Taylor & Francis
Taylor & Francis Group

International Journal of Electronics Letters

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/tetl20

A metastable RNG using interleaved NAND- and NOR-based TEROs

Chua-Chin Wang, Lean Karlo S. Tolentino, Shao-Wei Lu, Ralph Gerard B. Sangalang, Oliver Lexter July A. Jose & Tzung-Je Lee

To cite this article: Chua-Chin Wang, Lean Karlo S. Tolentino, Shao-Wei Lu, Ralph Gerard B. Sangalang, Oliver Lexter July A. Jose & Tzung-Je Lee (07 Feb 2024): A metastable RNG using interleaved NAND- and NOR-based TEROs, International Journal of Electronics Letters, DOI: 10.1080/21681724.2024.2312551

To link to this article: https://doi.org/10.1080/21681724.2024.2312551

Published online: 07 Feb 2024.

Submit your article to this journal

View related articles

View Crossmark data

Full Terms & Conditions of access and use can be found at
https://www.tandfonline.com/action/journalInformation?journalCode=tetl20

INTERNATIONAL JOURNAL OF ELECTRONICS LETTERS
https://doi.org/10.1080/21681724.2024.2312551

Taylor & Francis
Taylor & Francis Group

Check for updates

A metastable RNG using interleaved NAND- and NOR-based TEROs

Chua-Chin Wang [a,b], Lean Karlo S. Tolentino [a], Shao-Wei Lu [a], Ralph Gerard B. Sangalang [a,c], Oliver Lexter July A. Jose [a,c] and Tzung-Je Lee [a]

[a]Department of Electrical Engineering, National Sun Yat-Sen University, Kaohsiung, Taiwan; [b]Institute of Undersea Technology, National Sun Yat-Sen University, Kaohsiung, Taiwan; [c]Department of Electronics Engineering, Batangas State University - The National Engineering University, Batangas, Philippines

ABSTRACT

This study introduces a novel approach to address the limitations observed in existing random number generator (RNG) designs, focusing on the resolution for insufficiently covered problem statements and study purposes. In response to these challenges, we propose a high-throughput metastable-based RNG tailored for cryptography applications. Our design is featured with a two-layer transient effect ring oscillator (TERO) architecture, meticulously crafted to mitigate the locking phenomenon and enhance RNG randomness. Leveraging interleaved two-layer TEROs, realised through NAND and NOR SR latches, our RNG achieves unpredictable irregular sampling, crucial for cryptographic applications. To further enhance irregular sampling, the first layer of the RNG employs a multiplexer that selects inputs randomly. This multiplexer is governed by selection signals generated by the second layer of the RNG, ensuring superior randomness. Implemented using TSMC 40-nm CMOS process, our RNG passed the FIPS 140–1 randomness test at a clock frequency of 100 MHz, boasting a remarkable throughput of 50 Mbps. This study represents a significant advancement in RNG technology, addressing previous shortcomings and paving the way for high-speed communication systems' secure cryptographic applications.

ARTICLE HISTORY
Received 6 April 2023
Accepted 1 January 2024

KEYWORDS
Long run test; metastable; monobit test; random number generator; transient effect ring oscillator

1. Introduction

1.1. Motivation and incitement

In recent years, the development of network and wireless communication has made their security more important than ever (Yu & Kim, 2020). As the cloud usage becomes more and more popular, most of people's confidential information is stored and displayed in the internet. In addition, several devices and systems which are interconnected through the Internet (Internet of Things or IoT) for gathering data or controlling machines and equipment are being utilised especially in industry, agriculture, health, and banking (Basa et al., 2019; Dela Cruz & Tolentino, 2021; Jorda et al., 2019; Lee et al., 2020; Sangalang et al.,

CONTACT Chua-Chin Wang ccwang@ee.nsysu.edu.tw, Department of Electrical Engineering, Institute of Undersea Technology, National Sun Yat-Sen University, No. 70, Lian-Hai Road, Gushan District, Kaohsiung 80424, Taiwan

© 2024 Informa UK Limited, trading as Taylor & Francis Group

2022; L. K. Tolentino et al., 2017). Most of the information from these IoT-enabled devices and systems need confidentiality (Randa et al., 2020). For the information to be confidential and authentic, approaches involving cryptography on any network and communication system must be implemented (Chien, 2008). One of the approaches is generating unpredictable keys through a random number generator (RNG) (Fischer et al., 2013; Saqib et al., 2017). The purpose of the RNG is to provide highly unbreakable secret keys to ensure that the information will be authenticated and encrypted. The performance of the RNG depends on the following features: difficulty in predicting its output, difficulty in repeating its output, conformance with typically used randomness tests, and the ease and compatibility to be interfaced with communication systems (Schneier, 2007). It is also considered as one type of PUF (physically unclonable function) (Acar & Ergun, 2020; Cherkaoui et al., 2016).

Two types of RNGs such as pseudo RNG and true RNG have been widely researched and reported. In pseudo RNGs, the sequence output created may appear random, since the pseudo RNG is implemented based on mathematical equations or algorithms specifically statistical random numbers; hence, this can be applied only on systems with low level of security (Yang et al., 2014). For this reason, a true RNG which generates unpredictable and non-periodic true random numbers of digit sequences have become the research focus of communication cryptography. RNGs can also be classified into software and hardware implementations. RNGs which are implemented through software consumes large area and high power when the entropy in the software-based RNG mostly needs many structures which are replicated. On the other hand, entropy from hardware-based RNG is utilised from physical electronic components which makes it easily realised in circuits; thus, hardware-based RNGs with PUF features are more preferred than software-based. There are two types of hardware-based RNGs, namely, analog and digital. Analog hardware-based RNG requires auxiliary circuits to convert the analog signal from electronic components such as thermal resistors or avalanche diodes into digital signal. Digital hardware-based RNG which are typically employed using linear feedback shift register (LFSR) and field programmable gate array (FPGA) generates a pseudo-random signal which is poor in randomness (Acar & Ergun, 2020; Akiri et al., 2022; Guo & Zhou, 2018; Serfa Juan & Kim, 2018; L. K. S. Tolentino et al., 2019; Wang et al., 2022).

1.2. Literature review and research gaps

With the development of system-on-chip (SOC) becoming more popular, many real random number generators are realised by hardware and integrated circuit (IC) implementations. These approaches include direct amplification, oscillator sampling, discrete-time chaos (DTC), and transient effect ring oscillator (TERO) (Acar & Ergun, 2020; Akgul et al., 2017; Delgado-Restituto & Rodriguez-Vazquez, 2002; Rodriguez-Vazquez et al., 1991; Wang et al., 2005). In direct amplification, a small noise voltage, e.g. thermal noise is amplified then fed to the clocked comparator for non-biased accurate thresholding; as a result, it generates random digital signals. However, this method is difficult to be implemented in IC, because the noise source cannot be sufficiently shielded from the power supply and ground signals making this method works the best for embedded solutions only. In oscillator sampling, random bits are generated though the sampling of the phase noise output from a fast oscillator on the edges of

a slow clock where a D flip-flop is utilised. However, the generated phase jitter is not adequate for the oscillator-based RNG to generate random bits. Meanwhile, the DTC method utilises an analog-to-digital converter (ADC) where its input residue signal range of 0 to 1 is processed by a sample and hold circuit and is fed back again to the ADC input. However, it consumes large chip area, dissipates large power, processes slowly, and responds vulnerably to process drifting (Petrie & Connelly, 2000). Lastly, TERO which is metastable in nature uses SR latches where the enable signal or clock are connected to their inputs (S and R) and odd number of inverters which serves as ring oscillators (RO) (Acar & Ergun, 2020; Cherkaoui et al., 2016). The generated number of oscillations is exploited as the entropy source for the RNG making TERO a suitable RNG structure due to its ability to avoid electromagnetic influence and locking phenomenon (Acar & Ergun, 2020; Varchola & Drutarovsky, 2010). Locking phenomenon in ring oscillators is a condition where the said oscillators are locked becoming dependent to each other instead of being independent and free-running. This is the fundamental feature of PUF. Previous works related to RNGs which use RO have lower speed makes them difficult to be used in communication systems which usually demand high speed and throughput (Wang & Lu, 2020).

Many related works have been reported regarding true RNGs. A 65-nm RNG (Huang et al., 2012) which uses the sampled random telegraph noise of the CRRAM (contact-resistive random access memory) as entropy source occupies a small area of 45 μm^2, but it operates at a low clock frequency of 1 kHz. In (Amaki et al., 2013), a 65-nm oscillator-based RNG which has a clock frequency of 15.1 MHz and throughput of 7.5 Mbps was realised. A 180-nm DTC-based RNG was developed which operates at a low clock frequency of 216 kHz, but it consumes a large area of 0.21 mm^2 (Kim et al., 2017). In this research (Guler et al., 2017), an effective architecture was developed for an RO-based RNG. A synthetic bit stream of white noise, flicker noise, and their combination, was generated to study their effect on randomness. The entropy of bit streams is observed to be increased by flicker noise. The created synthetic bit streams are then used to investigate the entropy dependence of a bit stream on the sampling period, and the outputs of ROs in strong and weak inversion are analysed and compared for their entropy levels. The comparison shows that it may be possible to generate a sufficiently random bit stream using only a single RO running in weak inversion. Meanwhile, a quantum RNG was used for a clock frequency of 0.5 MHz (Siswanto & Rudiyanto, 2017). It is implemented using LFSRs of the FPGA. A 130-nm oscillator-based RNG was proposed in (Li et al., 2017) where its operating clock frequency is 1 MHz and throughput is 1 Mbps. Meanwhile, in (Zode et al., 2019), a high clock frequency of 33 MHz was utilised in an RNG which implemented LFSRs of the FPGA. Lastly, a study in (Acar & Ergun, 2020) presented a 180-nm, RSR (reconfigurable SR) latch-based RNG which uses TERO that has a throughput of 3.33 Mbps, but it operates at a higher frequency of 100 MHz. In this topology, every RSR latch consists of 1 multiplexer, 1 D flip-flop, and 1 source of entropy generated by the SR latch, which consists of a pair of NOT gates as well as a pair of AND gates. A total of 40 RSR latch circuits are coupled using an XOR gate for sufficient entropy generation. To choose between two distinct sampling strategies, the circuit includes a multiplexer (MUX): (1) In the case of regular sampling, the output of the XOR gate is routed through a D-type FF,

which then causes the generation of random bits. (2) In the case of irregular sampling, the output of the XOR gate is routed via a D-type FF. To give the requisite entropy for random bit creation in such a way that it fulfils the statistical tests, the output of the XOR gate is subsampled by a high-frequency clock. This ensures that the random bits generated are of sufficient quality.

Meanwhile, Kızmaz and Ergün (2021) proposed an RNG using a skew-tent map and chaotic sampling using TSMC 180 nm CMOS process. Simulations and statistical randomness tests, such as the FIPS-140-2 and NIST 800–22 suites, validated their RNG. Their proposed RNG passes randomness tests without post-processing, demonstrating its inherent randomness. It has robust immunity against external interference, a crucial feature for secure applications, due to the chaotic sampling method. And, it achieves impressive bit rates at 4.8 Mbps with a reasonable power consumption of 9.8 mW. This innovative architecture generates robust random bit streams and enables high-speed, low-power RNG systems for advanced security applications.

Lastly, Demir and Ergün (2022) used metastable behaviour in a double scroll chaotic attractor to numerically analyse, implement, and simulate an RNG. Random bits are generated by sampling a regular clock signal at the chaotic attractor scroll transition. The 65 nm TSMC process is used to develop this research's double-scroll chaotic oscillator using MOS transistors and MIM capacitors. Monolithic RNG circuits have chaotic attractors, Schmitt triggers, and dual-edge triggered D flip-flops. The metastable nature of chaos is shown by sampling a standard clock signal during the chaotic signal's scroll shift to generate the output bit stream. A MOS-based Schmitt trigger detects scroll transitions, producing an irregular clock signal. This signal samples the clock to create the RNG output using a dual-edge triggered D flip-flop. NIST 800–22 statistical randomness test suite standards were met by the bit stream after rigorous testing. The study details the RNG layout and circuit schematic, featuring a compact area of 0.004 mm^2, low power consumption of 30 μW, and a satisfactory data throughput of 0.72 Mbps.

RNGs are crucial components in various applications, particularly in cryptography, where the quality of randomness directly influences security. While the following studies primarily focus on power electronics and renewable energy systems, their innovative techniques and advanced algorithms offer valuable insights applicable to RNG research. The Bayesian Fusion Technique (BFT) in the first study showcases hybrid optimisation methods, combining Grey Wolf Optimisation (GWO) and Flower Pollination Algorithm (FPA), highlighting the significance of optimisation strategies (Hemalatha et al., 2023). The second study introduces intelligent control strategies, specifically Maximum Power Point (MPP) based control, essential for maintaining constant power output from Solar-PV arrays, reflecting the importance of precise control mechanisms in complex systems (Albert et al., 2023). The third study explores a Symmetric Voltage-Lift Inverter (SV-LI) with reduced semiconductor switches and Particle Swarm Optimisation (PSO) for maximising system voltage, demonstrating innovative inverter technologies that could inspire advancements in RNG designs (Albert et al., 2022). Lastly, the fourth study employs intelligent techniques such as Fuzzy Logic (FL) controllers, emphasising the value of sophisticated algorithms in optimising output voltage and reducing harmonics (Albert, 2022). These studies collectively underline the potential for integrating advanced algorithms and control methods to enhance RNG efficiency and randomness, vital for its applications in secure communication systems.

1.3. Contributions and paper organisation

In a previous study, a proposal was made for a random number generator (RNG) with a wide bandwidth (Wang & Lu, 2020). This RNG was implemented using interleaved NAND-based and NOR-based SR latches. However, the study only included post-layout simulations and did not involve any chip implementation, measurements, or theoretical analysis. As a solution and improvement to the above-mentioned drawbacks of the different RNG approaches and prior works, we developed a high-throughput RNG based on 2-layer interleaved TERO which can be utilised for high-speed communication systems. These TEROs composed of SR latches to achieve metastability which makes our proposed RNG randomise the output efficiently. The first layer of the RNG consists of two arrays of clock-enabled interleaved NAND-and-NOR-based TERO. The multiplexer (MUX) receives the resulting outputs from the first layer. It is controlled by the selection signals which are generated by the second layer of the RNG. This second layer also consists of two arrays of clock-enabled interleaved NAND-and-NOR-based TERO. The RNG was implemented and fabricated using TSMC 40-nm CMOS process. It passed the FIPS 140–1 statistical randomness test with a higher throughput of 50 Mbps and a power consumption of 23.4 mW at 100 MHz.

The rest of this paper is presented as follows: Section 2 presents the system architecture of the RNG; Section 3 discusses the results and the performance comparison with other RNGs; Finally, Section 4 concludes this paper.

2. System architecture of TERO-based random number generator

A block diagram of the proposed random number generator based on TEROs is shown in Figure 1. It is composed of 22 TEROs, two 8-to-1 MUXs, and an XOR gate for $n = 8$ in Figure 1. Of the 22 TEROs, 16 TEROs are used as inputs for the MUX, and the remaining 6 TEROs are used as selection signals for the MUX.

2.1. Transient Effect Ring Oscillator (TERO)

The TERO consists of an SR flip-flop (two NANDs or two NORs) and an odd number of buffers. It uses an SR flip-flop with oscillation stability by connecting the S and R inputs of the SR flip-flop to the clock (CLK) signal.

The NAND-based TERO in Figure 1 is shown in Figure 2. It is composed of two NAND gates and three buffers at either output path. Table 1 shows the truth table of the NAND-based TERO. Since the inputs S and R are both connected to the same signal CLK, there will be no different logic states for S and R. When the CLK logic is 0, the inputs S and R of the NAND-based TERO are both 0, and both Q and Qbar will be fixed at 1. When the CLK logic is 1, the inputs S and R of the NAND-based TERO are both 1. Both Q and Qbar will be undefined, which may be 0 or 1. Since the result of Q is unpredictable, this state is called a metastable state. When both SR outputs are defined, the NAND-based TERO SR latch is only at metastable state for a small period of time after the SR inputs go high randomly. Buffers were connected to the outputs of the NAND SR latch to generate the delay and path of the output signal Q and Qbar.

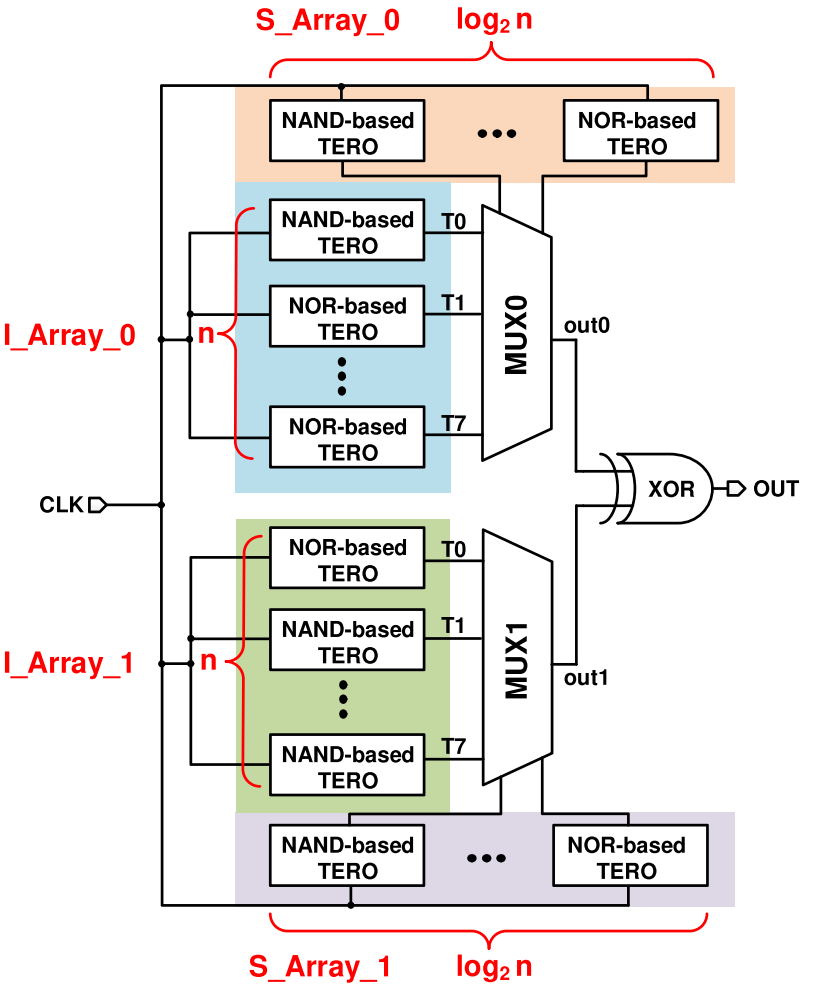


Figure 1. Generic 2-layer random number generator (RNG).

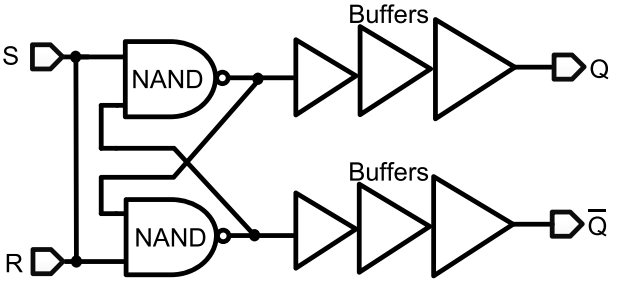


Figure 2. NAND-based Transient Effect Ring Oscillator (NAND-based TERO).

On the contrary, the NOR-based TERO in Figure 1 is shown in Figure 3. It is composed of two NOR gates and three buffers at either output path. Its truth table is shown in Table 2. When the CLK logic is 1, the inputs S and R of the NOR-based TERO are both 1, and both Q and Q will be set to 0. When the CLK logic is 0, the inputs S and R are both 0, both Q and Qbar will be undefined, which may be 0 or 1, entering the metastable state again.

Table 1. NAND-based TERO truth table.

S	R	Q
0	0	1
1	1	undefined

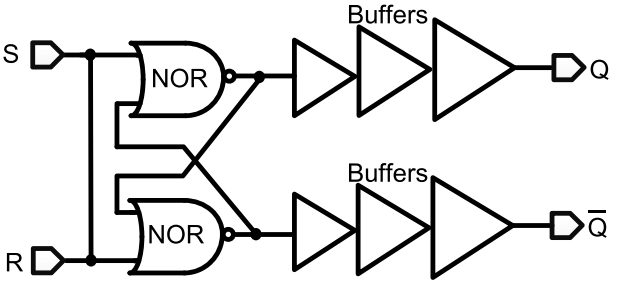


Figure 3. NOR-based Transient Effect Ring Oscillator (NOR-based TERO).

Table 2. NOR-based TERO truth table.

S	R	Q
0	0	undefined
1	1	0

2.2. *Theoretical analysis of TEROs' randomness*

Based from the logical truth tables of NAND and NOR gates, the probabilities of generating an output of ones in NAND and NOR gates are $\frac{3}{4}$ and $\frac{1}{4}$. Referring to the inputs of the NAND-based TERO in Figure 4, the probability of occurrence of both ones and zeroes is assumed as $\frac{1}{2}$ without any loss of robustness. Notably, the NAND-based TERO can be represented by an equivalent circuit having inputs whose probabilities are $\frac{1}{2}$ and $\frac{3}{4}$, respectively. Its probability of generating ones is $\frac{5}{8}$ which was determined by adding the conditional probabilities of having ones, P(1), for different input conditions as shown in Table 3. This means that the NAND-based TERO generates more ones than zeroes.

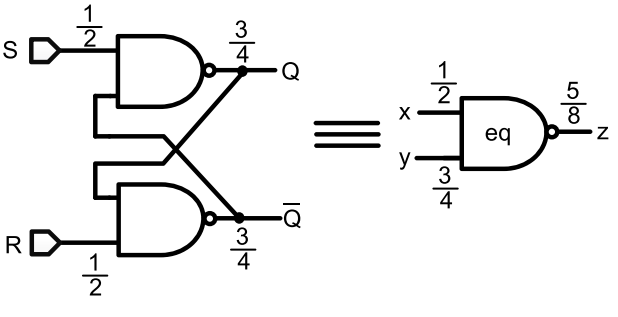


Figure 4. Equivalent circuit of a NAND-based TERO showing the probability of"1" in its inputs and outputs.

Table 3. Truth table of the NAND-based TERO equivalent circuit with its respective probabilities of generating the outputs.

x	y	z	P(1)
0	0	1	$\frac{1}{8}$
0	1	1	$\frac{3}{8}$
1	0	1	$\frac{1}{8}$
1	1	0	$\frac{3}{8}$

Meanwhile, using the similar principle in determining the probabilities of generating ones in NAND-based TERO, the corresponding equivalent circuit of NOR-based TERO is shown in Figure 5, while its truth table is seen in Table 4. Its probability of generating ones is $\frac{3}{8}$ which signifies that the NOR-based TERO has the feature of generating more zeroes instead. However, an almost equal number of zeroes and ones should be achieved in the design of any unbreakable RNG, which means we need to equalise the generation of ″1″s and ″0″s when NAND-based TEROs and NOR-based TEROs are integrated.

Another measurement of randomness of an RNG is entropy (H) represented by Equation (1), where P_i is the probability of an event, i.e. generating of ″1″ or ″0″ and S is the total number of events, i.e. 2 (generations of 1 and 0). The higher the entropy, the better the randomness is. Therefore, the closer the probability to 0.5, the higher the randomness.

$$H = -\sum_{i=1}^{S}(P_i \log_2 P_i) \tag{1}$$

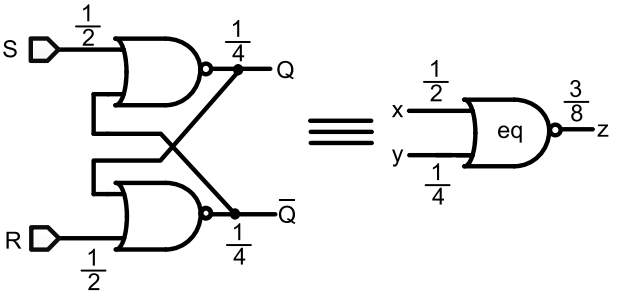


Figure 5. Equivalent circuit of a NOR-based TERO showing the probability of″1″ in its inputs and outputs.

Table 4. Truth table of the NOR-based TERO equivalent circuit with its respective probabilities of generating the outputs.

x	y	z	P(1)
0	0	1	$\frac{3}{8}$
0	1	1	$\frac{1}{8}$
1	0	1	$\frac{3}{8}$
1	1	0	$\frac{1}{8}$

2.3. Behavior of TEROs based on simulations

Figure 6 and Figure 7 show the outputs from the Monte-Carlo post-layout simulations (runs = 1000) performed on the NAND-based and NOR-based TEROs, respectively. Referring to Figure 6, the ones and zeroes percentages are 83.5% and 16.5%, respectively. Meanwhile, based on Figure 7, the ones and zeroes percentages are 27% and 73%, respectively. Though the reported percentages of zeroes and ones in the simulation results are not exactly equal to our theoretical calculation in Section 2.2, they still match with our theoretical prediction, i.e. more high (logic 1) pulses are generated by the NAND-based TERO while more low (logic 0) pulses are generated by the NOR-based TERO. From this statement, we can say that: No function units for this RNG can use either NAND-based

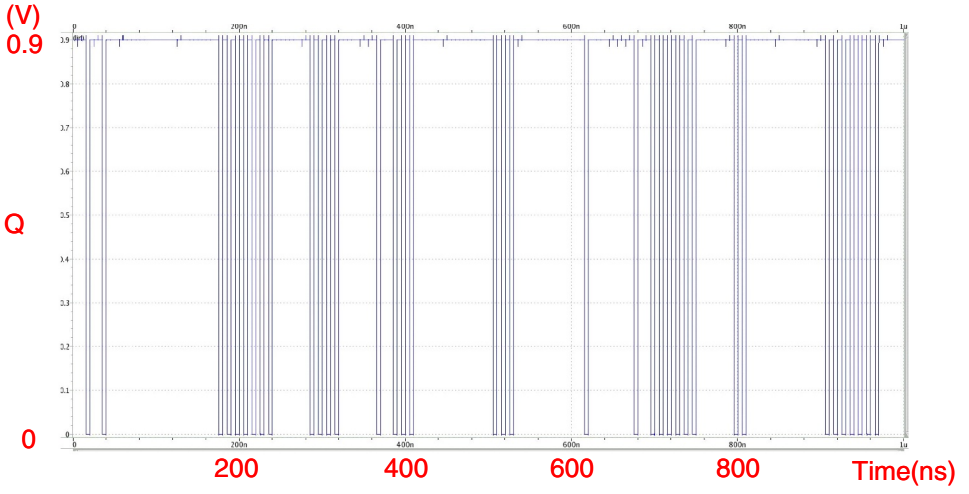


Figure 6. Single NAND-based TERO output waveform.

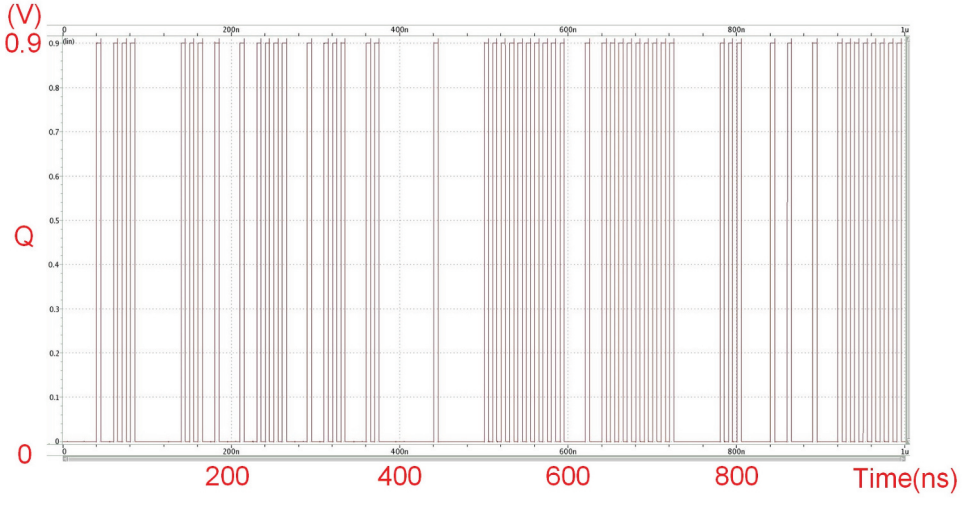


Figure 7. Single NOR-based TERO output waveform.

TERO or NOR-based TERO alone to achieve high-quality randomness; and, randomness can be enhanced if an additional scrambling approach is considered. Hence, interleaving of both NAND and NOR-based TEROs is initiated as discussed in the following subsections to generate bits with high randomness.

2.4. Multiplexer (MUX) with XORed output

The 8-to-1 MUX in Figure 1 is shown in Figure 8. XOR was used instead of OR and NAND for the processing of AND outputs, A0 to A7. Since the XOR is used, equal probabilities of generation of zeroes and ones (both 0.5) are expected at the output of XOR (Zhu et al., 2018). 8 TEROs are used as inputs and 3 TEROs are used as selection signals for the MUX. Referring to Figures 1 and 8 again, I Array 0 consists of interleaving blocks of the following order: NAND-based TERO, NOR-based TERO, . . ., while I Array 1 consists of interleaving blocks of the following order: NOR-based TERO, NAND-based TERO. . . MUX0, which accepts the outputs of I Array 0, is driven by the selection signals generated by S Array 0. S Array 0 has the same order and arrangement but different number of TEROs ($\log_2(n)$). Likewise, S Array 1 controls MUX1 which accepts the outputs of I Array 1. Lastly, the generated random signal is processed by the XORing of the outputs of MUX0 and MUX1 to implement additional scrambling approach for the improvement of the randomness of the RNG.

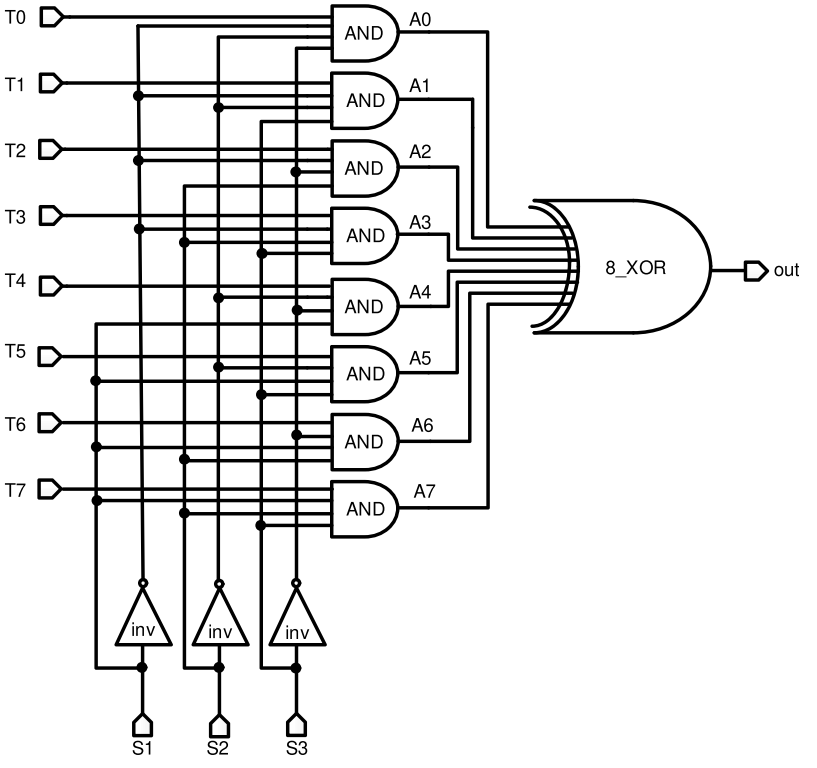


Figure 8. Multiplexer circuit (MUX0, MUX1 in Figure 1).

2.5. Theoretical analysis of randomness by MUX scrambling

Since both NAND and NOR-based TEROs cannot generate an almost equal number of zeroes and ones randomly, MUX was used to resolve this problem by using scrambling and interleaving the blocks of NAND and NOR TEROs alternately. Figures 9 and 10 illustrate the advantage of using MUX in increasing the randomness of NAND-and-NOR -based TEROs. Notably, the blue labels refer to the probabilities of generating ones, while the red labels refer to the probabilities of generating zeroes by TEROs. For example, referring to Figure 9(a): $P(1) = \frac{5}{8} \times \frac{5}{8} + \frac{3}{8} \times \frac{3}{8} = \frac{34}{64}$; and Figure 9(b): $P(1) = \frac{5}{8} \times \frac{3}{8} + \frac{3}{8} \times \frac{5}{8} = \frac{30}{64}$. Compared to only using NAND and NOR-based TEROS (no scrambling), these 4 cases (after MUX scrambling) as shown in Figures 9 and 10 demonstrate one thing: either $\frac{34}{64}$ or $\frac{30}{64}$ is better than $\frac{5}{8}$ or $\frac{3}{8}$, since the former is close to $\frac{1}{2}$. With this, an almost equal number of ones and zeroes is achievable. On the other

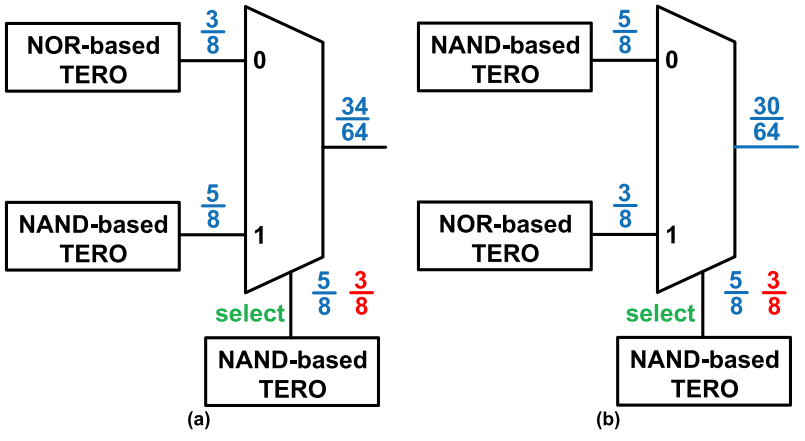


Figure 9. Probabilities of generating ones using NAND-based TERO as selection block, (a) NAND-based TERO as input block when select = 1; (b) NOR-based TERO as input block when select = 1.

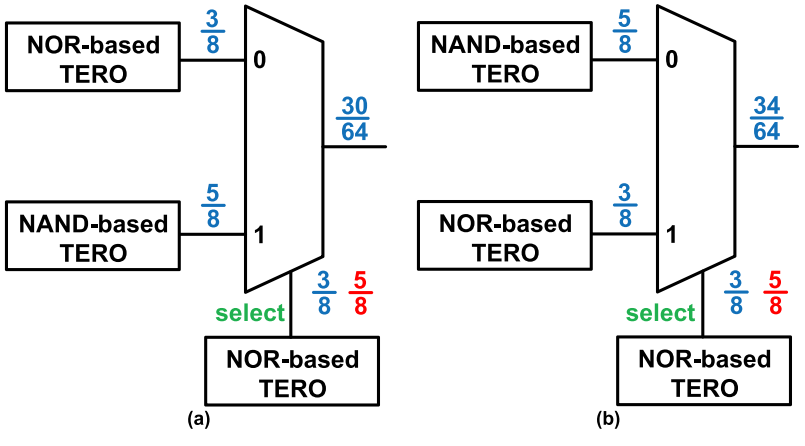


Figure 10. Probabilities of generating ones using NOR-based TERO as selection block, (a) NAND-based TERO as Input block when select = 1; (b) NOR-based TERO as Input block when select = 1.

hand, the entropies in Figure 9(a-b) are 0.48 and 0.51, respectively, based on Equation (1). However, when these two outputs are XORed, the total entropy is 0.48 + 0.51 = 0.99 indicating better randomness is to be achieved.

3. Measurement results

The metastable RNG based on interleaving NAND-and-NOR TEROs is realised using TSMC 40-nm process. As shown in Figure 11, the layout view of the core (centred) has an area of $0.084 \times 0.116\ mm^2$ while the chip (left side) has an area of $0.37 \times 0.37\ mm^2$. The die micrograph is also shown in the right side of Figure 11, where a dummy metal layer covered the core showing only the pads and the wire-bonds.

The measurement setup of the RNG chip is shown in Figure 12. The power supply, ITECH IT6333A, is used to provide the supply voltage required by the chip, and the signal generator, Keysight 33600A Series, is used to generate a clock signal on the chip as a random number. Finally, the Waverunner 6zi oscilloscope demonstrates the waveform of the output.

Within the domain of experimental validation, our carefully designed chip underwent a comprehensive series of tests, with particular emphasis placed on the esteemed FIPS 140–1 statistical randomness evaluation. This evaluation is widely regarded as the benchmark for assessing the credibility of RNGs. The successful

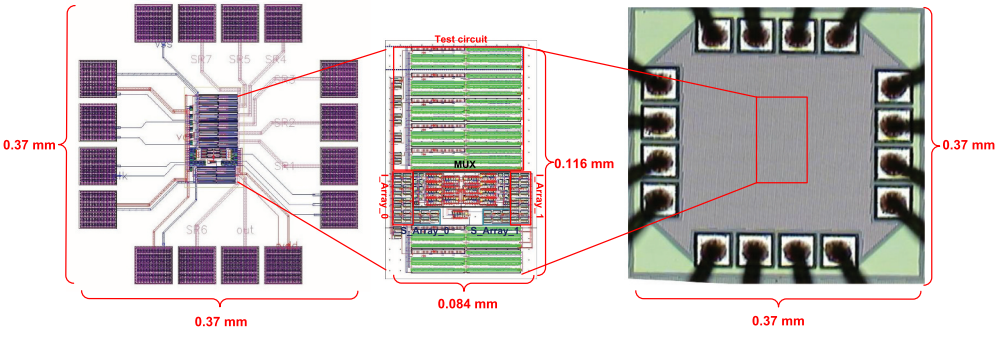


Figure 11. Chip layout (right), core layout (centered), and die micrograph (right) of the metastable RNG based on interleaving NAND-and-NOR TEROs.

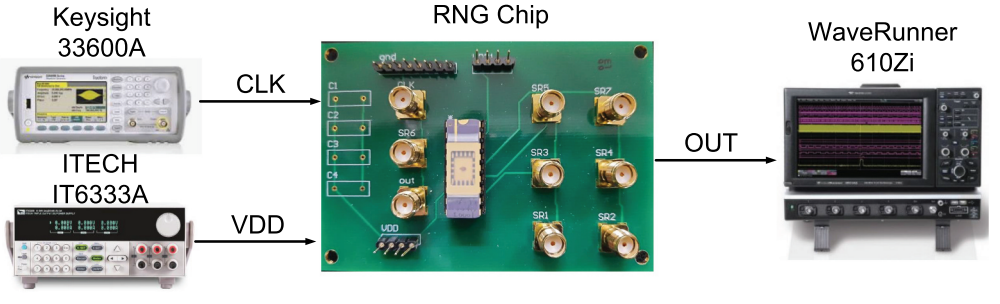


Figure 12. Measurement setup for the fabricated RNG chip.

outcome of the monobit test, a fundamental requirement for FIPS 140–1 compliance, marked a significant milestone for our RNG. The number of units within our carefully produced a 20,000-bit sequence flawlessly adhered to the narrow interval of 9,654 to 10,346 bits, highlighting the accuracy of our random number generator's results. Furthermore, the chip adeptly traversed the intricate maze of the long runs test, guaranteeing the absence of any prolonged sequences consisting of 34 or more consecutive zeros or ones, thereby preserving the sophistication of our 20,000-bit sequence. The success of our RNG is clearly demonstrated in Figure 13, which provides a detailed graphical representation of the distribution of runs generated by the RNG. This visual evidence serves as a strong indication of the RNG's strong performance and its ability to generate truly random numbers. Figure 14 presents a comprehensive examination of the complex waveform exhibited by a single prior TERO from previous measurements conducted at a clock frequency of 2 MHz. This waveform serves as a reference point for comparative analysis. In sharp contrast, Figure 15 presents a compelling narrative, illustrating the diverse assortment of random elements intricately intertwined by our suggested random number generator (RNG) with equal regularity.

Continuous 0

Length of Run	Required Interval
1	2701
2	709
3	507
4	210
5	193
6	82
else	253

Continuous 1

Length of Run	Required Interval
1	2702
2	786
3	524
4	218
5	155
6	88
else	182

Figure 13. Results generated by the RNG on its runs distribution.

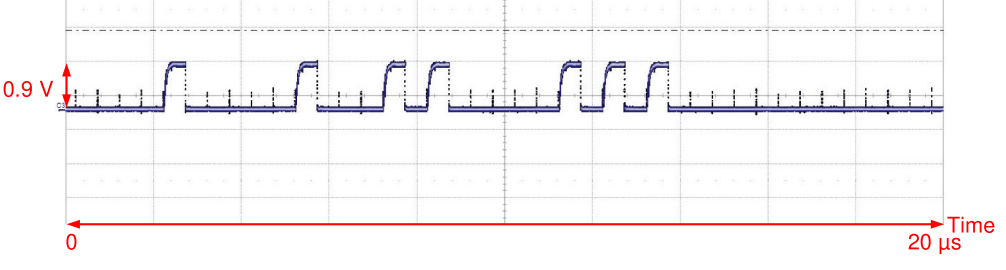


Figure 14. Sample measured output waveform of a single prior TERO at 2 MHz clock frequency.

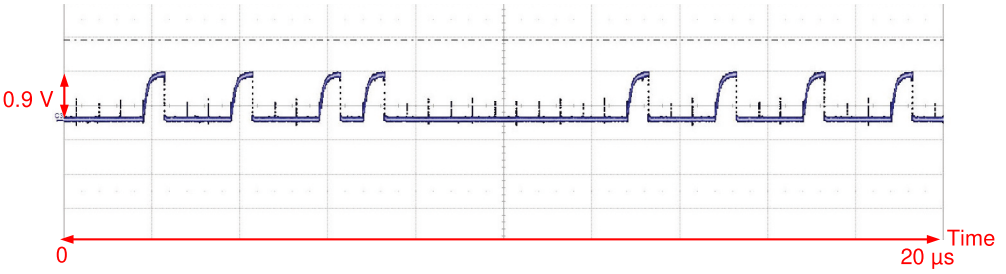


Figure 15. Sample measured output waveform of the proposed RNG up to 20 μs at 2 MHz clock frequency.

The RNG's design has significantly improved by effectively addressing the issue of unbalanced outputs commonly observed in single NAND-based TEROs or NOR-based TEROs. By strategically manipulating our generated bits, we mitigated this disparity by intentionally augmenting the frequency of "1"s. This approach resulted in a balanced distribution of ones and zeros, exemplifying a state of true randomness.

Referring to Table 5, despite its relatively higher power consumption (which measures 23.4 mW when operating at a frequency of 100 MHz) as compared to Acar and Ergun (2020) which was also implemented using TEROs, our RNG exhibits superior performance compared to the previous works. Moreover, despite the lower power consumption exhibited by the RNG of Demir and Ergün (2022), the said RNG was verified by simulations unlike our work which was measured on silicon.

The said above assertion is reinforced by a thorough comparative analysis, as shown in Table 5. Referring to the said table, the clock rate refers to the operating clock frequency of the RNG. The throughput pertains to the amount of bits that can be randomly generated in 1 s. The area here is the core area of the RNG excluding the auxiliary circuits. Then, a reported power consumption made by RNG is notably shown in the said table. Lastly, we defined the RNG's Figure of Merit (FOM) as the ratio between the product of throughput and clock rate and the product of power and normalised area. Our RNG's FOM, i.e. 213.7, is slightly lower than the RNG's FOM, i.e. 225.34, of Guler et al. (2017). However, the RNG's throughput, i.e. 3.02 Mbps, of Guler et al. (2017) is much smaller than ours, i.e. 50 Mbps. Notably, the experimental results obtained in our study align with the simulation results reported in previous research (Wang & Lu, 2020).

The distinguishing factor of our design lies in its exceptional throughput of 50 Mbps, which represents a significant accomplishment surpassing all the previous works in the field. The exceptional performance of our system can be attributed to our ground-breaking MUX scrambling technique, which involves a precise manipulation of data to optimise efficiency and significantly enhance the effectiveness of our RNG.

$$^{*}\text{FOM} = \frac{\text{Throughput} \times \text{Clock Rate}}{\text{Power} \times (\text{Normalized Area})}$$

Table 5. Comparison of the metastable RNG with the prior works.

	1	2	3	4	5	6	7	8	9	10	Ours
Year	2012	2013	2017	2017	2017	2019	2020	2021	2022	2020	2023
Verification*	Meas.	Meas.	Meas.	Meas.	Meas.	Meas.	Meas.	Sim.	Sim.	Sim.	Meas.
Implementation	RTN samp.	Osc.	DTC	Osc.	RO	LFSR Digital	TERO	skew-tent map	chaotic	TERO	
Process	65 nm	65 nm	180 nm	130 nm	250 nm	FPGA	180 nm	180 nm	65 nm	40 nm	
Assessment	NIST SP 800–22	NIST SP 800–22	NIST SP 800–22	NIST SP 800–22	NIST 140-2	NIST SP 800–22	FIPS 140-2	NIST SP 800–22	NIST SP 800–22	FIPS 140-1	
Clock Rate (MHz)	0.001	15.1	0.216	1	302.5	33	100	10	1	100	
Throughput (Mbps)	-	7.5	0.27	1	3.02	-	3.33	4.8	0.72	50	
Area (mm^2)	4.5×10^{-5}	0.0067	-	-	0.0206	-	0.7225	-	0.004	0.0016	
Normalised Area†	1.1×10^{-8}	1.59	-	-	0.3296	-	22.3	-	0.95	1.0	
Power (mW)	-	-	8.2×10^{-8}	-	12.3	-	11.827	9.8	0.03	23.4	
FOM*	-	-	-	-	225.34	-	1.263	-	25.26	213.7	

[a]Huang et al. (2012).
[b]Amaki et al. (2013).
[c]Kim et al. (2017).
[d]Siswanto and Rudiyanto (2017).
[e]Guler et al. (2017).
[f]Zode et al. (2019).
[g]Acar and Ergun (2020).
[h]Kızmaz and Ergün (2021).
[i]Demir and Ergün (2022).
[j]Wang and Lu (2020).
*Sim. = Simulation Results; Meas. = Measurement Results.

$$\dagger \text{Normalized Area} = \frac{\text{Area(nm)}}{\text{Process(nm)}^2} \times 10^6$$

.

4. Conclusions

We presented a 40-nm high-throughput RNG design which is implemented using 2-layer interleaved TERO for high-speed applications. SR latches for metastability were used for this interleaved TERO. The RNG was implemented and fabricated using TSMC 40-nm CMOS process. It passed the FIPS 140–1 statistical randomness tests, specifically monobit and long runs test with a higher clock frequency of 100 MHz and a power consumption of 23.4 mW. Among the prior works, our RNG exhibited the highest throughput of 50 Mbps and operated at a high frequency of 100 MHz.

Acknowledgments

The authors thank Taiwan Semiconductor Research Institute (TSRI) for the EDA tool assistance and chip fabrication.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This research was funded by National Science and Technology Council (NSTC), Taiwan, under grant NSTC 109-2218-E-110-007-, 109-2224-E-110-001-, and 111-2623-E-110-002-.

ORCID

Chua-Chin Wang http://orcid.org/0000-0002-2426-2879
Ralph Gerard B. Sangalang http://orcid.org/0000-0002-4120-382X
Oliver Lexter July A. Jose http://orcid.org/0000-0003-4565-9506

References

Acar, B., & Ergun, S. (2020). A reconfigurable random number generator based on the transient effects of ring oscillators. *IEEE Transactions on Circuits and Systems II, Express Briefs: A Publication of the IEEE Circuits and Systems Society*, *67*(9), 1609–1613. https://doi.org/10.1109/TCSII.2020.3013324

Akgul, A., Li, C., & Pehlivan, I. (2017). Amplitude control analysis of a four-wing chaotic attractor, its electronic circuit designs and microcontroller-based random number generator. *Journal of Circuits, Systems & Computers*, *26*(12), 1–20. https://doi.org/10.1142/S0218126617501900

Akiri, J., Tolentino, L. K. S., Yang, L.-J., Esakki, B., Sampath, S., & Wang, C.-C. (2022). A 500-MHz 32-bit DETFF-based shift register utilizing 40-nm CMOS technology. In *Proceeding of 2022 IEEE Asia Pacific Conference on Circuit and Systems (APCCAS)*, Shenzhen, China (pp. 251–255).

Albert, J. R. (2022). Design and investigation of solar PV fed single-source voltage- lift multilevel inverter using intelligent controllers. *Journal of Control, Automation and Electrical Systems*, *33*(5), 1537–1562. https://doi.org/10.1007/s40313-021-00892-w

Albert, J. R., Ramasamy, K., Jerard, V. J. M., Boddepalli, R., Singaram, G., & Loganathan, A. (2023). A symmetric solar photovoltaic inverter to improve power quality using digital pulsewidth modulation approach. *Wireless Personal Communications*, *130*(3), 2059–2097. https://doi.org/10.1007/s11277-023-10372-w

Albert, J. R., Stonier, A. A., & Vanchinathan, K. (2022). Testing and performance evaluation of water pump irrigation system using voltage-lift multilevel inverter. *International Journal of Ambient Energy*, *43*(1), 8162–8175. https://doi.org/10.1080/01430750.2022.2092773

Amaki, T., Hashimoto, M., & Onoye, T. (2013). A process and temperature tolerant oscillator-based true random number generator with dynamic 0/1 bias correction. In *Proc. 2013 IEEE Asian Solid-State Circuits Conference (A-SSCC)*, Singapore, Singapore (pp. 133–136).

Basa, J. J. A., Cu, P. L. G., Malabag, N. N., Naag, L. A. V., Abacco, D. F. P., Siquihod, M. J. M. & Tolentino, L. K. S. (2019). Smart inventory management system for photovoltaic-powered freezer using wireless sensor network. *International Journal of Emerging Trends in Engineering Research*, *7* (10), 393–397. https://doi.org/10.30534/ijeter/2019/057102019

Cherkaoui, A., Bossuet, L., & Marchand, C. (2016). Design, evaluation, and optimization of physical unclonable functions based on transient effect ring oscillators. *IEEE Transactions on Information Forensics and Security*, *11*(6), 1291–1305. https://doi.org/10.1109/TIFS.2016.2524666

Chien, C. (2008). *Digital radio systems on a chip*. Kluwer Academic Publishers.

Dela Cruz, L. A., & Tolentino, L. K. S. (2021). Telemedicine implementation challenges in underserved areas of the Philippines. *International Journal of Emerging Technology & Advanced Engineering*, *11* (7), 60–70. https://doi.org/10.46338/ijetae0721_08

Delgado-Restituto, M., & Rodriguez-Vazquez, A. (2002). Integrated chaos generators. *Proceedings of the IEEE*, *90*(5), 747–767. https://doi.org/10.1109/JPROC.2002.1015005

Demir, K., & Ergün, S. (2022). Random number generators based on metastable behavior in double-scroll chaotic attractors. In *Proceeding of 2022 IEEE 13th Latin America Symposium on Circuits and System (LASCAS)*, San Jose, Costa Rica (pp. 1–4).

Fischer, V., Bernard, F., & Haddad, P. (2013). An open-source multi-FPGA modular system for fair benchmarking of true random number generators. In *Proceeding of 2013 23rd International Conference on Field programmable Logic and Applications*, Porto, Portugal (pp. 1–4).

Guler, U., Pusane, A. E., & Dundar, G. (2017). Design of efficient CMOS ring oscillator-based random number generator. *International Journal of Electronics*, *104*(9), 1465–1482. https://doi.org/10.1080/00207217.2017.1312704

Guo, C., & Zhou, Y. (2018). A dynamic equilibrium algorithm to enhance randomness in TRNG. *Journal of Circuits, Systems & Computers*, *27*(6), 1–11. https://doi.org/10.1142/S0218126618500950

Hemalatha, S., Albert, J. R., Banu, G., & Indirajith, K. (2023). Design and investigation of PV string/central architecture for bayesian fusion technique using grey wolf optimization and flower pollination optimized algorithm. *Energy Conversion and Management*, *286*, 1–23. https://doi.org/10.1016/j.enconman.2023.117078

Huang, C.-Y., Shen, W., Tseng, Y.-H., King, Y.-C., & Lin, C.-J. (2012). A contact- resistive random-access-memory-based true random number generator. *IEEE Electron Device Letters*, *33*(8), 1108–1110. https://doi.org/10.1109/LED.2012.2199734

Jorda Jr., R., Alcabasa, C., Buhay, A., Cruz, E. C. D., Mendoza, J. P., Tolentino, A. & Arago, N. (2019). Automated smart wick system-based microfarm using internet of things. In *Proceeding of Lecture Notes on Research and Innovation in Computer Engineering and Computer Sciences (RICCES)*, Langkawi, Malaysia (pp. 68–74).

Kim, M., Ha, U., Lee, K., Lee, Y., & Yoo, H. (2017). A 82-nW chaotic map true random number generator based on a sub-ranging SAR ADC. *IEEE Journal of Solid-State Circuits*, *52*(7), 1953–1965. https://doi.org/10.1109/JSSC.2017.2694833

Kızmaz, M. M., & Ergün, S. (2021). Skew-tent map based CMOS random number generator with chaotic sampling. In *Proceeding of 2021 19th IEEE International New Circuits and Systems Conference (NEWCAS)*, Toulon, France (pp. 1–4).

Lee, S., Park, M., & Kim, J. (2020). Magniber v2 ransomware decryption: Exploiting the vulnerability of a self-developed pseudo random number generator. *Electronics*, *10*(1), 1–17. https://doi.org/10.3390/electronics10010016

Li, T., Wu, L., Zhang, X., Wu, X., Zhou, J., & Wang, X. (2017). A novel transition effect ring oscillator based true random number generator for a security SoC. In *Proceeding of 2017 International Conference on Electron Devices and Solid-State Circuits (EDSSC)*, Hsinchu, Taiwan (pp. 1–2).

Petrie, C., & Connelly, J. (2000). A noise-based IC random number generator for applications in cryptography. *IEEE Transactions on Circuits & Systems I: Fundamental Theory & Applications*, *47*(5), 615–621. https://doi.org/10.1109/81.847868

Randa, M., Samie, M., & Jennions, I. (2020). Delay-based true random number generator in sub-nanomillimeter IoT devices. *Electronics*, *9*(5), 1–15. https://doi.org/10.3390/electronics9050817

Rodriguez-Vazquez, A., Delgado, M., Espejo, S., & Huertas, J. (1991). Switched-capacitor broadband noise generator for CMOS VLSI. *IEEE Journal of Solid-State Circuits*, *27*(21), 1913–1915. https://doi.org/10.1049/el:19911188

Sangalang, R. G. B., Jose, O. L. J. A., Chua, A. V., & Peralta, J. F. (2022). BatStateU Integrated Response Drone (BIRD): A hybrid unmanned vehicle for disaster response. *International Journal of Computing and Digital Systems*, *12*(3), 629–642. https://doi.org/10.12785/ijcds/120151

Saqib, N. A., Zia, M., Mahmood, H., & Khan, M. A. (2017). On generating high- quality random numbers. *Journal of Circuits, Systems & Computers*, *26*(2), 1–21. https://doi.org/10.1142/S0218126617500190

Schneier, B. (2007). *Applied cryptography: Protocols, algorithms and source code in C*. Wiley.

Serfa Juan, R., & Kim, H. (2018). Reconfiguration of an FPGA-based time-triggered FlexRay network controller using EEDC. *Journal of Circuits, Systems & Computers*, *27*(6), 1–11. https://doi.org/10.1142/S0218126618500962

Siswanto, M., & Rudiyanto, B. (2017). Designing of quantum random number generator (QRNG) for security application. In *Proceeding of 2017 3rd International Conference on Science in Information Technology (ICSITech)*, Bandung, Indonesia (pp. 273–277).

Tolentino, L. K., Lapuz, K. T., Corvera, R. J., Guzman, A. D., Española, V. J., Gambota, C., & Gungon, A. (2017). AQUADROID: An app for aquaponics control and monitoring. In *Proceeding of 6th International Conference on Civil Engineering (6th ICCE 2017)*, Manila, Philippines (pp. 1–8).

Tolentino, L. K. S., Valenzuela, I. C., & Serfa Juan, R. O. (2019). Overhead interspersing of redundancy bits reduction algorithm by enhanced error detection correction code. *Journal of Engineering Science and Technology Review*, *12*(2), 34–39. https://doi.org/10.25103/jestr.122.05

Varchola, M., & Drutarovsky, M. (2010). New high entropy element for FPGA based true random number generators. In *CHES 2010: Cryptographic Hardware and Embedded Systems, Proceeding of International Workshop on Cryptographic Hardware and Embedded Systems*, Santa Barbara, CA, USA (pp. 351–365).

Wang, C.-C., Huang, J.-M., Cheng, H.-C., & Hu, R. (2005). Switched-current 3-bit CMOS 4.0-MHz wideband random signal generator. *IEEE Journal of Solid-State Circuits*, *40*(6), 1360–1365. https://doi.org/10.1109/JSSC.2005.848036

Wang, C.-C., & Lu, S.-W. (2020). 100 MHz random number generator design using interleaved metastable NAND/NOR latches. In *Proceeding of 2020 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*, Ha Long, Vietnam (pp. 98–101).

Wang, C.-C., Tolentino, L. K. S., Ekkurthi, U. K. N., Lou, P.-Y., & Sampath, S. (2022). A 100-MHz 3.352-mW 8-bit shift register using low-power DETFF using 90-nm CMOS process. *International Journal of Electronics Letters*, *11*(3), 1–16. https://doi.org/10.1080/21681724.2022.2087912

Yang, Y., Bai, G., & Chen, H. (2014). A 200Mbps random number generator with jitter-amplified oscillator. In *Proceeding of Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT)*, Hefei, China (pp. 1–5).

Yu, H., & Kim, Y. (2020). New RSA encryption mechanism using one-time encryption keys and unpredictable bio-signal for wireless communication devices. *Electronics*, *9*(2), 1–10. https://doi.org/10.3390/electronics9020246

Zhu, P., Song, X., Liu, L., Wang, Z., & Han, J. (2018). Stochastic analysis of multiplex Boolean networks for understanding epidemic propagation. *Institute of Electrical and Electronics Engineers Access*, *6*, 35292–35304. https://doi.org/10.1109/ACCESS.2018.2842726

Zode, P., Zode, P., & Deshmukh, R. (2019). FPGA based novel true random number generator using LFSR with dynamic seed. In *Proceeding of 2019 IEEE 16th India Council International Conference (INDICON)*, Rajkot, India (pp. 1–3).