Performance and Noise Trade-Off for SC-Based Power Side Channel Attack Detection Circuit

Nipun Kaushik and John Hu

Oklahoma State University

Outline

1. Side channel attacks - Countermeasures to detection
2. Power Side channel attack (P-SCA) and threat model
3. Circuit for noise analysis
4. Relationship of noise and circuit parameters
5. Results and Conclusion
6. 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)

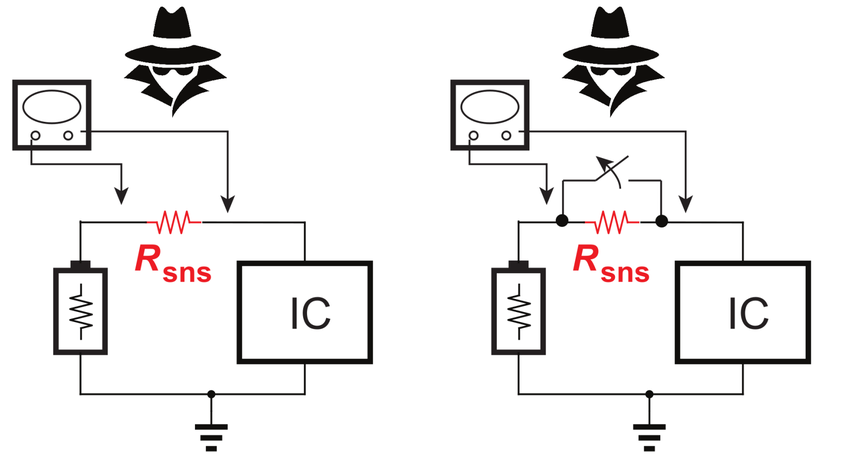
  Focus on detection of an attack in real time - machine learning [5]-[6],

  Ring oscillator based circuit [7]

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**

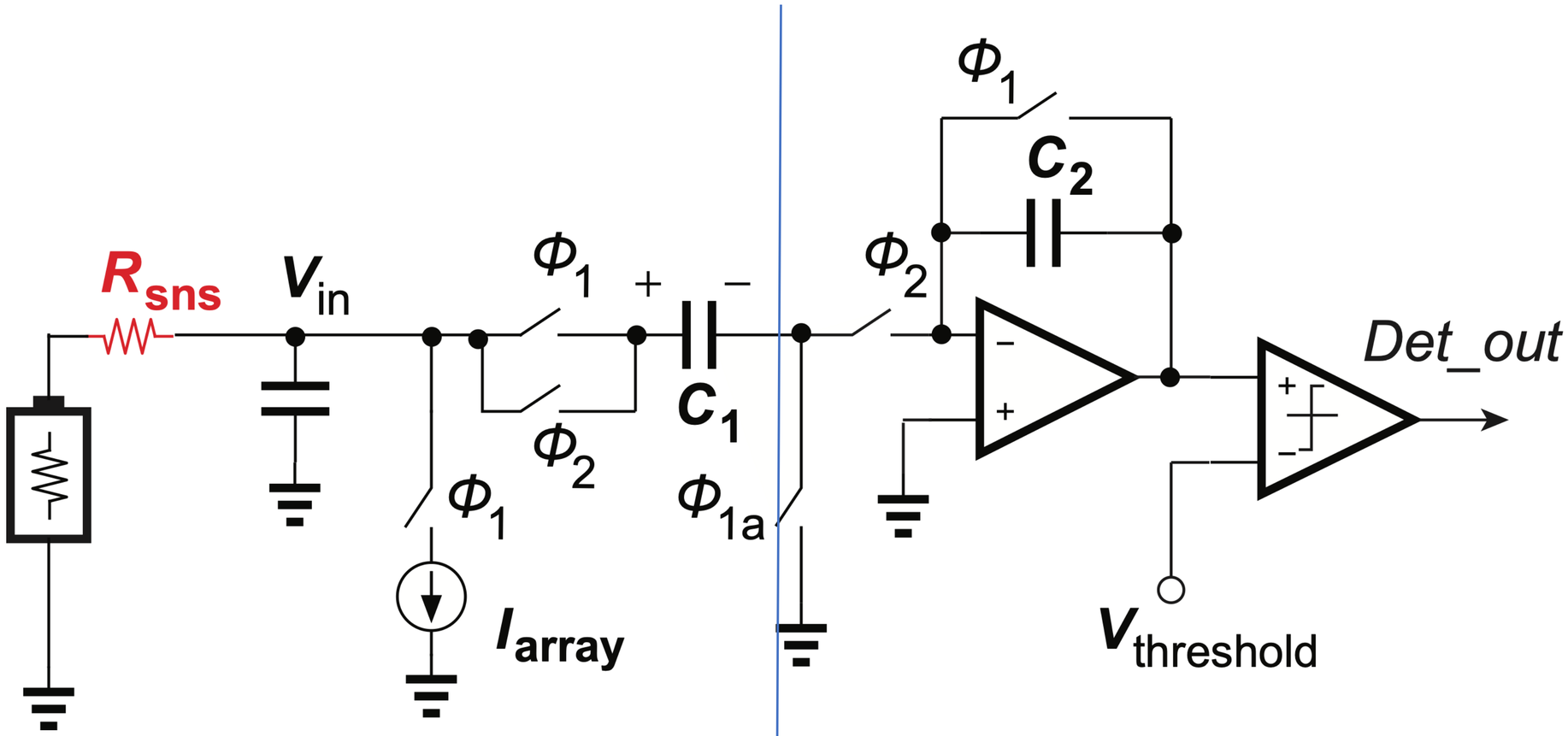
Contribution of this work

1.First mathematical noise analysis of SC based noise analysis P-SCA detection technique.

2.Provides a direct relationship between circuit parameters and minimum detectable resistance

3.Introduces a new power and area efficient SC detection circuit from the derived expression

SC circuit for noise analysis



Metrics for the topology

Sampling rate = 200KHz

Charge redistribution and conversion

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

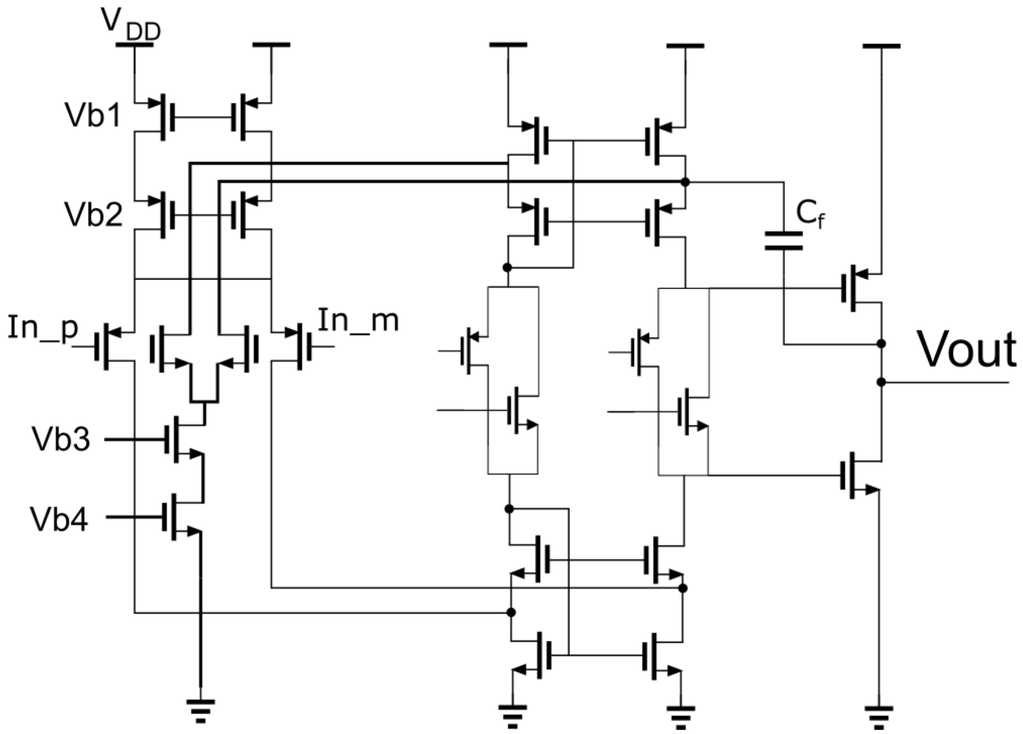
Output is a just a scaled and delayed version of input

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

Sampling frequency can be usually defined by

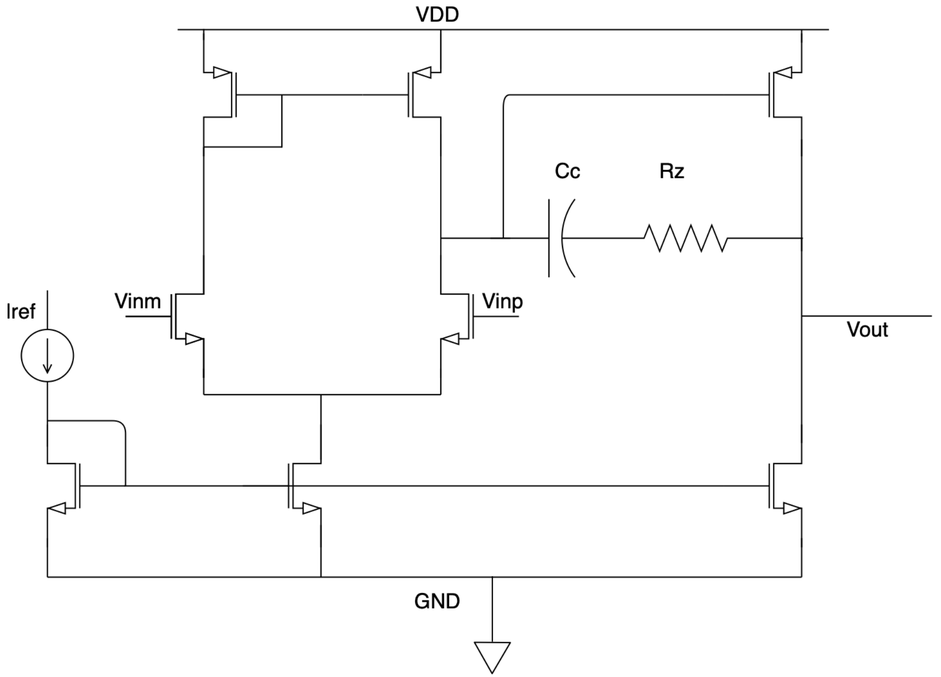
- Input time constant
- Bandwidth of the OTA (minimize settling error)

Amplifier in SC Circuit



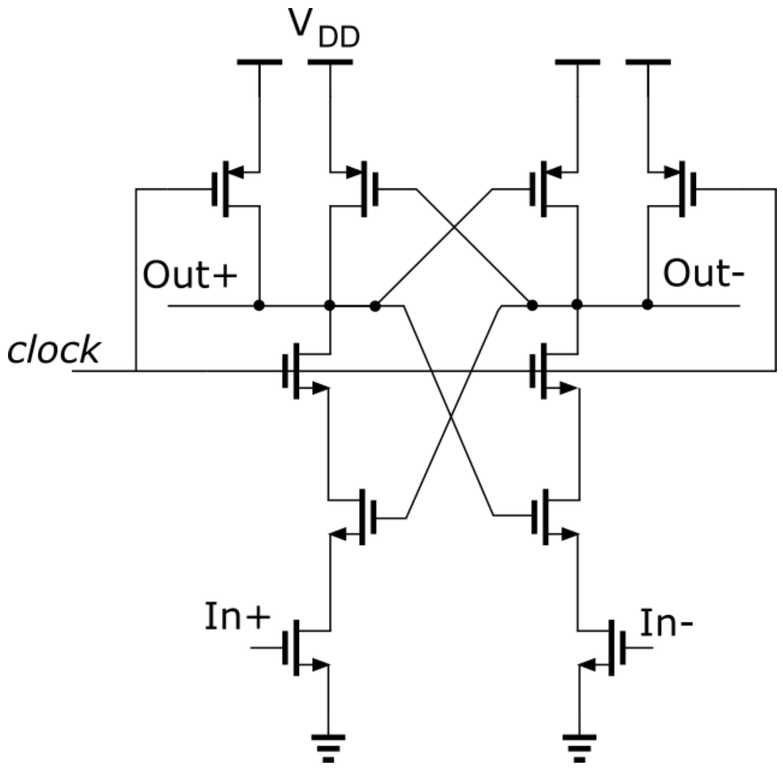
Rail-to-rail folded cascode with class AB

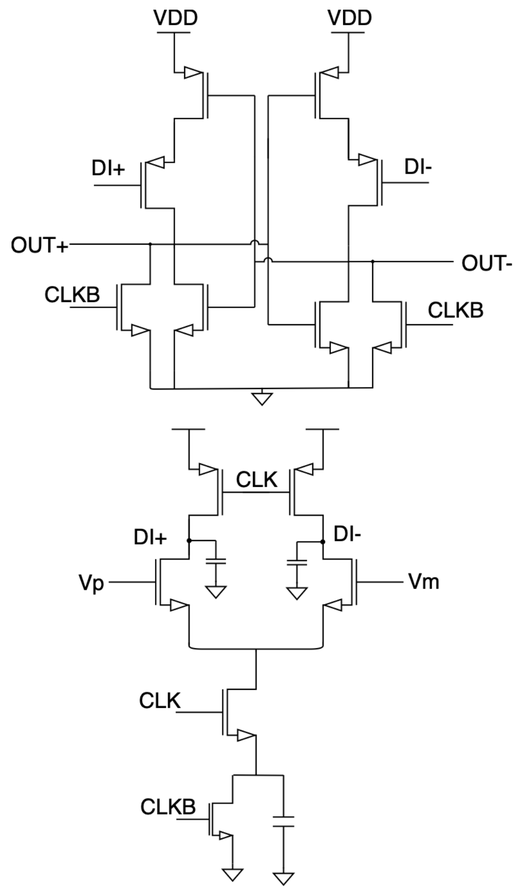
Baker, J. [10]



NMOS input two stage OTA

Comparator





Strong arm clocked comparator

Baker, J. [10]

Dynamic biased clocked comparator

Bindra, H. [11]

Relationship of noise with circuit

According to normal Z distribution table;

The equation represents the following parameters:

μ_0 = Threshold without sense resistor R_{sns}

μ_1 = Threshold with sense resistor R_{sns}

R_{sns} = Sense resistor

σ = Total noise distribution

G = Gain of the track and hold circuit

I_{array} = Excitation current used in the system

$$\overline{\sigma^2} = \overline{\sigma_{THA}^2} + \overline{\sigma_{comp}^2} \quad (1)$$

$$\mu_0 = G \cdot \Delta V = G \cdot I_{array} R_S \quad (2)$$

$$\mu_1 = G \cdot \Delta V' = G \cdot I_{array}(R_S + R_{sns}) \quad (3)$$

$$\mu_0 - \mu_1 \geq 2 \times 1.645\sigma = 3.29\sigma \quad (4)$$

$$R_{sns} \geq \frac{3.29\sigma}{G.I_{array}} \quad (5)$$

Relationship of noise with circuit

To further include the effects of noise from comparator and SC circuit the expression can be written as

Equation 7 provides deep insight into circuit design

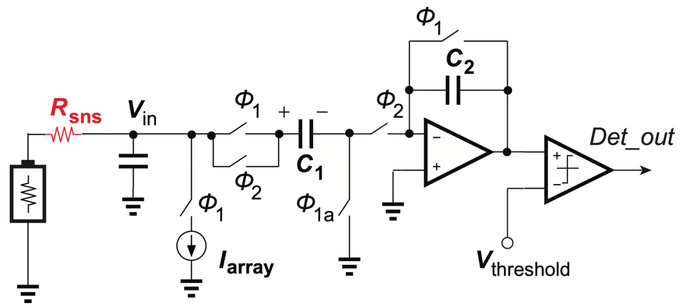
$$\sigma = \sqrt{G^2\sigma_{THA,in}^2 + \sigma_{comp}^2} \quad (6)$$

Substituting the following circuit parameters for minimal detectable sense resistor

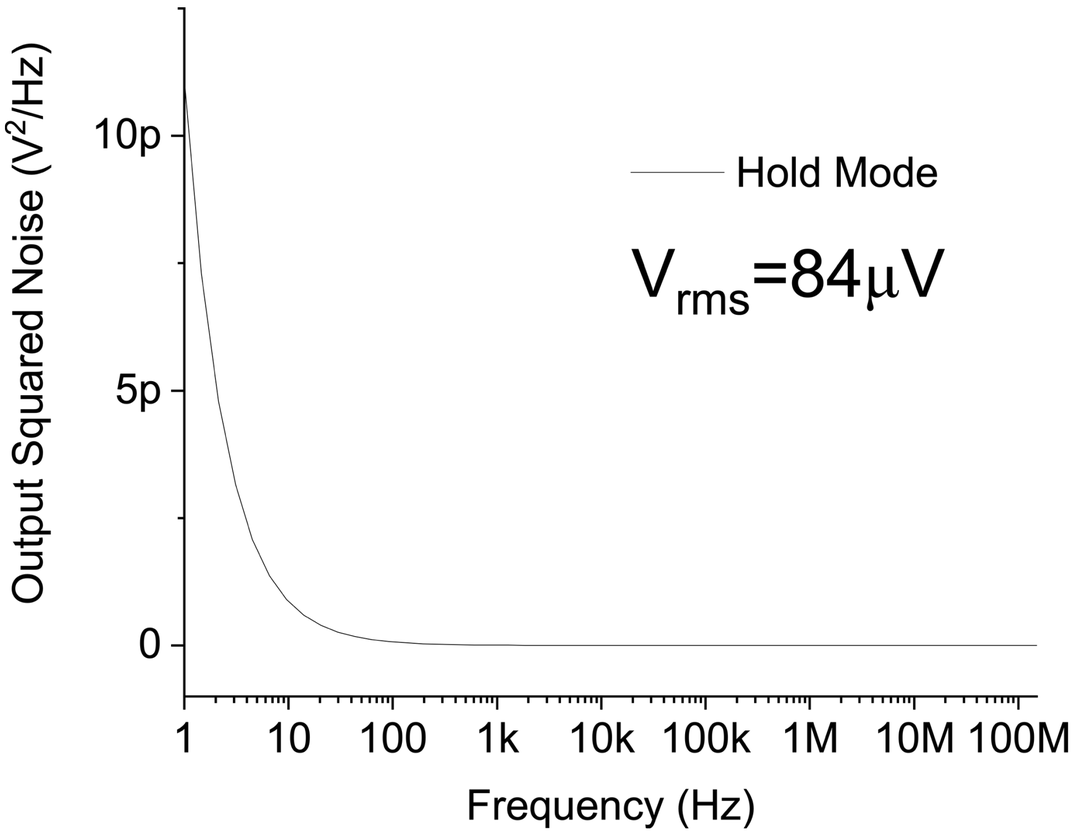
- $f(\alpha, \beta)$ for 95% confidence level = 3.29
- I_{array} = 100 μA
- Total noise distribution from SC circuit and comparator σ = 1.07mV
- Gain of the track and hold circuit G = 30

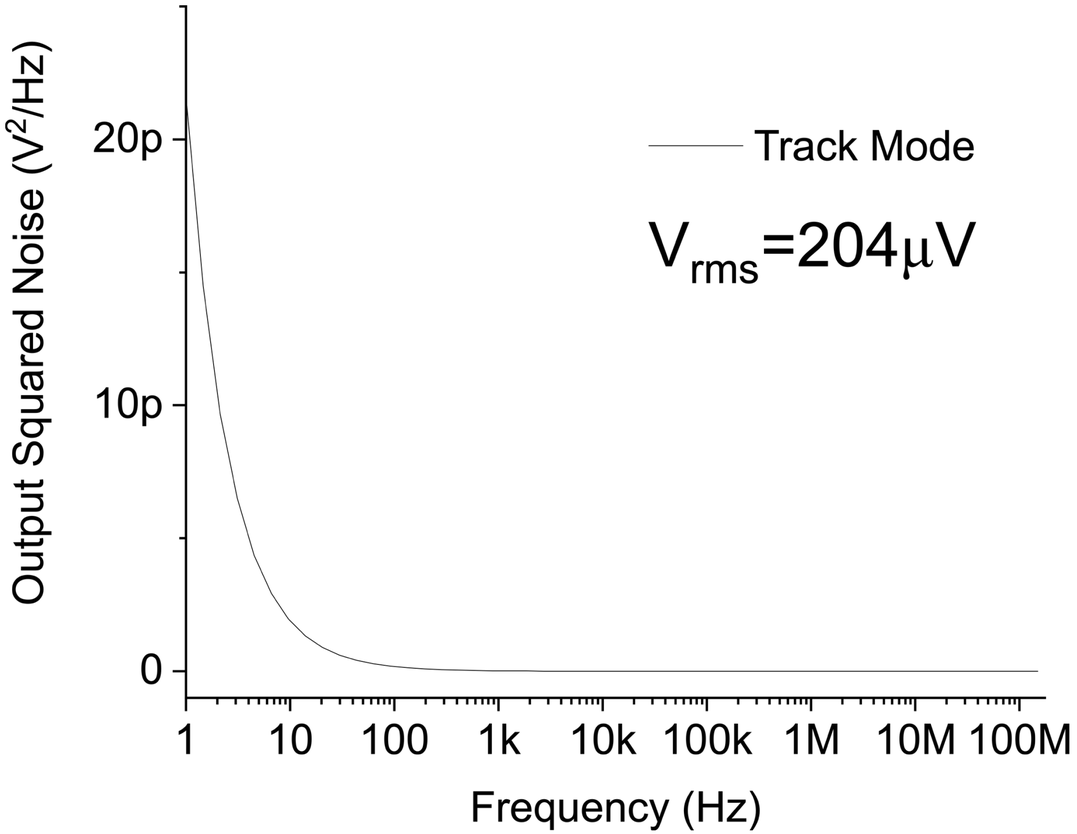
$$R_{SNS,min} = \frac{f(\alpha,\beta)}{I_{array}}\sqrt{\sigma_{THA,in}^2 + \frac{\sigma_{comp}^2}{G^2}} \quad (7)$$

We get $R_{sns} \geq \frac{3.29\times 33\mu V}{100\mu} A = 1.08\Omega$ (8)

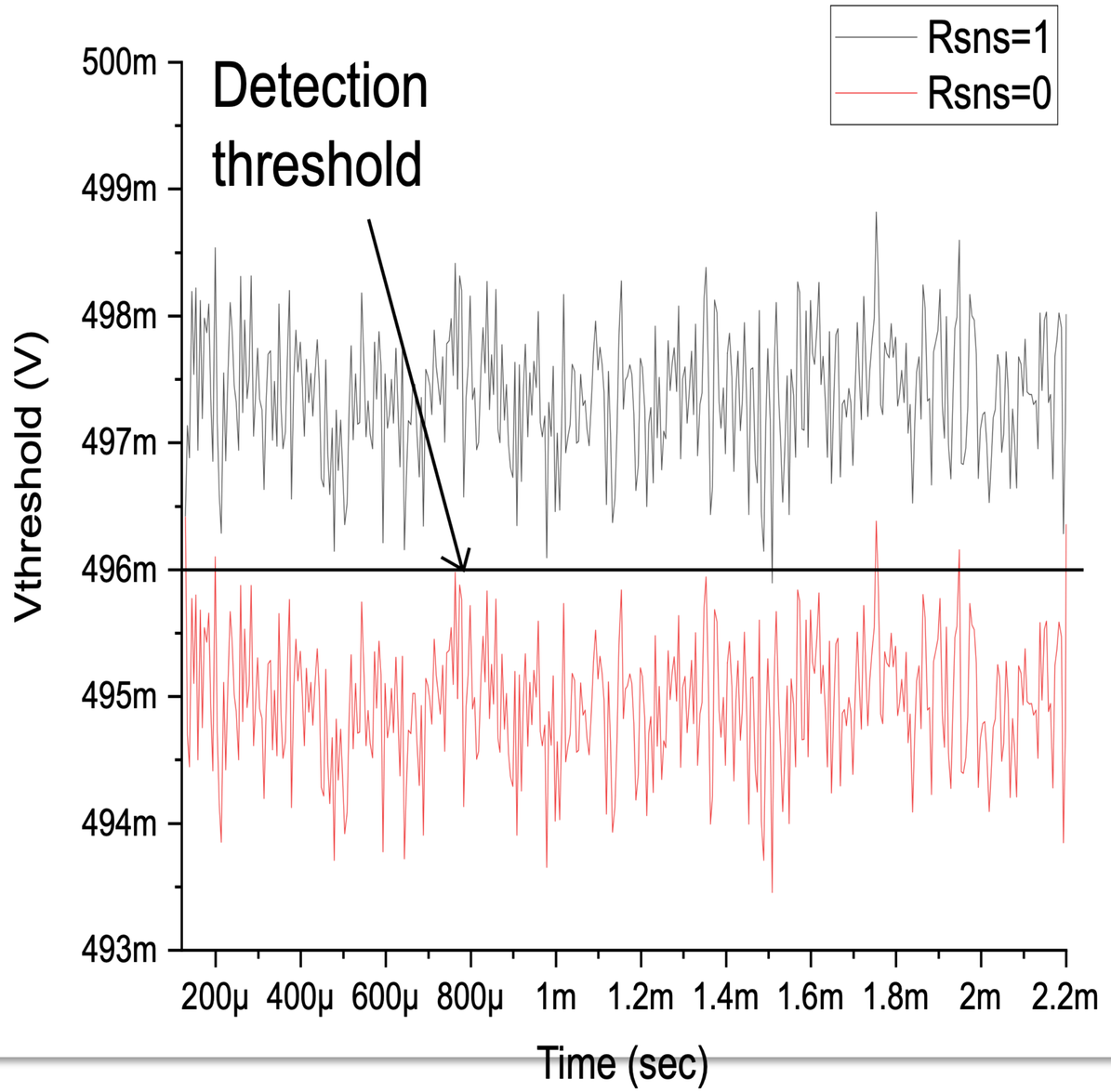


Simulations

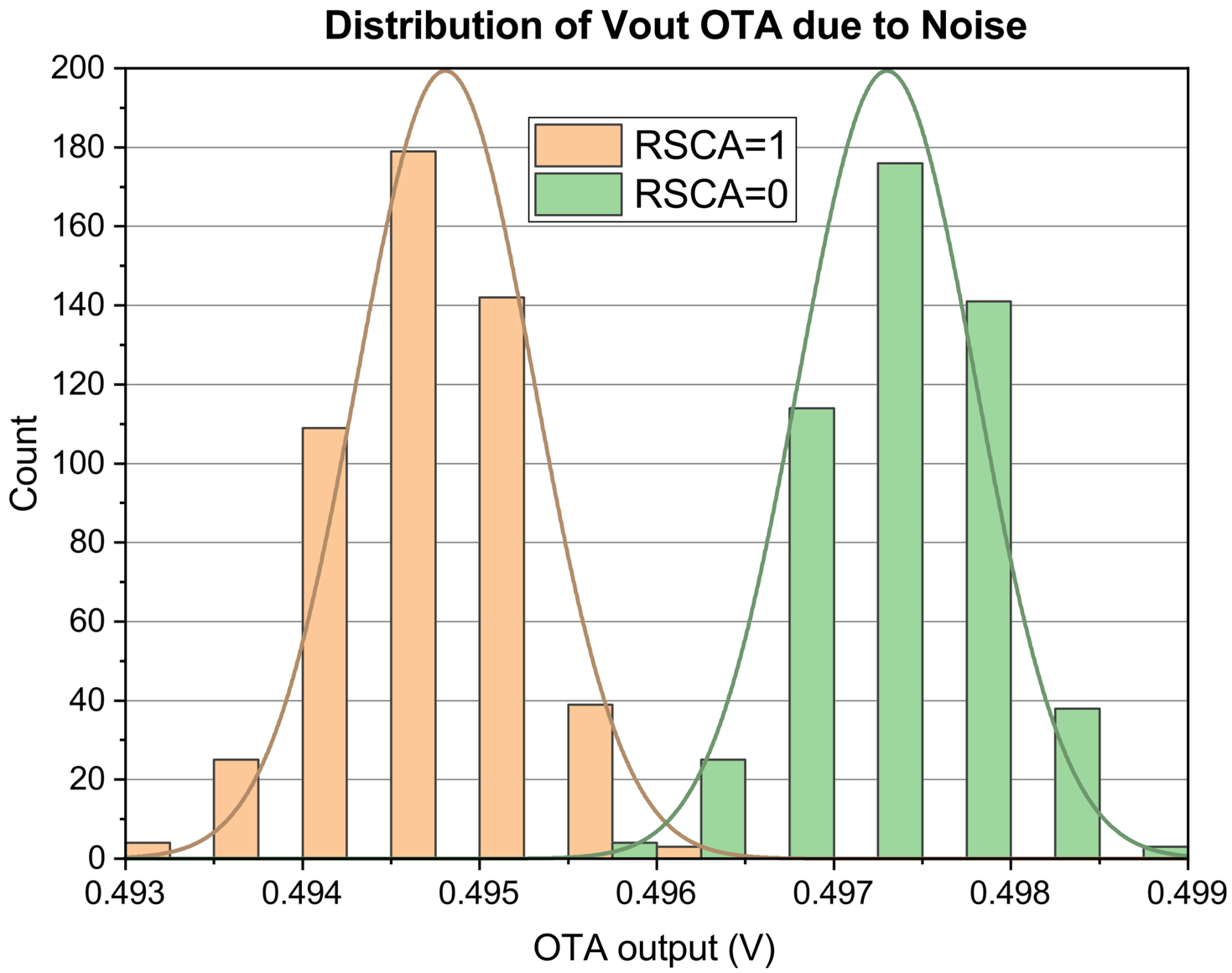




Simulations



Simulations



Resulting circuit and comparison

Measure	Value
Accuracy	0.9338
Precision	0.9363
Sensitivity	0.9310
F-1 Score	0.9336
MCC	0.8677

Table 1
Detection performance
when R_{sns} = 1

Publication	[12]	[15]	[13]	[14]	This work
Journal/Conference	TCAD	TCAS-I	ICCAD	ISCAS	MWSCAS
Year	2018	2019	2020	2021	2021
Detection Method	On-chip voltage variations	PDN voltage variation	ΔPhase and ΔN_{rising}	Total Supply Impedance	
Detection Algorithm	Linear, fixed threshold	Logistic regression	-	Binary classification with a set threshold	
Detection Circuit	6-bit ADC, ROM registers	8-bit ADC	RO Based	rail-to-rail input folded cascode Clocked comparator I_{array} = 10 mA	NMOS input two stage OTA Dynamic bias comparator I_{array} = 100 µA
Detection @PCB	YES	YES	NO	YES	YES
Detection Time	6.6 µs	-	2 µs	4.01 µs	(4.08 - 6.58) µs
Power Consumed	94 mW	-	0.1001 mW	2.97 mW	0.130 mW
Area (kGE)	44,444	749.62	1.9286	280	110
Technology (nm)	45	45	22	65	65

Table 2
Comparison with other work
23x improvement in power consumption with> 2x improvement in area

Conclusion

1.First mathematical noise analysis of SC based P-SCA detection technique.

2.The equation is used to optimize and present a new SC detection circuit.

$$R_{SNS,min} = \frac{f(\alpha,\beta)}{I_{array}} \sqrt{\sigma_{THA,in}^2 + \frac{\sigma_{comp}^2}{G^2}}$$

3.Introduces a new power and area efficient SC detection circuit from the derived expression

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

References

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

11. H. S. Bindra, C. E. Lokin, D. Schinkel, A. Annema and B. Nauta, "A 1.2-V Dynamic Bias Latch-Type Comparator in 65-nm CMOS With 0.4-mV Input Noise," in IEEE Journal of Solid-State Circuits, vol. 53, no. 7, pp. 1902-1912, July 2018, doi: 10.1109/JSSC.2018.2820147.

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