IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 20, 2021, accepted October 5, 2021, date of publication October 14, 2021, date of current version October 22, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3120047

A PVT Tolerant True Random Number Generator Based on Oscillator Phase Under Sub-Harmonic Injection Locking

ESLAM ELMITWALLI[1], (Graduate Student Member, IEEE), KAI NI[2], (Member, IEEE), AND SELÇUK KÖSE[1], (Member, IEEE)

[1]Electrical and Computer Engineering Department, University of Rochester, Rochester, NY 14620, USA
[2]Electrical and Microelectronic Engineering Department, Rochester Institute of Technology, Rochester, NY 14623, USA

Corresponding author: Eslam Elmitwalli (eelmitwa@ur.rochester.edu)

ABSTRACT A digital true random number generator based on the oscillator phase generated by the second-order sub-harmonic injection locking phenomenon is proposed in this paper. Owing to the thermal jitter, the phase difference between a free-running (*i.e.,* unsynchronized) oscillator and an injected external signal collapses to one of two stable solutions in a truly random manner. The injected external signal is generated from another oscillator operating at close to twice the frequency of the free-running oscillator. The random sequence extracted from the resulting stable solutions is bias- and correlation-free, nullifying the need for a bias compensation circuitry. The proposed design is demonstrated with extensive simulations to be robust under process, voltage, and temperature variations. The generated random patterns pass the National Institute of Standards and Technology test suite.

INDEX TERMS Hardware security, second-order injection locking, security, security primitive, true random number generator.

I. INTRODUCTION

Random number generators are major constituents of a wide range of applications. In statistical sampling and simulations such as Monte Carlo, reproducible randomness is often desired and can benefit from pseudo-random number generators. Alternatively, security-critical applications require high-quality true randomness that demonstrates no predictability, bias, or correlation. An example is encryption algorithms that stem their security from the unpredictable nature of cryptographic keys. True random number generators (TRNGs) extract the randomness from different physical phenomena that are known to be statistically random, such as thermal noise and radioactive decay.

Thermal noise has been intensively used as a source of randomness because of the inherent statistically random Gaussian distribution and abundance in electric circuits [1]–[5]. Randomness can be extracted from thermal noise using several methods, such as amplification of thermal noise directly from a resistance [1], and conversion of thermal noise to jitter [6]. Jitter resulting from PLL circuits has also been used in TRNG designs [7]–[9].

Additionally, process, voltage, and temperature (PVT) variation tolerance is an important parameter in TRNG designs [4], [10]. TRNG designs must be robust against variations in the operating conditions due to aging effects, environmental changes, or external physical attacks, such as those targeting the supply voltage level [11]. Several techniques for bias detection and correction have been proposed in the literature [12].

In this work, a novel TRNG design is proposed that extracts randomness from thermal jitter using second-order sub-harmonic injection locking (SHIL) phenomenon. Recently, a TRNG based on second-order SHIL was proposed in [13]. We argue that the existing design is not feasible to implement and may not work properly on a fabricated CMOS chip without certain modifications. The PVT variation effects were not considered, which could have strong implications for the TRNG operation, as shown by the analysis in this work. In this work, an improved design is proposed that includes bit generation, and a more extensive analysis is performed. The proposed design is resilient to different operating

The associate editor coordinating the review of this manuscript and approving it for publication was Mehdi Sookhak.

conditions, including process variations, temperature, and supply voltage levels, based on extensive SPICE simulations. The implications of process variations on bias and correlation can be mitigated with a lower design overhead in terms of complexity compared to other designs. The proposed design successfully passes the National Institute of Standards and Technology (NIST) SP800-22 test suite.

The remainder of this paper is organized as follows. A brief background on SHIL related to the proposed TRNG is presented in Section II. The proposed TRNG design is described in Section III. The extensive simulation results and NIST test evaluations are described in Section IV. The implications of PVT effects on the generated true random number sequence are described in Section V. Finally, conclusions are presented in Section VI.

II. SUB-HARMONIC INJECTION LOCKING BASED TRUE RANDOM NUMBER GENERATOR

Injection locking is a phenomenon observed when two oscillators in close frequency proximity synchronize with each other. In nature, for example, clock pendulums attached to the same wall would tick in synchrony after a period of time. This phenomenon was also observed in electrical oscillators and was first analyzed for LC tanks using Adler's equation [14]. A free-running oscillator with a natural frequency F_0 is injection-locked by a small external AC signal running at a frequency within a specific locking range $F_0 \pm \Delta F$. The oscillator eventually inherits the same frequency as the external AC signal while maintaining a constant phase difference under locking conditions. This phenomenon is often observed in RF circuits and is typically utilized in frequency division and frequency synchronization [15]. A generalized Adler's equation that describes the injection locking phenomenon for oscillators, regardless of their topology, was derived in [16].

Interestingly, oscillators can also be locked to frequencies that are m integer divisions of an external signal's frequency in what is known as SHIL [17]. The following *Alderized* SHIL equation can be used to determine the conditions under which m^{th} SHIL is possible

$$\frac{f_{ext} - mf_{osc}}{mf_{osc}} = g(\theta), \tag{1}$$

where the external perturbation frequency f_{ext} is close to m multiples of the free-running oscillator natural frequency f_{osc}, and $g(\theta)$ is a periodic function of the SHIL phase difference θ with a period of $1/m$. The solution of (1) provides the locking range for which mth-order SHIL is possible. In Fig. 1a, the two sides of (1) are plotted for the case where $m = 2$, and the solutions are the points of intersection. A total of $2 \times m$ solutions exist, but only half of these solutions are stable depending on the sign of dx/dy. It should be noted that the phase difference between the two stable solutions is 180°. In Fig. 1b, the realization of the two stable solutions is shown in the form of two different phase configurations for the free-running oscillator. In this work, the two phase

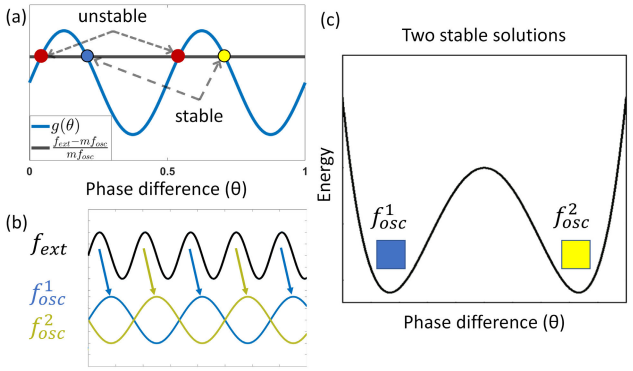


FIGURE 1. (a) Demonstration of the two sides of (1). Red dots represent the unstable solutions. The stable solutions are marked as either a yellow or a blue dot – this designation for the two stable solutions is maintained throughout the paper. (b) The two stable solutions are represented as two different phase configurations (f^1_{osc} and f^2_{osc}) while undergoing SHIL to an external signal (f_{ext}). (c) Representation of second-order SHIL as a metastability curve.

configurations are denoted as bit 1 and bit 0. The existence of two solutions under second-order SHIL can be represented as a metastability curve, as shown in Fig. 1c. The analysis of (1) demonstrated several important properties [17]. The properties that are most relevant to the proposed work are summarized as follows:

- There exists m stable solutions for each m^{th} order SHIL.
- Disturbances to the circuit can lead to changes from one solution to another.
- An asymmetric ring oscillator (RO) design enhances second-order SHIL.

To the best of the authors' knowledge, there is no analytical equation in the literature that describes which solution out of the m stable solutions the circuit will resolve to. In this work, the idea of the TRNG is built around second-order SHIL, where a free-running oscillator's phase resolves to one of two stable phase configurations when perturbed by an external signal running at a frequency close to twice its natural frequency. Based on extensive simulations, we argue that the resulting phase configuration depends on the relative phase of the free-running oscillator and the injected signal at the moment of locking, and that both stable phase configurations occupy half of the solution space. A jittery switch signal is utilized to create uncertainty in the circuit condition at the moment of locking, resulting in truly random output locking states that represent the two binary bits. As a result of the flexible locking range, the design is tolerant to frequency variations under different temperatures, voltage levels, and process variations. If both sources of frequency are designed based on the same platform, the circuit operation can be maintained under temperature and process variation changes as long as the oscillators remain within the locking range. The implications of the power supply variations can be mitigated by designing inverters in a tunable manner to alleviate extreme frequency changes similar to the work reported in [4]. Note that fine tuning is typically not required, and

only coarse tuning is sufficient to position the circuit within a reasonably wide frequency locking range.

III. RING OSCILLATOR IMPLEMENTATION OF THE PROPOSED DESIGN

The general circuit for the SHIL TRNG proposed in an earlier work [13] is shown in Fig. 2. In this circuit, a fast external signal is injected into a slower free-running RO designed with a natural frequency close to half the frequency of the externally injected signal. The slow RO is designed with asymmetric transistor sizing to enable second-order SHIL, as mentioned in [17]. The SHIL circuit is designed with the locking range considered, and the SHIL phenomenon is controlled using a switch. In the event of turning on the switch (logic high), SHIL occurs where the slow RO frequency synchronizes with half the frequency of the external signal. Because the external signal frequency is around twice as fast, each peak of the slow RO corresponds to two peaks of the external signal. Owing to SHIL, each slow RO peak synchronizes with either one of the two peaks of the external signal constituting the two stable phase configurations, as shown in Fig. 1b. Each peak of the external signal wave is designated as peak '0' or peak '1' to distinguish the two stable phase configurations. When the switch is turned off (logic low), the slow RO reverts to its natural frequency and loses synchronization with the external signal until the switch is turned on again.

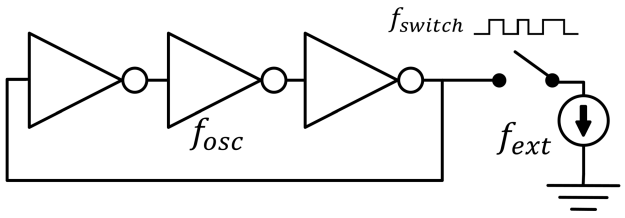


FIGURE 2. SHIL based TRNG design which is vulnerable under PVT variations (reproduced from [13]).

Several drawbacks can be noted in the design shown in Fig. 2. For example, consider the following hypothetical situation: Because of the PVT effects, the free-running RO natural frequency shifts to exactly half the frequency of the external signal. This is the same as saying that the free-running RO has a natural frequency equal to its frequency under second-order SHIL. Assume that both the external signal and the free-running RO are comprised of ideal components, and the switch is the only source of jitter. When the switch is turned on, the free-running RO synchronizes with the external signal following one of the two phase configurations shown in Fig. 1b. When the switch is turned off, the free-running RO will not lose synchronization because its natural frequency is the same as its frequency under SHIL. Therefore, the free-running RO will keep tracking the same phase configuration under ideal conditions. When the switch is turned on again, the free-running RO is more likely to maintain its phase configuration given that it already satisfies a stable solution for the SHIL equation. Under this hypothetical situation, the TRNG will be biased toward outputting the same bit regardless of the amount of jitter in the switch. In another hypothetical situation, assume that the natural frequency of the free-running RO is slightly different from its frequency under SHIL. A switch period that is too short may not allow enough time for the free-running RO to significantly desynchronize during the time between two successive SHIL events, resulting in a significant correlation between successive bits. In this case, a long switch period is needed to increase the likelihood of a change in the next switching event, depending on the proximity of the two frequencies. This places a constraint on the minimum switch jitter required to produce unbiased randomness. The aforementioned hypothetical situations show that the operation of the TRNG is sensitive to the difference between the free-running RO frequency and its frequency under SHIL and can be widely affected by PVT effects.

The main assumption in the previous hypothetical situations is that the resulting phase configuration under second-order SHIL depends on the phase difference between the free-running RO and the two stable phase configurations at the onset of SHIL. The phase difference, defined in the previous sentence, is determined by the rate of desynchronization between two successive SHIL events (*i.e.,* when the switch is turned off). The following simulation is conducted to test this assumption. The circuit in Fig. 2 is implemented on Cadence Virtuoso circuit simulator, where the free-running oscillator is designed with a natural frequency of 6GHz, and the frequency of the external signal is 11.6GHz. When the switch is turned on, the free-running oscillator undergoes SHIL and oscillates at a frequency of 5.8GHz. The onset of SHIL corresponds to the moment when the switch is turned on, as represented by (Point B) in Fig. 3. The phase configuration of the free-running RO under SHIL is measured as a function of both the free-running RO phase and the external signal phase at the onset of SHIL, and the resulting 2D map is shown in Fig. 4. Because the external signal frequency is twice that of the stable phase configuration, two cycles of the external signal correspond to one cycle of the stable phase configuration. The two stable phase configurations are equally represented in the 2D map, but their distribution is not symmetric because of the non-idealities in the circuit. In this 2D map, a constant phase difference between the free-running

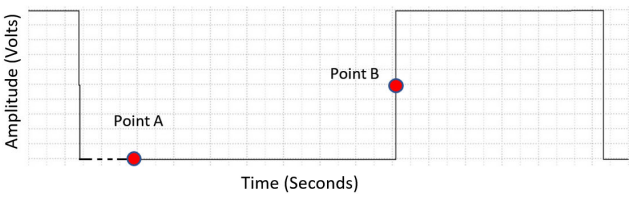


FIGURE 3. Switch signal with frequency (f_{switch}). Point A is a point where the two oscillatory signals are disconnected and desynchronized. Point B represents the onset of an SHIL event, where the two oscillatory signals start synchronizing.

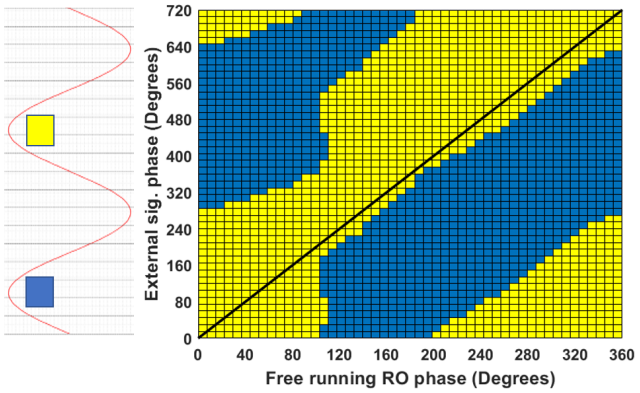


FIGURE 4. On the right: 2D map of the SHIL phase configuration of the RO as a function of the free-running RO phase (x-axis), and the external signal phase (y-axis). The SHIL phase configuration is measured when the signals completely synchronize. The phases are measured at the onset of SHIL before complete synchronization. The yellow (blue) squares refer to the phase configuration synchronized with the yellow (blue) marked peaks of the external signal wave (on the left). The line ($y = 2x$) plotted shows that no significant changes occur if the free-running RO maintains constant phase difference with any of the two phase configurations.

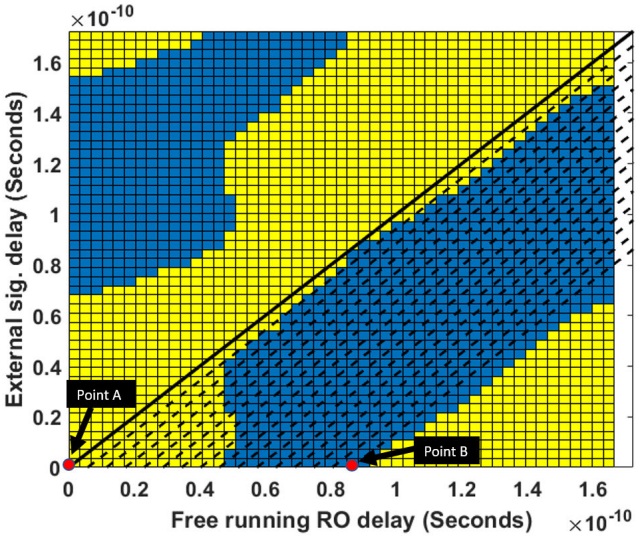


FIGURE 5. The x and y axes of Fig. 4 are converted to delay and replotted here. The solid black line is the line $y = x$ representing desynchronization when the switch is off. The dashed black lines are the extension of the solid line over successive periods. Point A is an arbitrary point when the switch is off and no frequency locking taking place. Point B represents 180° phase shift from Point A. The white region on the right depicts the mismatch between the frequency of the free-running RO (6GHz) and the phase configuration (5.8GHz).

RO and the SHIL phase configuration is maintained on lines parallel to $y = 2x$. In most cases, lines of constant phase difference cover only one of the two phase configurations except at the boundaries. The results show that if the phase difference is kept constant between two successive SHIL events, the phase configuration in both events is likely to be the same. Therefore, for unbiased randomness, the amount of jitter in the switch should allow for a significant change in the phase difference between successive SHIL events.

Because the free-running RO natural frequency is not exactly half the frequency of the external signal, the two signals desynchronize when the switch is turned off, which means that their phase difference is not maintained constant. To show the desynchronization between two successive SHIL events for the example in Fig. 4, the 2D map is converted from phase to delay, as shown in Fig. 5. The origin corresponds to (Point A) in Fig. 3, which is an arbitrary instance in time when the switch is turned off and the two signals are at phase 0°. When the switch is turned off, the two oscillatory signals are disconnected, and their phase difference starts to increase. The growth in phase difference results in the transition from one phase configuration region to another. The transition between the two phase regions over one period and its extensions over several periods are represented by the solid and dashed black lines, respectively, in Fig. 5. Because of the mismatch between the period of the free-running oscillator and the period of the SHIL phase configuration, the extensions of the solid black line ($y = x$) shift slightly to the right after every cycle. Point B in Fig. 5 is the point at which the phase difference between the two signals is 180°. The phase difference returns to Point A again after a time period corresponding to the beat frequency of the two signals. As the two phase configurations are equally distributed in the 2D map, a switch jitter covering the full 2D map will result in true randomness. Assuming a Gaussian distribution for the thermal jitter in the switch, an RMS jitter value covering 180° phase difference between the free-running RO and any of the phase configurations would be required to minimize the correlation between successive measurements. This value can be calculated from the beat period of the free-running RO signal and the phase configuration divided by half, as follows

$$RMS\ Jitter = \left(\frac{1}{|f_{ext} - 2f_{osc}|}\right), \tag{2}$$

where f_{ext} is the external signal frequency (which is twice the frequency of the phase configurations), and f_{osc} is the free-running RO frequency.

In (2), the values of the two frequencies in the denominator should be close to each other to satisfy the locking range requirement, resulting in a large thermal jitter requirement. Additionally, a small variation in the frequencies due to PVT will lead to a large variation in jitter requirements. For example, a 2% change in the free-running RO frequency could result in the doubling of the required RMS jitter. For the case where the free-running RO natural frequency is exactly half the external signal frequency, an infinite amount of RMS jitter is required, meaning that the output is always biased toward one of the phase configurations. Therefore, obtaining results with no bias or correlation may not be practical with the circuit shown in Fig. 2.

To minimize the RMS jitter requirement in (2), without violating the locking range, an improved design is proposed in which the oscillator is turned off with the switch, as shown in Fig. 6. In this design, when the switch is turned off, desynchronization occurs instantly because the free-running RO is disabled. When the switch is turned on, the free-running

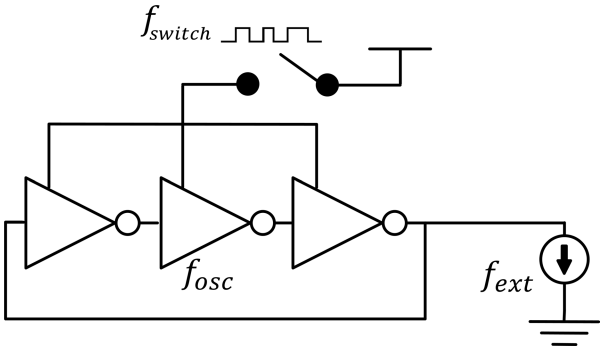


FIGURE 6. Proposed TRNG design where the switch is connected between the free-running RO and the supply voltage.

RO is powered up and is injection-locked to a phase configuration depending on the phase of the external signal at the moment of switching. Therefore, turning off the free-running RO with the switch results in eliminating the $2f_{osc}$ term from (2) leading to a much smaller RMS jitter requirement

$$RMS\ Jitter = \left(\frac{1}{f_{ext}}\right). \tag{3}$$

In this case, the switch edge can be viewed as sampling from a 2D solution space corresponding to one of the vertical lines in Fig. 5. This representation is shown in Fig. 7, where both phase configuration regions overlap periodically. Ideally, the best-case scenario is when the edge of the switch is situated at the midpoint between the two phase configuration regions. In this best-case scenario, any amount of thermal jitter is sufficient to produce a random phase configuration. However, with no constraint on the switch edge position, the worst-case scenario is equally probable, where the clock edge is situated in the middle of one of the two phase configuration regions. The Shannon entropy value is estimated based on the worst-case scenario as a function of the switch RMS jitter normalized to the external signal period. The most probable output in the worst-case scenario is calculated from the Gaussian CDF, and the resulting entropy is plotted in Fig. 8. An entropy value of 0.99994 is obtained when the RMS jitter is equivalent to one period of the external signal.

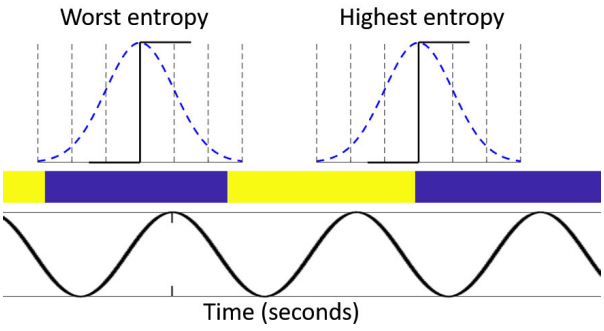


FIGURE 7. Worst-case entropy and best-case entropy position for the switch position.

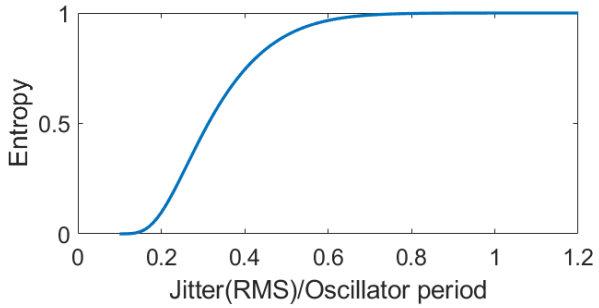


FIGURE 8. Shannon entropy estimation based on worst-case scenario.

IV. STATISTICAL ANALYSIS OF THE TRUE RANDOM NUMBER GENERATOR

The proposed design is implemented at the transistor level and simulated using Cadence Virtuoso circuit simulator using 28nm FDSOI technology, based on the circuit shown in Fig. 9. The free-running RO is designed with asymmetric transistor sizing, which is suitable for second-order SHIL. The external signal is generated from another on-chip ring oscillator - henceforth referred to as the external signal RO - connected to the free-running RO through a *sync* inverter. The sync inverter controls the connection strength between the two oscillators. The sizing of this inverter is important, and a strong connection could potentially drive the free-running RO to the frequency of the external signal RO. The sync inverter is disabled with the switch signal to reduce coupling between the signals on both sides of the sync inverter when the switch is turned off. Thermal jitter is

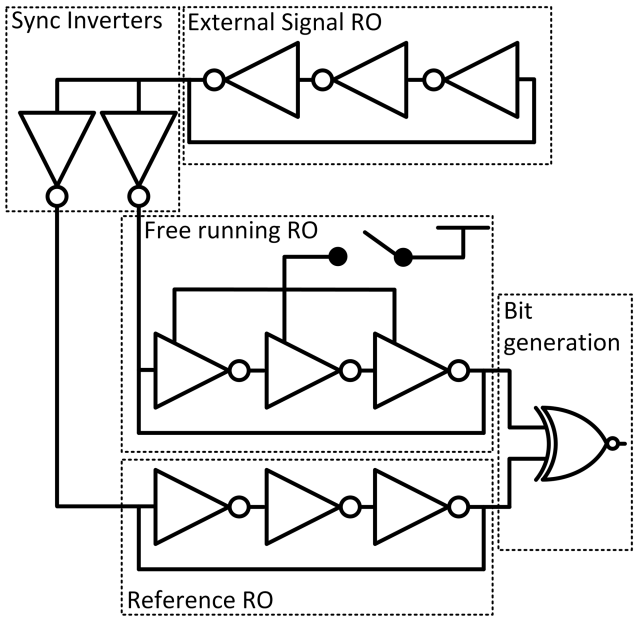


FIGURE 9. Proposed SHIL TRNG design with improved PVT tolerance and bit generation.

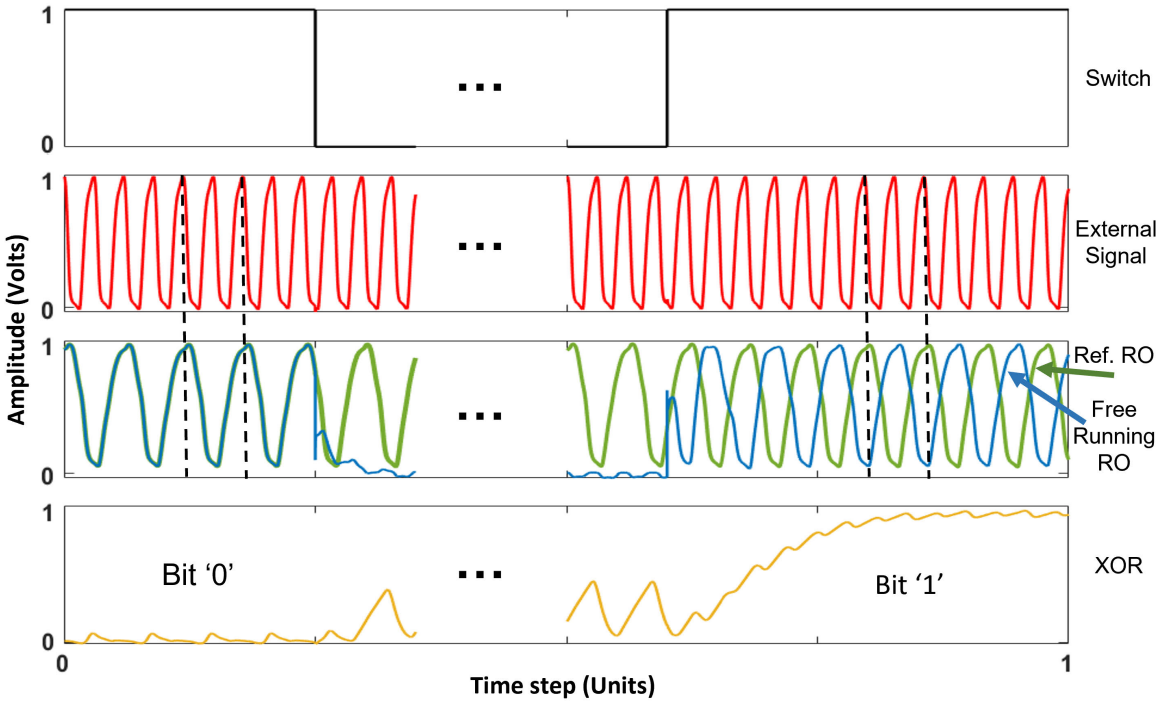


FIGURE 10. Signals from the circuit shown in Fig. 9. The topmost graph is for the switch signal. The Ref. RO (Green) is always synchronized with the external signal RO (Red). When the switch is high, the free-running RO (Blue) is powered up and starts synchronizing with the external signal RO. The XOR detects whether the reference and free-running signals are in phase or out of phase.

injected into the switch with an RMS jitter value equal to the external signal RO period.

For bit generation, a reference RO is added that is designed with the same natural frequency as the free-running RO. The reference RO is always powered and injection-locked to the external signal RO. The idea is that the reference RO will follow one phase configuration, whereas the free-running RO will switch between the two phase configurations according to the switch jitter. In this way, every time the switch is turned on, the free-running RO will be either in phase or out of phase with the reference RO. By XORing these two signals, a random binary bit can be obtained directly when the switch is turned on. The requirement that the reference RO maintains a constant phase configuration is not strict because the XOR gate will give a random output as long as one of its inputs is random.

The external signal RO is designed with a frequency of 16.9GHz, and the free-running oscillator is designed with a frequency of 8.4GHz close to the lock frequency of 8.45GHz. The switch frequency is designed at 700MHz to allow sufficient time for a stable phase configuration. The experimental results demonstrate that this frequency is sufficient for SHIL to occur, and for any uncertainties in the phase configuration, at the beginning of the lock, to resolve. Additionally, a switch frequency that is slower than that of the injection-locked ROs allows for thermal jitter effects to accumulate. The throughput of this design is determined based on the switch frequency and is therefore 700Mbps at a temperature of 25°C and a supply voltage of 1V. A total power of $511\mu W$ is reported from the simulation, resulting in an energy consumption of 1.16pJ/bit.

The output signals of this setup are shown in Fig. 10, where a representation of the two stable second-order SHIL phase configurations is shown. The free-running oscillator signal is in phase with one of the peaks of the external signal RO when the switch is high. Without loss of generality, the two peaks are designated as bit '1' and bit '0'. The XOR gate detects the resulting phase configuration by XORing the free-running RO signal with the reference RO. The simulation results are imported into MATLAB to extract the random binary sequence from the XOR signal. The generated binary sequence successfully passed all NIST SP800-22 tests based on P-values and proportions of passed sequences, as listed in Table 1. The binary sequence used in these tests is 2Mb long, which is limited by the long simulation time, as SHIL simulations require small sequential time steps that do not benefit from parallelization.

The design of this TRNG is not affected by deterministic jitter in the switch signal as long as the thermal jitter is sufficiently large. The reason is that any offset to the edge of the switch will be superimposed with the Gaussian thermal jitter, diminishing any correlation. This is accounted for by assuming the worst-case entropy position for the switch edge according to Fig. 7 and the entropy estimation in Fig. 8. This is further tested by running a simulation including deterministic jitter in addition to the thermal jitter components

TABLE 1. NIST SP800-22 randomness test results for a binary sequence of length ∼2Mb, divided into 110 sub-sequences of length 20Kb each. All tests are successful.

Randomness Test*	P-value$_T$	Proportion
Freq.	0.294867	108/110
Block Freq.	0.135861	110/110
Cumul. Sums (1)	0.480244	109/110
Cumul. Sums (2)	0.684327	108/110
Runs	0.033122	110/110
Longest Run	0.245833	110/110
Rank	0.088469	108/110
FFT	0.234594	110/110
Non-Overl. Templ.**	PASS	PASS
Overl. Templ.	0.775688	109/110
Approx. Entropy	0.480244	109/110
Serial (1)	0.646584	110/110
Serial (2)	0.739918	108/110
Linear Complexity	0.497956	109/110

* The test is successful if P-value$_T$ $>$ 0.0001, and the proportion of successful sequences is $>$ 105, where the alpha for each sub-sequence is set at 0.01.
** For Non-Overlapping Template test, "PASS" indicates that all 148 sub-tests meet the passing requirements.

with the resulting sequence successfully passing the NIST SP800-22 tests. Additionally, because the design is based on ROs, global deterministic jitter sources cancel out [18], [19].

V. PROCESS, VOLTAGE AND TEMPERATURE VARIATIONS

The design is evaluated at different temperatures to mimic different operating scenarios. The simulation is run over a temperature range from -50 °C to 110 °C and the results are tabulated in Table 2. The temperature affects the ROs in a similar fashion, resulting in a shift in their frequencies. The frequency values in this table are the natural frequencies of the external signal RO and the free-running RO. Although the frequency shift is different for each RO, SHIL can still occur as long as the value $f_{osc} - f_{ext}/2$ is within the locking range. According to the results, the binary sequences generated from the design pass the NIST test across the tested temperature range.

To demonstrate the effect of temperature on the entropy of the proposed design, the estimation of Shannon entropy is carried out using the results from Table 2. The resulting entropy curve is compared with the existing design, as shown in Fig. 11. The RMS jitter value is normalized to the frequency of the external signal RO at the nominal temperature. The results show that for the design proposed in this work, the required RMS jitter to obtain the same entropy value does not change significantly with temperature. However, for the existing design in [13], the required RMS jitter is much larger at any given temperature. Additionally, changes in temperature lead to large jumps in the required RMS jitter, which make it impractical to make a design that is robust across a large temperature range.

The process and mismatch variation effects are studied using Monte Carlo simulation files provided with the technology library. The simulation is run for 300 different samples to cover a large number of possible combinations. Generating a binary sequence that is long enough for the

TABLE 2. NIST test results for different temperature points. The reported frequency values are for the external signal RO and the free-running RO while both are disconnected from each other (*i.e.* No SHIL effects).

Temp. (°C)	$f_{ext.}$ (GHz)	$f_{osc.}$ (GHz)	$f_{osc} - f_{ext}/2$ (MHz)	NIST
-50	15.45	8.05	322	PASS
-30	15.88	8.18	237	PASS
-10	16.26	8.28	151	PASS
10	16.61	8.38	78	PASS
30	16.92	8.44	–20	PASS
50	17.19	8.48	–117	PASS
70	17.48	8.52	–220	PASS
90	17.69	8.55	–295	PASS
110	17.93	8.57	–398	PASS

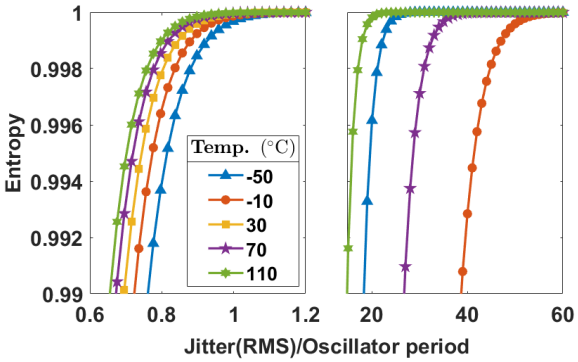


FIGURE 11. Shannon entropy estimation at different operating temperatures as a function of the switch RMS jitter normalized to the external signal Oscillator period at nominal temperature for the proposed design (left), and the existing design (right).

NIST test in each of the 300 samples requires a very long simulation time. Therefore, based on the temperature variation results listed in Table 2, the proposed design is assumed to generate the desired randomness as long as SHIL is correctly maintained in the circuit corresponding to each sample point. The basis for this assumption is that as long as SHIL takes place, the circuit entropy will follow the entropy curves similar to those shown in Fig. 11. The distribution of the value $(f_{osc} - f_{ext}/2)$, representing the mismatch between the free-running RO natural frequency and the sub-harmonic of the external signal RO frequency $(f_{ext}/2)$, over the Monte Carlo sample points is plotted in Fig. 12. SHIL is maintained across all of the sample points, which means that the mismatches in frequency are within the range of second-order SHIL, and the operation of the circuit is not affected. The highest mismatch in frequency due to the process and mismatch variations is smaller than ± 300MHz, and from Table 2, this range of mismatch successfully passed the NIST test.

The changes in the frequency values with varying supply voltage levels result in a larger frequency mismatch that can push the circuit outside the SHIL locking range. To counter this problem, tunable inverter cells are used in the design of the sync inverters. The tunable circuit used in the proposed design is shown in Fig. 13, which is similar to the coarse tuning reported in [4]. The sync inverter controls the injection

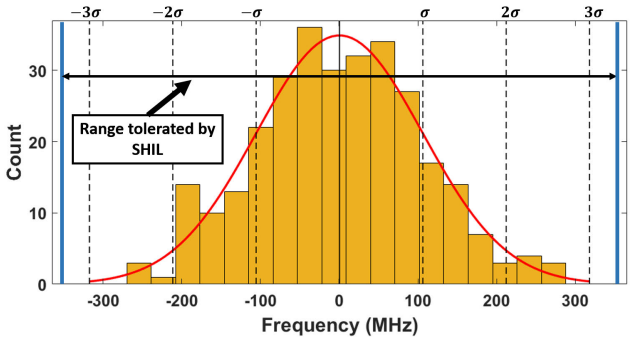


FIGURE 12. Distribution of the value ($f_{osc} - f_{ext}/2$) under process and mismatch variations. The circuit is designed to have a small frequency difference between the free-running RO and the locking frequency ($f_{ext}/2$), but due to the process and mismatch variations this difference changes. Frequencies are calculated by simulating both ROs disconnected while reproducing loading effects. The range tolerated by SHIL from temperature variation results is marked by a double headed arrow.

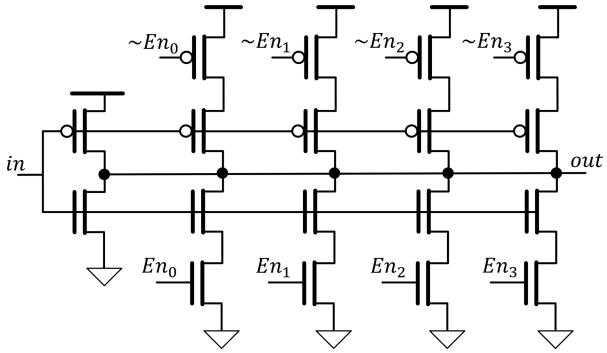


FIGURE 13. Tunable sync inverter cell design.

TABLE 3. Control signals to tune the locking range according to supply voltage.

Supply Volt.	Control signal ($En_{0:3}$)	SHIL
1V	1111	✓
0.9V	0111	✓
0.8V	0011	✓
0.7V	0001	✓
0.65V	0000	✓

strength of the SHIL while also affecting the loading of the external signal RO. By using a logic control circuitry to disable and enable the tunable gates, the locking range can be shifted. Under this tuning scheme, injection locking is successfully maintained over a power supply range from 0.65V to 1V, as shown in Table 3. However, a lower supply voltage makes the SHIL transition slower and may significantly decrease the external signal RO frequency, requiring a longer period and a larger RMS jitter for the switch, respectively.

A comparison with the state-of-the-art TRNG designs is presented in Table 4. It should be noted that the performance results in the table are for different technology nodes and operating points. The table demonstrates that the performance of our design is comparable to that of recent designs, while requiring lower energy consumption. Temperature and process variations are also tolerated without any additional tuning circuitry as compared to other variation-tolerant designs.

TABLE 4. Comparison with similar work.

Ref.	Bit rate	Temp. (°C)	Volt. (V)	Energy (pJ/bit)	Tech. (nm)
[4]	2.4Gbps	50	0.28 to 1.35	2.9	45
[20]	162.5Mbps	25	0.3 to 0.95	3	14
[10]	2Mbps	-40 to 120	0.6 to 0.9	23	40
[21]	1.48Gbps	25 to 110	0.55 to 0.75	2.5	14
[22]	23Mbps	25	0.9	23	28
This work	700Mbps	-50 to 110	0.65 to 1	1.16	28

VI. CONCLUSION

SHIL is a promising technique that can be used to generate truly random numbers owing to its metastability. A novel TRNG circuit design using second-order SHIL is proposed in this paper. Compared to existing work using the same phenomenon, the proposed design significantly improves the jitter requirement and tolerance for PVT variations. In this work, the proposed TRNG demonstrates a high tolerance for temperature variations across a range from −50°C to 110°C owing to the flexible locking range of SHIL. Process and mismatch variation tolerance across 300 Monte Carlo sample points are achieved without tuning. The lack of tuning requirements for temperature, process, and mismatch variations reduces the circuit complexity compared to state-of-the-art designs. Robustness against voltage supply variations within a range from 0.65V to 1V can be attained using tunable inverters. A tentative throughput of 700MHz was realized with an energy consumption of 1.16pJ/bit measured at a temperature of 25°C and supply voltage of 1V.

REFERENCES

[1] 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.

[2] V. von Kaenel and T. Takayanagi, "Dual true random number generators for cryptographic applications embedded on a 200 million device dual CPU SoC," in *Proc. IEEE Custom Integr. Circuits Conf.*, Sep. 2007, pp. 269–272.

[3] D. J. Kinniment and E. G. Chester, "Design of an on-chip random number generator using metastability," in *Proc. Eur. Solid-State Circuits Conf.*, Sep. 2002, pp. 595–598.

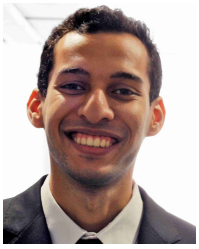
[4] S. K. Mathew, S. Srinivasan, M. A. Anders, H. Kaul, S. K. Hsu, F. Sheikh, A. Agarwal, S. Satpathy, and R. K. Krishnamurthy, "2.4 Gbps, 7 mW all-digital PVT-variation tolerant true random number generator for 45 nm CMOS high-performance microprocessors," *IEEE J. Solid-State Circuits*, vol. 47, no. 11, pp. 2807–2821, Nov. 2012.

[5] C. Liu and J. McNeill, "A digital-PLL-based true random number generator," *Res. Microelectron. Electron.*, vol. 1, pp. 113–116, Jul. 2005.

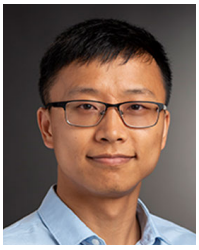
[6] C. S. Petrie and J. A. Connelly, "Modeling and simulation of oscillator-based random number generators," in *Proc. IEEE ISCAS*, vol. 4, May 1996, pp. 324–327.

[7] V. Fischer and M. Drutarovský, "True random number generator embedded in reconfigurable hardware," in *Cryptographic Hardware and Embedded Systems—(CHES)*. Berlin, Germany: Springer, 2002, pp. 415–430.

[8] B. Colombier, N. Bochard, F. Bernard, and L. Bossuet, "Backtracking search for optimal parameters of a PLL-based true random number generator," in *Proc. Design, Autom. Test Eur. Conf. Exhib. (DATE)*, Mar. 2020, pp. 1–6.
[9] E. N. Allini, O. Petura, V. Fischer, and F. Bernard, "Optimization of the PLL configuration in a PLL-based TRNG design," in *Proc. Design, Autom. Test Eur. Conf. Exhib. (DATE)*, Mar. 2018, pp. 1265–1270.
[10] K. Yang, D. Blaauw, and D. Sylvester, "A robust –40 to 120°C all-digital true random number generator in 40nm CMOS," in *Proc. Symp. VLSI Circuits (VLSI Circuits)*, Jun. 2015, pp. C248–C249.
[11] B. Yang, V. Rožic, N. Mentens, W. Dehaene, and I. Verbauwhede, "TOTAL: TRNG on-the-fly testing for attack detection using lightweight hardware," in *Proc. Design, Autom. Test Eur. Conf. Exhib. (DATE)*, 2016, pp. 127–132.
[12] M. T. Rahman, K. Xiao, D. Forte, X. Zhang, J. Shi, and M. Tehranipoor, "TI-TRNG: Technology independent true random number generator," in *Proc. 51st Annu. Design Autom. Conf. Design Autom. Conf. (DAC)*, Jun. 2014, pp. 1–6.
[13] A. Khanna, E. Elmitwalli, S. Dutta, S. Deng, S. Datta, S. Kose, and K. Ni, "A bias and correlation free true random number generator based on quantized oscillator phase under sub-harmonic injection locking," in *Proc. IEEE Symp. VLSI Technol.*, Jun. 2020, pp. 1–2.
[14] R. Adler, "A study of locking phenomena in oscillators," *Proc. IEEE*, vol. 61, no. 10, pp. 1380–1385, Oct. 1973.
[15] H.-T. Ng, R. Farjad-Rad, M. E. Lee, W. J. Dally, T. Greer, J. Poulton, J. H. Edmondson, R. Rathi, and R. Senthinathan, "A second-order semidigital clock recovery circuit based on injection locking," *IEEE J. Solid-State Circuits*, vol. 38, no. 12, pp. 2101–2110, Dec. 2003.
[16] P. Bhansali and J. Roychowdhury, "Gen-Adler: The generalized Adler's equation for injection locking analysis in oscillators," in *Proc. Asia South Pacific Design Autom. Conf.*, Jan. 2009, pp. 522–527.
[17] A. Neogy and J. Roychowdhury, "Analysis and design of sub-harmonically injection locked oscillators," in *Proc. Design, Autom. Test Eur. Conf. Exhib. (DATE)*, Mar. 2012, pp. 1209–1214.
[18] V. Fischer and D. Lubicz, "Embedded evaluation of randomness in oscillator based elementary TRNG," in *Cryptographic Hardware and Embedded Systems—CHES*, L. Batina and M. Robshaw, Eds. Berlin, Germany: Springer, 2014, pp. 527–543.
[19] V. Fischer, F. Bernard, N. Bochard, and M. Varchola, "Enhancing security of ring oscillator-based trng implemented in FPGA," in *Proc. Int. Conf. Field Program. Log. Appl.*, 2008, pp. 245–250.
[20] S. K. Mathew, D. Johnston, S. Satpathy, V. Suresh, P. Newman, M. A. Anders, H. Kaul, A. Agarwal, S. K. Hsu, G. Chen, and R. K. Krishnamurthy, "μ RNG: 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.
[21] S. K. Satpathy, S. K. Mathew, R. Kumar, V. Suresh, M. A. Anders, H. Kaul, A. Agarwal, S. Hsu, R. K. Krishnamurthy, and V. De, "An all-digital unified physically unclonable function and true random number generator featuring self-calibrating hierarchical Von Neumann extraction in 14-nm tri-gate CMOS," *J. Solid-State Circuits*, vol. 54, no. 4, pp. 1074–1085, Apr. 2019.
[22] K. Yang, D. Fick, M. B. Henry, Y. Lee, D. Blaauw, and D. Sylvester, "16.3 A 23Mb/s 23pJ/b fully synthesized true-random-number generator in 28nm and 65nm CMOS," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2014, pp. 280–281.



ESLAM ELMITWALLI (Graduate Student Member, IEEE) received the B.S. degree in nanotechnology and nanoelectronics engineering from the Zewail City of Science and Technology, 6th of October city, Giza, Egypt, in 2018. He is currently pursuing the Ph.D. degree in electrical and computer engineering with the University of Rochester, Rochester, NY, USA. His current research interests in hardware security include physical unclonable functions and true random number generators.



KAI NI (Member, IEEE) received the B.S. degree in electrical engineering from the University of Science and Technology of China, Hefei, China, in 2011, and the Ph.D. degree in electrical engineering from Vanderbilt University, Nashville, TN, USA, in 2016, by working on characterization, modeling, and reliability of III-V MOSFETs. Since then, he became a Postdoctoral Associate with the University of Notre Dame, working on ferroelectric devices for nonvolatile memory and novel computing paradigms. He is currently an Assistant Professor in electrical and microelectronic engineering with the Rochester Institute of Technology. He has 80 publications in top journals and conference proceedings, including *Nature Electronics*, IEDM, VLSI Symposium, IRPS, and EDL. His current interests include nanoelectronic devices empowering unconventional computing, AI accelerator, and 3D memory technology.

SELÇUK KÖSE (Member, IEEE) received the B.S. degree in electrical and electronics engineering from Bilkent University, Ankara, Turkey, in 2006, and the M.S. and Ph.D. degrees in electrical engineering from the University of Rochester, Rochester, NY, USA, in 2008 and 2012, respectively.

He was with TUBITAK, Ankara, Intel Corporation, Santa Clara, CA, USA, and Freescale Semiconductor, Tempe, AZ, USA. He is currently an Associate Professor with the Department of Electrical Engineering, University of Rochester. Prior to joining University of Rochester, he was an Associate Professor with the University of South Florida, Tampa, FL, USA. His current research interests include integrated voltage regulation, 3-D integration, hardware security, and green computing.

Dr. Kose was a recipient of the NSF CAREER Award, the Cisco Research Award, the USF College of Engineering Outstanding Junior Researcher Award, and the USF Outstanding Faculty Award. He is an Associate Editor of the *Nature Computer Science* (Springer) and *Microelectronics Journal* (Elsevier). He has served on the Technical Program and Organization Committees of various conferences.