A Power Side-Channel Attack on Flash ADC

Ziyi Chen
Department of Electrical and Computer Engineering
Drexel University
Philadelphia, PA
Email: ziyi.chen@drexel.edu

Ioannis Savidis
Department of Electrical and Computer Engineering
Drexel University
Philadelphia, PA
Email: isavidis@coe.drexel.edu

***Abstract*—In this paper, a monotonic power side-channel attack (PSA) is proposed to analyze the security vulnerabilities of flash analog-to-digital converters (ADC), where the digital output of a flash ADC is determined by characterizing the monotonic relationship between the traces of the power consumed and the applied input signals. A novel technique that leverages clock phase division is proposed to secure the power side channel information of a 4-bit flash ADC. The proposed technique adds randomness to decorrelate the input signal from the given power trace as the execution phase of each comparator depends on a thermometer code computed from the previous seven clock cycles. The monotonic PSA is executed on both a secured and unsecured ADC, with results indicating 1.9 bits of information leakage from an unprotected ADC and no data leakage from a protected ADC as the bit-wise accuracy is approximately 50% when secured. The monotonic PSA is more effective at attacking a flash ADC architecture than either a convolutional neural network based PSA or a correlation template PSA. The secured ADC core occupies approximately 2% more area than a non-secure ADC in a 65 nm process, and provides a sampling frequency of up to 500 MHz at a supply voltage of 1.2 V.**

***Index Terms*—power side-channel, ADC, side-channel attack**

I. Introduction

The security of analog and mixed-signal (AMS) circuits is gaining research traction due to the urgent need to secure the large amount of data generated and transmitted by AMS applications. Possible hardware threats that target the theft of sensitive data transmitted through a node within an IoT circuit are shown in Fig. 1, which includes a receiver front-end, an analog-to-digital converter (ADC), and a digital signal processing unit (DSP) with an encryption unit. By depackaging the integrated circuit (IC), the attacker is able to directly probe the output port of the receiver front-end or the ADC. However, direct measurement is often error prone due to the high sensitivity of analog circuit parasitics to probing. The second attack utilizes the power side-channel information generated from the activity of the ADC or the encryption block, where the correlation between the power traces and the transmitted data is analyzed [1]. The attacker then determines the data that results in the strongest correlation with the collected power traces.

Securing analog circuits and encryption units has been extensively studied [2]–[7]. Efforts to secure the information leaked from the power side-channel of a successive approximation register (SAR) ADC have been explored, where the overall power consumption is regulated [8] or the switching activities of the capacitor array are dithered [1] to maximize noise. However, the security of flash ADCs has been rarely studied, where the flash ADC architecture is a popular choice for applications that require transmitting data with high speed and mid-to-low resolution.

In this paper, a novel monotonic power side-channel attack (PSA) is proposed to identify and determine the digital output of a flash ADC by analyzing the monotonic response in the power consumption of a circuit when an analog input signal is applied to the converter. A technique that utilizes clock phase division is proposed to divide the operation of the comparator array into two phases, which results in the generation of a non-monotonic profile of the power consumed by the ADC when characterized with a ramp signal as input.

The rest of the paper is organized as follows. The power side-channel attack executed on a flash ADC is described in Section II. The architecture of the flash ADC and corresponding security vulnerabilities are discussed in Section III. The proposed technique that utilizes clock phase division to protect against PSA is described in Section IV. The simulated results are presented in Section V. Some concluding remarks are provided in Section VI.

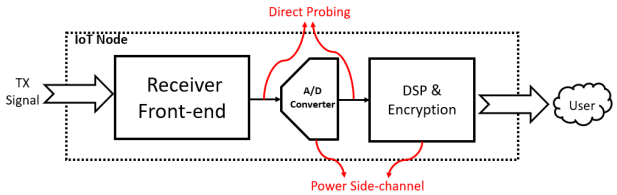


Fig. 1: Hardware attack scenarios of IoT circuits.

II. Power Side-Channel Attack on Flash ADC

In this section, the threat model considered for the attack of a flash ADC is described. A monotonic power side-channel attack is proposed to determine the digital output of an ADC. The attack utilizes the analysis of the power traces generated by applying input sequences to the ADC.

A. Assumed Threat Model

The objective of the attack is to determine the digital output of an ADC from the traces of the power consumed. The attacker is assumed to possess knowledge of the topology and the functionality of the target ADC, either from the specification data sheet or from reverse engineering the netlist of the circuit. An ADC used for training, which has the same architecture as the target ADC, is then prepared for the classification of the power traces. Full access is assumed to the input and output ports of the ADC used for training.

B. Monotonic Side-Channel Attack on a Flash ADC

The attack exploits the monotonic relationship between the magnitude of the applied analog input signal and the peak power consumed within each clock cycle. The power trace is collected from the power pins closest to the resistor-ladder of the DAC. First, a ramp signal is applied as an input to the flash ADC, and the peak power consumption along with the corresponding digital output is recorded for each clock cycle. The maximum peak power consumption is then determined for each quantization level by utilizing the monotonic relationship between the magnitude of the input signal and the power consumed. The pseudocode that identifies the boundary of the power consumed by the ADC at each quantization level is provided as Algorithm 1. In order to identify the boundary of the power consumed, the attacker must determine the maximum power consumption for each quantization level based on the given power trace(s) and corresponding digital output. Since the output of a 4-bit ADC is quantized to 16 levels, the full range of the peak power consumed by the ADC is subdivided into 16 continuous intervals, with each interval labeled to correspond to one quantization level. After learning and developing the model that accurately represents the monotonic response of the power consumed by the ADC, the attacker collects power traces from the target ADC. For each clock cycle, the digital output is determined by selecting the label of the interval that contains the corresponding peak power consumed during that clock cycle.

Algorithm 1: Monotonic Power Side-Channel Attack

Input: power trace and digital output pair PD = {(P_1, D_1), (P_2, D_2), ..., (P_N, D_N) }
where N = 5000;
Output: power boundary PB, where len(PB) = 16;
for $i = 0 \rightarrow 15$ **do**
  $PB[i]$ = 0;
  for $N = 1 \rightarrow 5000$ **do**
    if D_N = i *and max*(P_N) > $PB[i]$ **then**
      $PB[i]$ = max(P_N)
    end
  end
end

III. Circuit Implementation of Flash ADC and Security Vulnerabilities

In this section, the circuit implementation and security vulnerabilities of a flash ADC are described.

A. Implementation of Flash ADC

A 4-bit flash ADC consists of 15 comparators with switch capacitor sampling paths and a 4-bit resistor divider DAC as an analog front-end. In addition, a decoder is included in the digital back-end. The comparators are implemented as a StrongArm architecture [9], which compares the input voltage with a reference voltage. The comparator array generates a 15-bit thermometer code, which is first converted into a one-hot-code by a 3-input NAND gate array. A ROM-based decoder [10] is then utilized to convert the one-hot-code into a binary output.

B. Security Vulnerabilities of Flash ADC

The information leaked by the flash ADC is due to the unbalanced parasitic capacitance of the differential sampling paths shown in Fig. 2, where C_{P1} and C_{P2} represent the parasitic capacitance between the DAC and the sampling capacitors. Right after the falling edge of the CLK_{P1} signal, the charge Q_1 and Q_2 stored on the sampling capacitors C_1 and C_2 respectively, is given by

$$Q_1 = (V_{INN} - V_{CM})C_1 + V_{INN}C_{P1}, \text{ and} \quad (1)$$
$$Q_2 = (V_{INP} - V_{CM})C_2 + V_{INP}C_{P2}. \quad (2)$$

V_{INN} and V_{INP} represent the negative and positive paths, respectively, of the differential analog input centered at the common-mode voltage V_{CM}. When CLK_2 is high, the reference voltage from the DAC is sampled. The charge stored on capacitors C_1 and C_2 is now given by, respectively,

$$Q_3 = (V_{RNi} - V_{CM})C_1 + V_{RNi}C_{P1}, \text{ and} \quad (3)$$
$$Q_4 = (V_{RPi} - V_{CM})C_2 + V_{RPi}C_{P2}. \quad (4)$$

V_{RPi} and V_{RNi} represent the positive and negative reference voltage, respectively, of the i^{th} comparator. Since the sampling capacitors C_1 and C_2 are equal, both are given as C. Assuming the difference between the unbalanced capacitance is ΔC_P = C_{P1} - C_{P2}, the total charge drawn by the DAC is given by

$$Q = (Q_3 - Q_1) + (Q_4 - Q_2) \quad (5)$$
$$= (V_{RPi} + V_{RNi} - V_{INP} - V_{INN})C + (V_{RNi} - V_{INN})\Delta C_P. \quad (6)$$

For differential signals, V_{INP}+V_{INN} = V_{RPi}+V_{RNi} = $2V_{CM}$. Therefore, the total charge Q is given by

$$Q = (V_{RNi} - V_{INN})\Delta C_P. \quad (7)$$

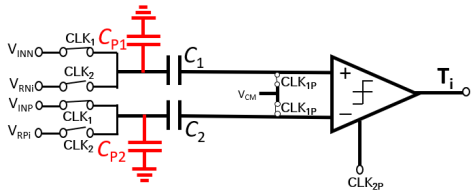


Fig. 2: Architecture of the sampling network of a 4-bit flash ADC. C_{P1} and C_{P2} represent parasitic capacitances between the DAC and the sampling capacitors.

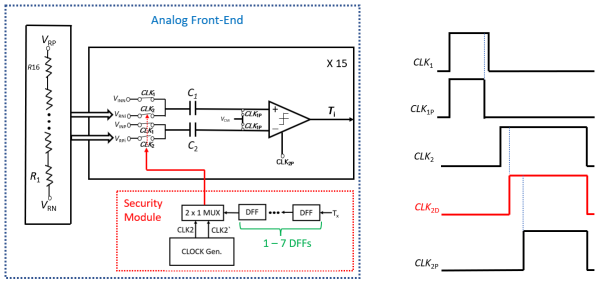
Since the DAC provides a reference voltage for 15 comparators, and the sampling network for all comparators are equal, the total charge drawn by the DAC is given by

$$Q = \sum_{i=1}^{15}(V_{RNi} - V_{INN})\Delta C_P. \quad (8)$$

The charge drawn from the DAC within one clock cycle is, therefore, proportional to the magnitude of the input signal, which allows an adversary to determine the correlation between the power consumed and the magnitude of the sampled input.

IV. Secure Flash ADC

In order to secure the power side-channel of a flash ADC, a clock phase division technique is developed to decorrelate the power consumed from the magnitude of the input signal. For a 4-bit flash ADC, 15 comparators are utilized to compare the sampled analog input signal to the corresponding 15 quantization levels. Since the reference voltage to each comparator is constant, the power consumed within a given clock cycle, given by the relationship to the total charge drawn by the DAC, is a function of the magnitude of the sampled input as expressed by (8). A clock phase division technique, as shown in Fig. 3a, is, therefore, proposed to decorrelate the peak power consumed during a given clock cycle by providing dependency on the magnitude of the input sampled during up to the previous seven clock cycles. Each sampling network includes a 2x1 MUX, with a select signal provided by a chain of D flip-flops (DFF). The number of delay stages of DFFs is randomly set in the range of 1 to 7, with at least one chain of DFFs assigned to each number. In addition, the switching activity of the i^{th} comparator is dependent on the thermometer code T_x computed by a randomly selected comparator, where x is between 0 to 15.



(a) (b)

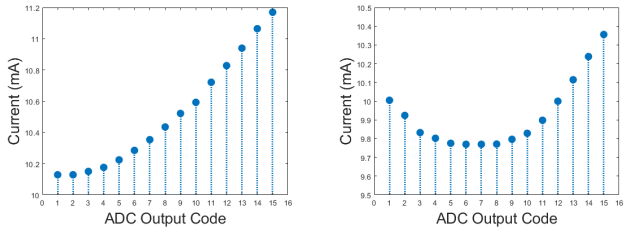
Fig. 3: The (a) circuit implementation of the analog front-end and (b) clock timing diagram of a secured 4-bit flash ADC.

The 15 comparators are divided into two sub-groups, with one group of comparators provided the delayed rising edge of clock CLK_2 as shown in Fig. 3b. The sub-division of the group is determined by the thermometer code computed from the previous seven clock cycles. The power consumed

by the switching activity of the circuit is, therefore, not only determined by the magnitude of the currently sampled input but also by the magnitude of the input sampled during the previous seven clock cycles. For a 4-bit ADC with 16 quantization levels, there are 16^7 possible division patterns in total. Therefore, a brute force attack of the ADC by matching the pattern of the power trace with input from the previous seven sampling cycles is of limited efficiency.

The determined boundary of the consumed peak current and the corresponding digital output for an applied ramp input signal is shown in Fig. 4 for both an unsecured and secured 4-bit flash ADC. For a secured ADC, the current consumed is no longer monotonically correlated to the magnitude of the input signal.

The parabolic curve shown in Fig. 4b of the current consumed indicates an obfuscation of the interval used to determine the output of the ADC. For example, the interval of current for output codes between 1 and 2 overlaps with output codes between 11 and 12. In addition, the power consumed by the ADC for a given input voltage varies for different input frequencies. Therefore, the proposed technique not only obfuscates the power consumption boundary that results in a parabolic curve but also obfuscates the frequency and magnitude of the input signal.



(a) (b)

Fig. 4: Analysis of the power consumption as given by the current drawn by an (a) unprotected 4-bit flash ADC and (b) secured 4-bit flash ADC.

V. Simulation Results

In this section, the performance of an unsecured and secured ADC are characterized. In addition, the simulated results from executing the monotonic power side-channel attack on the extracted layout view of both the unsecured and secured ADC are provided.

A. ADC Performance

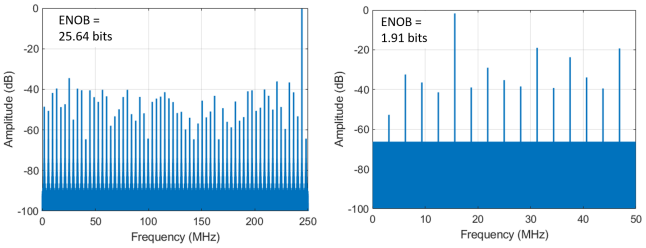
Both the secured and unsecured ADC are characterized with results as listed in Table I. The ADC is implemented in a 65 nm technology and occupies an area of approximately 0.05 mm^2. The maximum sampling frequency of both the unsecured and secured ADC is 500 MHz at a supply voltage of 1.2 V. The security module has no impact on the signal to noise and distortion ratio (SNDR) as both the secured and unsecured ADC provide an SNDR of 25.64 dB and an effective number of bits (ENOB) of 3.96. The output spectrum of the secured ADC for a 244 MHz input signal sampled at a frequency of 500 MHz is shown in Fig. 5a.

B. Evaluation of Monotonic PSA on Secured and Unsecured ADC

The monotonic PSA is executed on a 4-bit flash ADC with a sampling frequency of 100 MHz, 250 MHz, and 500 MHz. A ramp input that linearly increases in voltage from 0 V to V_{DD} (1.2 V) is applied to the ADC. For each clock cycle, the power trace is collected from the supply pin closest to the resistor ladder based DAC. The corresponding digital outputs from the decoder are observed and stored to determine the correlation between the power consumed and the output of the ADC. The complete data set includes 5K power traces and a

TABLE I
Characterization of Unsecured and Secured ADC.

	Unsecured	Secured
Resolution	4 bits	4 bits
ENOB	3.96 bits	3.96 bits
Conversion Rate	500 MHz	500 MHz
SNDR	25.64 dB	25.64 dB
DNL	0.03/-0.03 LSB	0.42/-0.38 LSB
INL	0.06/0 LSB	0.07/-0.34 LSB
Process	65 nm	65 nm
Area	0.05 mm^2	0.051 mm^2
Supply Voltage	1.2 V	1.2 V
Power	10.73 mW	12.16 mW
FOM	1.38 pJ/Conv	1.56 pJ/Conv



(a) (b)

Fig. 5: Characterization of the (a) FFT spectrum (8192 points) of the secured ADC for a 244 MHz input signal sampled at a frequency of 500 MHz, and (b) FFT spectrum (512 points) of the digital output reconstructed through monotonic PSA, with a 15.625 MHz input signal sampled at a frequency of 100 MHz.

corresponding 5K sets of digital outputs, which are utilized to identify the minimum and maximum current consumed for each of the 16 quantization levels. The determined peak current of the unsecured ADC is shown in Fig. 4a, where a monotonic relationship between the voltage of the input signal and the power consumed is observed.

After determining the boundary profile of the current consumed, the input to the ADC is replaced by a sine wave and power traces are collected from the supply pin closest to the resistor ladder based DAC. The peak current consumed within each clock cycle is then determined from the power traces for a sinusoidal input. Assuming the adversary has no direct access to the output of the ADC, the objective of the attack is to determine the digital output of the ADC by only analyzing the power traces. By utilizing the boundary of the current consumption as shown in Fig. 4a, the output of the ADC is determined by finding two adjacent boundaries that contain the target peak current consumed. For example, the corresponding output code of a peak current I_1 enclosed by the n^{th} and $(n+1)^{th}$ boundary is n.

The bit-wise accuracy of executing the monotonic PSA on an unsecured ADC with a sampling frequency of 100 MHz, 250 MHz, and 500 MHz, and for an input with a frequency of 0.1x, 0.3x, and 0.49x that of each sampling frequency is listed in Table II. For the 100 MHz sampling frequency, the D0 (most significant bit, MSB) and D1 are determined with accuracies greater than 95% for all three input frequencies, while D2 an D3 (least significant bit, LSB) are determined with accuracies between 77% and 88%. The accuracy of the prediction also drops as the frequency of the input increases. The frequency spectrum from calculating the fast fast Fourier transform (FFT) of the reconstructed digital output after executing the monotonic PSA on a 15.625 MHz input signal sampled at a frequency of 100 MHz is shown in Fig. 5b. The effective number of bits (ENOB) of the reconstructed signal is 1.91.

The monotonic PSA is also executed on the secured ADC, which results in the boundary profile of the current consumption as shown in Fig 4b. The bit-wise accuracy of executing the monotonic PSA on a secured ADC with sampling frequencies

TABLE II
BIT-WISE ACCURACY OF EXECUTING THE MONOTONIC PSA ON THE UNSECURED ADC.

(a) SAMPLING FREQUENCY f_S = 100 MHz

Bit	f_{in} = 0.1f_s	f_{in} = 0.3f_s	f_{in} = 0.49f_s
D0	100%	98.99%	98.99%
D1	98.49%	97.98%	95.97%
D2	88.44%	85.17%	83.41%
D3	84.42%	80.15%	77.63%

(b) SAMPLING FREQUENCY f_S = 250 MHz

Bit	f_{in} = 0.1f_s	f_{in} = 0.3f_s	f_{in} = 0.49f_s
D0	96.19%	98.39%	97.50%
D1	90.18%	89.67%	88.07%
D2	54.80%	67.23%	75.65%
D3	61.62%	63.42%	50.10%

(c) SAMPLING FREQUENCY f_S = 500 MHz

Bit	f_{in} = 0.1f_s	f_{in} = 0.3f_s	f_{in} = 0.49f_s
D0	97.14%	94.28%	96.99%
D1	90.00%	81.42%	78.05%
D2	65.71%	70.00%	59.01%
D3	57.14%	60.00%	64.02%

TABLE III
BIT-WISE ACCURACY OF EXECUTING THE MONOTONIC PSA ON THE SECURED ADC.

(a) SAMPLING FREQUENCY f_S = 100 MHz

Bit	f_{in} = 0.1f_s	f_{in} = 0.3f_s	f_{in} = 0.49f_s
D0	52.57%	58.76%	53.60%
D1	48.45%	53.60%	46.39%
D2	57.73%	61.85%	52.57%
D3	56.70%	59.79%	53.60%

(b) SAMPLING FREQUENCY f_S = 250 MHz

Bit	f_{in} = 0.1f_s	f_{in} = 0.3f_s	f_{in} = 0.49f_s
D0	56.12%	57.14%	51.02%
D1	44.89%	52.04%	42.85%
D2	55.10%	65.30%	62.24%
D3	59.18%	61.22%	58.16%

(c) SAMPLING FREQUENCY f_S = 500 MHz

Bit	f_{in} = 0.1f_s	f_{in} = 0.3f_s	f_{in} = 0.49f_s
D0	48.97%	50.00%	51.02%
D1	40.81%	51.02%	55.10%
D2	59.18%	52.04%	56.12%
D3	58.16%	47.95%	44.89%

of 100 MHz, 250 MHz, and 500 MHz and for inputs with frequencies of 0.1x, 0.3x, and 0.49x that of each sampling frequency is listed in Table III. For all input frequencies and sampling frequencies, the monotonic PSA executed on the secured ADC fails, with an accuracy of approximately 50% for all bits, which is equivalent to a random selection of a binary number.

C. Comparison with Other Side-channel Attack Methods

The efficacy of the monotonic PSA is compared with machine learning (ML)-based PSA and correlation template based PSA. The ML-based PSA described in [8] utilizes either an artificial neural network or convolutional neural network (CNN) to classify the digital output of an ADC from the collected current traces. For a 4-bit output, four neural networks are individually trained, where the output neuron of each network indicates the predicted value of each bit (either 1 or 0). In order to classify the current traces collected from a flash ADC, a CNN with two 2-D convolution layers, two pooling layers, and three fully connect layers is trained. A rectified linear unit (ReLU) function is applied to all convolution layers and pooling layers [8].

For the correlation template based PSA, a template of the current traces for each quantization level of the ADC is first developed. The correlation between the power trace sampled from the target ADC and each template power trace is then calculated utilizing a user defined equation [1] given by

$$\rho(X, Y_N) = \frac{\sigma_{X,Y_N}}{\sigma_X, \sigma_{Y_N}}, \tag{9}$$

where σ_X and σ_{Y_N} represent the standard deviation of, respectively, the template power trace and the target power trace, and σ_{X,Y_N} represents the covariance between the target power trace and the template power trace. For a 4-bit flash ADC, 16 power trace templates are prepared, one representing each of the 16 quantization levels of the ADC. The power trace template that results in the highest correlation with the target power trace is determined, and the corresponding quantization level is returned as the correct output.

TABLE IV
COMPARISON OF MONOTONIC PSA WITH CNN AND TEMPLATE PSA FOR A SAMPLING FREQUENCY f_S OF 100 MHZ.

(a) UNSECURED ADC

Bit	Monotonic	CNN	Template
D0	100%	100%	51.00%
D1	98.49%	90.09%	49.00%
D2	88.44%	66.00%	51.00%
D3	84.42%	65.70%	51.00%

(b) SECURED ADC

Bit	Monotonic	CNN	Template
D0	49.48%	42.50%	49.48%
D1	50.51%	36.25%	46.39%
D2	48.45%	56.25%	43.29%
D3	57.73%	76.85%	51.54%

The bit-wise accuracy of the monotonic PSA, the CNN PSA, and the power trace template PSA on both the unsecured and secured ADC is analyzed with results as listed in Table IV. For the analysis and comparison of the attacks, the sampling frequency is set to 100 MHz for an input with frequency of 0.1x that of the sampling frequency. The training data set for all PSA methods is collected for a ramp input. As compared to the CNN PSA, the monotonic PSA provides 38% higher accuracy on average for bits D2 to D4. The template PSA fails to predict any of the bits. Unlike the SAR ADC, the prediction error of the template PSA is due to the similarity of the power traces of a flash ADC across different inputs and the dominance of the covariance on the magnitude of the input signal. Therefore, the template that results in the largest magnitude provides the highest correlation for all the inputs.

VI. CONCLUSIONS

In this paper, the security vulnerabilities of a flash ADC are analyzed. A monotonic PSA is proposed to identify the boundary of the consumed current for each quantization level and to determine the digital output of the ADC. A technique that utilizes clock phase division is proposed to reduce the power side-channel leakage of the flash ADC, where the power consumption of the resistor ladder based DAC not only depends on the magnitude of the current input but also on the thermometer code computed during the previous seven clock cycles. The randomization in the power profile of the ADC leads to a non-monotonic response in the peak current consumed by the ADC as characterized with an applied ramp input signal.

Implemented in a 65 nm process, the unsecured and secured flash ADC operate with a sampling frequency of up to 500 MHz and with a resolution of 4-bits. The secured ADC occupies approximately 2% more area without degrading the sampling frequency or resolution. Execution of the monotonic PSA provides 1.9 bits of information when performed on the unsecured ADC. The monotonic PSA, CNN PSA, and template PSA all fail to decrypt the output of the secured ADC, resulting in approximately a 50% bit-wise accuracy for all output bits.

REFERENCES

[1] T. Miki, N. Miura, H. Sonoda, K. Mizuta, and M. Nagata, "A random interrupt dithering SAR technique for secure ADC against reference-charge side-channel attack," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 67, no. 1, pp. 14–18, February 2020.

[2] S. Ors, F. Gurkaynak, E. Oswald, and B. Preneel, "Power-analysis attack on an ASIC AES implementation," *Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC)*, vol. 2, pp. 546–552, April 2004.

[3] C. Tokunaga and D. Blaauw, "Secure AES engine with a local switched-capacitor current equalizer," *Proceedings of the IEEE International Solid-State Circuits Conference (ISSCC)*, pp. 64–65, February 2009.

[4] V. V. Rao and I. Savidis, "Performance and security analysis of parameter-obfuscated analog circuits," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 29, no. 12, pp. 2013–2026, December 2021.

[5] 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," *Proceedings of the IEEE International Solid- State Circuits Conference (ISSCC)*, pp. 404–406, February 2019.

[6] V. V. Rao and I. Savidis, "Mesh based obfuscation of analog circuit properties," *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 1–5, May 2019.

[7] V. V. Rao and I. Savidis, "Protecting analog circuits with parameter biasing obfuscation," *Proceedings of the IEEE Latin American Test Symposium (LATS)*, pp. 1–6, Mar. 2017.

[8] 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," *Proceedings of the IEEE Custom Integrated Circuits Conference (CICC)*, pp. 1–4, April 2020.

[9] B. Razavi, "The strongarm latch [A circuit for all seasons]," *IEEE Solid-State Circuits Magazine*, vol. 7, no. 2, pp. 12–17, June 2015.

[10] S. Kumar, M. K. Suman, and K. L. Baishnab, "A novel approach to thermometer-to-binary encoder of flash ADCs-bubble error correction circuit," *Proceedings of the International Conference on Devices, Circuits and Systems (ICDCS)*, pp. 1–6, March 2014.