S2ADC: A 12-bit, 1.25MS/s Secure SAR ADC with Power Side-Channel Attack Resistance

Citation: Jeong, Taehoon et al. "S2ADC: A 12-bit, 1.25MS/s Secure SAR ADC with Power Side-Channel Attack Resistance" 2020 IEEE Custom Integrated Circuits Conference (CICC), Boston, MA, USA, Institute of Electrical and Electronics Engineers (IEEE), April 2020

As Published: http://dx.doi.org/10.1109/cicc48029.2020.9075919

Publisher: Institute of Electrical and Electronics Engineers (IEEE)

Persistent URL: https://hdl.handle.net/1721.1/125779

Version: Author's final manuscript: final author's manuscript post peer review, without publisher's formatting or copy editing

S2ADC: A 12-bit, 1.25MS/s Secure SAR ADC with Power Side-Channel Attack Resistance

Taehoon Jeong, Anantha P. Chandrakasan, and Hae-Seung Lee
Massachusetts Institute of Technology, Cambridge, MA 02139, USA

***Abstract*—This paper presents a neural-network-based SAR ADC power side-channel attack (PSA) method and a 12-bit, 1.25MS/s secure SAR ADC whose current equalizers protect the ADC from PSA. A prototype SAR ADC was fabricated in 65nm CMOS to demonstrate the proposed concepts. Without PSA protection, the proposed PSA method decoded the power supply current waveforms of the prototype ADC into the corresponding A/D converter output bits with $>99\%$ bit-wise accuracy except for the LSB. With PSA protection, the prototype ADC demonstrated high resistance to the proposed PSA method, showing significant drop in bit-wise accuracy.**

I. Introduction

With increasing security concerns of sensor hardware, recent works [1], [2] have suggested ADC side-channel leakages as a security loophole. As illustrated in Fig. 1, after digitization, the sensitive information can be protected from attackers by using well-established encryption methods and side-channel attack countermeasures. However, at least two security loopholes still exist in analog/mixed-signal domain: direct measurement of sensor output and power side-channel attack (PSA) on analog/mixed-signal circuits. Direct measurements of sensor output can be prevented by using a tamper-proof package [1]. On the other hand, an attacker can perform PSA on analog/mixed-signal circuits without disturbing the sensitive analog signal. The tamper-proof package may not be extended to enclose the power source and power management circuits for practical reasons, such as provision for battery replacements and physical size limitations. This calls for countermeasures to protect analog/mixed-signal circuits from PSA.

Previous work [2] demonstrated a SAR ADC side-channel leakage through the voltage reference by employing template matching. In addition, random dithering was used as a countermeasure against the reference-charge side-channel attack, but leaves the side-channel through the power supply unprotected. This work demonstrates a robust attack method based on neural networks as well as a countermeasure against side-channel leakages through the power supply and the voltage reference. Neural networks were previously used to perform PSA on encryption engines [9], but this work is the first demonstration of applying neural networks for ADC PSA.

The proposed PSA technique shows that an attacker can easily reveal the A/D conversion results of a SAR ADC through the power supply current without a direct access to the reference-charge side-channel, due to the on-chip reference buffer. In typical SAR ADCs, the power side-channel leakage occurs not only through the reference charge current, but also through the comparator and the SAR logic. The prototype secure SAR ADC we report here protects all ADC blocks from leaking digitized data via their power side-channels by employing current equalizers [3], [4].

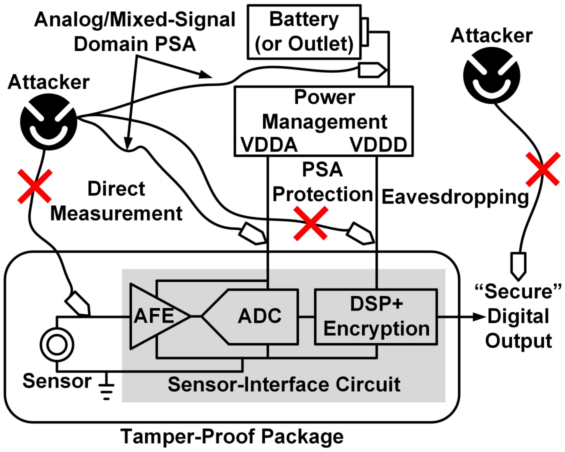


Fig. 1. Potential security threats in sensor hardware.

The rest of this paper is organized as follows. Section II describes the proposed neural-network-based SAR ADC PSA method. Section III provides circuit implementation details of the prototype SAR ADC. Section IV presents the measurement results and Section V concludes the paper.

II. Neural-network-based SAR ADC PSA Method

When performing a PSA on a SAR ADC, an attacker needs a mapping function that converts an ADC supply current waveform into the corresponding A/D conversion result. Based on an assumption that the target ADC is an off-the-shelf product, the attacker can obtain an ADC device of the same part number and perform profiling to build the mapping function. After that, the prepared mapping function is used to perform the PSA on the actual target ADC device.

Fig. 2(a) illustrates the profiling step of the proposed neural-network-based SAR ADC PSA method. After obtaining a training ADC, training data are collected. The training ADC is exercised with a full-scale training signal and the ADC supply current waveforms with their corresponding ADC outputs are simultaneously acquired. In our experiment, a ramp signal is used for training. From the raw supply current waveforms, feature vectors are extracted and then paired with corresponding ADC outputs to build training data. For every

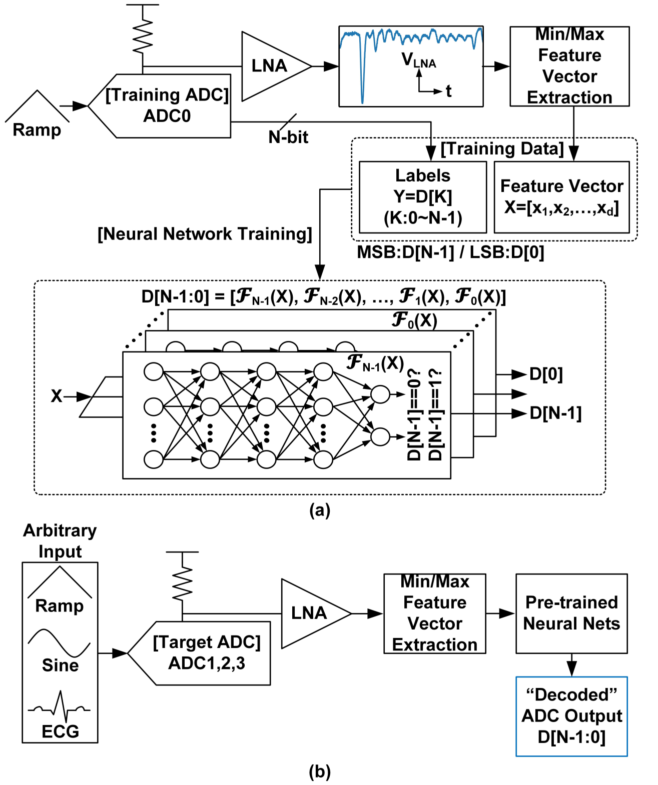


Fig. 2. Two steps of the proposed SAR ADC PSA: (a) Profiling step (b) Attacking step.

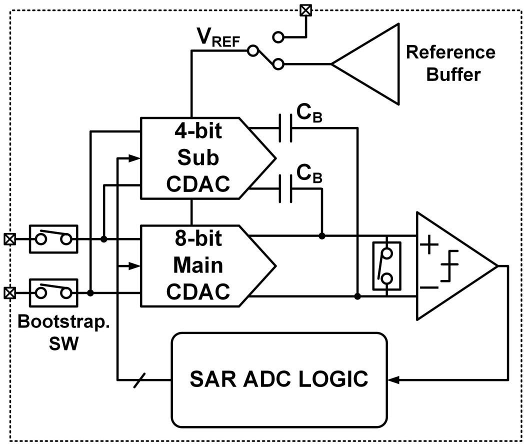


Fig. 3. Unprotected SAR ADC core architecture.

half clock period of the SAR ADC clock from the 2nd CDAC switching to the LSB bit-decision loading on the SAR logic, the instantaneous maximum and minimum values of the supply current waveform are extracted as elements of one feature vector. After training data acquisition, the mapping function is implemented by using multiple neural networks. To attack an N-bit SAR ADC, the mapping function consists of N fully-connected neural networks ($\mathcal{F}_{N-1}, \mathcal{F}_{N-2}, ..., \mathcal{F}_0$) where each of them infers different bit positions of A/D conversion result for the given feature vector. Each neural network comprises 3 hidden layers and each hidden layer consists of 100 neurons. The neural networks are trained offline. The trained neural networks are used to decode supply current waveforms of the target SAR ADC. The attacking step of the proposed SAR ADC PSA method is shown in Fig. 2(b). The supply current of the target ADC is measured and the feature vectors are extracted in the same way. By using the pre-trained neural networks ($\mathcal{F}_{N-1} \sim \mathcal{F}_0$), the feature vectors are decoded into the ADC output bits of the target ADC.

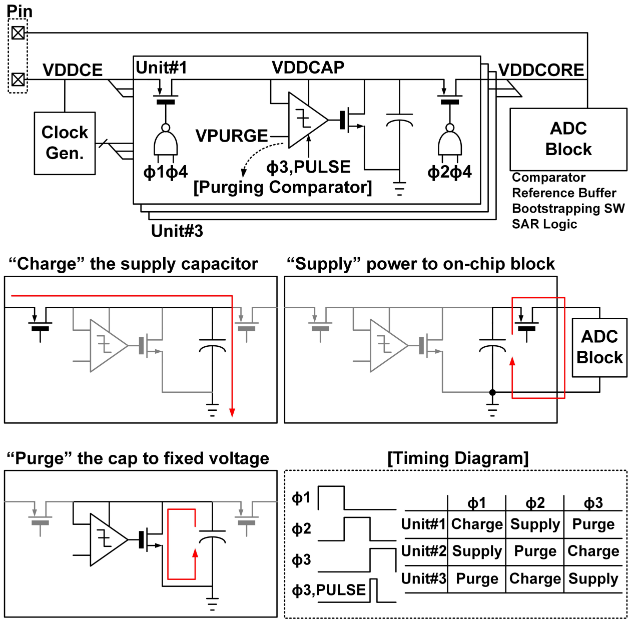
III. Circuit Implementation

A. SAR ADC Core

The prototype SAR ADC comprises a 12-bit, unprotected SAR ADC core and current equalizers for PSA protection. Fig. 3 illustrates the architecture of the fully-differential 12-bit SAR ADC core. The ADC operates synchronously and needs 16 clock periods to perform 1 A/D conversion. The ADC consists of a capacitive DAC (CDAC), a dynamic comparator, a reference buffer, bootstrapping switches, and a SAR logic. The CDAC consists of an 8-bit main-CDAC and a 4-bit sub-CDAC. Split-capacitor switching scheme [5] is used to reduce capacitor switching energy. A dynamic comparator [6] and an on-chip reference buffer based on flipped voltage follower [7] are included. The reference buffer prevents the attacker from accessing the reference-charge side-channel directly. For 12-bit performance, the loop gain of the reference buffer is increased by adding a telescopic opamp. Bootstrapping switches are used to enhance the linearity of sampling network and conventional SAR logic governs overall A/D conversion process of the prototype ADC.

B. Current Equalizer

To protect the SAR ADC from the proposed PSA method, every block of the ADC is equipped with a current equalizer shown in Fig. 4. Current equalizer is a circuit that was originally proposed to protect an AES encryption engine from PSA by de-correlating the on-chip activity and the power drawn from an off-chip supply [3]. Once enabled (Φ4=1), three identical switched-capacitor units of a current equalizer alternate three operations in a time-multiplexed manner: 1) charging a supply capacitor from an off-chip power source (VDDCE), 2) supplying power to the ADC block, and 3) purging the supply capacitor to a fixed voltage, which significantly reduces the correlation between the activity of the ADC block (VDDCORE) and the next charging current waveform drawn from the off-chip power source (VDDCE). During the supplying operation and purging operation, the switched-capacitor unit circulates its current within the on-chip current loop and thereby hides its on-chip activity from off-chip observation. The clock generator of a current equalizer is powered by VDDCE as it does not leak information. On the other hand, the purging comparator is powered by the supply capacitor of each switched-capacitor unit (VDDCAP) to avoid creating timing side-channel leakage [4]. The current equalizers for the reference buffer, comparator, bootstrapping switch, and logic contain 41pF, 2pF, 3pF, and 12pF switched-capacitor



	ϕ1	ϕ2	ϕ3
Unit#1	Charge	Supply	Purge
Unit#2	Supply	Purge	Charge
Unit#3	Purge	Charge	Supply

Fig. 4. Current equalizer and its operations.

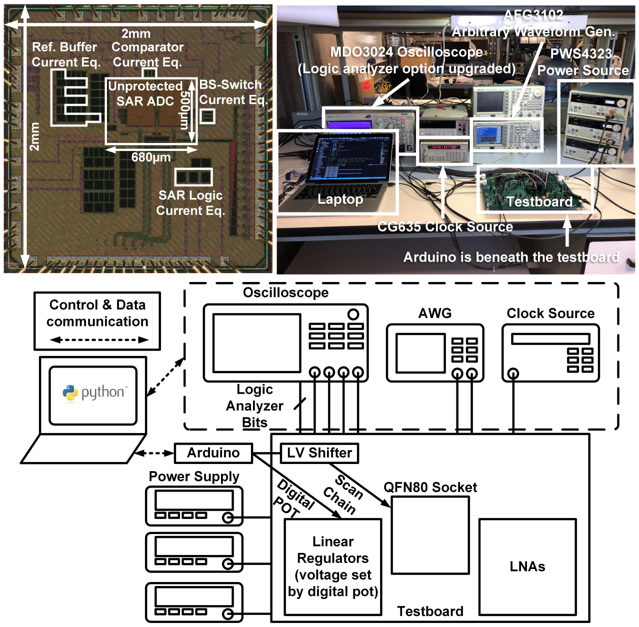


Fig. 5. Chip micrograph and measurement setup.

units, respectively. In addition, only for the current equalizer of the reference buffer, a 10pF switchable decoupling capacitor is employed to ensure smooth supply capacitor transitions. To reduce the power overhead from purging operation, clock gating was used so that only 12, 2, and 5 purging operations are performed throughout 1 A/D conversion in comparator, bootstrapping switch, and SAR logic current equalizers, respectively.

IV. Measurement Results

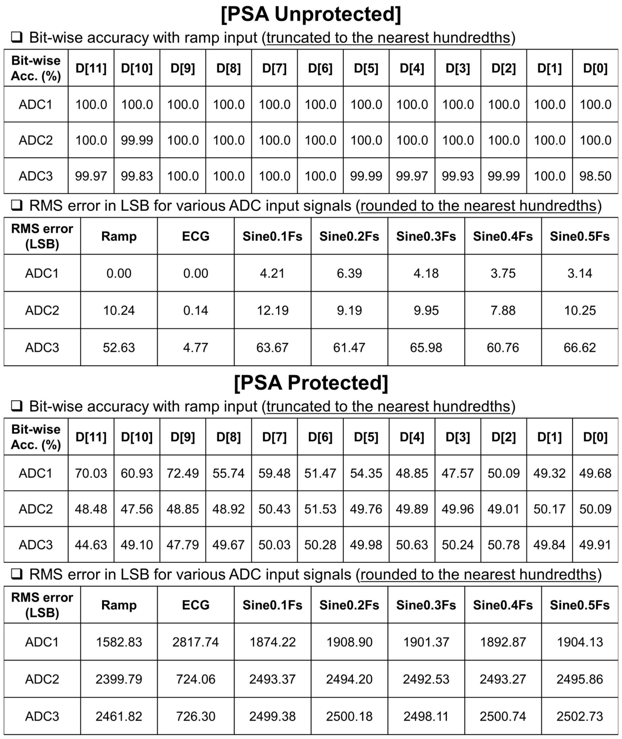
The die photo of the prototype SAR ADC in 65nm CMOS is shown in Fig. 5. The unprotected ADC core occupies 0.34mm^2 and the total area including all protection circuitry is 0.50mm^2.

A. PSA Results

The proposed PSA has been performed by measuring two supply current waveforms. One is the combined supply current waveform of the reference buffer, the comparator, and the bootstrapping switches. Another is the supply current waveform of the SAR logic. The supply current of the IO drivers is not included in our PSA experiments. This is because, in an actual sensor node, the ADC output usually drives on-chip digital circuits such as a DSP or an encryption engine without going through I/O pads. When PSA is performed on the unprotected mode of the ADC, the ADC is powered by separate VDDCORE pins after disabling all current equalizers by pulling $\Phi 4$ down to low (Fig. 4). With one ADC (ADC0 of Fig. 2(a)) used as a training ADC that samples a ramp signal, 500K feature vector-ADC output pairs are collected as training data and used to train neural networks. The pre-trained neural networks are tested on three different target ADCs (ADC1$\sim$3 of Fig. 2(a)) that sample 7 different waveforms (ramp, sine of 5 different frequencies, ECG [8]). For each test input signal, 50K supply current waveforms are decoded and compared against their true ADC output values. When PSA is performed on the protected mode of the ADC, the VDDCORE pins are all disconnected, and only VDDCE pins are connected to the external power supply. Same as unprotected mode PSA, training data are collected again to re-train the neural networks. Then, the re-trained neural networks are used to perform the same tests as unprotected mode PSA.

Table. I shows the PSA results on unprotected and protected modes of the ADC. The PSA results are quantified in two ways. The bit-wise accuracy with ramp input shows how the neural network for each bit of ADC output performs independently. The RMS error shows the difference between the attack results and the true ADC outputs. The unprotected bit-wise accuracy results of target ADCs demonstrate that the proposed PSA method can accurately reconstruct the 12-bit true digitized waveform. The RMS error of ADC3 is higher than other target ADCs due to the small bit-wise accuracy drop in MSBs. Previous template attack on 10-bit, unprotected ADC [2] extracted first 6 MSBs with 4.6 effective number of bits (ENOB) on sinusoid input. The protected bit-wise accuracy results are close to the random guess of 50% except for the first three MSBs of ADC1. The protected PSA results show that the current equalizers significantly reduce the power side-channel leakage of the prototype ADC to the point where the recovered signals have little correlation to the true signal. Although ADC1's protected bit-wise accuracy of the first three MSBs are higher than 50%, their large weights and high error rates render the attack ineffective. The large RMS errors indicate that the original waveform cannot be reconstructed from the power side-channel leakage after protection. In Fig. 6, for an actual ECG signal [8], the unprotected PSA results

TABLE I
PSA RESULTS OF UNPROTECTED AND PROTECTED VERSIONS OF THREE DIFFERENT ADCS (D[11]:MSB, D[0]:LSB)



[PSA Unprotected]

❑ Bit-wise accuracy with ramp input (truncated to the nearest hundredths)

Bit-wise Acc. (%)	D[11]	D[10]	D[9]	D[8]	D[7]	D[6]	D[5]	D[4]	D[3]	D[2]	D[1]	D[0]
ADC1	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0
ADC2	100.0	99.99	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0
ADC3	99.97	99.83	100.0	100.0	100.0	100.0	99.99	99.97	99.93	99.99	100.0	98.50

❑ RMS error in LSB for various ADC input signals (rounded to the nearest hundredths)

RMS error (LSB)	Ramp	ECG	Sine0.1Fs	Sine0.2Fs	Sine0.3Fs	Sine0.4Fs	Sine0.5Fs
ADC1	0.00	0.00	4.21	6.39	4.18	3.75	3.14
ADC2	10.24	0.14	12.19	9.19	9.95	7.88	10.25
ADC3	52.63	4.77	63.67	61.47	65.98	60.76	66.62

[PSA Protected]

❑ Bit-wise accuracy with ramp input (truncated to the nearest hundredths)

Bit-wise Acc. (%)	D[11]	D[10]	D[9]	D[8]	D[7]	D[6]	D[5]	D[4]	D[3]	D[2]	D[1]	D[0]
ADC1	70.03	60.93	72.49	55.74	59.48	51.47	54.35	48.85	47.57	50.09	49.32	49.68
ADC2	48.48	47.56	48.85	48.92	50.43	51.53	49.76	49.89	49.96	49.01	50.17	50.09
ADC3	44.63	49.10	47.79	49.67	50.03	50.28	49.98	50.63	50.24	50.78	49.84	49.91

❑ RMS error in LSB for various ADC input signals (rounded to the nearest hundredths)

RMS error (LSB)	Ramp	ECG	Sine0.1Fs	Sine0.2Fs	Sine0.3Fs	Sine0.4Fs	Sine0.5Fs
ADC1	1582.83	2817.74	1874.22	1908.90	1901.37	1892.87	1904.13
ADC2	2399.79	724.06	2493.37	2494.20	2492.53	2493.27	2495.86
ADC3	2461.82	726.30	2499.38	2500.18	2498.11	2500.74	2502.73

match the true waveform precisely. After protection, PSA results appear random. This is in contrast to the previous work, which showed the attack result still leaked the MSB of the input sinusoid signal after protection [2]. We also conducted PSA on GND current waveforms and found that the GND-side leakage was very weak in general, for both unprotected and protected versions of the ADC. The proposed PSA attack method has also been demonstrated in two different commercial 12-bit SAR ADC products from two different manufacturers exhibiting better than 99% ramp-signal bit-wise attack accuracy except the two last LSBs.

B. ADC Performance

ADC performance before and after PSA protection is summarized in Table. II. With an on-chip reference buffer, the unprotected and the protected versions of the ADC achieve SNDR of 69.3dB and 69.2dB, respectively. After protection, the INL slightly degrades from -0.87/+0.80 LSB to -1.01/+0.86 LSB. This is expected because of the voltage droop on the supply capacitors during the conversion. Before and after protection, the ADC draws 83.2μW and 158.5μW from a 1.2V power supply, which are translated to FoMs of 27.9fJ/c.-s. and 54.3fJ/c.-s., respectively.

V. CONCLUSIONS

This paper demonstrates a neural-network-based SAR ADC PSA method that can extract A/D conversion results from ADC supply current waveforms with high accuracy and a current-equalizer-based PSA protection scheme that protects all ADC blocks from the proposed PSA method.

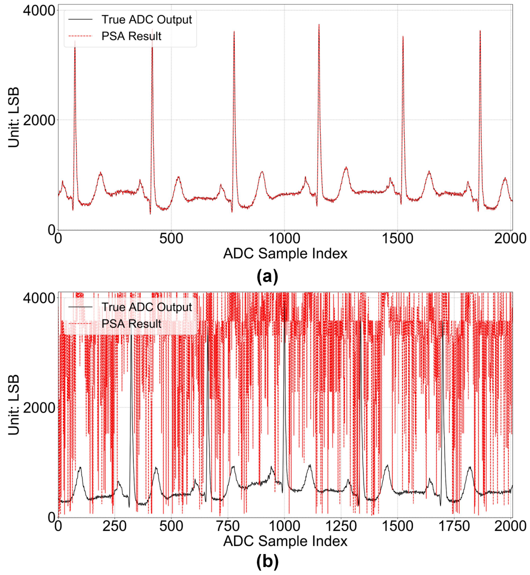
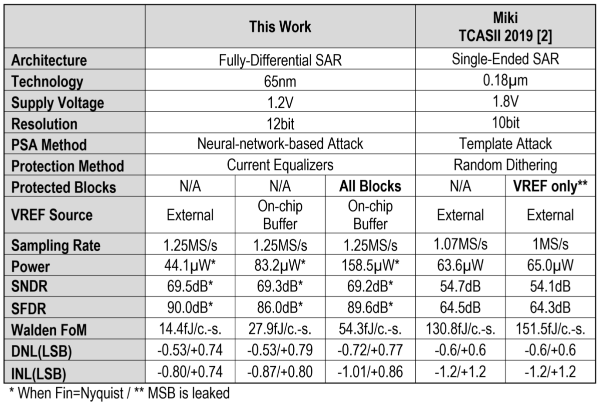


Fig. 6. Example time domain plot of PSA results (ADC1, ECG input) (a) Unprotected (50K sample RMS error: 0.00 LSB) (b) Protected (50K sample RMS error: 2817.74 LSB).

TABLE II
SUMMARY OF ADC PERFORMANCE



	This Work			Miki TCASII 2019 [2]	
Architecture	Fully-Differential SAR			Single-Ended SAR	
Technology	65nm			0.18μm	
Supply Voltage	1.2V			1.8V	
Resolution	12bit			10bit	
PSA Method	Neural-network-based Attack			Template Attack	
Protection Method	Current Equalizers			Random Dithering	
Protected Blocks	N/A	N/A	**All Blocks**	N/A	**VREF only****
VREF Source	External	On-chip Buffer	On-chip Buffer	External	External
Sampling Rate	1.25MS/s	1.25MS/s	1.25MS/s	1.07MS/s	1MS/s
Power	44.1μW*	83.2μW*	158.5μW*	63.6μW	65.0μW
SNDR	69.5dB*	69.3dB*	69.2dB*	54.7dB	54.1dB
SFDR	90.0dB*	86.0dB*	89.6dB*	64.5dB	64.3dB
Walden FoM	14.4fJ/c.-s.	27.9fJ/c.-s.	54.3fJ/c.-s.	130.8fJ/c.-s.	151.5fJ/c.-s.
DNL(LSB)	-0.53/+0.74	-0.53/+0.79	-0.72/+0.77	-0.6/+0.6	-0.6/+0.6
INL(LSB)	-0.80/+0.74	-0.87/+0.80	-1.01/+0.86	-1.2/+1.2	-1.2/+1.2

* When Fin=Nyquist / ** MSB is leaked

ACKNOWLEDGMENT

This research was supported by Analog Devices Inc., TSMC University Shuttle Program, MIT CICS, and Korea Foundation for Advanced Studies (KFAS).

REFERENCES

[1] V. V. Gadde, *et al.*, ASSCC, pp. 123-126, Nov. 2018.
[2] T. Miki, *et al.*, Trans. Circuits Syst. II (Early Access), 2019.
[3] C. Tokunaga and D. Blaauw, ISSCC, pp. 64-65, Feb. 2009.
[4] N. Miura, *et al.*, ASSCC, pp. 225-228, Nov. 2014.
[5] M. Yip and A. P. Chandrakasan, JSSC, vol. 48, no. 6, pp. 1453-1463, Jun. 2013.
[6] M. Miyahara, *et al.*, ASSCC, pp. 269-272, Nov. 2008.
[7] R. G. Carvajal, *et al.*, Trans. Circuits Syst. I, vol. 52, no. 7, pp. 1276-1291, Jul. 2005.
[8] A. L. Goldberger, *et al.*, Circulation, pp. e215-e220, Jun. 2000.
[9] R. Gilmore, *et al.*, HOST, pp. 106-111, May 2015.