Secure Analog-to-Digital Converters

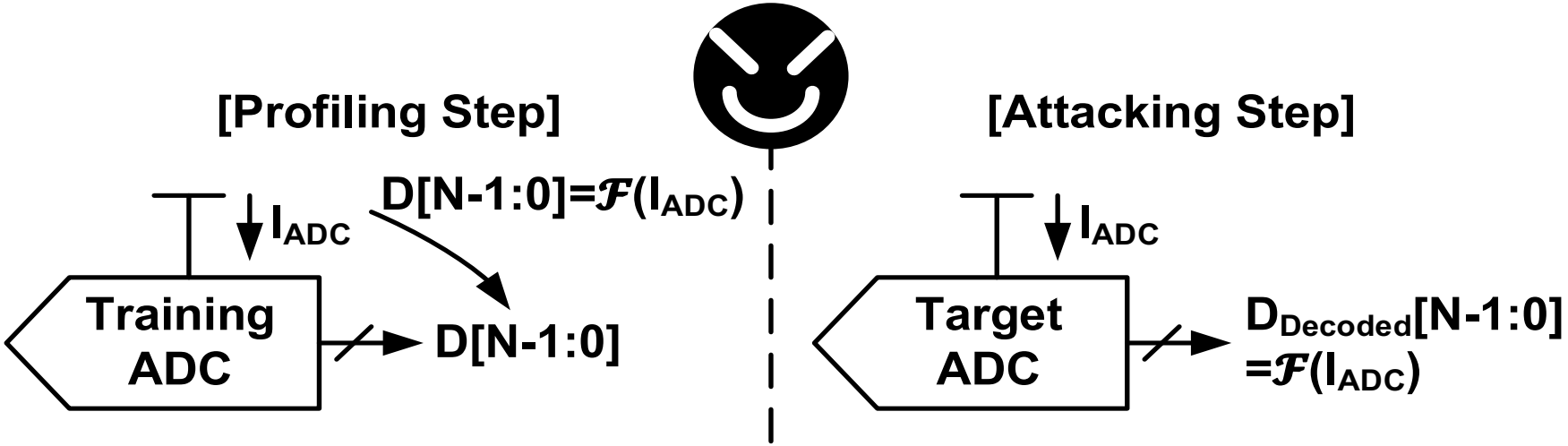
Hae-Seung (Harry) Lee
Collaborator: A. Chandrakasan

Massachusetts Institute of Technology

Problem Statement

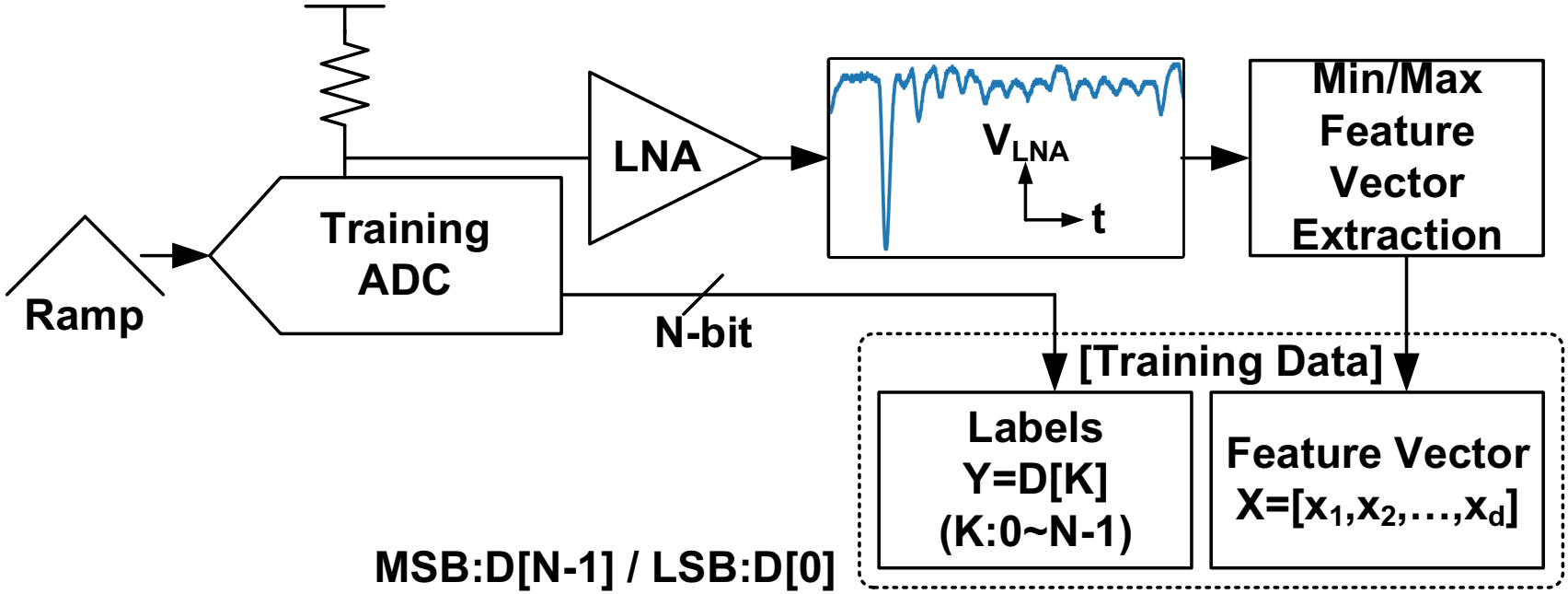
- Side-channel attacks (SCAs) such as power side-channel attacks (PSAs) and electromagnetic side-channel attacks (EMSAs) are of increasing concerns.
- Much research has been done on SCAs and countermeasures on digital systems.
- System security is only as good as the weakest link in the system.
- Analog-to-digital converters (ADCs) are ubiquitous in most electronic systems, yet their SCA vulnerability received little attention.
- ADCs, due to their switching activities, are vulnerable to SCAs.

Attack Overview



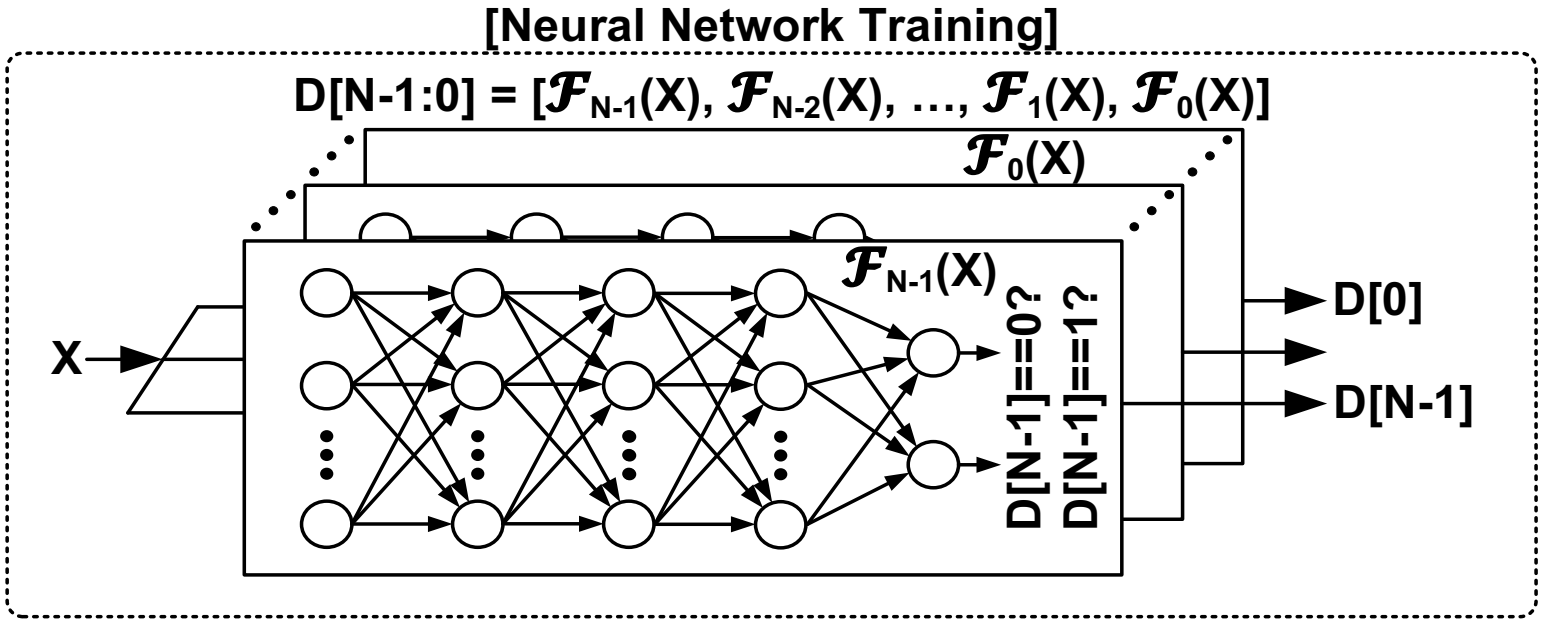
- PSA (or EMSA) consists of 2 steps
  - Profiling: Build mapping function D[N-1:0]=$\mathcal{F}$(I_{ADC})
    - Use **neural networks** to build $\mathcal{F}$
  - Attacking: Use $\mathcal{F}$ to decode I_{ADC} into $D_{Decoded}$[N-1:0]

Profiling – Training Data Acquisition (PSA)



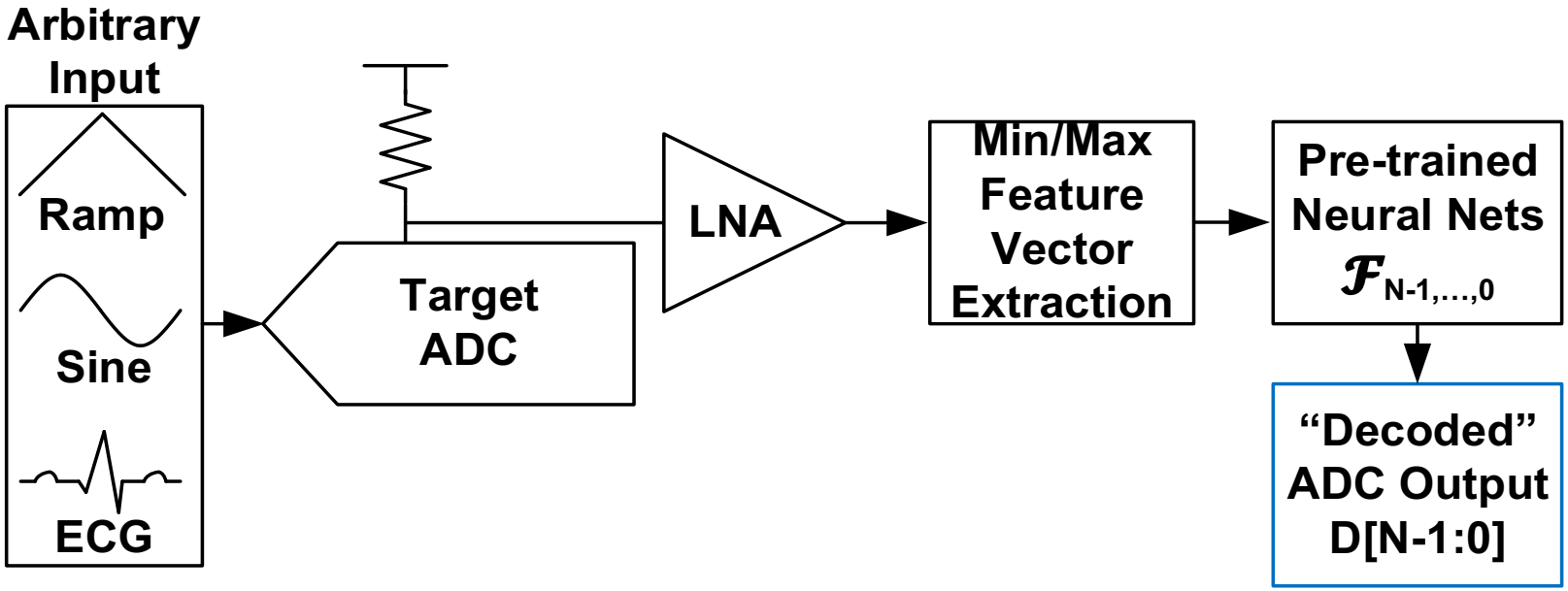
- Obtain [Feature vector : A/D conversion result] pairs from training ADC
  - We used Min/Max current values each ½ clock cycle as feature vector

Profiling – Neural Network Training



- Train “N” neural networks to build mapping function D[N-1:0]=$\mathcal{F}$(X)
  - Each fully-connected neural network decodes different bit of D[N-1:0]

Attacking



- By using pre-trained neural networks $\mathcal{F}(X)$, attack decodes supply current waveform of target ADC that is converting arbitrary input

PSA Results – Commercial ADC-A

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

Bit-wise Acc. (%)	D[11]	D[10]	D[9]	D[8]	D[7]	D[6]	D[5]	D[4]	D[3]	D[2]	D[1]	D[0]
ADC1	100.0	100.0	100.0	100.0	100.0	99.98	100.0	99.98	99.93	99.99	99.36	96.23
ADC2	100.0	100.0	100.0	100.0	99.99	100.0	99.99	99.98	99.78	100.0	99.33	97.30
ADC3	100.0	100.0	99.99	100.0	99.77	99.98	99.75	99.93	99.05	99.87	96.50	91.71

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

RMS error (LSB)	Ramp	ECG	Sine0.1Fs	Sine0.2Fs	Sine0.3Fs	Sine0.4Fs	Sine0.5Fs
ADC1	0.47	0.65	2.46	20.06	2.97	2.18	5.21
ADC2	1.26	1.12	2.69	3.47	4.34	6.08	5.27
ADC3	7.46	2.14	10.79	16.11	18.79	19.77	17.89

❑ R_{MEAS}=10Ω, LNA gain=10

PSA Results – Commercial ADC-B

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

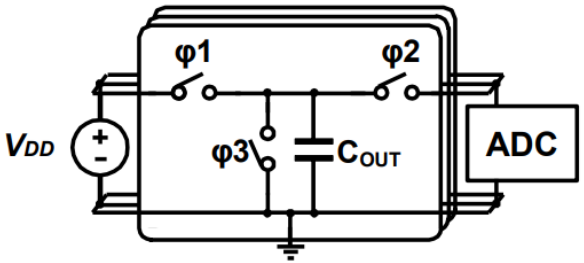
Bit-wise Acc. (%)	D[11]	D[10]	D[9]	D[8]	D[7]	D[6]	D[5]	D[4]	D[3]	D[2]	D[1]	D[0]
ADC1	100.0	100.0	99.81	99.97	99.82	99.36	99.85	99.23	99.82	99.96	99.69	63.87
ADC2	99.98	99.99	99.97	99.95	99.96	99.93	99.95	99.85	99.89	99.96	99.83	63.31
ADC3	99.90	99.95	98.73	99.48	99.16	99.30	99.66	99.21	99.68	99.93	97.08	55.62

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

RMS error (LSB)	Ramp	ECG	Sine0.1Fs	Sine0.2Fs	Sine0.3Fs	Sine0.4Fs	Sine0.5Fs
ADC1	25.24	5.51	14.10	10.21	11.41	12.66	13.51
ADC2	25.18	9.73	7.08	4.81	4.86	10.75	2.87
ADC3	72.80	32.27	50.88	40.79	58.59	44.70	63.79

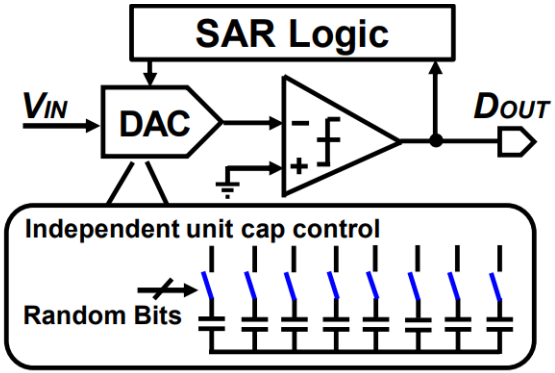
❑ R_{MEAS}=39Ω, LNA gain=10

Previous Secure ADCs (MIT)



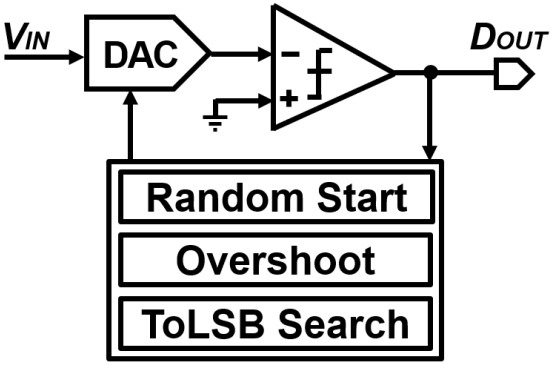
Switched capacitor Equalizer

T. Jeong, JSSC 2021



Random timing conversion

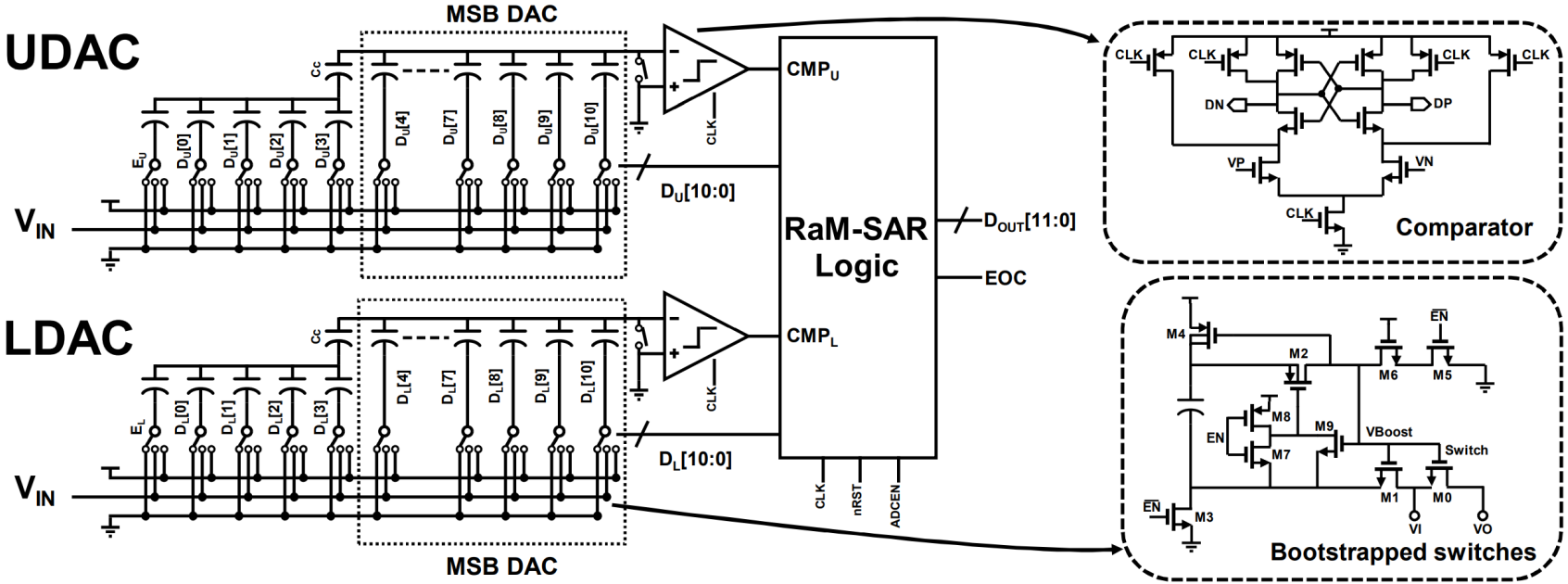
M. Ashok, CICC 2022



Random mapping Conversion

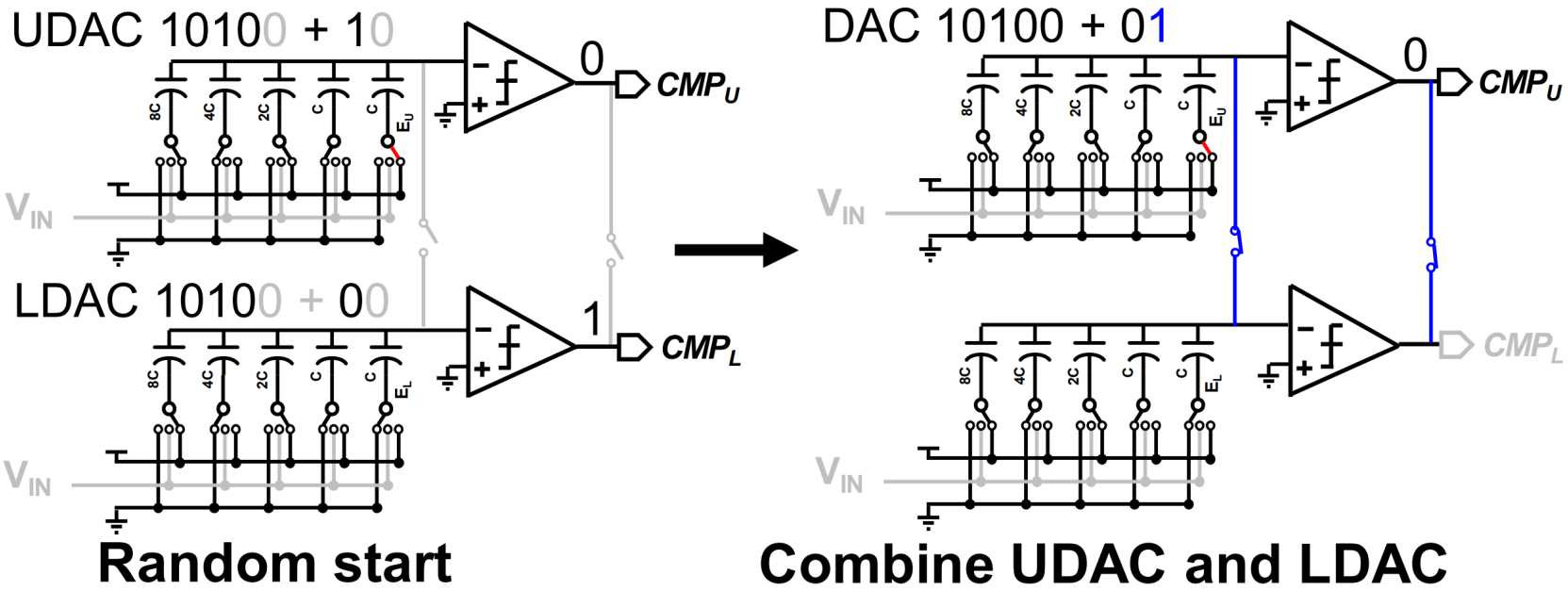
R. Chen, VLSI 2022

Enhanced Random Mapping ADC (1)



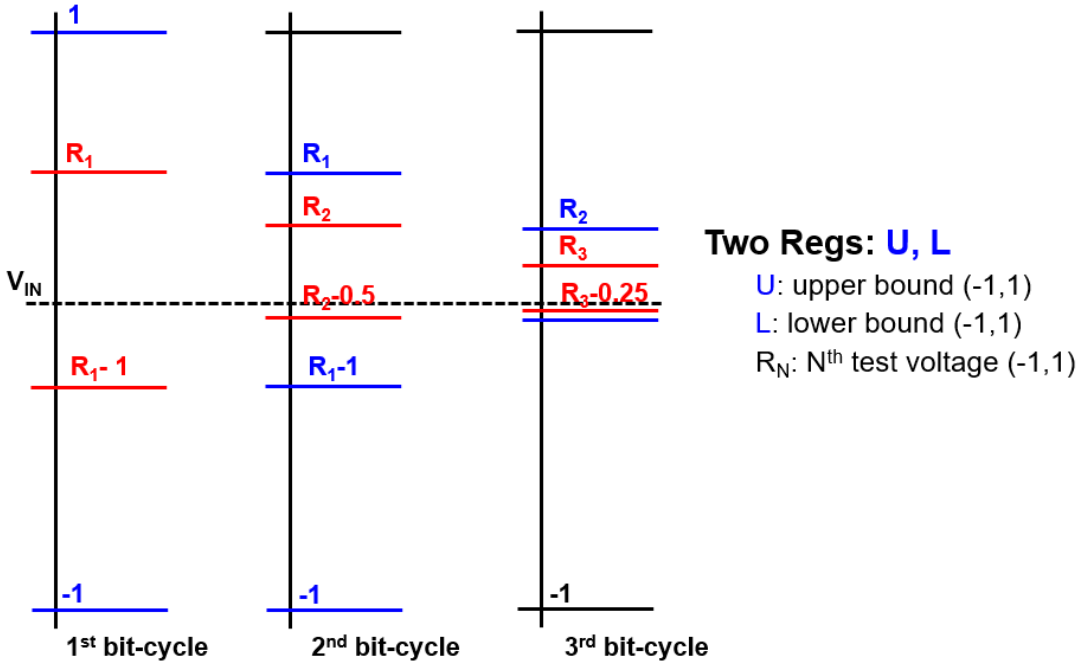
- Architecture
  - Split DAC into UDAC and LDAC (no power/area penalty)
  - Each bit search is randomized
  - Little power/area/conversion time overhead compared with unsecure ADCs
  - Much more effective power trace randomization

Enhanced Random Mapping ADC (2)



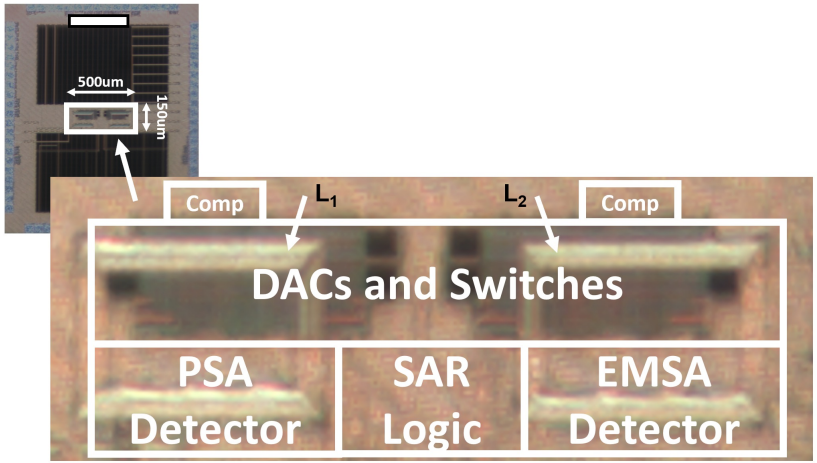
- **Combine DACs for LSB decision to lower noise**

Example Conversion Sequence



Provides on average 9×10^{12} different power supply traces for each digital output codes (if true random-number generator is used)
Total 3.6×10^{16} traces for a 12 bit ADC

Chip Micrograph



Chip specifications	
Process technology	65nm LP
VDD [V]	1.2
Resolution [b]	12
Sampling Rate [MS/s]	40
Area [mm²]	0.075
ENOB [b]	10.8
FoM (fJ/c.-s)	9.8

Side-channel Attack Results (1)

■ 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])	99.18	98.46	97.25	98.76	99.75	99.38	99.16	96.75	93.48	92.12	88.17	83.26
VDD-side PSA (protected)	52.76	51.72	48.19	48.76	49.76	50.76	50.28	53.17	54.71	57.15	55.86	45.76
GND-side PSA (unprotected)	99.56	99.42	96.16	97.48	96.23	99.81	99.43	98.23	97.84	85.16	76.48	78.63
GND-side PSA (protected)	48.76	49.75	51.76	52.84	53.91	53.27	45.86	52.74	50.17	46.26	50.75	50.19
EMSA[1] (unprotected)	99.43	98.16	99.47	99.28	98.71	99.72	98.63	99.75	96.17	93.28	90.45	88.94
EMSA (protected)	51.24	53.82	54.12	49.15	48.72	48.61	47.74	45.54	46.72	52.47	50.14	50.64

Side-channel Attack Results (2)

■ 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)	52.76	20.16	32.14	16.78	20.16	25.76	23.75	45.13
VDD-side PSA (protected)	1985.25	2675.17	1863.76	2516.78	2394.64	1963.76	2246.76	1876.18
GND-side PSA (unprotected)	48.91	45.18	36.76	32.17	25.18	28.76	32.17	42.73
GND-side PSA (protected)	2054.12	1986.47	2163.76	2246.46	1768.46	1732.94	2234.76	2346.71
EMSA (unprotected)	36.04	53.17	78.46	62.17	58.76	63.76	56.84	31.93
EMSA (protected)	1806.74	1746.52	2246.37	2634.76	2519.46	2476.83	2546.98	2246.83

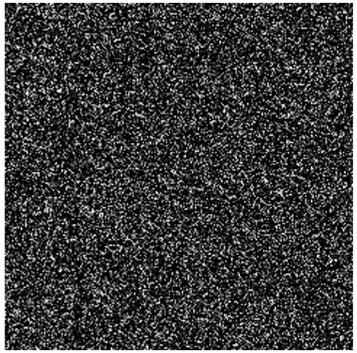
[1]Convolutional Neural Network (CNN) based side-channel attack is done by collecting 500K samples from a ramp signal as in [3] on a training ADC and performing the attack on 3 other ADCs with 50K samples for various inputs.
[2]The protected ADC is in the secure mode.

- **Small RMS error without protection**
- **Large RMS error with protection**

Example Images of EMSA

Original image

EMSA on the unprotected ADC



EMSA on the protected ADC

- **Information is leaked without protection**
- **Information is leakage is prevented with protection**

Conclusions

- Side-channel attack (SCA) on-chip countermeasure techniques incur non-negligible power and performance overheads
- A secure ADC with very effective protection scheme is proposed
- The prototype in 65nm process achieves a FoM of 9.8fJ/c.-s
- The prototype protects against PSA and an EMSA with high effectiveness and low power/area overhead