# A Synthesizable Thyristor-Like Leakage-Based True Random Number Generator

Seohyun Kim[1], Jang Hyun Kim[1,2] and Jongmin Lee[1,2]
[1]Dept. of Intelligent Semiconductor Engineering, Ajou University, Suwon, Korea
[2]Dept. of Electrical and Computer Engineering, Ajou University, Suwon, Korea
{ksh9954, janghyun, jongmin}@ajou.ac.kr

***Abstract*—As the demand for random data in cryptographic systems continues to rise, the importance of True Random Number Generators (TRNGs) becomes increasingly crucial for securing cryptographic applications. However, designing a TRNG that is reliable, secure, and cost-effective presents a significant challenge in hardware security. In this paper, we propose a synthesizable TRNG design based on a thyristor-like leakage-based (TL) structure, optimized for secure applications with small area and cost-efficiency. Our design has been validated using a 65-nm CMOS process, achieving a throughput of 0.397-Mbps within a compact area of 14.4-μm$^2$, offering considerable cost savings while maintaining high randomness and area-throughput trade-off of 27.57 Gbps/mm$^2$. Moreover, this TRNG can be synthesized as a standard cell through a semi-custom design flow, significantly reducing design costs and enabling design automation, which streamlines the process and reduces the time and effort required compared to traditional full-custom TRNGs. Additionally, as it is library characterized, the number of TL TRNG cells can be freely adjusted to meet specific application requirements, offering flexibility in both performance and scalability. To assess its randomness, the NIST statistical test suite was applied, and the proposed TL TRNG successfully passed all applicable tests, demonstrating its randomness.**

***Keywords—TRNG, Hardware security, Leakage-based, Synthesizable, Low-cost***

## I. Introduction

As the Internet of Things (IoT) and Artificial Intelligence (AI) continue to advance, a growing number of devices are collecting and processing user data to offer personalized services. AI, in particular, leverages this data to enhance its learning capabilities, further improving user experience. While these technological innovations have undoubtedly improved the quality of life, they have simultaneously heightened concerns about user privacy and data security. To protect personal information, cryptographic systems must rely on highly secure cryptographic keys, which can only be generated through the use of TRNGs. The inclusion of TRNGs is thus essential for strengthening the security and robustness of these systems.

In parallel, the rise of quantum computing presents significant threat to existing cryptographic infrastructures. Algorithms such as Shor's [1] have demonstrated that quantum computers, with their ability to use qubits and parallel processing, can break traditional encryption methods like Rivest-Shamir-Adleman (RSA) cryptography algorithm at unprecedented speeds. This challenge to current security systems is driving the development of Post-Quantum Cryptography (PQC) algorithms, which are designed to resist attacks by quantum computers. However, these PQC algorithms require large amounts of random numbers to perform cryptographic operations that can resist quantum computer-based attacks.

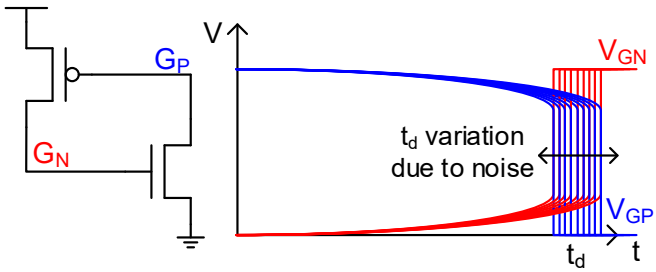


Fig. 1. Thyristor-like leakage-based structure and its operation.

TRNGs play a critical role across a range of security applications, from small-scale security systems to more sophisticated PQC accelerator-based systems. However, current TRNG designs encounter several limitations, such as difficulties in generating sufficient random numbers within restricted areas [2] Additionally, when designed as hard macros, TRNGs often struggle with parallel operation [3]-[6]. Furthermore, analog circuit-based TRNGs are particularly vulnerable to variations in process, supply voltage, and temperature (PVT) [7]-[8], and when CMOS-incompatible devices like MRAM are used, manufacturing costs escalate [9]-[10]. Even with digital circuit-based TRNGs, which are synthesizable, the scalability of parallelizing these modules is restricted due to their large size [11]-[14].

To overcome these obstacles, this paper introduces a thyristor-like leakage-based TRNG (TL TRNG), designed for implementation as a standard cell. This TL TRNG is capable of generating random numbers within a small area and can easily scale its throughput by parallelizing multiple TL TRNG cells. Additionally, the library characterization of the TL TRNG enables design automation, similar to that of digital circuits, which substantially reduces design costs. By addressing the limitations of hard macro-based TRNGs, this approach offers a cost-efficient solution for generating random numbers in a variety of digital circuits, introducing IoT device application processors (APs) and PQC accelerator-based hardware security systems.

The remainder of this article is organized as follows: In Section II, the operating principles of the TL TRNG are

978-3-9826741-0-0/DATE25/© 2025 EDAA

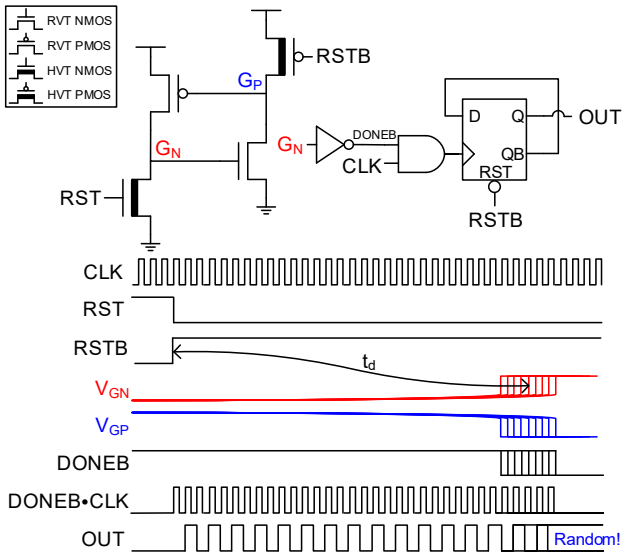


Fig. 2. Schematic of TL TRNG and its operation.

explained. Section III covers the implementation using TL TRNG cells and the library characterization process. Section IV analyzes the performance and randomness of the TL TRNG through simulations, and Section V concludes this article.

## II. Operating Principle of Thyristor-Like Leakage-Based TRNG (TL TRNG) Cell

The proposed thyristor-like leakage-based (TL) structure shown in Fig. 1 consists of a pair of PMOS and NMOS transistors which was previously used as a pair of PUF cell [15]. In the initial state, the $G_p$ node is pre-charged and the $G_n$ node is pre-discharged. When the circuit is triggered, the sub-threshold leakage currents from the PMOS and NMOS gradually charge and discharge the $G_n$ and $G_p$ nodes, respectively. During this process, the leakage current slowly changes the potential of $G_p$ and $G_n$, and random noise is gradually accumulated. Once the potentials of $G_n$ and $G_p$ have shifted sufficiently, the PMOS and NMOS transistors turn on, causing the $G_p$ and $G_n$ nodes to latch rapidly through positive feedback. The noise accumulated over the long period during which the potentials change due to the leakage current leads to significant variations in the time $t_d$ from the initial state to the completion of latching.

Fig. 2 illustrates the TRNG circuit designed using the TL structure. Pre-charge PMOS and pre-discharge NMOS transistors, controlled by RST and RSTB signals, reset the $G_n$ and $G_p$ nodes to their initial voltages. These transistors are implemented with high-threshold voltage (HVT) devices to ensure that the latching delay is primarily governed by the sub-threshold leakage current of the regular-threshold (RVT) transistors in TL structure. After releasing the RST signal, the TRNG begins to accumulate random noise as the potential of $G_p$ decreases and $G_n$ increases. Simultaneously, a gated clock signal is applied to the flip-flop, causing the OUT signal to toggle with each rising edge of the clock. As the leakage current shifts the potentials at $G_p$ and $G_n$, the transistors eventually exceed their threshold voltage, triggering a rapid latching through positive feedback. This process halts the clock applied to the flip-flop, allowing the accumulated noise to introduce sufficient variation

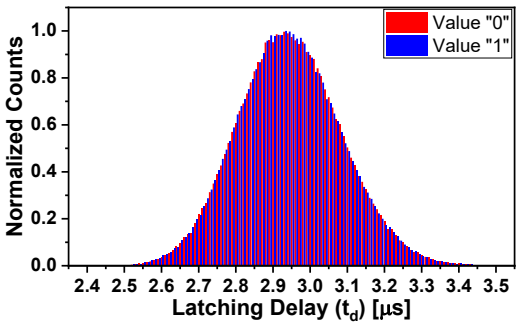


Fig. 3. Latching delay distribution of TL TRNG

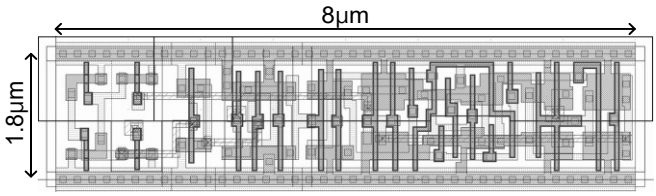


Fig. 4. TL TRNG layout with synthesizable standard cell shapes.

in $t_d$, thus making the OUT signal a source of randomness and a reliable entropy source.

In Fig. 3, the distribution of latching delays for the TL TRNG implemented in a 65-nm CMOS process is observed. The simulation results demonstrate that the TL TRNG accumulates enough noise during the extended latching delay to serve as a viable entropy source. Specifically, the TL TRNG cell latches on average after 2.94-µs, with a variance of 0.14-µs due to the accumulated noise. This provides ample time for noise accumulation within typical digital circuit clock frequencies, which range from hundreds of MHz to GHz. As depicted in Fig. 3, the latching delay distribution is broad relative to the clock period. For instance, when a 200-MHz clock signal is applied to the TL TRNG cell, the wide variation in latching delays results in equal probabilities of generating 0s and 1s, confirming that the TL TRNG can reliably generate random numbers with high entropy.

## III. Library Characterization and Parallelization of the TL TRNG Cell

Many prior art TRNG designs have been developed over the years, but most are implemented as hard macros [2]-[10], which come with inherent limitations. While some TRNGs have been implemented as soft macros [11]-[14], their relatively large macro block size limits parallelization to improve throughput. However, as IoT devices and AI technologies continue to evolve, the need for data security in cost-sensitive devices is becoming more pressing. Alongside the rise of quantum computing, PQC accelerators require large volumes of random numbers to maintain security. This increasing demand highlights the necessity of TRNGs that are not only compact size but also easily scalable in terms of throughput. Therefore, a critical consideration in TRNG design is ensuring the ease of parallelization to enhance throughput while minimizing non-recurrent engineering costs during the chip design process.

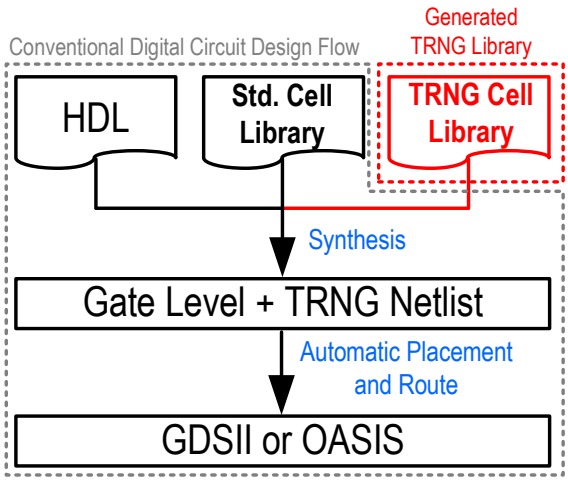


Fig. 5. Automated design flow of proposed TL TRNG.

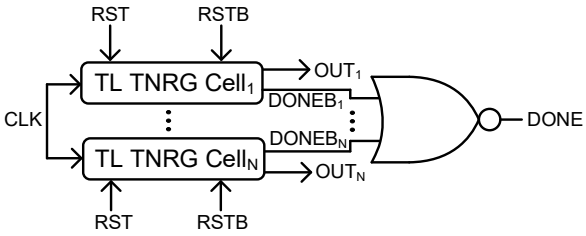


Fig. 6. Block diagram of parallelized TL TRNGs.

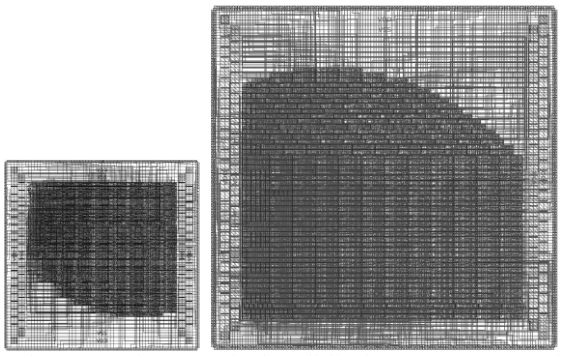

Fig. 7. Placement and route result of parallelized TL TRNGs generated from TL TRNG library for high-speed true random number generation. (128 TL TRNGs parallelized version (left), 512 TL TRNGs parallelized version (right))

To address these challenges and optimize both parallelization and cost-efficiency, library characterization of the TL TRNG cell was conducted. As depicted in Fig. 4, the layout of the TL TRNG cell was designed as a multiple of a unit tile, allowing the generation of random numbers within a small area of just 14.4-μm$^2$, tailored to the specific requirements of the library characterization as a standard cell. This standard cell layout enables flexibility and scalability. The characterization of proposed TL TRNG cell, based on its schematic and layout, provides the foundation for its integration into standard cell libraries.

Fig. 5 demonstrates the design flow employed using the characterized TL TRNG library. In this flow, the HDL code for the parallelized TL TRNG is synthesized together with the soft macro HDL code, the TL TRNG library, and the standard cell library. This synthesis process results in a netlist that integrates

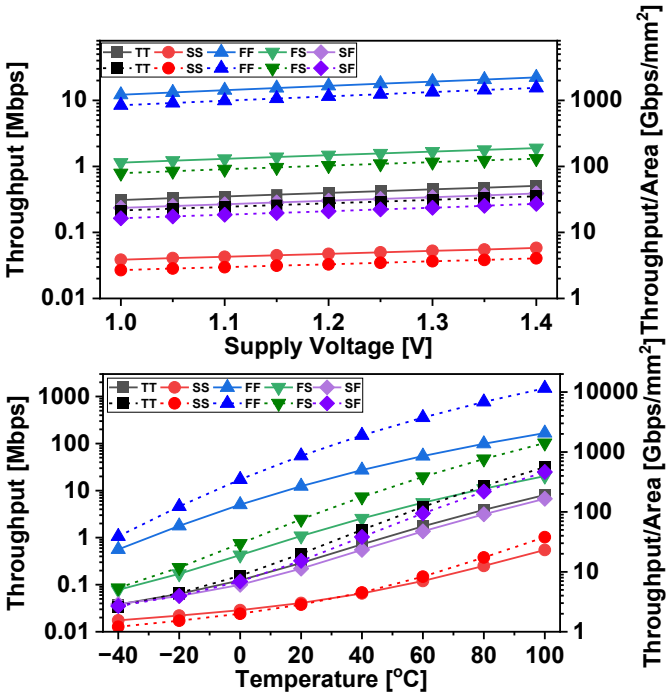


Fig. 8. Throughput and Area-throughput trade-off of single TL TRNG cell against supply voltage and temperature changes. (Solid line: Throughput, Dotted line: Area-throughput trade-off)

gate-level logic with the TL TRNG cells. The generated netlist then undergoes placement and routing to implement the parallelized TL TRNGs and soft macro as a single GDS.

As shown in Fig. 6, multiple TL TRNG cells can be arranged in parallel to generate N-bit random numbers by configuring N TL TRNG cells in parallel. The DONE signal, which indicates the successful generation of random numbers, is produced by a NOR operation on the DONEB$_k$ signals ($1 \le k \le N$) from each TL TRNG cell. It is important to note that the parallel arrangement shown in Fig. 6 is just one example, and various parallelization schemes can be applied depending on the specific requirements of the system being designed.

Fig. 7 illustrates the implementation results of the parallelized TL TRNG, as shown in Fig. 6, realized as a single digital module using the standard cell library and the TL TRNG cell library, following the design flow depicted in Fig. 5. On the left side of Fig. 7, the synthesis, placement, and routing results for 128 parallel TL TRNG cells are presented, while the right side shows the corresponding results for 512 parallel TL TRNG cells. With a core utilization rate of 0.8, core areas of 2,410-μm$^2$ for the 128-cell configuration and 9,801-μm$^2$ for the 512-cell configuration were achieved. These results clearly demonstrate that, by leveraging the TL TRNG library, TRNGs can be easily configured in parallel to deliver the required throughput. Moreover, the design seamlessly integrates multiple TRNGs into a single module using standard cell and TL TRNG cell libraries, ensuring efficient area utilization and scalability.

## IV. Implementation Results of TL TRNG

The proposed TL TRNG was implemented as a standard cell in a 65-nm CMOS process. To validate its effectiveness as a TRNG, both performance and randomness were thoroughly

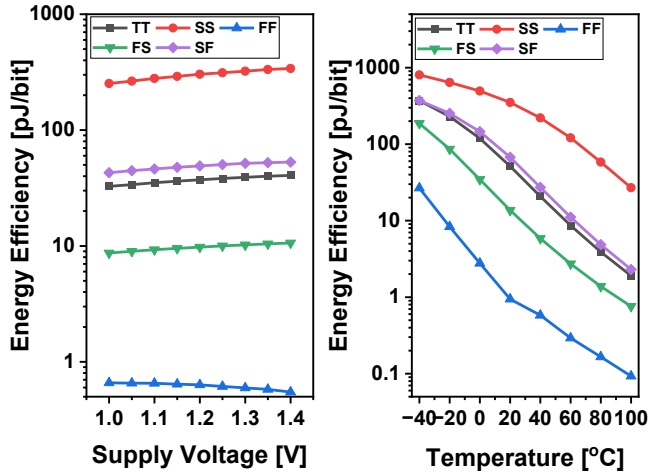


Fig. 9. Energy efficiency over supply voltage and temperature variations.

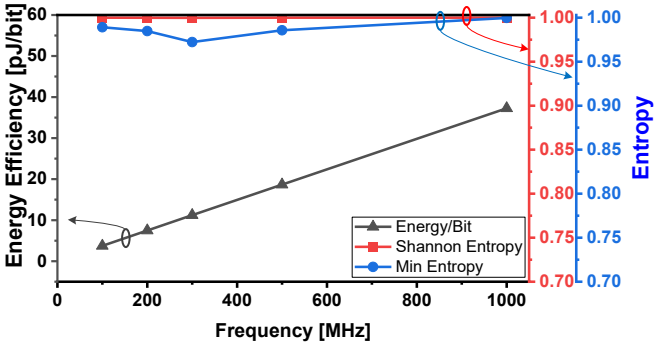


Fig. 10. Energy efficiency, Shannon entropy and min-entropy in relation to operating frequency.

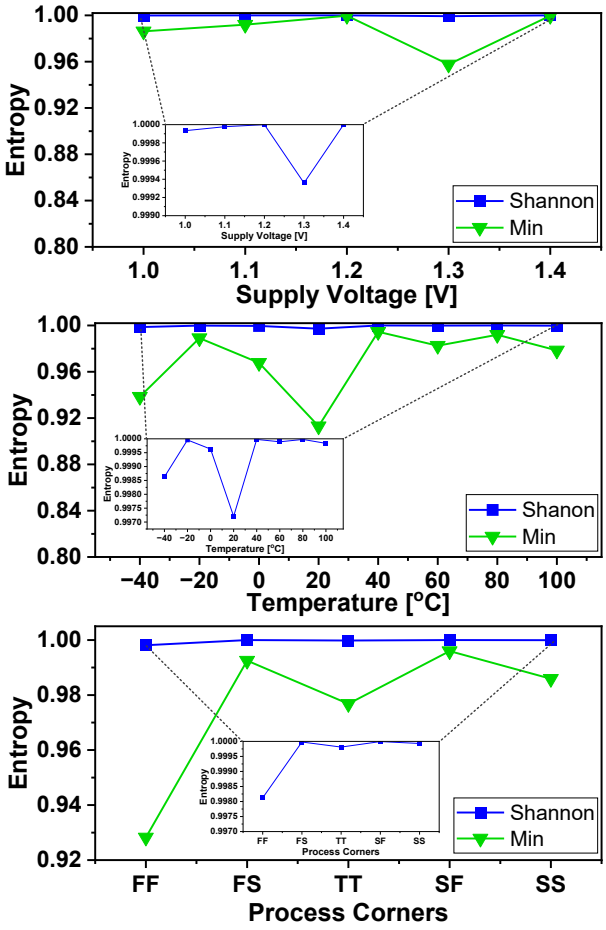


Fig. 11. Shannon and min entropy trend with supply voltage and temperature changes.

evaluated using a variety of metrics, and random values extracted from transient noise simulations were used for the analysis. These assessments were crucial to ensure that the TL TRNG cell meets the necessary criteria for reliable random number generation under diverse conditions.

Fig. 8 illustrates the throughput and performance per unit area of a single TL TRNG cell, with solid and dotted lines representing the two metrics, respectively, across different supply voltages and temperature variations at various process corners. The throughput is calculated as the inverse of the time until the DONEB signal is generated, indicating that the TL TRNG cell has been triggered and the random number generation is completed. Under nominal process, voltage, and temperature (PVT) conditions (TT, 1.2V, 27°C), a single TL TRNG cell generates 0.397-Mbits of random numbers per second. This corresponds to a performance of 27.57-Gbps/mm$^2$, demonstrating that the TL TRNG cell delivers a high rate of random number generation relative to its area. Although throughput tended to decrease in low voltage, low temperature, and slow corner (SS) conditions, it still maintained a reasonable area-throughput trade-off of 1.21-Gbps/mm$^2$ even at -40°C.

Fig. 9 presents the results of analyzing the energy consumed by the TL TRNG cell to generate a single bit of random number under various PVT conditions. At a clock frequency of 1-GHz, the energy efficiency was 37.26-pJ/bit under nominal conditions (TT, 1.2V, 27°C). The TL TRNG cell's architecture, where multiple internal nodes tied to the clock undergo frequent switching, makes the energy efficiency proportional to the number of clock toggles until the TL TRNG cell latches. Consequently, when the TL TRNG cell latches more quickly, the best energy efficiency was observed in high-temperature, high-voltage, and fast corner (FF) conditions, while lower efficiency was noted under low-temperature, low-voltage, and slow-corner (SS) conditions.

Fig. 10 further illustrates how energy efficiency fluctuates with operating frequency, even under consistent PVT conditions. When the clock period is shorter than the latching delay, energy efficiency improves without significantly compromising randomness. This balance is crucial in ensuring optimal performance in power-sensitive applications. As demonstrated, the TL TRNG maintained high entropy levels, even at low clock frequencies such as 100-MHz, showing minimal degradation in randomness. On the other hand, in the case of very low frequencies, where the clock period is not significantly different from the latching delay, a substantial difference in the sampling rates of "1" and "0" occurs, leading to a randomness degradation. Therefore, TL TRNG must be operated at a sufficient frequencies.

Fig. 11 shows how entropy varies with changes in supply voltage, temperature and process corner. Despite fluctuations in

TABLE I. CORE AREA AND THROUGHPUT TREND OF PARALLELIZED TL TRNGS

| | Number of Parallelized TL TRNGs[a] | | | | |
|---|---|---|---|---|---|
| | **32** | **64** | **128** | **256** | **512** |
| **Ideal Core Area[b] [µm²]** | 460.8 | 921.6 | 1843.2 | 3686.4 | 7372.8 |
| **Implemented Core Area[c] [µm²]** | 580 | 1197 | 2410 | 4788 | 9801 |
| **Throughput [Mbps]** | 6.159 | 13.06 | 25.91 | 46.81 | 120.3 |

[a] Simulated at nominal condition: TT, 1.2V, 27°C
[b] (Cell area) x (Number of parallelized TL TRNGs) [c] Core utilization = 0.8

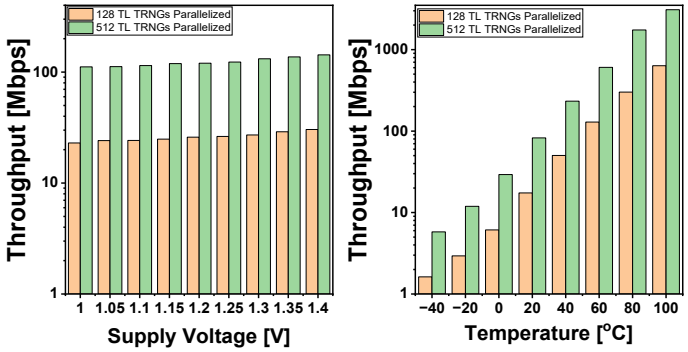


Fig. 12. Throughput of parallelized TL TRNGs (512 TL TRNG cells) against supply voltage and temperature changes.

these conditions, the TL TRNG cell consistently achieved a Shannon entropy greater than 0.997 and a min-entropy exceeding 0.913, indicating that the TL TRNG produces 0s and 1s with virtually identical probability without post processing. This consistency in entropy highlights the robustness of the TL TRNG in generating random numbers with stable randomness, regardless of environmental variations.

To maximize the effectiveness of the TL TRNG cell, it is crucial to ensure that its throughput meets the specific requirements of the application. For high-performance use cases, such as pairing with a PQC accelerator that demands a large volume of random numbers, parallel utilization of TL TRNG cells become essential. The parallelized configuration allows the generation of random numbers at the required rate within the specified time frame. While the exact method of parallelizing TL TRNG cells may vary based on the application, this paper evaluates the performance of a simple parallel utilization structure by varying the value of N in the parallelized TL TRNG structure, as shown in Fig. 7.

Table I shows the results of increasing the number of parallelized TL TRNG cells from 32 to 512 and analyzing the corresponding changes in area and throughput. The results indicate that with 32 cells in parallel, a throughput of 6.159-Mbps was achieved within an area of 580-µm$^2$. When 512 cells were used in parallel, the area increased to 9,801-µm$^2$, yielding a throughput of 120.3-Mbps. These results are highly competitive, even when compared to [13], which recorded a throughput of 100.8-Mbps in an area of 7,647-µm$^2$.

Fig. 12 presents the analysis of throughput for various configurations of parallelized TL TRNG cells under varying supply voltages and temperature changes. With 128 cells in

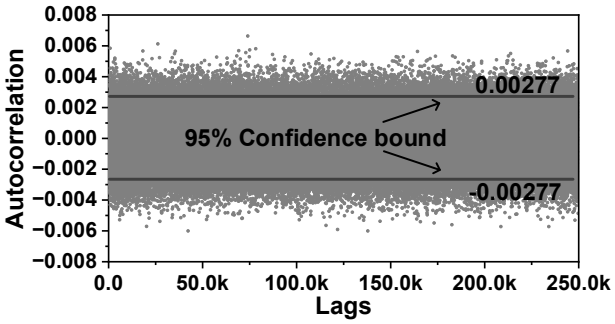


Fig. 13. Autocorrelation of proposed TL TRNG.

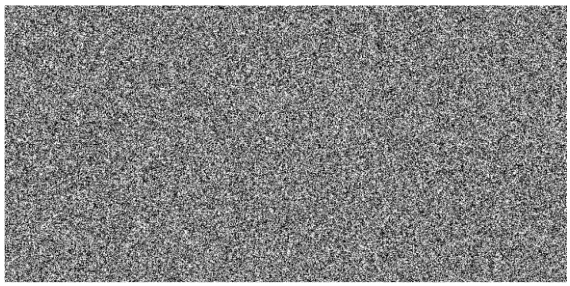

Fig. 14. Speckle pattern of TL TRNG.

parallel, the throughput of random number generation ranged from 23-Mbps to 30-Mbps depending on supply voltage changes, while temperature fluctuations caused a more significant deviation, varying between 1.62-Mbps and 635-Mbps. In the case of 512 parallel cells, the throughput ranged from 111-Mbps to 143-Mbps across different supply voltages but showed larger deviations due to temperature changes, with values between 5.78-Mbps to 3.09-Gbps. For comparison, [13] exhibited substantial variations in throughput, from 40-Mbps to 100-Mbps, when exposed to supply voltage changes. However, the proposed TL TRNG provides the distinct advantage of flexible cell parallelization, which can improve the worst case throughput under different conditions.

To assess the randomness of the proposed TL TRNG, an autocorrelation analysis was performed, as shown in Fig. 13. This analysis measured the correlation between random numbers generated at different time intervals. The autocorrelation function, with a 95% confidence interval of ±0.00277, indicates an extremely low correlation between previously generated and currently generated random numbers. This demonstrates that the random numbers generated by the TL TRNG are uncorrelated with previously generated random numbers. Additionally, the speckle pattern in Fig. 14 visually confirms that the generated random numbers are evenly distributed between 0s and 1s, lacking any detectable regularity, which highlights the true randomness of the TL TRNG.

Furthermore, the randomness of the TL TRNG was evaluated using the NIST SP800-22 statistical test suite, a standard tool for assessing randomness. The TL TRNG passed all applicable test items, as summarized in Table II. The NIST SP 800-90B test suite was also evaluated. In the IID test, the min-entropy was 0.9934 bits, and the Chi-square (Independence), Chi-square (Goodness-of-fit), LRS Test, and IID permutation tests were all successfully passed. The results

TABLE II. RESULT OF NIST SP800-22 RANDOMNESS TESTS FOR TL TRNG

| Test Name | Avg. P-Value | Pass Rate | Pass? |
|---|---|---|---|
| **Approximate Entropy** | 0.502 | 0.98 | Pass |
| **Block Frequency** | 0.509 | 0.98 | Pass |
| **Cumulative Sums** | 0.594 | 1 | Pass |
| **FFT** | 0.482 | 1 | Pass |
| **Frequency** | 0.597 | 1 | Pass |
| **Longest Run** | 0.531 | 1 | Pass |
| **Non-Overlapping Template** | 0.514 | 0.984 | Pass |
| **Rank** | 0.461 | 0.98 | Pass |
| **Runs** | 0.456 | 0.96 | Pass |
| **Serial** | 0.491 | 0.99 | Pass |

Tested condition: 0.5Mbit, TT, 1.2V, 27°C

TABLE III. RESULT OF NIST SP800-90B RANDOMNESS TESTS FOR TL TRNG

| Test Name | p-max | h-min |
|---|---|---|
| **MCV** | 0.502 | 0.993 |
| **Collision** | 0.536 | 0.899 |
| **Markov** | 3.50E-39 | 0.997 |
| **Compression** | 0.0206 | 0.933 |
| **t-Tuple** | 0.534 | 0.905 |
| **LRS** | 0.501 | 0.996 |
| **Multi-MCW** | 0.519 | 0.944 |
| **Lag** | 0.501 | 0.996 |
| **Multi-MMC** | 0.532 | 0.909 |
| **LZ78Y** | 0.502 | 0.994 |

Tested condition: 1Mbit, TT, 1.2V, 27°C

of the non-IID tests are summarized in Table III, confirming that the random numbers generated by the TL TRNG meet the stringent criteria required for cryptographic applications.

The performance of the proposed TL TRNG, along with its comparison to prior state-of-the-art designs, is summarized in Table IV. While the TL TRNG was designed with a minimal area to facilitate its integration into standard cell libraries, leading to a slightly lower throughput than some competing designs, the throughput per unit area remains highly competitive. Additionally, the library characterization of the TL TRNG allows it to be synthesized alongside any digital circuit that requires a TRNG, making it suitable for integration as a single IP block. This flexibility, combined with reduced design costs and scalability, distinguishes the proposed TL TRNG from conventional designs.

## V. CONCLUSION AND PERSPECTIVES

A synthesizable thyristor-like leakage-based True Random Number Generator (TL TRNG) is proposed in this paper. The proposed TL TRNG addresses key challenges in the hardware security primitive design, particularly in cost-efficiency, scalability and design automation. The proposed TL TRNG cell was designed and evaluated using a 65-nm CMOS process, achieving a throughput of 0.397-Mbps in a compact area of 14.4-$\mu m^2$, resulting in an impressive throughput per area of 27.57-Gbps/$mm^2$. The randomness of the generated numbers was rigorously tested using the NIST randomness test suites, where the TL TRNG passed all applicable tests, confirming its robustness as a reliable entropy source.

TABLE IV. PERFORMANCE COMPARISONS WITH PRIOR ARTS

| | Proposed | [10] | [13] | [14] |
|---|---|---|---|---|
| **Technology** | 65-nm | 28-nm | 65-nm | 4-nm |
| **CMOS-Compatibility** | Yes | No[a] | Yes | Yes |
| **Synthesizability** | Yes | No | Yes | No |
| **Throughput [Mbps]** | 0.397[b.] | 35.1[c] | 100.8 | 60 |
| **Area [$\mu m^2$]** | 14.4[b] | 402 | 7647.25[d] | 1289 |
| **Throughput/Area [Gbps/mm2]** | 27.57 | 87.31[c] | 13.18[d] | 46.54 |
| **Energy efficiency [pJ/bit]** | 37.26[e] | 18.3 | 27.28 | - |
| **Library Characterization** | Yes | No | No | No |

[a] Using MRAM as an entropy source [b] Single TL TRNG cell [c] 2-bit STT-ANGIE
[d] Including On –chip FSM [e] @1GHz operating frequency

Furthermore, the library characterization of the TL TRNG enables seamless integration into larger digital systems, significantly simplifying the design automation process compared to traditional hard macro-based TRNGs. This reduction in design complexity and cost makes the TL TRNG highly suitable for a wide range of security-critical applications, including IoT devices and Post-Quantum Cryptography (PQC) accelerators, where low-cost and efficient random number generation is paramount. The ability to synthesize the TL TRNG as a part of a semi-custom design flow further enhances design automation, allowing for faster and more cost-effective implementation across various platforms without the need for full-custom design flows.

Looking forward, the scalability of the TL TRNG provides a promising solution for applications requiring large volumes of random numbers, the ability to easily parallelize the TL TRNG cells allows the design to scale up throughput as needed, ensuring that even the most demanding systems, such as PQC-based cryptographic frameworks, can benefit from the TL TRNG's flexibility. As demonstrated, increasing the number of parallelized TL TRNG cells can effectively meet the requirements of systems that rely heavily on robust and unpredictable randomness, especially in security applications where strong encryption is critical.

In conclusion, the proposed TL TRNG provides a viable, cost-effective solution in the growing demands of cryptographic systems, promoting broader adoption of secure and efficient random number generation in modern digital systems.


## ACKNOWLEDGMENT

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. RS-2023-00249784, RS-2024-00408040). And the EDA Tool was supported by the IC Design Education Center (IDEC), Korea.

## REFERENCES


[1] P. W. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," *Proceedings 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, NM, USA, 1994, pp. 124-134.

[2] V. R. Pamula, et al., "An All-Digital True-Random-Number Generator with Integrated De-correlation and Bias Correction at 3.2-to-86Mb/s, 2.58pJ/bit in 65-nm CMOS," *IEEE Symposium on VLSI Circuits*, Honolulu, HI, USA, 2018, pp. 1-2.

[3] Q. Tang, B. Kim, Y. Lao, K. K. Parhi and C. H. Kim, "True Random Number Generator Circuits Based on Single- and Multi-Phase Beat Frequency Detection," *IEEE Custom Integrated Circuits Conference*, San Jose, CA, USA, 2014, pp. 1-4.

[4] S. K. Mathew, et al., "µRNG: A 300-950 mV, 323 Gbps/W All-Digital Full-Entropy True Random Number Generator in 14 nm FinFET CMOS," *IEEE Journal of Solid-State Circuits*, vol. 51, no. 7, pp. 1695-1704, July 2016.

[5] E. Kim, M. Lee and J. J. Kim, "8Mb/s 28Mb/mJ Robust True-Random-Number Generator in 65nm CMOS Based on Differential Ring Oscillator with Feedback Resistors," *IEEE International Solid-Sate Circuits Conference*, San Francisco, CA, USA, 2017, pp. 144-145.

[6] T. Amaki, M. Hashimoto and T. Onoye, "Jitter Amplifier for Oscillator-Based True Random Number Generator," *Asia and South Pacific Design Automation Confernece (ASP-DAC)*, Yokohama, Japan, 2011, pp.81-82.

[7] S. G. Bae, Y. Kim, Y. Park and C. Kim, "3-Gb/s High-Speed True Random Number Generator Using Common-Mode Operating Comparator and Sampling Uncertainty of D Flop-Flop," *IEEE Journal of Solid-State Circuits*, vol. 52, no. 2, pp. 605-610, Feb. 2017.

[8] J. Kim and H. Chae, "A 10-Gbps, 0.121-pJ/bit, All-Digital True Random-Number Generator using Middle Square Method," *IEEE Asian Solid-State Circuits Confernece*, Taipei, Taiwan, 2022, pp. 1-3.

[9] Y. Qu, J. Han, B. F. Cockburn, W. Pedycz, Y. Zhang and W. Zhao, "A True Random Number Generator based on Parallel STT-MTJs," *Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Lausanne, Switzerland, 2017, pp. 606-609.

[10] B. Perach and S. Kvatinsky, "STT-ANGIE: Asynchronous True Random Number GEnerator Using STT-MTJ," *Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Florence, Itlay, 2019, pp. 264-267.

[11] M. T. Rahman, K. Xiao, D. Forte, X. Zhang, J. Shi and M. Tehranipoor, "TI-TRNG: Technology Independent True Random Number Generator," *ACM/EDAC/IEEE Design Automation Conference (DAC), San Francisco*, CA, USA, 2014, pp. 1-6.

[12] B. Colombier, N. Bochard, F. Bernard and L. Bossuet, "Backtracking Search for Optimal Parameters of PLL-based True Random Number Generator," *Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Grenoble, France, 2020, pp. 1-6.

[13] Y. He and K. Yang, "A Fully Synthesizable 100Mbps Edge-Chasing True Random Number Generator," *IEEE Symposium on VLSI Technology and Circuits*, Kyoto, Japan, 2023, pp. 1-2.

[14] J. Park, Y. K. Lee, K. Bodhan, Y. Choi, J. Shin, H-G. Rhew and J. Shin, "A 60Mb/s TRNG with PVT-Variation-Tolerant Design Based on STR in 4nm," *IEEE International Solid-State Circuits Conference, San Francisco*, CA, USA, 2024, pp. 310-312.

[15] J. Lee, D. Lee, Y. Lee and Y. Lee, "A 445F$^2$ leakage-based physically unclonable Function with Lossless Stabilization Through Remapping for IoT Security" *IEEE International Solid-State Circuits Conference, San Francisco*, CA, USA, 2018, pp. 132-134.