0.6–1.2 V, 0.22 pJ/bit True Random Number Generator Based on SAR ADC

Akshay Jayaraj, Nimish Nitin Gujarathi, Illakiya Venkatesh, and Arindam Sanyal

***Abstract*—This brief proposes a true-random number generator (TRNG) based on a successive approximation register (SAR) analog-to-digital converter (ADC). After the SAR ADC has finished conversion, the comparator is fired again to quantize the residue. The 1-bit quantized residue acts as a true random sequence and no additional circuits are required for the TRNG. A prototype fabricated in 65nm process acts as a TRNG over 0.6V-1.2V power supply and −5°C to 50°C temperature range without any calibration or post-processing. The TRNG outputs a random sequence at 1.25Mbps and consumes state-of-the-art energy of 0.22pJ/bit.**

***Index Terms*—True-random number generator, successive approximation register, analog-to-digital converter, entropy.**

I. Introduction

RANDOM numbers are an integral part of cryptography, secure communications and statistical operations, like monte-carlo simulations. Random number generators can be broadly classified into two groups- pseudo random number generator (PRNG) and true random number generator (TRNG). A widely used PRNG is a linear feedback shift register which generates pseudo-random patterns based on the seed. While PRNG can be designed to make its output appear random to an adversary, it is vulnerable to attacks, particularly on Internet-of-Things (IoT) devices with limited resources (such as, number of external seed input). In contrast, a TRNG derives randomness from physical sources, such as thermal noise, and does not require external seed. Thus, TRNGs are more suitable for use with IoT devices.

As mentioned above, the most common source of randomness or entropy for silicon TRNG is thermal noise. Random fluctuations of current in a conductor, such as resistor or MOS transistor, due to brownian motion of charge carriers give rise to the well known Johnson noise or thermal noise. As such, an intuitive technique is to amplify thermal noise of a resistor and digitize it to generate a true random sequence [1]. However, high bandwidth amplifier is not energy efficient to design in advanced CMOS technologies that are generally used for low power IoT devices. Latch metastability is another widely used source of entropy for on-chip TRNG [2]–[4]. A common implementation of metastable latch is a cross-coupled inverter which transitions between two stable states (‘0’ and ‘1’) depending on thermal noise. While metastable latches provide a simple and fast TRNG, they are very sensitive to PVT variations which leads to bias in the latch output and loss of randomness. Hence, TRNGs using metastability as entropy source requires background calibration. Ring oscillators are yet another popular choice for TRNG. Ring oscillators use entropy from phase noise to provide high randomness but are sensitive to PVT variations. This has led to edge-chasing TRNGs which can decouple oscillator bias from PVT variations [5], [6]. In edge-chasing TRNGs, edges are inserted at different points in the oscillator which leads to collapse of oscillation. The time between injection of the edges and collapse of oscillation is digitized and the least significant bits (LSBs) of the digitized time acts as TRNG. The mean and standard deviation of the time to oscillation collapse are used as monitors for background calibration for robustness against PVT variations [7]. In contrast to TRNGs that derive randomness from an entropy source, chaotic-map based TRNGs derive randomness from initial condition of a system and its dynamic properties. While chaotic systems usually have large power consumption in mWs, a recent sub-ranging SAR ADC based chaotic TRNG is proposed in [8] that consumes low power. However, an additional feedback loop around the first-stage coarse ADC is required for creating the chaotic map in [8].

In this brief, we propose a TRNG which is based on a successive approximation register (SAR) analog-to-digital converter (ADC) without requiring any additional hardware. We show that once SAR ADC has finished quantization, its residue when quantized using a 1-bit quantizer, acts as a true random sequence. There are no restrictions placed on the normal SAR operation, and thus, the proposed architecture acts as both an ADC and a TRNG. A prototype 10-b SAR ADC fabricated in 65nm CMOS process shows that the quantized residue acts as TRNG over a wide power supply range of 0.6V-1.2V, temperature range of −5°C to 50°C and consumes only 0.22pJ/bit without any calibration or post-processing. The ADC has an ENOB of 8.6 bits and walden FoM of 7.8fJ/step. The rest of this brief is organized as follows: the architecture of the SAR-based TRNG is discussed in Section II, measurement results are presented in Section III and the conclusion is brought up in Section IV.

Manuscript received June 13, 2019; revised August 28, 2019 and October 9, 2019; accepted October 10, 2019. Date of publication October 28, 2019; date of current version October 5, 2020. This brief was recommended by Associate Editor I.-C. Park. *(Corresponding author: Akshay Jayaraj.)*

The authors are with the Electrical Engineering Department, University at Buffalo, Buffalo, NY 14260 USA (e-mail: akshayja@buffalo.edu; arindams@buffalo.edu).

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCSII.2019.2949775

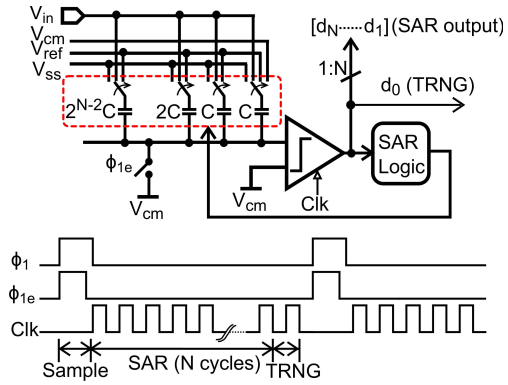


Fig. 1. Proposed TRNG with timing diagram.

II. Proposed Architecture

Once a SAR ADC has finished quantization, the residue V_{res} is present at the inputs to the comparator, and can be written as $V_{res} = \epsilon_1 + n_{th}$, where ϵ_1 is quantization noise of the ADC and n_{th} is thermal noise from comparator and digital-to-analog converter (DAC). The SAR residue acts as an entropy source for random number generation under conditions which will be discussed later in this Section. If the SAR residue is quantized to 1-bit, the quantized bitstream behaves as a TRNG. In the proposed architecture, we quantize SAR residue by firing the comparator again after SAR conversion. Since the same comparator is used for SAR conversion and TRNG generation, comparator offset does not add any bias to the TRNG and, hence, does not affect entropy of the proposed TRNG. This is a key advantage of the proposed TRNG in that comparator offset calibration is not required to remove bias in the random sequence. The 1-bit quantized version of V_{res} can be written as $d_0 = Q(V_{res}) = \epsilon_1 + n_{th} + \epsilon_2$, where $Q(\cdot)$ denotes 1-bit quantization operation and ϵ_2 denotes TRNG quantization noise due to $Q(\cdot)$.

Fig. 1 shows schematic of the proposed TRNG architecture with timing diagram. A single-ended schematic of the SAR ADC is shown for the sake of simplicity. Bottom-plate sampling technique is used to improve SAR linearity. Bi-directional single-sided switching (BDSS) scheme [9], [10] is used in the SAR ADC to reduce switching energy. In traditional BDSS technique, the SAR residue is not zero mean since the LSB decision (d_1) is not fed to the capacitive DAC. Thus, traditional BDSS technique cannot be directly used for TRNG. In the proposed architecture, the LSB decision is fed to the capacitive DAC in the last cycle of the SAR conversion to make the residue zero-mean. After SAR conversion is completed, the comparator is fired 1 more time, and the comparator output d_0 acts as TRNG sequence.

For the SAR residue to act as entropy source for random number generation, SAR quantization noise, ϵ_1, should have a white power spectral density (PSD), and hence, ϵ_1 should have very low correlation with input signal. Use of a low power comparator, such that its thermal noise is greater than ADC quantization noise, further whitens PSD of V_{res} at the cost of effective-number-of-bits (ENOB). 1-bit quantized version of a random sequence is also random, and thus, if V_{res} has a white PSD, d_0 will also have a white PSD. Supply variations induced by switching in the SAR DAC can degrade randomness of the TRNG by making the residue correlated with input signal. However, the BDSS technique adopted in this design results in very low correlation between switching energy and input signal [10]. In addition, the low-bandwidth comparator low-pass filters supply noise. Thus, switching induced supply noise has little effect on randomness of the proposed TRNG.

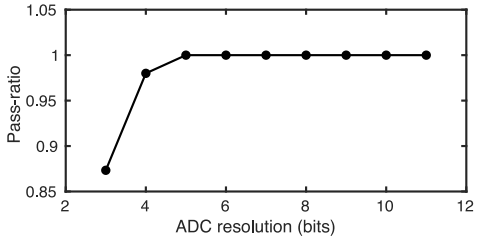


Fig. 2. Simulated DFT pass ratios vs ADC resolution.

Low correlation between ϵ_1 and input signal is achieved if the ADC resolution is high. To determine the ADC resolution required for random sequence generation, we varied ADC resolution and applied DFT test to determine randomness of d_0. DFT test is one the 15 tests in the NIST statistical randomness suite [11] and detects periodic features in a sequence that would indicate non-white PSD and deviation from randomness. While passing DFT test is a necessary condition for statistical randomness, it is not a sufficient condition and a sequence has to pass the entire NIST test suite to be considered statistically random. We applied a sinusoid input at -2dBFs and frequency of $f_s/349$ (f_s is the sampling frequency) to a SAR ADC whose resolution is varied from 3 to 11 bits. Standard deviation of thermal noise is kept at 0.6LSB and the simulation is repeated 150 times for each ADC resolution. Fig. 2 shows the pass ratios for DFT test versus ADC resolution. For ADC resolution exceeding 6 bits, the pass ratio for DFT tests is 1, i.e., the TRNG passes all 150 DFT tests, which indicates a high confidence of randomness. A 10-bit SAR ADC is chosen for this brief based on the DFT test results shown in Fig. 2. It should be pointed out here that an on-chip sinusoidal input generator is not required for the proposed TRNG; rather the TRNG works with analog input seen by the ADC during its normal operation.

While high resolution of ADC ensures good de-correlation between quantization noise and input signal, correlation between input and quantization noise is also related to the input amplitude. Fig. 3(a) shows the pass ratios for 150 DFT tests for different thermal noise standard deviations as input amplitude is varied. A sinusoidal input at frequency of $f_s/349$ is used for the simulations. Fig. 3(a) shows that at low input amplitude and for small thermal noise, sar residue is not random. Once thermal noise exceeds 0.7LSB, sar residue is sufficiently de-correlated with input signal and pass ratio for DFT tests is 1 over the entire span of input amplitudes. The simulation result raises the question can a low noise comparator be used for SAR conversions to have good ENOB ADC and a high-noise comparator be used only for the TRNG generation from SAR residue? Fig. 3(b) shows DFT test results for fixed thermal noise of 0.5LSB for SAR phase and varying thermal noise only for TRNG phase. It can be seen from Fig. 3(b) that a high-noise comparator with noise standard deviation exceeding

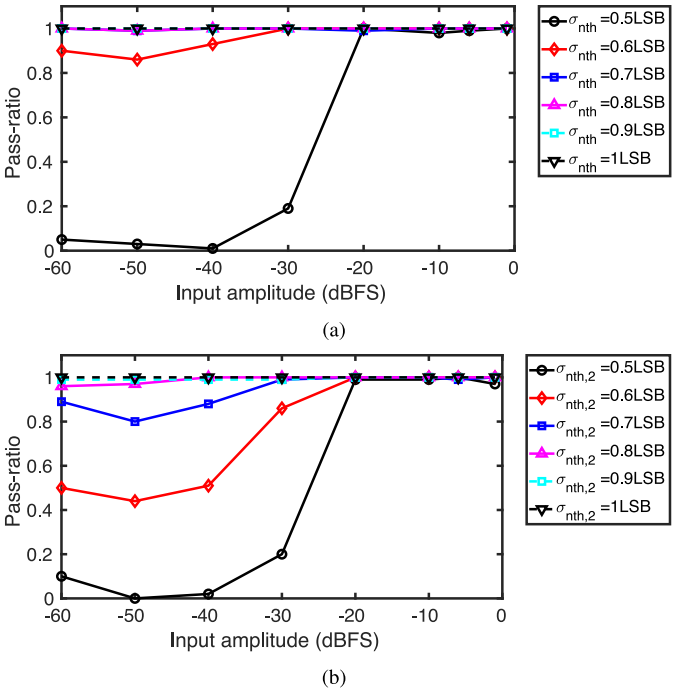


Fig. 3. Simulated DFT pass ratios vs input amplitude for (a) same thermal noise for both SAR and TRNG phases (b) fixed thermal noise of 0.5LSB for SAR phase and varying thermal noise for TRNG phase.

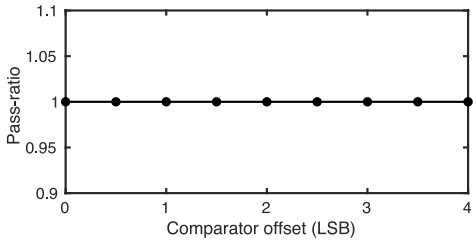


Fig. 4. Simulated DFT pass ratios vs comparator offset.

0.9LSB can be used for TRNG phase and a low-noise comparator can be used for SAR phase to realize both high ENOB ADC and TRNG. However, using different comparators for SAR and TRNG phases results in offset mismatch between the two comparators and adds bias to the TRNG sequence. Hence, offset calibration is required if two comparators are used. For the proposed TRNG, we have used same comparator for both SAR and TRNG to avoid comparator offset calibration.

Fig. 4 shows the effect of comparator offset on randomness of the proposed TRNG. A sinusoid input at −2dBFs and frequency of $f_s/349$ is applied to 10-bit SAR ADC. 0.6LSB thermal noise is used for the simulations and the comparator offset is varied from 0 to 4LSB. Pass ratios for 150 DFT tests for each comparator offset value is shown in Fig. 4. It can be seen that comparator offset does not affect the pass ratio which remains at 1. Thus, comparator offset calibration is not required for the proposed TRNG architecture.

Mismatch in the capacitive DAC can lower randomness of the proposed TRNG. Fig. 5 shows pass ratios for DFT tests as unit capacitor mismatch is varied from 0% to 15% for 10-bit SAR ADC. A sinusoid input at −2dBFs and frequency of $f_s/349$ is applied to the SAR ADC. 0.6LSB thermal noise is

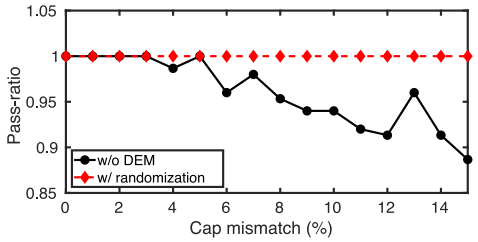


Fig. 5. Simulated DFT pass ratios vs capacitor mismatch.

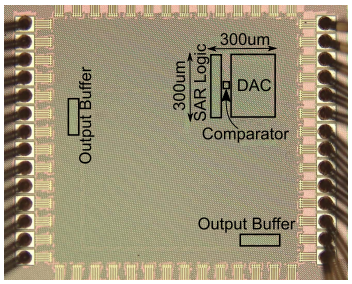


Fig. 6. Die microphotograph.

used for the simulations. Without dynamic element matching (DEM), pass ratio for DFT test is 1 for capacitor mismatch upto 3% and the pass ratio drops once mismatch exceeds 3%. If the element selection pattern in the DAC is randomized, pass ratio of DFT test remains at 1 even for capacitance mismatch as high as 15%. Instead of randomizing element selection pattern which requires complicated routing to each unit capacitance and reduces SNR, we have sized the unit capacitance to limit mismatch. Based on foundry mismatch data, a 4.8fF unit metal-on-metal (MOM) capacitor is used for the capacitive DAC to ensure unit capacitance mismatch of 0.5%. The kT/C sampling noise is 10x smaller than comparator thermal noise. While simulation results based on DFT tests have been used in TRNG design phase to get intuitive insights, we show measurement results on test chips in Section III that confirm that the proposed TRNG passes all NIST randomness tests and is indeed truly random.

III. Measurement Results

A prototype TRNG was fabricated in 65nm process and the die microphotograph is shown in Fig. 6. The ADC+TRNG combination occupies an area of 0.09mm^2. The TRNG produces random bits at the rate of 1.25Mbps and consumes 0.27μW from 0.8V power supply. The quality of our TRNG is tested using the NIST statistical suite [11]. 3 test chips were evaluated using NIST randomness tests and each test was repeated 18 times for the 3 test chips. Table I shows measured p-values and pass ratios for the 15 NIST randomness statistical tests for the 3 test chips at room temperature and 0.8V power supply. A sinusoidal input at 50kHz frequency and amplitude of −6dBFS was used for the measurements. A TRNG is considered statistically random with a confidence of 0.99 if the p-values for all 15 tests exceed 0.01. All 3 test chips passed the NIST randomness tests.

Fig. 7 shows the measured p-values for test chip1 across power supply voltage from 0.6V-1.2V. The measured p-values

TABLE I
NIST TEST RESULT

	chip1		chip2		chip3	
Test Name	p-val	pratio	p-val	pratio	p-val	pratio
Frequency monobit	0.48	18/18	0.53	18/18	0.44	18/18
Block frequency	0.84	18/18	0.68	18/18	0.7	18/18
Runs test	0.52	18/18	0.47	18/18	0.46	18/18
Longest run of ones	0.49	18/18	0.36	18/18	0.45	18/18
Binary matrix rank	0.39	18/18	0.47	17/18	0.47	18/18
DFT	0.59	18/18	0.61	18/18	0.63	18/18
Non-overlapping	0.14	18/18	0.71	18/18	0.7	18/18
Overlap matching	0.42	18/18	0.14	18/18	0.14	18/18
Maurers universal	0.79	18/18	0.52	18/18	0.47	18/18
Linear complexity	0.39	18/18	0.48	18/18	56	18/18
Serial test	0.78	18/18	0.91	18/18	0.87	18/18
Approximate entropy	0.53	18/18	0.26	18/18	0.54	18/18
Cumulative sums	0.35	18/18	0.39	18/18	0.43	18/18
Random excursions	0.35	18/18	0.33	18/18	0.43	17/18
Random exc. variant	0.52	18/18	0.56	18/18	0.42	18/18

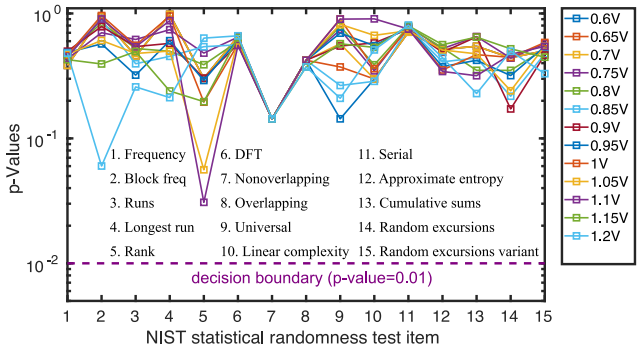


Fig. 7. Measured p-values versus power supply.

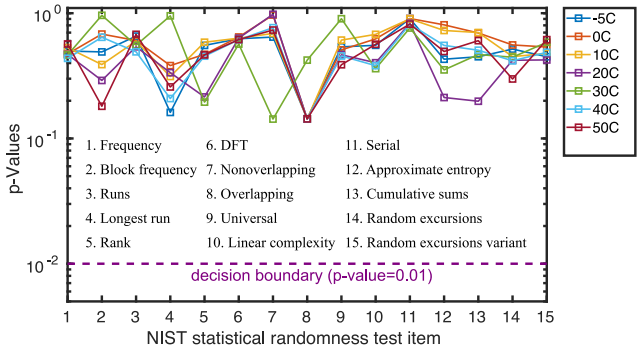


Fig. 8. Measured p-values versus temperature.

are greater than 0.01 across the supply voltage range, and hence, the prototype is statistically random over 0.6V-1.2V power supply. Fig. 8 shows the measured p-values for test chip1 across temperature range of −5°C to 50°C. The measured p-values are greater than 0.01 across the temperature range.

Fig. 9 shows the raw entropy of 2M TRNG bits from test chip1 over voltage corners of 0.6V-1.2V and temperature corners of −5°C to 50°C. The raw entropy is >0.9992 over the voltage and temperature corners. Fig. 10 shows the variation of raw TRNG entropy versus ADC input amplitude (Fig. 10(a)), input frequency (Fig. 10(b)) and comparator offset (Fig. 10(c)) for test chip1. The raw TRNG entropy remains >0.9996 across input amplitude and frequency variation, thus showing that TRNG quality is independent of ADC operation.

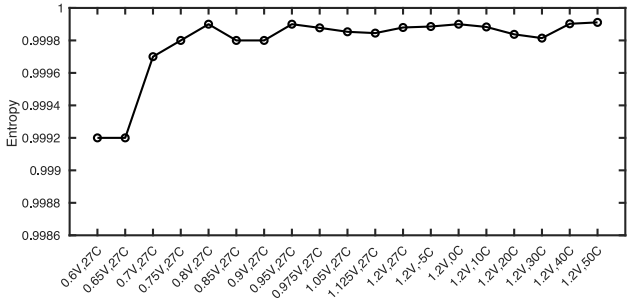


Fig. 9. Measured raw entropy versus corners.

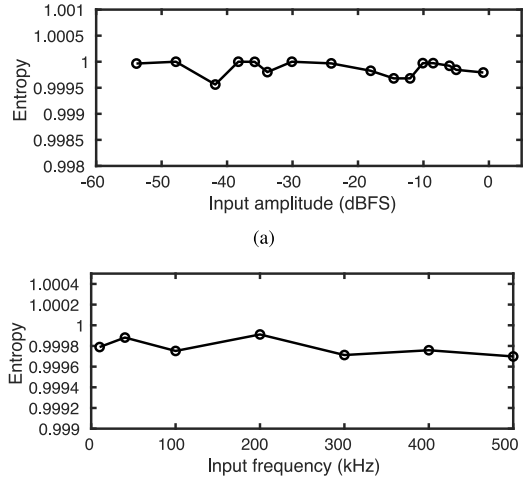


Fig. 10. Measured raw entropy vs (a) input amplitude (b) input frequency.

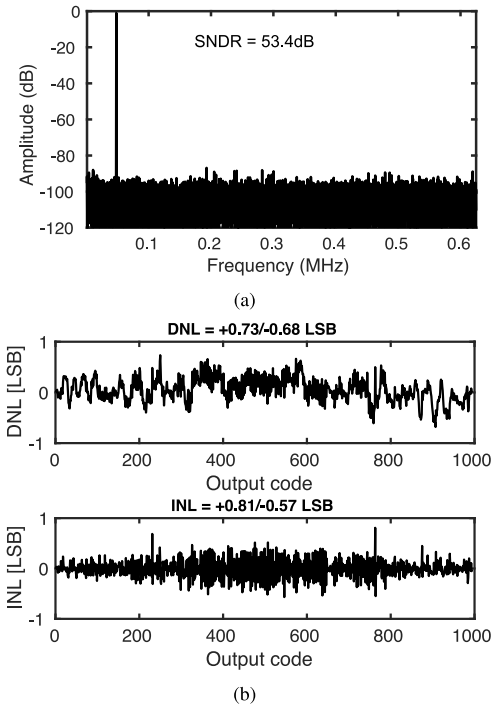


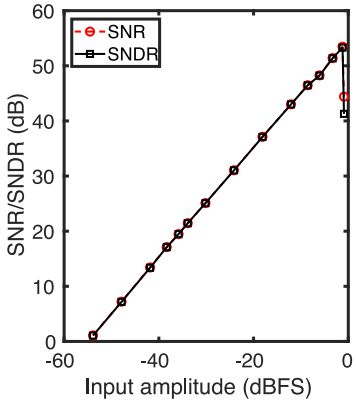
Fig. 11. Measured a) ADC spectrum b) DNL and INL plots.

Table II compares our TRNG with state-of-the-art TRNGs. The proposed TRNG has the lowest energy consumption of 0.22pJ/b and has a wide operating range of 0.6V-1.2V and

TABLE II
COMPARISON WITH STATE-OF-THE-ART TRNGS

	[5] ISSCC'14	[6] CICC'14	[7] JSSC'16	[12] ISSCC'17	[8] JSSC'17	[4] VLSI'18	[13] VLSI'18	**This Work**
Process(nm)	65	65	40	65	180	14	65	**65**
Entropy Source	Jitter accum.	Jitter accum.	Jitter accum.	Jitter accum.	Chaotic map	Meta-stability	Meta-stability	**SAR residue**
Supply(V)	0.9	0.8	0.9	1.08	0.6	0.65	0.53	**0.8**
Power(μW)	46	130	46	289	0.082	3700	8.33	**0.27**[1]
Operating voltage(V)	–	0.8-1.2	0.6-1	1.08-1.44	0.6-0.85	0.55-0.75	0.5-1.00	**0.6-1.2**
Throughput(Mbps)	2.8	2	2	8.2	0.216	1480	3.2	**1.25**
Energy(pJ/b)	57	66	23	36	0.38	2.5	2.58	**0.22**
Area(mm^2)	0.00096	0.006	0.0008	0.00092	0.21[2]	0.0021[3]	0.01	**0.09**[2]
Calibration needed	No	Yes	Yes	No	No	Yes	Yes	**No**
Post-processing	No	Yes	No	No	Yes	No	Yes	**No**

[1]measured at 0.8V power supply, [2]includes area of ADC+TRNG, [3]includes area of PUF+TRNG



ADC performance	
Process(nm)	65
Supply(V)	0.8
Power(μW)	3.8
Fs(MHz)	1.25
Resolution(bits)	10
SNDR(dB)	53.4
DR(dB)	54
ENOB(bits)	8.6
FoM(fJ/step)	7.8

Fig. 12. ADC DR plot and performance summary.

−5°C to 50°C. The chaotic-map TRNG presented in [8] consumes 0.38pJ/b, which is 73% higher than the proposed work, and requires post-processing to achieve a high entropy unlike the proposed technique which does not use post-processing. The proposed TRNG has more than 100× lower energy than [5], [12] which also do not require either calibration or post-processing. Since energy consumption in the proposed TRNG is primarily due to digital switching, energy consumption can be reduced for a lower throughput.

Fig. 11(a) shows the measured 2^{17} point FFT of the ADC with a 50kHz input signal and 1.25MHz sampling frequency. The ADC has an SNDR of 53.4dB. Fig. 11(b) shows the measured DNL and INL plots for the ADC. The ADC has DNL of +0.73/−0.68 LSB and INL of +0.81/−0.57 LSB. Fig. 12 shows the measured ADC SNDR versus input amplitude and performance summary. The ADC has a dynamic range of 54dB and walden FoM of 7.8fJ/step.

IV. CONCLUSION

A SAR ADC based TRNG is presented in this brief. Measured results demonstrate high quality random sequence while consuming the lowest energy of only 0.22pJ/b. The proposed architecture can operate as both ADC and TRNG independently. Since the architecture is highly digital, we expect lower energy consumption in advanced CMOS technology nodes.

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] 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.

[3] C. Tokunaga, D. Blaauw, and T. Mudge, "True random number generator with a metastability-based quality control," *IEEE J. Solid-State Circuits*, vol. 43, no. 1, pp. 78–85, Jan. 2008.

[4] S. Satpathy *et al.*, "An all-digital unified static/dynamic entropy generator featuring self-calibrating hierarchical von neumann extraction for secure privacy-preserving mutual authentication in IoT mote platforms," in *Proc. IEEE Symp. VLSI Circuits*, Honolulu, HI, USA, 2018, pp. 169–170.

[5] K. Yang, D. Fick, M. B. Henry, Y. Lee, D. Blaauw, and D. Sylvester, "A 23Mb/s 23pJ/b fully synthesized true-random-number generator in 28nm and 65nm CMOS," in *Proc. IEEE Int. Solid-State Circuits Conf. (ISSCC)*, San Francisco, CA, USA, 2014, pp. 280–281.

[6] 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 Proc. Custom Integr. Circuits Conf. (CICC)*, San Jose, CA, USA, 2014, pp. 1–4.

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

[8] 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.

[9] L. Chen, A. Sanyal, J. Ma, and N. Sun, "A 24-μW 11-bit 1-MS/s SAR ADC with a bidirectional single-side switching technique," in *Proc. IEEE Eur. Solid-State Circuits Conf. (ESSCIRC)*, 2014, pp. 219–222.

[10] A. Sanyal and N. Sun, "An energy-efficient low frequency-dependence switching technique for SAR ADCs," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 61, no. 5, pp. 294–298, May 2014.

[11] L. E. Bassham *et al.*, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," NIST, Gaithersburg, MD, USA, Rep. 800-22 Rev 1a, 2010.

[12] E. Kim, M. Lee, and J.-J. Kim, "8Mb/s 28Mb/mJ robust true-random-number generator in 65nm CMOS based on differential ring oscillator with feedback resistors," in *Proc. IEEE Int. Solid-State Circuits Conf. (ISSCC)*, San Francisco, CA, USA, 2017, pp. 144–145.

[13] V. R. Pamula, X. Sun, S. Kim, F. U. Rahman, B. Zhang, and V. S. Sathe, "An all-digital true-random-number generator with integrated de-correlation and bias correction at 3.2-to-86 Mb/s, 2.58 pJ/bit in 65-nm CMOS," in *Proc. IEEE Symp. VLSI Circuits*, Honolulu, HI, USA, 2018, pp. 1–2.