2021 IEEE International Symposium on Circuits and Systems (ISCAS) | 978-1-7281-9201-7/20/$31.00 ©2021 IEEE | DOI: 10.1109/ISCAS51556.2021.9401507

33-200Mbps, 3pJ/bit True Random Number Generator Based on CT Delta-Sigma Modulator

Sanjeev Tannirkulam Chandrasekaran*, Akshay Jayaraj†, Naveen Ramesh*and Arindam Sanyal*
*Electrical Engineering Department, University at Buffalo, Buffalo, NY 14260, USA.
†Intel Corporation, Folsom CA 95630, USA. Email: stannirk@buffalo.edu

***Abstract*—This work presents a true random number generator (TRNG) that uses noise and jitter in a continuous-time, delta-sigma modulator (CTDSM) as entropy source. A multi-bit non-return-to-zero (NRZ) feedback digital-to-analog converter (DAC) ensures that input swing seen by the front-end integrators is small and dominated by CTDSM noise and jitter, thus allowing the proposed circuit to simultaneously operate as both CTDSM and TRNG which is a key differentiation of this work compared to state-of-the-art TRNGs. Voltage controlled ring oscillators are used to implement integrators in the proposed CTDSM. Fabricated in 65nm CMOS, the TRNG has an energy efficiency of 3pJ/bit at throughput of 33Mbps and 3.5pJ/bit at 200Mbps, and passes all NIST tests with a minimum pass rate > 0.96. The measured minimum entropy of the TRNG bits is > 0.9995 across multiple chips and voltage/temperature corners without any calibration.**

***Index Terms*—true random number generator, voltage-controlled oscillator, analog-to-digital converter, delta-sigma**

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 sub-ranging successive approximation register (SAR) analog-to-digital converter (ADC) and TRNG, and [2] which works as physical unclonable function (PUF) and TRNG.

In this work, we present a mixed-signal TRNG that can simultaneously operate as both $\Delta\Sigma$ ADC and TRNG, with entropy source of the TRNG being noise and jitter in the continuous-time (CT) ADC. The additional hardware needed for TRNG operation is only an XOR-gate that takes as input LSB bits of the differential ADC output and provides a TRNG sequence. Re-using ADC architecture for TRNG generation can achieve 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 65nm CMOS process passes all NIST tests, has entropy (H) > 0.9995 across multiple test chips and voltage-temperature (VT) conditions without calibration (H > 0.99999 with offset correction), and is resistant to power supply attacks.

II. Proposed Architecture

The proposed TRNG is based on a second-order, CT $\Delta\Sigma$ VCO-ADC as shown in Fig. 1. The ADC architecture is based on the work reported in [6]. The TRNG derives its entropy from thermal noise and jitter in the ADC and LSB of the ADC differential outputs are XOR-ed to produce TRNG bitstream 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) to track each other irrespective of the input signal and ensures that the input swing of VCO1 is set primarily by thermal noise and out-of-band quantization noise rather than the input signal. This is in contrast to the beat frequency TRNG in which the differential VCOs directly see the input signal and can only act as TRNG when no input signal is applied.

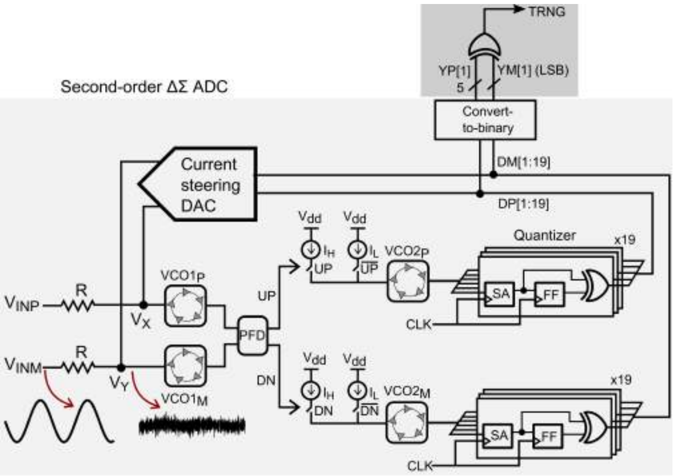


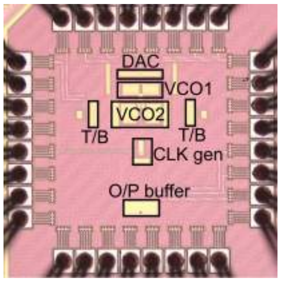
Fig. 1: Circuit schematic of the proposed TRNG

Mismatch in the ADC circuit can bias the TRNG output and degrade its entropy. Mismatch in the DAC is high-pass shaped

978-1-7281-9201-7/21/$31.00 ©2021 IEEE

by intrinsic DWA due to barrel shifting element selection pattern in the quantizer. Static mismatch between the input VCOs can limit entropy of the TRNG, but mismatch between second-stage VCOs does not affect the TRNG quality since their mismatch is high-pass shaped by the $\Delta\Sigma$ loop. Mismatch between the input VCOs can be removed through foreground offset correction and is discussed later.

Fig. 2 shows die photo of the test chip fabricated in 65nm process and the ADC performance summary at 32.6MHz sampling frequency. The ADC has state-of-the-art energy efficiency of 8.6fJ/step. The core area of the ADC+TRNG combination is 0.06mm^2.



Process(nm)	65
Supply(V)	1
Power(mW)	0.1
Area(mm^2)	0.06
F$_s$(MHz)	32.6
BW(MHz)	2.3
SNDR(dB)	70.2
SFDR(dB)	81
FoM$_w$(fJ/step)	8.6

Fig. 2: Die photo and ADC performance summary

III. TRNG MEASUREMENT RESULTS

A. NIST test results

We measured 4 test chips at 9 different VT corners - 3 power supply points $\{0.9, 1, 1.1\}$V and 3 temperature points $\{0, 27, 60\}$°C with the nominal VT corner being (1V, 27°C). The test chips are used simultaneously as ADC and TRNG. The TRNG output is recorded 32 times for each VT corner corresponding to 288 runs for each chip. A sinusoidal input with -6dBFS amplitude and frequency of 50kHz is applied to the test chips and the TRNG output is sampled at 32.6MHz. No calibration is performed on the test chips. Table I shows the pass-rates for NIST tests for each chip. All the 4 chips pass the NIST tests with a minimum pass-rate>0.96.

Fig. 3 shows the measured entropy gap for the test chips across VT corners. The test chips have raw entropy>0.9995 across the VT corners. Fig. 4 shows the measured autocorrelation of 1M bits with lags upto 2^{14}. The autocorrelation coefficients are within 95% confidence bounds of gaussian distribution with mean of 0 and standard deviation of 0.001. The very low autocorrelation coefficients indicate that there are no perceptible patterns in the raw TRNG bits.

B. Test results with different inputs

The test chip is measured with different inputs - a) sine wave with varying amplitude b) ECG and sinc function inputs. Fig. 5 shows the measurement results with sinusoidal inputs. Fig. 5(a) shows raw entropy and minimum NIST pass-rates as the input amplitude is swept. At very low input amplitudes (around -60dBFS), the quantizer output spans only 3 levels out of 19 which reduces randomness of quantization error and limits entropy of the LSB. Hence, the measured entropy is low at very small signal amplitudes and increases as the signal amplitude is increased. The NIST pass rate remains above 0.96 for the entire range of input amplitude.

TABLE I: NIST test result

Pass rates for NIST tests				
Test Name	**chip1**	**chip2**	**chip3**	**chip4**
Frequency monobit	1	1	1	1
Block frequency	1	0.9896	0.9965	0.9931
Runs test	0.9861	0.9688	0.9826	0.9826
Longest run of ones	0.9896	0.9965	0.9931	0.9931
Binary matrix rank	1	1	1	1
DFT	0.9965	1	1	1
Non-overlapping	1	1	1	1
Overlap matching	1	1	1	1
Maurers universal	1	1	1	1
Linear complexity	1	1	1	1
Serial test	0.9757	0.9931	1	0.9653
Approximate entropy	1	1	1	1
Cumulative sums	0.9965	0.9931	0.9965	0.9931
Random excursions	0.9965	1	1	0.9965
Random exc. variant	1	1	1	0.9965

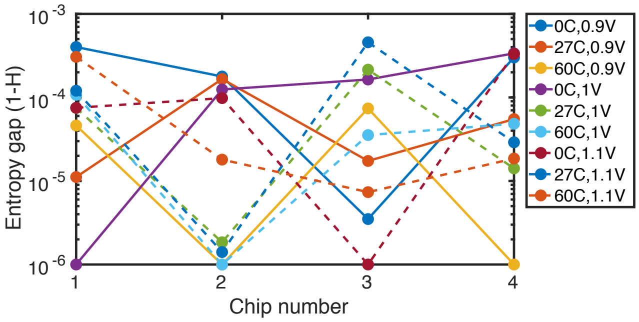


Fig. 3: Measured entropy gap across VT corners

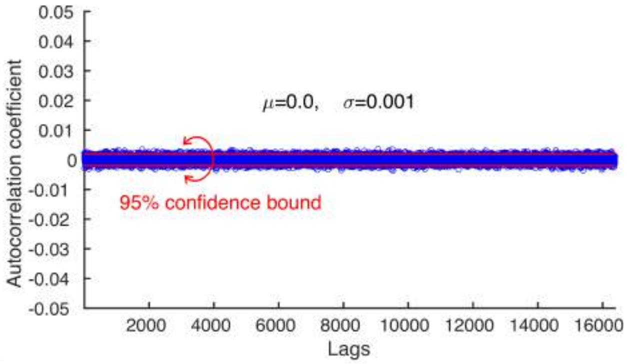
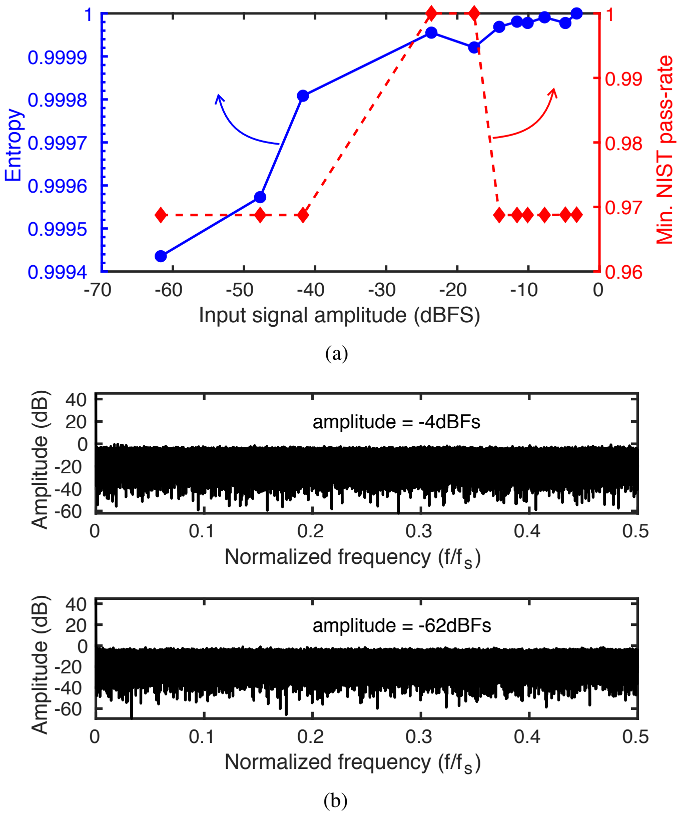


Fig. 4: Measured autocorrelation on TRNG output

Fig. 6 shows measured ADC transient output and TRNG output spectrum with an ECG input signal. The TRNG output has a raw entropy of 0.9995. The TRNG output is recorded 32 times and passes all the NIST tests with minimum pass-rate >0.96. Fig. 7 shows measured ADC transient output and TRNG output spectrum with a sinc$(\cdot)$ input signal. The TRNG output has a raw entropy of 0.9993. The TRNG output is recorded 32 times and passes all the NIST tests with minimum pass-rate >0.96. The measurement results with sinusoidal, ECG



(a)

(b)

Fig. 5: (a) TRNG raw entropy and minimum NIST pass-rate versus sinusoidal input amplitude (b) TRNG FFT for large and small sinusoidal input signals

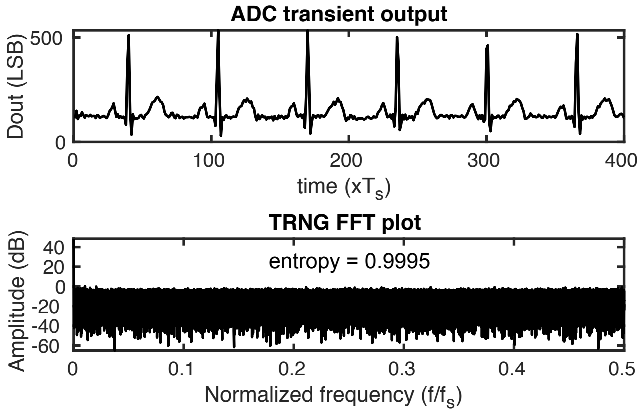


Fig. 6: Measured ADC transient output and TRNG FFT plot for an ECG input signal

and sinc$(\cdot)$ inputs demonstrate that the proposed circuit can simultaneously operate as both ADC and TRNG irrespective of the type of input signal.

C. Power supply attacks

To investigate robustness of the TRNG against power supply attacks, we injected 30kHz sinusoidal signals with amplitudes from 50mV to 250mV to the core power supply driving the VCOs. Fig. 8 shows the measured entropy and minimum NIST pass-rates from 32 runs versus amplitude of injected signal.

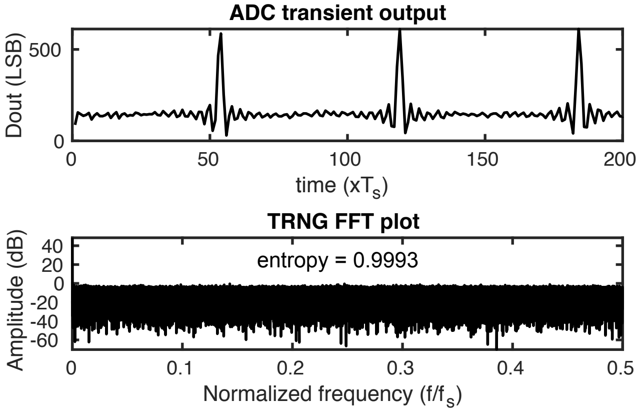


Fig. 7: Measured ADC transient output and TRNG FFT plot for sinc$(\cdot)$ input signal

The TRNG passes all NIST tests with pass-rate$>$ 0.96 and raw entropy$>$ 0.9995 as the injected signal amplitude varies from 50mV to 250mV, thus, showing that the TRNG is robust against power supply attacks.

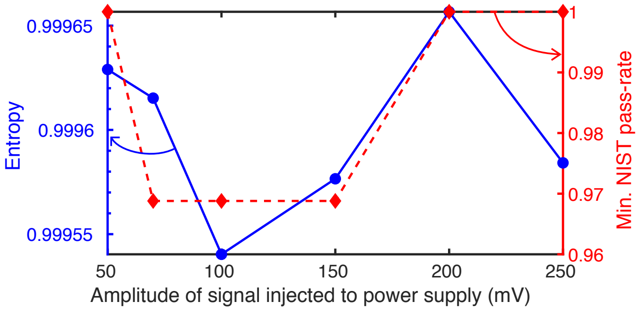


Fig. 8: Measured entropy for varying amplitude of signal injected into power supply

D. Effect of noise and offset

To investigate the effect of thermal noise on the TRNG performance, we swept the ADC thermal noise by varying the center frequency of VCO1. Increasing center frequency of VCO1 increases its input referred thermal noise, and has to be accompanied by proportional increase in sampling frequency to prevent instability due to phase overflow in VCO1. The center frequency of VCO2 is also increased proportionally to keep quantization error unchanged. Fig. 9 shows the measured entropy with change in sampling frequency for -60dBFS sinusoidal input. The TRNG entropy increases monotonically as ADC sampling frequency, and VCO1 thermal noise, increases. The ADC can maintain almost constant SNDR as sampling frequency is increased, since the input swing increases in proportion to sampling frequency, but with increased power consumption, i.e, trade-off of having better TRNG entropy is reduced energy efficiency of the ADC.

Input offset biases the TRNG output and degrades quality of the TRNG sequence. Keeping input common-mode voltage of VCO1$_P$ constant, we swept input common-mode voltage of

TABLE II: Comparison with state-of-the-art TRNGs with similar throughput

	Process (nm)	Entropy source	Area (mm^2)	Throughput (Mbps)	Power (mW)	Efficiency (pJ/bit)	Multi-function	V_{dd} attack robust	Needs calibration
JSSC'19 [2]	14	metastability	–	1480	3.7	2.5	PUF/TRNG	✓	✓
VLSI'18 [1]	65	metastability	0.01	86	0.52	6.1	×	✓	✓
ISSCC'17 [7]	65	jitter	0.00092	9.9	0.42	42.4	×	✓	×
JSSC'17 [8]	65	metastability	0.0016	3000	5	1.6	×	N/A	✓
JSSC'16 [9]	14	metastability	0.001	162.5	1.5	9.23	×	✓	✓
ISSCC'14 [3]	28	jitter	0.00037	23.16	0.54	23	×	✓	✓
This Work	**65**	**jitter**	**0.06**[1]	**33**	**0.1**[2]	**3**	ADC/TRNG	✓	×
				200	**0.7**[2]	**3.5**			

[1]combined area of ADC and TRNG; [2]combined power consumption of ADC and TRNG

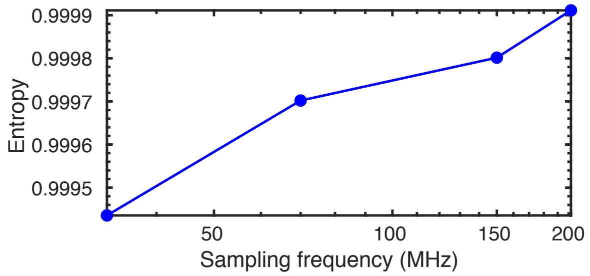


Fig. 9: Measured TRNG entropy versus ADC noise

VCO1$_M$ and calculated NIST pass rates and entropy. The measured entropy gap and NIST pass rates are plotted in Fig. 10 versus difference in common-mode voltages of VCO1$_P$ and VCO1$_M$, ΔVcmi. The TRNG has a high entropy ($>$ 0.99999) as long as ΔVcmi is between 0 and -6mV and the NIST pass rate drops below 0.96 once ΔVcmi exceeds 10mV/$-$20mV. The asymmetric bounds on ΔVcmi is due to offset in the chip due to mismatch between VCO1$_P$ and VCO1$_M$, and the results demonstrate that the TRNG can reach high entropy ($>$ 0.99999) with offset correction.

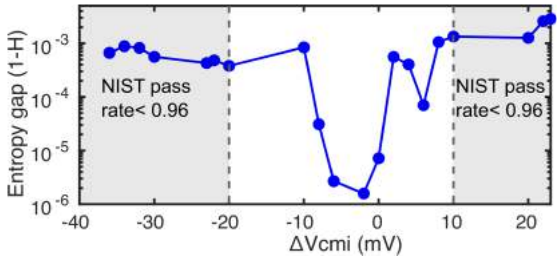


Fig. 10: Measured TRNG entropy versus input offset

E. Comparison with other works

Table II compares this work with state-of-the-art TRNGs with similar throughput. While our TRNG does not have the best efficiency since it is shared with a 12-bit ADC and the power consumption comes almost entirely from the ADC, the proposed circuit can simultaneously operate as both high-performance ADC and TRNG, is robust against power supply attacks and does not require calibration. No other state-of-the-art TRNG meets all three above-mentioned criteria - 1) multiple functionality, 2) demonstrated robustness against power supply attack, and 3) calibration free. 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.

IV. Conclusion

We have presented a mostly digital architecture that can simultaneously operate as both CT $\Delta\Sigma$ ADC and TRNG, and achieve high entropy without calibration. The highly digital nature of the proposed architecture ensures that it can be easily scaled to more advanced CMOS technologies with accompanying improvement in energy efficiency.

Acknowledgment

This work is supported by Semiconductor Research Corporation (SRC) task # 2712.020 through The University of Texas at Dallas' Texas Analog Center of Excellence (TxACE).

References

[1] V. R. Pamula *et al.*, "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 *IEEE Symposium on VLSI Circuits*, 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 Journal of Solid-State Circuits*, vol. 54, no. 4, pp. 1074–1085, 2019.

[3] K. Yang *et al.*, "A 23Mb/s 23pJ/b fully synthesized true-random-number generator in 28nm and 65nm CMOS," in *IEEE International Solid-State Circuits Conference (ISSCC)*, 2014, pp. 280–281.

[4] Q. Tang *et al.*, "True random number generator circuits based on single- and multi-phase beat frequency detection," in *IEEE Proceedings of the Custom Integrated Circuits Conference (CICC)*, 2014, pp. 1–4.

[5] M. Kim *et al.*, "A 82-nw chaotic map true random number generator based on a sub-ranging SAR ADC," *IEEE Journal of Solid-State Circuits*, vol. 52, no. 7, pp. 1953–1965, 2017.

[6] A. Jayaraj *et al.*, "8.6fJ/step VCO-Based CT 2nd-Order $\Delta\Sigma$ ADC," in *IEEE Asian Solid State Circuits Conference (A-SSCC)*, 2019.

[7] 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 *IEEE International Solid-State Circuits Conference (ISSCC)*, 2017, pp. 144–145.

[8] S.-G. Bae *et al.*, "3-Gb/s high-speed true random number generator using common-mode operating comparator and sampling uncertainty of D flip-flop," *IEEE Journal of Solid-State Circuits*, vol. 52, no. 2, pp. 605–610, 2016.

[9] 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 Journal of Solid-State Circuits*, vol. 51, no. 7, pp. 1695–1704, 2016.