SC DETECTION CIRCUIT

NIPUN KAUSHIK

OUTLINE

1. Side Channel Attacks (SCA) – Countermeasures to detection
2. Power Side Channel Attack (PSCA) and threat model
3. System and Circuit design
    1. First Tapeout (July 2021)
    2. Second Tapeout (July 2022)
    3. Simulation Results
4. Results

SIDE CHANNEL ATTACKS

- Threat to devices handling sensitive information (Smart cards, servers, AES, DES, 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 [7]
- Detection circuit can be improve by decreasing the number of required sensors, sensing the resistor insertion at PCB level.

POWER SIDE CHANNEL ATTACKS (PSCA) 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 large number of traces during encryption process
4. Use statistical methods to extract the secret key.
5. Statistical operation include Differential Power Analysis (DPA), Correlational Power Analysis (CPA) etc.

THREAT MODEL

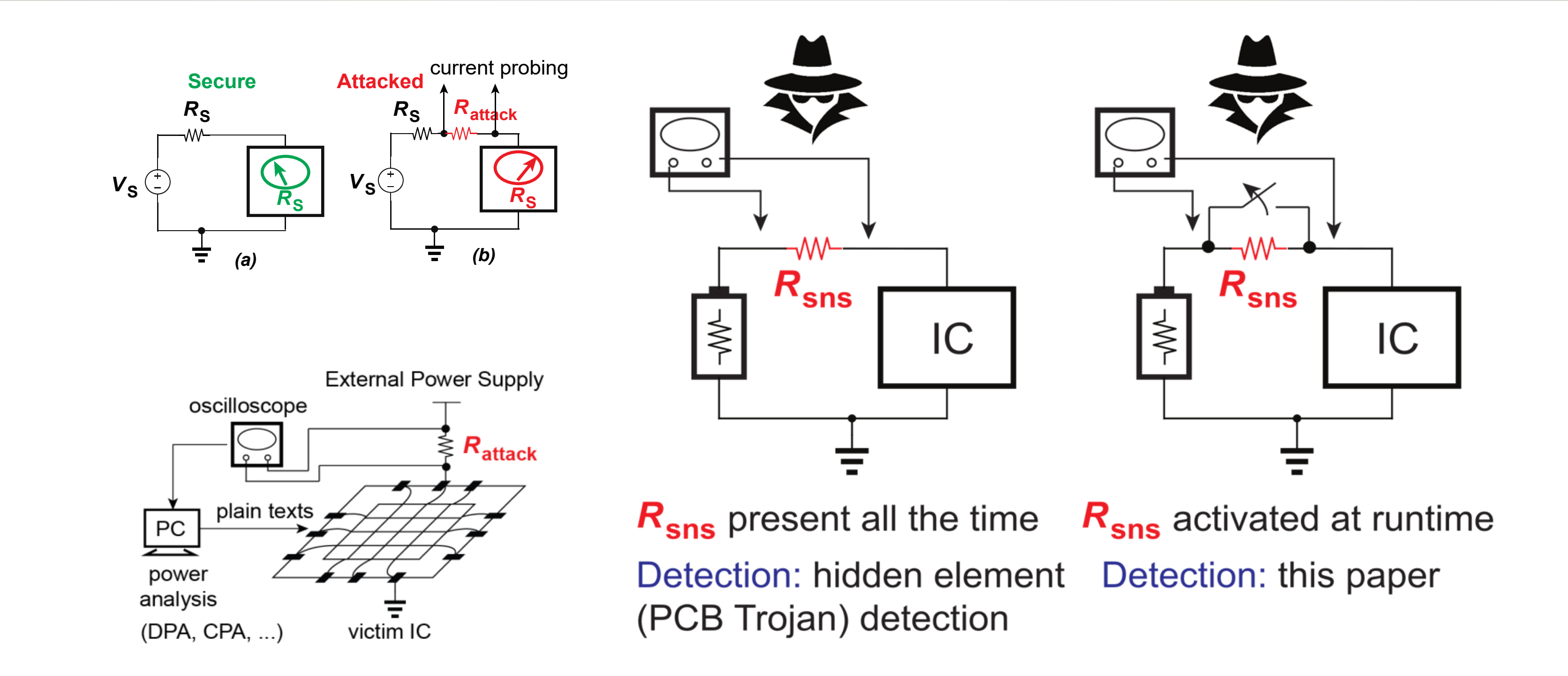
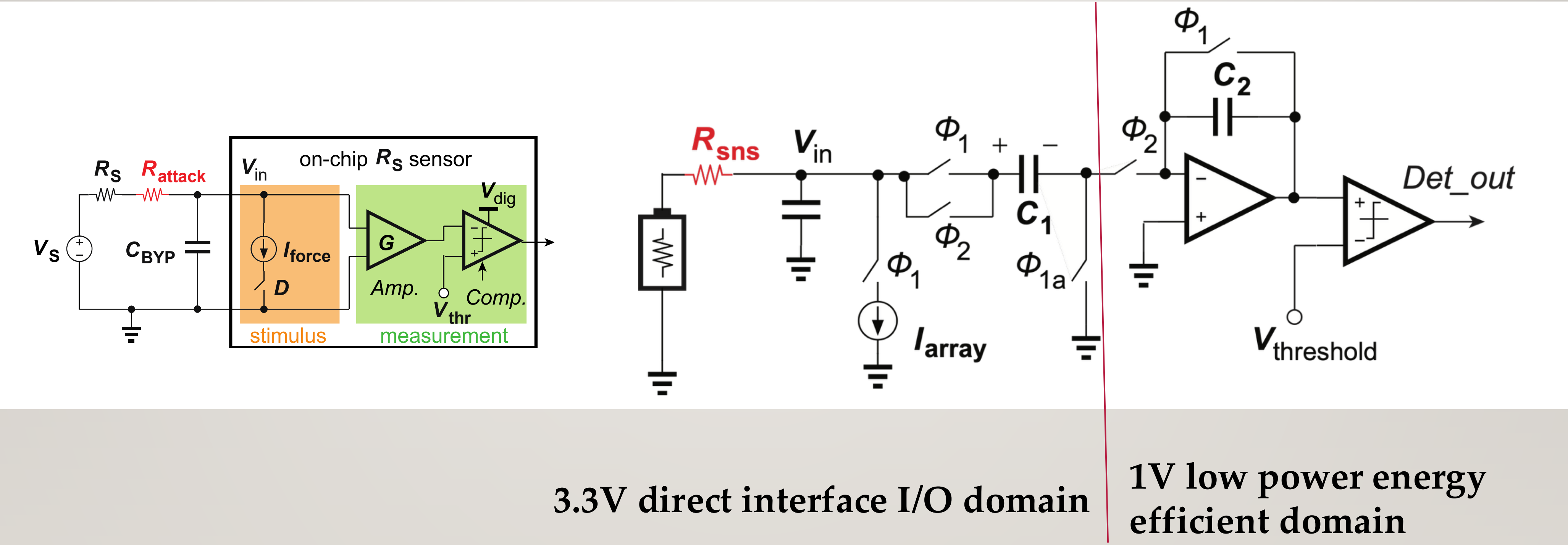


Fig 1:Threat model

SYSTEM LEVEL DESIGN & CIRCUIT TOPOLOGY

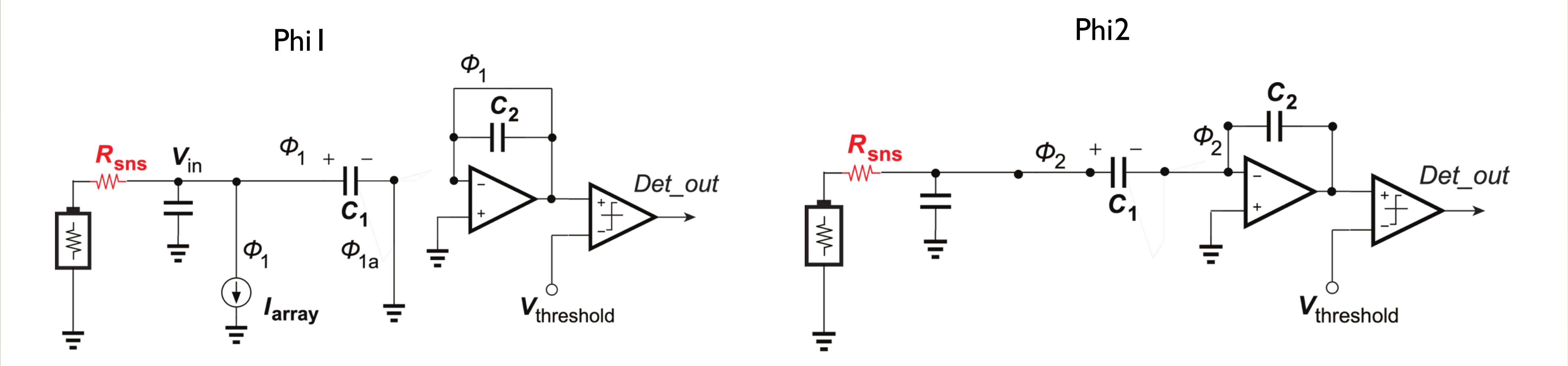


3.3V direct interface I/O domain

1V low power energy efficient domain

Fig 2: System and Circuit topology

PHI1 AND PHI2 FOR SC CIRCUIT



$$Q_x = -(I_{array}.R_{sense})(n).C_1$$

$$Q_x = -V_{out}(n + 1/2).C_2$$

Fig 3: Circuit operation in different phases

METRICS

Sampling rate = 200KHz

Charge redistribution and conversion

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

Output is a scaled and delayed version of input

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

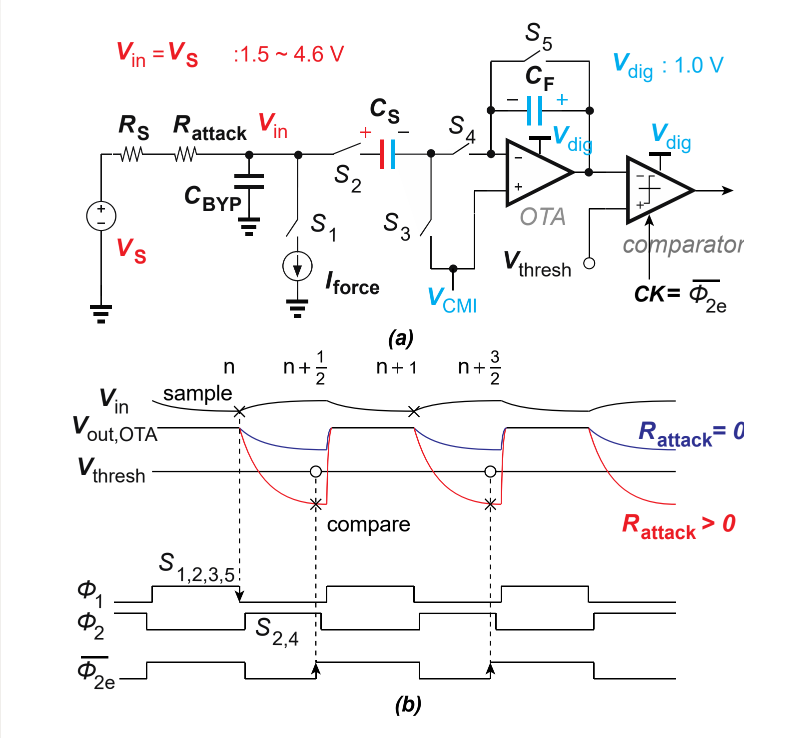
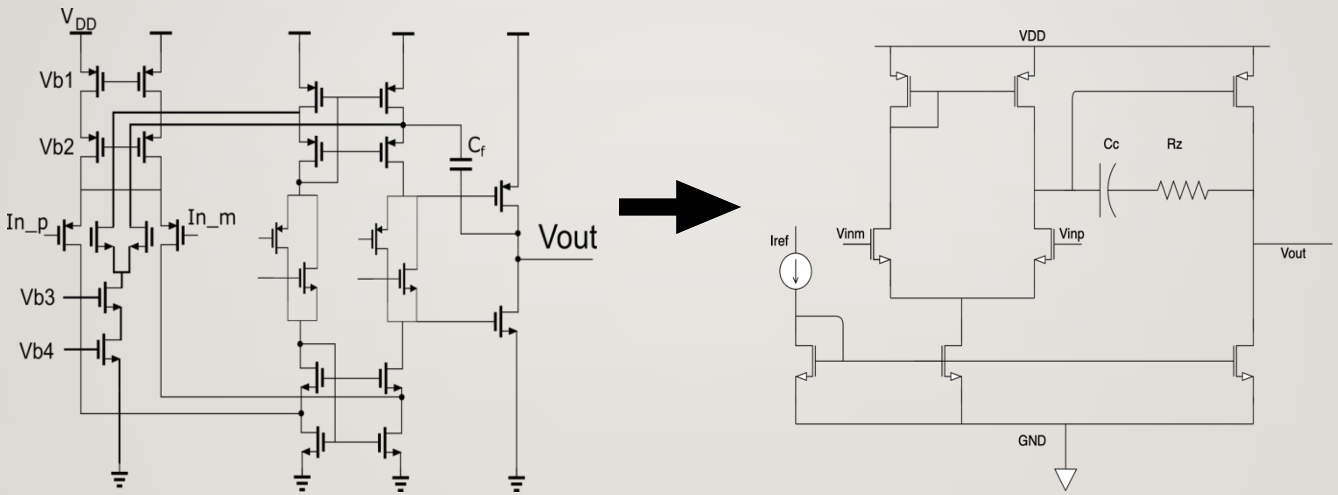


Fig 4: Sensing operation a) Circuit configuration b) Timing waveform

AMPLIFIER



a) b)

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

Trade speed with power efficiency, keep gain similar

Bandwidth = 16MHz with PM 89°

Figure 5: Operational amplifier used in SC amplifier a) Folded Cascode b) Two-stage OTA

COMPARATOR

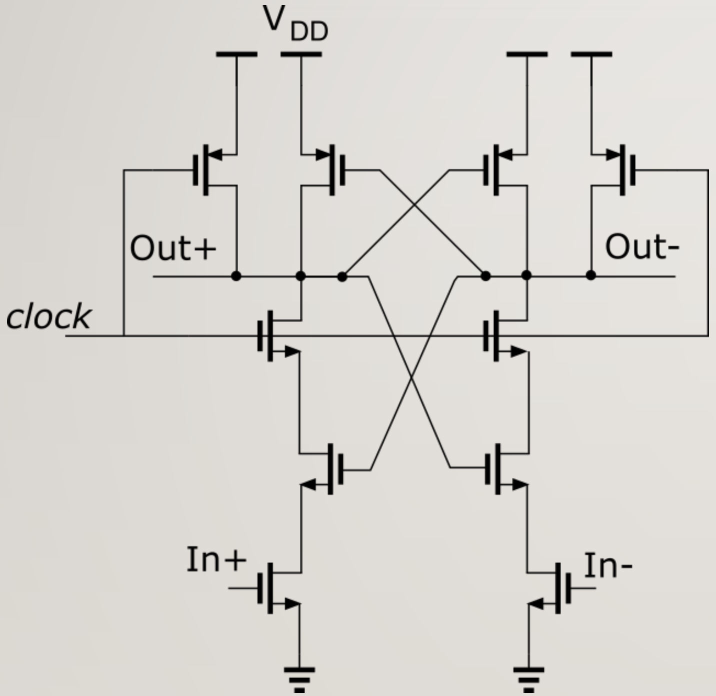


Fig 6: Strong arm clocked comparator, Baker. J [8]

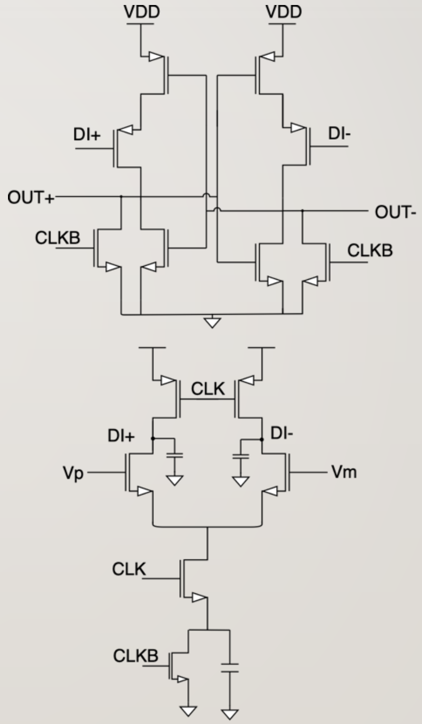


Fig 7: Dynamic Bias comparator, Bindra H. [9]

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

$$\overline{\sigma^2} = \overline{\sigma_{THA}^2} + \overline{\sigma_{comp}^2}$$

$$\mu_0 = G \cdot \Delta V = G \cdot I_{array} R_S$$

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

$$\mu_0 - \mu_1 \geq 2 \times 1.645\sigma = 3.29\sigma$$

$$R_{sns} \geq \frac{3.29\sigma}{G. I_{array}}$$

NOISE ANALYSIS

- $f(\alpha, \beta)$ 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

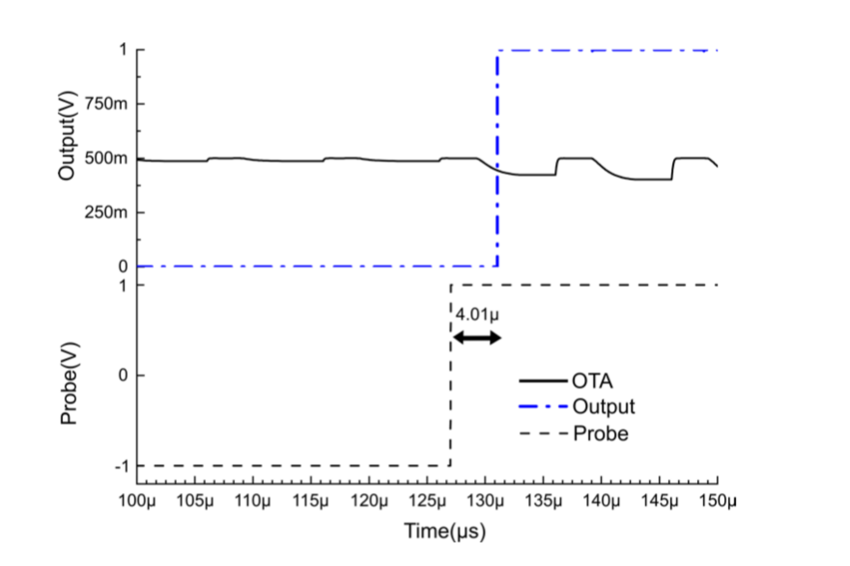
$$\sigma = \sqrt{G^2\sigma_{THA,in}^2 + \sigma_{comp}^2}$$

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

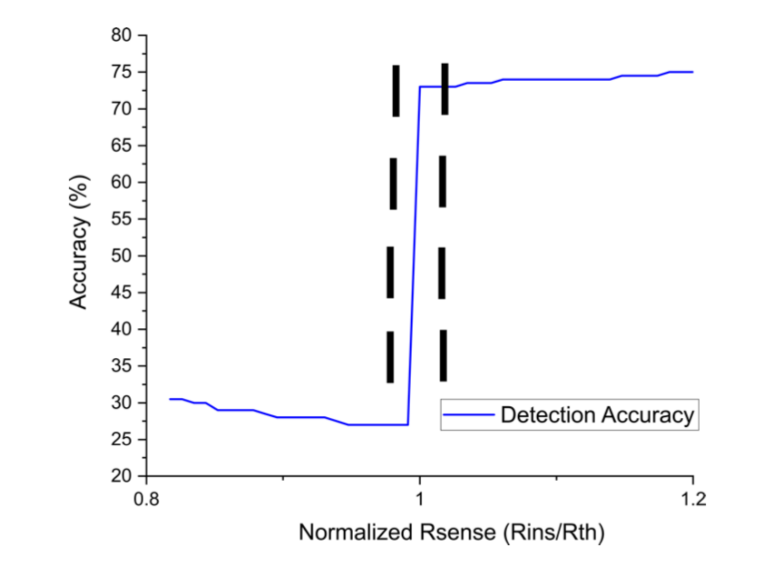
We get $R_{sns} \geq \frac{3.29\times 33\mu V}{100\mu}A = 1.08\Omega$

RESULTS

TYPICAL CORNER SIMULATION – 1ST ITERATION



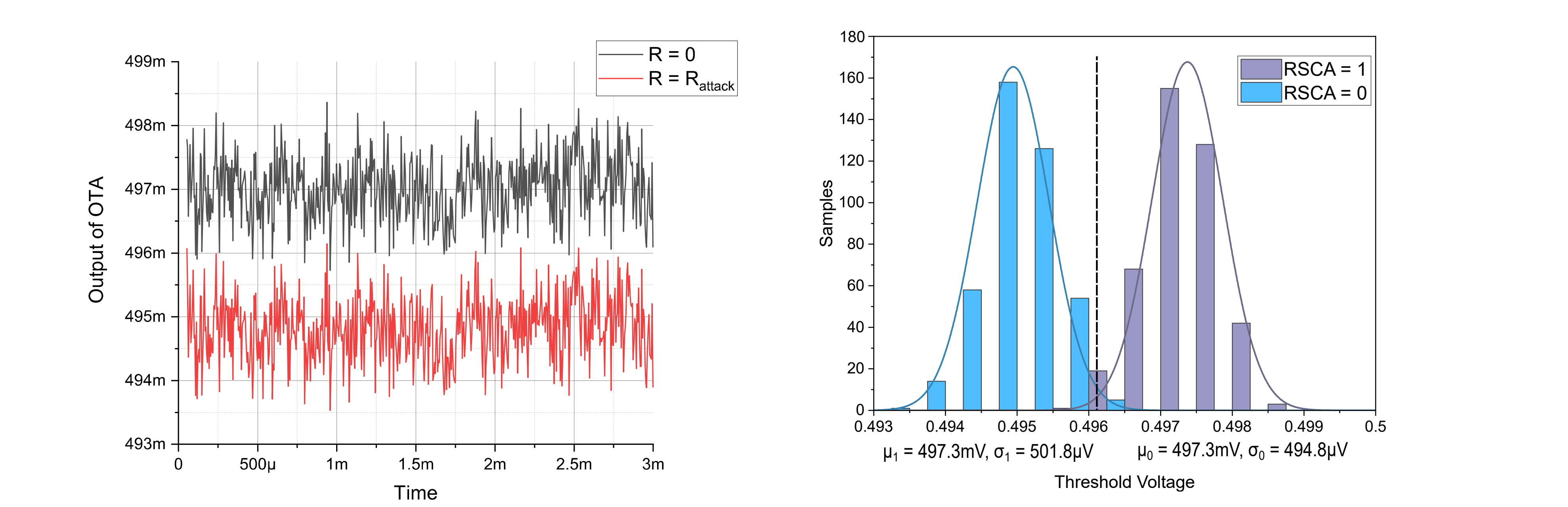
a)



b)

Fig 8: a) Detection time and b) Detection accuracy

AFTER NOISE ANALYSIS– 2ND ITERATION

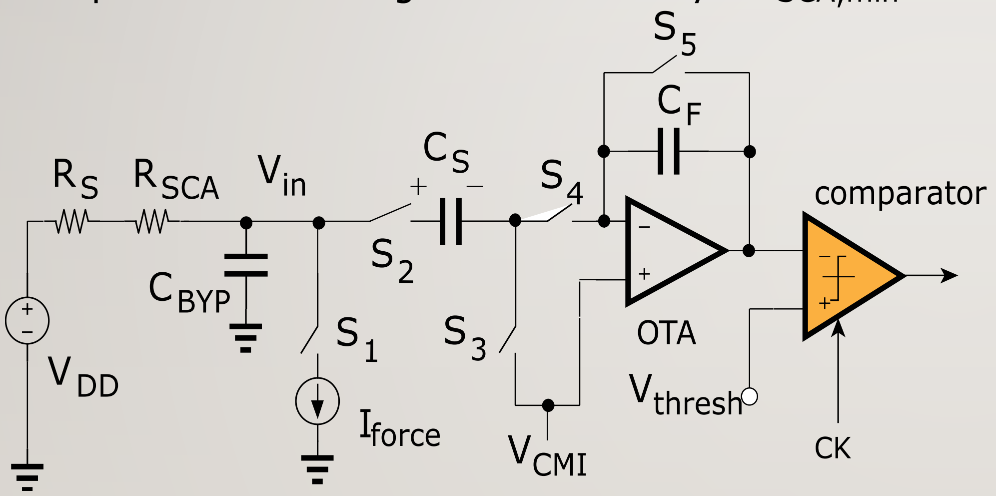


a) b)

Fig 9: a) Transient Noise at the output of OTA and b) Noise distribution at the output of OTA

COMPARATOR NOISE

Comparator Noise degrades sensitivity



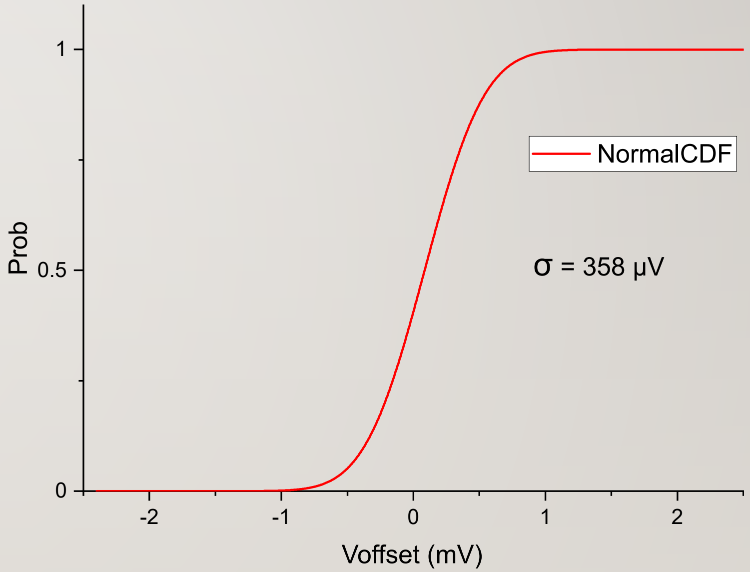
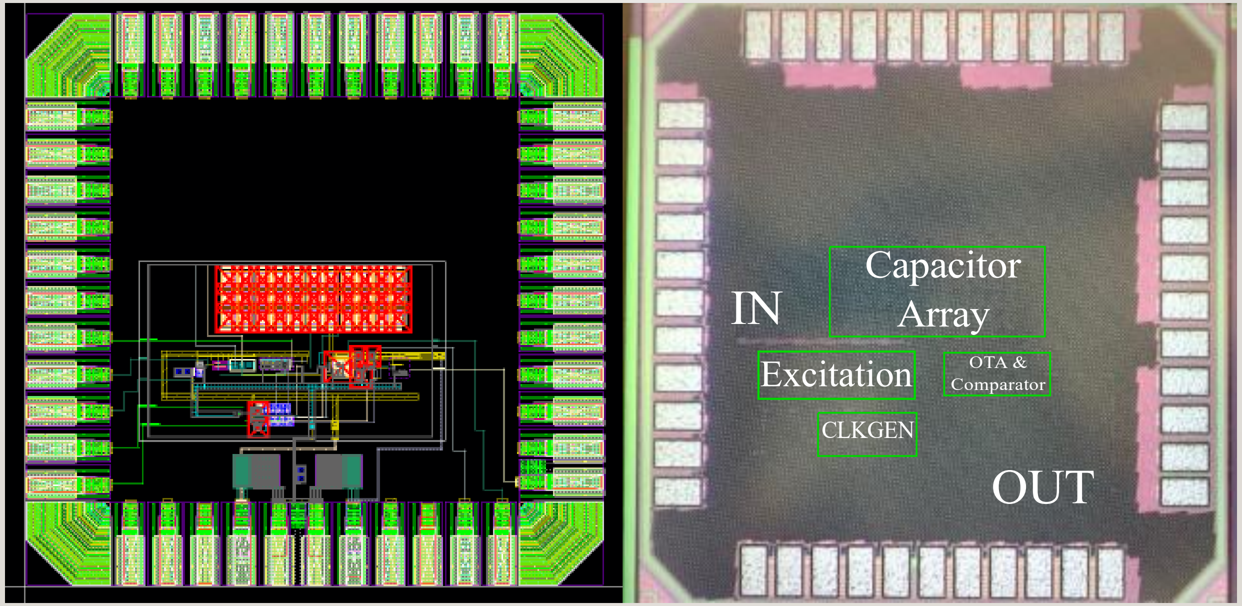


Fig 10: Comparator Noise performance

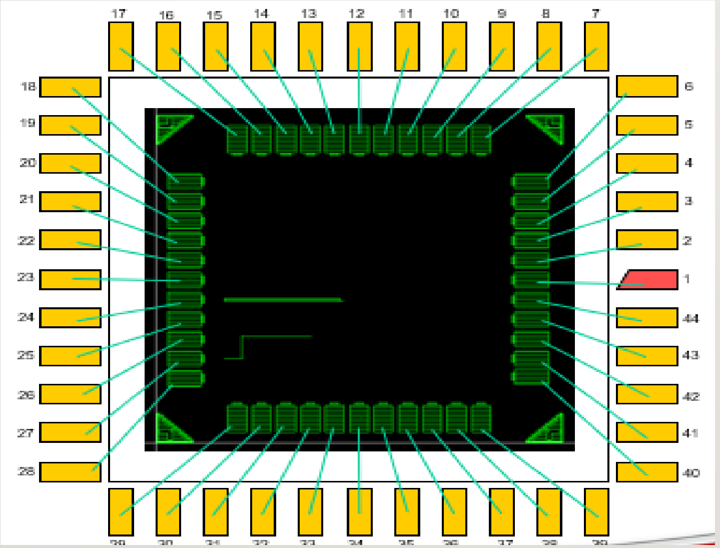
TAPEOUT 1



a b

Fig 11: a) Chip layout in the simulator b) Die photo

BONDING DIAGRAM



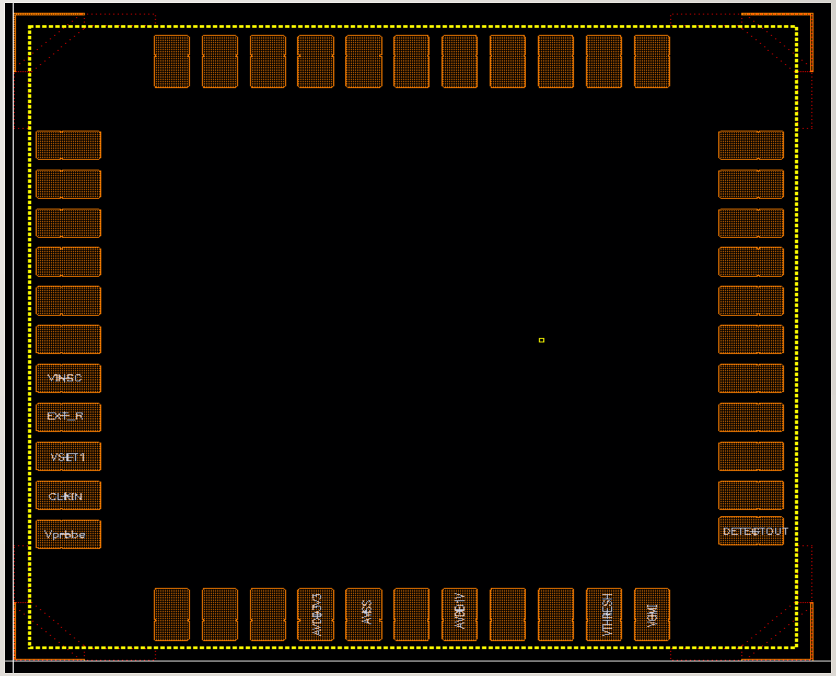
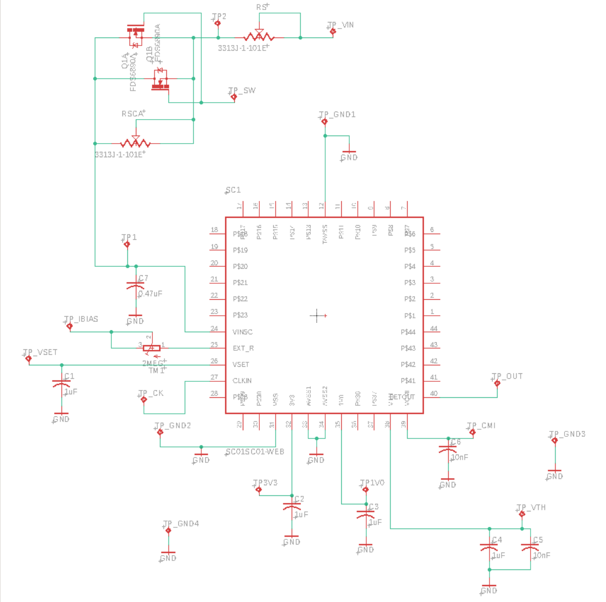
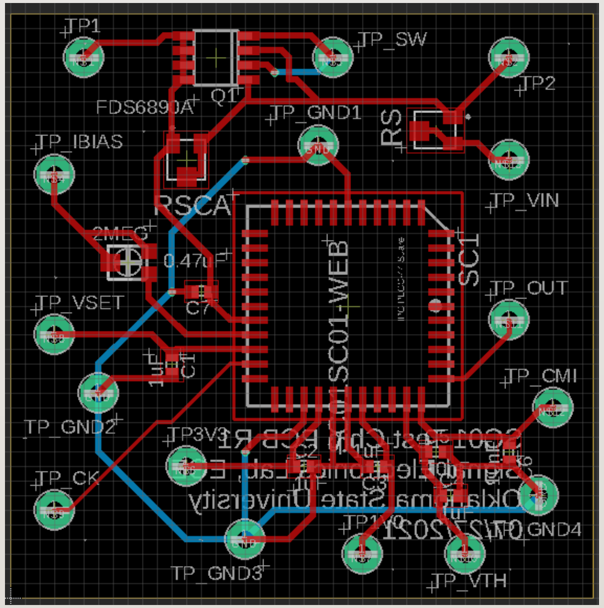


Fig 12: 40 pin CLCC package for the first iteration

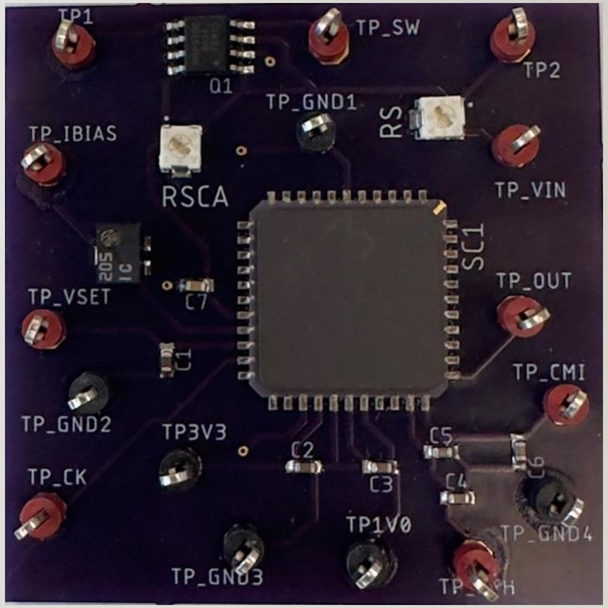
PCB DESIGN



a)



b)



c)

Fig 13: PCB design for test chip in EAGLE a) Schematic b) Board layout c) Fabricated board

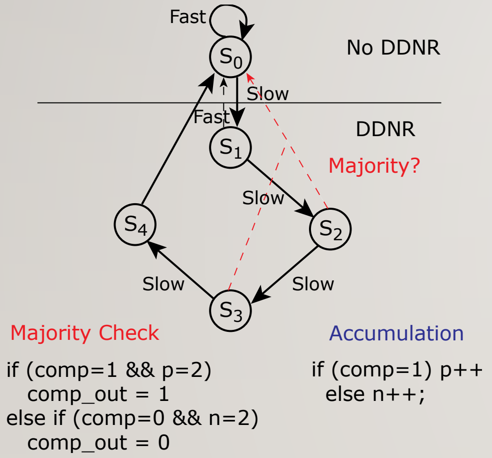
RESULT

- PCB designed, signal at the input, and the tunable current array works.
- An additional latch at the end of the comparator output caused the problem at the output.
- Noise is a problem; can we use data-driven noise reduction to further improve performance?

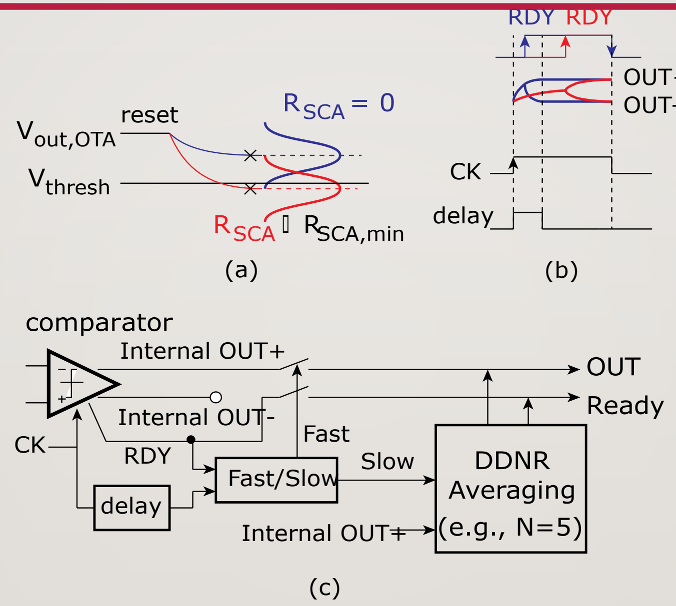
LEARNINGS FROM FAILURE - 1

- Create test modes to test various points in the chip – Created test modes for second tapeout
- Removed the latch at the end to resolve the ESD problem.
- Investigate DDNR for the second tapeout, add a digital block to take more than one sample, and improve the confidence level. This can reduce false positive detection.

DATA DRIVEN NOISE REDUCTION

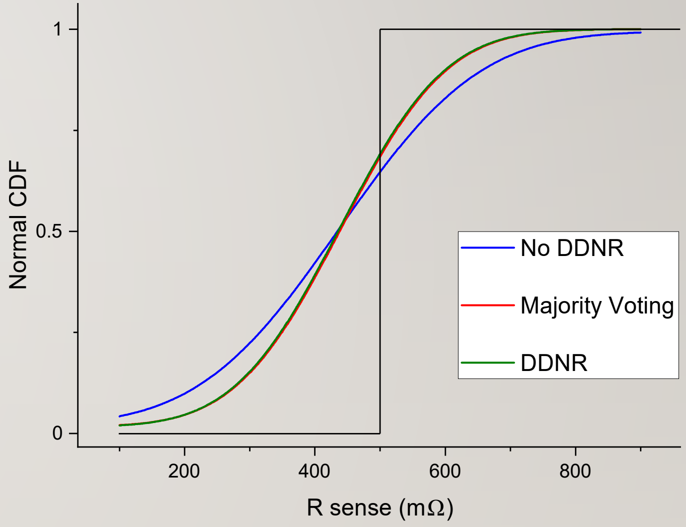


a)



Date-driven Noise Reduction (DDNR)

b)



c)

Fig 14: Finite state machine for DDNR b) System level update c) Comparison with majority voting scheme

DDNR SIMULATION RESULT

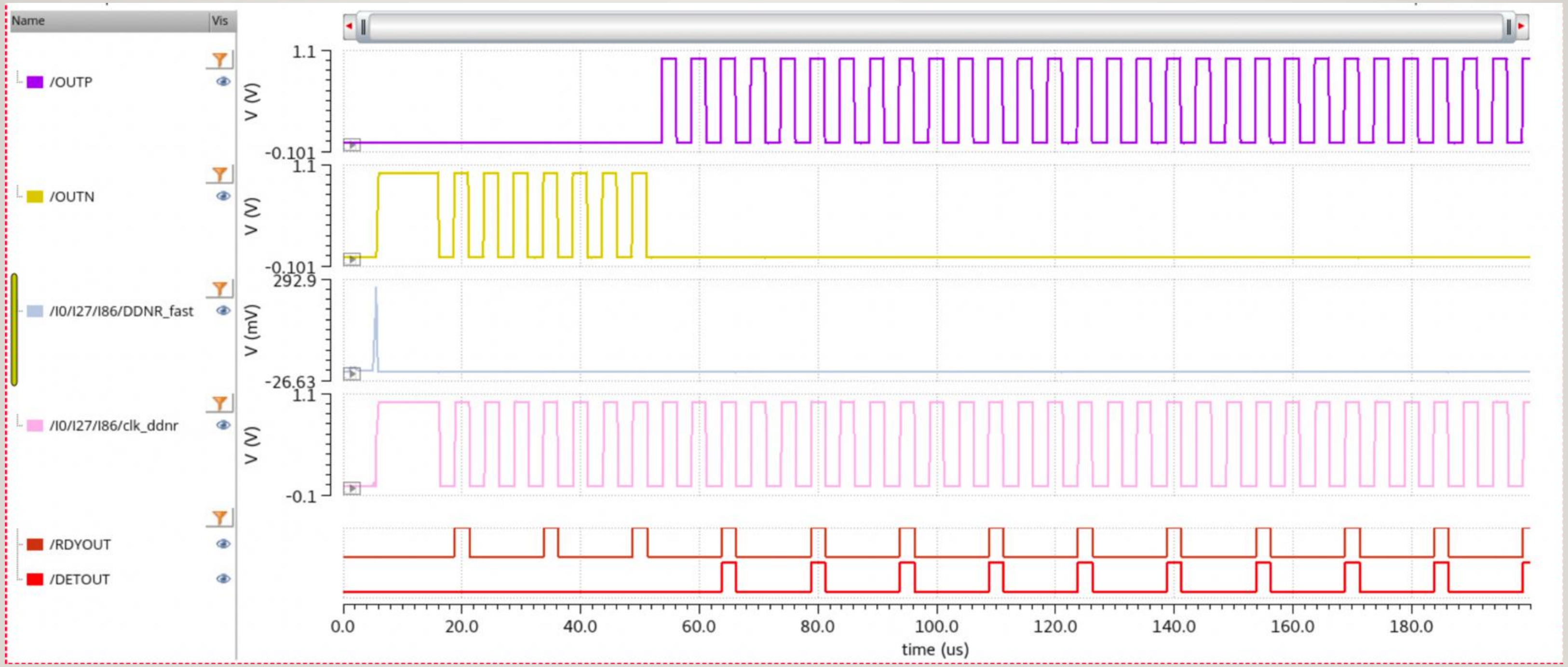
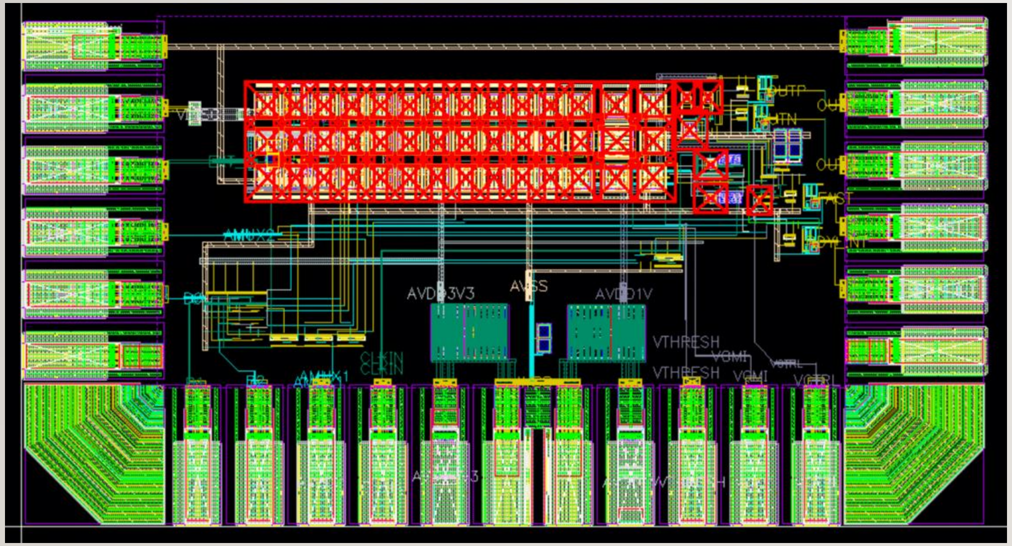
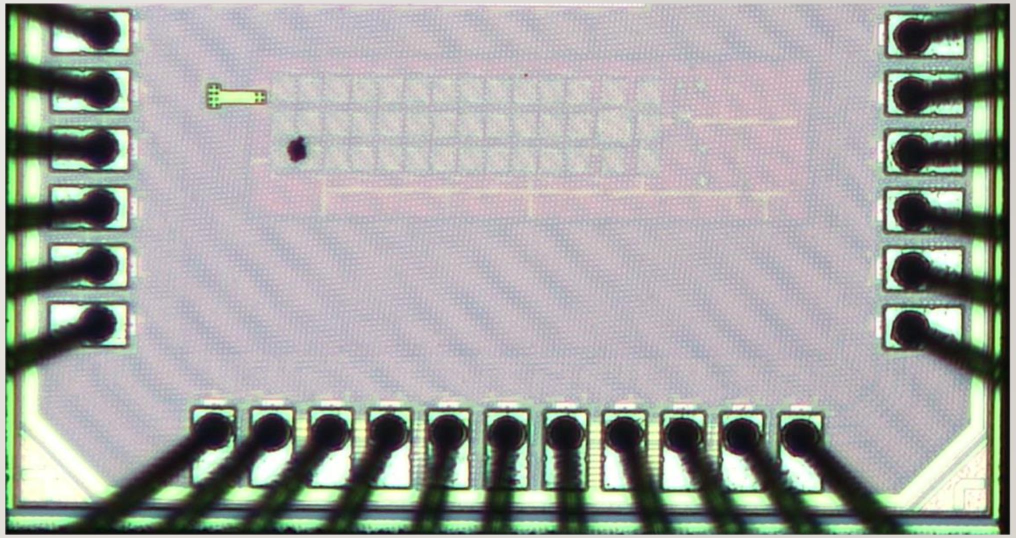


Fig 15: Simulation result with digital DDNR block

TAPEOUT 2



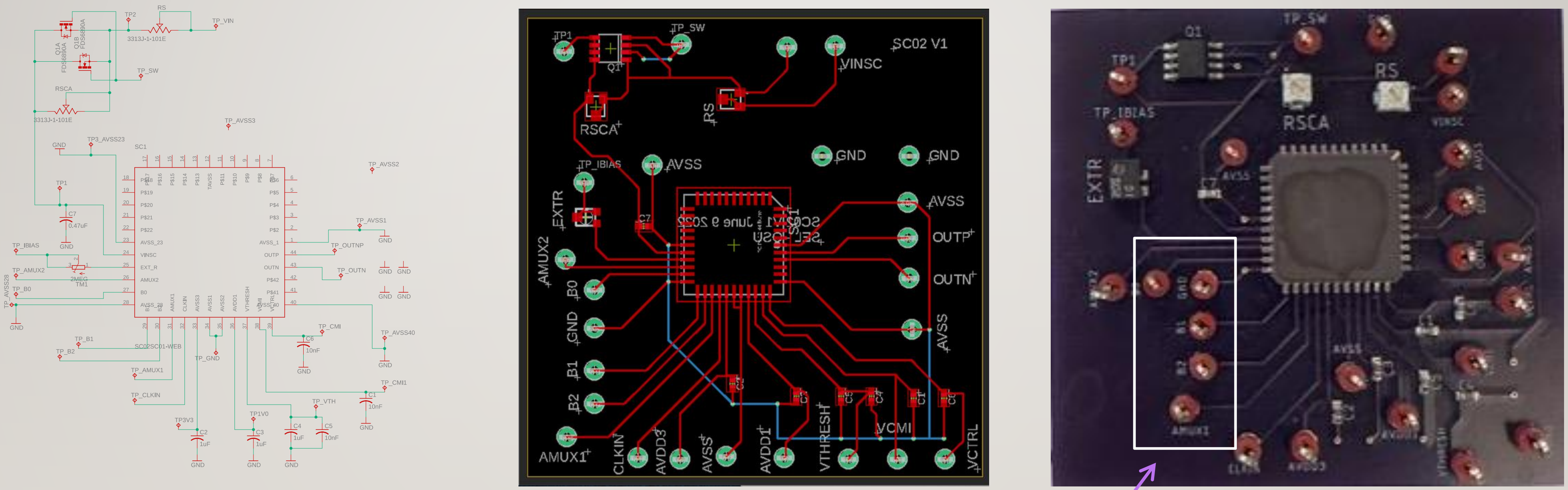
a) SC02 Chip Layout



b) Die photo

Fig 16 : Second tapeout with corrections

PCB PLAN - 2



a) b) c)

Fig 17: PCB for second chip a) Schematic b) Board layout c) Fabricated PCB

TESTMODES

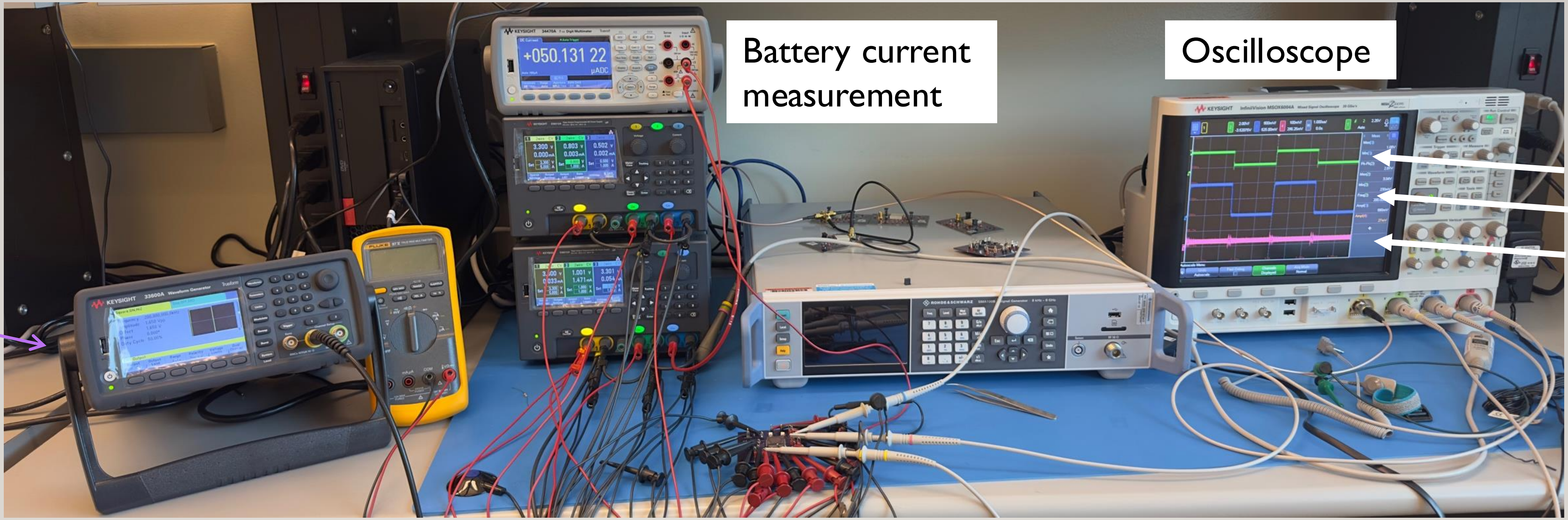
Table 4: Test Mode Operation

B_2	B_1	B_0	**Testmode**	**AMUX1**	**AMUX2**	**Goal**
0	0	0	TM0	NC	NC	Normal operation
0	0	1	TM1	$V_{OUT,OTA}$	V_{C2}	Input/output of OTA accessible; external feedback on PCB
0	1	0	TM2	$V_{OUT,OTA}$	RDY_{INT}	$V_{OUT,OTA}$ in unity feedback; test comparator, V_{CMI}, and $V_{Threshold}$ accessible
0	1	1	TM3	$V_{OUT,OTA}$	Fast	Set Fast threshold; $V_{OUT,OTA}$ accessible
1	0	0	TM4	NC	Fast	Normal operation; observe Fast
1	0	1	TM5	NC	$Fast_{EXT}$	Fast accessible

Table 1: Table of test modes for the second iteration

MEASUREMENT SETUP

Clock source



CLK
OUTP
OUTN

Fig 18: Measurement setup for the board with sources and oscilloscope

MEASUREMENT RESULT

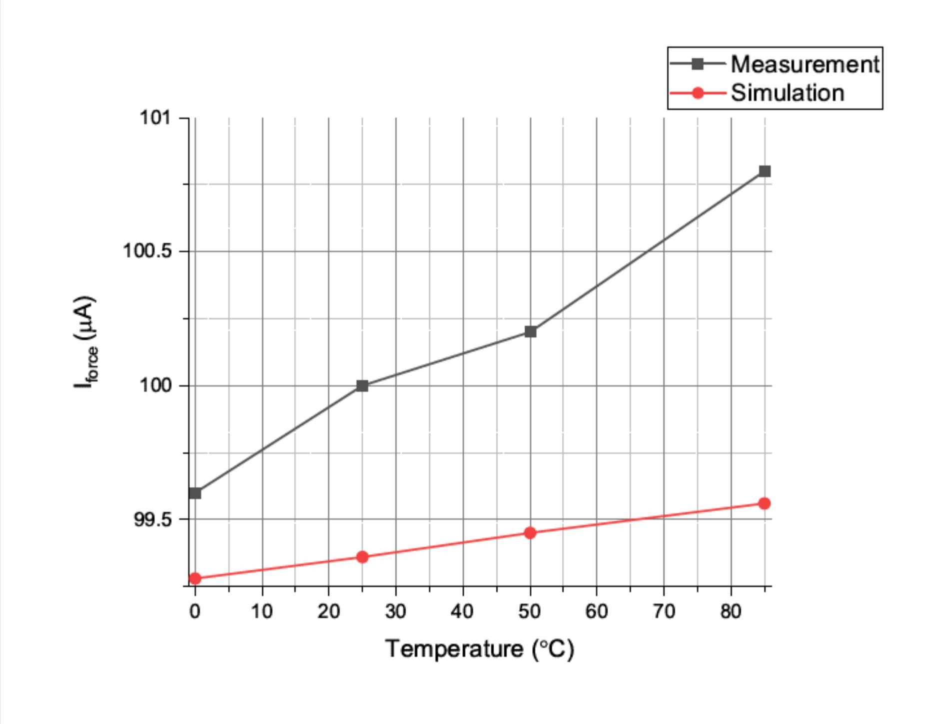


Fig 19 : Iforce variation with Temperature

NOTES

- The sensor didn't work as expected. The test modes verified the problem with OTA. The output stage was not balanced, causing a systematic offset.
- The dynamic comparator worked, but the offset was more than around 1mV.
- Duty cycling the current gives the expected waveform and values.
- The result couldn't be verified with DDNR due to a failure in detection.
- This project was not pursued any further due to advances in detection circuits using a delta-sigma modulator [10].

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

REFERENCES

5. 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
6. 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
7. Murmann, B. (2012). "Thermal Noise in Track-and-Hold Circuits: Analysis and Simulation Techniques." IEEE Solid-State Circuits Magazine 4(2): 46-54.
8. Baker, R. J., "CMOS Circuit Design, Layout, and Simulation, Third Edition," Wiley-IEEE Press, 2010. ISBN 9780470881323
9. 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.
10. S. Konno, A. Golder, and A. Raychowdhury, "1-b Delta-Sigma ADC-Based Power Side-Channel Attack Detection Sensor," *IEEE Sens. Lett.*, vol. 7, no. 4, pp. 1–4, Apr. 2023, doi: 10.1109/LSENS.2023.3259301.