ISSN 2347 - 3983

Volume 11. No.5, May 2023
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter011152023.pdf
https://doi.org/10.30534/ijeter/2023/011152023

An Energy Efficient and High Performance Modified Trng based Two Phase Multi Bit Per Cycle Ring Oscillator for IoT Applications

R. Kiran Kumar[1], T.Nanditha[2], B.Pravalika[2], J.Pushpa[2]
Assistant Professor, Electronics & Communication Engineering, Madanapalle Institute of Technology and Sciences, Madanapalle, India. Mail: royalkiran406@gmail.com.
UG Scholars, Electronics & Communication Engineering, Madanapalle Institute of Technology and Sciences, Madanapalle, AP, India. Mail:19691a04b8@mits.ac.in, 20695a0414@mits.ac.in, 20695a0415@mits.ac.in.

Received Date: March 26, 2023 Accepted Date: April 15, 2023 Published Date : May 07, 2023

ABSTRACT

The modified TRNG (true random number generator) is mainly focused due to minimize the power wasted by the superfluous oscillations at higher frequency operations. To boost fan-out condition, random bits are collected from both phases of the slow ROs (Ring oscillators), and the fast RO is only engaged during the brief transition time difference between two slow ROs that are symmetrically built. In order to lower the power consumption of the suggested design, the slow jittery ROs are implemented utilising current starved inverters (CSI) biassed in the weak inversion zone. By decreasing the transistors' drain current and oscillation frequency, their jitter amplitudes are made more pronounced. The quickest three-stage RO quantizes the narrow jittery pulse produced by the differential pair of slow ROs. By counting the number of oscillatory cycles of the quick RO, a gigahertz dynamic toggled D flip-flop counter may be used to extract two random bits from each phase of the jittery ROs. The proposed TRNG is fabricated in a standard 45 nm using 1V supply of CMOS process.

Key words: True random number generator, low energy consumption, current starved ring oscillator, power gating.

1.INTRODUCTION

Many modern cryptographic applications rely heavily on unpredictable random numbers for eys, hash salts, Monte Carlo simulations, initialization parameters, session IDs, and nonces in authentication protocols are all produced based on random number generators (RNGs). Unfortunately, most cryptographic systems lack a consistent source of real random bit streams [2]. Pseudo-random number generators (PRNGs) are usually employed to generate random numbers at the speed required by modern digital computers. PRNG is essentially a mathematical model or formula whose output is completely determined by its initial state, more often known as the "seed". It has a finite periodicity bounded by its number of states.

Abstract-The modified TRNG (true random number generator) is mainly focused due to minimize the power wasted by the superfluous oscillations at higher frequency operations. To boost fan-out condition, random bits are collected from both phases of the slow ROs (Ring oscillators), and the fast RO is only engaged during the brief transition time difference between two slow ROs that are symmetrically built. In order to lower the power consumption of the suggested design, the slow jittery ROs are implemented utilising current starved inverters (CSI) biassed in the weak inversion zone. By decreasing the transistors' drain current and oscillation frequency, their jitter amplitudes are made more pronounced. The quickest three-stage RO quantizes the narrow jittery pulse produced by the differential pair of slow ROs. By counting the number of oscillatory cycles of the quick RO, a gigahertz dynamic toggled D flip-flop counter may be used to extract two random bits from each phase of the jittery ROs. The proposed TRNG is fabricated in a standard 45 nm using 1V supply of CMOS process.

Albeit statistically sound and easily realised with digital logic for custom integrated circuit implementation, PRNG is vulnerable for security-critical applications as the unknown state can be easily predicted once the seed is known [2], [3]. As opposed to a PRNG, a true random number generator (TRNG) is a hardware security primitive that can produce independent and identically distributed (IID) random numbers from a fundamentally non-deterministic physical process. TRNG is non-periodic, or more precisely, it has an infinite number of states. It meets the security goal of the most demanding white box cryptography as its output is unpredictable even when all the design information, such as algorithms, schematics, operations, etc., is known to the adversaries [4].

TRNG is now widely used in not only cryptography, but also Markov Chain Monte Carlo analysis, neural network simulation, industrial labelling, statistical testing, gambling, election auditing, etc., where a number of deterministic PRNGs are found to exhibit artefacts that make them less reliable and secure than expected to generate adequate results [4], [5]. As the demand for applications to be moved to the resource-constrained IoT edges grows, so does the demand for lighter, faster, and lower-power TRNG [6].

Silicon TRNGs are attractive because they are low-cost for mass production and easy for integration. Most silicon TRNGs use the following four ways to get noise from natural or random sources: First, direct amplification of the random noise is a widely used method to produce TRNGs. Thermal noise, for example, is a good source of randomness in semiconductor devices because it is frequency independent and technology independent [1], [7],[9]. However, as thermal noise is often very weak, a wide-bandwidth, high-gain amplifier is required, which can consume significant power and area. To raise the thermal noise to a measurable level, Matsumoto et al. [10] proposed to add a SiN layer in a standard CMOS process.

The amplifier area is reduced with no quality checker employed at the cost of an extra-expensive SiN mask. Recently, another TRNG based on thermal noise amplification was proposed by Bae et al. [11]. It uses a common-mode comparator and the sampling uncertainty of a D flip-flop (DFF) to generate true randomness. It can work at a very high speed, i.e., 3 GB/s, but the power consumption is as high as 5 mW, which is not suitable for IoT devices with a low power budget. Besides, an external high-speed and power-hungry clock generator is also required for sampling the asynchronous input at 3 Gb/s.

Random telegraphic noise (RTN) in single oxide trap MOSFETs can also be utilised for random number generation [12],[14]. The drawback is that RTN is naturally a very slow random signal, even with all the acceleration techniques. Second, met-stability in cross-coupled inverters, latches, and SRAMs can also be used to generate a random bit stream at a high bit rate [15],[17]. The major problem with this random source is that it necessitates a complex post-processing unit to eliminate the systematic bias due to manufacturing process variations. The third entropy source is the clock jitter of free running ring oscillators (ROs) [4], [18]. It offers high flexibility and simplicity in its extractor implementation.

Elementary jitter-based TRNG uses the slow jittery frequency clock to sample the fast jittery clock, but additional power-hungry clock generators are required to provide adequate jitter variations. Yang et al. [19] proposed a jitter-based TRNG that uses the oscillation collapse in a double-edge injected RO, which exhibits good randomness and good process variation tolerance. The last category of TRNGs is based on chaotic systems described by deterministic equations.

Defined using a chaotic map and a bit generation function, these TRNGs can provide long-term unpredictability because they are extremely sensitive to the initial conditions [20],[22]. However, the map characteristics are also susceptible to PVT variations, resulting in a degradation of randomness in real-time operation. The bit rate of the deterministic post-processing functions that can generate nearly i.i.d. bits from this process is limited by their entropy rate. It turns out that the optimal bit generation function for achieving the highest possible entropy rate from a map function is non-trivial to implement. Hence, such TRNGs usually occupy a large silicon area and consume great power.

This project presents a compact and energy-efficient jitter-based TRNG design [23]. The entropy of the proposed TRNG is extracted from the jitter noise contributed by both phases of two free running current starved ring oscillators (CSROs) with a symmetric layout. The CSRO pair's jittery phase difference is represented by a random pulse width modulated waveform. Its short, non-deterministic pulse

duration is used to briefly induce oscillation in a fast RO. The two least significant bits of the quantized pulse duration are extracted by counting the oscillatory cycles of the very fast RO with an ultra-high-speed counter implemented by custom extended true single phase clock (E-TSPC) DFFs. This has cut down on a large number of superfluous oscillations from the fast RO. To further increase the jitter noise and reduce the power consumption, the CSROs are biased in the weak inversion (subthreshold) region.

The proposed TRNG is fabricated in a standard 45 nm 1.2 V CMOS process. The TRNG chip occupies an area of only 366 μm2. Measurement results from ten chips show a high bit rate of 52 Mbps and a low power consumption of only 260 μW, resulting in Figure of Merit (FoM) of 5 pJ/b. The produced bit streams have passed all the bias, autocorrelation, and National Institute of Standards and Technology (NIST) tests.

Digital circuits' guiding principle is high speed and low power. Flip-flops are the fundamental building blocks of digital systems, and their delay and power directly affect their efficiency and power. As stated in [1], a sizable percentage of the power used by the digital system is provided by flip-flops. Additionally, the maximum clock frequency of the system is directly impacted by the setup time and CK-to-Q delay of the flip-flop. Consequently, improving the delay and power of flip-flops will immediately enhance the efficiency and lower the power consumption of digital systems.

TSPC D Flip Flop:

Conventional latches require both true and complementary clock signals. The True Single-Phase-Clock (TSPC) circuit technique uses only one clock signal that is never inverted and fits both static and dynamic CMOS circuits. Integrated high-speed operations using dynamic logic frequently employ edge-triggered D flip-flops. Therefore, even though the device is not transitioning, the digital output is being stored on parasitic device capacitance. Because the reset process may be completed by merely discharging one or more internal nodes, this architecture of dynamic flip flops also permits straightforward resetting. True single-phase clocks (TSPC), a popular dynamic flip-flop version that operates at high speeds with low power, are used to perform flip-flops.

However, dynamic flip-flops will typically not work at static or low clock speeds: given enough time, leakage paths may discharge the parasitic capacitance enough to cause the flip-flop to enter invalid states. TSPC D Flip Flop has four basic stages: precharged p- and n-stages and non-precharged (static) p- and n-stages known as precharged N (PN), precharged P (PP), non-precharged N (SN), and non-precharged P (SP). The following figure shows the architecture of a falling edge-triggered true single phase (TSPC) flip flop. This architecture includes the reset facility by adding a PMOS pass transistor and inverter at the last stages to invert the D-bar logic into D-i.e.Q.

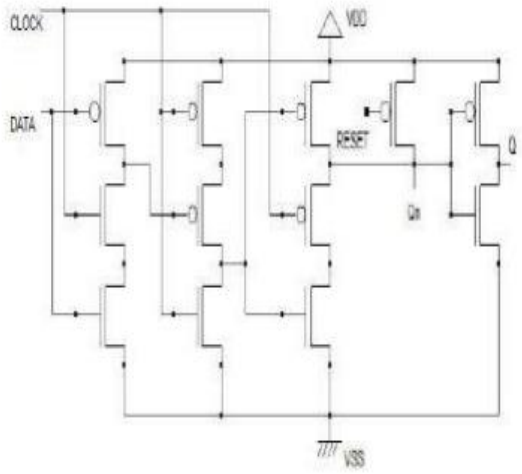

Figure 1: Shows an implementation of a TSPC D flip-flop with reset is triggered on the negative edge of the clock.

Counters are sequential circuits that keep track of the number of pulses applied to their inputs. They occur frequently in real-world, practical digital systems, with applications in computer systems, communication equipment, scientific instruments, and industrial control, to name a few. Many counter designs have been proposed in literature, patented, and/or used in practice. Counters are usually classified into synchronous counters, such as ring counters and twisted counters, and asynchronous counters, such as ripple counters. In CPUs, microcontrollers, DSPs, and many other digital designs that include a programme counter and a timer counter, synchronous counters are usually preferred. Counters are often clocked at a very high rate, usually with an activity factor of 1. In a good design, however, the activity factor can be substantially less than 1 and data-dependent, leading to lower power consumption.

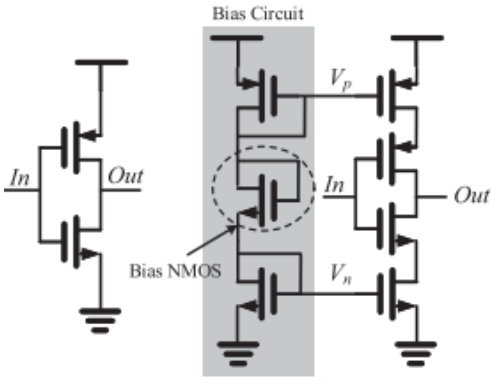

Figure 2: Shows Schematics of (a) a regular inverter and (b) a current-starved inverter.

A CSRO exhibits greater jitter noise amplitude than a regular RO, as demonstrated in [23]. Each CSRO in the proposed TRNG consists of one NAND gate and eight current starved inverters. The NAND gate is equivalent to a regular inverter with the EN signal asserted high. When EN = 1, a nine-stage CSRO is formed. As illustrated in Fig. 4, two extra transistors are added to a regular inverter to construct a current-starved inverter. Due to their low electromagnetic radiation, the interference and coupling effects between the two CSROs are minimised [25]. Besides, the oscillation frequency of the CSRO is tunable by biassing the working currents of the current starved inverters. The bias voltages Vp and Vn control the charging current and discharging current, respectively, of the current starved inverter. The two NMOS transistors and one PMOS transistor in the shaded region of Figure shows 2(b) are used to produce the biassing voltages Vp and Vn on chip, and are shared with other current starved inverters to minimise the silicon area and power consumption.

The static entropy contributed by the process variation of the CSROs can be minimised by symmetric layout and frequency tuning. In fact, the biassing provides a mechanism to fine tune the CSROs' frequencies to eliminate their frequency mismatch due to the manufacturing process variability. The small fixed frequency mismatch between the two CSROs due to the intra-die process variations has been significantly minimised by the symmetric layout at design time. It can be further eliminated by tuning the bias voltages of the CSROs upon chip fabrication.

2.EARLIER WORK

Symmetric Current Starved Ring Oscillators:

A CSRO exhibits greater jitter noise amplitude than a regular RO, as demonstrated in [23]. Each CSRO in the proposed TRNG consists of one NAND gate and eight current starved inverters. The NAND gate is equivalent to a regular inverter with the EN signal asserted high. When EN = 1, a nine-stage CSRO is formed. As illustrated in Figure 3, two extra transistors are added to a regular inverter to construct a current-starved inverter. Due to their low electromagnetic radiation, the interference and coupling effects between the two CSROs are minimised [25]. Besides, the oscillation frequency of the CSRO is tunable by biassing the working currents of the current-starved inverters.

The bias voltages Vp and Vn control the charging current and discharging current, respectively, of the current-starved inverter. The two NMOS transistors and one PMOS transistor in the shaded region of Figure 4(b) meant by used to produce the biassing voltages Vp and Vn on chip and are shared with other current-starved inverters to minimise the silicon area and power consumption. The static entropy contributed by the process variation of the CSROs can be minimised by symmetric layout and frequency tuning. In fact, the biassing provides a mechanism to fine-tune the CSROs' frequencies to eliminate their frequency mismatch due to the manufacturing process variability.

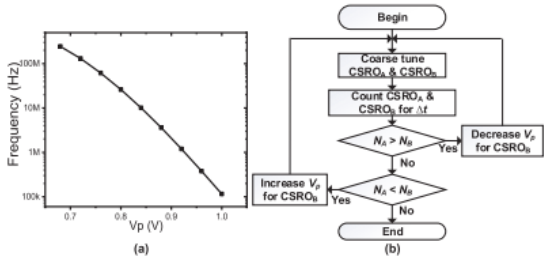

Figure 3: Shows Simulated frequency versus bias voltage Vp; and flow chart for matching the CSROs

The running frequency decreases logarithmically with Vp. This provides a means for the CSROs to adapt to the frequency mismatch due to the intra-die process variations. Figure 3(b) meant Depicts a simple control programme to

tune the CSROs. The two CSROs are coarsely tuned to a desired frequency.

Two counters are used to count the number of cycles of the two CSROs. The counter outputs, NA and NB, are compared after a certain time. If NA is not equal to NB, the bias of CSROB will be adjusted until the two frequencies are almost equal. This calibration is independently applied to each chip after production. The tuned Vp and Vn voltages may differ subtly between two chips since process variations may affect the oscillation frequency of the same CSRO in each chip differently.

There is a tradeoff between tuning time and tuning resolution. The longer the counting time, the finer the frequency it can measure, and the closer the frequency match when NA = NB. The matching process can be automated by the procedure depicted in Figure. 3(b) to reduce the time and cost of tuning.

It is noted that the randomness contributed by the minute phase difference due to the intra-die process variations, if any after tuning, is periodic and cannot be counted towards the true entropy of the proposed TRNG. This static entropy will not affect the original jitter amplitude but will extend the oscillatory duration of the regular RO by a small constant offset.

Hence, the lower-order bits of the quantized phase variation are still unpredictable due to the strong jitter appearing at each edge of the pulse at node C. The regular RO will oscillate for a random number of cycles in every interval when C is high. Since the number of cycles of the regular RO is sufficiently high in each active interval, the counter length can be shortened so that the LSBs extracted in each counting cycle are contributed predominantly by the jitter. The omitted count of the spurious oscillations of the regular RO will contribute to a small excess in power consumption.

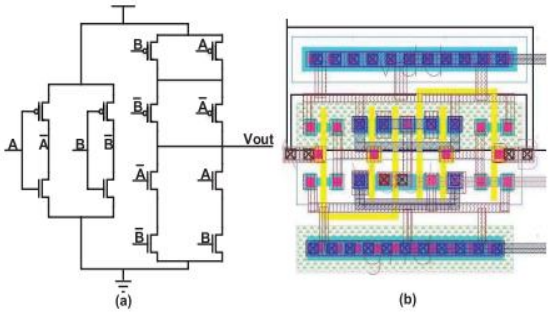

Figure 4 : Shows The schematic and the layout of the XOR gate.

An XOR gate is used to convert the timing jitters between the two symmetrically designed CSROs into a random pulse width modulated signal. It is implemented with the minimum-length transistor to minimise parasitics and maximise driveability. To ensure a fully symmetric and uniform layout, the XOR gate is designed as a mirror CMOS logic circuit with a centroid-symmetric layout. The schematic and layout of the XOR gate are shown in Figure 4. The number of extracted bits per clock phase is determined; the TRNG bit rate can be calculated as bit rate = 2 frequency times the CSRO number of extracted bits per clock phase.

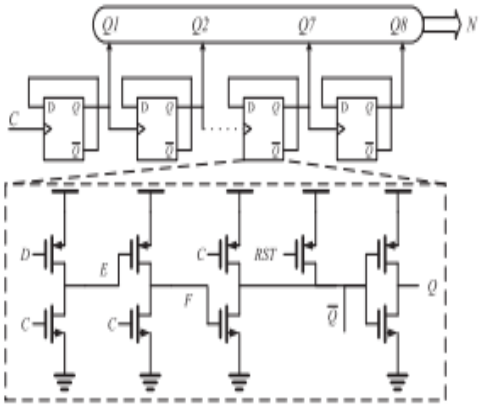

Figure 5: Shows Implementation of an ultra-high-speed 2-bit E-TSPC counter and the schematic of an E-TSPC DFF

Extended True Single Phase Clock (E-TSPC):

When operating the dynamic latch at a very high frequency, a true single-phase clock (TSPC) is used to prevent the clock skew issue. E-TSPC is an extension of TSPC by using only one transistor per stage instead of two clocked

transistors per stage to further reduce the RC delay [32]. With reference to the schematic of the E-TSPC DFF circuit in Figure. 5, the divide-by-two clock Q is obtained by feeding the signal Q of the DFF back to the D input.

Assume that Q is low initially, and then D = Q will precharge E to VD D to turn off the PMOS transistor of the second dynamic latch. By sizing the PMOS transistor larger than its NMOS transistor, the output E of the first dynamic latch can be kept high while the NMOS transistor is turned on. Now, the voltage at node F depends on the clock signal C. If C is high, F is low, and Q will remain low; if C is falling, F will retain its logic state, which enables the PMOS transistor in the third stage to precharge Q more quickly to VD D. The next rising edge of the clock signal causes node E to switch from high to low.

The state of F will be retained when C is still high. Node F of the second dynamic latch will be precharged to VD D when C is falling, which in turn switches the output Q from high to low. The above process repeats with the feedback from Q to D. The ratioing of NMOS and PMOS transistors trades static power consumption for speed, as indicated by the shaded region.

3.PROPOSED WORK

The entropy of the modified TRNG is extracted from the jitter noise contributed by both phases of two free running current starved ring oscillators (CSROs) with a symmetric layout. The CSRO pair's jittery phase difference is represented by a random pulse width modulated waveform.Its short, non-deterministic pulse duration is used to briefly induce oscillation in a fast RO. The power optimization of the design circuitry-based power gating will improve operation and increase fan-out.

The two least significant bits of the quantized pulse duration are extracted by counting the oscillatory cycles of the very fast RO with an ultra-high-speed counter implemented by custom extended true single phase clock (E-TSPC) DFFs. This has cut down on a large number of superfluous oscillations from the fast RO. To further increase the jitter noise and reduce the power consumption, the CSROs are biassed in the weak inversion (sub threshold) region. The proposed TRNG is fabricated in a standard 45-nm 1V CMOS process. The TRNG chip occupies an area of only 366 μm2. Measurement results from ten chips show a high bit rate of 52 Mbps, and a low power consumption of only 260 μW, resulting in Figure of Merit (FoM) of 5 pJ/b. The produced bit streams have passed all the bias, autocorrelation, and National Institute of Standards and Technology (NIST) tests.

Power gating:

One important issue with all of the above-mentioned techniques so-far is that they work for dynamic power reduction of a circuit and are poorly suited to higher frequency applications as they significantly increase the total silicon area by adding extra components (e.g., a level converter in the case of dual voltage scaling, a gated buffer, and enable-logic for clock gating) and therefore have a negative impact on static power dissipation. Power gating is an exception, though, as it involves cutting off the power to inactive circuit components, which aids in lowering both dynamic and static power. In devices where components are idle for extended periods of time, it is therefore a particularly effective optimization.

As shown in Figure 6 the technique involves inserting a sleep transistor between the actual VDD (power supply) rail and the component's VDD, resulting in a virtual supply voltage known as VV DD.Similarly, a sleep transistor between the actual GND (ground) rail and the component’s GND can also be added, creating a virtual ground called VGND. The sleep transistor, in the first case, allows the supply voltage of the block to be cut off to dramatically reduce leakage currents. In practice, power gating is implemented using Dual VT CMOS or Multi-Threshold CMOS (MTCMOS) techniques . Research is also being done on the sleep transistor size to further reduce the leakage power caused by the sleep transistor insertion.

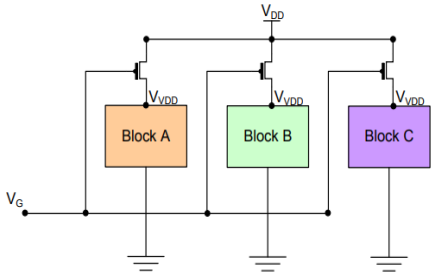

Figure 6 : Shows the use of power gating to reduce the overall circuit power

Since one centralised sleep transistor design suffers from large interconnect resistances between distant blocks, such resistance has to be compensated by an extra-large sleep transistor area that could result in extra load capacitance and delay for driving logic. Hence, two approaches have been proposed to divide the overall circuit into segments and apply several sleep transistors to achieve a more-efficient design. Proposed a cluster-based design structure, where each cluster, consisting of several gates, is accommodated by a sleep transistor separately.

The size of the sleep transistor is determined by the current of the cluster. Their approach achieved a 90% reduction in static power consumption as well as a 15% reduction in dynamic power consumption. Long et all proposed another approach that uses a distributed network of sleep transistors. This approach is better than the cluster-based approach in terms of sleep transistor area and circuit performance and obtains sleep transistor networks that are 70% more area-efficient than the cluster-based networks. Most of the above-mentioned VLSI power-optimization techniques have been deployed in ultra-low-power microcontrollers targeted towards low-power embedded system applications.

Power gated Symmetric Current Starved Ring Oscillators:

A CSRO exhibits greater jitter noise amplitude than a regular RO, as demonstrated in [23]. Each CSRO in the proposed TRNG consists of one NAND gate and eight current starved inverters. The NAND gate is equivalent to a regular inverter with the EN signal asserted high. When EN = 1, a nine-stage CSRO is formed.As illustrated in Figure. 4, two extra transistors are added to a regular inverter to construct a current-starved inverter. Due to their low electromagnetic radiation, the interference and coupling effects between the two CSROs are minimised [25]. Besides, the oscillation frequency of the CSRO is tunable by biassing the working currents of the current-starved inverters. The bias voltages Vp and Vn control the charging current and discharging current, respectively, of the current starved inverter. The two NMOS transistors and one PMOS transistor in the shaded region of Figure. 4(b) are used to produce the biassing voltages Vp and Vn on chip, and are shared with other current starved inverters to minimise the silicon area and power consumption.

Even though the CSRO's static power consumption is cut, the design's average power consumption remains the same, which is due to both static and dynamic power consumption, so in order to reduce the unwanted operation caused by the circuitry, we are applying the power gating at the node supply voltage of the CSRO.

The CSRO frequency should only be tuned once, when the chip is made, to get rid of the small frequency mismatch caused by differences between dies and during maintenance.It is noted that any randomness caused by a small difference in phase due to changes in the die process, if there is any after tuning, is periodic and can't be added to the TRNG's true entropy.

This static entropy will not affect the original jitter amplitude but will extend the oscillatory duration of the regular RO by a small constant offset. The regular RO will oscillate for a random number of cycles in every interval when C is high. Since the number of cycles of the regular RO is sufficiently high in each active interval, the counter length can be shortened so that the LSBs extracted in each counting cycle are contributed predominantly by the jitter. By not counting the spurious oscillations of the regular RO, a small amount of extra power will be used.

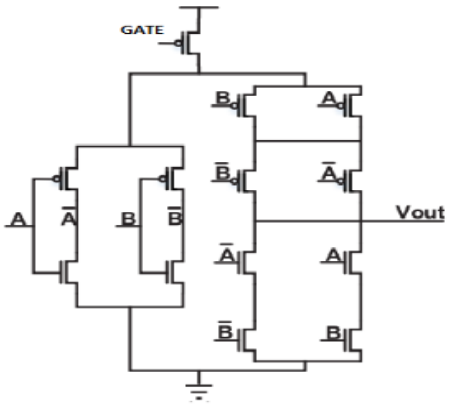

Figure 7: Shows The schematic and the layout of the XOR gate

An XOR gate is used to convert the timing jitters between the two symmetrically designed CSROs into a random pulse width modulated signal. It is implemented with the shortest transistor possible to minimise parasitics and maximise

driveability. To ensure a fully symmetric and uniform layout, the XOR gate is designed as a mirror CMOS logic circuit with a centroid-symmetric layout.

Extended True Single Phase Clock (E-TSPC):

To avoid the clock skew problem when operating the dynamic latch at very high frequency, a true single-phase clock (TSPC) is used. E-TSPC is an extension of TSPC by using only one transistor per stage instead of two clocking transistors per stage to further reduce the RC delay [32]. With reference to the schematic of the E-TSPC DFF circuit in Figure. 4, the divide-by-two clock Q is obtained by feeding the signal Q of the DFF back to the D input.

Assume that Q is low initially, and then D = Q will precharge E to VD D to turn off the PMOS transistor of the second dynamic latch. By sizing the PMOS transistor larger than its NMOS transistor, the output E of the first dynamic latch can be kept high while the NMOS transistor is turned on. Now, the voltage at node F depends on the clock signal C. If C is high, F is low, and Q will remain low; if C is falling, F will retain its logic state, which enables the PMOS transistor in the third stage to precharge Q more quickly to VD D.

The next rising edge of the clock signal causes node E to switch from high to low. The state of F will be retained when C is still high. Node F of the second dynamic latch will be precharged to VD D when C is falling, which in turn switches the output Q from high to low. The above process repeats with the feedback from Q to D. The ratioing of NMOS and PMOS transistors trades static power consumption for speed, as indicated by the shaded regions.

4.EXPERIMENTAL RESULTS

The proposed design is compared with the existing design, and the output results of the proposed design are optimised in such a way that the average power is optimised by utilising the power gating technique at the supply node of the main parts of the overall design. So as power gating can optimise the power results, it can be done at the supply node, or else we can also do it at the ground node.

One million consecutive raw bits were generated by the proposed TRNG at the nominal working condition (1.2 V, 27 ◦C). With one million bits generated from each chip, the average entropy of ten chips is calculated to be 0.999998 by (13). Its corresponding redundancy is defined as R = 1H/Hmax, ,where H is the entropy of the set of states in question with a priori probabilities for each state and Hmax is the maximum entropy for the same number of states.

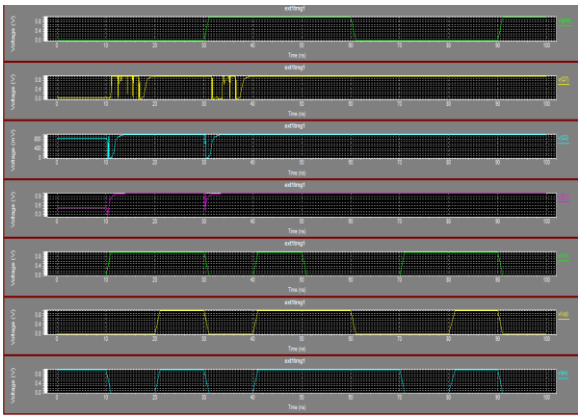

Figure 8: Shows output waveforms of the proposed TRNG

5. CONCLUSION

The design of the modified TRNG-based ring oscillator achieved the high fan-out per cycle due to generating multiple bits for each pulse at a lower power. It extracts randomness from jitter noise produced by CSROs in power gates. The jitter noise is boosted by lowering the oscillation frequency and reducing the charging and discharging currents of the CSRO. A three-stage regular RO with a fast oscillation frequency and a high-speed E-TSPC DFF-based asynchronous counter are used to quantize the jitter into a random sequence of bits. The power-hungry regular RO is only active during the narrow jittery phase of the CSRO pair, which reduces superfluous oscillations significantly. The proposed TRNG is fabricated in standard 45-nm 1V CMOS technology. Its simplicity and energy efficiency make it attractive to resource-constrained IoT devices.

REFERENCES

[1] 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 J. Solid-State Circuits, vol. 51, no. 7, pp. 1695–1704, Jul. 2016.

[2] J. Kelsey, B. Schneier, D. Wagner, and C. Hall, Cryptanalytic attacks on pseudorandom number generators, in Proc. Int. Workshop Fast Softw. Encryption. Paris, France: Springer, Mar. 1998, pp. 168–188.

[3] M. Dichtl, How to predict the output of a hardware random number generator, in Proc. Workshop Cryptograph. Hardw. Embedded Syst., vol. 2779, 2003, pp. 181–188.

[4] M. Sipcevic and C. K. Koc, True random number generators, in Open Problems in Mathematics and Computational Science, C. K. Koc, Ed. Cham, Switzerland: Springer, 2014, pp. 275–315.

[5] D. Hurley-Smith, C. Patsakis, and J. Hernandez-Castro, On the unbearable lightness of FIPS 140-2 randomness tests, IEEE Trans. Inf. Forensics Security, early access, Apr. 17, 2020, doi: 10.1109/TIFS.2020.2988505.

[6] K. Lee, S. Lee, C. Seo, and K. Yim, TRNG (true random number generator) method using visible spectrum for secure communication on 5G network, IEEE Access, vol. 6, pp. 12838–12847, 2018.

[7] C. S. Petrie and J. A. Connelly, A noise-based IC random number generator for applications in cryptography, IEEE Trans. Circuits Syst. I, Fundam. Theory Appl., vol. 47, no. 5, pp. 615–621, May 2000.

[8] R. Brederlow, R. Prakash, C. Paulus, and R. Thewes, A low-power true random number generator using random telegraph noise of single oxide-traps, in IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers, Sacramento, CA, USA, Feb. 2006, pp. 536–537.

[9] F. Tehranipoor, P. Wortman, N. Karimian, W. Yan, and J. A. Chandy, DVFT: A lightweight solution for power-supply noise-based TRNG using dynamic voltage feedback tuning system, IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 26, no. 6, pp. 1084–1097, Jun. 2018.

[10] M. Matsumoto, S. Yasuda, R. Ohba, K. Ikegami, T. Tanamoto, and S. Fujita, 1200μm2 physical random-number generators based on SiN MOSFET for secure smart-card application, in IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers, Feb. 2008, pp. 414–624.

[11] 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 flip-flop, IEEE J. Solid-State Circuits, vol. 52, no. 2, pp. 605–610, Feb. 2017.

[12] A. Mohanty, K. B. Sutaria, H. Awano, T. Sato, and Y. Cao, RTN in scaled transistors for on-chip random seed generation, IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 25, no. 8, pp. 2248–2257, Aug. 2017.

[13] R. Govindaraj, S. Ghosh, and S. Katkoori, CSRO-based reconfigurable true random number generator using RRAM,IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 26, no. 12, pp. 2661–2670, Dec. 2018.

[14] L. T. Clark, S. B. Medapuram, and D. K. Kadiyala, SRAM circuits for true random number generation using intrinsic bit instability, IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 26, no. 10, pp. 2027–2037, Oct. 2018.

[15] C. Tokunaga, D. Blaauw, and T. Mudge, True random number generator with a metastability-based quality control, in IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers, Sacramento, CA, USA, Feb. 2007, pp. 404–405.

[16] J. Holleman, S. Bridges, B. P. Otis, and C. Diorio, A 3 μw CMOS true random number generator with adaptive floating-gate offset cancellation, IEEE J. Solid-State Circuits, vol. 43, no. 5, pp. 1324–1336, May 2008.

[17] S. Srinivasan, S. Mathew, V. Erraguntla, and R. Krishnamurthy, A 4Gbps 0.57pJ/bit process-voltage-temperature variation tolerant alldigital true random number generator in 45 nm CMOS, in Proc. 22nd Int. Conf. VLSI Design, Jan. 2009, pp. 301–306.

[18] 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, in Proc. IEEE Custom Integr. Circuits Conf., San Jose, CA, USA, Sep. 2014, pp. 1–4.

[19] K. Yang, D. Blaauw, and D. Sylvester, An all-digital edge racing true random number generator robust against PVT variations, IEEE J. SolidState Circuits, vol. 51, no. 4, pp. 1022–1031, Apr. 2016.

[20] T. Stojanovski, J. Pihl, and L. Kocarev, Chaos-based random number generators—Part II: Practical realization, IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 38, no. 3, pp. 281–288, Mar. 2001.

[21] F. Pareschi, G. Setti, and R. Rovatti, Implementation and testing of high-speed CMOS true random number generators based on chaotic systems, IEEE Trans. Circuits

Syst. I, Reg. Papers, vol. 57, no. 12, pp. 3124–3137, Dec. 2010.

[22] M. Kim, U. Ha, K. J. Lee, Y. Lee, and H.-J. Yoo, A 82-nW chaotic map true random number generator based on a sub-ranging SAR ADC, IEEE J. Solid-State Circuits, vol. 52, no. 7, pp. 1953–1965, Jul. 2017.

[23] Y. Cao, C.-H. Chang, Y. Zheng, and X. Zhao, An energy-efficient true random number generator based on current starved ring oscillators, in Proc. Asian Hardw. Oriented Secur. Trust Symp. (AsianHOST), Oct. 2017, pp. 37–42.

[24] T. Amaki, M. Hashimoto, and T. Onoye, "A process and temperature tolerant oscillator-based true random number generator with dynamic 0/1 bias correction," in Proc. IEEE Asian Solid-State Circuits Conf. (ASSCC), Singapore, Nov. 2013, pp. 133–136.

[25] Y. Cao, X. Zhao, W. Ye, Q. Han, and X. Pan, "A compact and low power RO PUF with high resilience to the EM side-channel attack and the SVM modelling attack of wireless sensor networks," Sensors, vol. 18, no. 2, p. 322, Jan. 2018.

[26] H. Song, The Arts of VLSI Circuit Design. Bloomington, IN, USA: Xlibris, 2011. [27] U. Guler and G. Dundar, "Modeling CMOS ring oscillator performance as a randomness source," IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 61, no. 3, pp. 712–724, Mar. 2014.

[28] B. Razavi, Design of Analog CMOS Integrated Circuits. New York, NY, USA: McGraw-Hill, 2001.

[29] N. Modak, B. Chatterjee, A. Anvesha, and M. S. Baghini, "A 120 nW, tunable, PVT invariant voltage reference with 80 dB supply noise rejection," in Proc. IEEE Int. Symp. Nanoelectronic Inf. Syst., Dec. 2015, pp. 181–184.

[30] Q.-C. Chen and L.-H. Wang, "A 100nW 6PPM/◦C voltage reference with all MOS transistors," in Proc. Int. Conf. Commun. Problem-Solving (ICCP), Sep. 2016, pp. 1–2.

[31] I. Lee, D. Sylvester, and D. Blaauw, "A subthreshold voltage reference with scalable output voltage for low-power IoT systems," IEEE J. SolidState Circuits, vol. 52, no. 5, pp. 1443–1449, May 2017.

[32] X. P. Yu, M. A. Do, W. M. Lim, K. S. Yeo, and J.-G. Ma, "Design and optimization of the extended true single-phase clock-based prescaler," IEEE Trans. Microw. Theory Tech., vol. 54, no. 11, pp. 3828–3834, Nov. 2006.

[33] M. Baudet, D. Lubicz, J. Micolod, and A. Tassiaux, "On the security of oscillator-based random number generators," J. Cryptol., vol. 24, no. 2, pp. 398–425, Oct. 2010.

[34] T. M. Cover and J. A. Thomas, Elements of Information Theory. New York, NY, USA: Wiley, 1991.

[35] Claude Shannon & Information Theory—Redundancy. Accessed: May 2, 2021. [Online]. Available:https://cs.stanford.edu/people/ eroberts/courses/soco/projects/1999-00/information-theory/redundancy_ 5.html

[36] NIST. (Apr. 2019). Sp 800-90b, Entropy Sources Used for Random Bit Generation. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-90b/final

[37] A. Rukhin et al., "A statistical test suite for random and pseudorandom number generators for cryptographic applications," NIST, Gaithersburg, MD, USA, NIST Special Publication 800-22, 2010.