Design of a TRNG in 600-nm IGZO-TFT FlexICs for Secure IoT Applications

João Cabacinho*[1], Diogo Sousa[2], João Marcelino[2], Marco Fernandes[2],
Pedro Barquinha[2], João Goes[1], João Casaleiro[3], Luis Bica Oliveira[1]
*j.cabacinho@campus.fct.unl.pt

[1]*DEEC, NOVA FCT*
CTS-UNINOVA & LASI
2829-516 Caparica, Portugal

[2]*DCM, NOVA FCT*
CENIMAT | I3N
2829-516 Caparica, Portugal

[3]*DEETC, ISEL*
CTS-UNINOVA & LASI
1959-007 Lisbon, Portugal

2025 IEEE International Symposium on Circuits and Systems (ISCAS) | 979-8-3503-5683-0/25/$31.00 ©2025 IEEE | DOI: 10.1109/ISCAS56072.2025.11043564

***Abstract*—As the demand for secure Internet of Things (IoT) devices increases, the need for hardware security solutions has become more critical, particularly in applications with strict power and area constraints. Thin-film transistors (TFTs) are an emerging technology, that enables the integration of complex circuits onto thin, flexible substrates offering both low-cost manufacturing and compatibility with large-area system implementations. This paper, presents, to the best of the authors' knowledge, the first true random number generator (TRNG) based on jittered oscillator sampling, implemented in 600 nm Indium-Gallium-Zinc-Oxide (IGZO) TFT flexible integrated circuits (FlexICs) technology.**

The proposed TRNG achieves a throughput of 1.33 Mbits/s, an energy consumption of 4.68 nJ/bit, and occupies an area of 0.920 mm^2. The TRNG showed promising results by passing 8 NIST (National Institute of Standards and Technology) randomness tests under nominal conditions. This opens new opportunities for embedding security primitives in flexible electronics, allowing for integration of hardware security in wearable electronics, biomedical devices, communication tags and other applications.

***Index Terms*—True Random Number Generator (TRNG), Flexible Integrated Circuits (FlexICs), IGZO, Hardware Security, Dynamic Entropy, Ring Oscillator.**

I. Introduction

The rapid expansion of internet of things (IoT) has significantly increased the demand for wearable, environmental sensors and implantable medical devices [1].

As IoT devices evolve and share sensitive information, robust security measures become of great importance. Secure cryptographic primitives are needed to prevent data breaches and protect against malicious attacks. While most security is softwared-based, there's a shift towards hardware solutions. This trend is driven by the growing need for stringent security in systems where the area and power overhead of traditional software methods is impractical due to the devices' smaller sizes and/or strict power constraints [2].

To address these issues, there is a rising interest in hardware security, where security primitives are integrated as system on chip (SoC) solutions. Cryptography algorithms and protocols rely heavily on the randomness and unpredictability of the generated numbers. Consequently, true random number generators (TRNGs), which generate random bits from intrinsically nondeterministic physical processes, are receiving significant attention for their ability to meet strict security requirements while maintaining low area and power consumption [3]. In this paper, we focus on dynamic entropy generation using TRNGs, which play a fundamental role in cryptographic operations, device authentication, and secure communications.

In response to the growing need of IoT devices, thin-film transistors (TFTs) have emerged as a promising technology due to their unique properties. TFTs enable the integration of complex circuits onto thin, flexible substrates while offering low-cost manufacturing and compatibility with large-area system. Additionally, they are environmentally friendly, making them well-suited for a wide range of IoT applications [4].

Recent advances in TFT technology have led to the development of various complex analog and digital circuits, such as microprocessors [5], amplifiers [6], [7] and comparators [7]. The TFTs' ability to integrate complex circuitry makes them suited for implementing secure hardware solutions for IoT devices. Unlike traditional silicon-based systems, the physical flexibility of TFTs allows for their seamless integration into unconventional form factors, such as wearable electronics for biomedical [8] and healthcare [9] applications and integration of information with people, objects and the environment, such as communication tags (RFID/NFC) [10] and machine learning circuits [11].

This paper proposes a TRNG based on jittered oscillator sampling, implemented in 600 nm Indium-Gallium-Zinc-Oxide (IGZO) TFT flexible integrated circuits (FlexICs) technology from Pragmatic. To the authors' knowledge, this is the first TRNG implemented using TFT technology, marking a significant advancement in secure hardware solutions for flexible electronics. The TRNG under nominal conditions was able to pass 8/8 tests from NIST (National Institute of Standards and Technology) test suite. The implementation showcases the potential for integrating advanced security features directly into flexible devices.

This work was supported by FCT under PhD grant 2023.00267.BD, IDS-Paper project PTDC/CTM-PAM/4241/2020, CTS multiannual funding program CTS/00066, CENIMAT|i3N pluriannual funding LA/P/0037/2020, UIDP/50025/2020 and UIDB/50025/2020.

II. TRNG Entropy

TRNGs rely on inherently random physical processes to generate dynamic entropy [3]. A typical TRNG consists of two primary components: an entropy source and an entropy extractor, with an optional post-processing block to improve the output. While post-processing allows for more relaxed requirements from the raw TRNG output, it increases the circuit's area and power consumption.

a) Entropy Source: This module is the source of randomness of the output bitstream by maximizing inherently unpredictable and random processes such as oscillator jitter and thermal noise, while mitigating predictable, deterministic variations like process, voltage and temperature (PVT) variations, aging and mismatch. The randomness prevents prediction of future and past values based on current observations [2]. This unpredictability is what fundamentally distinguishes TRNGs from other types of random number generators.

The most common TRNG techniques are based on: metastability [12], [13], chaotic mapping [14] and jittered oscillator sampling [15]–[17].

b) Entropy Extraction: The role of this stage is to convert the randomness from the entropy source into a usable bitstream. It leverages the random processes (for example, amplitude variations and adding jitter from several sources) to create a signal that can then be sampled, producing a random bit. Jittered oscillator sampling TRNGs extract entropy by sampling a low-jitter, fast oscillator with a slower high-jitter clock signal (entropy source), typically through D flip-flop (DFF). The inherent jitter in the clock introduces uncertainty in the sample value, causing the DFF's output to randomly switch between logic 1 and 0.

One of the main challenges with this type of TRNG is that the oscillator jitter may not be sufficiently large to generate a statistically random output. Moreover, the commonly used ring oscillators in such configurations are highly sensitive to PVT variations, requiring additional compensation and calibration circuits. These additional measures increase power consumption, and the overall circuit complexity.

III. Proposed Circuit

The proposed circuit, is a TRNG based on jittered oscillator sampling in 600 nm IGZO-TFT FlexICs technology which exhibits higher noise levels than CMOS devices. This increased noise enhances oscillator jitter and improves entropy generation. Different from common designs that use a low-jitter, fast oscillator sampled by a high-jitter, slow oscillator, this circuit samples a signal generated by combining the noise from 10 oscillators through an XOR gate. The XOR is used to increase the number of jittered transition in the time frame, thus, increase the ability of jitter to generate a statistically random output. This technique has been proven in CMOS technology [18]. To minimize deterministic regions at the XOR output, each oscillator can be delayed relative to one another [19]. This work also adapts the oscillators delay technique for IGZO-TFT FlexICs technology.

A. Inverter in IGZO-TFT FlexIC technology

One of the primary challenges of IGZO-TFT FlexICs technology is the absence of a complementary device. To address this, techniques such as resistive load, pseudo-CMOS and bootstrapping are employed to mimic the p-type functioning (e.g., for inverters, as illustrated in Fig. 1). These different techniques can be strategically used throughout the TRNG design. For instance, by using noise-susceptible configurations like resistive load inverters for the entropy source oscillators, the randomness can be enhanced while also reducing circuit area. Meanwhile, faster and more reliable configurations, such as pseudo-CMOS bootstrapping technique, are utilized in stages requiring accurate processing, such as the entropy extraction stage.

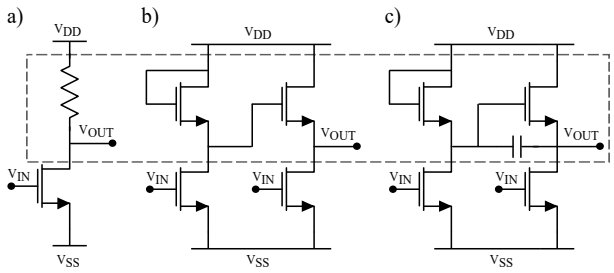

Fig. 1. Inverter techniques a) Resistive load b) Pseudo-CMOS c) Pseudo-CMOS bootstrap

B. TRNG Entropy Source

The entropy source is based on 10 ring oscillators, each composed of one NAND gate, and 10 inverters, totaling 11 inverting blocks, along with a buffer at the oscillator output. The oscillator schematic is represented in Fig. 2 b). These oscillators are activated sequentially to introduce randomness into the system. An enable signal triggers the first oscillator, driving the initial inverting stage (NAND gate) and initiating oscillation.

To ensure each oscillator operates out-of-phase, thereby enhancing randomness, each subsequent oscillator is activated with a delay. This delay is introduced by sampling the signal after the third inverting stage. The sampled signal is then passed to a resistive load DFF, which controls the activation of the next oscillator stage. The resistive load DFF was selected for its high V_{OH}, lower area and power consumption and because resistors are a primary source of noise, thereby increasing the entropy of the system.

To further improve oscillator performance, stage capacitors are used to introduce a slight delay, improving singal stability in IGZO-TFT circuits. A buffer stage is incorporated at the oscillator outputs to compensate the limited drive capabilities of the inverters, ensuring stable signal transmission. Resistive load inverters and NAND gates are used due to their higher jitter characteristics compared to pseudo-CMOS or enhancement-mode gates. This jitter contributes beneficially to the overall entropy, thereby enhancing the randomness of the system.

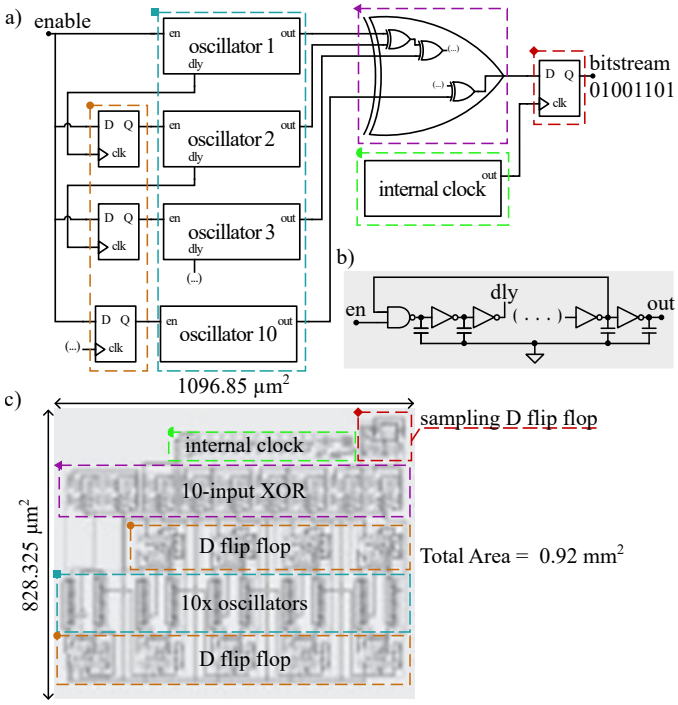

Fig. 2. a) Circuit schematic b) Oscillator schematic c) Circuit layout.

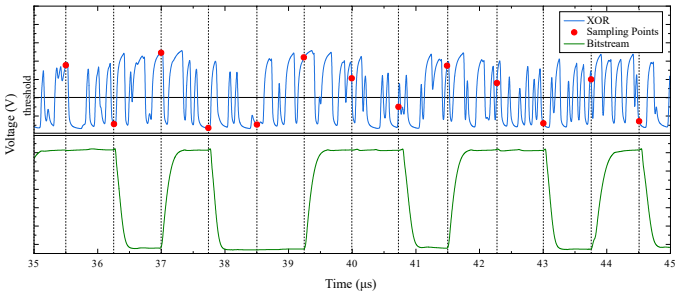

Fig. 3. Simulated TRNG final output (top) and XOR output (bottom) overlaid with sampling points (dots).

Finally, a 10-input XOR gate is implemented by cascading nine two-input XOR gates. This XOR combines the outputs of the oscillators, leveraging the jitter in each signal to produce a noisy signal to enhance the overall randomness. The output signal from the XOR is shown in Fig. 3, showing the result of XORing the signal from 10 oscillators.

Pseudo-CMOS bootstrap logic is used for the XOR gates to ensure faster response times which allows the XOR to accurately process the oscillator signals without delay, preventing any compromise in the expected XOR result that could lead to biased outputs. Alternative configurations were simulated, but they led to skewed results, with outputs tending towards biased values over time, ultimately compromising the quality of the random numbers.

C. TRNG Entropy Extraction

The entropy extraction consists of a pseudo-CMOS bootstrap DFF, which samples the output of the XOR gate with the use of an internal clock. The sampling points are represented in Fig. 3 as red dots which match with the rising edge of the internal clock.

The pseudo-CMOS bootstrap DFF, was chosen for its superior response time, ensuring precise sampling of the signal. Sampling occurs at significantly lower frequency than the XOR gate's output, which reduces correlation between successive samples and further improves the quality of the generated random bits.

The clock signal that triggers the DFF is generated by a ring oscillator composed of pseudo-CMOS bootstrap logic gates, providing a robust signal with operation close to the supply rails, fast switching times and low jitter. Each sampled value represents a bit of the final bitstream.

IV. Simulation Results

In this section, we present a simulation circuit analysis of the jitter, performance, energy efficiency, and throughput of the proposed circuit, along with NIST randomness test results. The TRNG has been designed in the Pragmatic 600 nm IGZO-TFT technology with a supply voltage (VDD) of 3 V, at 25 °C and a load of 1 pF (nominal conditions). The simulation results were obtained through transient noise analysis on Cadence ADE Assembler. Additionally, we evaluate the circuit's performance under a 10% supply voltage variation and across different process corners.

To ensure realistic simulation results, the circuit's layout was designed, and all simulations were based on post-layout parasitic extraction. The layout was also performed with the goal of minimizing area while maintaining uniform signal paths between the oscillators (Fig. 2 c)). Fig. 2 also correlates components between the schematic and the layout using corresponding symbols for clarity.

To accurately assess jitter, multiple noise seeds were used, allowing for the evaluation of both average jitter and standard deviation across different test runs.

A. Jitter

The period jitter was measured across all 10 ring oscillators under nominal conditions, resulting in an average absolute value of 0.33 ps and a standard deviation of approximately 381 ps, indicating significant random variations between periods. Fig. 4 illustrates the jitter from a single oscillator, where the average jitter is near zero because the calculation of period jitter derives the average frequency over the simulation time and determines the deviation of each period from that average. The operating frequencies of the ring oscillators were measured, with all blocks oscillating consistently at approximately 1.48 MHz under nominal conditions.

B. Performance

To evaluate the overall efficiency of the design, performance metrics such as energy per bit, power consumption and throughput were measured across corners. The results, summarized in Table I, include both nominal conditions and worst-case scenarios for each metric.

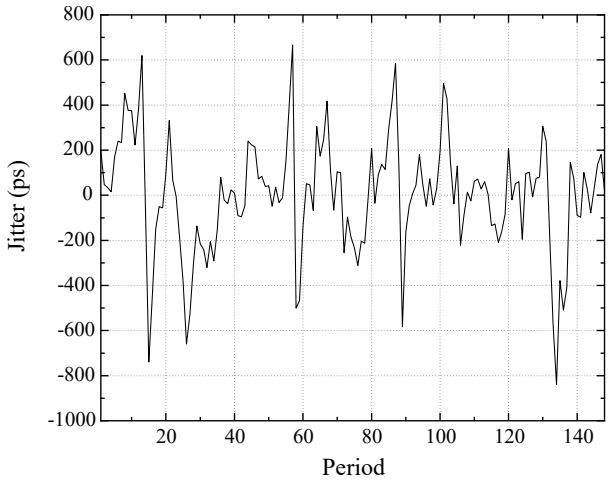

Fig. 4. Simulated period jitter of one oscillator.

The final output signal, used to evaluate the TRNG randomness, is displayed in Fig. 3 above the XOR signal. The results show that the final output correctly reflects the sampled value. When the XOR output is at low at the time of sampling, the DFF output decreases, indicating a logic "0". Conversely, when the XOR is sampled at a higher voltage, the final output rises to near the rail voltage, representing a logic "1".

To evaluate randomness, bitstreams were collected from the circuit's final output signal using a Python script that evaluated the clock signal, detected the final output rising edges, and collected voltage values of the final output after a delay, ensuring the circuit had enough time to respond to the stimulus. These bitstreams were then processed through NIST testing suite to evaluated randomness.

The NIST test suite consists of 15 tests, however some of these require large bit sequences, often on the order of 10^6 bits. Due to the computational complexity and extensive simulation time needed to generate larger bitstreams, only 2K bits sequence was extracted. As a result, we are able to run 8 out of 15 tests, all of which were passed under nominal conditions. Table II presents the NIST test suite results under nominal conditions, that are comparable with the results of traditional TRNGs implemented in CMOS technology.

TABLE I
TRNG SUMMARIZED SIMULATION RESULTS

Parameter	Nominal	Worst-Case
Area (mm^2)	0.920	
RMS Power (mW)	6.23	10.52
Energy per Bit (nJ/bit)	4.68	6.66
Throughput (Mbit/s)	1.33	0.74

V. Conclusion

The proposed TRNG, based on jittered oscillator sampling and implemented in 600 nm IGZO-TFT FlexIC technology, achieved a throughput of 1.33 Mbit/s with an energy consumption of 4.68 nJ/bit and an area of 0.920 mm^2. To the best of the authors' knowledge, this is the first implementation of a TRNG using TFT technology, making direct comparisons in terms of area, energy, and throughput challenging as it cannot be compared with implementation at different technologies. However, the statistical properties of the design can be compared: the TRNG successfully passed 8 NIST tests under nominal conditions. These results demonstrate promising potential for the development of TRNGs in TFT technology.

The ability to implement TRNGs in TFT technology opens new opportunities for embedding hardware security into various applications, such as wearable electronics, biomedical devices, and communication devices. This integration improves the security of these devices while retaining the inherent advantages of TFT technology, including flexibility, low-cost manufacturing, and suitability for large-area implementations.

References

[1] S. Bi, B. Gao, X. Han, Z. He, J. Metts, C. Jiang, and K. Asare-Yeboah, "Recent progress in printing flexible electronics: A review," *Science China Technological Sciences*, vol. 67, pp. 2363–2386, Aug. 2024.

[2] M. Alioto, "Trends in Hardware Security: From Basics to ASICs," *IEEE Solid-State Circuits Magazine*, vol. 11, no. 3, pp. 56–74, 2019.

[3] M. Grujić, V. Rožić, D. Johnston, J. Kelsey, and I. Verbauwhede, "Design Principles for True Random Number Generators for Security Applications," in *Proceedings of the 56th Annual Design Automation Conference 2019*, (Las Vegas NV USA), pp. 1–3, ACM, June 2019.

TABLE II
TRNG NIST RANDOMNESS TEST RESULTS CMOS COMPARISON

Test	This work IGZO-TFT		CICC'24 [15] CMOS		VLSI Tech. and Circuits'23 [16] CMOS		A-SSCC'21 [17] CMOS	
	p-value	Result	p-value	Result	p-value	Result	p-value	Results
Frequency (Monobit) Test	0.79	Pass	0.437	20/20 Pass	0.212	100/100 Pass	0.749	985/1000 Pass
Frequency Test within a Block	1.00	Pass	0.0001	20/20 Pass	0.016	100/100 Pass	0.138	979/1000 Pass
The Runs Test	0.93	Pass	0.067	18/20 Pass	0.887	99/100 Pass	0.635	988/1000 Pass
Tests for the Longest-Run-Of-Ones in a Block	0.37	Pass	0.964	20/20 Pass	0.01	97/100 Pass	0.534	990/1000 Pass
The Non-overlapping Template Matching Test	Pass*		Pass*		Pass*		Pass*	
The Serial Test**	0.50	Pass	0.213	19/20 Pass	0.348	98/100 Pass	0.879	981/1000 Pass
The Approximate Entropy Test	1.00	Pass	0.116	18/20 Pass	0.577	97/100 Pass	0.986	986/1000 Pass
The Cumulative Sums (Cusums) Test**	0.83	Pass	0.740	20/20 Pass	0.117	98/100 Pass	0.576	986/1000 Pass

* Test with several subtests, some papers only show if it passed or not.

** Tests with two subtests. P-value is the median values and pass ratio is of the subtest with least pass.

[4] S. M. S. Faramarzi, N. Papadopoulos, J. Genoe, and K. Myny, "Flexible TFT Read-out Circuit Blocks for Large Area Sensor Array System Integration Measuring Photovoltaic Modules and Batteries," *IEEE Journal on Flexible Electronics*, pp. 1–1, 2024.
[5] H. Celiker, A. Sou, B. Cobb, W. Dehaene, and K. Myny, "Flex6502: A Flexible 8b Microprocessor in 0.8µm Metal-Oxide Thin-Film Transistor Technology Implemented with a Complete Digital Design Flow Running Complex Assembly Code," in *2022 IEEE International Solid- State Circuits Conference (ISSCC)*, (San Francisco, CA, USA), pp. 272–274, IEEE, Feb. 2022.
[6] D. Sousa, J. Marcelino, Â. Santos, H. Viana, J. Xavier, P. Barquinha, P. Toledo, and P. Crovetti, "A Pseudo-CMOS bootstrap DIGOTA in a 600nm Flexible IGZO Technology," *International Flexible Electronics Technology Conference*, 2024.
[7] A. Sharma, P. Bahubalindruni, M. Bharti, and P. Barquinha, "High gain operational amplifier and a comparator with a-IGZO TFTs," *IET Circuits, Devices & Systems*, vol. 14, no. 78, pp. 1214–1219, 2020.
[8] D. C. Monga and K. Halonen, "Flexible RF to DC Converter for Wireless Power Transfer in NFC and Biomedical Systems," in *2024 IEEE International Conference on Flexible and Printable Sensors and Systems (FLEPS)*, (Tampere, Finland), pp. 1–4, IEEE, June 2024.
[9] Y. Ma, Y. Zhang, S. Cai, Z. Han, X. Liu, F. Wang, Y. Cao, Z. Wang, H. Li, Y. Chen, and X. Feng, "Flexible Hybrid Electronics for Digital Healthcare," *Advanced Materials*, vol. 32, p. 1902062, Apr. 2020.
[10] V. Fiore, P. Battiato, S. Abdinia, S. Jacobs, I. Chartier, R. Coppard, G. Klink, E. Cantatore, E. Ragonese, and G. Palmisano, "An Integrated 13.56-MHz RFID Tag in a Printed Organic Complementary TFT Technology on Flexible Substrate," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 62, pp. 1668–1677, June 2015.
[11] E. Ozer, J. Kufel, J. Myers, J. Biggs, G. Brown, A. Rana, A. Sou, C. Ramsdale, and S. White, "A hardwired machine learning processing engine fabricated with submicron metal-oxide thin-film transistors on a flexible substrate," *Nature Electronics*, vol. 3, pp. 419–425, July 2020.
[12] J. Kim and H. Chae, "A 10-Gbps, 0.121-pJ/bit, All-Digital True Random-Number Generator using Middle Square Method," in *2022 IEEE Asian Solid-State Circuits Conference (A-SSCC)*, (Taipei, Taiwan), pp. 1–3, IEEE, Nov. 2022.
[13] R. Zhang, X. Wang, K. Liu, and H. Shinohara, "A 0.186-pJ per Bit Latch-Based True Random Number Generator Featuring Mismatch Compensation and Random Noise Enhancement," *IEEE Journal of Solid-State Circuits*, vol. 57, pp. 2498–2508, Aug. 2022.
[14] M. Kim, U. Ha, K. J. Lee, Y. Lee, and H.-J. Yoo, "A 82-nW Chaotic Map True Random Number Generator Based on a Sub-Ranging SAR ADC," *IEEE Journal of Solid-State Circuits*, vol. 52, pp. 1953–1965, July 2017.
[15] J. Hao, Q. Zhuang, J. Zhang, and X. Zhao, "A 98fJ/Bit Current-Starved-Ring-Oscillator-Based TRNG with High PVT Tolerance and Resilience to Frequency Injection Attack Up to 1V," in *2024 IEEE Custom Integrated Circuits Conference (CICC)*, (Denver, CO, USA), pp. 1–2, IEEE, Apr. 2024.
[16] Y. He and K. Yang, "A Fully Synthesizable 100Mbps Edge-Chasing True Random Number Generator," in *2023 IEEE Symposium on VLSI Technology and Circuits (VLSI Technology and Circuits)*, (Kyoto, Japan), pp. 1–2, IEEE, June 2023.
[17] X. Cheng, H. Zhu, X. Xing, Y. Zhang, Y. Zhang, G. Xie, and Z. Zhang, "A Feedback Architecture of High Speed True Random Number Generator based on Ring Oscillator," in *2021 IEEE Asian Solid-State Circuits Conference (A-SSCC)*, (Busan, Korea, Republic of), pp. 1–3, IEEE, Nov. 2021.
[18] B. Sunar, W. Martin, and D. Stinson, "A Provably Secure True Random Number Generator with Built-In Tolerance to Active Attacks," *IEEE Transactions on Computers*, vol. 56, pp. 109–119, Jan. 2007.
[19] J. Cabacinho, J. Casaleiro, and L. Oliveira, "Design of a 28nm CMOS Self-Biased Ring Oscillator for Intrinsically Robust PVT TRNG," in *2023 18th Conference on Ph.D Research in Microelectronics and Electronics (PRIME)*, (Valencia, Spain), pp. 225–228, IEEE, June 2023.