0.36-mW, 52-Mbps True Random Number Generator Based on a Stochastic Delta–Sigma Modulator

Sanjeev Tannirkulam Chandrasekaran, *Graduate Student Member, IEEE*, Vinay Elkoori Ghantala Karnam, and Arindam Sanyal, *Member, IEEE*

***Abstract*—This letter presents a true random number generator (TRNG) based on a stochastic delta–sigma modulator (DSM) with ring oscillator (RO) integrators. The TRNG leverages noise and jitter in the ROs as entropy source. A multibit nonreturn-to-zero (NRZ) digital-to-analog converter (DAC) in the feedback path ensures DSM noise dominates input swing seen by the front-end integrators. Hence, the DSM can concurrently operate as an ADC and TRNG. A 65-nm prototype achieves Shannon entropy >0.999998 with lower-bound min-entropy >0.995 at 52 Mb/s throughput while passing all NIST tests across multiple chips and voltage/temperature corners without needing calibration. The combined power consumption of ADC and TRNG is 0.36 mW which is the lowest among state-of-the-art RO TRNGs. Low power consumption, high entropy, and concurrent operation of the TRNG as an ADC are principal contributions of this letter.**

***Index Terms*—Analog-to-digital converter (ADC), delta–sigma, true random number generator (TRNG), voltage-controlled oscillator.**

I. Introduction

Random numbers are an integral part of cryptography, secure communications, and statistical operations, like monte-carlo simulations. Si-based true random number generators (TRNGs) usually derive their randomness from thermal noise or jitter sources. A widely used TRNG is a metastable latch [1], [2] which randomly outputs "0/1" based on thermal noise. However, a metastable latch is very sensitive to offset and PVT variations and requires careful background calibration to remove bias which degrades randomness. Ring voltage-controlled oscillator (VCO) is another popular architecture for TRNG which leverages VCO thermal noise and clock jitter to derive TRNG. Architectures using VCO-based TRNG include edge-chasing TRNG of [3] and beat-frequency detector of [4]. Both edge-chasing and beat-frequency TRNGs require calibration for PVT variations and offset. State-of-the-art TRNGs reported so far are designed to operate as stand-alone circuit, with the exception of [5] which works simultaneously as subranging successive approximation register (SAR) analog-to-digital converter (ADC) and TRNG, and [2] which works as physical unclonable function (PUF) and TRNG.

In this letter, we present a mixed-signal TRNG that can simultaneously operate as both continuous-time (CT) $\Delta\Sigma$ ADC and TRNG, with entropy source of the TRNG being noise and jitter in the ADC. An averaging ADC architecture with 4 sub-ADCs is used, and the LSB bits of each sub-ADC are combined together using XOR gates to produce the TRNG bitstream. Averaging reduces both noise and distortion of sub-ADCs and is an attractive option for increasing ADC resolution in advanced technology nodes [6]. The additional hardware needed for TRNG operation are only 7 XOR-gates. Reusing ADC architecture for TRNG achieves both area and power savings in SoC with already existing ADC. Compared to [5], the proposed TRNG has a much higher throughput, and compared to [2], the proposed TRNG does not require calibration. A test chip fabricated in 65-nm CMOS process passes all NIST tests, has entropy (H) >0.999998 across multiple test chips and voltage–temperature (VT) conditions without calibration and is resistant to power supply attacks.

Manuscript received May 18, 2020; revised July 2, 2020; accepted July 15, 2020. Date of publication July 21, 2020; date of current version August 7, 2020. This article was approved by Associate Editor Stefan Rusu. This work was supported by the Semiconductor Research Corporation Task through the Texas Analog Center of Excellence, University of Texas at Dallas under Grant 2712.020. *(Corresponding author: Sanjeev Tannirkulam Chandrasekaran.)*

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

Digital Object Identifier 10.1109/LSSC.2020.3010901

II. Proposed Architecture

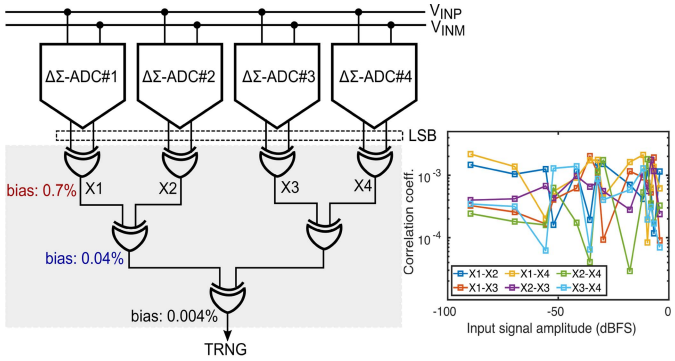
The averaging ADC architecture is shown in Fig. 1(a). Each sub-ADC is based on the architecture reported in [7] and shown in Fig. 1(b). The TRNG derives its entropy from thermal noise and jitter in the ADC and LSB of the ADC differential outputs are XOR-ed together to produce TRNG sequence as shown in Fig. 1. The basic reason why the proposed architecture can act as both ADC and TRNG simultaneously is due to the negative feedback loop which forces the differential input VCOs [VCO1 in Fig. 1(b)] to track each other irrespective of the input signal and ensures that the input swing of VCO1 is set by noise rather than the input signal. This is in contrast to open-loop architecture, such as the beat-frequency architecture [4], in which the differential VCOs directly see the full input signal and can only act as a TRNG for very small or no input signal. Fig. 2 shows the input swing and XOR-ed LSB for an open-loop VCO ADC and the closed-loop sub-ADC shown in Fig. 1(a). For both cases, the VCOs have the same tuning gain and number of stages. The open-loop ADC sees the full input swing and the XOR-ed LSB output shows tones. Shannon entropy for the open-loop XOR-ed LSB output is 0.9632. When the same input signal is applied to our closed-loop sub-ADC, the input swing seen by the first and second VCO integrators are substantially attenuated compared to the open-loop case, and the entropy of the XOR-ed LSB output is significantly improved to 0.9999.

While static mismatch in the DAC is high-pass shaped by intrinsic DWA due to barrel shifting element selection pattern in the quantizer, mismatch in differential path in each sub-ADC can bias the TRNG output and degrade entropy of the raw bitstream. XOR-ing the sub-ADC outputs suppresses bias and improves raw entropy. The measured mean bias after each round of XOR is annotated in Fig. 1(a). While sub-ADC output has a mean bias of 0.7%, the combined ADC output has a mean bias of only 0.004%. Fig. 1(a) also shows the measured correlation coefficients between each ADC LSB output. The correlation coefficients are all less than 0.005 across input amplitude range which shows that the XOR-ed LSB outputs of each ADC have negligible correlation between them. Fig. 3 shows the die photograph of the test chip fabricated in 65-nm process and the ADC performance summary at 52-MHz sampling frequency.

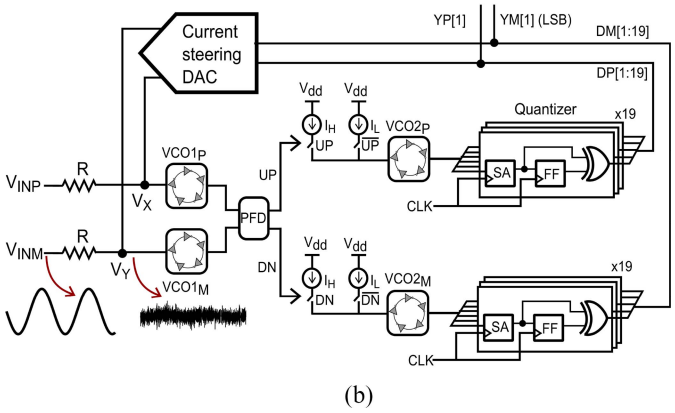
III. TRNG Measurement Results

A. Results Across Corners

We measured five test chips for five different power supply voltages from 0.8 to 1.2 V in steps of 0.1 V at room temperature, and over

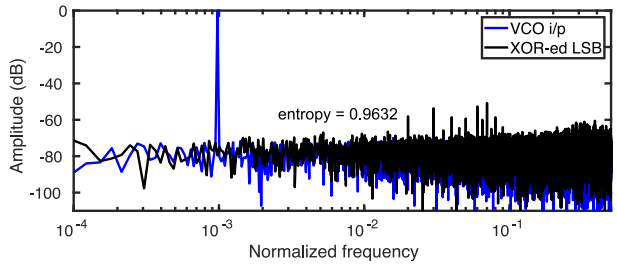


(a)

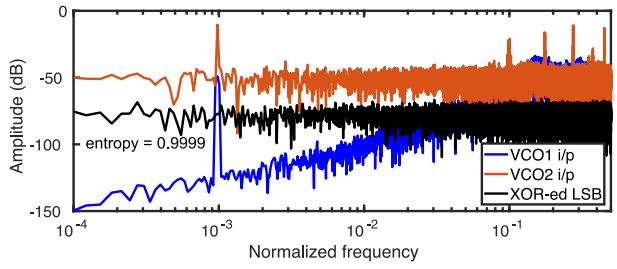


(b)

Fig. 1. Circuit schematic of the (a) proposed TRNG and (b) sub-ADC.



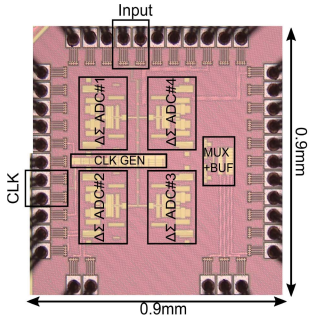
(a)



(b)

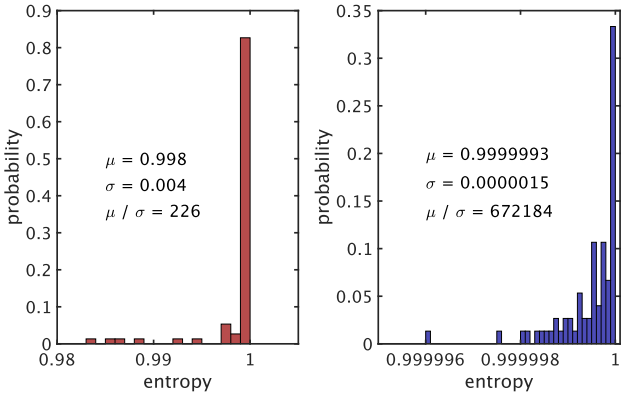
Fig. 2. Input swing and LSB output for (a) open-loop VCO-ADC and (b) closed-loop sub-ADC from Fig. 1(a).

temperature range of −20 °C to 70 °C in steps of 10 °C at 1.2 V. Fig. 4 shows the histogram of measured entropy across VT corners for a sub-ADC output and the combined ADC output. Combining 4 sub-ADC output improves mean entropy and reduces standard deviation of entropy by 3 orders of magnitude compared to that of a single sub-ADC.



Process(nm)	65
Supply(V)	0.9
Power(mW)	0.36
F_s(MHz)	52
BW(MHz)	0.4
SNDR(dB)	67.3
DR(dB)	68.4
FoM$_s$(dB)	159

Fig. 3. Die photograph and ADC performance summary.



(a) (b)

Fig. 4. Measured entropy across VT corners and 5 chips for (a) single sub-ADC and (b) combined output of 4 sub-ADCs.

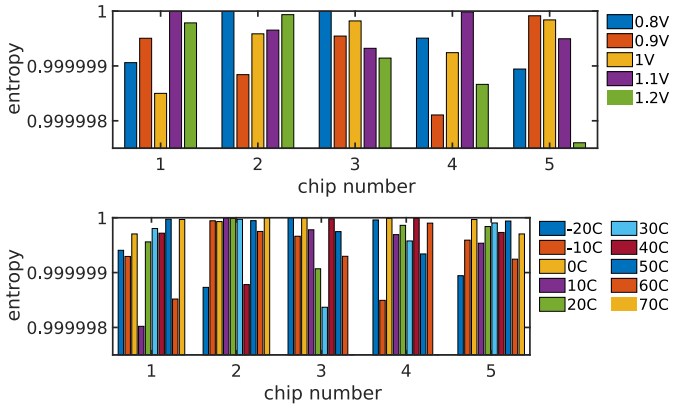


Fig. 5. Measured entropy across VT corners.

Fig. 5 shows the measured raw entropy for the 5 test-chips across VT corners. The minimum entropy is >0.999998 across the VT corners. NIST SP 800-90B tests are used to verify that the raw TRNG outputs across VT corners are independent and identically distributed (IID) and the lower-bound min-entropy H_∞ is >0.995 which is 5× higher than that in [8]. Fig. 6(a) shows the measured autocorrelation of 1M bits with lags up to 2^{14}. The autocorrelation coefficients are within 95% confidence bounds of Gaussian distribution with mean of 0 and standard deviation of 0.003. The very low autocorrelation coefficients indicate that there are no perceptible patterns in the raw TRNG bits.

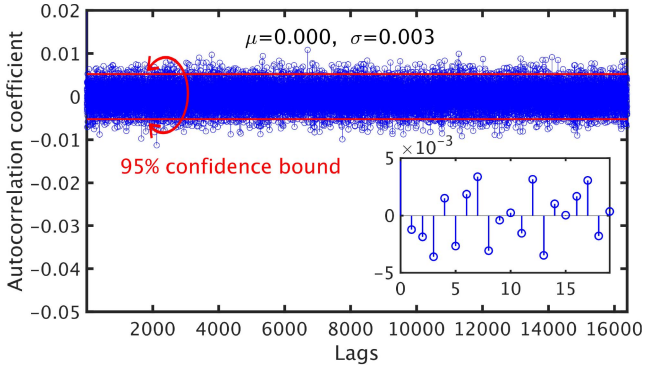


Fig. 6. Measured autocorrelation on TRNG output.

TABLE I
NIST TEST RESULTS

	1.2V				27C			
	-20C		70C		0.8V		1.2V	
	pass	pval	pass	pval	pass	pval	pass	pval
Freq. monobit	1.00	0.50	1.00	0.50	1.00	0.49	1.00	0.50
Block freq.	1.00	0.49	1.00	0.49	1.00	0.49	1.00	0.49
Runs	1.00	0.50	0.99	0.50	0.99	0.51	1.00	0.54
Longest run	0.96	0.44	0.99	0.44	0.97	0.41	0.99	0.39
Binary matrix	1.00	0.29	1.00	0.28	1.00	0.29	1.00	0.29
DFT	1.00	0.61	1.00	0.61	1.00	0.59	1.00	0.57
Non-overlapping	1.00	0.51	1.00	0.51	1.00	0.50	1.00	0.49
Overlap matching	1.00	0.63	1.00	0.61	1.00	0.69	1.00	0.64
Maurers universal	1.00	0.14	1.00	0.14	1.00	0.14	1.00	0.14
Linear complexity	1.00	0.99	1.00	0.99	1.00	0.99	1.00	0.99
Serial	1.00	0.37	1.00	0.37	0.99	0.33	1.00	0.31
Approx. entropy	1.00	0.89	1.00	0.88	1.00	0.89	1.00	0.87
Cumulative sum	1.00	0.44	0.97	0.43	0.99	0.44	0.99	0.44
Random excursions	0.97	0.28	1.00	0.28	0.99	0.24	0.99	0.25
Random exc. variant	1.00	0.52	1.00	0.52	1.00	0.51	0.99	0.48

B. NIST Test Results

Table I summarizes the results of NIST statistical tests at four different VT corners. The TRNG passes all the NIST tests with a minimum pass rate of 0.96.

Fig. 7 shows the measurement results with sinusoidal inputs at nominal conditions. Fig. 7(a) shows raw entropy and minimum NIST pass-rates as the input amplitude is swept. The entropy remains high (>0.999998) throughout the amplitude range. The minimum NIST pass rate is above 0.97 for the entire range of input amplitude. Fig. 7(b) shows the FFT for −4 dBFS and −70 dBFS input signals.

Fig. 8 shows the result of repeated evaluations of TRNG output at nominal conditions. The raw entropy corresponds to Shannon entropy for each evaluation point. The NIST pass-rate is calculated cumulatively and the minimum pass-rate across the 15 tests is shown in Fig. 8. The raw entropy remains consistently >0.999998 and the minimum pass-rate remains >0.98 across the evaluation points. Fig. 9 shows the measured ADC output and TRNG FFT plot for sinc(·) input signal. The TRNG has a raw entropy of 0.9999992 which shows that the proposed circuit can operate as both ADC and TRNG with nonsinusoidal inputs.

C. Power Supply Attacks

To investigate robustness of the TRNG against power supply attacks, we injected sinusoidal signals with amplitudes from 30 to 190 mV to the core power supply driving the VCOs. Frequency of the injected signals is varied from 1 kHz to 99 MHz. Fig. 10 shows

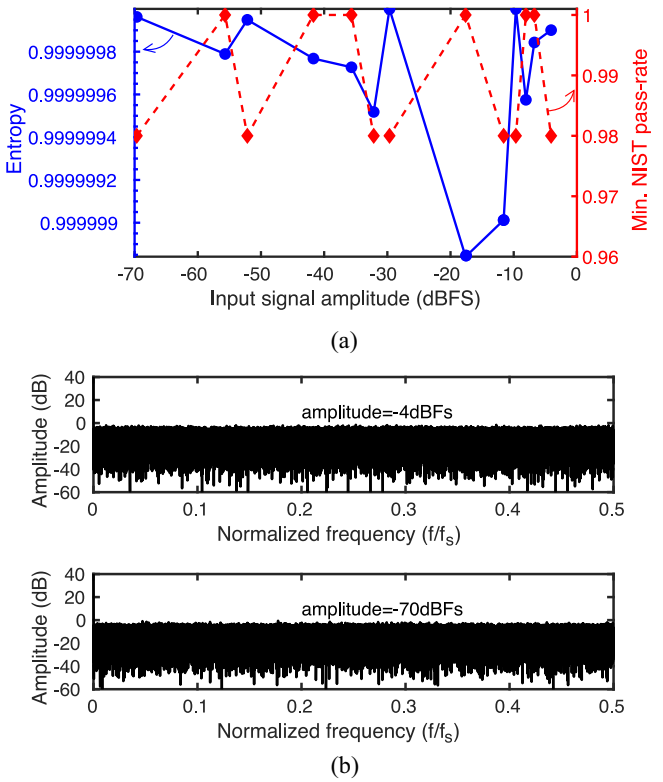


Fig. 7. (a) TRNG raw entropy and minimum NIST pass-rate versus sinusoidal input amplitude. (b) TRNG FFT for large and small sinusoidal input signals.

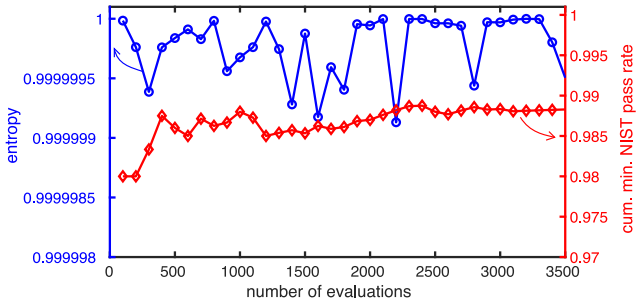


Fig. 8. Measured entropy and cumulative NIST pass rates for repeated evaluation.

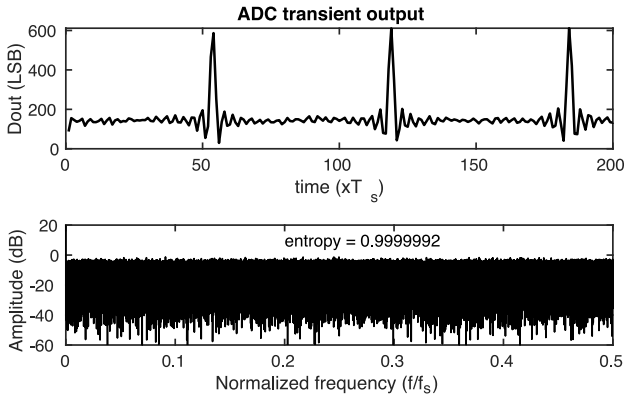


Fig. 9. Measured ADC output and TRNG FFT for sinc input.

the measured entropy versus amplitude of the injected signal. The raw entropy starts dropping with input amplitude for injected signal frequency of 96 MHz for amplitudes >140 mV. This is most likely

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

	Process (nm)	Entropy source	Entropy	Throughput (Mbps)	Area (mm^2)	Power (mW)	Efficiency (pJ/bit)	Multi-function	V_{dd} attack robust ?	Calibration free ?
JSSC'19 [2]	14	metastability	0.99997	1480	0.29	3.7	2.5	PUF/TRNG	✓	×
VLSI'18 [1]	65	metastability	0.999996	86	0.0	0.52	6.1	×	✓	×
ISSCC'17 [9]	65	jitter	–	9.9	0.001	0.42	42.4	×	✓	✓
JSSC'17 [10]	65	metastability	0.9996	3000	0.002	5	1.6	×	N/A	×
JSSC'16 [8]	14	metastability	> 0.9999999	162.5	0.001	1.5	9.23	×	✓	×
ISSCC'14 [3]	28	jitter	–	23.16	0.0004	0.54	23	×	✓	×
This work	**65**	**jitter**	**0.999998**	**52**	**0.06**	**0.36**[1]	**6.9**	**ADC/TRNG**	✓	✓

[1]combined power consumption of ADC and TRNG

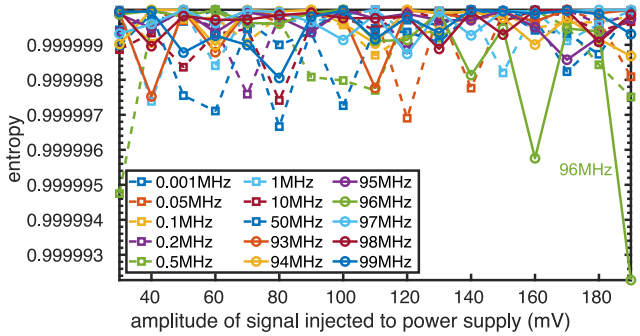


Fig. 10. Measured entropy for varying amplitude of signal injected into power supply.

due to injection locking of the VCOs in the ADCs since the VCO center frequency is in the range of 95–96 MHz. The raw entropy drops by 7× for 190-mV amplitude at 96 MHz, but is consistently >0.999997 across the amplitude range for other frequencies. The measurement results show that the TRNG is robust against power supply attacks for injected signal amplitudes less than 140 mV. Robustness at higher amplitudes can be increased by low-pass filtering the power supply [3].

D. Comparison With Other Works

Table II compares this letter with the state-of-the-art TRNGs with similar throughput. The proposed TRNG has the lowest energy consumption compared to other TRNGs with jitter as entropy source. While our TRNG does not have the best efficiency since it is shared with a 12-bit ADC, the merits of the proposed work are: 1) it has dual functionality (ADC/TRNG); 2) is robust against power supply attacks; and 3) does not require calibration. No other state-of-the-art TRNG meets all three above-mentioned criteria. The work in [2] acts as both PUF and TRNG and is robust against power supply attacks, but requires calibration to de-bias the metastable latch. Our chip area is also 5× smaller than the unified PUF/TRNG work [2] which is in an advanced 14-nm process.

REFERENCES

[1] V. R. Pamula, X. Sun, S. Kim, F. ur 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.

[2] S. K. Satpathy *et al.*, "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," *IEEE J. Solid-State Circuits*, vol. 54, no. 4, pp. 1074–1085, Apr. 2019.

[3] 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. Dig. Tech. Papers (ISSCC)*, San Francisco, CA, USA, 2014, pp. 280–281.

[4] Q. Tang, B. Kim, Y. Lao, K. K. Parhi, and C. H. Kim, "True random number generator circuits based on single- and multi-phase beat frequency detection," in *Proc. IEEE Custom Integr. Circuits Conf. (CICC)*, San Jose, CA, USA, 2014, pp. 1–4.

[5] 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.

[6] H. Sun, K. Sobue, K. Hamashita, and U.-K. Moon, "An oversampling stochastic ADC using VCO-based quantizers," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 65, no. 12, pp. 4037–4050, Dec. 2018.

[7] A. Jayaraj, M. Danesh, S. T. Chandrasekaran, and A. Sanyal, "Highly digital second-order ΔΣ VCO ADC," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 66, no. 7, pp. 2415–2425, Jul. 2019.

[8] S. K. Mathew *et al.*, "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.

[9] E. Kim, J. Lee, and J. Kim, "8.2 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.

[10] S.-G. Bae, Y. Kim, Y. Park, and C. Kim, "3-Gb/s high-speed true random number generator using common-mode operating comparator and sampling uncertainty of D flip-flop," *IEEE J. Solid-State Circuits*, vol. 52, no. 2, pp. 605–610, Feb. 2017.