A Side-Channel Attack-Resilient Single-Slope ADC for Image Sensor Applications

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

[*]Department of Electrical and Electronics Engineering, Boğaziçi University, Istanbul, Turkiye
[†]School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, USA
[‡]School of Computer Science, Georgia Institute of Technology, Atlanta, USA

ceyda.korpe@std.bogazici.edu.tr

8 July, 2025

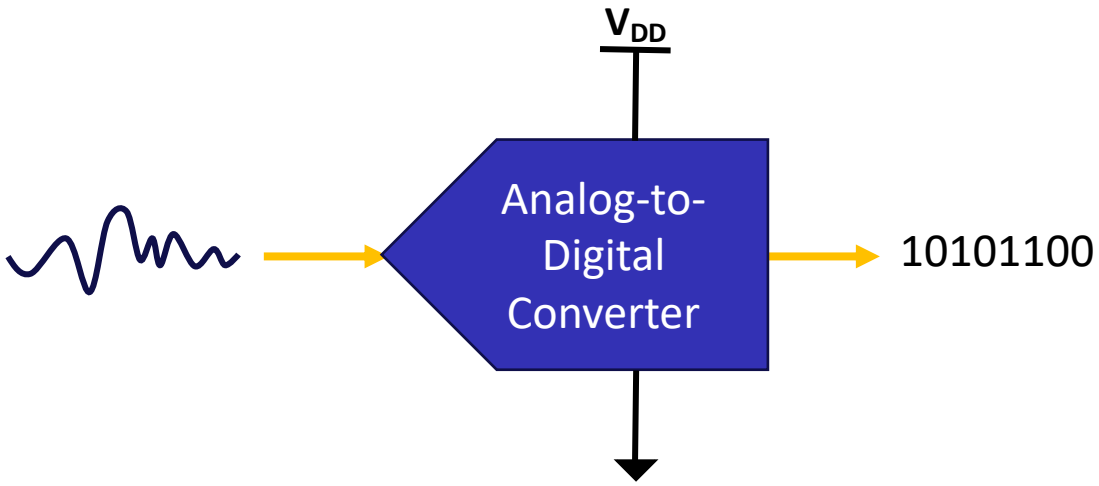
21th International Conference on Synthesis, Modeling, Analysis and Simulation Methods, and Applications to Circuit Design 7 - 10 of July 2025, Istanbul - TÜRKİYE

Outline

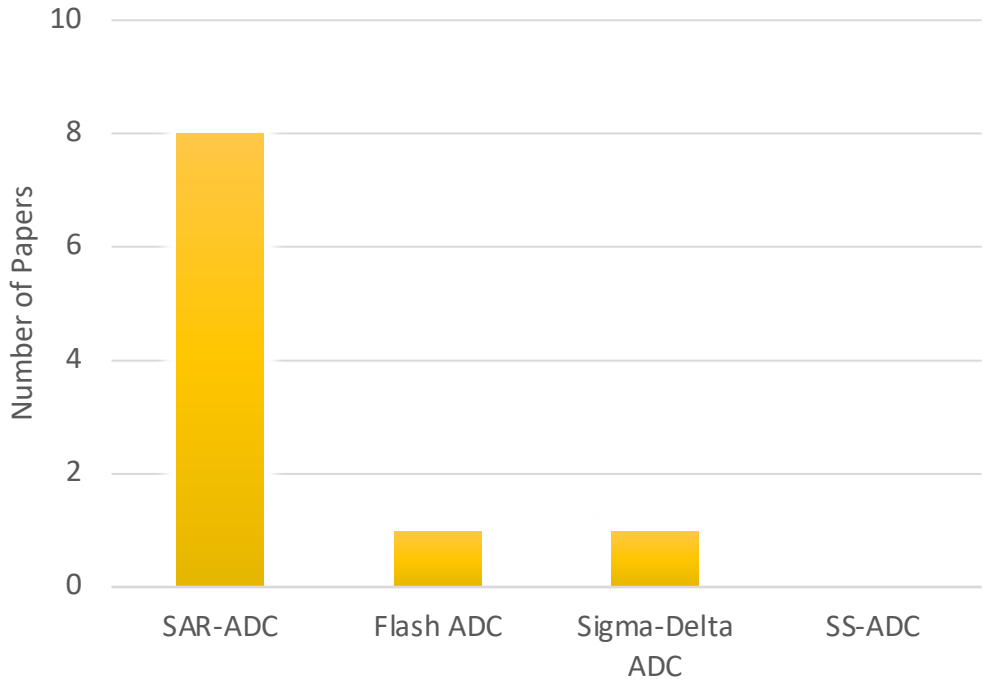
- Introduction & Motivation
- Background
- Threat Model
- SAR vs SS-ADC in Power Side-Channel Attacks
- Design & Simulation Setup
- Analog Leakage Sources
- Power Trace Behavior
- CNN-Based Attack Methodology
- Proposed Countermeasure
- Experimental Results
- Conclusion
- Future Work

Introduction & Motivation

ADC Operation

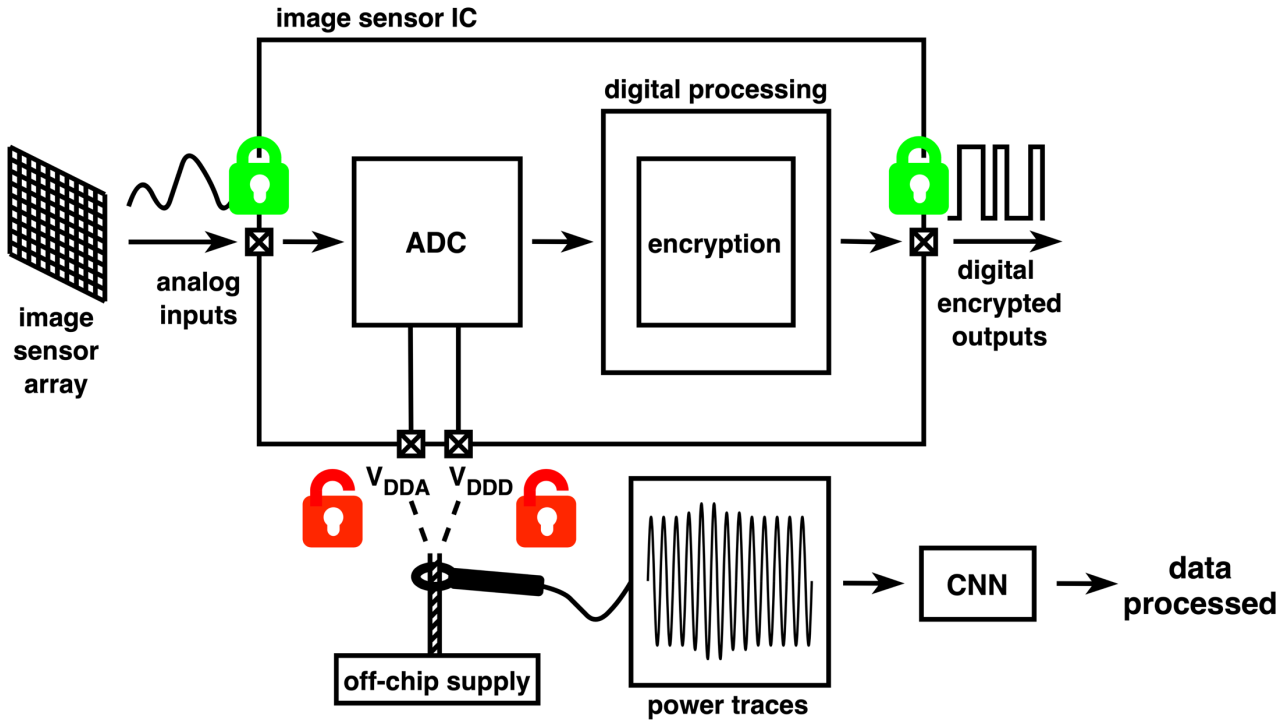


Power Side-Channel Attack Focus in Literature



**Data based on IEEE Xplore literature review.*

Threat Model

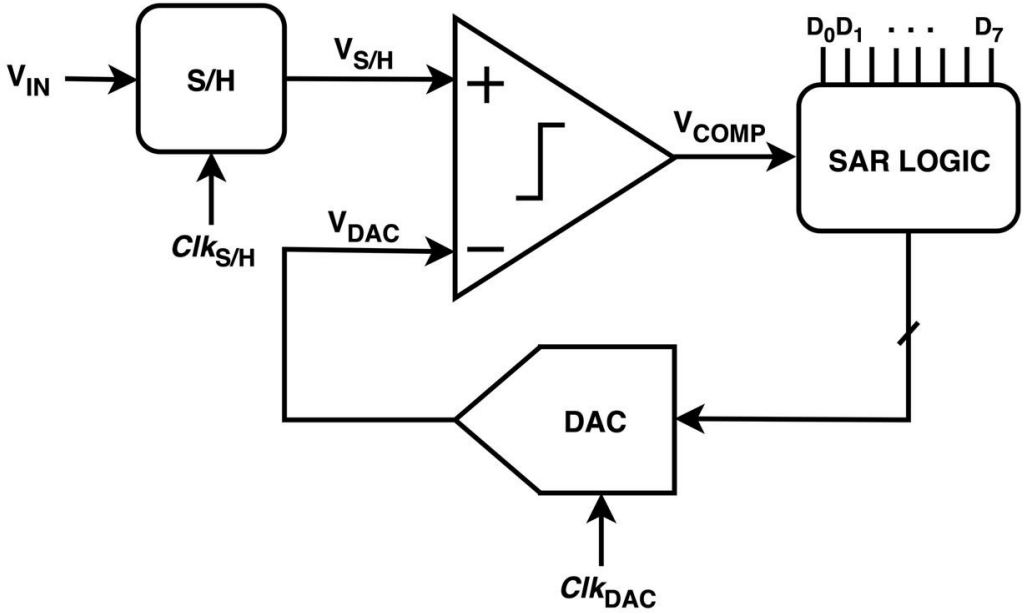


Power side-channel attack for a typical image-sensing application

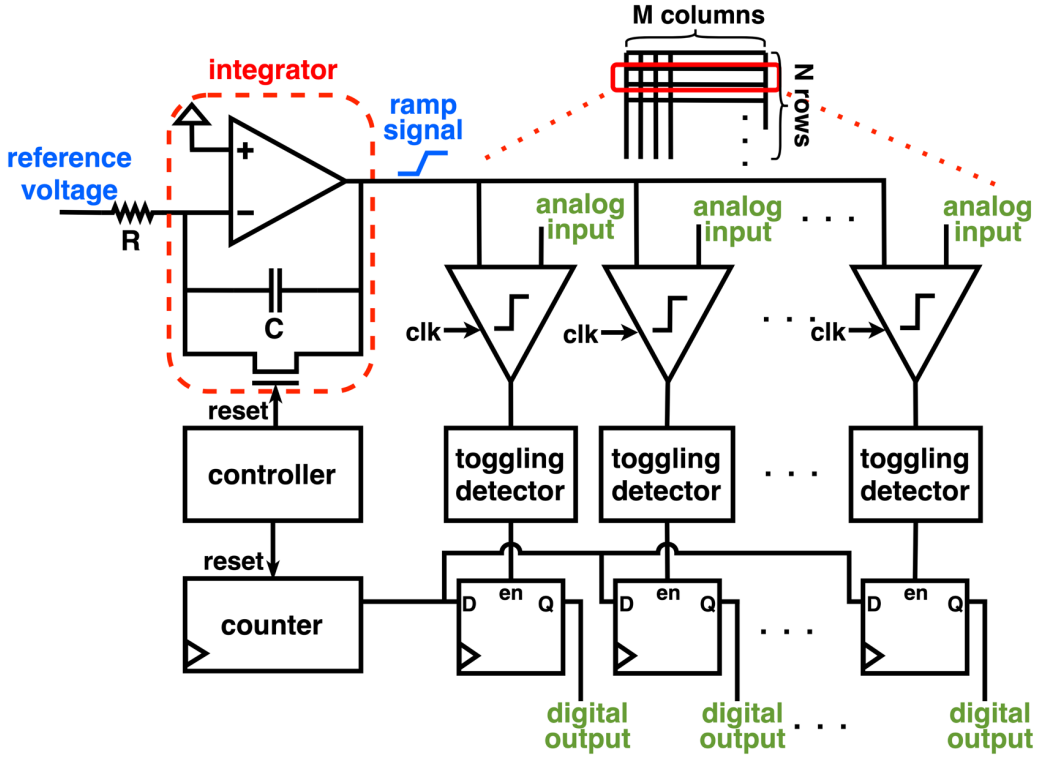
- Even with encrypted I/Os, power lines remain vulnerable.
- External probing of supply current can reveal internal activity.
- Our countermeasure targets leakage from the comparator and preamplifier.

SAR vs SS-ADC in Power Side-Channel Attacks

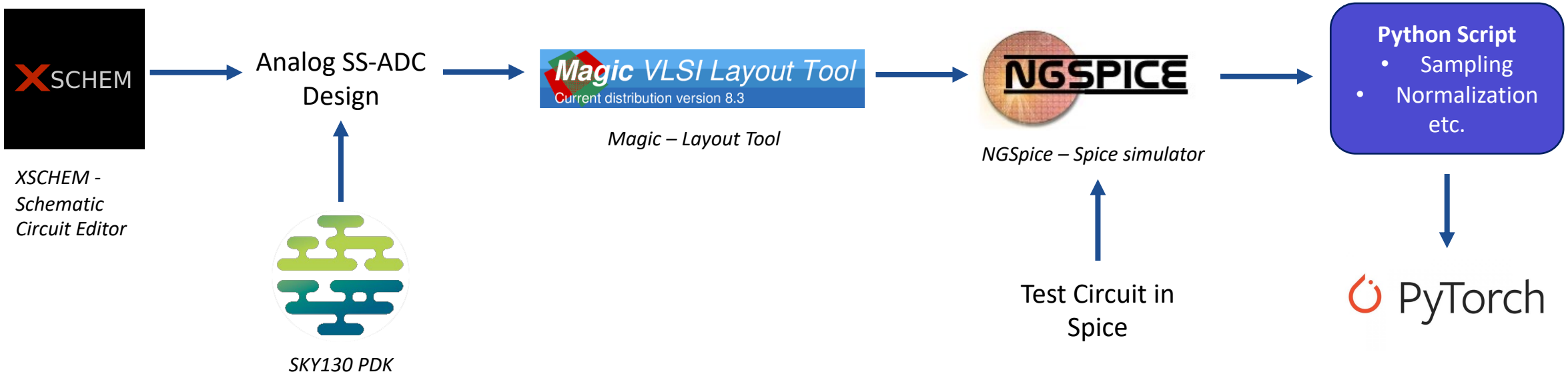
SAR ADC Architecture



Single-Slope ADC Architecture

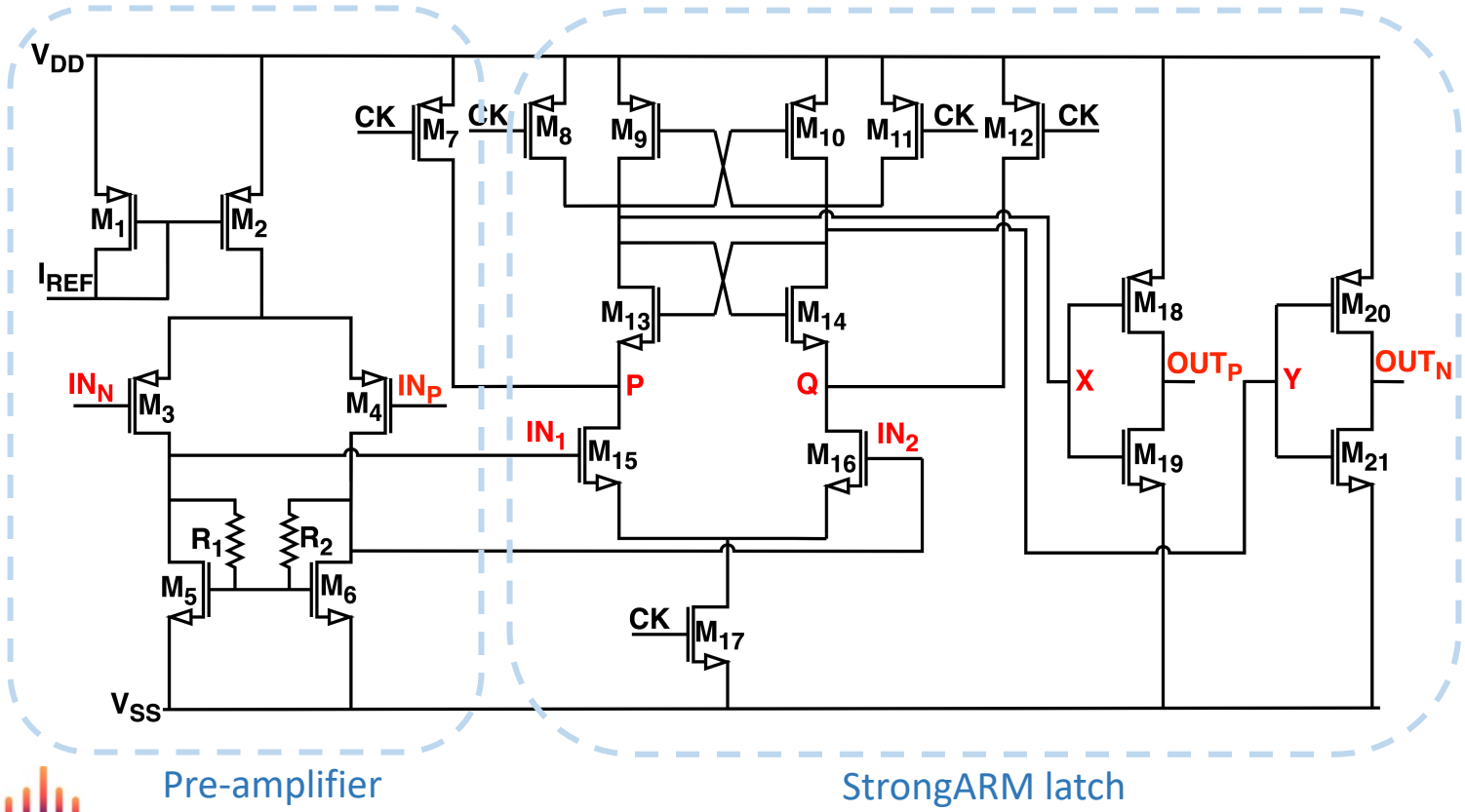


Design & Simulation Setup



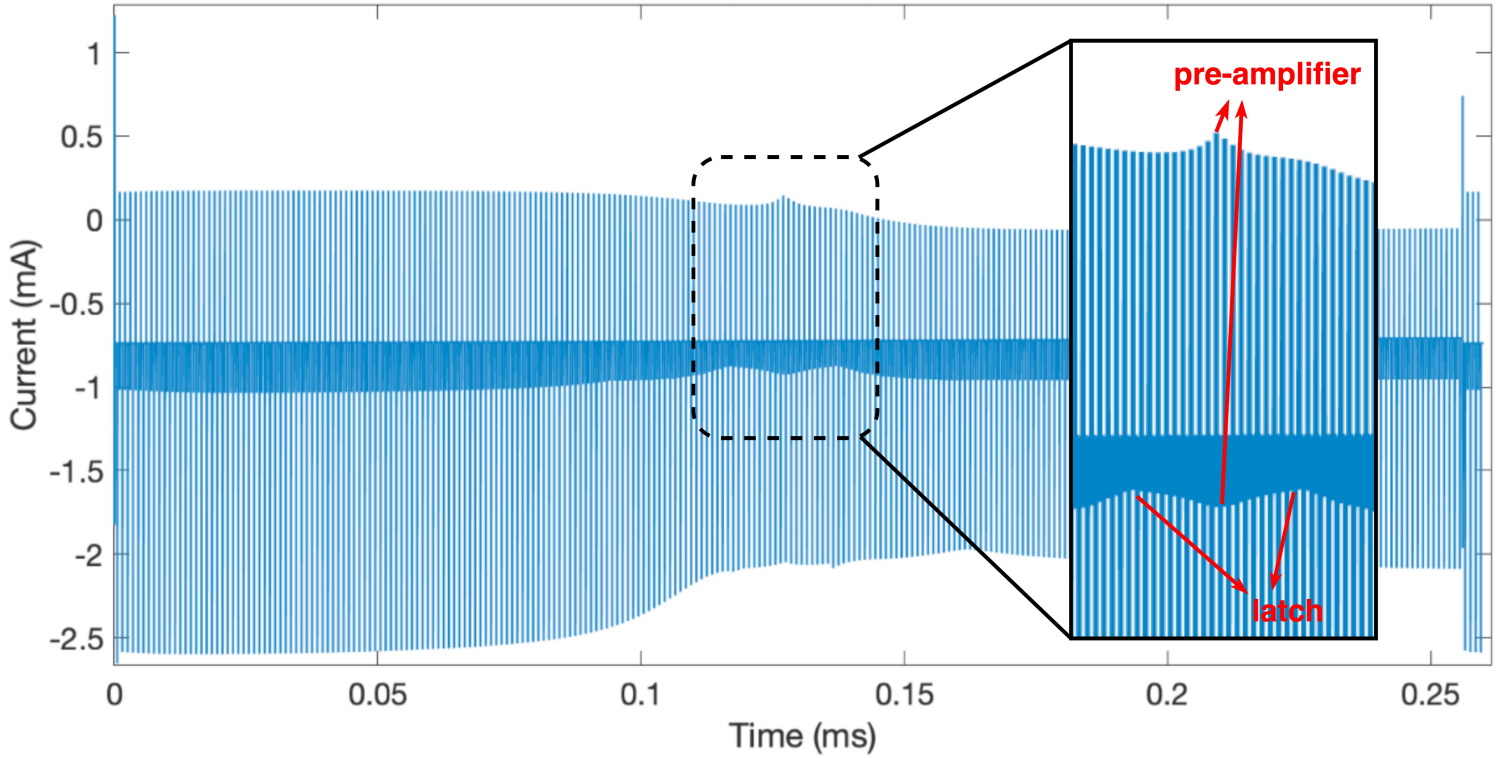
Analog Leakage Sources

Comparator Schematic



- Preamplifier: responds to ramp input & kickback noise
- StrongARM latch: exhibits input-dependent decision delay
- Output buffer: minimal leakage impact

Power Trace Behavior



Analog Block Power Trace – The comparator toggles around 120µs

CNN-Based Attack Methodology

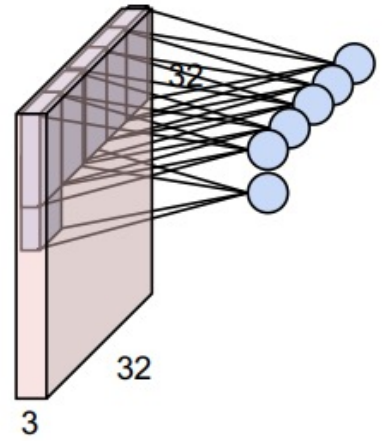
TABLE I - CNN Architecture

	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

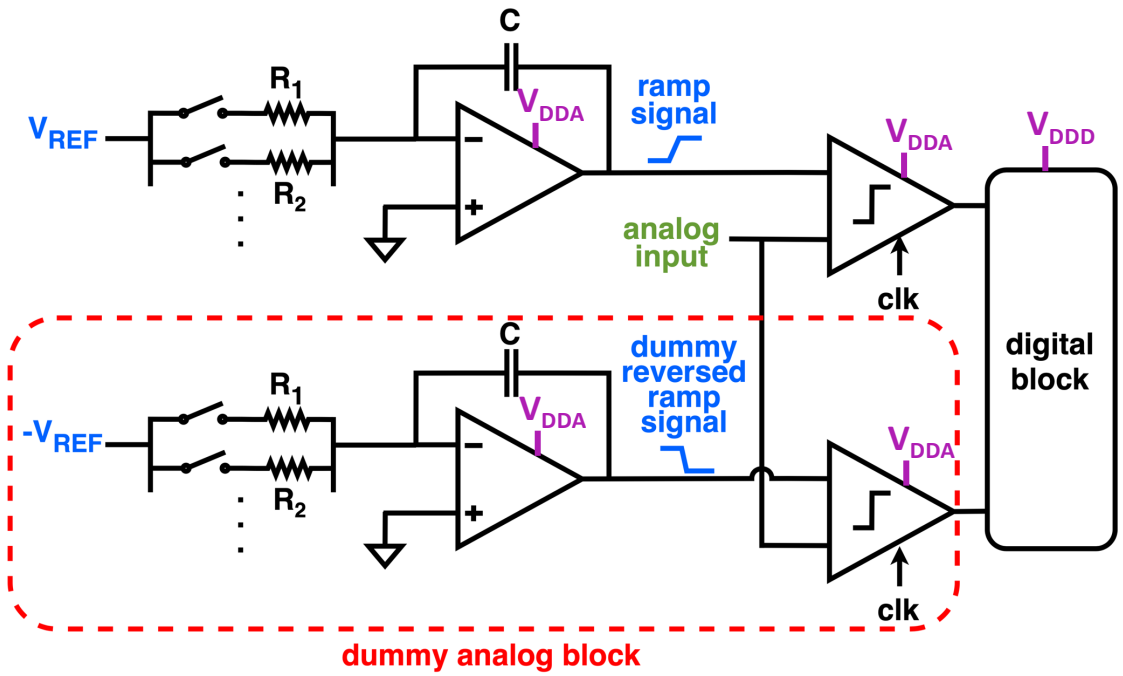
[a]Convolution Parameters are $Size, Channels, Stride$

[b]Pooling Layers are MaxPooling with parameters $Size, Stride$

[c]SX refers to Softmax



Proposed Countermeasure



Block Diagram of Proposed Protected SS ADC

- Dummy analog block adds signal-independent activity
- Ramp slope changes 4× per conversion
- 32 random slope combinations via PRNG

Experimental Results

TABLE II: CNN PSA Performance on Unprotected Analog ADC

Bit	Accuracy			Average Training Time
	Train	Test	Test (PL)	
7	100.%	99.8%	96.7%	15 seconds
6	99.4%	99.2%	77.8%	10 seconds
5	96.8%	96.3%	79.9%	18 seconds
4	99.1%	99.1%	72.3%	17 seconds
3	97.8%	98.1%	64.3%	21 seconds
2	93.1%	93.6%	57.1%	27 seconds
1	93.4%	94.0%	50.5%	28 seconds
0	90.3%	90.1%	54.7%	29 seconds
BW	73.1%	73.5%	4.4%	164 seconds
SE	94.2%	71.2%	1.2%	99 seconds

TABLE III: CNN PSA Performance on Protected Analog ADC

Second values shows accuracy of the CNN trained on unprotected traces.

Bit	Accuracy		
	TT	SF	Post-Layout
7	99.1% (64%)	93.4% (53%)	95.1% (62%)
6	98.0% (53%)	69.1% (60%)	73.7% (62%)
5	93.5% (54%)	58.8% (53%)	57.8% (53%)
4	80.6% (51%)	60.8% (51%)	49.1% (51%)
3	69.4% (51%)	49.8% (50%)	51.2% (52%)
2	64.1% (50%)	51.4% (50%)	50.7% (50%)
1	55.4% (50%)	49.0% (50%)	52.3% (51%)
0	51.9% (49%)	50.8% (50%)	49.7% (55%)
BW	9.4% (0.6%)	1.47% (0.5%)	1.36% (0.7%)
SE	17.1% (0.3%)	0.00% (0.2%)	4.69% (0.0%)

Conclusion

- We systematically analyzed **PSA vulnerabilities in SS ADCs**, focusing on comparator, preamplifier, and ramp-related leakages.
- CNN-based attacks achieved **>90% accuracy on all bits** in unprotected designs.
- We proposed a protection scheme using a dual-ramp generator with randomized slopes and dummy comparators.
- The approach significantly reduces CNN classification accuracy, especially for lower bits.
- Importantly, in the SF corner, the attack accuracy remains close to random, demonstrating **robustness under process variations**.

Future Work

- Refine protection strategies to improve resilience for MSBs.
- Extend PSA analysis to digital control logic in SS ADCs. *(ongoing in a parallel study)*
- Develop unified countermeasures combining analog and digital leakage models.
- Explore area, power, and performance trade-offs.

References

- B. Razavi, "The StrongARM Latch," IEEE Solid-State Circuits Magazine, vol. 7, no. 2, pp. 12–17, 2015. doi:10.1109/MSSC.2015.2418155
- Google / SkyWater Technology Foundry, "SkyWater 130nm PDK," 2020. [Online]. Available: https://skywater-pdk.readthedocs.io/
- C. Wolf et al., "Yosys Open Synthesis Suite," 2013. [Online]. Available: https://yosyshq.net/yosys/
- The NGSpice Project, "NGSpice Circuit Simulator," 2025. [Online]. Available: http://ngspice.sourceforge.net/
- J. Ousterhout, "Magic VLSI Layout Tool," 2025. [Online]. Available: http://opencircuitdesign.com/magic/
- PyTorch Developers, "PyTorch: An Open Source Machine Learning Framework," 2025. [Online]. Available: https://pytorch.org/
- T. Jeong et al., "S2ADC: A 12-bit, 1.25MS/s Secure SAR ADC with Power Side-Channel Attack Resistance," in Proc. IEEE CICC, 2020, pp. 1–4. doi:10.1109/CICC48029.2020.9075919
- L. Fang et al., "LSB-Reused Protection Technique in Secure SAR ADC against Power Side-Channel Attack," in Proc. AsianHOST, 2022, pp. 1–6. doi:10.1109/AsianHOST56390.2022.10022192
- R. Chen et al., "RaM-SAR: A Low Energy and Area Overhead, 11.3 fJ/conv.-step 12b 25MS/s Secure Random-Mapping SAR ADC," in Proc. IEEE VLSI Symposium, 2022, pp. 94–95.
- S. N. Karanth et al., "Randomization Approaches for Secure SAR ADC Design Resilient Against Power Side-Channel Attacks," in Proc. IEEE HOST, 2024, pp. 282–292. doi:10.1109/HOST55342.2024.10545378
- T. Miki et al., "A Random Interrupt Dithering SAR Technique for Secure ADC Against Reference-Charge Side-Channel Attack," IEEE TCAS-II: Express Briefs, vol. 67, no. 1, pp. 14–18, 2020. doi:10.1109/TCSII.2019.2901534