# PSCA-Resilient Fully Differential 8-bit Hybrid Flash-SAR ADC

Nipun Kaushik, *Student Member, IEEE*, Andrew Ash, *Student Member, IEEE*,
John Hu, *Senior Member, IEEE*

***Abstract*—This brief presents a power side-channel attack (PSCA) resilient fully differential hybrid Flash-SAR ADC. The design utilizes the Spread Sampling (SS) technique along with architectural modifications to gain security enhancement. The ADC doesn't utilize a random number generator due to power, performance, and area (PPA) penalty. The secure ADC is compared with an unsecure 8-bit ADC by a CNN attack. The ADCs are designed in TSMC 65nm process with a 1V supply. The proposed ADC achieves a normalized root mean square error (NRMSE) of 0.4386. Operating at 11.11 MSPS with an energy efficiency of 117 fJ/step, the design demonstrates high-speed, low-power operation while enhancing security against side-channel attacks.**

***Index Terms*—Secure Analog-to-Digital Conversion, Power Side-Channel Attack Resistance, Hybrid Flash-SAR ADC, Secure ADC Design, Temporal Spread Techniques, Power Side-Channel Mitigation, ADC, Secure Circuit Design, Signal Randomization**

## I. Introduction

SECURE Analog-to-Digital Converters (ADCs) have recently seen a boost in security through various techniques. This is amplified by the use of sensors for the Internet of Things (IoT) and edge devices. An eavesdropper can extract the sensitive input data at these nodes by constantly improving artificial intelligence algorithms. Software-based algorithms develop faster than silicon fabrication. This requires reliable and cost-effective implementations that provide high security.

Implementing security comes with additional circuits that can incur higher costs in terms of area, power consumption, or performance (PPA) compared to the original design. An efficient design for a usual application is a secure conversion with minimal overhead. Recent designs used randomization techniques, which bring excellent security at the cost of generating random numbers [1]–[5].

Comparison of secure devices has also been challenging due to different architectures. In this work, we refer to the root mean square error (RMSE) of the attacker's recreation compared to the actual ADC's output code. This can be normalized based on the number of bits to yield the NRMSE. This helps bring a clear picture of the security improvement, regardless of ADC resolution or the type of quantizer.

## II. Recent Work

A secure ADC using random interrupt dithering was introduced by Miki et al. to prevent against reference side channel attacks (SCAs) [1]. The security of the method was evaluated using template attacks, which clearly show the pattern with bit correlation. This was followed by a current equalizer-based protection scheme to break the correlation of power consumption [6]. A multi-layer perceptron (MLP) and a convolutional neural network (CNN) were used to characterize the security of the design. This also highlights the benefits of using a CNN in security characterization due to training simplicity and automatic feature extraction. Further work explores randomness techniques to break the correlation of the input signal. Sniff-SAR proposes two modes of operation for secure and unsecure conditions by employing detection circuits for Power Side Channel Attacks (PSCA) and Electromagnetic Side Channel (EMSCA).

Recent secure ADC research has been simulation-based. Flash ADCs received their first secure architecture, featuring a design that randomly delays comparator outputs based on conversions from the past seven clock cycles [7]. Karanth et al. recommended a simple security strategy by randomly selecting which input is connected to the positive C-DAC. When the inputs are swapped, the comparator inputs are also exchanged to maintain the intended output [8]. This design was improved by also randomly determining whether each capacitor would begin charged to a 0 or 1 to begin each data conversion; the result was a design with $2^{\text{resolution}}$ different current signatures possible for a given input [5]. Recently, a secure 1st-order delta-sigma modulator was proposed using on-chip capacitor banks, similar to [2], alongside constant current consumption to hide leakage unique to delta-sigma modulators [9]. Finally, a single-slope ADC was proposed that compares against both an upward and a downward ramp signal with a randomly selected slope to hide the moment when the actual conversion is completed [10].

This work introduces a fully differential 8-bit secure hybrid Flash-SAR ADC. The ADC is designed in the TSMC 65nm process with a 1V supply range. Fully differential design provides rejection against common mode disturbance and doubles the input range to $2V_{pp}$.

## III. Circuit Design

The ADC is designed in the TMSC 65nm process with a 1 V supply. The design of an unsecured 8-bit fully differential SAR ADC based on a switch capacitor scheme [11]. Figure 1 shows the block diagram of a positive side for simplicity. A similar capacitor bank is connected to the negative terminal of the comparator.

### A. SAR Conversion

The input signal is sampled via bottom plate sampling on the top and bottom side arrays through a bootstrapped switch. In this state, the input at the comparator is connected to $V_{CM}$.

Manuscript received August 22, 2025.

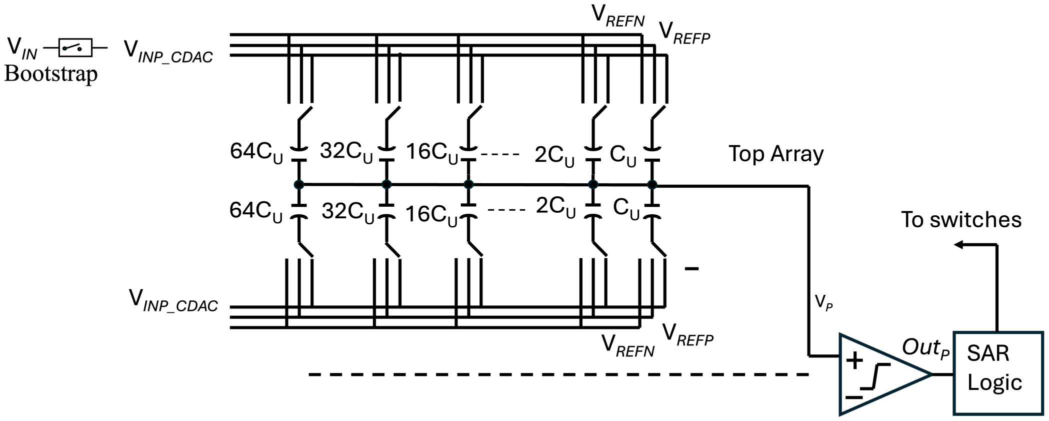

Fig. 1. 8-Bit SAR based on switch capacitor scheme

In the hold and redistribution phase, the CDAC is connected to a fixed reference voltage on the top and bottom sides. The voltage on the top side of the array shown in figure 1 connects to the power supply, and the bottom side connects to ground. The negative side is arranged in a complementary fashion by connecting the top side to ground and the bottom side to the power supply. In this phase, the sensitive input signal is distributed on the capacitive arrays. This is important for secure design as this moves charge based on the input signal, evident in the current from the reference node. This is followed by the SAR conversion phase, wherein the most significant bit (MSB) is first released from the reference according to the default logic, thereby setting the comparator input node. The comparator subsequently latches the decision, which is stored in the SAR register and asserts bit decisions in the following cycle. The voltages at the comparator input node are then updated, and the conversion process proceeds iteratively until all bits are resolved.

Figure 2 shows the synchronous SAR logic for this scheme. It consists of a D flip-flop array to generate state logic. The result is stored in the SAR register bit after each bit trail. The conversion process begins with the most significant bit (MSB) and concludes upon latching the least significant bit (LSB).

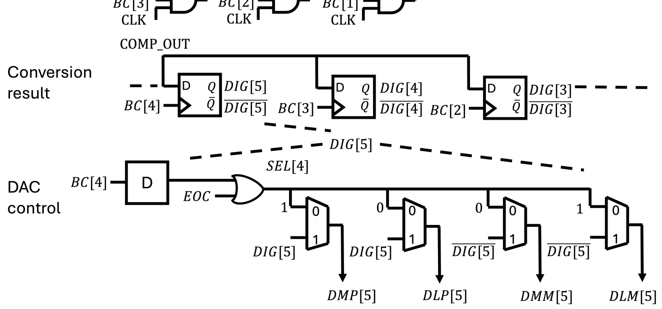

Fig. 2. SAR logic for switch capacitor scheme

## IV. Secure ADC

The secure ADC modifies the front end to obfuscate the reference current with other parameters, thereby breaking the correlation of the sensitive input signal. Flash-SAR hybrid ADCs are utilized for fast conversion and energy efficiency [12]. Flash leverages a reference ladder to generate references for comparators and generate the result in one cycle. A caveat with flash is that the number of comparators increases exponentially with resolution. To maintain speed and power efficiency, this design uses a 2-bit Flash converter for the top two bits. The SAR logic remains the same, with optimizations to the CDAC for enhanced security.

### A. Coarse-Flash ADC

Figure 3 shows a slice of the flash comparator to produce a thermometer code. This code can be directly used to control the top two bits of the SAR $64C+32C = 96C$. The capacitors in CDAC are divided based on thermometer codes. The input is sampled on the sampling capacitor signal against $V_{CM}$ in phase 1. This sampling capacitor should be five times larger than the parasitic capacitance on the input differential pair [13]. In the second phase, differential references are connected to the sampling capacitor, and the comparator is turned on after a slight delay, ensuring full signal settlement. The thermometer code is followed by bubble correction logic to suppress incorrect transitions. The corrected code is converted

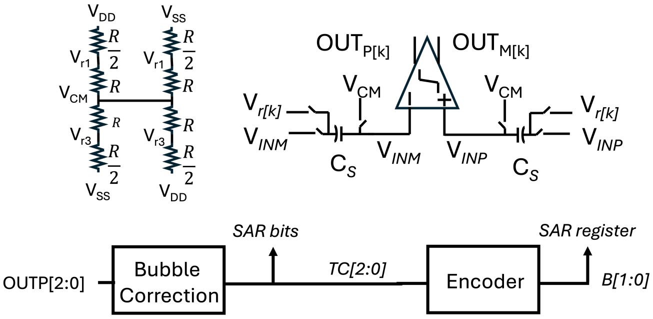

Fig. 3. Fully differential 2-bit Flash ADC

into an equivalent binary code by the encoder. The binary code represents the sub-range of SAR representing the top two bits $MSB$ and $MSB-1$. A non-interger flash can be used with digital correction to improve offset in the front stage. The design uses a pre-amplifier to suppress offset noise.

### B. SAR-Fine ADC

Figure 4 shows the top CDAC array of the Flash-SAR ADC. The top two bits are divided based on thermometer code into $32C+32C+32C=96C$ parts. The bottom array follows the same architecture with complementary control signals.

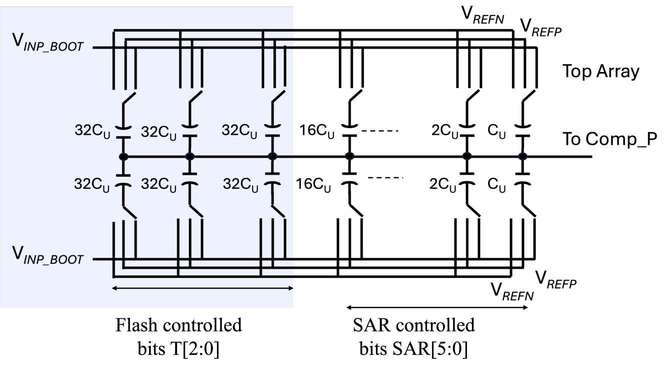

Fig. 4. CDAC arrangement for Flash-SAR ADC

### C. Security Enhancement Technique

The conversion process consists of sampling the signal on sub-ADCs in the first phase. Flash resolves the first two bits and initializes the CDAC before the first SAR conversion. The final result is the top two bits from flash and the remaining six bits from SAR conversion.

**Sampling Spread(SS)**: The input charge is redistributed during hold mode in a typical SAR conversion process. The results in a large $I_{ref}$ spike, leaking information during a CNN-based attack. SS spreads the hold mode signal via delay lines to distribute the connection of the reference to the capacitor [14]. To further boost the security, the bits are triggered LSB first, which leaks the least amount of information. This technique introduces temporal signal spread, requiring a higher-speed acquisition system to capture fine changes. An attacker needs 1GHz sampling for a 10ns signal, but if the signal is shifted to 10.01ns, the required rate rises to 100GHz—an increase of **100×**. This is used solely to trigger the hold-mode signal, thereby breaking the correlation of the biggest current spike during conversion.

**The architecture** of the CDAC is modified for $MSB$ and $MSB-1$ bits. The two bits that carry the most information are resolved using a flash ADC that initializes the CDAC before the first conversion, further reducing the correlation. To obscure the current signature, three equally sized capacitors are employed in place of conventional binary-weighted capacitors. Thermometer-coded control of the capacitors ensures high linearity while eliminating binary bit correlations.

## V. Simulation Results

The CDAC reference input current is used for CNN characterization based on previous works [6]. The security of the two ADCs is compared after collecting the same number of samples for a 40 LSB/conversion slow ramp across the full range. The analysis uses bit-wise accuracy to probe deeper into error contribution from secure and unsecure bits. Figure 5 shows the comparison of bit-wise error contribution from two ADCs. A higher error reflects the prediction error by the CNN. The Most Significant Bit (MSB) carries the highest information content. In secure ADC designs, prediction errors tend to be larger for the higher-order bits, such as the MSB and its neighbors. The secure ADC exhibits a higher overall prediction error, as measured by the normalized root mean square error (N-RMSE). The RMSE is normalized to compare similar secure ADCs with different resolutions.The error rate per bit can be interpreted as the prediction probability for each bit. Figure 6 shows the prediction probability of each bit based on the number of prediction errors. Higher prediction probability demonstrates the vulnerability of leaky MSB in an unsecure design. The LSB is triggered first in the sequences during **SS**, resulting in more leakage compared to an unsecured version.

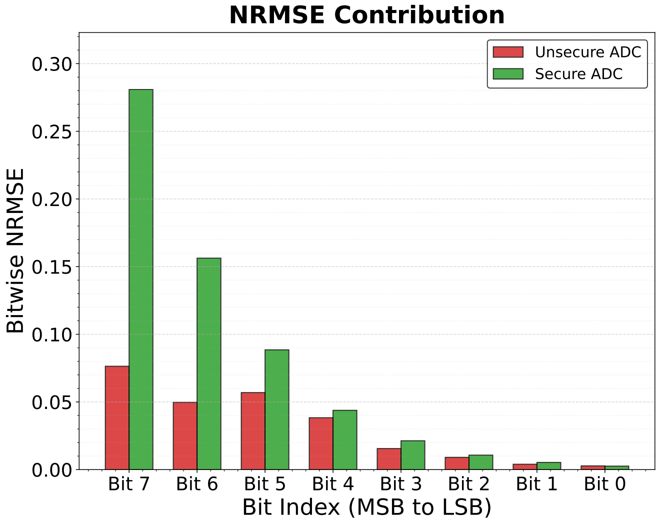

Fig. 5. Normalized bit-wise RMSE for secure and unsecure ADC

The comparison demonstrates that the Flash-SAR ADC enhances security, exhibiting vulnerability only in the least significant bit (LSB), which inherently carries minimal information. Figure 7 highlights the effectiveness of the Flash-SAR architecture in reducing bit error correlation, which attackers could exploit to infer the correct code. The results clearly show that the most significant bits exhibit significantly higher security compared to the vulnerable top bits in the unsecured design.

Table I compares the secure and unsecured ADC performances against a full 8-bit random code guess. The secure ADC achieves a higher resistance to code prediction errors, confirming its improved security margin relative to random baseline guessing. The secure ADC achieves an NRMSE of

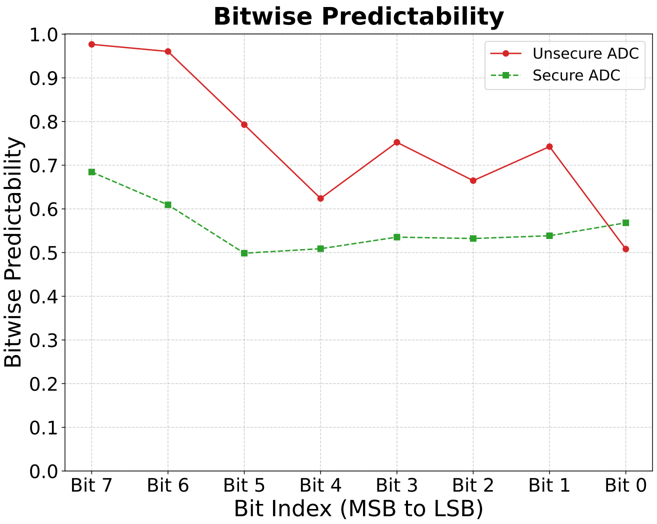

Fig. 6. Bit-wise predictability for secure and unsecure ADC

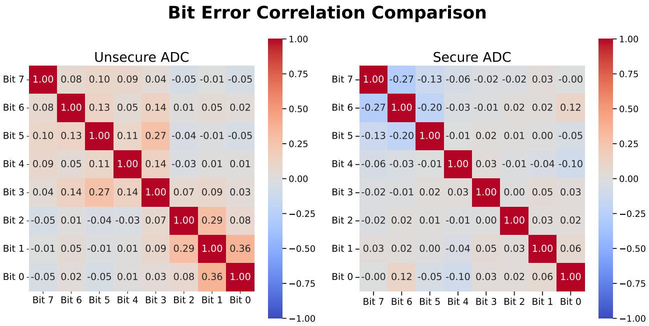

Fig. 7. Bit error correlation for secure and unsecure ADC

0.4386 compared to the standard version with an NRMSE of 0.1183. The secure design provides a boost of 0.3203.

This provides a boost of 0.3203 from the secure version.

## VI. Comparison with Prior Works

Table II summarizes the results of prior secure SAR ADC works as well as the proposed design. It is important to note that only [6] and the newly proposed Flash-SAR ADC achieve a security improvement with no dependence on random number generation. While the security and design efficiency results can be viewed in detail here, it is challenging to compare fairly between architectures with different resolutions. Fig. 8 facilitates a fair comparison between secure ADC architectures of different resolutions.

Based on the secure encryption hardware analysis in [15], the relative increase in the product of power, sample rate, and die area is compared against the relative security improvement of each ADC. Relative costs are found using (1), which tracks a loss in operating speed (performance) and gains in power and area. In cases where implementing security increases the operating speed (this work) or reduces the power ([4]), the relative cost is manually subtracted from 1 to reflect the improved efficiency of the secure architecture.

TABLE I
RMSE Comparison of Different ADCs

| Metric | Full random code guess | Unsecure ADC | Secure ADC |
|---|---|---|---|
| Total RMSE | 104.51 | 30.29 | 112.28 |

$$Relative\,Cost = 1 + \frac{|Unprotected - Secure|}{Unprotected} \qquad (1)$$

Relative security improvement is measured by subtracting the unprotected leakage NRMSE from the protected leakage NRMSE. This subtraction enables comparisons across ADCs with different resolutions without giving an advantage to higher-resolution designs and helps reduce the impact of variations in SCA implementation.

This work achieves an NRMSE improvement only 0.005 less than the ADC proposed in [5] without relying on any random number generation. The only other secure SAR ADC architecture that does not require random number generation is [6], which achieves a much lower NRMSE improvement. The cost of random number generation is not considered in the PPA costs of prior secure architectures. The additional area and power costs of random number generation would impact the reported efficiency of [3], [5], [2], and [4].

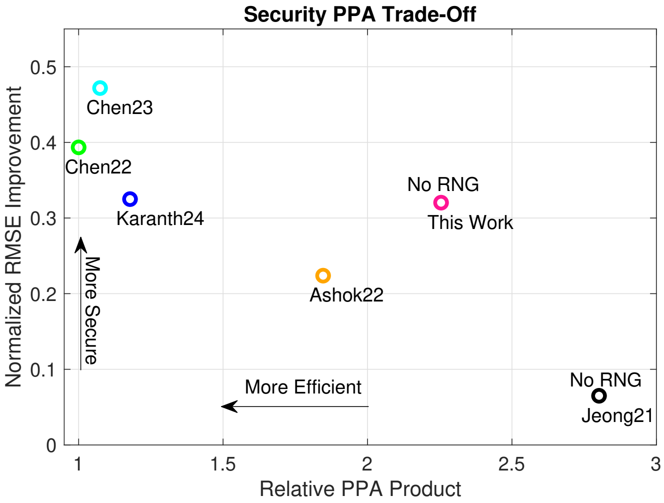

Fig. 8. Relative increase in power, performance, and area versus the security improvement achieved by secure ADCs. The proposed design achieves a higher RMSE improvement than [6] with a lower cost in PPA.

## VII. Conclusion

The work presents a secure hybrid Flash-SAR ADC in the TMSC 65nm process with a 1V supply voltage. The design does not rely on a random number generator, thereby avoiding the associated PPA overhead. The increased cost of the Flash ADC is offset by its superior performance in conversion speed. DNL/INL performance of the SAR only portion is -0.008/0/0.115 and -0.074/0.066, respectively. The degradation in DNL/INL from flash transition points can be corrected by non-integer Flash with digit correction. The technique enhances security by using existing architecture without

TABLE II
SECURE ADC COMPARISON

| Publication | TCAS-II'20 [1] | | JSSC'21 [6] | | CICC'22 [2] | | VLSI'22 [3] | | CICC'23 [4] | | HOST'24 [5] | | This Work | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Process (nm) | 180 | | 65 | | 65 | | 65 | | 65 | | 65[a] | | 65[a] | |
| Supply (V) | N/A[b] | | 1.2 | | 1.2 | | 1.2 | | 1.2 | | 1 | | 1 | |
| Resolution (bits) | 10 | | 12 | | 8 | | 12 | | 12 | | 8 | | 8 | |
| Topology | Single-Ended | | Differential | | Differential | | Differential | | Differential | | Differential | | Differential | |
| Protected | No | Yes | No | Yes | No | Yes | No | Yes | No | Yes | No | Yes | No | Yes |
| Power (μW) | 63.5 | 65 | 83.2 | 158.5 | 43.4 | 50.2 | 539.8 | 539.8 | 722 | 698 | 145 | 150.7 | 138.96 | 373.45 |
| Sample Rate (MS/s) | 1.07 | 1 | 1.25 | 1.25 | 3.33 | 2 | 25 | 25 | 45 | 40 | 20 | 20 | 9.09 | 11.11 |
| Area (mm$^2$) | 0.07 | 0.075 | 0.34 | 0.5 | 0.064 | 0.073 | 0.072 | 0.072 | 0.075 | 0.075 | 0.015 | 0.017 | 0.356 | 0.384 |
| ENOB (bit) | 8.8 | 8.7 | 11.2[c] | 11.2[c] | 7.2 | 7.7 | 10.9 | 10.9 | 10.9[c] | 10.8[c] | 7.86 | 7.8 | 7.52 | 7.91 |
| FoM$_\text{W}$ (fJ/c.-s.) | 130.8 | 151.5 | 27.9 | 54.3 | 88.6 | 120.7 | 11.3 | 11.3 | 8.5 | 9.8 | 31 | 33.8 | 7.49 | 124.30 |
| INL | -1.2<br>+1.2 | -1.2<br>+1.2 | -0.87<br>+0.80 | -1.01<br>+0.86 | N/A[b] | -0.46<br>+0.44 | -0.76<br>+0.67 | -0.76<br>+0.67 | -0.67<br>+0.72 | -0.73<br>+0.69 | -0.53<br>+0.53 | -0.56<br>+0.58 | -0.16<br>0.11 | -0.74<br>0.59 |
| DNL | -0.6<br>+0.6 | -0.6<br>+0.6 | -0.53<br>+0.79 | -0.72<br>+0.77 | N/A[b] | -0.31<br>+0.37 | -0.49<br>+0.35 | -0.49<br>+0.35 | -0.62<br>+0.37 | -0.68<br>+0.31 | -0.5<br>+0.45 | -0.6<br>+0.52 | -0.13<br>0.14 | -0.62<br>0.61 |
| SFDR (dB) | 64.5 | 64.3 | 86 | 89.6 | 53.7 | 54.6 | 86.6 | 86.6 | 80.5 | 80.2 | N/A[b] | N/A[b] | 60.26 | 60.05 |
| Leakage RMSE (LSBs) | -[d] | -[d] | 117.74/<br>4096 | 384.04/<br>4096 | 0.7/<br>256 | 58/<br>256 | 14.21/<br>4096 | 1625.39/<br>4096 | 52.76/<br>4096 | 1985.25/<br>4096 | 24.5/<br>256 | 103/<br>256 | 30.29/<br>256 | 112.28/<br>256 |
| NRMSE | -[d] | -[d] | 0.0287 | 0.0938 | 0.0027 | 0.2266 | 0.0035 | 0.3968 | 0.0129 | 0.4847 | 0.095 | 0.42 | 0.1183 | 0.4386 |
| Random Bits (Mb/s) | NA | 1 | NA | 0 | NA | 360[e] | NA | 275 | NA | 4080[e] | NA | 200 | NA | 0 |

[a] Simulation only
[b] Value not disclosed
[c] Calculated from FoM$_\text{W}$, Power, and Sample Rate
[d] Reported an unprotected leakage ENOB of 4.6 bits and a protected leakage ENOB of 0.8, RMSE was not reported
[e] A variable amount of random bits are required, the reported value is the average per conversion

adding additional complexity. The security characterization of the ADC demonstrates a high NRSME of 0.4386 compared to the standard design's NRMSE of 0.1183.**Simulation results** indicate that, operating at $11.11\ \text{MSPS}$ with an input frequency of $f_{\text{in}} = 2.71\ \text{kHz}$ and $152\ \text{fJ}/\text{conversion}$, the ADC achieves an effective number of bits (ENOB) of $7.91\ \text{bits}$ and a spurious-free dynamic range (SFDR) of $60.05\ \text{dB}$, demonstrating a balanced combination of speed, accuracy, and energy efficiency. The author encourages researchers to investigate hybrid ADC topologies as a potential approach for enhancing security.

## 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," in *IEEE Trans. Circuits Syst. II*, vol. 67, no. 1, 2019, pp. 14–18.

[2] M. Ashok, E. V. Levine, and A. P. Chandrakasan, "Randomized Switching SAR (RS-SAR) ADC Protections for Power and Electromagnetic Side Channel Security," in *2022 IEEE Custom Integr. Circuits Conf. (CICC)*, Apr. 2022, pp. 1–2.

[3] R. Chen, H. Wang, A. Chandrakasan, and H.-S. Lee, "RaM-SAR: A Low Energy and Area Overhead, 11.3fJ/conv.-step 12b 25MS/s Secure Random-Mapping SAR ADC with Power and EM Side-channel Attack Resilience," in *2022 IEEE Symp. VLSI Technol. Circuits*, Jun. 2022, pp. 94–95.

[4] R. Chen, A. Chandrakasan, and H.-S. Lee, "Sniff-SAR: A 9.8fJ/c.-s 12b secure ADC with detectiondriven protection against power and EM side-channel attack," in *2023 IEEE Custom Integr. Circuits Conf. (CICC)*, Apr. 2023, pp. 1–2.

[5] S. N. Karanth, S. Oruganti, M. Wang, and J. P. Kulkarni, "Randomization Approaches for Secure SAR ADC Design Resilient Against Power Side-Channel Attacks," in *2024 IEEE Int. Symp. Hardware Oriented Security Trust (HOST)*. Tysons Corner, VA, USA: IEEE, May 2024, pp. 282–292.

[6] T. Jeong, A. P. Chandrakasan, and H.-S. Lee, "S2ADC: A 12-bit, 1.25-MS/s secure SAR ADC with power side-channel attack resistance," *IEEE J. Solid-State Circuits*, vol. 56, no. 3, pp. 844–854, 2021.

[7] Z. Chen and I. Savidis, "A Power Side-Channel Attack on Flash ADC," in *2023 IEEE Int. Symp. Circuits Syst (ISCAS)*, May 2023, pp. 1–5.

[8] S. N. Karanth, S. Oruganti, M. Wang, and J. P. Kulkarni, "RI-SAR: Randomized Input SAR ADC Resilient to Power Side Channel Attacks," in *2023 IEEE Physical Assurance Inspection Electronics (PAINE)*, Oct. 2023, pp. 1–7.

[9] N. Koo, "A Hybrid Equalizer for Protection of 1st-Order Delta-Sigma Modulator Against Side-Channel Attack," *IEEE Access*, vol. 12, pp. 175 742–175 751, 2024.

[10] C. Körpe, K. Ahmad, E. Öztürk, K. Tihaiya, R. Tran, H. Yang, J. Yang, G. Dündar, V. J. Mooney, and K. Ozanoglu, "A Side-Channel Attack-Resilient Single-Slope ADC for Image Sensor Applications," in *2025 21st Int. Conf. Synthesis, Model., Analysis Simul. Methods, Appl. Circuits Des. (SMACD)*, Jul. 2025, pp. 1–4.

[11] B. Ginsburg and A. Chandrakasan, "An energy-efficient charge recycling approach for a sar converter with capacitive dac," in *2005 IEEE Int. Symp. Circuits Syst. (ISCAS)*, 2005, pp. 184–187 Vol. 1.

[12] Y.-K. Cho, J.-H. Jung, and K. C. Lee, "A 9-bit 100-ms/s flash-sar adc without track-and-hold circuits," in *2012 Int. Symp. Wireless Commun. Syst. (ISWCS)*. IEEE, 2012, pp. 880–884.

[13] B. Razavi, "The flash adc [a circuit for all seasons]," *IEEE Solid-State Circuits Magazine*, vol. 9, no. 3, pp. 9–13, 2017.

[14] P. G. Flikkema, "Spread-spectrum techniques for wireless communication," *IEEE Signal Processing Magazine*, vol. 14, no. 3, pp. 26–36, 2002.

[15] A. Ghosh, D. Das, J. Danial, V. De, S. Ghosh, and S. Sen, "Syn-S$^{\text{TEL}}$LAR: An EM/Power SCA-Resilient AES-256 With Synthesis-Friendly Signature Attenuation," *IEEE J. Solid-State Circuits*, vol. 57, no. 1, pp. 167–181, Jan. 2022.