Protection of the Digital Circuitry of a Single Slope ADC against Side Channel Attacks

Kareem Ahmad[1], Ece Öztürk[2], Ceyda Körpe[2],
Hyunsoo Yang[3], Junbin Yang[3], Kanishk Tihaiya[1], Ryanh Tran[1],
Günhan Dündar[2], Vincent John Mooney III[1,3] and Kemal Ozanoglu[2]

[1] School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, USA
[2] Department of Electrical and Electronics Engineering, Boğaziçi University, Istanbul, Turkiye
[3] School of Computer Science, Georgia Institute of Technology, Atlanta, USA

Georgia Tech

BOĞAZİÇİ UNIVERSITY 1863

Table of Contents

Table of Contents

Problem Statement

- Most power side channel attacks on ADC's focus on SAR and other ADCs
- Single Slope ADC (SS ADC) security is under-explored
- SS ADCs are common in image sensors, which are commonly used in security applications

Table of Contents

Threat Model

- Attacker has access to power pins
- Attacker does not have non-destructive access to internal analog sensor pins
- Attacker does not have access to unencrypted digital outputs

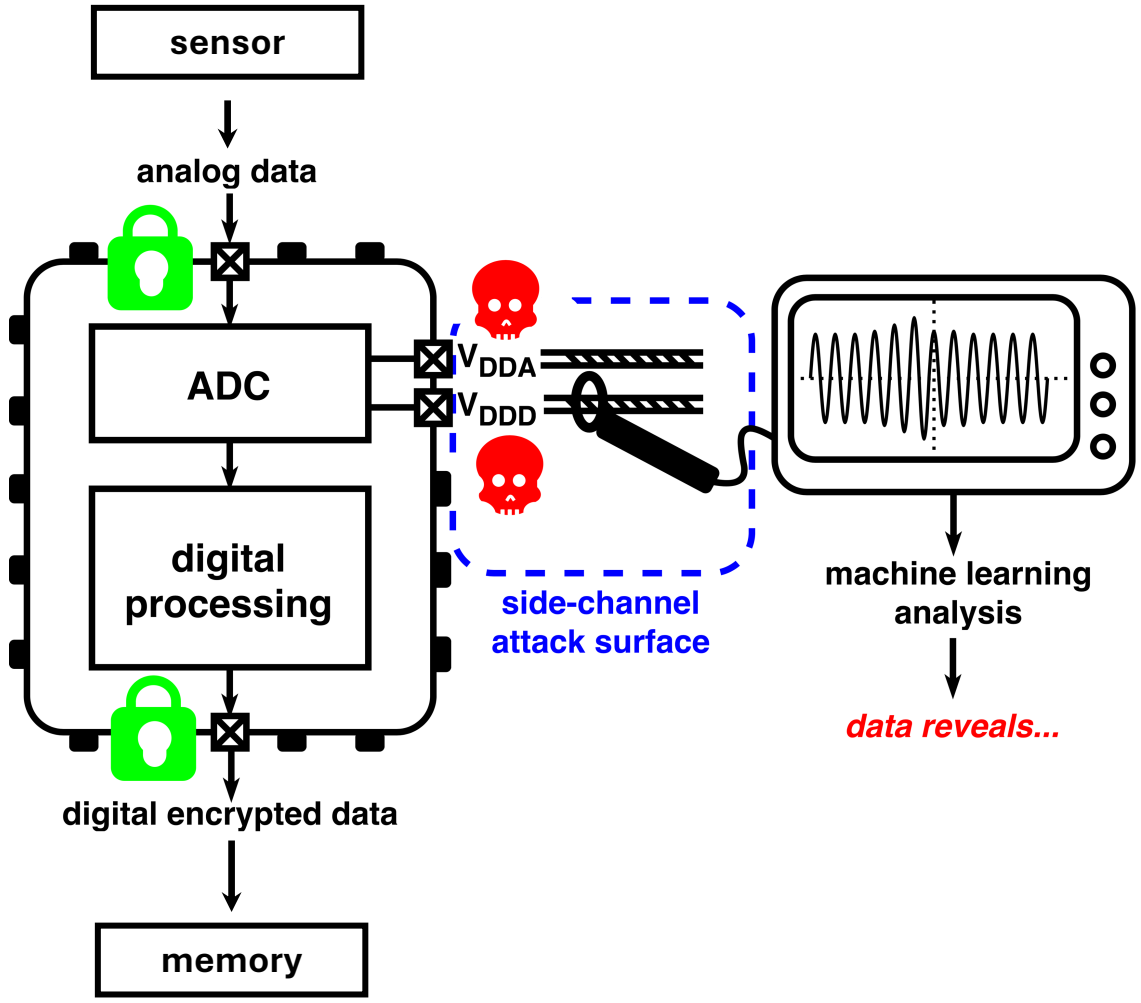
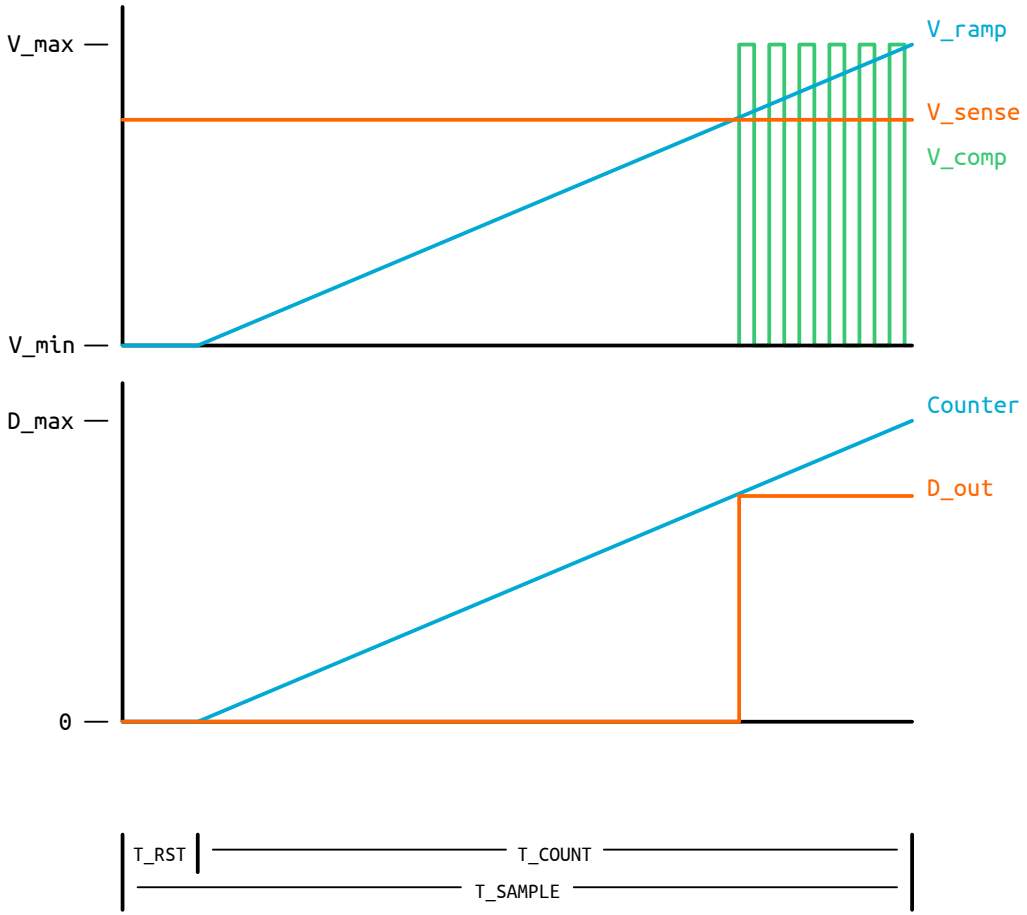


Table of Contents

Single Slope ADC Operation



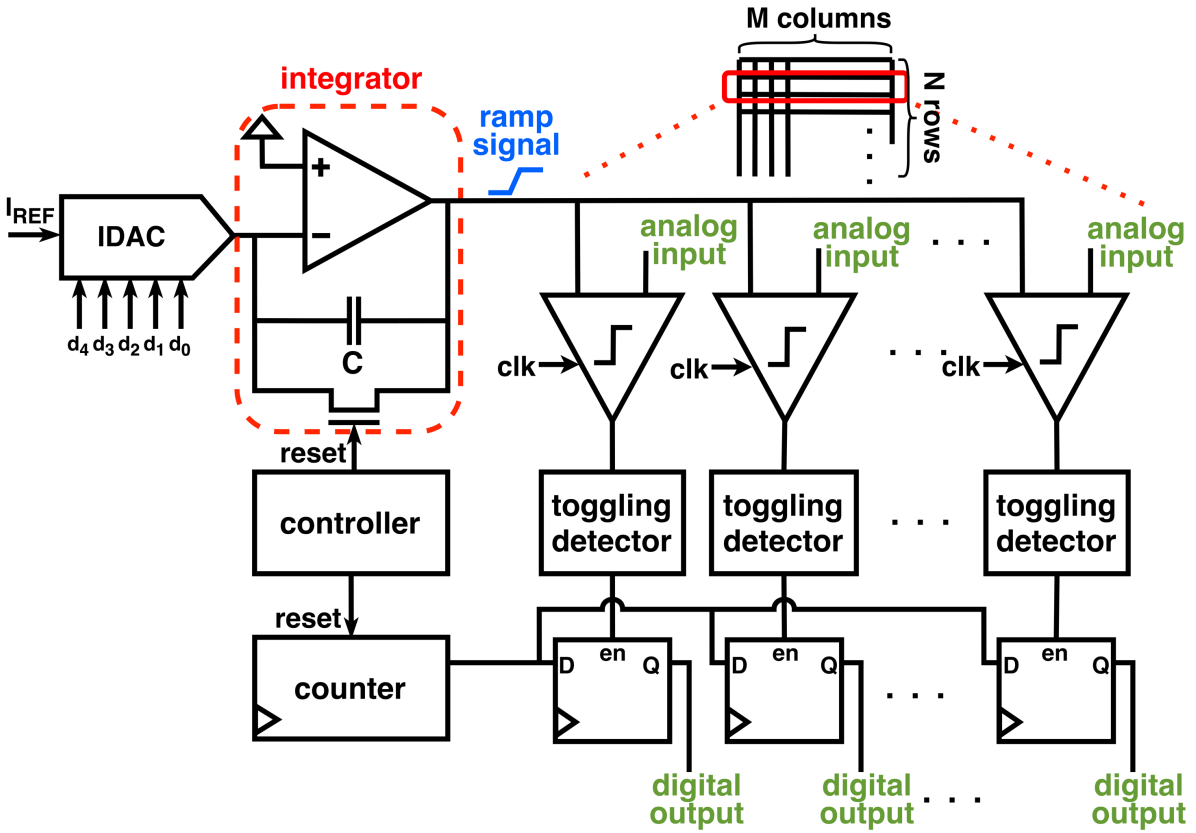


Table of Contents

Research Questions

- Does the **digital** portion of a Single-Slope ADC leak information about the sensed values through the **power side channel**?
- Can information leakage from the **digital** portion, through the **power side channel** be reduced?

- Prior work [5] explored vulnerability of the analog circuitry via the power side channel

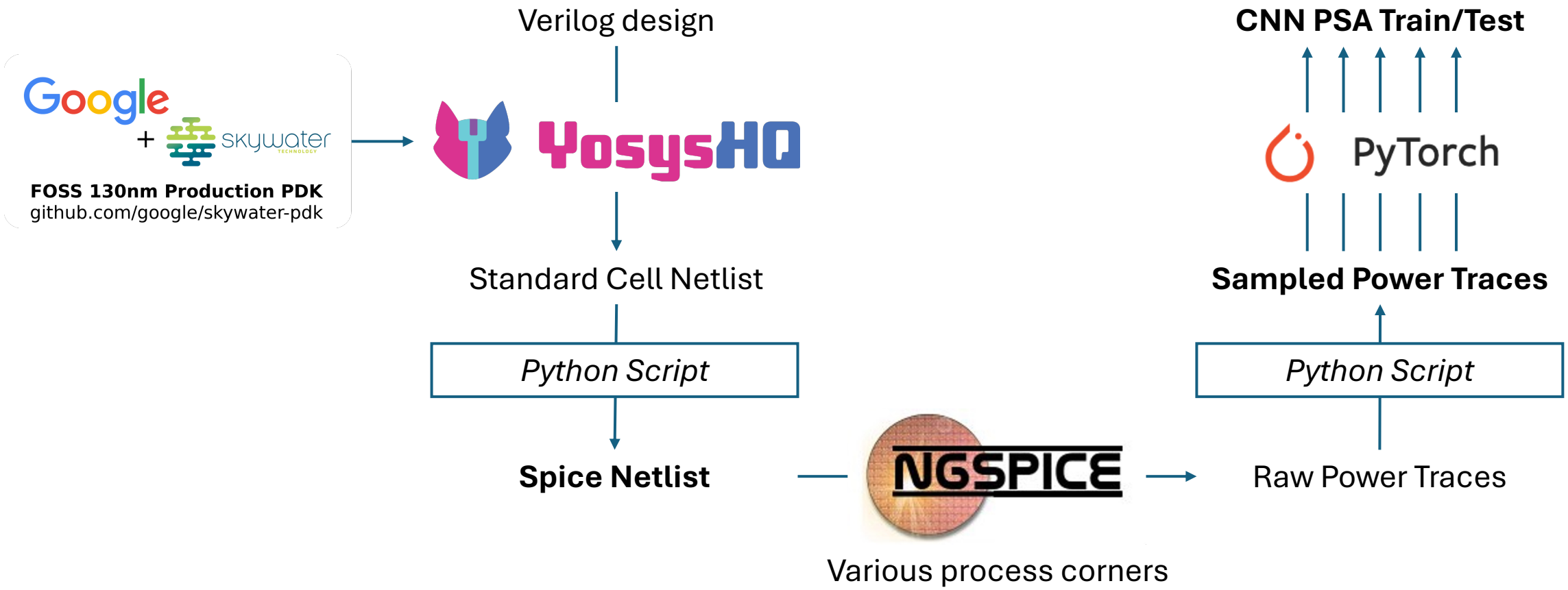
[5] C. Körpe, K. Ahmad, E. Öztürk, K. Tihaiya, R. Tran, H. Yang, J. Yang, G. Dündar, V. J. Mooney III, and K. Ozanoglu, “A Side-Channel Attack-Resilient Single-Slope ADC for Image Sensor Applications,” in Proceedings of the 2025 International Conference on Synthesis, Modeling, Analysis and Simulation Methods and Applications to Circuit Design (SMACD), 2025.

Table of Contents

Methodology: Sample Size

- We attack SPICE simulations of a single pixel measurement
- Key idea:
  - if a single pixel cannot be protected, then the protection of multiple pixels will likely be problematic
  - if a single pixel can be protected, we can then proceed with perhaps similar techniques to protect large simultaneous samples of a realistic pixel array size

Methodology: Tool Flow



Methodology: Tool Flow Iteration

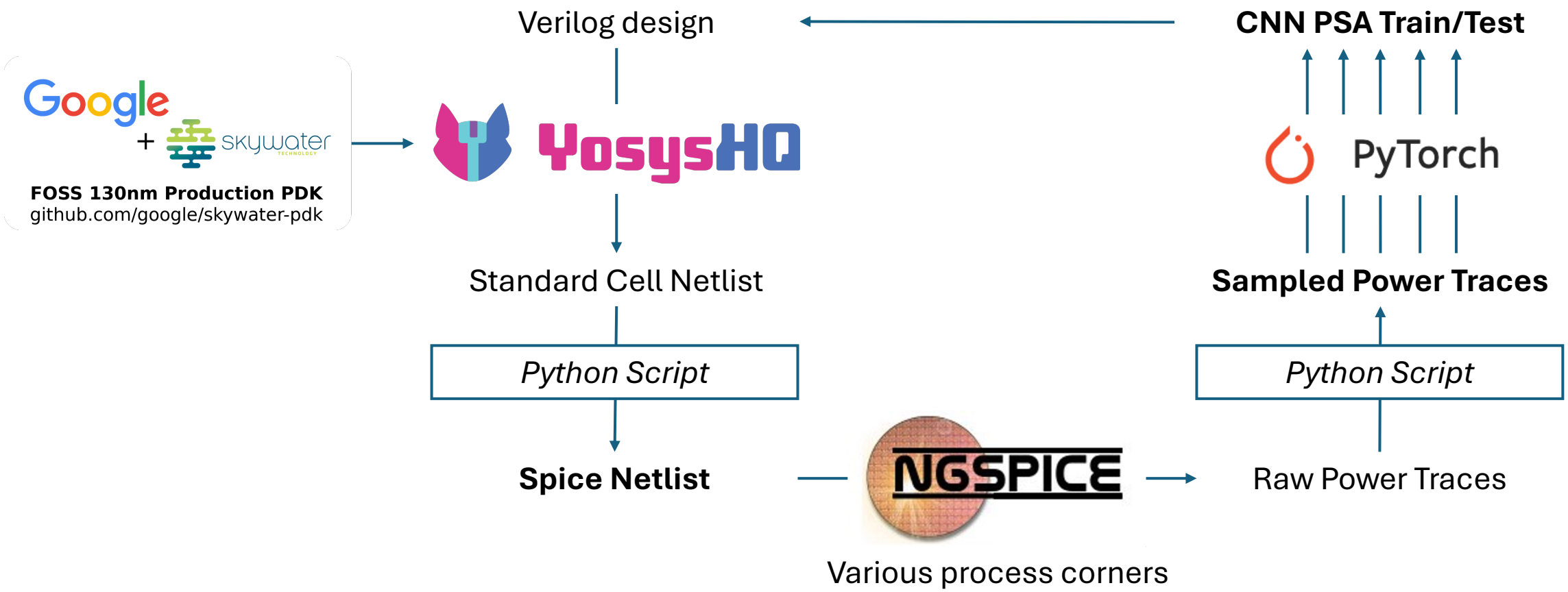


Table of Contents

CNN Architecture

TABLE I: CNN Architecture

	Conv1	**Pool1**	**Conv2**	**Pool2**	**FC1**	**FC2**	**FC3**	**Out**
BW	5,5,1[a]	5,5[b]	5,3,1[a]	2,2[b]	100	100	100	2,SX[c]
SE	5,5,1[a]	5,5[b]	5,3,1[a]	2,2[b]	100	100	100	1

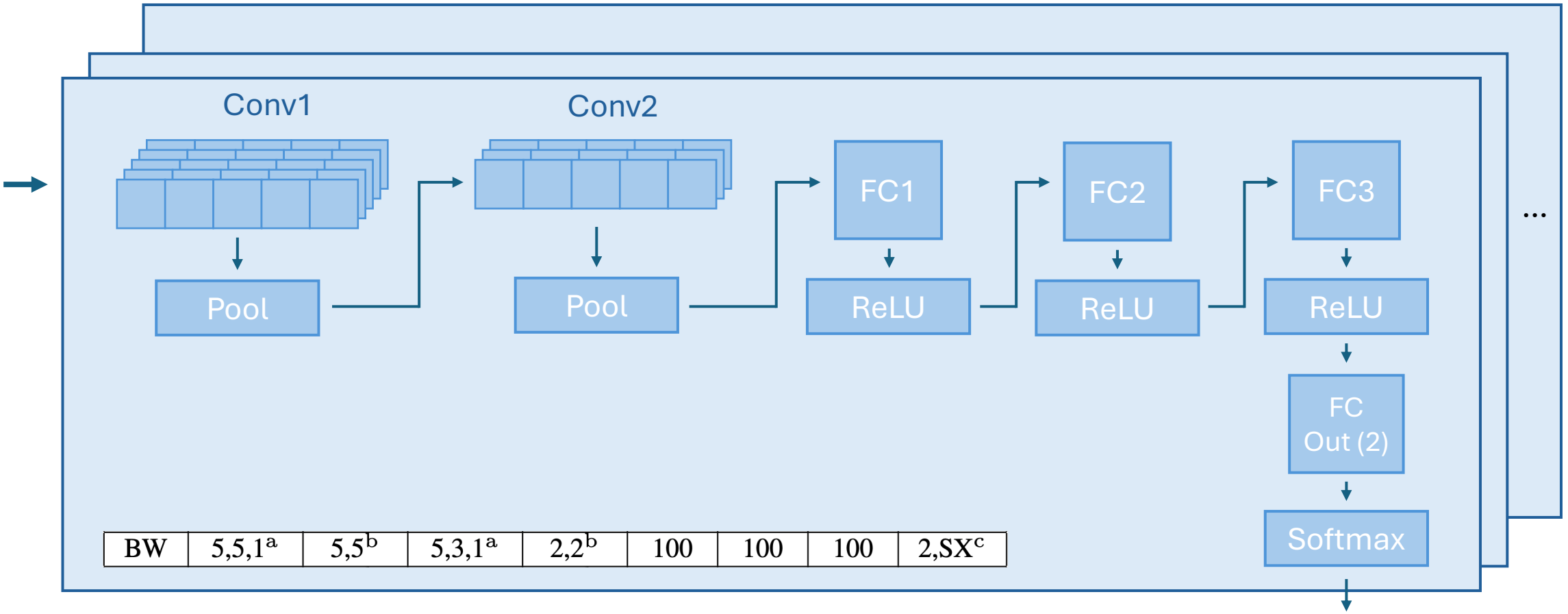
[a]Convolution Parameters are $Size, Channels, Stride$
[b]Pooling Layers are MaxPooling with parameters $Size, Stride$
[c]SX refers to Softmax

CNN Architecture: Bitwise

8 CNNs, one per bit of digital output

$$P(Correct\ Guess) = \frac{1}{2} = \ 50\%$$

CNN Architecture: Bitwise



CNN Architecture: Single-Ended

1 CNN predicting entire 8-bit output

$$P(Correct\ Guess) = \frac{1}{256} \approx 0.39\%$$

CNN Architecture: Single-Ended

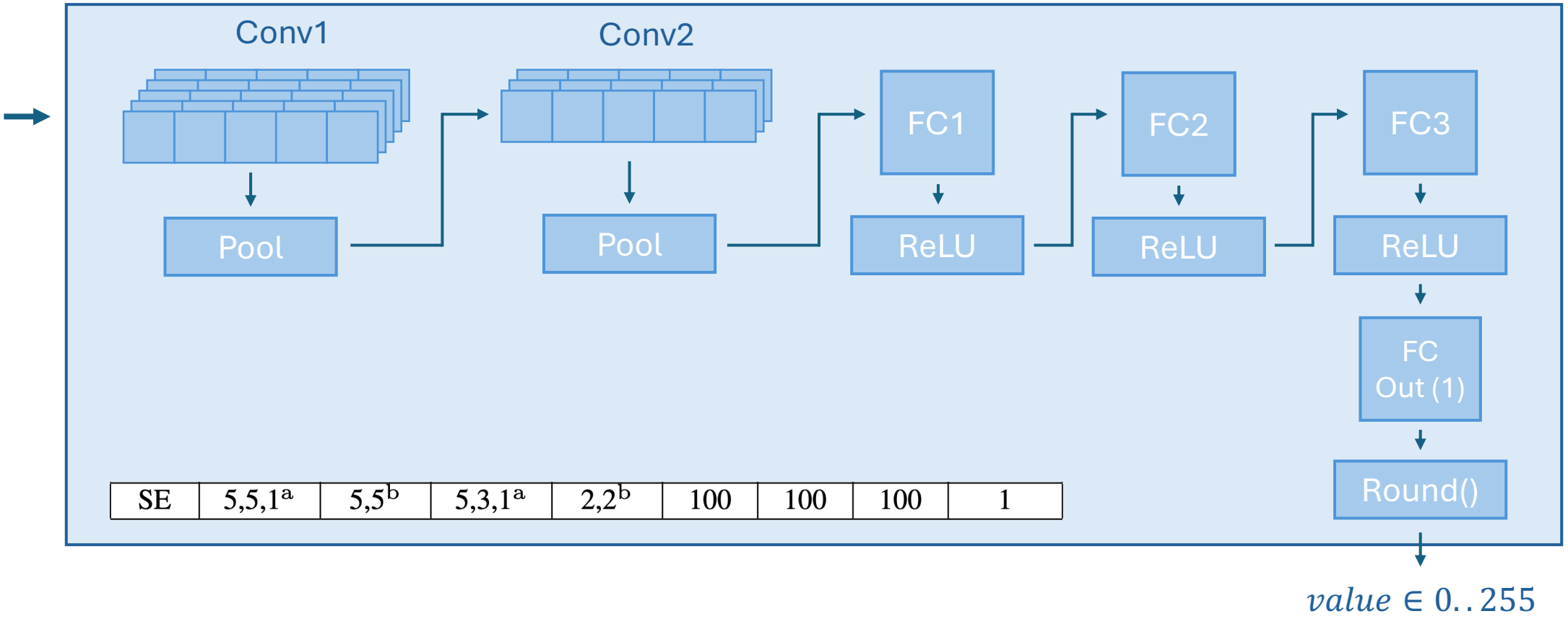
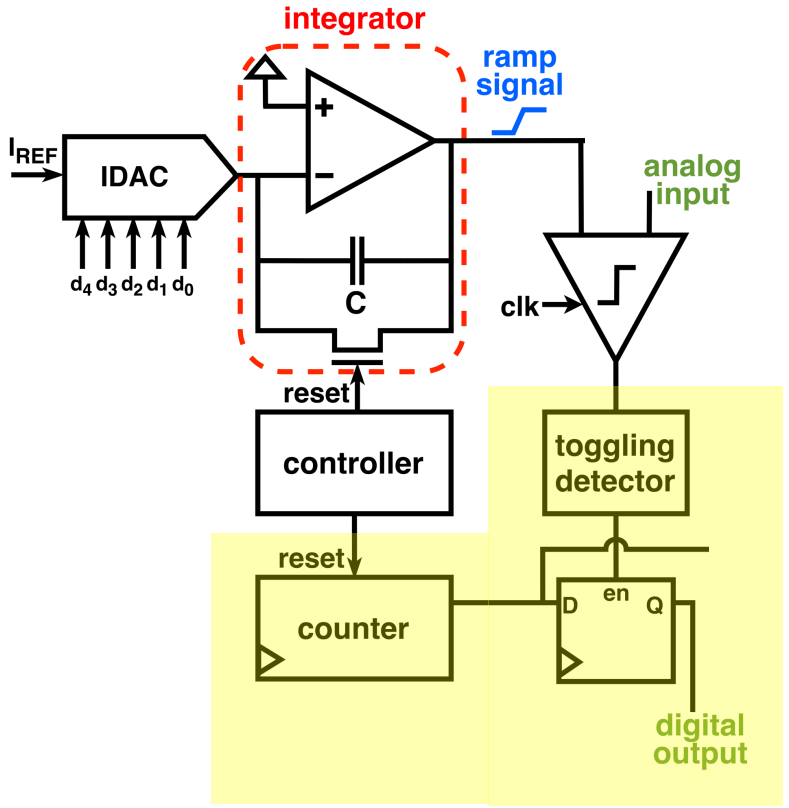


Table of Contents

Table of Contents

Experiment 1 – Unprotected ADC

- Area of standard cells: 513 nm^2
- Train Dataset:
  - 256 traces @ FF corner
- Test Datasets:
  - 256 traces @ FS Corner
  - 256 traces @ SS Corner



Experiment 1 – Leakage

- Current spikes observed at comparator toggle point
- Increased power consumption after comparator toggle point

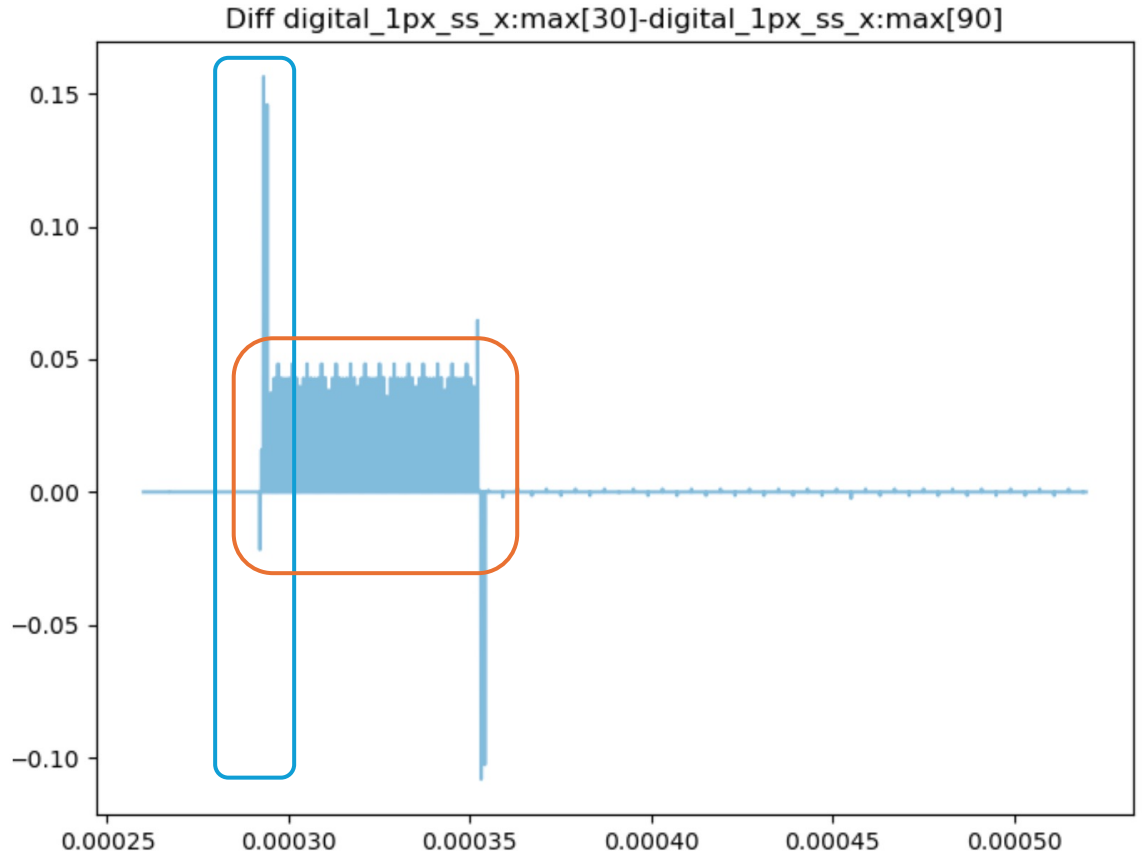
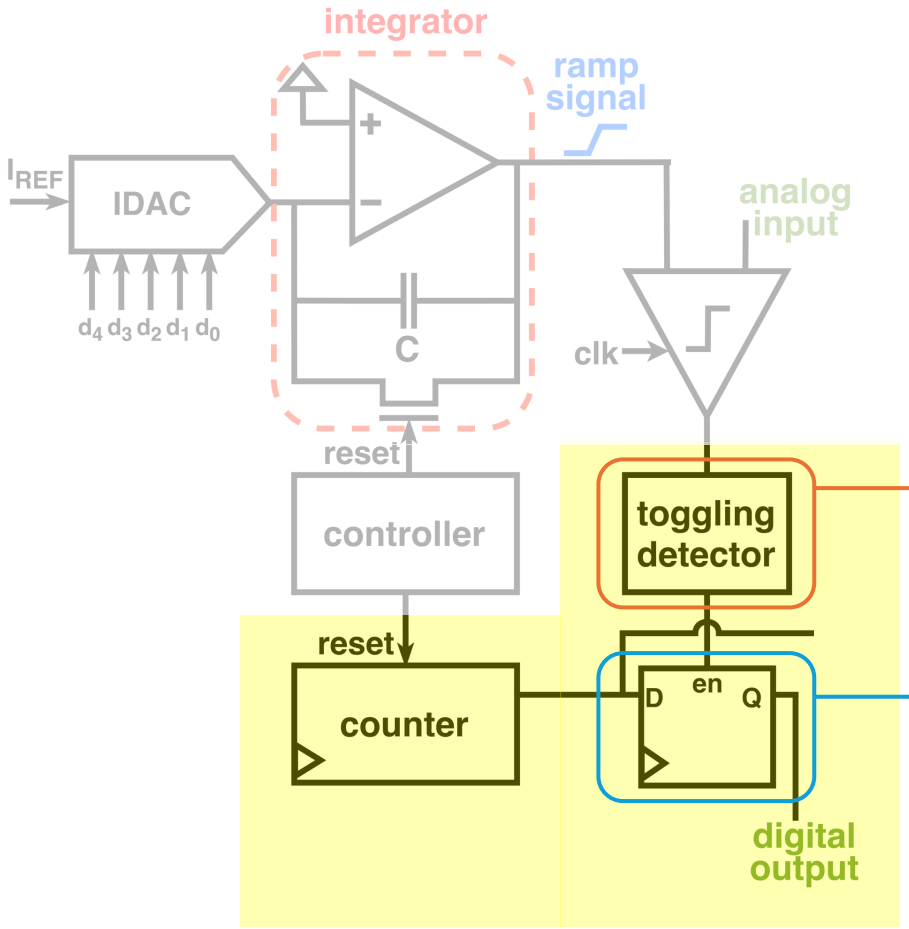


Fig. 3: Difference between unprotected power traces for input values of 30 and 90.

Experiment 1 – Leakage



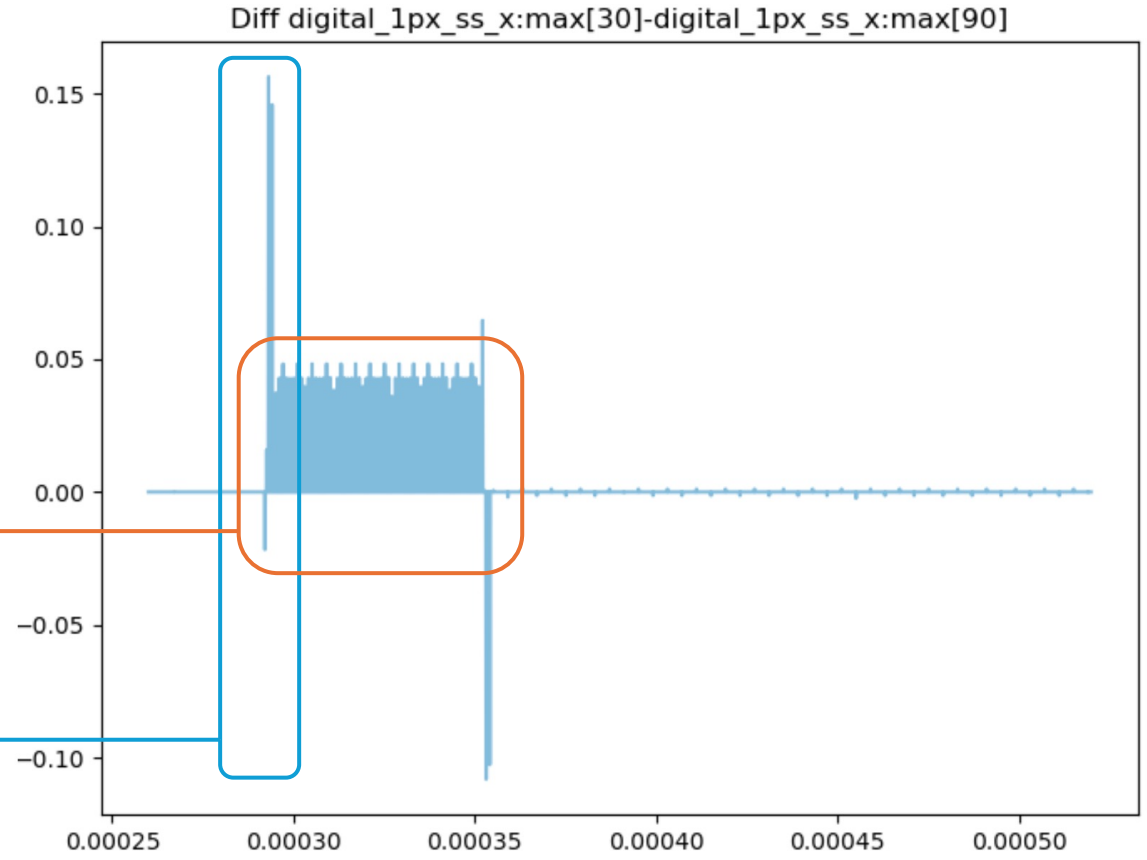


Fig. 3: Difference between unprotected power traces for input values of 30 and 90.

Experiment 1 – Results

Bit	Accuracy		
	Train	Test (SS)	Test (FS)
7	99.8%	99.0%	99.0%
6	99.5%	99.7%	99.4%
5	99.3%	97.8%	99.2%
4	99.3%	99.0%	99.2%
3	98.9%	97.7%	98.7%
2	98.5%	96.4%	98.0%
1	98.8%	96.2%	97.8%
0	98.7%	97.0%	98.1%
BW	93.1%	83.9%	89.8%
SE	96.5%	85.5%	86.8%

Experiment 1 – Results

Bit	Accuracy		
	Train	Test (SS)	Test (FS)
7	99.8%	99.0%	99.0%
6	99.5%	99.7%	99.4%
5	99.3%	97.8%	99.2%
4	99.3%	99.0%	99.2%
3	98.9%	97.7%	98.7%
2	98.5%	96.4%	98.0%
1	98.8%	96.2%	97.8%
0	98.7%	97.0%	98.1%
BW	93.1%	83.9%	89.8%
SE	96.5%	85.5%	86.8%

Experiment 1 – Results

Bit	Accuracy		
	Train	Test (SS)	Test (FS)
7	99.8%	99.0%	99.0%
6	99.5%	99.7%	99.4%
5	99.3%	97.8%	99.2%
4	99.3%	99.0%	99.2%
3	98.9%	97.7%	98.7%
2	98.5%	96.4%	98.0%
1	98.8%	96.2%	97.8%
0	98.7%	97.0%	98.1%
BW	93.1%	83.9%	89.8%
SE	96.5%	85.5%	86.8%

Experiment 1 – Results

Bit	Accuracy		
	Train	Test (SS)	Test (FS)
7	99.8%	99.0%	99.0%
6	99.5%	99.7%	99.4%
5	99.3%	97.8%	99.2%
4	99.3%	99.0%	99.2%
3	98.9%	97.7%	98.7%
2	98.5%	96.4%	98.0%
1	98.8%	96.2%	97.8%
0	98.7%	97.0%	98.1%
BW	93.1%	83.9%	89.8%
SE	96.5%	85.5%	86.8%

Experiment 1 – Results

Bit	Accuracy		
	Train	Test (SS)	Test (FS)
7	99.8%	99.0%	99.0%
6	99.5%	99.7%	99.4%
5	99.3%	97.8%	99.2%
4	99.3%	99.0%	99.2%
3	98.9%	97.7%	98.7%
2	98.5%	96.4%	98.0%
1	98.8%	96.2%	97.8%
0	98.7%	97.0%	98.1%
BW	93.1%	83.9%	89.8%
SE	96.5%	85.5%	86.8%

Table of Contents

Experiment 2 – Protection Attempt

- Area of standard cells: 994 nm^2
- Training:
  - TT corner
- Testing:
  - SS, FS corners

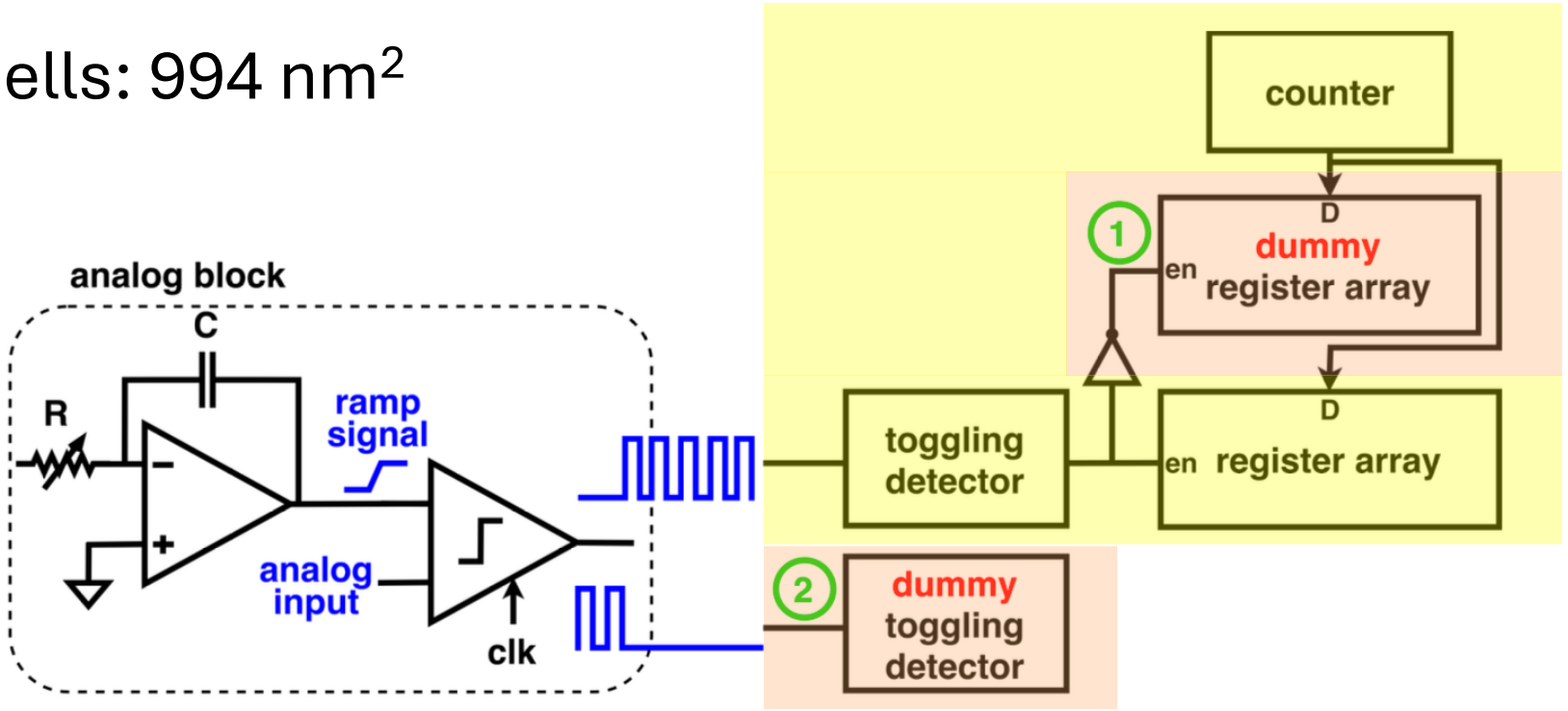


Fig. 4: Initial protection attempt with adding a register array (1) and a dummy toggling detector (2).

Experiment 2 – Leakage

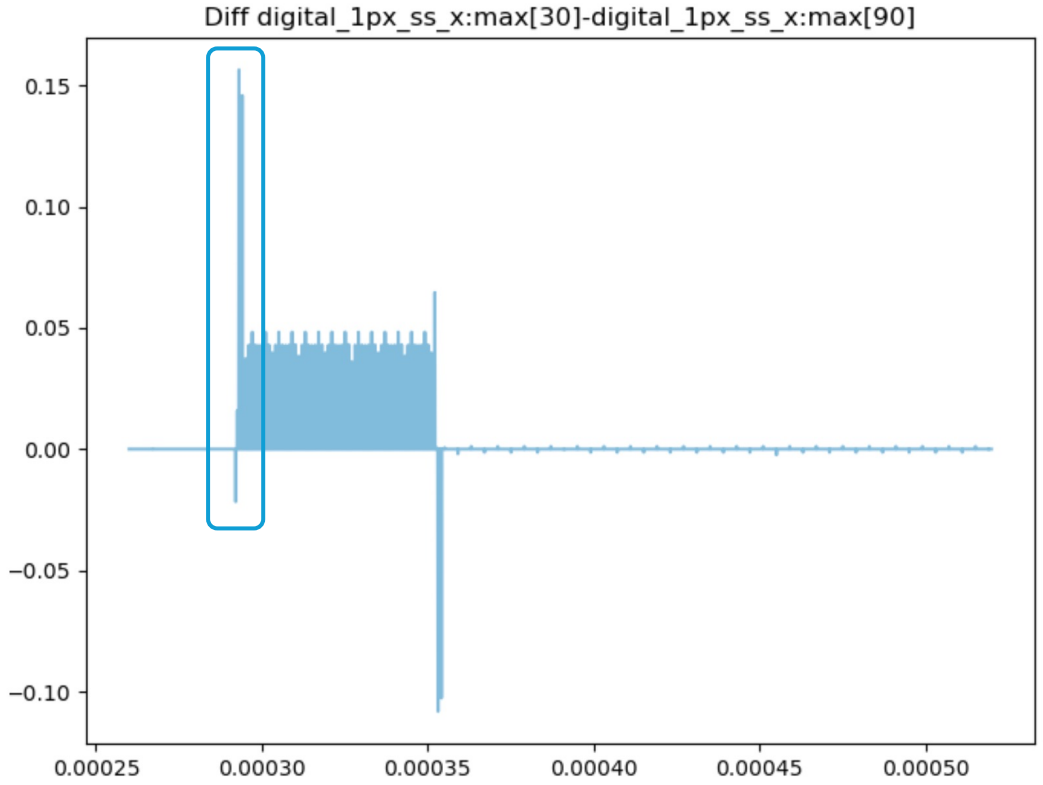


Fig. 3: Difference between unprotected power traces for input values of 30 and 90.

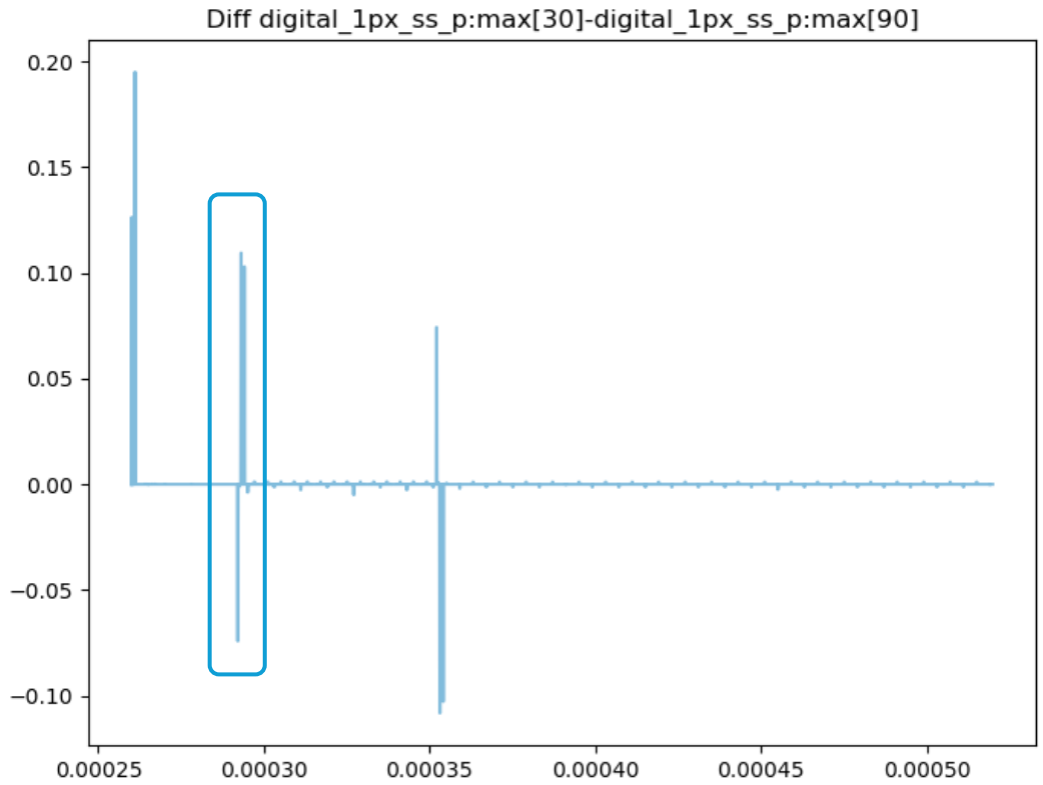
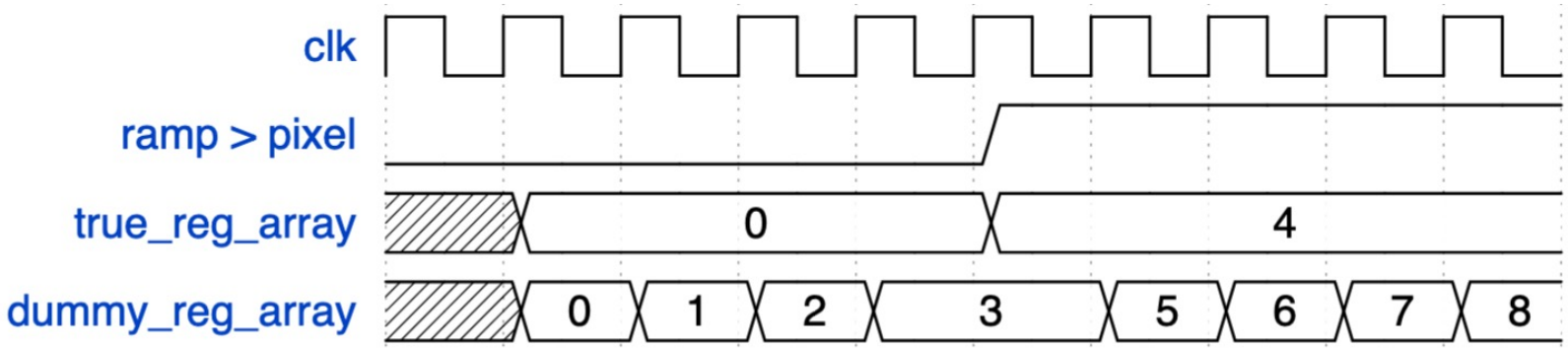


Fig. 5: Difference between power traces for input values of 30 and 90 using first attempt at masking.

Experiment 2 – Leakage

- Hamming distance (HD) of register transitions does not match between true and dummy arrays.
- True Register: $0 \rightarrow value$
  - $HD = Hamming\ weight(value)$
- Dummy Register: $value - 1 \rightarrow value$
  - $HD \in [1, Hamming\ weight\ (value)]$



Experiment 2 – Results

Bit	Accuracy		
	Train	Test (SS)	Test (FS)
7	99.0%	98.8%	98.8%
6	99.0%	98.8%	98.9%
5	99.1%	98.9%	98.9%
4	98.9%	98.1%	97.9%
3	98.9%	98.7%	98.7%
2	98.1%	97.7%	97.9%
1	98.3%	98.1%	98.2%
0	98.6%	98.3%	98.4%
BW	90.4%	88.0%	88.3%
SE	98.8%	96.1%	96.3%

Experiment 2 – Results

Bit	Accuracy		
	Train	Test (SS)	Test (FS)
7	99.0%	98.8%	98.8%
6	99.0%	98.8%	98.9%
5	99.1%	98.9%	98.9%
4	98.9%	98.1%	97.9%
3	98.9%	98.7%	98.7%
2	98.1%	97.7%	97.9%
1	98.3%	98.1%	98.2%
0	98.6%	98.3%	98.4%
BW	90.4%	88.0%	88.3%
SE	98.8%	96.1%	96.3%

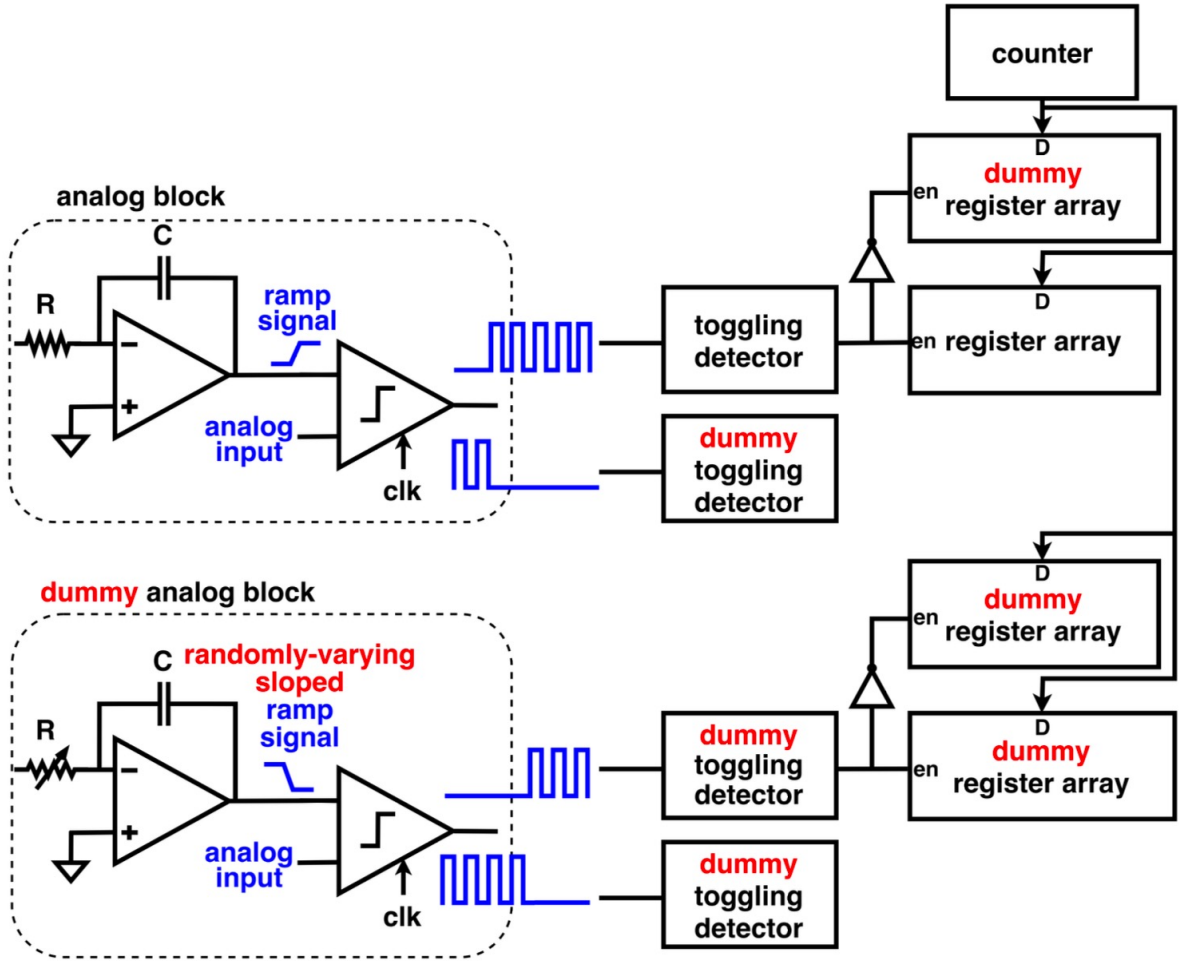
Experiment 2 – Results

Bit	Accuracy		
	Train	Test (SS)	Test (FS)
7	99.0%	98.8%	98.8%
6	99.0%	98.8%	98.9%
5	99.1%	98.9%	98.9%
4	98.9%	98.1%	97.9%
3	98.9%	98.7%	98.7%
2	98.1%	97.7%	97.9%
1	98.3%	98.1%	98.2%
0	98.6%	98.3%	98.4%
BW	90.4%	88.0%	88.3%
SE	98.8%	96.1%	96.3%

Table of Contents

Experiment 4 – Randomized Protection

- Area of Standard Cells: 1956 nm^2
- Builds upon analog protection in prior work [1]
- Duplicates logic from experiment 2 and drives the copy with a randomized comparator



Experiment 4 – Results

Bit	Accuracy		
	Train	Test (SS)	Test (FS)
7	94.6%	56.2%	57.0%
6	97.0%	55.9%	61.4%
5	96.5%	57.8%	65.5%
4	95.8%	54.6%	63.2%
3	95.3%	52.5%	50.9%
2	93.7%	53.3%	54.1%
1	94.4%	49.9%	49.6%
0	98.5%	46.3%	39.7%
BW	85.8%	0.64%	0.79%
SE	97.3%	0.10%	0.18%

Experiment 4 – Results

Bit	Accuracy		
	Train	Test (SS)	Test (FS)
7	94.6%	56.2%	57.0%
6	97.0%	55.9%	61.4%
5	96.5%	57.8%	65.5%
4	95.8%	54.6%	63.2%
3	95.3%	52.5%	50.9%
2	93.7%	53.3%	54.1%
1	94.4%	49.9%	49.6%
0	98.5%	46.3%	39.7%
BW	85.8%	0.64%	0.79%
SE	97.3%	0.10%	0.18%

Experiment 4 – Results

Bit	Accuracy		
	Train	Test (SS)	Test (FS)
7	94.6%	56.2%	57.0%
6	97.0%	55.9%	61.4%
5	96.5%	57.8%	65.5%
4	95.8%	54.6%	63.2%
3	95.3%	52.5%	50.9%
2	93.7%	53.3%	54.1%
1	94.4%	49.9%	49.6%
0	98.5%	46.3%	39.7%
BW	85.8%	0.64%	0.79%
SE	97.3%	0.10%	0.18%

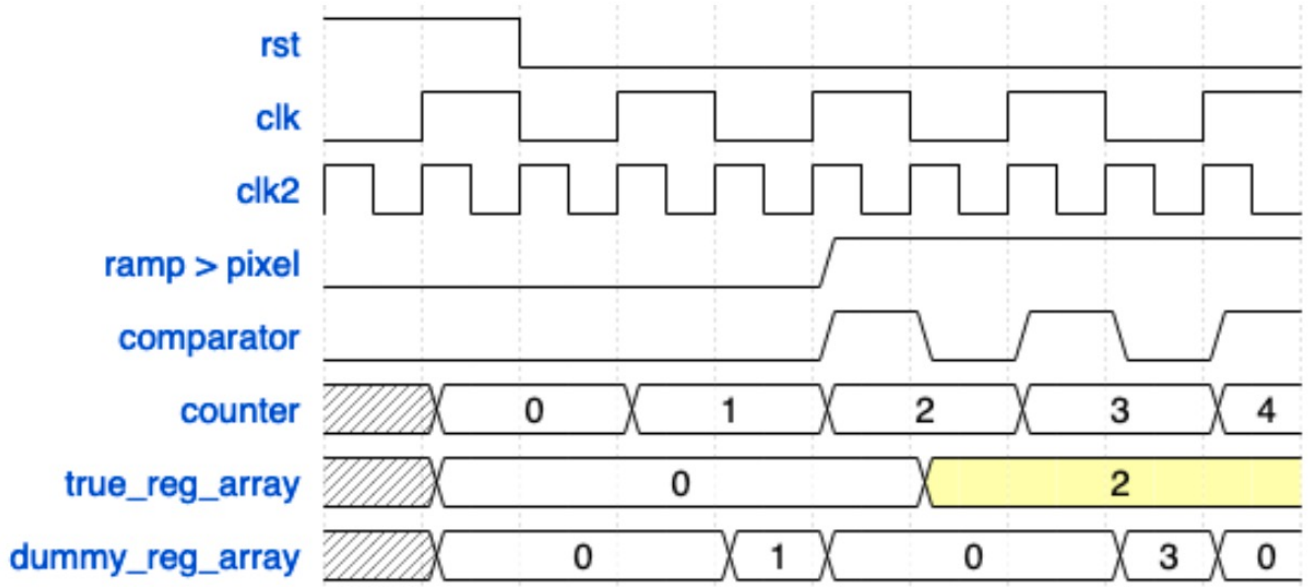
Experiment 4 – Results

Bit	Accuracy		
	Train	Test (SS)	Test (FS)
7	94.6%	56.2%	57.0%
6	97.0%	55.9%	61.4%
5	96.5%	57.8%	65.5%
4	95.8%	54.6%	63.2%
3	95.3%	52.5%	50.9%
2	93.7%	53.3%	54.1%
1	94.4%	49.9%	49.6%
0	98.5%	46.3%	39.7%
BW	85.8%	0.64%	0.79%
SE	97.3%	0.10%	0.18%

Table of Contents

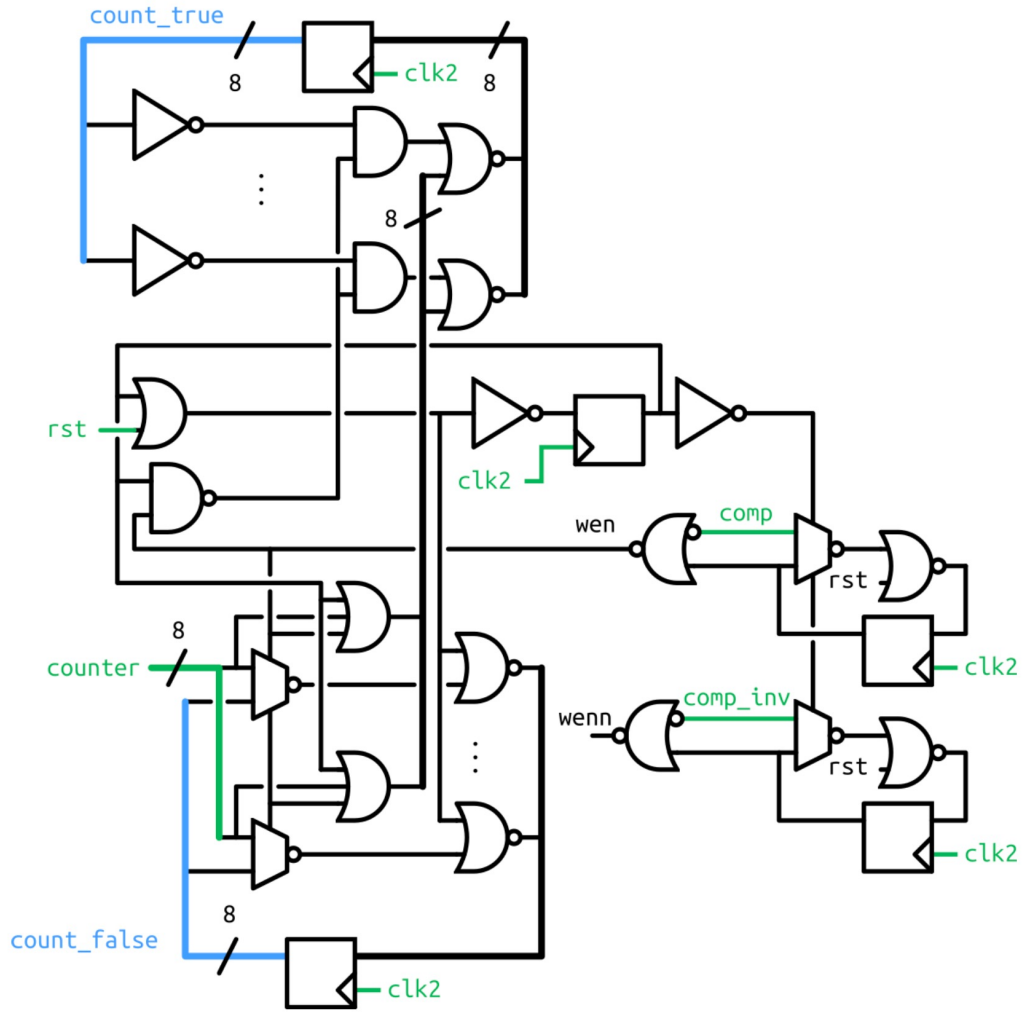
Experiment 3 – Masked Protection

- Goal: dummy register transitions should have HD from zero as with true register transitions
- Add second clock to reset dummy register between writes
- Area of Standard Cells: 1440 nm^2



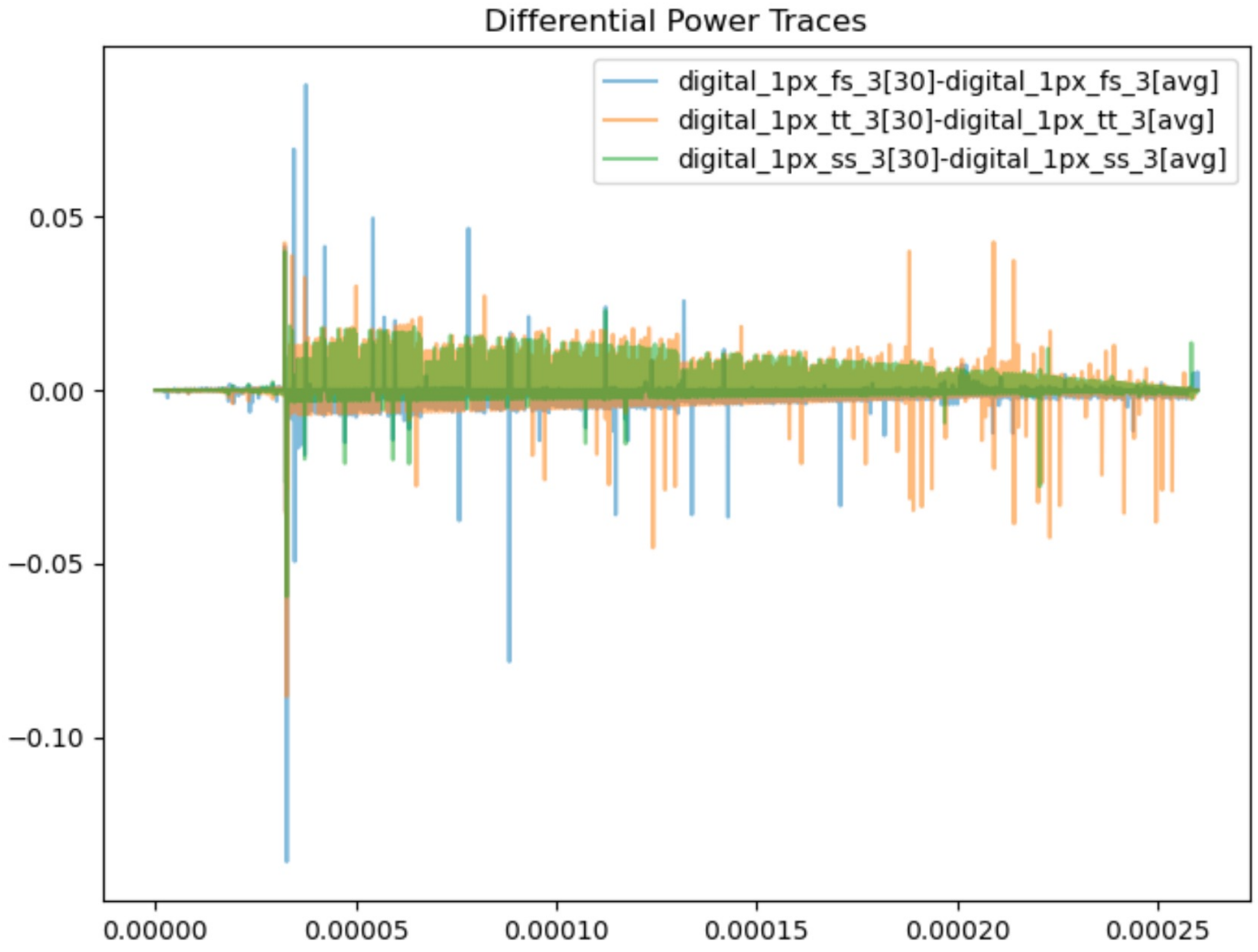
Experiment 3 – Masked Protection

- Goal: dummy register transitions should have HD from zero as with true register transitions
- Add second clock to reset dummy register between writes
- Area of Standard Cells: 1440 nm^2



Experiment 3 – Leakage

- Power (energy consumption) patterns are not consistent across process corners



Experiment 3 – Results

Bit	Accuracy		
	Train	Test (SS)	Test (FS)
7	99.6%	50.6%	47.4%
6	99.3%	50.7%	48.7%
5	98.9%	50.2%	51.0%
4	96.9%	50.2%	51.7%
3	98.1%	50.4%	51.7%
2	96.8%	50.3%	52.6%
1	97.7%	51.4%	53.4%
0	97.1%	50.1%	51.2%
BW	85.3%	0.42%	0.45%
SE	92.9%	0.20%	0.49%

Experiment 3 – Results

Bit	Accuracy		
	Train	Test (SS)	Test (FS)
7	99.6%	50.6%	47.4%
6	99.3%	50.7%	48.7%
5	98.9%	50.2%	51.0%
4	96.9%	50.2%	51.7%
3	98.1%	50.4%	51.7%
2	96.8%	50.3%	52.6%
1	97.7%	51.4%	53.4%
0	97.1%	50.1%	51.2%
BW	85.3%	0.42%	0.45%
SE	92.9%	0.20%	0.49%

Experiment 3 – Results

Bit	Accuracy		
	Train	Test (SS)	Test (FS)
7	99.6%	50.6%	47.4%
6	99.3%	50.7%	48.7%
5	98.9%	50.2%	51.0%
4	96.9%	50.2%	51.7%
3	98.1%	50.4%	51.7%
2	96.8%	50.3%	52.6%
1	97.7%	51.4%	53.4%
0	97.1%	50.1%	51.2%
BW	85.3%	0.42%	0.45%
SE	92.9%	0.20%	0.49%

Table of Contents

Summary: Table 6 (original)

	Unprotected	Failed	Masked	Randomized
Bit 7	99.0%	98.8%	47.4%	57.0%
Bit 6	99.4%	98.9%	48.7%	61.4%
Bit 5	99.2%	98.9%	51.0%	65.5%
Bit 4	99.2%	97.9%	51.7%	63.2%
Bit 3	98.7%	98.7%	51.7%	50.9%
Bit 2	98.0%	97.9%	52.6%	54.1%
Bit 1	97.8%	98.2%	53.4%	49.6%
Bit 0	98.1%	98.4%	51.2%	39.7%
BW	89.8%	88.3%	0.45%	0.79%
SE	86.8%	96.3%	0.49%	0.18%
Area	$513\,nm^2$ 100%	$994\,nm^2$ 190%	$1440\,nm^2$ 280%	$1956\,nm^2$ 380%

Summary: Table 6 (amended)

	Unprotected	Failed	Masked	Randomized
Bit 7	99.0%	98.8%	47.4%	57.0%
Bit 6	99.4%	98.9%	48.7%	61.4%
Bit 5	99.2%	98.9%	51.0%	65.5%
Bit 4	99.2%	97.9%	51.7%	63.2%
Bit 3	98.7%	98.7%	51.7%	50.9%
Bit 2	98.0%	97.9%	52.6%	54.1%
Bit 1	97.8%	98.2%	53.4%	49.6%
Bit 0	98.1%	98.4%	51.2%	39.7%
BW	89.8%	88.3%	0.45%	0.79%
SE	86.8%	96.3%	0.49%	0.18%
Area	$996\,nm^2$ 100%	$1477\,nm^2$ 148%	$1440\,nm^2$ 145%	$2439\,nm^2$ 245%

Summary

	Unprotected	Failed	Masked	Randomized
Bit 7	99.0%	98.8%	47.4%	57.0%
Bit 6	99.4%	98.9%	48.7%	61.4%
Bit 5	99.2%	98.9%	51.0%	65.5%
Bit 4	99.2%	97.9%	51.7%	63.2%
Bit 3	98.7%	98.7%	51.7%	50.9%
Bit 2	98.0%	97.9%	52.6%	54.1%
Bit 1	97.8%	98.2%	53.4%	49.6%
Bit 0	98.1%	98.4%	51.2%	39.7%
BW	89.8%	88.3%	0.45%	0.79%
SE	86.8%	96.3%	0.49%	0.18%
Area	$996\,nm^2$ 100%	$1477\,nm^2$ 148%	$1440\,nm^2$ 145%	$2439\,nm^2$ 245%

Summary

	Unprotected	Failed	Masked	Randomized
Bit 7	99.0%	98.8%	47.4%	57.0%
Bit 6	99.4%	98.9%	48.7%	61.4%
Bit 5	99.2%	98.9%	51.0%	65.5%
Bit 4	99.2%	97.9%	51.7%	63.2%
Bit 3	98.7%	98.7%	51.7%	50.9%
Bit 2	98.0%	97.9%	52.6%	54.1%
Bit 1	97.8%	98.2%	53.4%	49.6%
Bit 0	98.1%	98.4%	51.2%	39.7%
BW	89.8%	88.3%	0.45%	0.79%
SE	86.8%	96.3%	0.49%	0.18%
Area	996 nm^2 100%	1477 nm^2 148%	1440 nm^2 145%	2439 nm^2 245%

Summary

	Unprotected	Failed	Masked	Randomized
Bit 7	99.0%	98.8%	47.4%	57.0%
Bit 6	99.4%	98.9%	48.7%	61.4%
Bit 5	99.2%	98.9%	51.0%	65.5%
Bit 4	99.2%	97.9%	51.7%	63.2%
Bit 3	98.7%	98.7%	51.7%	50.9%
Bit 2	98.0%	97.9%	52.6%	54.1%
Bit 1	97.8%	98.2%	53.4%	49.6%
Bit 0	98.1%	98.4%	51.2%	39.7%
BW	89.8%	88.3%	0.45%	0.79%
SE	86.8%	96.3%	0.49%	0.18%
Area	996 nm^2 100%	1477 nm^2 148%	1440 nm^2 145%	2439 nm^2 245%

Summary

	Unprotected	Failed	Masked	Randomized
Bit 7	99.0%	98.8%	47.4%	57.0%
Bit 6	99.4%	98.9%	48.7%	61.4%
Bit 5	99.2%	98.9%	51.0%	65.5%
Bit 4	99.2%	97.9%	51.7%	63.2%
Bit 3	98.7%	98.7%	51.7%	50.9%
Bit 2	98.0%	97.9%	52.6%	54.1%
Bit 1	97.8%	98.2%	53.4%	49.6%
Bit 0	98.1%	98.4%	51.2%	39.7%
BW	89.8%	88.3%	0.45%	0.79%
SE	86.8%	96.3%	0.49%	0.18%
Area	996 nm^2 100%	1477 nm^2 148%	1440 nm^2 145%	2439 nm^2 245%

Digital Area Estimates for 50 pixel array

- Counter logic is shared
- Independent sampling logic

	Unprotected	Failed	Masked	Randomized
Area	24571 nm^2	48626 nm^2	96738 nm^2	46788 nm^2
	100%	198%	294%	190%

Future Work

- Post-layout/PNR simulations including parasitics
- Markov-based process variations in addition to process corners
- Attack using both SS ADC power traces (analog and digital traces)
  - Power overhead cost calculation for the protected system including both analog and digital circuitry
- Multi-pixel attacks

References

[1] T. Jeong, A. Chandrakasan, and H.-S. Lee, “S2ADC: A 12-bit, 1.25MS/s Secure SAR ADC with Power Side-Channel Attack Resistance,” in 2020 IEEE Custom Integrated Circuits Conference (CICC), 2020, pp. 1–4.

[2] R. Chen, H. Wang, Chandrakasan, and H.-S. Lee, “RaM-SAR: a low energy and area overhead, 11.3 fj/conv.-step 12b 25ms/s secure random-mapping SAR ADC with power and EM side-channel attack resilience,”in 2022 IEEE Symposium on VLSI Technology and Circuits. IEEE, 2022, pp. 94–95.

[3] S. N. Karanth et al., “Randomization Approaches for Secure SAR ADC Design Resilient Against Power Side-Channel Attacks,” in 2024 IEEE Int. Symp. on Hardware Oriented Security and Trust (HOST), 2024, pp. 282–292.

[4] T. Miki et al., “A Random Interrupt Dithering SAR Technique for Secure ADC Against Reference-Charge Side-Channel Attack,” IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 67, no. 1, pp. 14–18, 2020.¨

[5] C. Körpe, K. Ahmad, E. Öztürk, K. Tihaiya, R. Tran, H. Yang, J. Yang, G. Dündar, V. J. M. III, and K. Ozanoglu, “A Side-Channel Attack-Resilient Single-Slope ADC for Image Sensor Applications,” in Proceedings of the 2025 International Conference on Synthesis, Modeling, Analysis and Simulation Methods and Applications to Circuit Design (SMACD), 2025.

[6] Veripool, “Verilator,” https://veripool.org/verilator/documentation/, 2025.

[7] Google / SkyWater Technology Foundry, “SkyWater 130nm PDK,” https://skywater-pdk.readthedocs.io/, 2020.

[8] C. Wolf et al., “Yosys open synthesis suite,” https://yosyshq.net/yosys/, 2013.

[9] T. N. Project, “NGSpice circuit simulator,” http://ngspice.sourceforge.net/, 2025.

[10] P. Developers, “PyTorch: An open source machine learning framework,” https://pytorch.org/, 2025.