INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2025, VOL. 71, NO. 4, PP. 1-6
Manuscript received July 29, 2024; revised September 2025. doi: 10.24425/ijet.2025.155477

The True Random Number Generator design using a high-noise oscillator

Igor Butryn, Mariusz Derlecki, Arkadiusz Łuczyk, Jakub Jasiński, Andrzej Wielgus, and Krzysztof Siwiec

***Abstract*—The growing importance of creating appropriate safeguards in electronic systems forces design of integrated circuits dedicated for cryptographic purposes. The paper focuses on True Random Number Generator (TRNG) circuits design allowing generation of random bit stream. Presented TRNG architecture uses low frequency high-noise oscillator for sampling high frequency clock signal. The article also describes a method for obtaining a high noise level in the oscillator. Achieved bit rate of designed TRNG equals 1 Mb/s. The circuit dissipates 144 µW. The design of the TRNG, simulation and measurement results of the manufactured IC chips have been described in the paper also. TRNG circuit has been implemented in 180 nm CMOS technology.**

***Keywords*—TRNG; Cryptography; Encryption; Random Numbers; Jitter**

I. Introduction

With the rapid development and widespread adoption of modern technologies, the use of wireless communication systems, contactless smart cards, and contactless payment solutions have become increasingly prevalent in everyday life. These technologies enable fast, convenient, and efficient data exchange and transactions without the need for physical contact. However, this growth also brings new challenges related to data security and user privacy, which must be addressed to ensure the safe use of such systems [1].

As the amount of sensitive information being transmitted wirelessly continues to grow, the demand for robust and reliable security mechanisms becomes critical. In order to safeguard confidential data against unauthorized access or tampering, modern systems rely on encryption algorithms such as DES (Data Encryption Standard) and AES (Advanced Encryption Standard). These cryptographic algorithms form the backbone of secure communication protocols and depend on the availability of high-quality, unpredictable cryptographic keys. The generation of these keys is made possible through Random Number Generators (RNGs), which produce random sequences that serve as the foundation for cryptographic operations. RNGs can be broadly classified into two main types: Pseudo Random Number Generators (PRNGs) and True Random Number Generators (TRNGs). PRNGs use deterministic algorithms and an initial seed value to produce sequences that appear random but are, in fact, predictable if the seed is known. While PRNGs are sufficient for some applications, they do not provide the level of unpredictability required for high-security systems. For security-critical applications, such as those found in contactless smart cards and secure payment terminals, TRNGs are the preferred choice. TRNGs generate truly random values by exploiting inherently unpredictable physical processes, such as electronic noise or oscillator jitter. As a result, TRNGs offer significantly better randomness quality, which is essential for ensuring the strength of encryption and protecting against various forms of cryptographic attacks.

There are several established methods for generating true random numbers, and they can be generally categorized into three major approaches [2]:

1. **Direct amplification of electronic noise** – This method involves using a wideband, high-gain amplifier to capture and amplify the natural thermal or shot noise present in electronic components. The amplified noise is then processed to extract random bits.

2. **Discrete-time chaotic systems** – These systems utilize nonlinear analog circuits designed to exhibit chaotic behavior. The analog signals generated by such systems are inherently unpredictable and can be sampled to produce random digital outputs.

3. **Sampling of a high-frequency oscillator using a low-frequency jittery oscillator** – In this approach, a high-frequency clock signal is sampled at intervals determined by a lower-frequency oscillator that exhibits significant timing jitter. The variation in the sampling intervals introduces randomness into the output sequence.

Among these methods, the use of oscillator-based TRNGs has become especially popular in the field of contactless applications. This is due to several advantages, including high-quality randomness, relatively simple circuit design, and low power consumption—factors that are particularly important for battery-powered and size-constrained devices like smart cards.

This paper focuses on the implementation of TRNG architecture based on oscillator jitter. The proposed solution aims to achieve a balance between high entropy output and low hardware complexity, making it suitable for integration into

This work was supported in part by the Polish National Center for Research and Development under project No. CYBERSECIDENT/369203/I/NCBR/2017.

First Author, Third Author, Fourth Author, Fifth Author and Sixth Author are with Institute of Microelectronics and Optoelectronics, Warsaw University of Technology (e-mail: igor.butryn@pw.edu.pl, arkadiusz.luczyk@pw.edu.pl, jakub.jasinski@pw.edu.pl, andrzej.wielgus@pw.edu.pl, krzysztof.siwiec@pw.edu.pl).

Second Author is with Techinsights Europe Sp. z o.o. Poland (e-mail: mderlecki@techinsights.com).

compact and resource-limited systems. The work presented in [3] describes the development of a TRNG circuit designed using the Hua Hong Grace 90 nm technology. However, reference [3] is limited to simulation results.

This paper is organized as follows: Section II describes the design of the oscillator-based TRNG. Section III presents the jitter enhancement technique employed to improve the randomness of the generated numbers. Section IV and V presents simulation and measurements results respectively and Section VI concludes the paper.

II. The True Random Number Generator Design

In the oscillator-based True Random Number Generator (TRNG), a low-frequency noisy clock is utilized to sample a high-frequency clock. Most often, the high-frequency clock is generated by a ring oscillator. The ring oscillator architecture is widely used due to its simplicity and compact implementation. To ensure that the oscillator maintains a stable frequency across variations in Process, Supply Voltage, and Temperature (PVT), the supply current is typically sourced from a highly stable reference, such as the current source proposed in [4]. This solution is preferred over conventional bandgap references due to its lower power consumption and suitability for ultra-low-voltage applications.

The architecture chosen to generate the low-frequency clock signal is based on a triangular waveform generator. Fig. 1 presents a simplified block diagram of the proposed TRNG. The subsystem enclosed within the dashed rectangle is responsible for producing the low-frequency jittered clock.

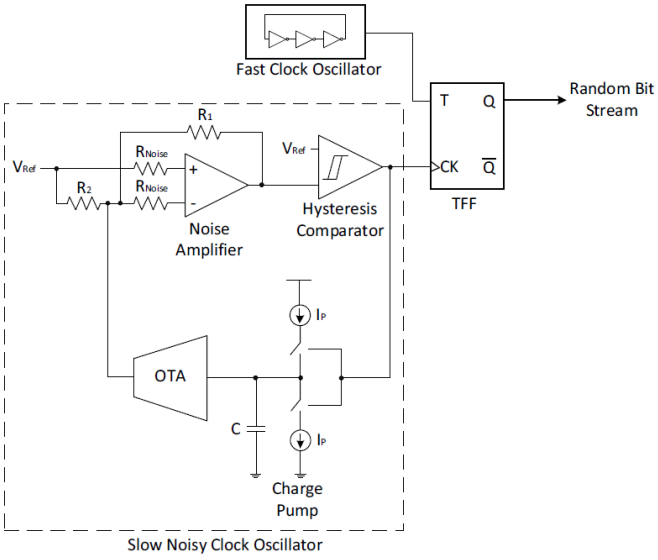

Fig.1. A simplified block diagram of the TRNG.

The operating principle of the designed TRNG is as follows: A charge pump periodically charges and discharges the capacitor C. During the discharge phase, the input voltage of the Operational Transconductance Amplifier (OTA) decreases, causing current to flow to the OTA output connected to the noise amplifier's input. The output voltage of the noise amplifier increases until it reaches the upper hysteresis threshold of the comparator. At this point, the comparator output transitions to a low logic level.

The reverse process initiates when the comparator switches back to a high state. This feedback mechanism continuously generates a triangular waveform at the output of the operational amplifier. The thermal noise generated by the resistor R_{noise} is amplified and superimposed onto the triangular signal. The resulting noisy triangular signal at the output of the Noise Amplifier (as illustrated in Fig. 2) is then converted into a square waveform by the comparator, resulting in a jittery clock signal.

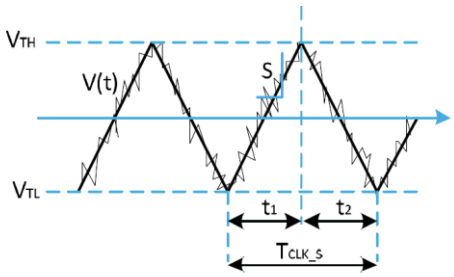

Fig. 2. Noisy triangular waveform.

This jittered clock is subsequently sampled by a high-frequency oscillator signal [5]. Due to significant jitter, the sampled signal at the output of a T-type flip-flop (TFF) becomes unpredictable, yielding a random bit stream. Employing a TFF instead of a D-type flip-flop (DFF) enhances robustness against pattern repetition [6]. To achieve high-quality randomness, the jitter must exceed the period of the high-frequency clock.

The high-frequency signal is generated using a ring oscillator circuit which is commonly used to provide a clock signal. In the era of large-scale development of integrated circuits, ring oscillators are increasingly used in various types of circuits. Their advantages are their small size and low power consumption. As already mentioned in the previous chapter, in the random number generator circuit, a ring oscillator is used to generate a fast clock signal. The frequency of the output signal of this circuit is given by the following formula:

$$f_{osc} = \frac{1}{2*N*t_d}, \quad (1)$$

where N is the number of inverters while t_d denotes signal propagation delay of a single inverter.

Schematic diagram of a ring oscillator is shown in Fig. 3. The use of a highly stable current source in a ring oscillator circuit allows to generate a frequency that is weakly dependent on the operating temperature of the circuit. There are various circuit solutions to generate temperature-independent current. The one presented in [4] seems to be the most relevant and thus was implemented in this design. Figure 4 presents a schematic diagram of the reference current source.

The period of the low-frequency oscillator is calculated as:

$$T_{CLK\_LF} = t_1 + t_2, \quad (2)$$

where t_1 and t_2 are triangular wave rise and fall times, respectively. The average period of the noisy clock is given by (see Fig. 2):

$$E(T_{CLK\_LF}) = \frac{2(V_{TH}-V_{TL})}{S}, \quad (3)$$

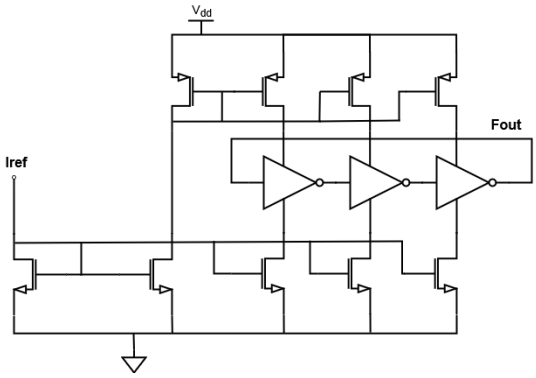

Fig. 3. Schematic diagram of the ring oscillator

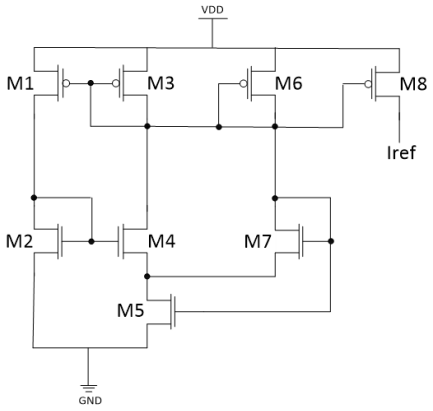

Fig. 4. Schematic diagram of the reference current source

where V_{TH} and V_{TL} are the low and high voltages of comparator hysteresis. The standard deviation of the low-frequency oscillator signal period jitter is defined as:

$$\sigma\left(T_{CLK\_LF}\right) = 2 \cdot \frac{\delta(tn)}{S}, \tag{4}$$

where $\delta(v_n)$ is defined by:

$$\delta\left(v_n\right) = \sqrt{8kTB_W R_{noise} A_V^2}. \tag{5}$$

Finally, the wave slope can be defined by the formula:

$$S = \pm \frac{I_p G_m R_2 A_V}{C}, \tag{6}$$

where k is the Boltzmann constant, T is the absolute temperature, B_w is closed loop gain bandwidth of the operational amplifier, A_v is closed loop gain of the operational amplifier, charge pump current is defined as I_P, and the transconductance of the OTA is G_m [5].

III. Increase Oscillator Jitter

The effectiveness of oscillator-based True Random Number Generators (TRNGs) is fundamentally dependent on the characteristics of timing jitter, particularly in the slow clock signal that governs the sampling process. Jitter, defined as the stochastic variation in the timing of signal transitions, serves as the primary physical entropy source in such systems. Therefore, controlling and optimizing jitter is crucial to ensuring the statistical quality and unpredictability of the generated random bitstream.

To guarantee that successive bits are temporally uncorrelated and exhibit high randomness, the standard deviation of the slow clock jitter, denoted as $\delta(T_{CLK\_S})$, should significantly exceed the period of the fast clock T_{CLK_F}, as expressed in the following inequality [8]:

$$\delta\left(T_{CLK\_S}\right) \gg T_{CLK\_F}. \tag{7}$$

This condition ensures that the sampling instants, determined by the fast clock, occur at effectively unpredictable points along the noisy slow clock edge transitions. Additionally, to avoid deterministic overlaps and ensure uniform entropy distribution, the average period of the slow clock, $E(T_{CLK\_S})$, should also be significantly greater than the fast clock period:

$$E\left(T_{CLK\_S}\right) \gg T_{CLK\_F}. \tag{8}$$

While the presence of significant jitter is indispensable for ensuring high entropy, it is important to note that this relationship is not strictly linear. Empirical analyses, including those referenced in [9], indicate that beyond a certain threshold, increasing jitter yields diminishing returns in terms of entropy enhancement. Once this saturation point is reached, further increases in jitter do not contribute to improved statistical quality of the output stream. Conversely, if jitter falls below this threshold, the entropy per bit diminishes, potentially compromising the cryptographic robustness of the TRNG. Therefore, careful tuning of jitter magnitude is required to achieve an optimal trade-off between performance, entropy, and implementation cost.

In the TRNG architecture, discussed in this work, the dominant contributor to jitter is a resistive noise source, denoted as R_{noise}. Thermal noise generated by this resistor directly affects the temporal variability of the slow clock signal. An increase in the resistance value leads to a higher noise voltage, and consequently, greater jitter. However, this comes at the cost of increased silicon area, which is undesirable in integrated circuit design. To mitigate this trade-off, additional noise was introduced through the use of a current source designed specifically to enhance jitter generation. In contrast to conventional current source design, this implementation adopts an unconventional approach. Here, the current source is intentionally designed to exhibit elevated noise levels, thereby contributing positively to the jitter and overall entropy of the system. Normally current sources are designed with as low noise as possible. In this paper the opposite strategy is used. First, the noise of the current source was analyzed. The input-referred noise of a MOS transistor is given by [10]:

$$i_n^2 = -4kT\frac{q}{L^2}Q_l\Delta f, \tag{9}$$

where q is carrier mobility, L is transistor channel length, Δf is bandwidth. The total inversion charge Q_l is proportional to the channel width W and decreased with the channel length. Noise depends on the transistor's dimensions. As demonstrated in [11], noise increases significantly for very short channels. An increase in channel width also results in a higher noise level. Therefore, a current source with short L and large W was designed to achieve high noise efficiency.

Using a lower reference current combined with a higher current multiplication ratio leads to increased noise. Figure 5 presents electrical diagram of designed current mirror. Since miniaturization is one of the main design objectives, implementing a high-noise current source is a more efficient solution than increasing resistance. Resistor noise is not the only source of jitter. A properly designed current source can also significantly increase the period jitter of the oscillator which is a desired effect in this specific application.

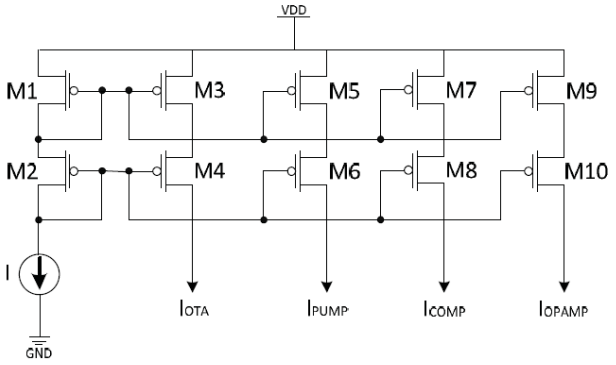

Fig. 5. Electrical diagram of designed current mirror.

IV. Simulations Results

The proposed ring oscillator-based true random number generator was implemented in the CMOS 180 nm XFAB technology using the Cadence Design Systems package. All simulations were performed using Spectre SPICE software. The results of simulation let us estimate the major parameters of the circuit which are summarized in Table I. It is worth to mention that very low power dissipation was achieved, which makes the proposed solution particularly suited for systems with limited energy budget, such as IoT systems or mobile devices.

TABLE I
DESIGN PARAMETERS OF THE TRNG CIRCUIT

Parameter	Value
Supply voltage	1,8 V
Current	80 uA
Fast clock signal frequency	200 MHz
Slow clock signal frequency	1 MHz
Output transmission speed	1 Mb/s
Jitter	48 ns
PSRR [1MHz]	90.4 dB

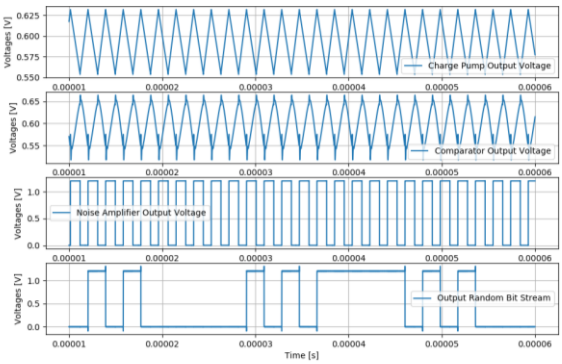

Fig. 6. Time waveforms of the output signals of the TRNG major blocks

Figure 6 presents the time waveforms of the output signals of the TRNG major blocks: the charge pump, the amplifier and the hysteresis comparator. A triangular wave, generated by the charge pump, is added to the noise at the amplifier output. Next, the hysteresis comparator produces the jittery slow clock signal, which is used to sample the fast clock signal. At the bottom chart the random output bit stream is presented.

The randomness of the output bit stream was verified using NIST statistical test suit [12]. The test results obtained for 10000-bit stream are shown in Table III.

The tests applied aim to check whether a given bit sequence exhibits randomness that is, a lack of predictible patterns as well as an even distribution of ones and zeros. This is crucial in cryptographic applications as cecurity strongly depends on the quality of randomness. The following NIST tests were conducted:

- Frequency (Monobit) Test – checks whether the numer of ones and zeros in a sequence are aproximately the same;
- Block Frequency Test – evaluates the frequency of ones in non-overlapping blocks of the sequence;
- Runs Test – analyzes the lengths of runs of ones and zeros;
- Longest Run of Ones in a Block Test – examines the longest run of ones in the blocks;
- DFT Test – detects periodicity in data using the fast Fourier transform;
- Non-overlapping Template Matching Test – counts the occurrences of specific patterns in a sequence;
- Serial Test – evaluates the frequency of occurrence of all possible *m*-bit overlapping patterns;
- Approximate Entropy Test – measures the entropy of a sequence;
- Cumulative Sums Test – examines the cumulative sum of deviations from perfect randomness.

TABLE II
NIST TEST RESULTS FOR SIMULATED TRNG OUTPUT

Test Name	Value	Result (Pass/Fail)
Monobit Frequency Test	0.6155	Pass
Block Frequency Test	0.7063	Pass
Runs Test	0.7283	Pass
Longest Runs in a Block Test	0.2034	Pass
DFT Test	0.5621	Pass
Non-Overlapping Match Test	0.8123	Pass
Serial Test	0.0736	Pass
Approximate Entropy Test	0.1342	Pass
Cumulative Sums Test	0.5632	Pass

The results of all applied tests confirm the randomness of the operation of the proposed circuit. All the tests passed which means that the obtained randomness meets the design requirements.

The TRNG circuit was simulated under various PVT conditions in the temperature range from -40°C to 120°C. Monte Carlo analysis was also performed. The designed circuit works properly under all analyzed conditions. Even in the worst-case scenarios, the level of randomness was sufficient to meet the project requirements. Table III shows the results of NIST test simulations at temperatures of -40°C and 120°C.

TABLE III
NIST TEST RESULTS FOR -40°C AND 120°C WORKING TEMPERATURE

Test Name	Value -40°C	Value 120°C	Result (Pass/Fail)
Monobit Frequency Test	0.4576	0.5843	Pass
Frequency Block Test	0.5463	0.6574	Pass
Runs Test	0.8132	0.7355	Pass
Longest Runs in a Block Test	0.2265	0.3210	Pass
DFT Test	0.5034	0.5874	Pass
Non-Overlapping Match Test	0.7341	0.6743	Pass
Serial Test	0.1167	0.1456	Pass
Approximate Entropy Test	0.1202	0.1090	Pass
Cumulative Sums Test	0.6743	0.5784	Pass

In addition, a simulation was performed to check the resistance of the randomness of the generated signal to supply voltage disturbances. During the simulation, a periodic rectangular signal with a peak-to-peak value of 200 mV was added to the supply voltage. The results of simulations are presented in Table IV. Despite disturbances introduced into the supply voltage, the system operates correctly. Figure 6 presents the supply voltage with an added periodic waveform.

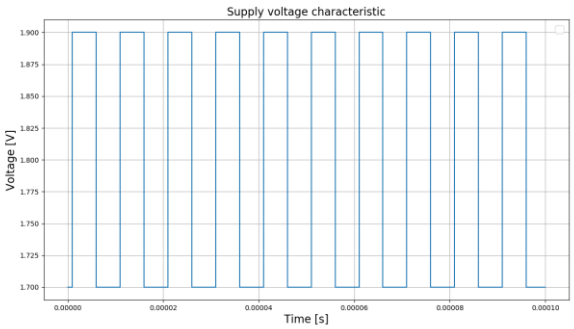

Fig. 6. Supply voltage with an added periodic waveform.

TABLE IV
NIST TEST RESULTS FOR DISRUPTED POWER SUPPLY

Test Name	Value	Result (Pass/Fail)
Monobit Frequency Test	0.6752	Pass
Frequency Block Test	0.7345	Pass
Runs Test	0.8052	Pass
Longest Runs in a Block Test	0.2476	Pass
DFT Test	0.5983	Pass
Non-Overlapping Match Test	0.8932	Pass
Serial Test	0.0734	Pass
Approximate Entropy Test	0.0913	Pass
Cumulative Sums Test	0.5412	Pass

V. MEASUREMENTS RESULTS

The prototype of the TRNG circuit was fabricated and measured. Figure 7 presents the layout of the TRNG integrated circuit. To perform measurements of the designed TRNG circuit, a dedicated test board was developed to enable proper communication with the fabricated chip. Figure 8 presents a photograph of the designed test board. The table presents the parameters of the measured circuit, while Table V shows the results of NIST tests conducted for samples generated during the measurements. The measurement results confirm that the circuit operates correctly and that the generated samples meet the requirements of the NIST test suite.

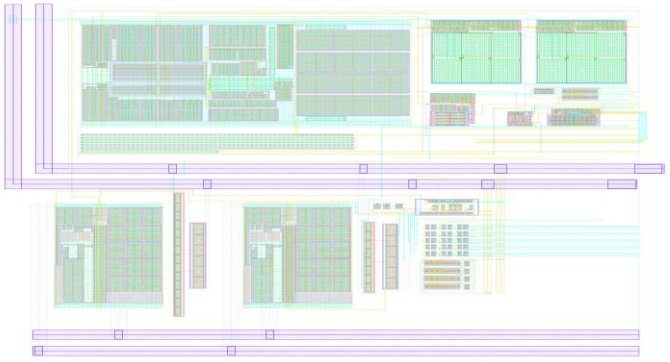

Fig. 7. A layout of the TRNG.

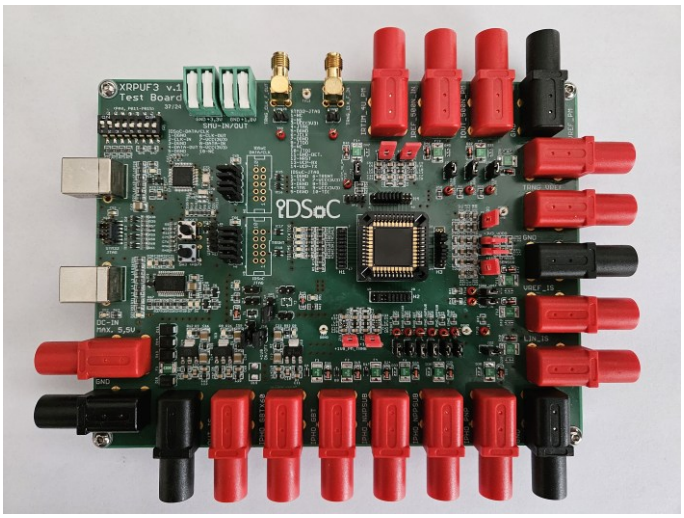

Fig. 8. Photograph of the designed testing board.

TABLE V
DESIGN PARAMETERS OF THE TRNG CIRCUIT

Parameter	Value
Supply voltage	1,8 V
Fast clock signal frequency	165 MHz
Slow clock signal frequency	850 kHz
Output transmission speed	850 kb/s

TABLE VI
NIST TEST RESULTS FOR TRNG PROTOTYPE

Test Name	Value	Result (Pass/Fail)
Monobit Frequency Test	0.6331	Pass
Block Frequency Test	0.5918	Pass
Runs Test	0.7327	Pass
Longest Runs in a Block Test	0.4552	Pass
DFT Test	0.3479	Pass
Non-Overlapping Match Test	0.8216	Pass
Serial Test	0.0949	Pass
Approximate Entropy Test	0.1284	Pass
Cumulative Sums Test	0.4072	Pass

VI. Conclusion

This paper presents the design and implementation of the true random number generator (TRNG) based on an oscillator based architecture, specifically tailored for integration in hardware security modules and cryptographic systems. The proposed TRNG architecture exploits intrinsic jitter arising from thermal and electronic noise sources in ring oscillators, which are highly sensitive to variations in process, voltage, and temperature (PVT) conditions. Such sensitivity is harnessed to generate a non-deterministic bitstream suitable for cryptographic applications where unpredictability and entropy are of critical importance.

To rigorously evaluate the quality of the generated random sequences, the TRNG output was subjected to a comprehensive statistical analysis using the NIST test suite. This widely accepted standard encompasses a series of tests designed to detect non-random patterns in binary sequences. The test results confirm that the generated bitstream passes all required criteria, indicating a high level of entropy and validating the correctness and robustness of the proposed architecture.

A key innovation introduced in this work is a novel method for enhancing jitter amplitude, which directly contributes to the entropy pool of the TRNG. Instead of relying on traditional techniques such as increasing the resistance or complexity of the delay elements, the proposed approach utilizes a high-noise current source to bias the oscillator blocks. This current source is specifically engineered to introduce additional noise into the system by leveraging stochastic fluctuations inherent in noisy current mirror circuits. As a result, this design not only increases the entropy of the output bitstream but also achieves this with a significant reduction in the required silicon area, a critical factor in resource-constrained embedded systems and integrated circuit (IC) design.

The implemented noise-based current sources, realized using modified current mirror topologies, were optimized to maximize jitter while maintaining low power consumption and minimal die area overhead. This makes the proposed TRNG architecture particularly attractive for low-power, high-security applications such as Internet of Things (IoT) devices, hardware wallets, and secure microcontrollers.

In summary, the proposed TRNG demonstrates a favorable trade-off between entropy quality, circuit complexity, and area efficiency, while introducing a novel design methodology that enhances randomness generation through noise-augmented power delivery.

Acknowledgements

We are very grateful to prof. Lidia Łukasiak and prof. Witold Pleskacz for his constructive suggestions and valuable feedback.

References

[1] C. S. Petrie and J. A. Connelly, "A noise-based IC random number generator for applications in cryptography," IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, vol. 47, no. 5, pp. 615-621, May 2000.

[2] G. K. Balachandran, R. E. Barnett and J. A. Connelly, "A 440-nA true random number generator for passive RFID tags," IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 55, no. 11, pp. 3723-3732, Nov. 2008.

[3] M. Derlecki, K. Siwiec, P. Narczyk and W. A. Pleskacz, "Design of a True Random Number Generator Based on Low Power Oscillator with Increased Jitter," 2019 IEEE 22nd International Symposium on Design and Diagnostics of Electronic Circuits & Systems (DDECS), Cluj-Napoca, Romania, 2019, pp. 1-4, https://doi.org/10.1109/DDECS.2019.8724643

[4] M. Łukaszewicz, T. Borejko and W. A. Pleskacz, "A resistorless current reference source for 65 nm CMOS technology with low sensitivity to process, supply voltage and temperature variations," 14th IEEE International Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS), Cottbus, Germany, 2011, pp. 75-79, https://doi.org/10.1109/DDECS.2011.5783051

[5] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti and M. Varanonuovo, "A high-speed oscillator-based truly random number source for cryptographic applications on a smart card IC," IEEE Transactions on Computers, vol. 52, no. 4, pp. 403–409, Apr. 2003.

[6] W. Che, Z. Bi, J. Wang, N. Yan, X. Tan, J. Wang and H. Min, "A 1.04 μW truly random number generator for Gen2 RFID tag," in 2009 IEEE Asian Solid-State Circuits Conference (ASSCC), Taiwan, Nov. 2009, pp. 117–120, https://doi.org/10.1109/ASSCC.2009.5357193

[7] R. S. Assaad and J. Silva-Martinez, "The Recycling Folded Cascode: A General Enhancement of the Folded Cascode Amplifier," IEEE Journal of Solid-State Circuits, vol. 44, no. 9, pp. 2535–2542, Sept. 2009, https://doi.org/10.1109/JSSC.2009.2024819

[8] E. Bejar, J. Saldana, E. Raygada and C. Silva, "On the jitter-to-fast-clock-period ratio in oscillator-based true random number generators," in Proc. 24th IEEE Int. Conf. Electronics, Circuits and Systems (ICECS), Batumi, Georgia, Dec. 2017, pp. 243–246, https://doi.org/10.1109/ICECS.2017.8292100

[9] C. Guo, Y. Zhou, H. Liu and N. Zhu, "On the jitter and entropy of the oscillator-based random source," in Proc. 7th International Conference on Computer, Communication and Networking Technologies (ICCNT), Jul. 2015.

[10] A. Emira, E. Sanchez-Sinencio and M. Schneider, "Design tradeoffs of CMOS current mirrors using one-equation for all-region model," 2002 IEEE International Symposium on Circuits and Systems. Proceedings (Cat. No.02CH37353), Phoenix-Scottsdale, AZ, USA, 2002, pp. V-V, https://doi.org/10.1109/ISCAS.2002.1010636

[11] L. N. Alves and R. L. Aguiar, "Noise performance of classical current mirrors," in Proc. 9th IEEE International Conference on Electronics, Circuits and Systems (ICECS), vol. 1, Dubrovnik, Croatia, Sept. 2002, pp. 277–280, https://doi.org/10.1109/ICECS.2002.1045387

[12] A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, E. B. Barker, S. D. Leigh, M. Levenson, M. Vangel, D. L. Banks, A. Heckert, J. F. Dray Jr. and S. C. Vo, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," NIST Special Publication 800-22, April 2010.