardware imperfections [2]. As a result, QRNGs are largely immune to process variations and environmental effects, enabling high-quality, reliable, and scalable random number generation with minimal calibration, compensation circuitry, and post-processing as shown in Fig.1. Consequently, QRNGs provide stronger security assurance and more consistent performance than conventional TRNGs.

In the upcoming section, I focus on approaches to improve the efficiency of TRNGs and discuss the challenges associated with their practical implementation in real-time scenarios.

III. Existing approches and challanges

Among the existing TRNG architectures, Ring Oscillator (RO)-based TRNGs are one of the most widely adopted approaches, where randomness is extracted from the inherent jitter present in oscillator signals [1].

A Ring Oscillator consists of an odd number of inverters connected in a closed loop, which generates a continuous oscillating signal. Due to variations in manufacturing processes, temperature fluctuations, supply voltage variations, and

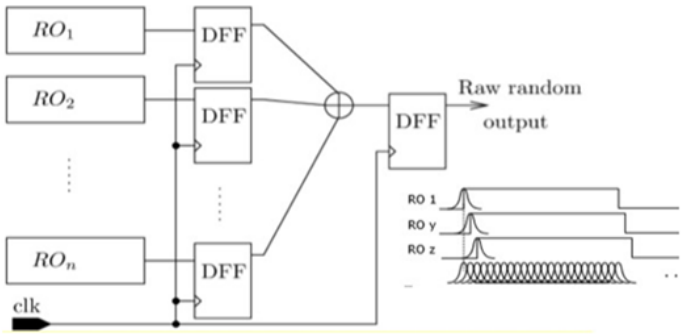

Fig. 2. Ring oscillator based TRNG

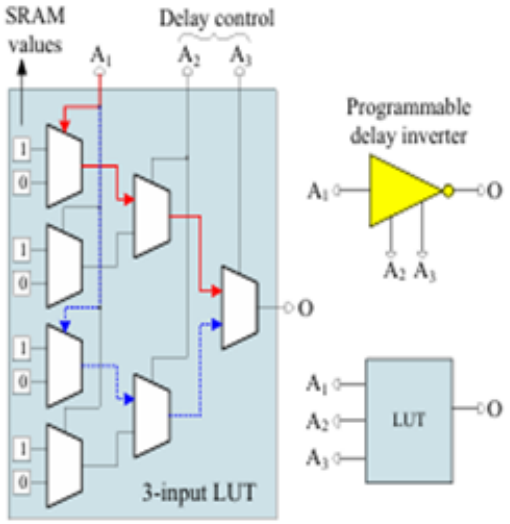

Fig. 3. Delay tuning in 3-input LUT

environmental noise, the propagation delay of the oscillator stages experiences small temporal variations, resulting in unpredictable timing jitter. This jitter serves as the primary source of entropy for random number generation. The oscillator output is sampled and further processed to generate random bits as shown in Fig.2.

A. Challenges

In practical RO-based TRNGs, a major challenge is mutual locking between closely placed oscillators, which reduces entropy and affects the security of generated random numbers [1], [4].

1) Self-tuning challenge (Delay and Jitter variation): To overcome oscillator locking, delay tuning is commonly introduced using programmable delay elements to adjust the oscillation characteristics of ROs as shown in Fig.3 [3]. However, tuning each RO individually and verifying the randomness quality through continuous self-testing increases design complexity and introduces additional latency. Moreover, delay variations caused by process, voltage, temperature (PVT), and aging effects make it difficult to identify and maintain the optimal tuning point during operation.

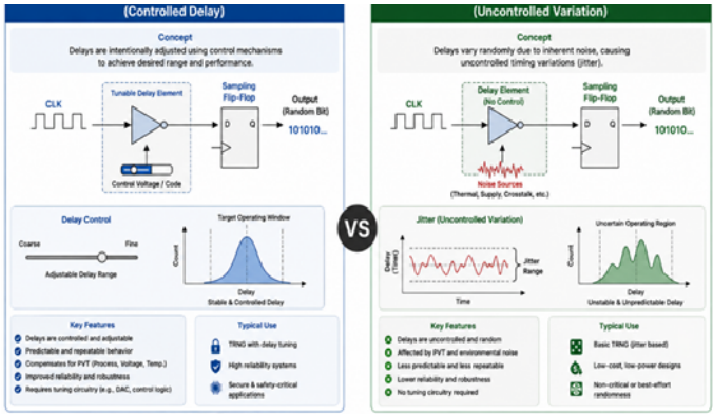

Fig. 4. Delay tuning vs jitter tuning

Alternatively, jitter-based tuning can provide a more adaptive randomness source by utilizing inherent timing variations as shown in Fig.4. However, jitter is highly sensitive to environmental conditions, and controlling the required amount of jitter while maintaining stable oscillator operation remains challenging.

2) Aging effect: Aging is another major concern in TRNGs, as transistor degradation changes oscillator delay and jitter characteristics over time, which can reduce entropy quality and impact long-term reliability.

3) Manufacturing variation and chip wastage: Since chip fabrication is a one-time process, insufficient randomness caused by process variations cannot be corrected after manufacturing. If the required entropy level is not achieved even with tuning flexibility, the fabricated chip may become unsuitable for secure applications, leading to silicon wastage.

To address these challenges, an efficient TRNG design requires a fast adaptive tuning mechanism along with a failsafe entropy enhancement technique. Such a mechanism should compensate for delay and jitter variations, process deviations, and aging effects while ensuring reliable and consistent random number generation over long-term operation.

IV. Approach Explored:

In this work, we explore different approaches to efficiently tune Ring Oscillator (RO)-based TRNGs to achieve improved randomness performance. The effectiveness of each approach is evaluated using the NIST statistical test suite.

To construct the experimental setup, a 3-input LUT-based programmable delay buffer is implemented to introduce tunable delay elements in the RO-based TRNG architecture, as shown in Fig. 5, Fig. 6, and Fig.7. Each programmable buffer consists of two selection lines to select different delay paths, enabling dynamic control of the oscillator behavior. The proposed design operates at a frequency of 100 MHz.

A. First Approach: Constant Selection-Based Tuning

In the first approach, all selection lines of the programmable delay buffers are assigned with constant values (”0” or ”1”), as shown in Fig. 5. This configuration evaluates the randomness behavior of the RO without dynamic tuning.

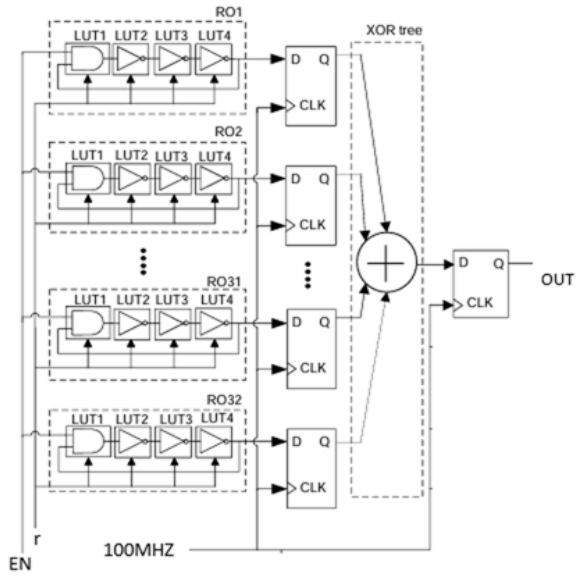

Fig. 5. Constant selection-based tuning

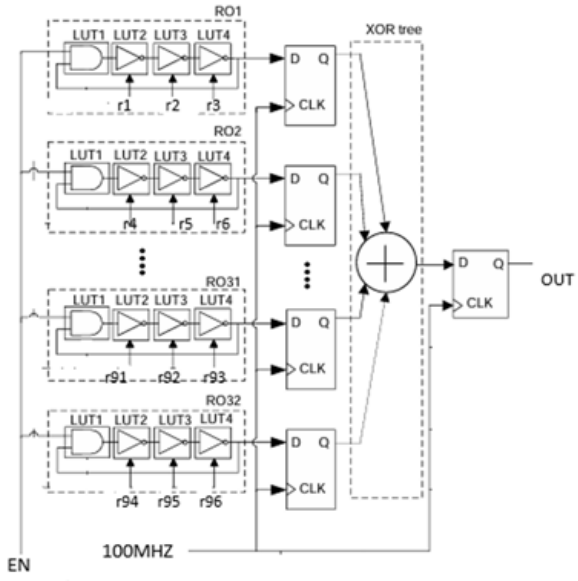

Fig. 6. Random LUT Configuration-Based Tuning

1) Result:: A 10,000 KB random bitstream was collected and evaluated using the NIST statistical test suite. The generated random sequence failed for maximum number of NIST tests, indicating insufficient randomness in the fixed delay configuration for 100 MHZ frequency .

B. Second Approach: Random LUT Configuration-Based Tuning

In the second approach, random bit patterns are applied to the configuration inputs of all programmable LUT-based delay buffers (r1, r2, ..., r96) as shown in Fig.6.

1) Result:: Experimental observations show that programming random configurations into the 3-input LUTs influences the randomness characteristics of the TRNG output. For certain LUT configurations, the randomness quality improves, while other configurations result in degraded randomness performance. These results indicate that programmable LUT configurations can be utilized as an effective tuning mechanism to control the entropy characteristics of RO-based TRNGs.

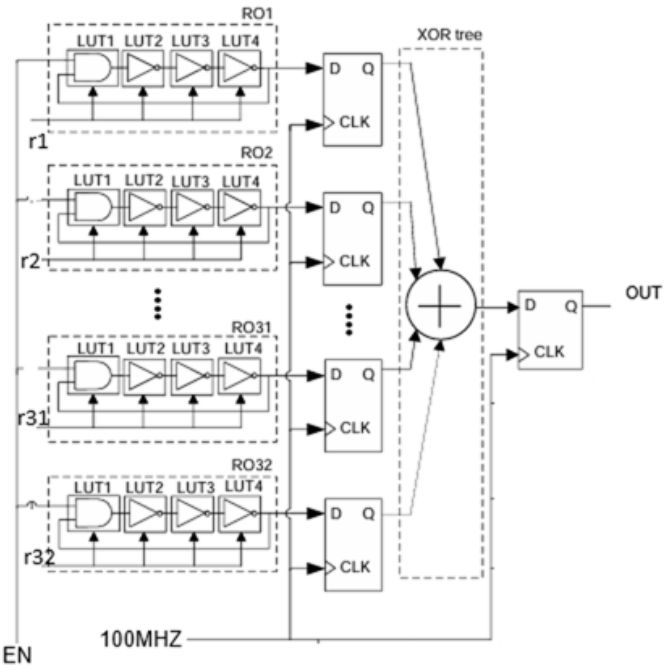

Fig. 7. Random RO-Level Tuning

C. Third Approach: Random RO-Level Tuning

In the third approach, random bits are applied simultaneously to all programmable delay elements within each Ring Oscillator (r1, r2, ..., r32), as shown in Fig.7. In this approach, a single random bit pattern is used to tune all delay buffers within an individual RO, enabling parallel tuning of the oscillator.

1) Result:: Experimental results demonstrate that random configuration of the Ring Oscillator significantly affects the randomness characteristics of the generated bitstream. The proposed approach achieved the highest number of successful NIST test iterations for a 100,000 KB dataset. These observations indicate that direct random tuning of the RO provides an efficient mechanism for controlling the randomness characteristics of RO-based TRNGs.

D. Observation and Discussion

From the above observations, it can be concluded that the third approach provides a faster and more efficient method for tuning RO-based TRNGs. Conventional sequential tuning of individual ROs introduces additional complexity and latency due to the requirement of tuning and evaluating each oscillator separately. In contrast, the proposed approach enables parallel tuning of multiple delay elements, significantly reducing tuning overhead and improving adaptability.

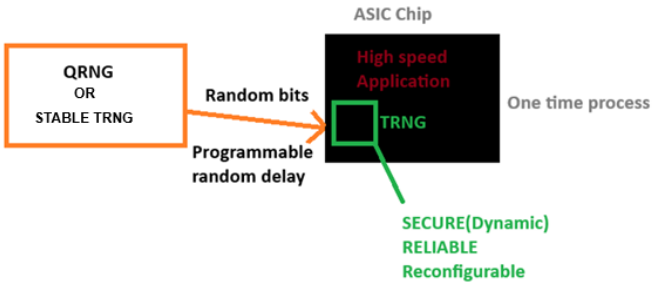

Fig. 8. External source to Trigger Delay elements

Furthermore, the flexibility of this approach can be extended by utilizing LUTs with higher input configurations to provide a larger tuning space and finer control over oscillator characteristics.

However, the proposed approach has certain limitations. The initial tuning process requires random input bits to configure the delay elements. If the RO does not provide sufficient entropy during the initial phase, an external random source may be required to generate the initial tuning patterns.

In addition, long-term reliability challenges such as aging effects and process, voltage, and temperature (PVT) variations need to be considered. To address these issues, a hybrid approach combining delay tuning with jitter-based entropy enhancement can be explored. For example, multiple delay paths can be integrated through a multiplexer, where delay configurations are dynamically selected to introduce adaptability and compensate for environmental and device variations. This approach can improve the robustness and long-term stability of RO-based TRNGs.

E. External Source to generate random bits to tune delay or jitter variation as failsafe mechanism

Currently self-test-based tuning methods is available to ensure the strength of entropy. But its relay on routine process will have threads in modern world and there should be a need of failsafe mechanism, if RO's not produce enough randomness, so from this work, I suggest to use the a QRNG-driven or stable TRNG based random delay tuning approach for RO-based TRNGs as shown in Fig.8. In this methods,random bits are used to randomly control and tune all delay elements within the RO structure, including inverter stages such as A1, A2, A3, and others. These random bits are continuously or periodically refreshed after a fixed time interval, allowing the internal delay configuration of the TRNG to change dynamically over time. As a result, the TRNG does not operate as a fixed circuit, but behaves like a newly reconstructed random circuit during each refresh cycle. This dynamic behavior reduces the possibility of predictable patterns and hardware attacks while also minimizing RO locking issues and improving entropy stability. This make the TRNG secure, reliable and reconfigurable. Overall, the proposed approach simplifies the complexity of delay tuning and significantly enhances the randomness quality, reliability, flexibility and hardware security of both RO-based and arbiter-based TRNG systems.

F. PRO's CON's

1) Post-Silicon Tunability Fail-Safe Entropy Compensation: Since ASIC fabrication is irreversible, integrating a QRNG or stable TRNG-assisted adaptive control path into the TRNG enables post-silicon entropy calibration and jitter compensation. This mitigates process-voltage-temperature (PVT)- and aging-induced randomness degradation and reduces the need for costly re-fabrication. The architecture therefore introduces a fail-safe entropy stabilization mechanism with enhanced design flexibility.

2) Dynamic Entropy Adaptation: The QRNG-assisted architecture makes the TRNG more adaptive and reconfigurable, thereby improving operational reliability, entropy robustness, and security resilience under varying on-chip conditions.

3) Area–Security Trade-off: Integrating QRNG support incurs additional silicon overhead due to extra entropy-conditioning and control circuitry, resulting in a moderate increase in area and power consumption.

4) Security Dependence on Entropy Refresh Strategy: The overall security strength depends on the efficiency of QRNG-bit post-processing, entropy extraction quality, and refresh frequency. Higher refresh rates improve unpredictability

V. Conclusion and Future Work

In summary, this work analyzed different approaches for tuning a ring oscillator (RO)-based TRNG by applying random bits to the delay tuning unit. Among the explored methods, random RO-level delay tuning achieved the best randomness performance, demonstrating that random delay tuning can significantly improve the effectiveness of self-tested tuning.

Furthermore, we propose using a QRNG, or alternatively a highly stable TRNG, as an external entropy source for worst-case operating conditions. Combined with additional control logic, this approach enables post-silicon entropy control, thereby improving randomness quality, reliability, and throughput under process, voltage, and temperature (PVT) variations in ASIC implementations. As a result, the proposed architecture becomes more adaptive, secure, and robust, while also providing the flexibility required to address future quantum-era security requirements.

However, automating the entropy tuning and control process remains an open challenge and requires further investigation, which will be considered as future work.

References

[1] M. Majzoobi, F. Koushanfar, and S. Devadas, "FPGA-Based True Random Number Generation Using Circuit Metastability with Adaptive Feedback Control," in Cryptographic Hardware and Embedded Systems – CHES 2011. Springer Berlin Heidelberg, 2011, pp. 17–32.

[2] Quantis QRNG Chips - ID Quantique

[3] M. Majzoobi, F. Koushanfar and S. Devadas, "FPGA PUF using programmable delay lines," 2010 IEEE International Workshop on Information Forensics and Security, Seattle, WA, USA, 2010, pp. 1-6.

[4] N. Nalla Anandakumar, S. K. Sanadhya, and M. S. Hashmi, "FPGA-based true random number generation using programmable delays in oscillator-rings," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 67, no. 3, pp. 570–574, Mar. 2020. doi: 10.1109/TCSII.2019.2919891.