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

Taehoon Jeong, Member, IEEE, Anantha P. Chandrakasan, Fellow, IEEE, and Hae-Seung Lee, Life Fellow, IEEE

Abstract—When an ADC is converting a confidential analog signal into digital codes, it may expose a critical hardware security loophole. By exploiting the strong correlation between the ADC digital output codes and the ADC supply current waveforms, an attacker can perform an ADC power side-channel attack (PSA) to steal the sensitive A/D conversion results by tapping into the power supply of the ADC. In this regard, this article demonstrates two neural-network-based successive approximation register (SAR) ADC PSA methods and a 12-bit, 1.25-MS/s prototype SAR ADC with current-equalizer-based PSA protection. The first ADC PSA method employs multi-layer perceptron networks (MLP-PSA), while the second ADC PSA method uses convolutional neural networks (CNN-PSA). With the protection disabled, both MLP-PSA and CNN-PSA extract the A/D conversion results from the ADC supply current waveforms with >99% bit-wise accuracy. With the protection enabled, strong PSA-resistance against MLP-PSA is demonstrated. The same SAR ADC exhibits weaker PSA-resistance against CNN-PSA but generally provides significant protection of A/D conversion results.

Index Terms—Analog-to-digital converter (ADC), convolutional neural network (CNN), current equalizer, multi-layer perceptron (MLP), neural network, power side-channel attack (PSA), successive approximation register (SAR) ADC.

I. INTRODUCTION

A HARDWARE security loophole exists at the mixed-signal interface between analog circuits and a digital processor. Recent studies [1]–[3] have discovered that an analog-to-digital converter (ADC) can expose a critical security loophole by leaking the confidential signal data through its supply current waveforms or electromagnetic emissions. Considering a wide range of ADC applications, identifying and removing ADC-related security vulnerabilities are important to enhance the information security of the entire signal chain.

Fig. 1 illustrates an example ADC PSA scenario for sensor applications. It is assumed that the attacker can physically access the target sensor hardware. Once the ADC of sensor hardware digitizes the confidential sensor output signal (e.g., healthcare), data encryption [4], [5] can protect the sensitive data from eavesdropping. To break the data encryption, an attacker can try to extract the secret key of the encryption algorithm from the supply current waveforms of the encryption engine by performing a security attack referred to as a power side-channel attack (PSA). However, established digital PSA countermeasure schemes [6]–[11] can be used to protect the encryption engine from the PSA. The attacker can then try to tap into the sensor output node and measure the analog sensor signal, but a tamper-proof package can prevent the direct measurement [1]. Even without a tamper-proof package, the attacker cannot avoid disturbing the sensitive analog signal chain due to the high sensor output impedance [2]. Instead, the attacker can perform a PSA on analog/mixed-signal circuits, especially on ADCs. The strong correlation between an A/D conversion process and the resulting digital output code allows the attacker to gain the desired information by monitoring the ADC supply current waveforms. Due to the battery replacement or form factor limitation, enclosing the entire sensor hardware and the power source with a tamper-proof package might not be practical as an analog/mixed-signal circuit PSA countermeasure [3].

In this context, the PSA and protection methods of successive approximation register (SAR) ADCs have been...
demonstrated in [2] and [3]. In [2], a template attack reveals the first six MSBs of a 10-bit SAR ADC by monitoring the CDAC reference current waveform, which could be accessed via a separate reference voltage pin. As a protection method against the template attack, large random dithering is injected at the second CDAC capacitor switching to mask the CDAC reference current waveform for the remaining A/D conversion process. However, this countermeasure does not protect the information leakage of other SAR ADC blocks through the power supply pin. In [3], a multi-layer-perceptron-based attack (MLP-PSA) reveals all A/D conversion bits from the supply current waveform of a 12-bit SAR ADC, whose on-chip reference buffer merges the CDAC reference current waveform with the supply current of other analog circuit blocks. The reference buffer removes the separate reference voltage pin, a possible loophole for the direct access to the CDAC reference current waveform, but does not reduce the information leakage of CDAC that is contained in the macro-level supply current waveform. As a protection method against the MLP-PSA, switched-capacitor circuits called current equalizers [8], [9] are employed to reduce the information leakage of the SAR ADC, protecting all vulnerability, including the power supply and ground current waveforms.

This article extends the work presented in [3] with an analysis of the SAR ADC information leakage and experimental PSA results based on a newly proposed convolutional-neural-network-based SAR ADC PSA method (CNN-PSA). Although the work of this article focuses on SAR ADCs, the power side-channel vulnerability may also be found in delta-sigma ADCs or pipelined ADCs if there exists a correlation between ADC digital output codes and ADC supply current waveforms. To attack different types of ADCs, the attacker can extend the proposed neural-network-based SAR ADC PSA approach with appropriate modifications of neural network architecture. More specifically, for a delta-sigma ADC PSA, the attacker can try to extract the raw quantizer output by only inputting the ADC supply current waveform between two oversampling clock edges. For an N-stage pipelined ADC PSA, the attacker may need to input N-consecutive ADC supply current waveforms to extract the corresponding ADC digital output code of the first ADC supply current waveform.

The rest of this article is organized as follows. Section II reviews the previous MLP-PSA method and introduces the proposed CNN-PSA method. Section III describes the unprotected SAR ADC core of the prototype SAR ADC and analyzes primary information leakage sources of the SAR ADC. Section IV explains the current-equalizer-based ADC PSA protection scheme. Section V presents the measurement results with a discussion on possible second-order information leakage sources of a current equalizer. Finally, Section VI concludes this article.

II. NEURAL-NETWORK-BASED SAR ADC PSA METHODS

A. MLP-PSA

Fig. 2(a) illustrates the two steps of the previously proposed MLP-PSA [3]. To perform a PSA on the target ADC, an attacker needs a mapping function that converts a supply current waveform of the target ADC into the corresponding ADC digital output code. The first step of MLP-PSA is the profiling step where an attacker prepares the mapping function by using a training ADC. The profiling step starts with training data collection. If the target ADC is an off-the-shelf product, the attacker can obtain a training ADC that is nominally identical to the target ADC and runs the training ADC to convert a training signal. The training signal should ideally span the full input signal range of the ADC to cover all ADC digital output codes. For every A/D conversion of the training ADC, an instantaneous ADC supply current waveform and its corresponding ADC digital output code are obtained. From the ADC supply current waveform, a min/max feature vector is extracted to perform the MLP-PSA. Based on the intuition that a SAR ADC supply current waveform mainly consists of a capacitor switching current and a crowbar current that become most distinctive at their peaks, the minimum and maximum supply current values within a half SAR ADC clock period are extracted as elements of a min/max feature vector. A large number of min/max feature vector-ADC digital output code pairs constitute the training data. After training data collection, the mapping function is implemented by using multiple MLP networks [12]. For an N-bit SAR ADC PSA, the mapping function is built upon N MLP networks \((\mathcal{F}_{N-1}, \mathcal{F}_{N-2}, \ldots, \mathcal{F}_0)\) where each of them performs a binary classification to decode each bit of the A/D conversion result for the shared min/max feature vector input \((x)\). Each bit-wise MLP network contains three fully connected hidden layers with 100 neurons and rectified linear (ReLU) activation and an output layer with two neurons and softmax activation. With the acquired training data, the MLP networks are trained offline. In practice, before being fed into the neural networks, the min/max feature vectors are linearly re-scaled to make all elements of a min/max feature vector span similar ranges [13].

The second step of MLP-PSA, the attacking step, is also shown in Fig. 2(a). The attacker accesses the target ADC that is converting an unknown input signal. The attacker measures the supply current waveforms of the target ADC and extracts min/max feature vectors in the same way. By using the pre-trained neural networks of the profiling step, the extracted feature vectors are decoded into the digital output codes of the target ADC.

B. CNN-PSA

The proposed CNN-PSA also consists of the two steps that are the same as the MLP-PSA. The key difference between the CNN-PSA and the MLP-PSA is the bit-wise neural network architecture that is used to implement the mapping function. As shown in Fig. 2(b), the CNN-PSA implements its mapping function by using CNNs whose shared input is the raw ADC supply current waveform \((v_{LNA} \text{ of Fig. 2})\). In contrast to the MLP-PSA that relies on a heuristic min/max feature vector extraction, the CNN-PSA makes its CNNs find the most informative feature vectors by themselves, in a way that they can fully exploit the details of a raw ADC supply current waveform. The frontend convolutional layers, max-pooling layers, and a flattened layer are used as a feature extractor. In a
Fig. 2. Two steps of (a) MLP-PSA and (b) CNN-PSA.

bit-wise CNN, each convolutional layer has five filters whose kernel size, stride, and activation function are 5, 1, and ReLU, respectively. The pooling size and stride of max-pooling layers are 5 and 5, respectively. The back-end fully connected layers have the same architecture, as described in Section II-A. Similar to MLP-PSA, the raw ADC supply current waveforms are linearly re-scaled to make all half-clock-period waveforms span similar ranges.

III. CIRCUIT IMPLEMENTATION AND INFORMATION LEAKAGE SOURCES OF UNPROTECTED SAR ADC

A. Unprotected SAR ADC Architecture

In this work, the prototype PSA-protected SAR ADC consists of a 12-bit, 1.25-MS/s unprotected SAR ADC core and current equalizers. The architecture of the unprotected SAR ADC is shown in Fig. 3. The ADC employs a fully differential architecture to reject power supply and common-mode disturbances. To improve the linearity of its bottom-plate sampling network, the ADC adopts bootstrapped switches [14]. Once the ADC samples its input voltage, the ADC performs a binary search to find the closest digital representation of its sampled input voltage by using a segmented capacitor DAC [15] and a dynamic comparator [16]. Based on the split-capacitor switching scheme [17], the first eight MSBs are resolved by the main-CDAC, while the remaining four LSBs are determined by the sub-CDAC. A synchronous SAR logic [18] controls the overall A/D conversion process and requires 16 clock periods to perform one A/D conversion. An on-chip reference buffer supplies a reference voltage to CDAC, preventing a side-channel attack through direct access to the CDAC reference current waveforms.
JEONG et al.: S2ADC: A 12-bit, 1.25-MS/s SECURE SAR ADC WITH PSA RESISTANCE

Fig. 3. Unprotected SAR ADC core architecture.

Fig. 4. Single-ended 8 + 4 segmented CDAC using split-capacitor switching scheme.

B. CDAC

Fig. 4 shows the segmented CDAC [19], where a single-ended version is shown for simplicity. To accommodate the split-capacitor switching scheme [17] for energy saving, the MSB capacitor (128C) of the main-CDAC is split into another capacitor array that is identical to the rest of the array [15]. The unit capacitance of the CDAC is 11.3 fF, and the corresponding single-ended sampling capacitance of the SAR ADC is 2.9 pF. The CDAC employs 1 V (V_{REF}) and 0 V (ground) as its positive and negative reference voltages, respectively.

As shown in Fig. 5, the total switching energy of CDAC correlates with part of the ADC digital output code, from the second MSB to the second LSB. More specifically, starting from the third bit-cycling, an arbitrary kth bit-cycling CDAC switching energy correlates with the A/D conversion result from the second MSB to the (k − 1)th MSB. Since there is no CDAC switching after the LSB decision of the comparator, the CDAC switching energy does not leak the LSB of the ADC digital output code.

C. Comparator

The dynamic comparator is shown in Fig. 6 [16]. The comparator consists of a two-stage dynamic preamplifier and a regenerative latch. An RS-latch is employed to hold the bit-decision result (D_{OUT}) during the resetting phase of the comparator.

Fig. 7 illustrates the information leakage of the comparator. First, both bit-decision energy (E_{BDc}) and resetting energy (E_{RST}) depend on the magnitude of differential comparator input voltage \( |V_{DACP} - V_{DACN}| \). Since \( |V_{DACP} - V_{DACN}| \) is determined by the sampled ADC input voltage and the previous bit-decision results of the comparator, the comparator energy correlates with the ADC digital output code. Second, due to the asymmetric loading capacitor, the RS-latch also consumes a different amount of energy depending on the change between the two consecutive comparator bit-decision results. Combined with the information leakage of the CDAC, the information leakage of the comparator and the RS-latch can be used to infer the MSB and the LSB.

D. SAR Logic

Fig. 8 shows that the SAR logic whose logic gates are not shown for simplicity [18]. The sequencer triggers each
operation of the A/D conversion process by sequentially raising its flip-flop outputs from 0 to 1, but its energy does not correlate with the ADC digital output code. The switch controller controls CDAC switches, and its energy correlates with the ADC digital output code since its registers consume a different amount of power depending on the comparator bit-decision result (D_OUT).

IV. CURRENT-EQUALIZER-BASED ADC PSA PROTECTION

Fig. 9(a) shows the current equalizer used in the PSA-protected prototype SAR ADC. Originally developed as an encryption engine PSA countermeasure [8], [9], the current equalizer equalizes the off-chip-drawn supply current waveforms regardless of different on-chip circuit activities, thereby reducing the information leakage of the PSA-protected circuit. In the prototype SAR ADC, the reference buffer, comparator, bootstrapped switches, and SAR logic are equipped with their own current equalizers. In real systems, a metal tamper-proof package or an \( LC \)-oscillator-based sensor [20] can also be employed to complement current equalizers against EM side-channel attack. When an ADC PSA is performed on the unprotected mode SAR ADC, all current equalizers are disabled (4 = 0), and the ADC blocks are powered by using separate VDDCORE pins. When an ADC PSA is performed on the protected mode SAR ADC, all current equalizers are enabled (4 = 1) and powered by using VDDCE pins. VDDCORE pins are disconnected from the off-chip power source.

Each current equalizer consists of three identical switched-capacitor units and a clock generator. When the current equalizer is enabled (4 = 1), each switched-capacitor unit performs one of the three operations in a time-interleaved manner, which is illustrated in Fig. 9(b): 1) charge; 2) supply; and 3) purge. During the charge operation (4 = 1 for Unit#1), a switched-capacitor unit pre-charges its supply capacitor to the full supply voltage level by drawing power from an off-chip power source. During the supply operation (4 = 1 for Unit#1), the unit powers its corresponding ADC block. After the supply operation, the leftover voltage on the supply capacitor correlates with the activity of the ADC block. During the purge operation (4 = 1 for Unit#1), the unit purges its supply capacitor to a fixed voltage by using a shunt switch and a purging comparator. By doing so, the current drawn from the off-chip power source during the next charge operation gets equalized since the off-chip power source not only supplies the same amount of charge but the load impedance seen from the off-chip power source is always constant. During the supply and the purge operations, the current of the unit only circulates within the on-chip current loop to cancel out the opposite charge on the two capacitor plates. Hence, the on-chip ground node only serves as a voltage reference node, and no leakage current conducts through the ground node.

The detailed circuit implementations of the purging comparator and the clock generator are shown in Fig. 10. As shown in Fig. 9(a), an off-chip power source (VDDCE) directly powers the clock generator of a current equalizer since the activity of the clock generator does not correlate with the A/D conversion process. However, if the purging comparator of a switched-capacitor unit is directly powered by the VDDCE pin, an attacker may monitor the duration of purge operation and infer the initial leftover voltage of the supply capacitor.
to correlate it with the ADC activity [9]. To prevent this second-order timing side-channel attack, the supply capacitor of each switched-capacitor unit powers the purging comparator of the same unit. When the purge operation starts ($\Phi_3 = 1$ for Unit#1), a 1-ns-width pulse ($\Phi_{3,PULSE} = 1$) is produced to turn the diode-connected level shifter (M0 and M1) and the shunt switch ON ($EN = 1$) without being affected by the level of initial $VOUT$ node voltage. After the $\Phi_{3,PULSE}$ becomes 0, $VLV$, a level-shifted version of $VDDCAP$, still maintains a higher voltage level than $VPURGE$ and keeps the shunt switch purging the supply capacitor ($EN = 1$). Once $VLV$ becomes lower than $VPURGE$, the purging comparator pulls down $EN$ to the ground ($EN = 0$), thereby completing the purge operation.

Each switched-capacitor unit of the current equalizers for the reference buffer, the comparator, the bootstrapping switch, and the SAR logic have an MoM supply capacitor of 41, 2, 3, and 12 pF, respectively. Also, when the reference buffer is powered by its current equalizer, a 10-pF switchable decoupling capacitor is enabled and connected to $VDDCORE$ of the reference buffer to ensure smooth supply capacitor transitions. During one A/D conversion, the current equalizers for the reference buffer, the comparator, the bootstrapping switch, and the SAR logic perform 16, 12, two, and five supply capacitor transitions. The current equalizers for dynamic-power-consuming ADC blocks execute less supply capacitor transitions to reduce the power overhead of the purge operation.

V. MEASUREMENT RESULTS

This section presents the measurement results of the prototype SAR ADC. The die photograph and the measurement setup of the prototype SAR ADC are shown in Fig. 11. The unprotected ADC core occupies 0.34 mm$^2$, and the total area, including all protection circuitry, is 0.50 mm$^2$.

A. PSA Results

1) Experimental Setting: As a proof of concept of the neural-network-based ADC PSA approach, VDD-side MLP-PSA experiments have been first performed on two 12-bit, 1.25-MS/s prototype SAR ADCs from different manufacturers (ADC-A and ADC-B). ADC-A and ADC-B are not equipped with PSA countermeasures and run at 1.0 and 0.8 MS/s, respectively. The commercial ADC PSA experiments are performed by only measuring the ADC core supply current waveforms. A series resistor and a low-noise amplifier (LNA) are employed to convert the current into voltage waveform and amplify the voltage waveform, respectively. The series resistances of ADC-A and ADC-B are heuristically determined as 10 and 39 $\Omega$, respectively. LNA gains are the same as 10.

The LNA output waveforms are digitized by a 2.5-GS/s oscilloscope with an input bandwidth of 20 MHz. For each commercial ADC, the training data set is acquired separately, and hence, the mapping functions are also separately trained based on different training data set.

Both MLP-PSA and CNN-PSA are used to attack the 12-bit, 1.25-MS/s prototype SAR ADC. For each PSA method, four different PSA experiments are performed, including VDD-side and GND-side attacks conducted on the unprotected and protected modes of the prototype SAR ADC. The prototype ADC PSA experiments are done by measuring two supply current waveforms: 1) the combined supply current waveform of analog circuit blocks (reference buffer, comparator, and bootstrapped switches) and 2) the SAR logic supply current waveform. The two supply current waveforms are acquired by using 33- and 200-MHz oscilloscope bandwidth. During PSA experiments, it was heuristically found that using 20-MHz oscilloscope bandwidth for the combined analog supply current waveform measurements generally improves the unprotected mode PSA results. The SAR logic supply current waveforms are measured with 200-MHz oscilloscope bandwidth. To focus on the major experimental results, the attack results with 20-MHz analog supply current bandwidth setting are only presented.
MLP-PSA: VDD-SIDE, COMMERCIAL ADCs (D[11]:MSB, D[0]:LSB).
(a) ADC-A. (b) ADC-B

| Bit-wise accuracies with ramp input (routed 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 | 99.99 | 100.0 | 100.0 | 99.98 | 99.99 | 99.99 | 99.80 | 99.79 |
| ADC2                   | 100.0 | 100.0 | 99.98 | 100.0 | 99.99 | 100.0 | 99.96 | 99.98 | 99.94 | 99.99 | 99.93 | 99.96 |
| ADC3                   | 100.0 | 100.0 | 99.93 | 99.99 | 99.73 | 99.97 | 99.72 | 99.63 | 99.83 | 99.07 | 99.42 |
| RMS error in LSB for various ADC input signals (routed to the nearest hundredths) |
|-------------------------|------------------|------------------|------------------|------------------|------------------|------------------|
| RMS error (LSB)         | Ramp | ECG | Sine0.1Fs | Sine0.2Fs | Sine0.3Fs | Sine0.4Fs | Sine0.5Fs |
| ADC1                   | 1.62  | 1.62 | 6.52      | 49.34       | 6.63       | 10.01       | 20.19        |
| ADC2                   | 5.69  | 1.09 | 7.92      | 21.62       | 12.88      | 11.17       | 4.50         |
| ADC3                   | 15.20 | 5.28 | 16.54     | 15.72       | 20.19      | 20.79       | 21.43        |

To utilize the two supply current waveforms, the mapping functions are slightly modified from Section II. For MLP-PSA, the two min/max feature vectors are concatenated as a single vector and then provided to each bit-wise MLP neural network. For CNN-PSA, in each bit-wise neural network, the two raw supply current waveforms are processed by different feature extractors. Each feature extractor has the same convolutional layers, max-pooling layers, and a flatten layer described in Section II-B. Similar to MLP-PSA, the output vectors of the flatten layers are concatenated as a single vector and then fed into the back-end fully connected layers. Neural networks are re-trained for each PSA experiment. The neural networks for the unprotected mode MLP-PSA and CNN-PSA are trained by using the training data collected from the unprotected mode SAR ADC. The neural networks for the protected mode MLP-PSA and CNN-PSA are trained by using the training data collected from the protected mode SAR ADC.

Each training data set is collected from one training ADC that is converting a full-scale ramp signal. 500K feature vectors (or raw power traces)–ADC digital output code pairs constitute a training data set. With the pre-trained neural networks, three different target ADCs (ADC1-3) that are nominally identical to the training ADC are attacked. When a PSA is performed on a target ADC, seven different input signals are tested (ramp signal and sine waves whose frequencies are 0.1/0.2/0.3/0.4/0.5× of the ADC sampling rate and an ECG signal [21]). Each test input case consists of 50k feature vectors (or raw power traces) that are decoded into the corresponding ADC digital output codes and compared against the true ADC digital output codes.

The ADC PSA results are quantified in two different ways. The first is the bit-wise accuracy with a ramp input signal, and the second is the root-mean-square error (rms error) between the PSA results and the true ADC digital output codes. The bit-wise accuracy quantifies the independent performance of a bit-wise neural network, while the rms error quantifies the performance of the entire mapping function.

2) MLP-PSA Results for Commercial SAR ADCs: Table I shows the VDD-side MLP-PSA results on the two commercial ADCs. Overall, the neural-network-based ADC PSA approach is successfully demonstrated on commercial SAR ADCs. For all target ADCs of ADC-A and ADC-B, the ramp-signal bit-wise accuracy is shown to be higher than 99% for all bits from the MSB (D[11]) to the LSB (D[0]).

3) MLP-PSA Results for Unprotected Prototype SAR ADC: Table II shows the VDD-side and GND-side MLP-PSA results on the prototype SAR ADC in the unprotected mode. Along with the MLP-PSA results of Table I, the VDD-side results of Table II(a) demonstrate that the VDD-side MLP-PSA can accurately decode the supply current waveforms of an arbitrary SAR ADC into the corresponding ADC digital output codes. For all target ADCs, the VDD-side ramp-signal bit-wise accuracy is shown to be higher than 99% for all bits. The GND-side results of Table II(b) indicate that the GND-side supply current waveforms of the prototype SAR ADC reveal less information than the VDD-side supply waveforms.
TABLE III
MLP-PSA: PROTECTED MODE (D[11]:MSB, D[0]:LSB).
(a) VDD-SIDE. (b) GND-SIDE

|                | Ramp | ECG | Sine0.1Fs | Sine0.2Fs | Sine0.3Fs | Sine0.4Fs | Sine0.5Fs |
|----------------|------|-----|-----------|-----------|-----------|-----------|-----------|
| **ADC1**       | 1588.23 | 2842.10 | 1973.91 | 2039.24 | 2123.93 | 2200.26 | 2229.23 |
| **ADC2**       | 2354.75 | 723.55 | 2469.44 | 2485.29 | 2482.69 | 2489.03 | 2491.63 |
| **ADC3**       | 2410.12 | 722.52 | 2447.22 | 2455.66 | 2484.17 | 2488.62 | 2487.80 |
| **RMS error in LSB for various ADC input signals (rounded to the nearest hundredths)** | | | | | | | |
| **ADC1**       | 84.33 | 85.61 | 90.66 | 82.63 | 93.95 | 95.17 | 96.96 |
| **ADC2**       | 81.54 | 70.28 | 76.27 | 78.15 | 85.05 | 70.62 | 74.70 |
| **ADC3**       | 70.92 | 75.24 | 79.78 | 82.34 | 74.32 | 72.54 | 53.97 |
| **RMS error in LSB for various ADC input signals (rounded to the nearest hundredths)** | | | | | | | |

Fig. 12. Time domain plot of VDD-side MLP-PSA results (Target ADC1 of prototype SAR ADC. ECG input, and 20-MHz setting). Top: unprotected (50k sample rms error: 0.00 LSB). Bottom: protected (50k sample rms error: 2842.10 LSB).

Table III shows the VDD-side and GND-side MLP-PSA results on the prototype SAR ADC in the protected mode. The overall rms values of Table III indicate that current equalizers are providing strong resistance against the VDD-side and GND-side MLP-PSA. Especially, many bit-wise accuracy values of Table III(a) fall close to 50%, which is the bit-wise accuracy of a random binary decision.

For all target ADCs, the GND-side ramp-signal bit-wise accuracy is higher than 95% only from the MSB to the fifth MSB (D[7]). Also, the GND-side shows higher rms error values than the VDD-side.

4) MLP-PSA Results for Protected Prototype SAR ADC: Table III shows the VDD-side and GND-side MLP-PSA results on the prototype SAR ADC in the protected mode. The overall rms values of Table III indicate that current equalizers are providing strong resistance against the VDD-side and GND-side MLP-PSA. Especially, many bit-wise accuracy values of Table III(a) fall close to 50%, which is the bit-wise accuracy of a random binary decision.

Fig. 12 shows the time-domain plots of the true ADC input waveform and the VDD-side MLP-PSA results on the prototype SAR ADC with an ECG input. Without protection, the true ADC input waveform and the PSA result plot overlap each other completely. With protection, the PSA result plot is random and does not disclose useful information of the original ECG signal.

6) CNN-PSA Results for Protected Prototype SAR ADC: Table V shows the VDD-side and GND-side CNN-PSA results on the prototype SAR ADC in the protected mode. The overall rms error values of Table V indicate that current equalizers prevent an attacker from extracting a meaningful
TABLE V
CNN-PSA: PROTECTED MODE (D[11]:MSB, D[0]:LSB).
(a) VDD-SIDE. (b) GND-SIDE

| Bit-wise accuracies with ramp input (tuncated to the nearest hundredths) | D[11] | D[10] | D[9] | D[8] | D[7] | D[6] | D[5] | D[4] | D[3] | D[2] | D[1] | D[0] |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| (a) | Bit-wise Acc. (%) | 99.19 | 91.56 | 98.15 | 90.06 | 73.42 | 96.71 | 97.09 | 50.49 | 51.65 | 51.55 | 54.38 | 55.76 |
| ADC1 | 99.85 | 96.76 | 94.85 | 82.05 | 77.86 | 95.63 | 93.74 | 70.26 | 62.22 | 63.91 | 63.15 | 64.52 |
| ADC2 | 99.31 | 96.81 | 91.48 | 68.20 | 64.85 | 77.61 | 75.85 | 65.25 | 63.93 | 62.07 | 49.34 | 54.32 |
| ADC3 | | | | | | | | | | | | |
| (b) | Bit-wise Acc. (%) | 99.19 | 91.56 | 98.15 | 90.06 | 73.42 | 96.71 | 97.09 | 50.49 | 51.65 | 51.55 | 54.38 | 55.76 |
| ADC1 | 99.85 | 96.76 | 94.85 | 82.05 | 77.86 | 95.63 | 93.74 | 70.26 | 62.22 | 63.91 | 63.15 | 64.52 |
| ADC2 | 99.31 | 96.81 | 91.48 | 68.20 | 64.85 | 77.61 | 75.85 | 65.25 | 63.93 | 62.07 | 49.34 | 54.32 |

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

| RMS error (LSB) | Ramp | ECG | Sinew1.0Fs | Sinew1.2Fs | Sinew2.0Fs | Sinew3.0Fs | Sinew4.0Fs | Sinew5.0Fs |
|---|---|---|---|---|---|---|---|---|
| ADC1 | 386.25 | 591.55 | 508.04 | 585.55 | 597.59 | 668.92 | 701.10 |
| ADC2 | 258.14 | 262.95 | 300.55 | 381.25 | 372.18 | 419.14 | 445.06 |
| ADC3 | 507.74 | 652.03 | 642.67 | 658.57 | 574.25 | 620.94 | 753.31 |

C. Second-Order Information Leakage Sources of a Current Equalizer

As demonstrated by the protected mode CNN-PSA results of the prototype SAR ADC, the current-equalizer-based ADC PSA countermeasure still discloses a limited amount of correlation between the ADC supply current waveforms and the ADC digital output codes (i.e., does not achieve 50% bit-wise accuracy for all bits). This section discusses two possible second-order information leakage sources of a current equalizer, which might be exploited by CNN-PSA.

The first possible second-order information leakage source of a current equalizer is the voltage droop on the supply capacitors of current equalizers during the supply operations. As shown in Fig. 13, this on-chip ADC ground node voltage disturbance makes the effective VPRUGE voltage vary over time. Depending on the initial capacitor voltage (VDDCAP) of the purging switched-capacitor unit, the unit takes a different amount of time before making a level-shifted version of VDDCAP [VLV in Fig. 10(a)] and the effective VPURGE. Since the effective VPURGE varies over time, after the unit completes its purge operation, the leftover voltage on VDDCAP of...
Fig. 14. Simulated node voltage waveforms of a current equalizer under a GND-side PSA. All voltage waveforms are referenced to on-chip ADC ground voltage. Initial VDDCAP ($t = 0$ ns) of VLV:A is lower than that of VLV:B by 100 mV.

the supply capacitor correlates with its initial voltage and creates an information leakage in the next charge operation. The VDD-side PSA does not have this information leakage since both VPURGE and VLV are referenced to the PCB ground. By generating an on-chip VPURGE bias voltage, this second-order information leakage can be prevented.

The second possible second-order information leakage source of a current equalizer is the OFF-switch current feedthrough. To facilitate capacitor switching activities, the PMOS switches of a current equalizer [M1 and M2 in Fig. 13(a)] are sized large enough, and thus, they have non-negligible parasitic overlap capacitance. The gate-driving NAND gates are directly powered by an off-chip power source [VDDCE of Fig. 9(a)] as they are merely buffering periodic pulses that have no correlation with on-chip ADC activities. Therefore, the current equalizer shorts the gates of M1 and M2 to the external supply voltage (VDDCE) when it turns off its PMOS switches [see Fig. 15(a)–(c)]. However, the external supply voltage (VDDCE) and the on-chip ADC block VDD (VDDCORE) are coupled by the OFF-switch parasitic capacitance. This capacitive coupling enables the on-chip ADC block to draw current from the off-chip supply voltage and creates the information leakage path.

VI. CONCLUSION

ADC PSA is a rising hardware security issue. This article presents two neural-network-based SAR ADC PSA methods and a 12-bit, 1.25-MS/s prototype SAR ADC with a current-equalizer-based PSA countermeasure. When applied to commercial SAR ADCs and the unprotected prototype SAR ADC, the MLP-PSA decoded the ADC supply current waveforms into the corresponding A/D conversion results with high accuracy. The second PSA attack method, CNN-PSA, was also successfully demonstrated on the unprotected prototype SAR ADC. The successful unprotected SAR ADC PSA results show how ADC PSA can be a critical security threat. When applied to the current-equalizer-protected SAR ADC, the ADC demonstrated strong PSA-resistance against MLP-PSA but showed somewhat weaker PSA-resistance against more sophisticated CNN-PSA, enlightening the importance of choosing the appropriate neural network architecture and input for an ADC PSA protection assessment. The possible sources of second-order information leakage were discussed and must be included in future research to make the protection more resistant to CNN-PSA.

ACKNOWLEDGMENT

The authors would like to thank Prof. Song Han, Massachusetts Institute of Technology, for technical discussions. The chip fabrication was donated by the TSMC University Shuttle Program.

REFERENCES

[1] V. V. Gadde, H. Awano, and M. Ikeda, “An encryption-authentication unified A/D conversion scheme for IoT sensor nodes,” in Proc. IEEE Asian Solid-State Circuits Conf. (A-SSCC), Nov. 2018, pp. 123–126.
[2] T. Miki, N. Miura, H. Sonoda, K. Mizuta, and M. Nagata, “A random interrupt dithering SAR technique for secure ADC against reference-charging side-channel attack,” IEEE Trans. Circuits Syst. II: Exp. Briefs, vol. 67, no. 1, pp. 14–18, Jan. 2020.
[3] T. Jeong, A. P. Chandrakasan, and H.-S. Lee, “S2ADC: A 12-bit, 1.25MS/s secure SAR ADC with power side-channel attack resistance,” in Proc. IEEE Custom Integ. Circuits Conf. (CICC), Mar. 2020.
[4] L. Chen et al., “Report on post-quantum cryptography,” Nat. Inst. Standards Technol., (NISTIR), Gaithersburg, MD, USA, NIST Internal Rep. 8105, Apr. 2016. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/nistpubs/IR/2016/nist.8105.pdf, doi: 10.6028/NIST.IR.8105.
[5] M. J. Dworkin et al., “Advanced encryption standard (AES),” NIST Federal Inf. Process. Standards Publications (NIST FIPS), Tech. Rep. 197, Nov. 2001, doi: 10.6028/NIST.FIPS.197.
[6] M. Rivain and E. Prouff, “Provably secure higher-order masking of AES,” in Proc. 12th Int. Workshop Cryptograph. Hardware Embedded Syst. (CHES), Santa Barbara, CA, USA, Aug. 2010, pp. 413–427.
[7] M.-L. Akkar and C. Giraud, “An implementation of DES and AES, secure against some attacks,” in Proc. Int. Workshop Cryptographic Hardw. Embedded Syst. (CHES), Paris, France, May 2001, pp. 309–318.

[8] C. Tokunaga and D. Blaauw, “Secure AES engine with a local switched-capacitor current equalizer,” in IEEE ISSCC Dig. Tech. Papers, Feb. 2009, pp. 64–65.

[9] N. Miura, D. Fujimoto, R. Korenaga, K. Matsuda, and M. Nagata, “An intermittent-driven supply-current equalizer for 11x and 4x power-overhead savings in CPA-resistant 128bit AES cryptographic processor,” in Proc. IEEE Asian Solid-State Circuits Conf. (A-SSCC), Nov. 2014, pp. 225–228.

[10] M. Kar, A. Singh, S. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, “Improved power-side-channel-attack resistance of an AES-128 core via a security-aware integrated buck voltage regulator,” in IEEE ISSCC Dig. Tech. Papers, Feb. 2017, pp. 142–143.

[11] A. Singh, M. Kar, S. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, “A 128b AES engine with higher resistance to power and electromagnetic-side-channel attacks enabled by a security-aware integrated all-digital low-dropout regulator,” in IEEE ISSCC Dig. Tech. Papers, Feb. 2019, pp. 404–406.

[12] C. M. Bishop, Pattern Recognition and Machine Learning (Information Science and Statistics). Berlin, Heidelberg: Springer-Verlag, 2006.

[13] H. Li, C. C. L. Philip, and H.-P. Huang, Fuzzy Neural Intelligent Systems: Mathematical Foundation and the Applications in Engineering, 1st ed. Boca Raton, FL, USA: CRC Press, 2000.

[14] A. M. Abo and P. R. Gray, “A 1.5-V, 10-bit, 14.3-MS/s CMOS pipeline M. Miyahara, Y. Asada, D. Paik, and A. Matsuzawa, “A low-noise self-

[15] B. P. Ginsburg and A. P. Chandrakasan, “An energy-efficient charge

[16] H. Li, C. C. L. Philip, and H.-P. Huang, Fuzzy Neural Intelligent Systems: Mathematical Foundation and the Applications in Engineering, 1st ed. Boca Raton, FL, USA: CRC Press, 2000.

[17] B. P. Ginsburg and A. P. Chandrakasan, “An energy-efficient charge recycling approach for a SAR converter with capacitive DAC,” in Proc. IEEE Int. Symp. Circuits Syst., May 2005, pp. 184–187.

[18] T. O. Anderson, “Optimum control logic for successive approximation analog-to-digital converters,” Deep Space Netw. Prog. Rep., vol. 13, pp. 168–176, Feb. 1973. [Online]. Available: https://ipnpr.jpl.nasa.gov/progress_report/XII/XIIW.PDF

[19] Y. P. Tsividis, P. R. Gray, D. A. Hodges, and J. Jacob Chacko, “A segmented µ-255 law PCM voice encoder utilizing NMOS technology,” IEEE J. Solid-State Circuits, vol. 11, no. 6, pp. 740–747, Dec. 1976.

[20] N. Miura et al., “A local EM-analysis attack resistant cryptographic engine with fully-digital oscillator-based tamper-access sensor,” in Proc. Symp. VLSI Circuits Dig. Tech. Papers, Jun. 2014, pp. 172–173.

[21] A. L. Goldberger et al., “PhysioBank, PhysioToolkit, and PhysioNet: Components of a new research resource for complex physiologic signals,” Circulation, vol. 101, no. 23, pp. e215–e220, Jun. 2000. [Online]. Available: http://circ.ahajournals.org/content/101/23/e215.full

[22] Y. Chen et al., “Split capacitor DAC mismatch calibration in successive approximation ADC,” in Proc. IEEE Custom Integr. Circuits Conf., Sep. 2009, pp. 279–282.

[23] M. Ding, P. Harpe, Y.-H. Liu, B. Busze, K. Philips, and H. de Groot, “A 5.5fJ/conv-step 6.4MS/S 13b SAR ADC utilizing a redundancy-facilitated background error-detection-and-correction scheme,” in IEEE ISSCC Dig. Tech. Papers, Feb. 2015, pp. 460–461.

Anantha P. Chandrakasan (Fellow, IEEE) received the B.S., M.S., and Ph.D. degrees in Electrical engineering and computer sciences from the University of California at Berkeley, CA, USA, in 1989, 1990, and 1994, respectively. Since September 1994, he has been with the Massachusetts Institute of Technology (MIT), Cambridge, MA, USA, where he is currently the Vannevar Bush Professor of Electrical Engineering and Computer Science. He was the Director of the Microsystems Technology Laboratories, MIT, from 2006 to 2011. From July 2011 to June 2017, he was the Head of the Department of Electrical Engineering and Computer Science, MIT. Since July 2017, he has been Dean of the MIT School of Engineering. He is a co-author of Low Power Digital CMOS Design (Kluwer Academic Publishers, 1995), Digital Integrated Circuits (Pearson Prentice-Hall, second edition, 2003), and Sub-Threshold Design for Ultra-Low Power Systems (Springer 2006). His research interests include ultralow-power circuit and system design, energy harvesting, energy-efficient RF circuits, and hardware security.

Dr. Chandrakasan was a co-recipient of several awards, including the 2007 ISSCC Beatrice Winner Award for Editorial Excellence and the ISSCC Jack Kilby Awards for Outstanding Student Paper from 2007 to 2009. He received the 2009 Semiconductor Industry Association (SIA) University Researcher Award, the 2013 IEEE Donald O. Pederson Award in Solid-State Circuits, an Honorary Doctorate from KU Leuven in 2016, the UC Berkeley EE Distinguished Alumni Award in 2017, and the 2019 IEEE Solid-State Circuits Society Distinguished Service Award. In 2015, he was elected to the National Academy of Engineering. In 2019, he was elected to the American Academy of Arts & Sciences. He has served in various roles for the IEEE ISSCC including Program Chair, the Signal Processing Sub-Committee Chair, and the Technology Directions Sub-Committee Chair. He has served as the Conference Chair of ISSCC from 2010 to 2018. He serves as the Senior Technical Advisor to the Conference starting ISSCC 2019.

Hae-Seung Lee (Life Fellow, IEEE) received the Ph.D. degree in electrical engineering from the University of California at Berkeley, Berkeley, CA, USA, in 1984. He developed self-calibration techniques for A/D converters at the University of California at Berkeley. Since 1984, he has been on the faculty at the Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology (MIT), Cambridge, MA, USA, where he is currently the Advanced Television and Signal Processing Professor of Electrical Engineering. He is the Director of the Microsystems Technology Laboratories and the Director of the Center for Integrated Circuits and Systems, MIT. He has published more than 160 peer-reviewed journal articles and conference papers. He is an inventor or a co-inventor of 64 issued U.S. patents and numerous international patents. His research interests are in the areas of analog and mixed-signal integrated circuits in scaled CMOS technologies and medical electronics.

Prof. Lee was a recipient of the 1988 Presidential Young Investigators’ Award and a co-recipient of the ISSCC Jack Kilby Outstanding Student Paper Award in 2002 and 2006. He has served a number of technical program committees for various IEEE conferences, including the International Electron Devices Meeting, the International Solid-State Circuits Conference, the Custom Integrated Circuits Conference, and the IEEE Symposium on VLSI circuits. He has served the Technology Advisory Committee for Samsung Electronics, Cypress Semiconductor, Sensata Technologies, and Dual Aperture, Inc.