ISCAS 2021
Daegu, KOREA, MAY 22-28
IEEE International Symposium on Circuits and Systems

IEEE
Advancing Technology for Humanity

CAS

A Switched Capacitor Power Side Channel Attack (P-SCA) Detection Circuit in 65nm

Nipun Kaushik and John Hu

Oklahoma State University

2021 IEEE International Symposium on Circuits and Systems
May 22-28, 2021 Virtual & Hybrid Conference

Outline

1. Side channel attacks - Countermeasures to detection
2. Power Side channel attack (P-SCA) and threat model
3. Circuit and System Level considerations
4. Results and Conclusion
5. Future Work

Side Channel Attacks

- Threat to devices handling sensitive information (Smart cards, servers, etc.)
- Countermeasure against SCA

  Work towards making the device robust to against side channel attacks [1-4]
- Detection circuits for power side channel attacks (P-SCA)

  Focus on detection of an attack in real time - machine learning [5]-[6],

  Ring oscillator based circuit [7]

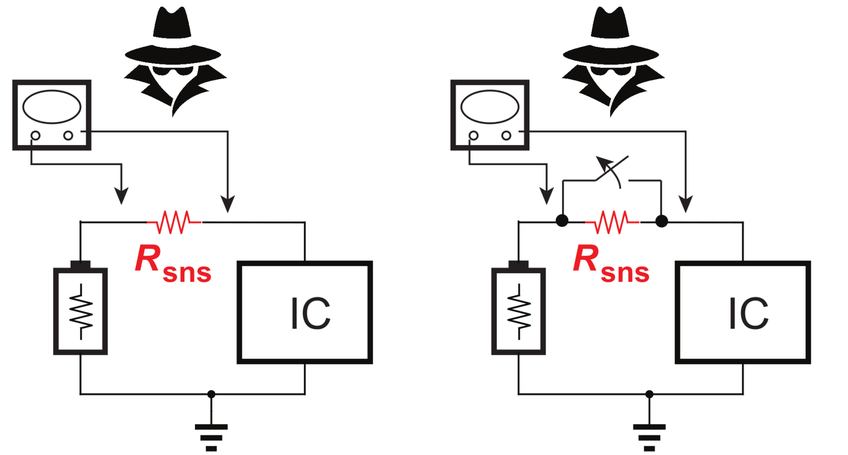
Prior Arts

Threat Model	TCAS-I	ICCAD
Detection Method	PDN	ΔV Sensing
Sensing circuit	ADC	Ring OSC
No. of Sensors	Multiple	Multiple
Classification	Data intensive	Simple
R_{sns} @ BGA	YES	YES
R_{sns} @ PCB	YES	NO

Power side channel attack and threat model

How is a P-SCA conducted?

1. Insertion of a sense resistor in the power supply of the device.
2. Send plain text to the device
3. Collect a large number of traces during encryption process
4. Use statistical methods to extract the secret key.

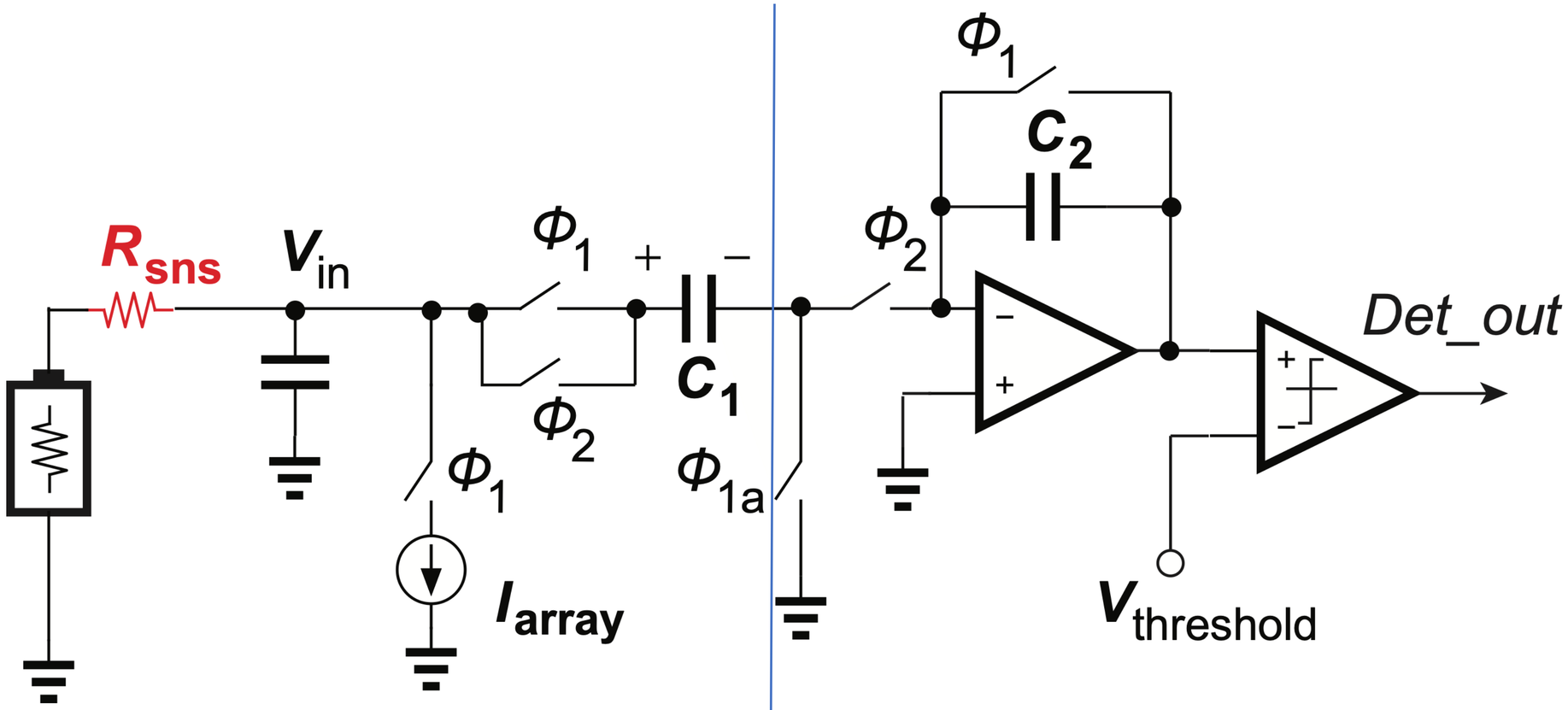


R_{sns} present all the time
Detection: hidden element (PCB Trojan) detection

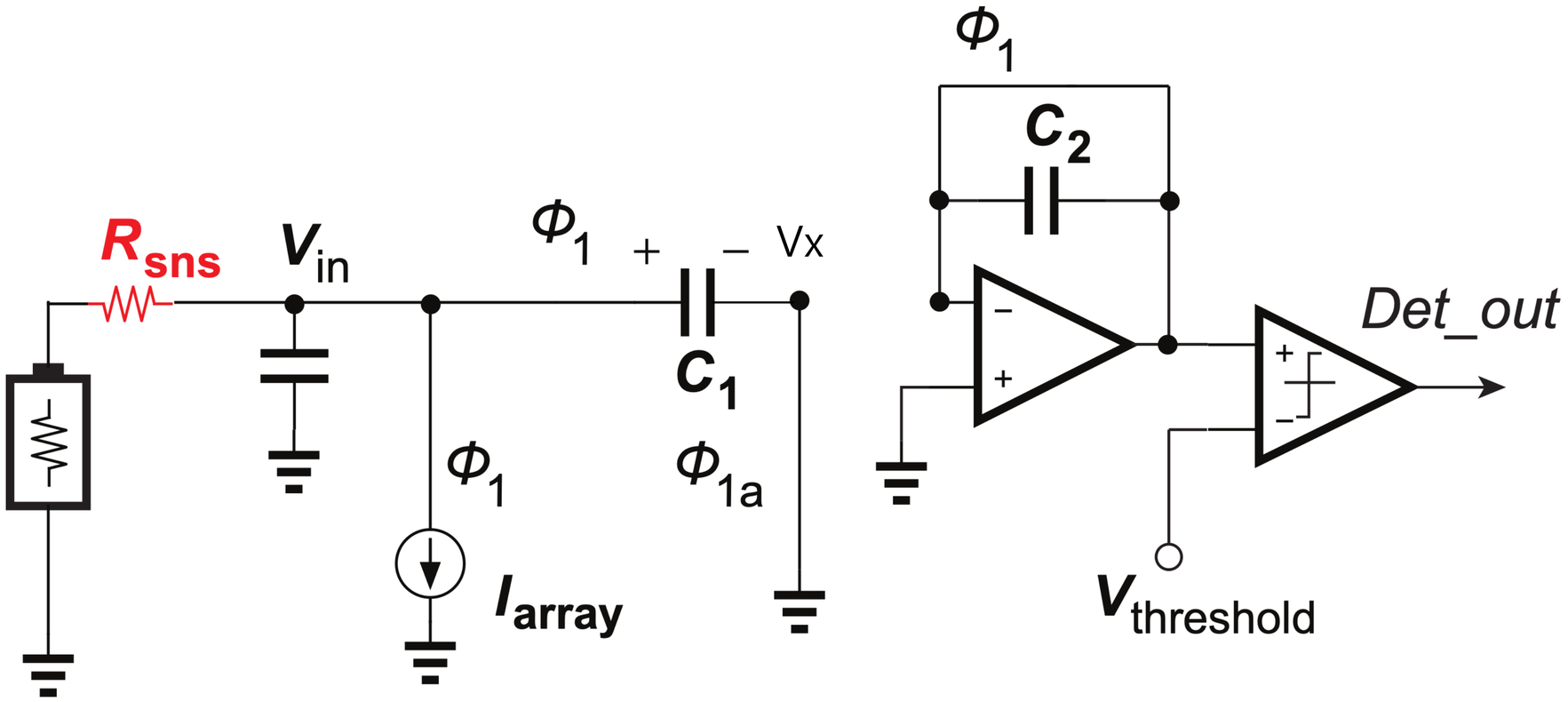
R_{sns} activated at runtime
Detection: this paper

Threat model for this approach assumes that the **sense resistor is inserted at runtime**

System and circuit level considerations

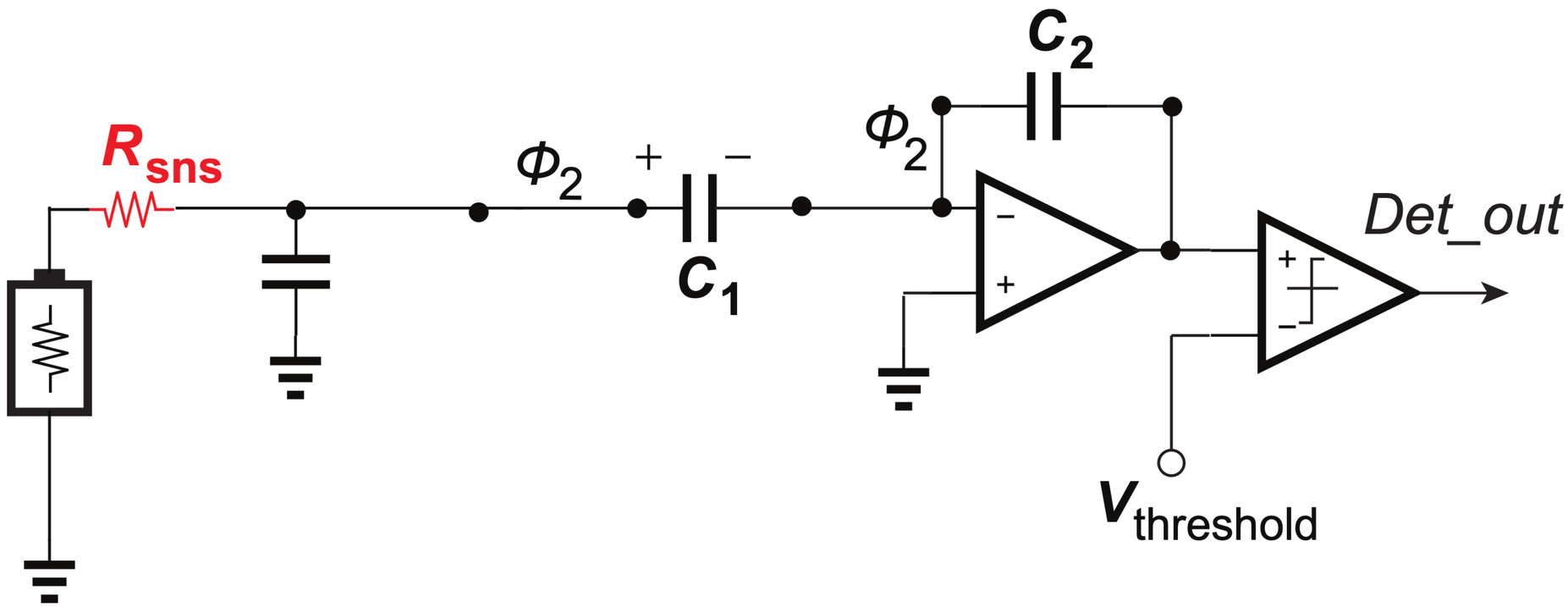


In Phi1



Charge at Vx $Q_x = -(I_{array}.R_{sense})(n).C_1$ Phi 1(advance) Bottom plate sampling [8]-[9]

In Phi2



Charge at Vx $Q_x = -V_{out}(n + 1/2).C_2$ 1/2 is the next half of the cycle

Metrics for the topology

Sampling rate = 200KHz

Charge redistribution and conversion

$$-V_{in}C_1 = -Vout\left(n+\frac{1}{2}\right)C_2$$

Output is a just a scaled and delayed version of input

$$V_{out}\left(n+\frac{1}{2}\right) = \frac{C_1}{C_2}.V_{in}(n) \quad [10]$$

Sampling frequency can be usually defined by

- Input time constant
- Speed of current array
- Bandwidth of the OTA (minimize settling error)

Operational transconductance amplifier

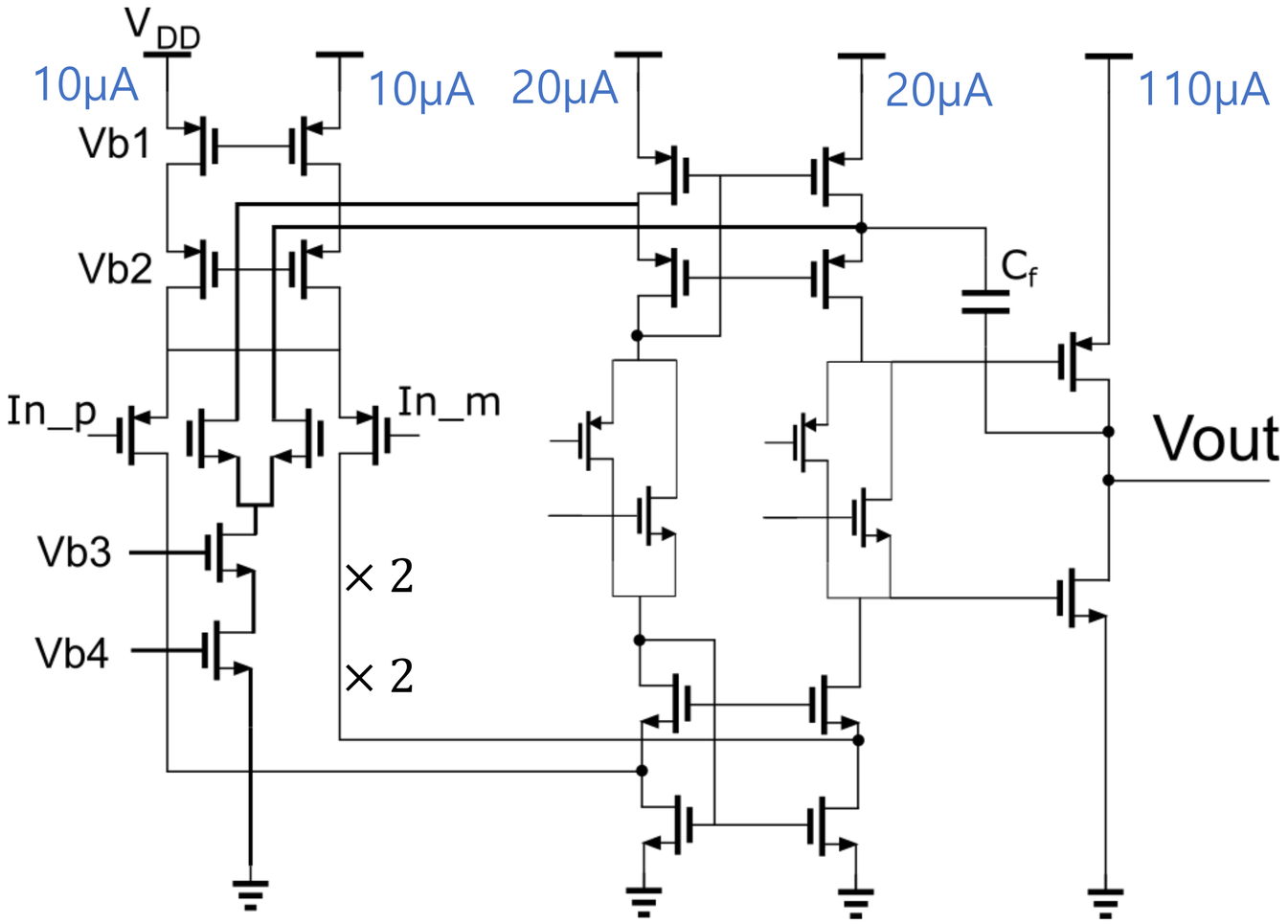
Vdd = 1V

Length = 120nm

$Gain = (gm_n + gm_p)R_{ocas}.(gm_n +$

$gm_p)R_{out}$ = 51 dB

Bandwidth = 16MHz with PM 89º



Baker, J. [11]

General Guideline

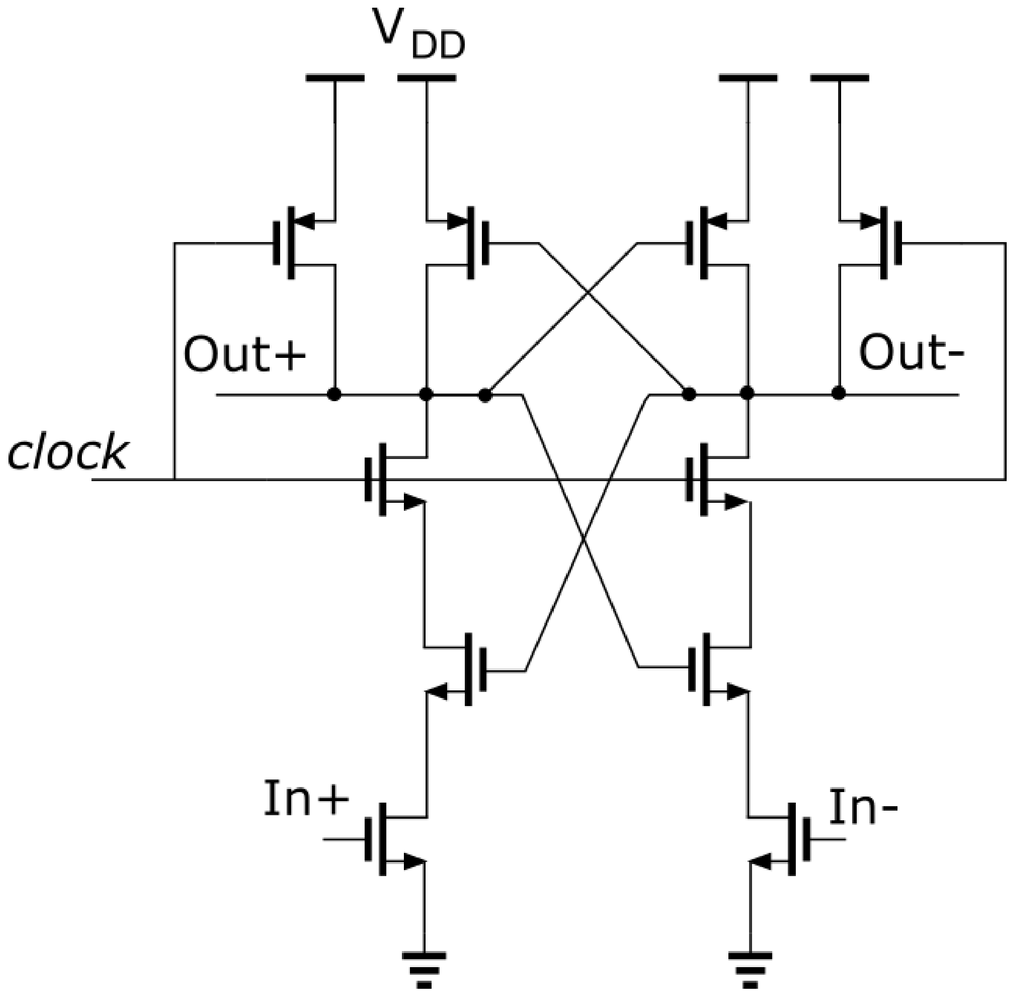
VDD = 1V

Clocked comparator for final result

$V_{threshold}$ tuned outside, ideally $\frac{VDD}{2}$

This topology used to minimize kickback noise

Channel Length = 120nm



Baker, J. [11]

Metrics for P-SCA detection

1. Number of sensors/detectors
2. Area
3. Power
4. Method of detection
5. Detection Time
6. Accuracy

Detection Time

Transient simulation in Cadence at 65nm CMOS at typical corner

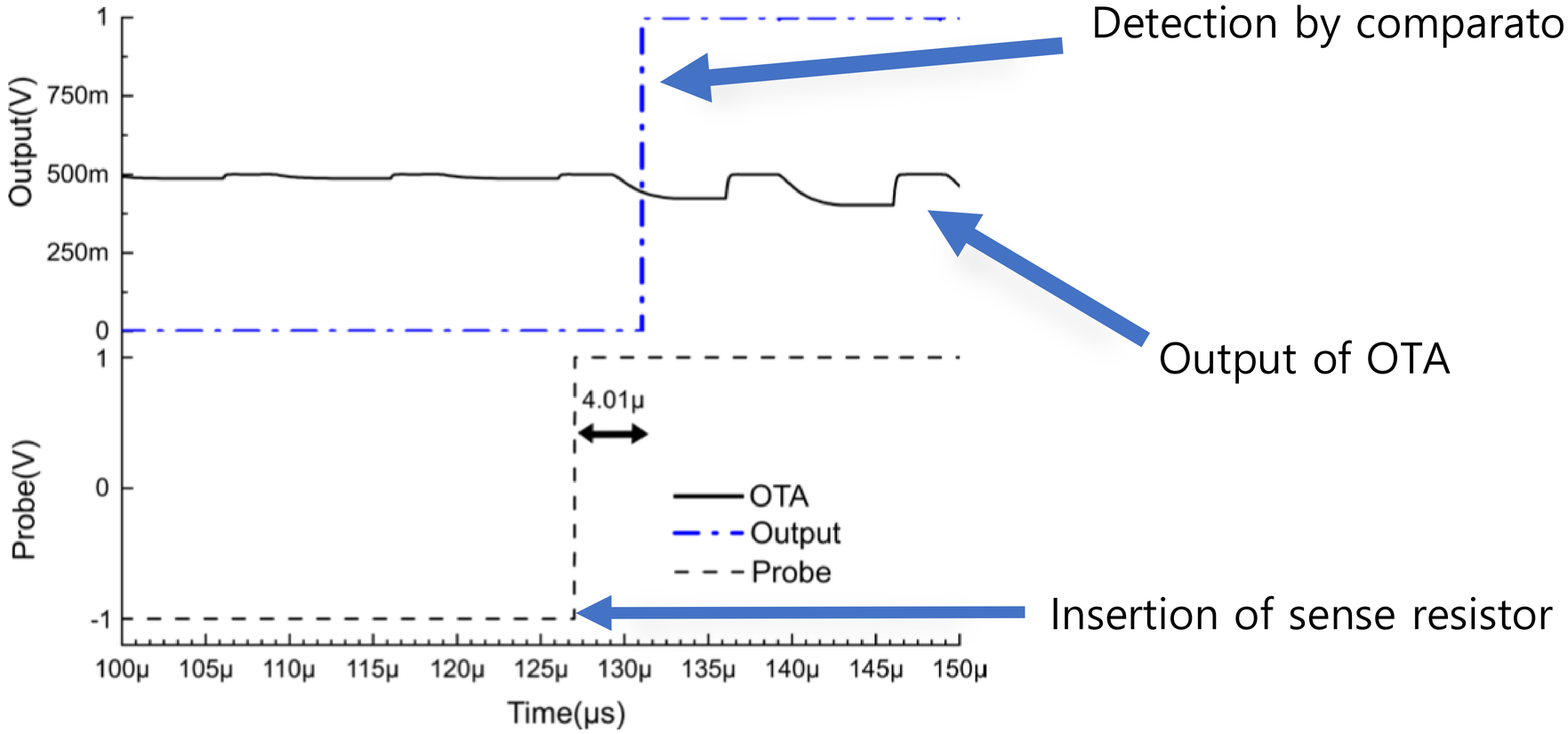
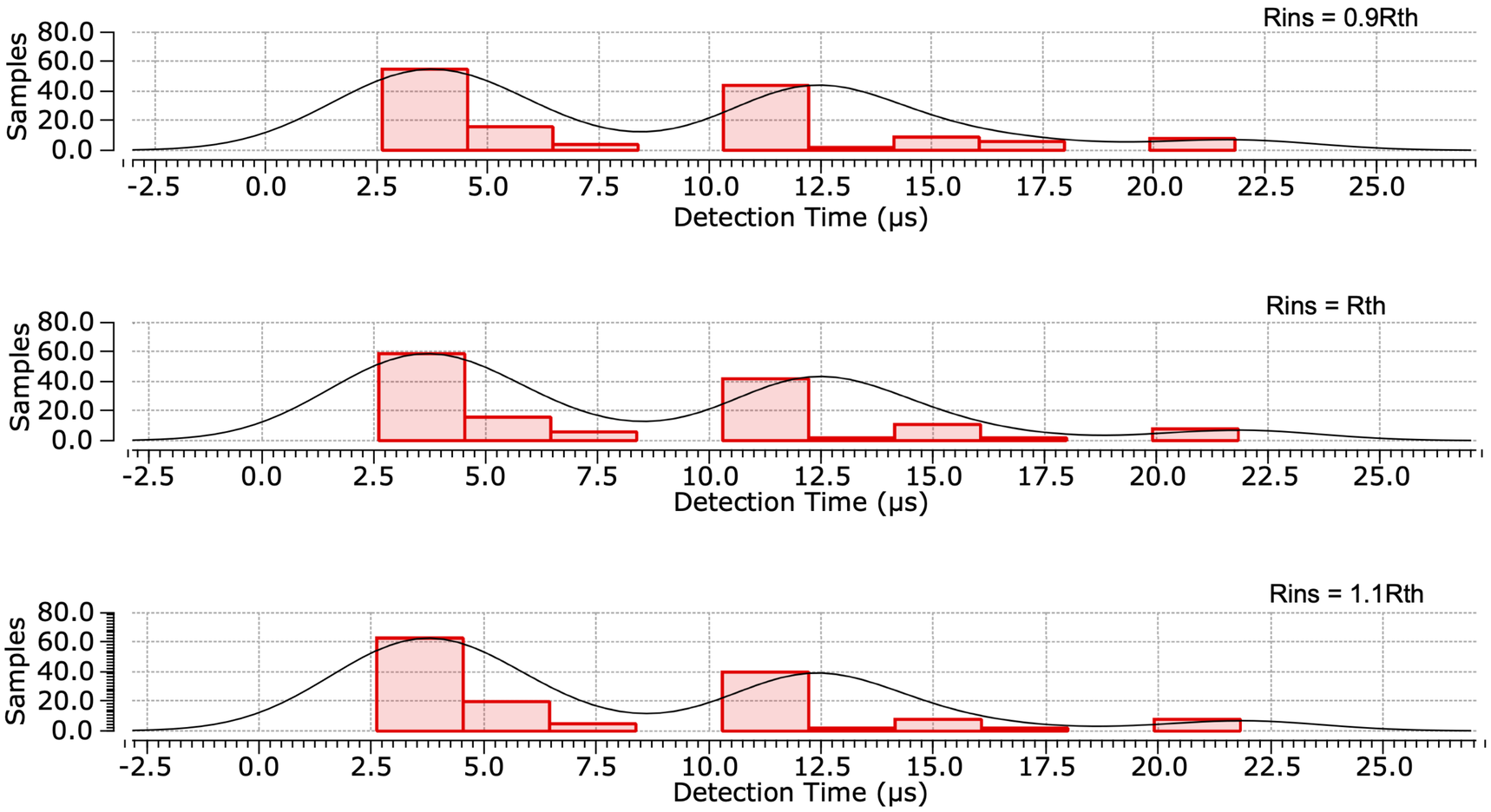


Fig. 5. Detection Time

Detection Accuracy MC analysis

Detection time and detection accuracy using Monte Carlo analysis

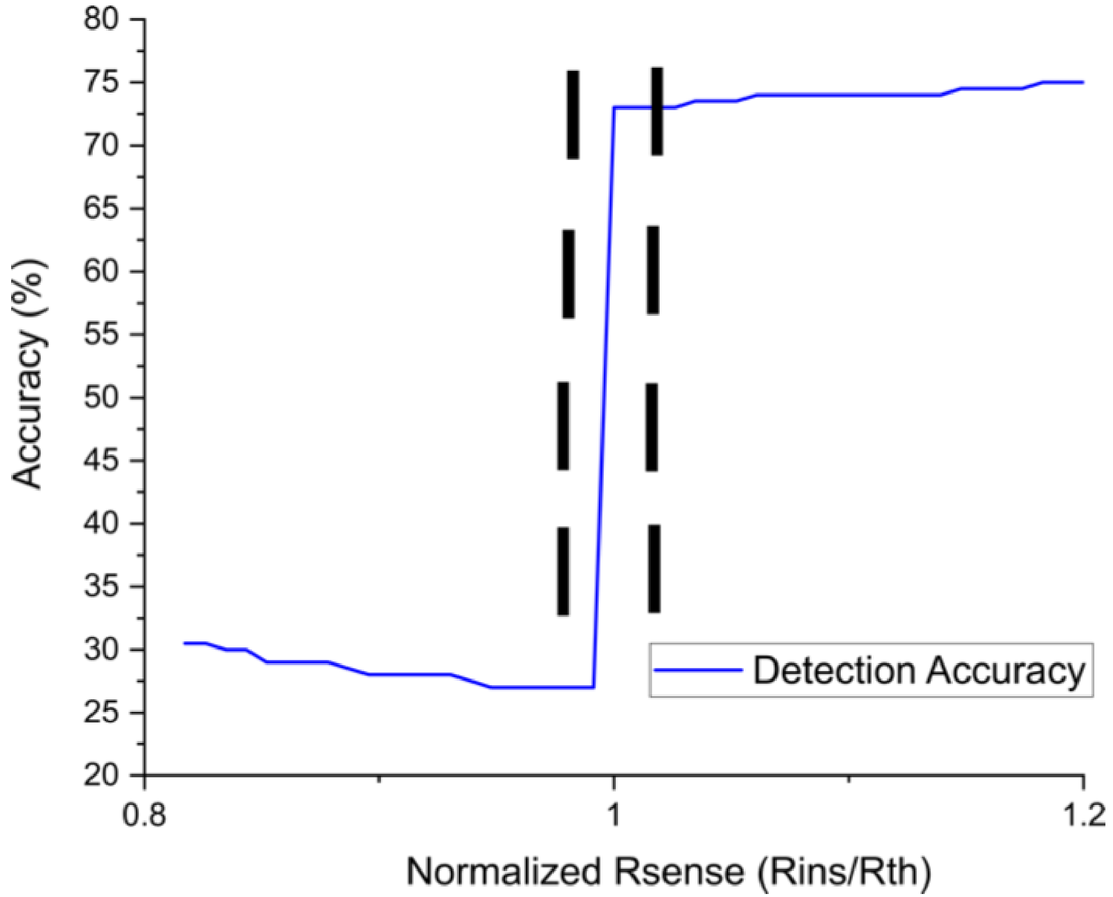


Detection Accuracy

Transient simulation in Cadence:

Sweeping value of sense resistor

Nominal sense resistor =1Ω



Increasing value of sense Resistor

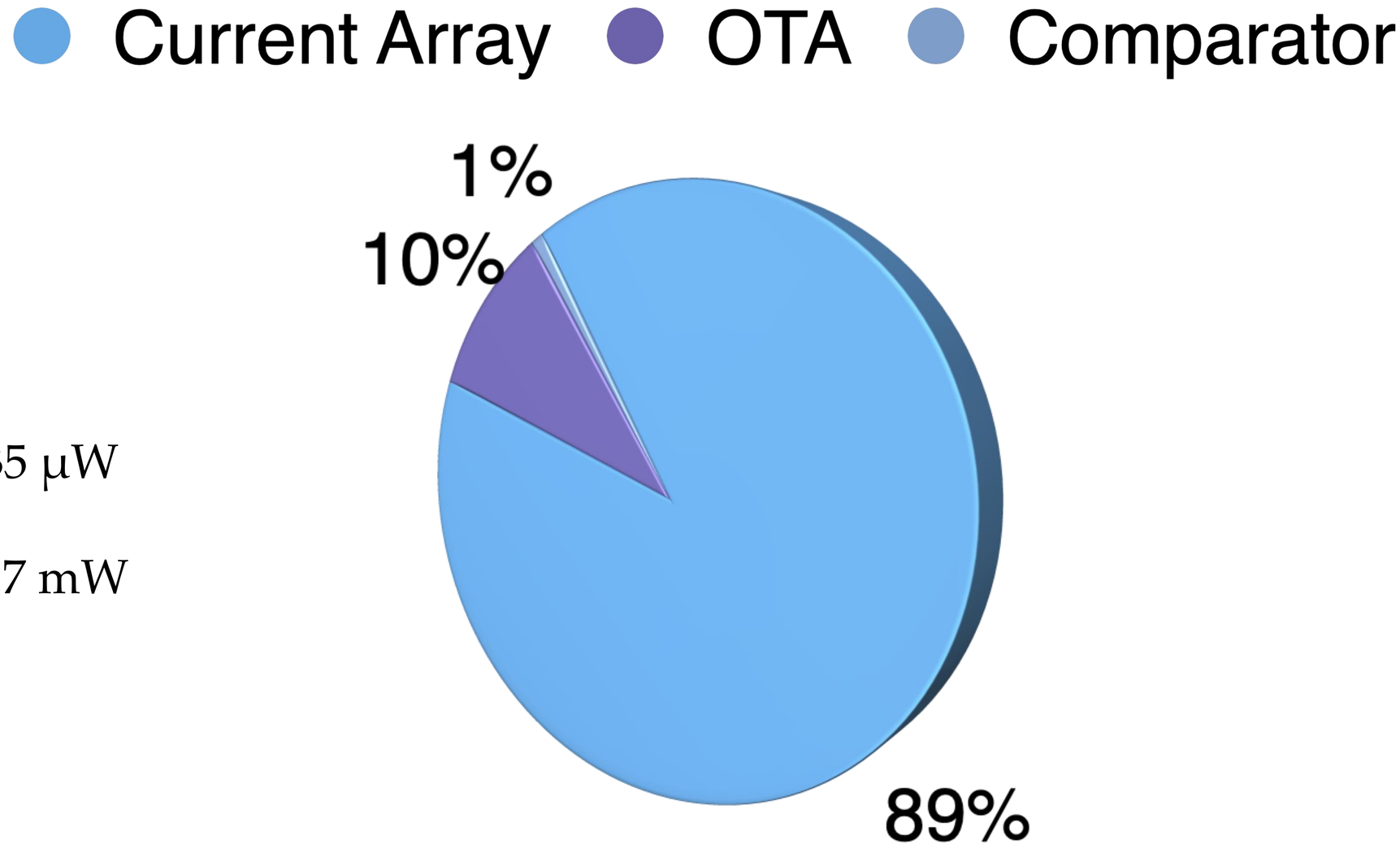
Power Breakdown

Total = 2.97mW

OTA = 285 μW

Comparator = 23.35 μW

Current Array = 2.7 mW



Results

A: Simulink models. Not implemented in circuits

B: Theoretical implementations based on ADC survey [11]

C:Number of sensors required to secure IBMpgIT Processor with reported detection accuracy

TABLE I
COMPARISON TABLE

		TCAD 2018	TCAS-I 2019	This Work
	Method	On-Chip voltage grid		PCB Impedance
Sensor	Circuit	6-bit ADC	8-bit ADC	SC Amplifier
	Area/sensor	NA[A]	3036 μm^2 [B]	350.000 μm^2
	Power/sensor	NA[A]	3.1 mW [B]	2.97mW
	# of sensor/chip	3	50 [C]	1
	Coverage/chip	<100% (proportional to sensor # and radius)		100%
Detector	Circuit	MUX, linear regressor	ML-classifier (Flip-flops, adder)	Comparator
	Area/detector	NA[A]	76 μm^2	1500 μm^2
	Power/detector	NA[A]	34.71 µW @85 MHz	23.35 µW
	# of detector/chip	1	30	1
	ML training	600	2800	None
System	Accuracy	98% (No Noise)	60% (10% noise) or 90% (2% noise)	72.5% (10% noise)
	Detection Time	6.6 µs	364.5 ns	4.1µs
	Process	NA[A]	45 nm	65 nm CMOS

Conclusion

✦ We proposed a switched capacitor side channel attack detection circuit in 65nm CMOS (2.97mW, 4.01μs detection time, 72% accuracy, 350k μm^2

✦ This circuit overcomes limitations in power, area, computation requirement, attack surface coverage

✦ Future work: Study of internal (thermal and flicker noise) and external (temperature and package parasitic) factors for detection accuracy

	TCAS-I	ICCAD	This Work
Threat model	Current sense resistor (R_sns)		
Detection	PDN sensing	ΔV sensing	R_S sensing
Sensor circuit	ADC	Ring OSC	SC THA
Sensor #	Multiple	Multiple	Single
Classification	Data intensive	Simple	Simple
R_{sns} @ BGA	YES	YES	YES
R_{sns} @ PCB	YES	NO	YES

References

1. D. Das, S. Maity, S. B. Nasir, S. Ghosh, A. Raychowdhury, and S. Sen, “ASNI: Attenuated signature noise injection for low-overhead power side-channel attack immunity,” *IEEE Trans. Circuits Syst. I*, vol. 65, no. 10, pp. 3300–3311, 2018
2. A. Singh, M. Kar, S. K. Mathew, A. Rajan, V. De, and S. Mukhopad- hyay, “Improved power/EM side-channel attack resistance of 128-bit AES engines with random fast voltage dithering,” *IEEE J. Solid-State Circuits*, vol. 54, no. 2, pp. 569–583, 2018
3. P.-C. Liu, H.-C. Chang, and C.-Y. Lee, “A true random-based differential power analysis countermeasure circuit for an AES engine,” *IEEE Trans. Circuits Syst II*, vol. 59, no. 2, pp. 103–107, 2012 [Online]. Available: https://dx.doi.org/10.1109/TCSII.2011.2180094
4. N. Miura, D. Fujimoto, D. Tanaka, Y.-i. Hayashi, N. Homma, T. Aoki, and M. Nagata, “A local EM-analysis attack resistant cryptographic engine with fully-digital oscillator-based tamper-access sensor,” in *Symp. VLSI circuits Tech. Dig.* IEEE, 2014 pp. 1–2
5. D. Utyamishev and I. Partin-Vaisband, “Real-time detection of power analysis attacks by machine learning of power supply variations on-chip,” *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 39, no. 1, pp. 45–55, 2020. [Online]. Available: https://dx.doi.org/10.1109/TCAD.2018.2883971
6. F. Kenarangi and I. Partin-Vaisband, “Exploiting machine learning against on-chip power analysis attacks: Tradeoffs and design considerations,” *IEEE Trans. Circuits Syst. I*, vol. 66, no. 2, pp. 769–781, 2019
7. N. Gattu, M. N. Imtiaz Khan, A. De, and S. Ghosh, “Power side channel attack analysis and detection,” in *2020 IEEE/ACM International Conference On Computer Aided Design ICCAD*, 2020, pp. 1–7
8. D. G. Haigh and B. Singh, “A switching scheme for SC filters which reduces the effect of parasitic capacitances associated with switch control terminals,” in Proc. IEEE Int. Symp. Circuits and Systems, 1983, pp. 586–589

References

9. K.-L. Lee and R. G. Meyer, “Low-distortion switched-capacitor filter design techniques,” IEEE J. Solid-State Circuits, vol. 20, no. 6, pp. 1103–1113, Dec. 1985

10. Murmann, B. (2012). "Thermal Noise in Track-and-Hold Circuits: Analysis and Simulation Techniques." IEEE Solid-State Circuits Magazine 4(2): 46-54.

11. Baker, R. J., “CMOS Circuit Design, Layout, and Simulation, Third Edition,” Wiley-IEEE Press, 2010. ISBN 9780470881323

12. B. Murmann, “, ”ADC Performance Survey 1997-2020,” [online]. available: http://web.stanford.edu/murmann/adcsurvey.html.”