A Chaotic Ring Oscillator based Random Number Generator

Siva Nishok Dhanuskodi, Arunkumar Vijayakumar, Sandip Kundu
Department of Electrical and Computer Engineering
University of Massachusetts, Amherst, USA
Email: {sdhanusk, avijayakumar, kundu}@ecs.umass.edu

***Abstract*—True Random Number Generator (TRNG) circuits play an important role in hardware security. Traditional Ring Oscillator (RO) based TRNGs aim to amplify thermal noise and supply noise jitters. To increase randomness, traditional RO based TRNGs harvest random noise from large number of stages resulting in large area and power. We propose a Chaotic Ring oscillator based random number Generator (CRNG) for CMOS implementation. This circuit uses nonlinear elements which are straightforward to implement in CMOS to bring about chaotic behavior. We demonstrate that the proposed CRNG passes tests for randomness and are immune to modeling attacks. Albeit small in magnitude, the proposed CRNG also harvests physical noise which acts as a compounder over chaos. The proposed CRNG circuit is small in area, scales well with technology, operates at low voltages and does not require any special manufacturing process. The output bit stream of the proposed CRNG implemented in a 45nm process was tested using the NIST test suite and it passes 11 tests. Results show that the proposed CRNG occupies an area of $93.1\mu m^2$ and has a throughput of 127 Mbps at a power of 1.1 mW. This compares very well against state of the art TRNGs.**

I. Introduction

Hardware security has become one of the main challenges as applications of Integrated Circuits have become widespread. Random number generators are widely used in such security applications. Pseudo Random Number Generators (PRNGs) are based on deterministic algorithms but TRNGs rely on a physical source of randomness to generate random numbers. The output bit stream of a TRNG is unpredictable, statistically independent and follows a uniform distribution. TRNGs play an important role in cryptographic algorithms to ensure secure exchange of information. Other applications of TRNGs include statistics, simulations, communication, seeding PRNGs, and VLSI testing.

A TRNG has three basic components: an entropy source, an entropy harvesting mechanism and a post-processing mechanism. Various entropy sources have been described in literature such as thermal noise [1], chaos [2] and unpredictable events in a system such as DRAM access latencies [3]. Physical sources of randomness such as thermal noise is unpredictable. In theory, chaos can be modeled, but in practice strong dependence on initial conditions and system parameters make it extremely hard to predict chaos. The second component in a TRNG, entropy harvesting, is a means by which the aforementioned entropy sources can be tapped into. This is a critical component which decides the quality of a TRNG. Several entropy harvesting mechanisms have been described in the literature. In one scheme, thermal noise is amplified using a noise amplifier which is fed to a Voltage Controlled Oscillator, which then is used to sample a high speed oscillator to produce a random bit stream [1]. In another scheme, a pair of cross-coupled identical inverters is forced into metastability by precharging both nodes to the same voltage, and then thermal noise is used to resolve the metastability thus producing a random bit [4]. Yet another entropy harvesting mechanism involves sampling phase jitter in oscillators: a high jitter low frequency signal is used to sample a high frequency signal to produce a random bit stream in [5]. A TRNG's quality is assessed in terms of its unbiased nature and its resilience to process variations and security attacks. The random bit stream obtained using a harvesting mechanism may be subjected to post-processing to improve quality. Some examples of post-processing are XOR [6], von-Neumann correction, cryptographic hash compression and linear code based compression [7]. In the case of XOR, two or more random bit streams are XORed to remove any correlation. In von-Neumann correction, an output is not produced when a pair of identical bits is seen. After post-processing the random bit stream, tests such as NIST [8] and Diehard [9] are used to assess the statistical properties of the bit stream.

We propose to use two oscillators that are coupled by non-linear elements for chaotic random number generation. Chaotic systems are deterministic systems if and only if the initial condition and circuit parameters are known. However, for all practical purposes the proposed CRNG output is fully random, because *(i)* it cannot be modeled by a linear system of any order, *(ii)* initial condition is internal to the circuit and is unknown, *(iii)* in presence of variations, the circuit parameters are also unknown, and finally *(iv)* the proposed CRNG *also* harvests entropy from thermal noise, though the entropy is low due to smaller number of noise collection stages, the compounding effect from non-linear coupling is high. Further background on non-linear dynamics and chaos is provided in section II-A.

The main goals of this paper are the following:

- Build an embedded CRNG that scales well with technology and has no special manufacturing process requirements
- Produce random bit stream at a high throughput with low area
- Develop a simple methodology to design such CRNG circuit

TRNGs which use random phase jitter resulting from thermal

978-1-4799-4112-4/14/$31.00

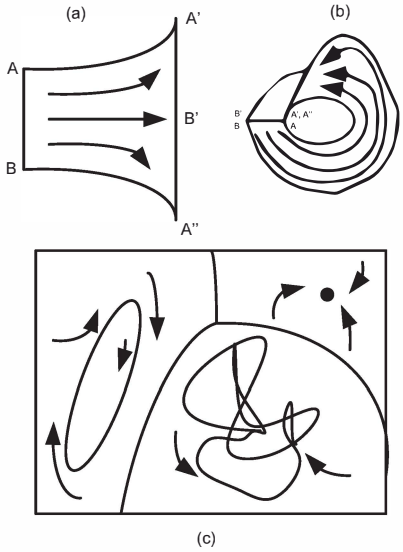


Fig. 1. Chaotic Systems:(a) Local expansion (b) Folding (c) Sensitivity to initial conditions [13]

noise in oscillator circuits have been explored in the literature [11], [5]. Generally, the output of a jittery oscillator is used to sample a high frequency oscillator to generate a random bit stream. Ring Oscillator (RO) based TRNG circuits become bulky when designed to amplify jitter. The circuit proposed in this paper also amplifies jitter but is area efficient, has a simple design and can be implemented in the regular CMOS process. It utilizes non-linear elements to generate chaotic behavior and thereby achieve the necessary jitter magnification. Previously, a ring oscillator-based chaotic circuit has been proposed in [2], [12], the limitations of which are discussed in this paper.

The paper is organized as follows. In section II, we describe the necessary background and the related work. The proposed CRNG design is described in section III. Section IV includes the design methodology and the results obtained. In section V, we present concluding remarks and future work.

II. Background and Related Work

A. Non-linear Dynamics and Chaos

A system whose dynamics (equations of motion from present state to the next state) are non-linear exhibits unpredictable behavior in certain special cases. An orbit or trajectory is the path traced in the state space during the temporal evolution of the system. The orbit of a dynamical system can be of different shapes. Fig. 1 (c) shows orbits such as fixed points, limit cycles and chaotic orbits depending on the initial condition.

For a dynamical system to exhibit chaotic behavior, it must be sensitive to initial conditions, topologically mixing and its periodic orbits must be dense [14]. In a chaotic system, the orbits of two adjacent states separate at a rapid rate as in Fig. 1 (a). So a small external noise grows and leads to a totally different temporal behaviour for the same initial state. That is, there is local instability. Topological mixing has to do with global stability - two different orbits converge after some time shown in Fig. 1 (b). Density of periodic orbits means every point in the state space of the system is arbitrarily close to periodic orbits. All these three properties, make a dynamical system chaotic.

Several TRNGs which rely on chaotic behavior to produce a random output have been reported in the literature. In [15], ADCs are used to realize discrete time chaotic models (piece wise affine Markov 1-D maps) and produce a random bit stream. In [2], [12], two oscillators are non-linearly coupled using diodes. Chaotic behavior is seen when the amplitude and frequency of the oscillators are adjusted using resistors and capacitors. A Double-Scroll chaotic oscillator circuit using differential amplifiers with power and throughput adjustable is described in [16]. Random bits are generated by amplifying and sampling the chaotic signal generated by the oscillator. TRNGs are often difficult to integrate, bulky and consume a lot of power.

B. Ring Oscillator based TRNGs

Jitter in oscillator is a frequently exploited source of randomness. Due to simplicity of design and ease of integration, a number of Ring Oscillator (RO) based TRNGs have been reported in literature [5], [11], [17], [18]. Typically, jitter due to thermal noise is captured by sampling signal transition using a reference. In one implementation [5] a high jitter low frequency RO was used to sample a high frequency signal. Different configurations of the high jitter RO have been explored in literature as described below. The phase noise and jitter Voltage Controlled Oscillator has been exploited in [11], which proposes an array of RNGs. The frequency of an RNG's VCO is controlled by another RNG in the array leading to an increase in the jitter spread. Fibonacci and Galois Ring Oscillator configurations are detailed in [17]. Two oscillators of the same frequency are arbitrated to produce a random bit stream in [18]. Jitter improvement by XORing the signals from several high jitter low frequency ROs is demonstrated in [5]. If a single RO were to be used, increasing number of stages also yields similar result but leads to a bigger circuit. The motivation behind the configurations described above is to improve the amount of random jitter. However, the design complexity and/or area increases as a result.

C. Related Work

The main objective of this paper is to increase the amount of random jitter in RO circuits and use the same to generate a random bit-stream. [2] proposes a chaotic circuit in which two ROs are coupled non-linearly with two diode-connected transistors. Resistors and a capacitor are used to control the frequency and amplitude of the oscillators. The ring oscillators play a role of expansion (sensitivity to initial conditions) and the diode-connected transistors play a role of folding (topological mixing) [2]. A TRNG circuit implementation is shown in [12] with some modifications. A 35% jitter to period ratio and 3.2Mbps bit throughput is reported. However the circuit is not easily integrable. Furthermore, the diode-connected transistors' saturation current is less non-linear in smaller technologies than the $0.5\mu m$ process used in [2].

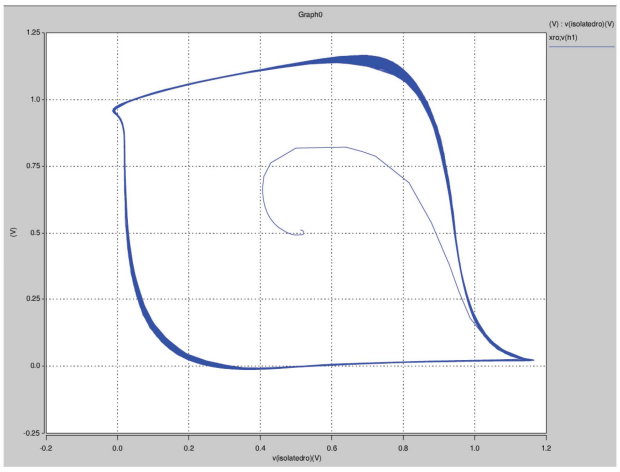


Fig. 2. Phase Portrait of a Ring Oscillator

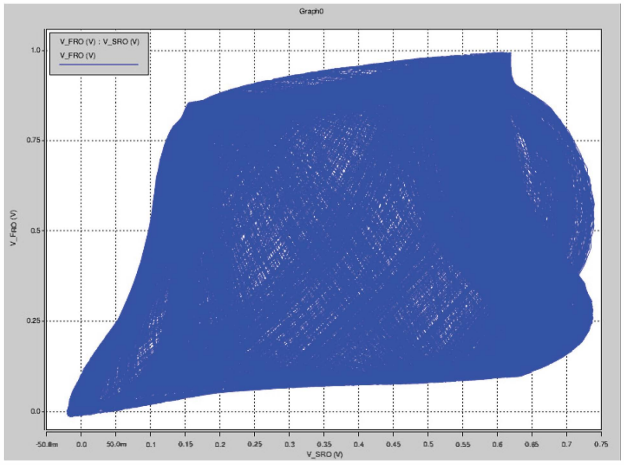


Fig. 3. Phase Portrait of the proposed CRNG

Another cross-coupled chaotic oscillator with an order of hundreds of Mbps throughput is reported in [19], [20]. The shortcoming is again is integrability. Jitter amplification of 8.4 through the use voltage programmable delay buffers is reported in [21]. However the ROs and buffers used result in large area.

III. Proposed Scheme

In this section, we describe our Chaotic Ring oscillator based random Number Generator (CRNG) circuit. The proposed CRNG circuit is an electronic analogue of a Double Pendulum [22] that exhibits chaotic behavior. A double pendulum consists of a pendulum with another attached to its end. The double pendulum described in [22] consists of two pendulums of different frequencies impacting each other's motion. Analogously in the electronic domain, two oscillators of different frequencies impacting each other can lead to chaos. Ring Oscillators (ROs) are easy to implement in CMOS. There are many advantages of the proposed circuit:

- The oscillators in the proposed circuit feature a small number of stages that results in smaller area.
- Fewer number of stages also results in higher frequency of oscillation, hence higher throughput.
- The proposed CRNG scales well into future technologies. Process variation reduces randomness of TRNGs. Process variation is a concern for highly scaled technologies. Since the proposed CRNG relies primarily on chaos and secondarily on thermal noise, scaling is not a concern as demonstrated by the experimental results below.

The proposed CRNG circuit is shown in Fig. 4. It comprises two ROs: a Slow Ring Oscillator (SRO) and a Fast Ring Oscillator (FRO). The SRO has slower and more number of inverters than the FRO. In our experimental setup, SRO has 5 stages and FRO has 3. The difference in the number of inverter stages is used to bring about a large disparity in frequency between SRO and FRO. The amplitude of SRO is modulated by an NMOS (M_{NR}) whose gate is controlled by FRO. M_{NR} behaves as a non-linear resistor. Thus FRO has an impact on

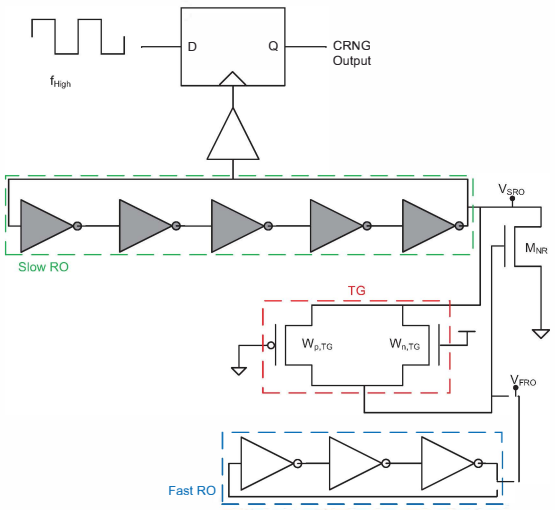


Fig. 4. The proposed CRNG circuit

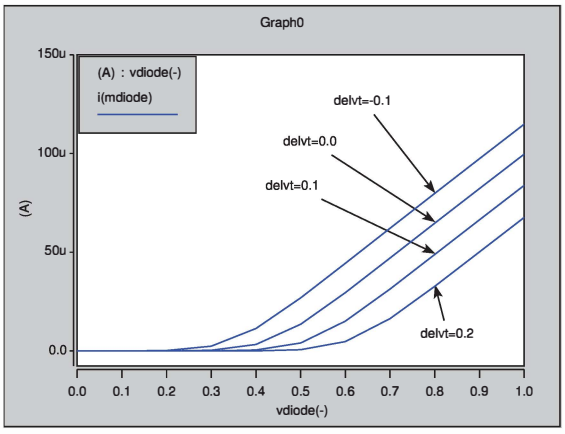


Fig. 5. Diode current variation with change in V_t

SRO. Furthermore, SRO and FRO are coupled by an always-on Transmission Gate (TG). So, both SRO and FRO impact each other. The circuit is analogous to a double pendulum in that the two ROs are attached via a Transmission Gate, and one RO modulates the load on the other.

A phase portrait is helpful to understand the temporal evolution of a system. Fig. 2 shows the phase portrait of a 3-stage Ring Oscillator circuit which does not exhibit a chaotic behavior. The portrait is obtained by plotting a nodal voltage against another nodal voltage of the Ring Oscillator. It is clear from the figure that both the voltage start at 0.5 V (half the supply voltage) and thereafter exhibit deterministic behavior. In contrast, CRNG's phase portrait is shown in Fig. 3. The portrait shows the chaotic behavior in the system, and is obtained by plotting V_{SRO} against V_{FRO} where the nodal voltages V_{SRO} and V_{FRO} are annotated in Fig. 4.

The chaotic behavior of the circuit in turn translates into jitter in the output waveform. The isolated FRO by itself has a jitter to period ratio of $(\frac{\sigma}{\mu})_{isolated,FRO} = \frac{3.85p}{2.74n} = 0.14\%$. FRO in the CRNG has a jitter to period ratio of $(\frac{\sigma}{\mu})_{CRNG,FRO} = \frac{1.94n}{3.88n} = 50\%$. Similarly for the SRO we obtain $(\frac{\sigma}{\mu})_{isolated,SRO} = 0.027\%$ and $(\frac{\sigma}{\mu})_{CRNG,SRO} = 1.9\%$. An improvement more than 70x in jitter to period ratio is seen, thanks to chaotic behaviour. The chaotic signal (V_{SRO}) in turn is used to sample a high frequency clock (f_{high}) to generate a random bit-stream as shown in Fig. 4. f_{high} can be generated from the system clock or a dedicated RO can be used.

The proposed circuit is also amenable to technology scaling. With scaling, the non-linearity is enhanced, which in turn helps improve chaos. To illustrate this, we compare the proposed circuit with the Diode Couple Chaotic RO-based Circuit (DCCC) described in [2]. The non-linearity of this circuit comes from the diode-connected transistors. As technology scales, the diode current becomes more linear as shown in Fig. 5. This is due to scaling down of threshold voltage V_t. As V_t gets close to 100mV, the diode's current is linear for more that 50% of the voltages (V_{diode}). Ideally, V_t should be half the supply voltage for the diode current to have highest non-linearity. The CRNG proposed in Fig. 4 relies on non-linear resistor M_{NR}. M_{NR} actually performs better at lower V_t due to the fact that even a small voltage V_{FRO} can impact SRO. Also, the circuit in [2] is not easy to implement in CMOS. Further experimental results are shown in Section IV.

IV. Methodology and Experimental Results

As mentioned in section I, chaos is dependent on proper parameter choice. Writing out differential equations and solving them for circuit parameters, such that chaotic behavior is exhibited, is feasible only when the circuit is simple enough. Here we present an approach in which we use the phase portrait to optimize the circuit sizes.

The phase portrait would represent chaotic behavior if for a given value of SRO voltage, there are several possible FRO voltage. These voltage pairs occur at various instances of time. So a metric that describes the "goodness" of a phase portrait is calculated as follows. SRO's voltages are binned and in each bin, the corresponding FRO voltages are added. In a given SRO

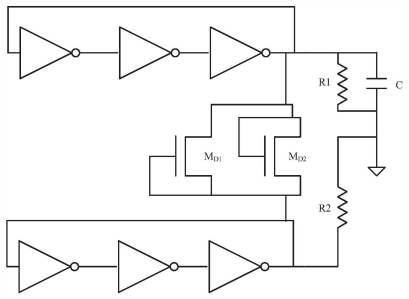


Fig. 6. Diode Coupled Chaotic Circuit (DCCC)

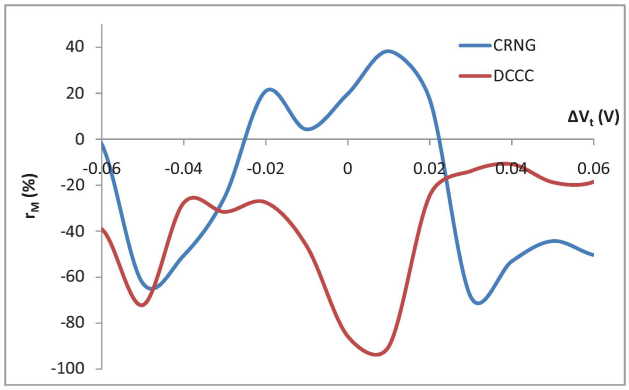


Fig. 7. Effect of technology scaling on CRNG and DCCC

bin 'i', R_i is the range of FRO voltages, F_i is the proportion of R_i that is "filled" and E_i is the proportion of R_i that is "empty". The "goodness" of SRO bin 'i' is computed as shown in equation 1. The final metric 'M' is the geometric mean of all the 'n' SRO bin metrics as shown in equation 2.

M is large when the phase portrait represents chaotic behaviour and is small in the case of period behavior. For example, the metrics of the phase portraits shown in Fig. 2 and Fig. 3 are 116 and 11929 respectively.

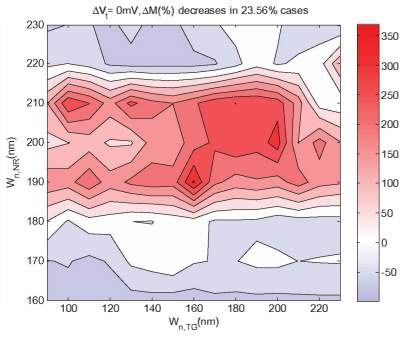
$$B_i = R_i \frac{F_i}{1 + E_i} \tag{1}$$

$$M = \left(\prod_{i=1}^{n} B_i \right)^{1/n} \tag{2}$$

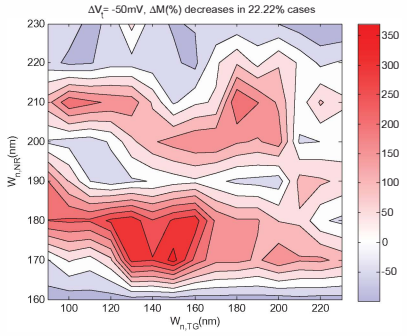
The transistors in CRNG are sized in such a way that the value of metric M is maximized. As an example a contour showing the dependence of M on TG size and width of M_{NR}

TABLE I. Circuit Parameters

Component	$W_p(\mu m)$	$L_p(\mu m)$	$W_n(\mu m)$	$L_n(\mu m)$
SRO inverter	7.875	0.506	0.900	0.506
FRO inverter	15.750	0.360	1.800	0.360
M_{NR}	-	-	0.200	0.045
CRNG1 TG	0.330	0.045	0.110	0.045
CRNG2 TG	0.450	0.045	0.150	0.045



(a) $\Delta V_t = 0mV$



(b) $\Delta V_t = -50mV$

Fig. 8. Change in $r_M(w.r.t.\Delta V_t = 50mV)$ at different ΔV_t

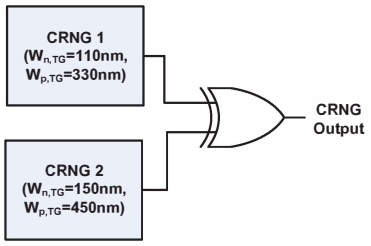


Fig. 9. Post-processing setup for CRNG output

is shown in Fig. 10. We narrow down on the parameters for which M is high and hence the circuit is chaotic. The optimized set of circuit parameters are listed in Table I.

The circuit was designed in 45nm (PTM model)technology node and Synopsys HSPICE was used for circuit simulation. The proposed circuit in Fig. 9 fits within an area of $94\mu m^2$ (45nm PTM model [23]) and consumes $1.1mW$ of power when a dedicated RO is used to generate $f_{high} = 15.8GHz(16.2GHz)$ for CRNG 1 (CRNG 2). 10 million bits each were generated from CRNG1 and CRNG2, and their statistical properties were tested using the NIST suite. Upon post-processing (XORing) the bitstreams from CRNG1 and CRNG2, the final bitstream passed NIST tests. The results are tabulated in Table II. We show only the worst case results in the event of multiple entries for the same test.

In Table III we present a comparison of the proposed CRNG with previous reports in the literature. It may be observed that the proposed CRNG provides a superior throughput at a lower area in comparison to most of the designs.

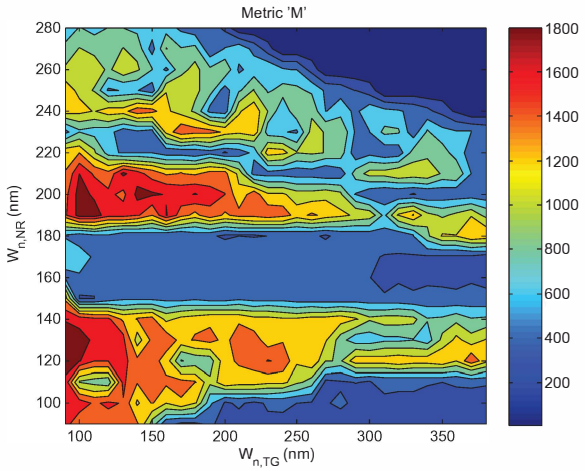


Fig. 10. Dependence of metric 'M' on transistor sizes

TABLE II. NIST TEST RESULTS

Statistical Test	P-value	Proportion
Frequency	0.739918	1
BlockFrequency	0.213309	1
CumulativeSums	0.350485	1
Runs	0.739918	1
LongestRun	0.739918	1
Rank	0.739918	1
FFT	0.739918	0.9
Universal	0.911413	1
ApproximateEntropy	0.534146	1
Serial	0.350485	1
LinearComplexity	0.739918	0.9

As described in section III, the circuit in [2] does not scale well with technology because of the diode coupling. A 45 nm implementation of this circuit shown in Fig. 6 is used for comparison purposes. The parameters used are as follows: inverter $(W_p = 15.75\mu m, L_p = .36\mu m, W_n = 1.8\mu m, L_n = .36\mu m)$, M_{D1} and M_{D2} $(W_n = 1.8\mu m, L_n = .045\mu m)$, $R_1 = R_2 = 10K\Omega$ and $C = 0.5pF$. Fig. 7 compares percentage change in metric 'M', $r_M(= \Delta M/M)$ of the CRNG and DCCC circuits' phase portraits as threshold variation (ΔV_t) is changed from 60mV to -60mV with the former as the reference. It is clear that DCCC does better initally but fairs badly at lower values of V_t. Further, Fig. 8a (Fig. 8b) shows how r_M changes as ΔV_t is changed from 50mV to 0mV (-50mV). The rate of change (r_M) is studied at various parameter values. It is seen that M decreases (blue shade in figure) in 23.56% (22.22%) of the cases for the parameter space shown. This decrease is accounted for by the parameters which were worse to begin with. Further, the maximum rate of increase (350%) r_M outweighs that of decrease (-50%) as can be seen from the scale of the plot.

V. CONCLUSION

Traditional TRNGs harvest thermal and supply noise. However, amplification of such noise requires a large number of stages in a ring oscillator with associated cost in area and

TABLE III. PERFORMANCE COMPARISON

Scheme	Area (μm^2)	Power P (mW)	Supply (V)	Bit-rate T (Mbps)	Tech. (nm)	T/P (Mbps/mW)
[24]	1024	2.26	1.1	4000	45	1769.9
[25]	5600	0.00055	1.25	0.32	130	581.8
CRNG	**93.1**	**1.0967**	**1**	**127**	**45**	**115.8**
[26]	20k	0.00091	1.3	0.1	350	109.8
[27]	-	0.003	3	0.2	350	66.6
[28]	50k	0.00104	0.8	0.04	180	38.4
[29]	1600	2.3	1.8, 3.3	10	180	4.3
[30]	520k	30	3.3	40	350	1.3

power. We propose a non-linearly coupled ring oscillator pair for generating chaotic signal. Apart from inherent chaos, such oscillators also harvest physical noise. This overcomes the need to use ring oscillators with large number of stages to amplify jitter. A random number generator which samples the chaotic oscillator's output to generate random bit-stream was presented. The proposed CRNG passes NIST test suite for randomness. It was also shown to be scalable with technology and CMOS friendly for implementation. The demonstration circuit was designed in a 45nm process. It occupies an area of $93.1\mu m^2$ and provides a throughput of 127 Mbps at a power of 1.1 mW. Simplicity of design, ease of integration in CMOS, lower area, higher throughput and proven randomness makes this an attractive alternative to traditional TRNG designs.

REFERENCES

[1] B. Jun and P. Kocher, "The intel random number generator," *Cryptography Research Inc. white paper*, Apr 1999. [Online]. Available: http://www.cryptography.com/public/pdf/IntelRNG.pdf

[2] Y. Hosokawa and Y. Nishio, "Simple chaotic circuit using cmos ring oscillators," *International Journal of Bifurcation and Chaos*, vol. 14, no. 07, pp. 2513–2524, 2004.

[3] C. Pyo, S. Pae, and G. Lee, "Dram as source of randomness," *Electronics Letters*, vol. 45, no. 1, pp. 26–27, 2009.

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

[5] B. Sunar, W. Martin, and D. Stinson, "A provably secure true random number generator with built-in tolerance to active attacks," *Computers, IEEE Transactions on*, vol. 56, no. 1, pp. 109–119, 2007.

[6] M. Dichtl, "Bad and good ways of post-processing biased physical random numbers," in *Fast Software Encryption*. Springer, 2007, pp. 137–152.

[7] S.-H. Kwok, Y.-L. Ee, G. Chew, K. Zheng, K. Khoo, and C.-H. Tan, "A comparison of post-processing techniques for biased random number generators," in *Information Security Theory and Practice. Security and Privacy of Mobile Devices in Wireless Communication*. Springer, 2011, pp. 175–190.

[8] A. Rukhin, J. Soto, J. Nechvatal, E. Barker, S. Leigh, M. Levenson, D. Banks, A. Heckert, J. Dray, S. Vo, A. Rukhin, J. Soto, M. Smid, S. Leigh, M. Vangel, A. Heckert, J. Dray, and L. E. B. Iii, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," 2001.

[9] G. Marsaglia, "Diehard test suite," 1998.

[10] G. Chen and T. Ueta, *Chaos in circuits and systems*. World Scientific Publishing Company, 2002, vol. 11.

[11] N. Stefanou and S. Sonkusale, "High speed array of oscillator-based truly binary random number generators," in *Circuits and Systems, 2004. ISCAS '04. Proceedings of the 2004 International Symposium on*, vol. 1, 2004, pp. I–505–8 Vol.1.

[12] I. Cicek and G. Dundar, "A hardware efficient chaotic ring oscillator based true random number generator," in *Electronics, Circuits and Systems (ICECS), 2011 18th IEEE International Conference on*, 2011, pp. 430–433.

[13] Non-linear dynamics and chaos. [Online]. Available: $http://www.advancedlab.org/mediawiki/index.php/Non-Linear\_Dynamics\_and\_Chaos$

[14] B. Hasselblatt and A. Katok, *A first course in dynamics: with a panorama of recent developments*. Cambridge University Press, 2003.

[15] S. Callegari, R. Rovatti, and G. Setti, "Embeddable adc-based true random number generator for cryptographic applications exploiting nonlinear signal processing and chaos," *Signal Processing, IEEE Transactions on*, vol. 53, no. 2, pp. 793–805, 2005.

[16] F. Cao and S. Li, "A double-scroll based true random number generator with power and throughput adjustable," in *ASIC, 2009. ASICON '09. IEEE 8th International Conference on*, 2009, pp. 309–312.

[17] J. Golic, "New methods for digital generation and postprocessing of random data," *Computers, IEEE Transactions on*, vol. 55, no. 10, pp. 1217–1229, 2006.

[18] J. Angulo, E. Kussener, H. Barthelemy, and B. Duval, "A new oscillator-based random number generator," in *New Circuits and Systems Conference (NEWCAS), 2012 IEEE 10th International*, 2012, pp. 21–24.

[19] S. Ozoguz, A. Elwakil, and S. Ergun, "Cross-coupled chaotic oscillators and application to random bit generation," *Circuits, Devices and Systems, IEE Proceedings -*, vol. 153, no. 5, pp. 506–510, 2006.

[20] S. Ergun, "Regional random number generator from a cross-coupled chaotic oscillator," in *Circuits and Systems (MWSCAS), 2011 IEEE 54th International Midwest Symposium on*, 2011, pp. 1–4.

[21] T. Amaki, M. Hashimoto, and T. Onoye, "Jitter amplifier for oscillator-based true random number generator," *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 96, no. 3, pp. 684–696, 2013.

[22] R. B. Levien and S. M. Tan, "Double pendulum: An experiment in chaos," *American Journal of Physics*, vol. 61, no. 11, pp. 1038–1044, 1993. [Online]. Available: http://link.aip.org/link/?AJP/61/1038/1

[23] Predictive technology model. [Online]. Available: $http://ptm.asu.edu/latest.html$

[24] S. Srinivasan, S. Mathew, V. Erraguntla, and R. Krishnamurthy, "A 4gbps 0.57pj/bit process-voltage-temperature variation tolerant all-digital true random number generator in 45nm cmos," in *VLSI Design, 2009. 22nd International Conference on*, 2009, pp. 301–306.

[25] G. Balachandran and R. Barnett, "A 440-na true random number generator for passive rfid tags," *Circuits and Systems I: Regular Papers, IEEE Transactions on*, vol. 55, no. 11, pp. 3723–3732, 2008.

[26] S. hua Zhou, W. Zhang, and N.-J. Wu, "An ultra-low power {CMOS} random number generator," *Solid-State Electronics*, vol. 52, no. 2, pp. 233 – 238, 2008. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S003811010700295X

[27] J. Angulo, E. Kussener, H. Barthelemy, and B. Duval, "A new oscillator-based random number generator," in *Faible Tension Faible Consommation (FTFC), 2012 IEEE*, 2012, pp. 1–4.

[28] W. Chen, W. Che, Z. Bi, J. Wang, N. Yan, X. Tan, J. Wang, H. Min, and J. Tan, "A 1.04 μw truly random number generator for gen2 rfid tag," in *Solid-State Circuits Conference, 2009. A-SSCC 2009. IEEE Asian*, 2009, pp. 117–120.

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

[30] F. Pareschi, G. Setti, and R. Rovatti, "A fast chaos-based true random number generator for cryptographic applications," in *Solid-State Circuits Conference, 2006. ESSCIRC 2006. Proceedings of the 32nd European*, 2006, pp. 130–133.