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

Ruicong Chen, Hanrui Wang, Anantha Chandrakasan, Hae-Seung Lee
Massachusetts Institute of Technology, Cambridge, MA

2022 IEEE Symposium on VLSI Technology and Circuits (VLSI Technology and Circuits) | 978-1-6654-9772-5/22/$31.00 ©2022 IEEE | DOI: 10.1109/VLSITechnologyandCir46769.2022.9830365

Abstract: This paper presents RaM-SAR, a 12b 25MS/s 11.3fJ/conv.-step secure random-mapping SAR ADC with power and EM side-channel attack resilience. Each conversion is randomly mapped to one of the thousands of conversion sequences to randomize power supply traces. This technique protects against neural network based power and EM side-channel attacks. It enables protection with much lower energy and area overheads compared to the prior works. A prototype in 65nm CMOS demonstrates significant improvements with 12.5× higher bandwidth and 4.8× better energy-efficiency over prior works.

Introduction: As shown in Fig. 1**,** an attacker can perform an ADC power side-channel attack (PSA) or Electro-magnetic side-channel attack (EMSA) to steal confidential and sensitive information by tapping into the power supply of the ADC [1,2,3,4]. [3] (Fig. 2, left) implemented a current equalizer to decorrelate the supply current of all blocks from digital outputs. [4] (Fig. 2, middle) proposed to control the unit capacitors for the MSB bits independently and switch them randomly to randomize the power traces. Recently, integrated regulators with control loop randomizers [5,6] and shunt linear regulators [7,8] have been proposed for general PSA and EMSA protection with trade-off of the performance of the core circuit. The current work reduces the area and energy overhead and increases the sampling rate, which broadens the secure ADCs into video applications.

Proposed RaM-SAR Architecture: In this work, we propose an energy-efficient and high-speed secure SAR based on random mapping (RaM-SAR) to randomize the conversion scheme (Fig. 2, right). It is based on the LSB-first SAR [9]. The LSB-first SAR has different conversion switching sequences for each digital output but it's deterministic as the initial guess is always the previous digital output. Therefore, the LSB-first SAR is not inherently safe from attacks. However, by randomizing the initial guess instead, the conversion sequence for a given input is also randomized. The LSB-first SAR needs up to 25 cycles for a 12bit conversion, which limits its usage in high sampling rate applications. As will be explained, the RaM-SAR uses only 15 cycles. A RaM-SAR prototype fabricated in a 65nm CMOS achieved a FoM of 11.3fJ/conv.-step.

Fig. 3 shows the single-ended version of the proposed RaM-SAR architecture along with its block design. Differential version is implemented. The SAR ADC is split into two half DACs and two half-sized comparators to provide two thresholds. Two thresholds reduce the worst-case number of cycles needed per conversion from 25 to 15. Noise averaging between the two halves is performed in the last couple of LSB decisions to eliminate the noise penalty due to half-size DACs and comparators. Therefore, there is no extra area/power overhead in this split DAC design. Foreground calibration removes the effect of capacitor mismatches.

Fig. 4 shows example conversions of RaM-SAR. In the first phase (P1), the differential input voltage is sampled onto the bottom plates of the CDAC (Fig. 5). D_{RND}, the 11b pseudo-random number generated by on-chip linear feedback shift registers, is set to the random start. The thresholds of the comparators are set according to the random start. If both outputs of the comparators are high, then the random start was too low, so the direction of bit-cycling DIR is set to 1 to increase the thresholds. The inverse holds if both outputs of the comparators are low. The DIR controls both extra LSBs. Otherwise, the random start is correct, and the RaM-SAR combines the DACs for LSB decision as in Fig. 6.

The conversion sequence is randomized by the random start, which significantly weakens the correlation between power/EM side-channel leakage and digital outputs. The two-threshold, two half-DAC arrangement further randomizes the power supply traces. In the second phase (P2), R and S are set to the index of the lowest one and two-bits of the random start that are not currently set to DIR, respectively. Two thresholds make P2 faster compared to [9]. Bit R for the lower DAC and bits S for upper DAC are inverted to move in the desired direction. This is repeated until one of the outputs of the comparators flips, indicating that the target value has overshot. The rest of the MSBs are now finalized for this conversion. Let N be the current bit under test. The conversion proceeds to the LSB in the Ternary Search Phase (P3) first and then the Binary Search Phase (P4) if N is less than 3. In the P3, 3b conversion is finished in 2 bit-cycles. The bit-cycling continues as the ToLSB phase in [9] in the P4 and the DACs are combined. When bit-cycling has gone back down to the LSB, conversion is completed, and the DACs are purged.

Measurement Results: Fabricated in the 65nm LP process, the RaM-SAR takes 0.072mm^2 (Fig. 7). The prototype demonstrates significant improvements with 12.5× higher bandwidth and 4.8× better energy-efficiency over prior secure ADCs (Fig. 8). We performed CNN based PSA and EMSA against both the unprotected and protected ADCs (Fig. 9). An example image is fed into the ADCs to test the efficacy of the protection scheme (Fig. 10). With protection, the EMSA result is random and does not disclose useful information of the original image. In Fig 9 and 10, it is shown that RaM-SAR protects the input signals from both PSA and EMSA. The SFDR is 86.6dB (Fig. 11). The DNL is -0.49/+0.35LSB and the INL is -0.76/+0.67LSB. The ADC achieves a FoM of 11.3fJ/c.-s, which is comparable with the state-of-the-art energy-efficient ADCs [10,11], with both PSA and EMSA resilience (Fig. 12).

Acknowledgment: This research was supported by DARPA and Navy-ONR under contract N00014-20-1-4005 and MIT Center for Integrated Circuits and Systems. The authors thank Prof. Song Han and Maitreyi Ashok at MIT for their support and feedback.

References: [1] V. Gadde, *et al.*, ASSCC 2018; [2] M. Kim, *et al.*, T-CAS II 2020; [3] T. Jeong, *et al.*, JSSC 2021; [4] M. Ashok, *et al.*, CICC 2022, accepted for publication; [5] M. Kar, *et al.*, ISSCC 2017; [6] A. Singh, *et al.*, ISSCC 2019; [7] A. Ghosh, *et al.*, ISSCC 2021; [8] D. Das, *et al.*, ISSCC 2020; [9] F. Yaul, *et al.*, ISSCC 2014; [10] X. Tang, *et al.*, ISSCC 2021; [11] J. Liu, *et al.*, ISSCC 2020;

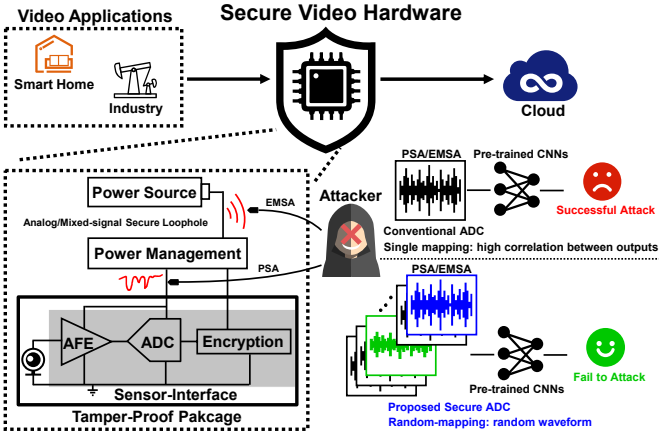


Fig. 1 . Potential security loopholes in video hardware

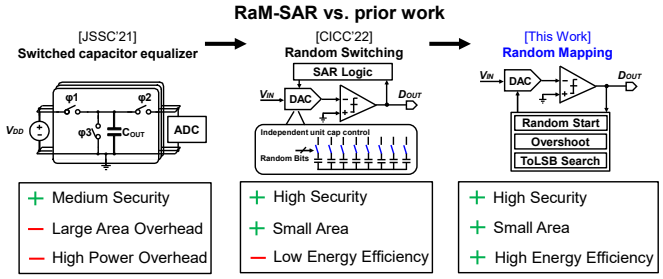


Fig. 2 . Comparison with prior works

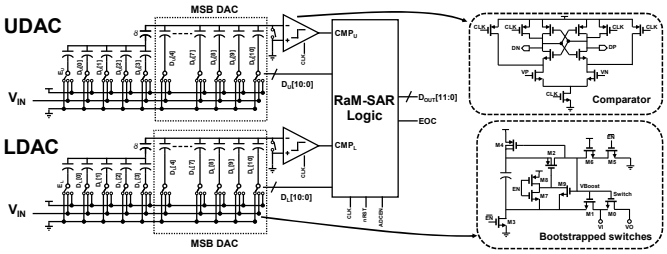
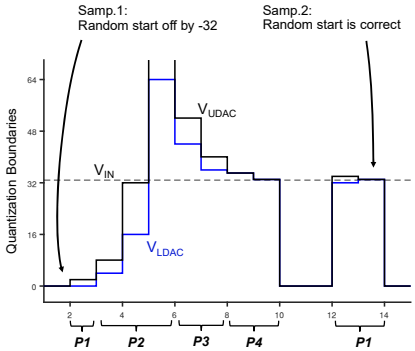


Fig. 3 . Proposed RaM-SAR architecture and block diagram

Samp.1 Conversion Table

Cycle	$D_L[5:0]+E_L$ $D_U[5:0]+E_U$	CMP_L CMP_U	
1	000000 + 00	Hi	P1[1]
	000000 + 10	Hi	
2	000010 + 10	Hi	P2[2]
	000011 + 10	Hi	
3	001110 + 10	Hi	
	011110 + 10	Hi	
4	111110 + 10	Lo	
	111110 + 10	Lo	
5	101010 + 10	Lo	P3[1]
	110010 + 10	Lo	
6	100010 + 10	Lo	
	100110 + 10	Lo	
7	100010 + 01	Lo	P4[2]
8	100000 + 01	Lo	
End	100000		



[1]LSB in P1~P3 is in gray code since the weight of E_L and E_U is 2LSB in the 12b resolution when the DAC is split into UDAC and LDAC.
[2]E_L is always 0 after combination of UDAC and LDAC in P4. The weight of E_U now is one LSB due to the combination in P4.

Fig. 4 . Example conversions of RaM-SAR

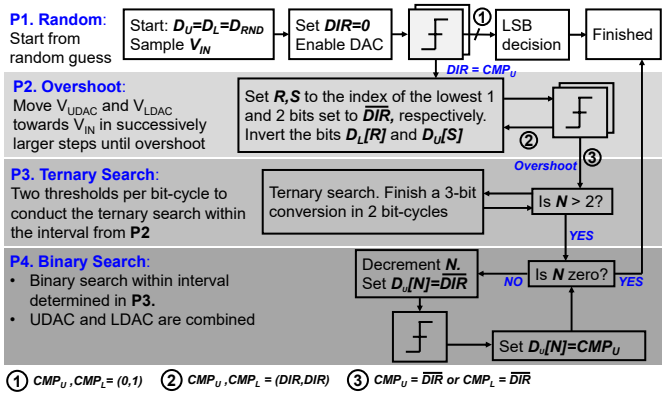


Fig. 5 . Flowchart of RaM-SAR

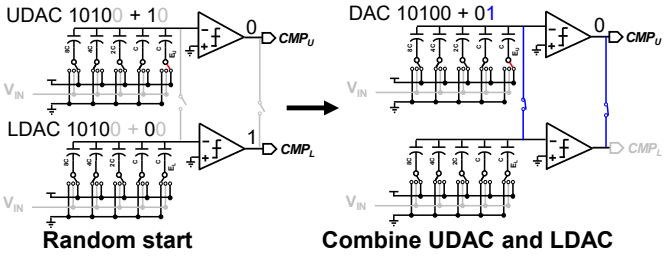


Fig. 6 . Conversion for a correct random start

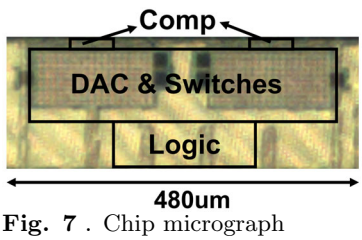


Fig. 7 . Chip micrograph

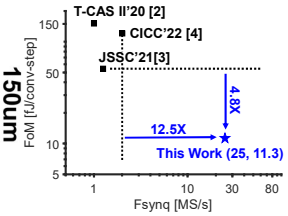


Fig. 8 . FoM vs Speed

■ **Bit-wise accuracy with ramp input (averaged across 3 ADCs)**

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]
VDD-side PSA[1] (unprotected[2])	99.72	99.83	99.45	99.36	99.56	99.85	99.32	99.17	99.23	96.47	91.03	92.21
VDD-side PSA (protected)	62.35	58.41	61.23	55.39	53.27	46.38	48.73	52.19	53.14	47.26	49.71	50.10
GND-side PSA (unprotected)	99.19	99.43	99.58	99.16	99.75	99.43	99.28	99.71	99.26	95.43	86.17	76.15
GND-side PSA (protected)	67.16	54.61	62.13	54.16	46.73	44.72	56.43	57.16	53.71	52.18	55.46	49.78
EMSA[1] (unprotected)	99.26	98.97	99.20	98.92	98.94	98.78	98.70	97.58	98.11	95.89	92.79	89.93
EMSA (protected)	56.04	56.12	54.33	48.71	47.57	57.88	58.00	45.14	51.67	49.71	50.18	50.40

■ **RMS error in LSB for various ADC input signals (averaged across 3 ADCs)**

RMS error (LSBs)	Ramp	ECG	Image	Sine0.1Fs	Sine0.2Fs	Sine0.3Fs	Sine0.4Fs	Sine0.5Fs
VDD-side PSA (unprotected)	14.21	5.32	25.16	16.74	21.46	17.21	16.72	25.76
VDD-side PSA (protected)	1625.39	1534.95	1764.82	1763.27	2436.01	2134.87	2246.82	2114.94
GND-side PSA (unprotected)	25.45	13.15	21.46	43.16	34.94	26.18	25.64	28.32
GND-side PSA (protected)	1546.73	1374.28	1964.72	2641.76	2463.18	2397.64	2267.83	2846.76
EMSA (unprotected)	37.06	20.58	84.65	28.45	33.28	23.77	25.38	42.19
EMSA (protected)	1839.42	1944.80	1729.53	1943.56	2137.39	2365.32	2274.85	2371.84

[1]Convolutional Neural Network (CNN) based side-channel attack is done by collecting 500K samples from a ramp signal as in [3] on a training ADC and performing the attack on 3 other ADCs with 50K samples for various inputs.
[2]Unprotected mode uses a fixed initial guess rather than random guess in protected mode.

Fig. 9 . Power/EM attacks of unprotected vs. protected ADCs

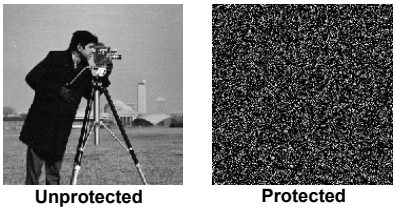


Fig. 10 . Example image of EMSA results

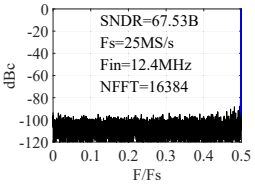


Fig. 11 . Measured FFT plot of RaM-SAR

		This Work	JSSC'20[3]	CICC'2022[4]	T-CAS II'20[2]	ISSCC'21[10]	ISSCC'20[11]
Architecture		RaM-SAR	SAR	RS-SAR	SAR	Pipe-line SAR	SAR
Technology [nm]		65	65	65	180	40	40
Supply Voltage [V]		1.2	1.2	1.2	1.2	1.2	1.2
Resolution [b]		12	12	8	10	13	13
Protection	Protect Method	Random Mapping	Current Equalizer	Random Switching	Noise Injection	-	-
	Protected Blocks	All Blocks	All Blocks	All Blocks	CDAC only	-	-
	Neutralized Attacks	EM + Power	Power only	EM + Power	Power only	-	-
	Attack Method	CNN[1]	CNN	CNN	Template-Matching	-	-
	VDD-PSA RMSE[2]	0.40	0.094	0.23	0.92[3]	-	-
	GND-PSA RMSE	0.38	0.21	N/A	N/A	-	-
	EMSA RMSE	0.45	N/A	0.18	N/A	-	-
Sampling Rate [MS/s]		25	1.25	2	1	40	40
Area [mm^2]		0.072	0.5	0.073	0.075	0.056	0.005
ENOB [b]		10.9	11.2	7.7	8.7	12.3	11.2
FoM (fJ/conv.-step.)		11.3	54.3	120.7	151.5	4.1	6.4

[1]Convolutional Neural Network (CNN) based side-channel attack
[2]Root-mean-square error (RMSE) in LSB is normalized to full scale
[3]Attack is done on V_{ref} only
[4]Does not include random number generator

Fig. 12 . Comparison Table