Machine Learning-Based Real-Time Detection of Power Analysis Attacks Using Supply Voltage Comparisons

Nan Wang, Ruichao Liu, Yufeng Shan, Yu Zhu ,Song Chen

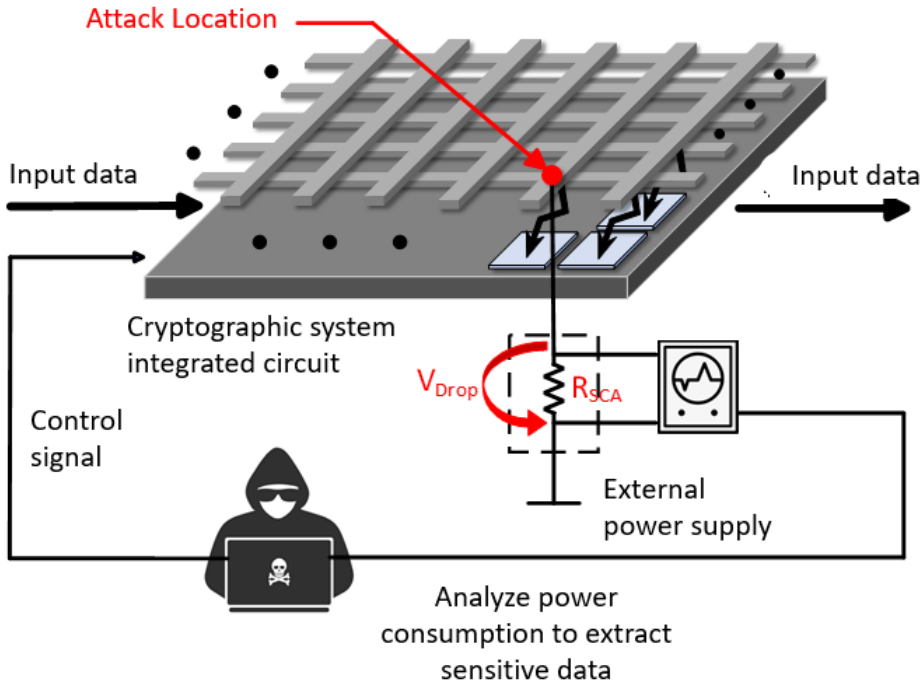
Presenter: RuiChao Liu

2025.1.21

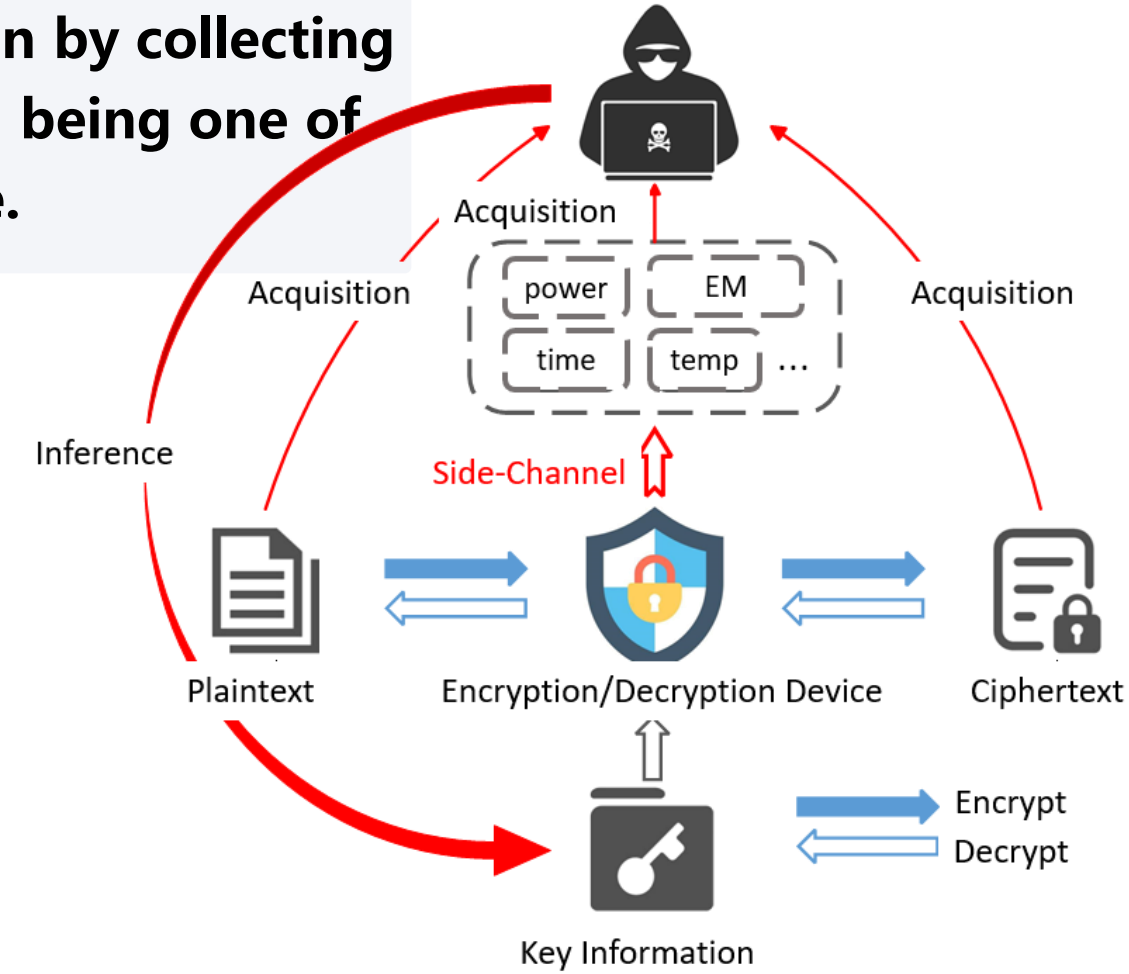
contents

➢ Introduction — PAA

- **Side-channel attacks steal sensitive information by collecting physical data, with power analysis attack(PAA) being one of them, focusing on power supply voltage curve.**



Examples of Power Analysis Attacks

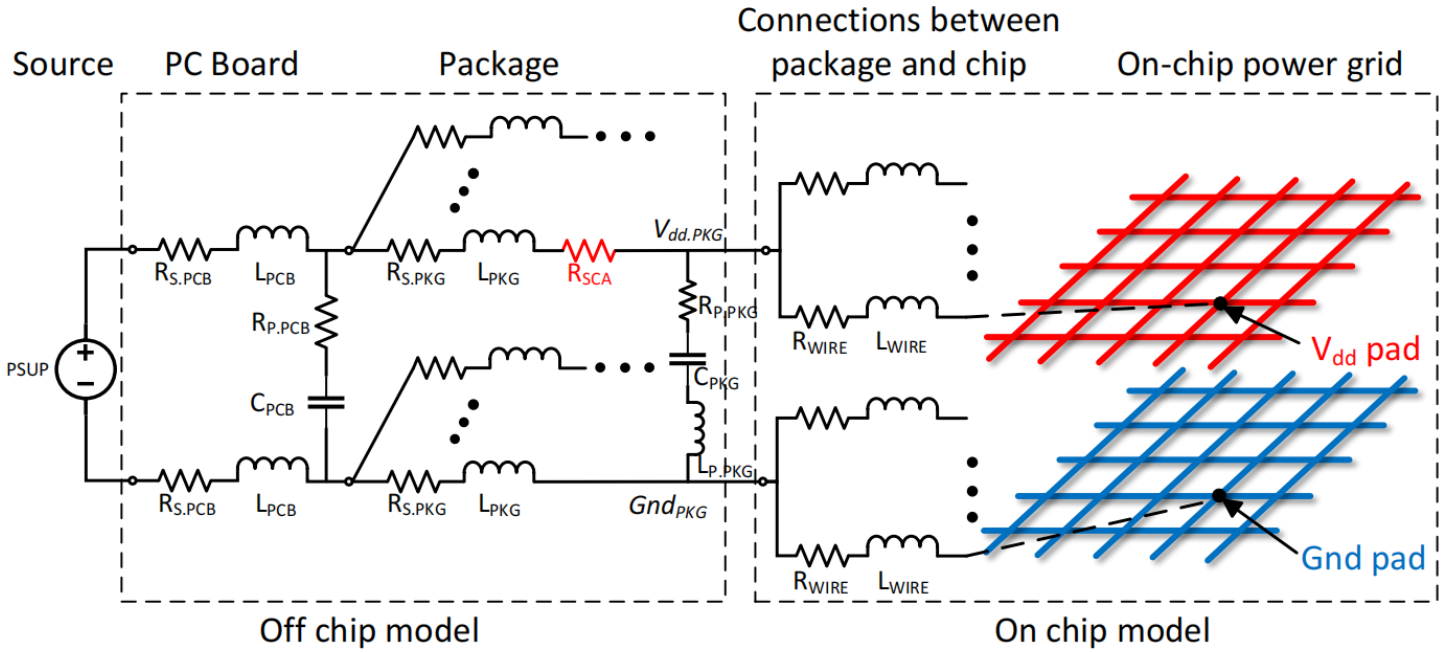


Examples of Side - Channel Attacks

➢ PAA Model

Targeting the pins inside the package responsible for powering the target encryption core, to obtain a favorable power consumption curve for analysis, it is necessary to insert an attack resistor R_{SCA} at the chip package location.

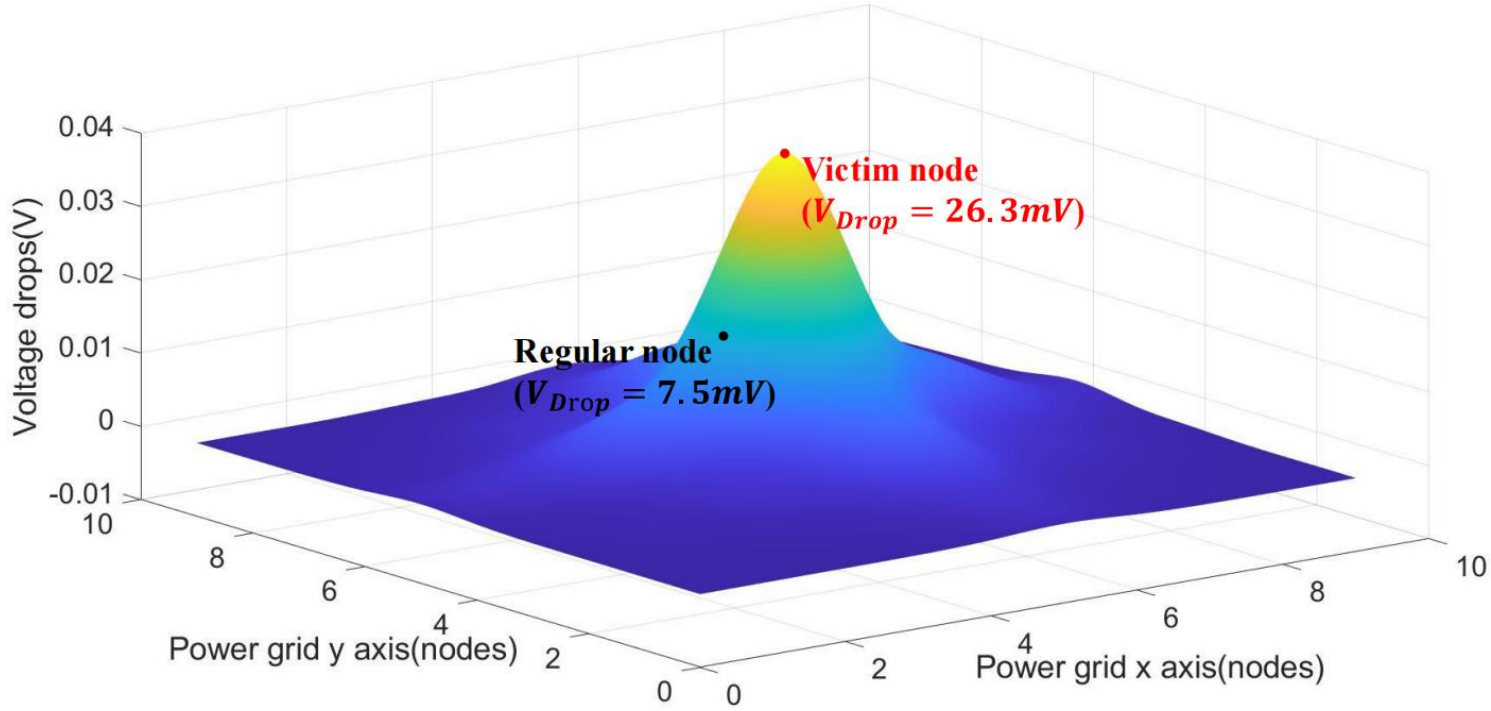
PAA Model



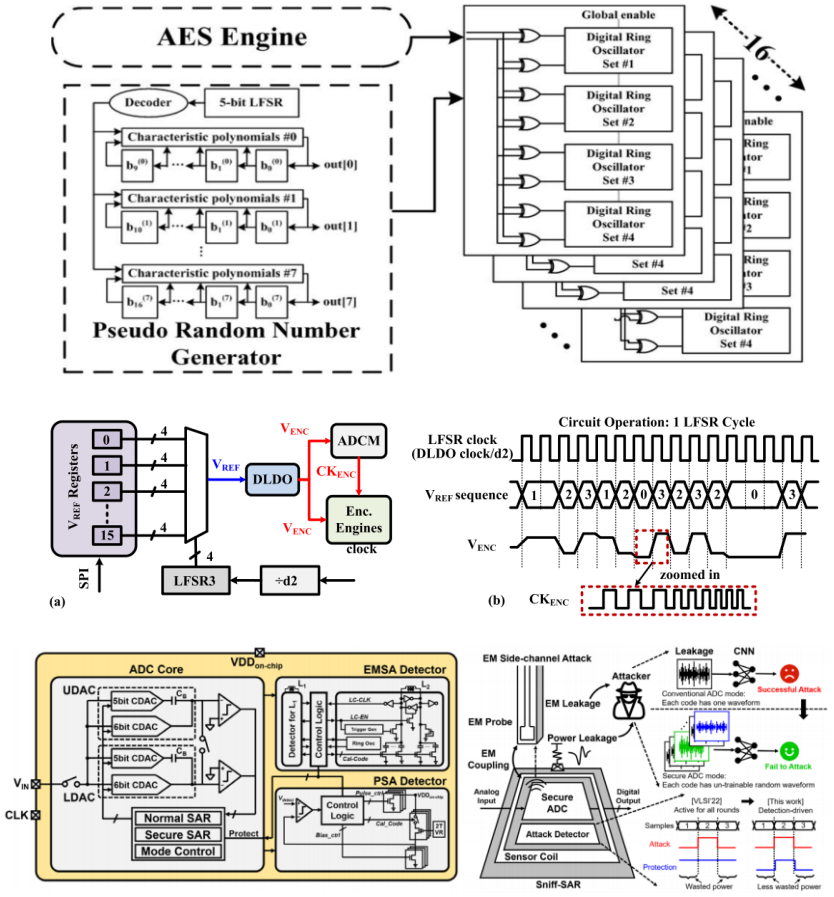
➢ Circuit Response of PAA

The attack resistor R_{SCA} will cause a voltage drop across the nodes on the power grid, resulting in the maximum V_{drop} at the affected node.

Circuit Response



Protection

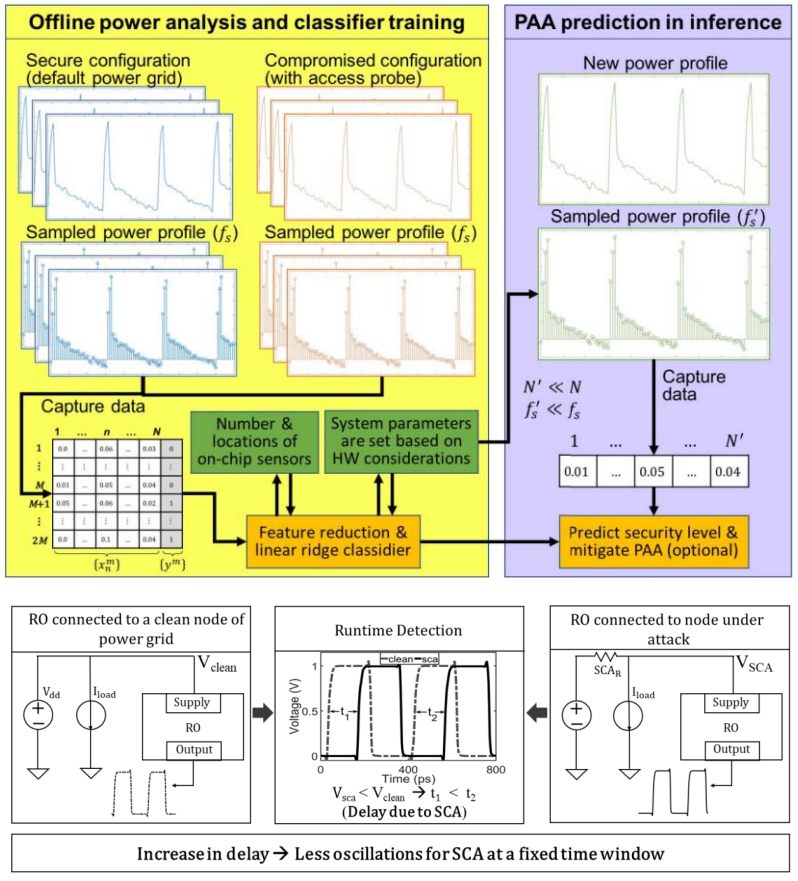


1. Insert **constant current source** and use **low metal layer routing** to mitigate PAA.

2. **Add noise to power curve** to lower data-power correlation via random switching capacitor distribution, confusing time-domain waveforms.

No countermeasures against attacks

Detection



1. Capture power curves, detect intrusions with **real-time linear classifier** analysis.

2. Use **ring oscillators** to identify abnormal voltage changes in the power grid caused by the R_{SCA}.

- Noise resistance capability is **limited**.
- **significant** area and power consumption overhead.

➢ Research Objectives

1. Propose a method with high detection efficiency.
2. Reduce the significant area and power consumption overhead.
3. Enhance the detection capability under high noise levels.

design a PAA detection method.

- ✓ Voltage comparison between nodes.
- ✓ Accumulation of comparison results.

⇨

simulation

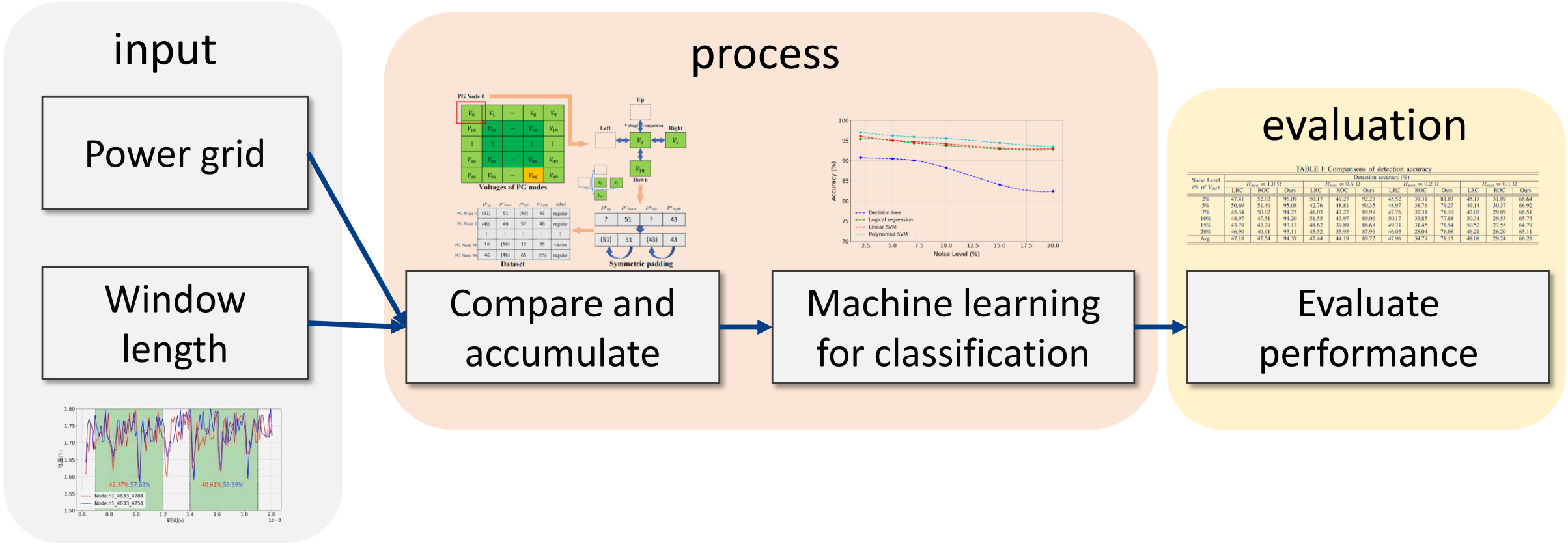
- ✓ Use Xyce for simulation.
- ✓ Use SVM for classification.

⇨

hardware design of our method

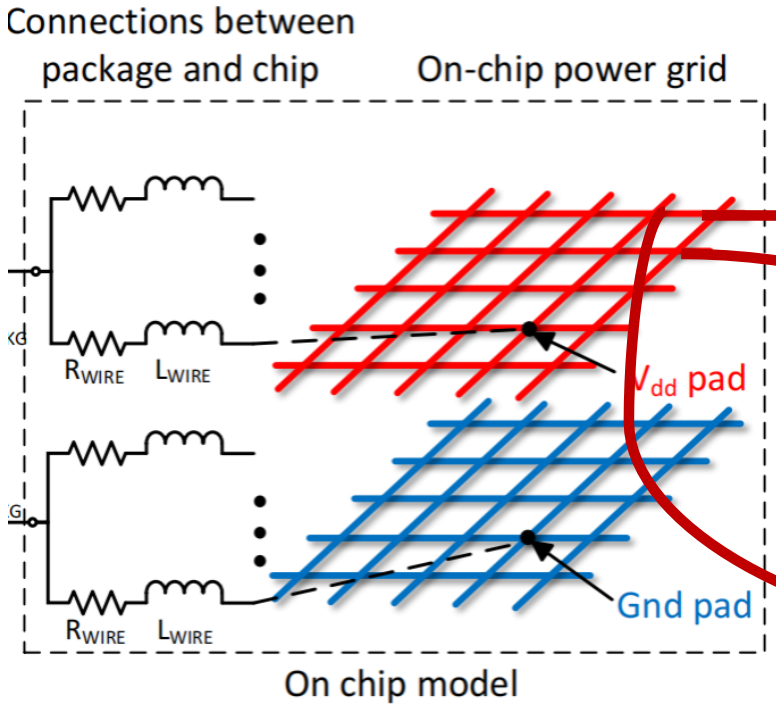
- ✓ Complete modules using Verilog.
- ✓ Use DC synthesis to evaluate resource consumption.

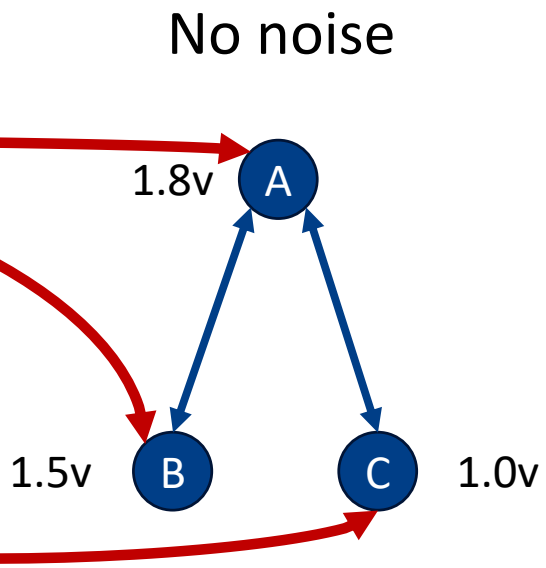
➢ Overall Framework

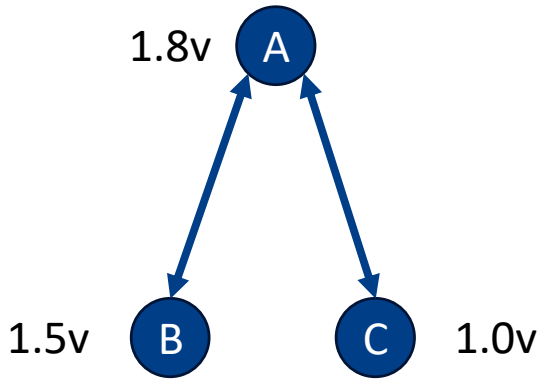


➢ Principle of Detecting Voltage Drop

$$V_{diff} \propto pr(V_i > V_j)$$







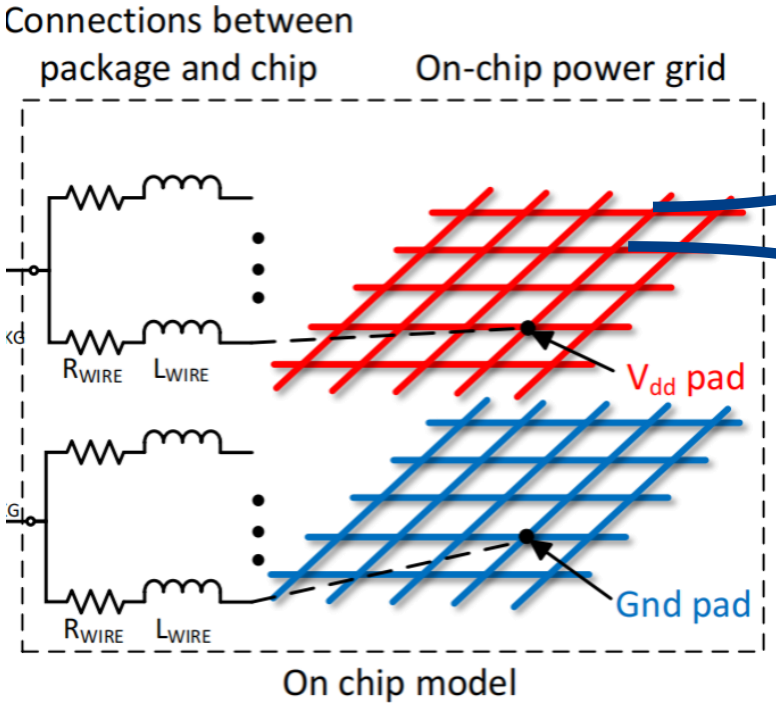
$$pr(V_A > V_B) = pr(V_A > V_C)$$

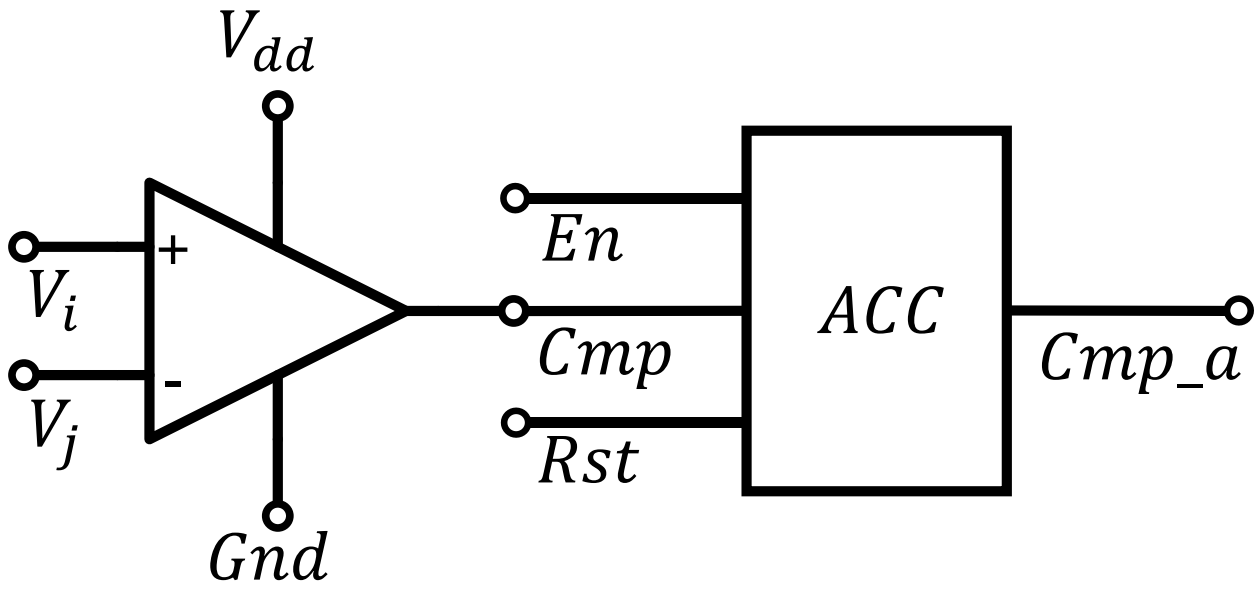
$$pr(V_A > V_B) < pr(V_A > V_C)$$

➢ Estimate Probability

How can $pr(V_i > V_j)$ be estimated? By conducting multiple comparisons and accumulating the results.

Examples of Voltage Comparison and Accumulation

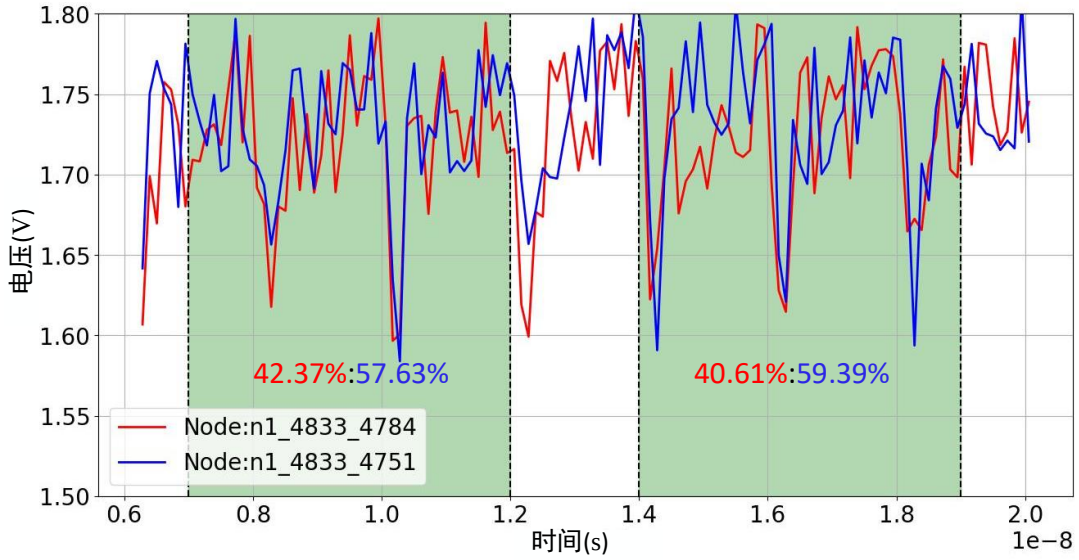




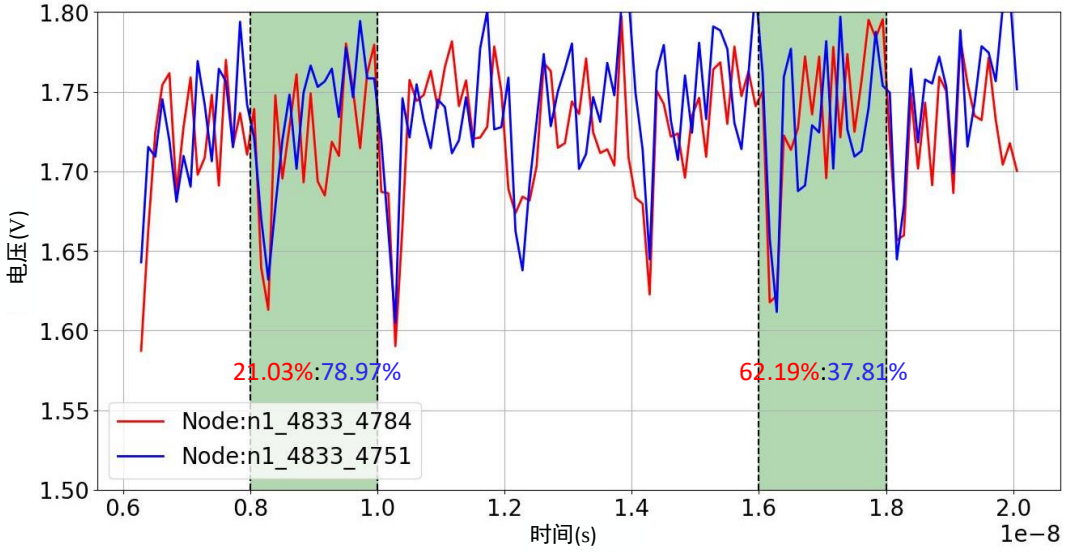
$$Cmp = \begin{cases} 1, & V_i > V_j \\ 0, & V_i < V_j \end{cases}$$

➢ Window Length

For a given node voltage, the difference in $pr(V_i > V_j)$ between any two time windows of equal length does not exceed the probability threshold $pr(V_{dif\_i\_j} > 0)$ determined by the user.



Examples of Suitable Time Window Length



Examples of Excessively Small Time Window Length

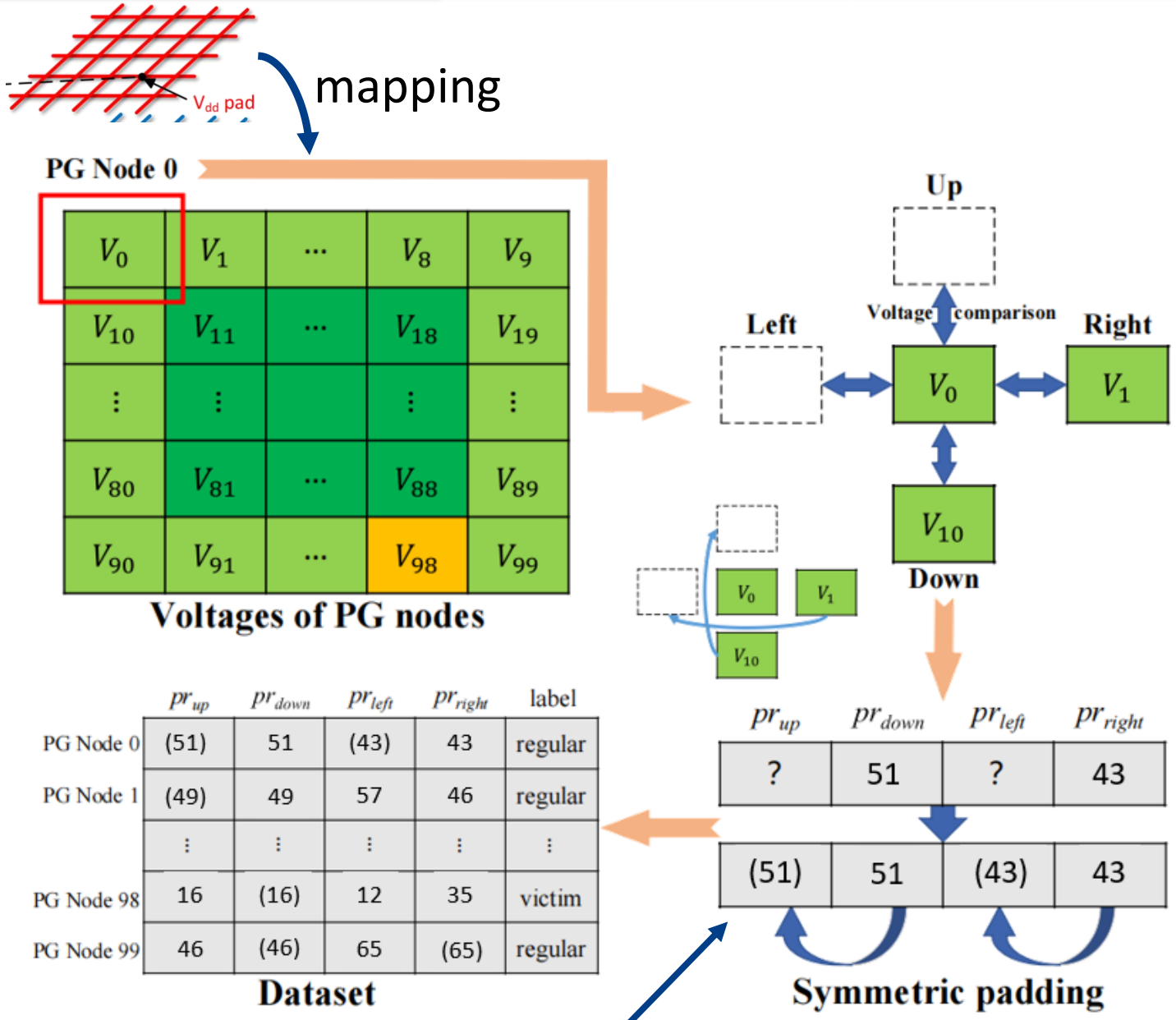
➢ Feature Vector Preparation

For each node:

- Four neighboring nodes: up, down, left and right.
- Four-dimensional feature set

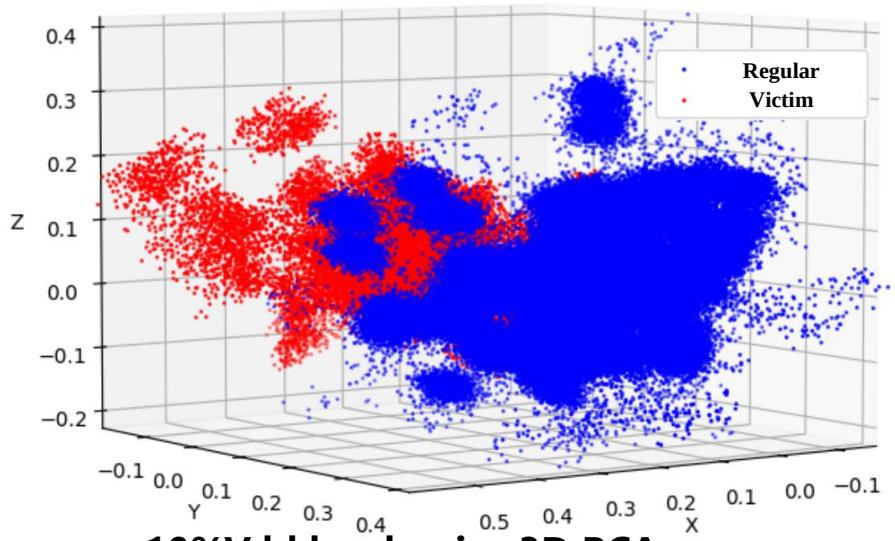
For missing dimension:

- duplicate another dimension to make sure four dimension

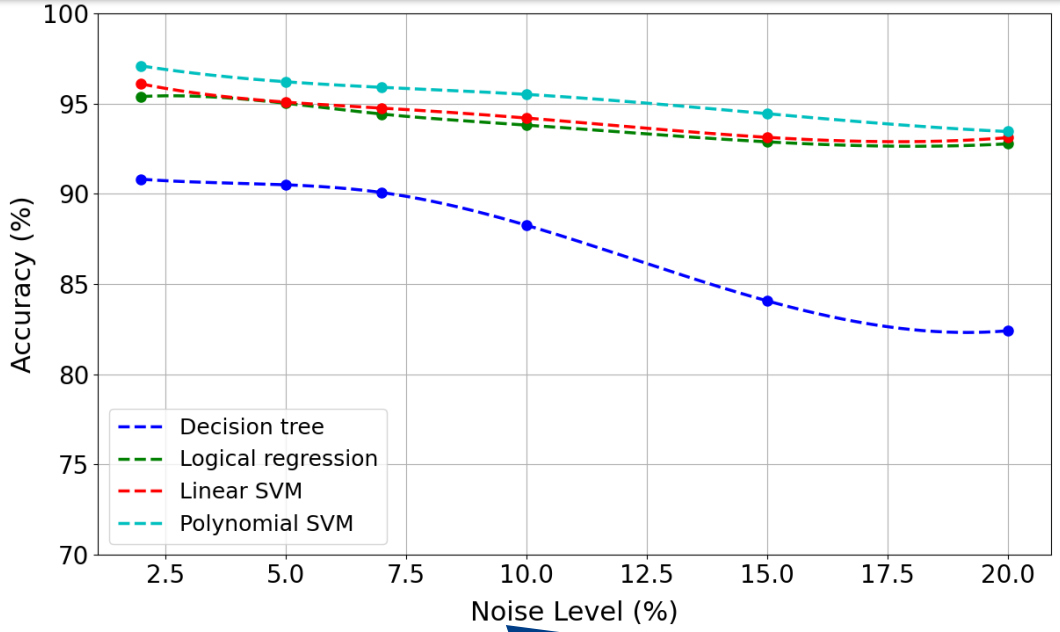


➢ Machine Learning Algorithms

- Simulate intrusions on IBM ibmpg1t benchmark via transient analysis, creating a dataset with 20,000 entries for victim nodes and 23,700 for regular nodes.
- Deciding Linear SVM since its low resource consumption and high performance.



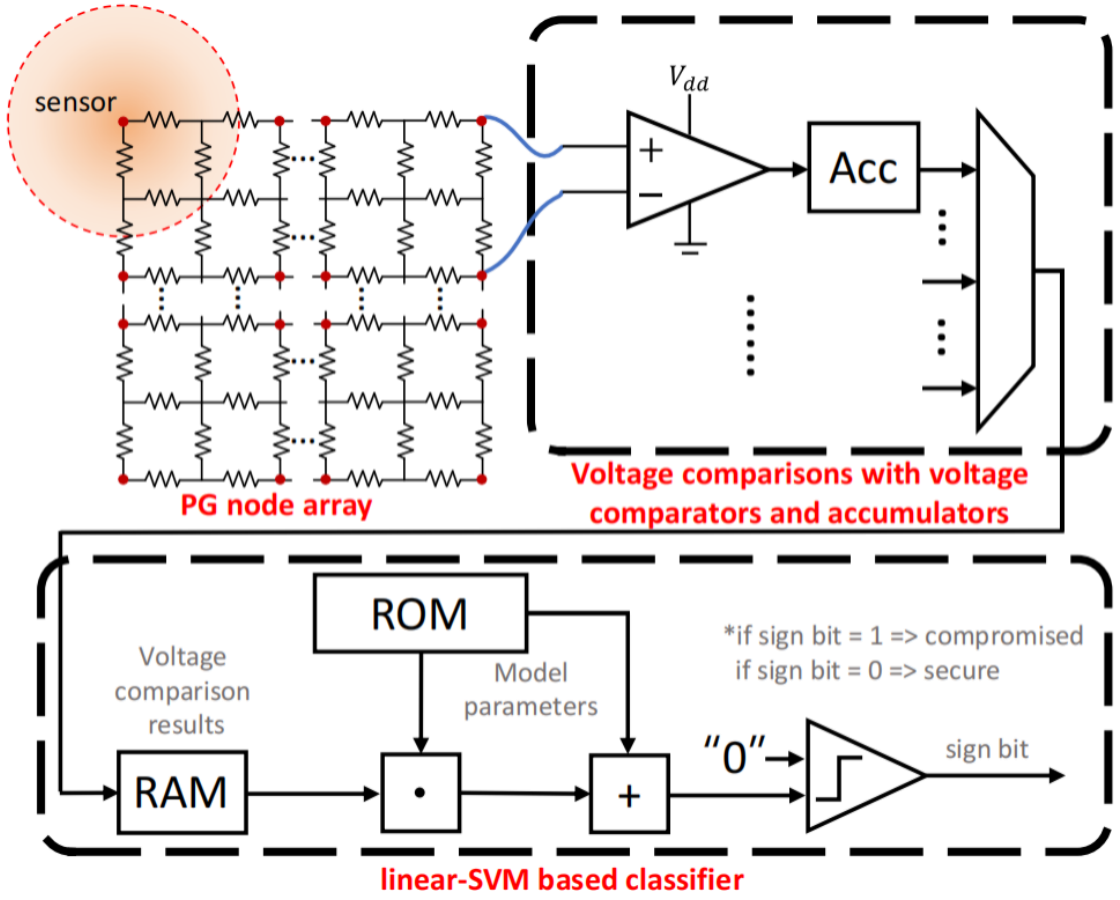
10%Vdd level noise 3D PCA



using different machine learning algorithms to classify data under different noise conditions

*conducting transient analysis simulations by Xyce

➢ Hardware Design



- Comparison results between sensor nodes, obtained via analog voltage comparators and accumulators;
- Results are stored in RAM for classif-ication.
- Model parameters are stored in ROM.
- Model output "0" indicates security; output "1" suggests compromise.

➢ Experimental Results

TABLE I: Comparisons of detection accuracy

Noise Level (% of V_{dd})	Detection accuracy (%)											
	$R_{sca} = 1.0\ \Omega$			$R_{sca} = 0.5\ \Omega$			$R_{sca} = 0.2\ \Omega$			$R_{sca} = 0.1\ \Omega$		
	LRC	ROC	Ours	LRC	ROC	Ours	LRC	ROC	Ours	LRC	ROC	Ours
2%	47.41	52.02	96.09	50.17	49.27	92.27	45.52	39.31	81.03	45.17	31.89	68.64
5%	50.69	51.49	95.08	42.76	48.81	90.35	48.97	38.76	79.27	49.14	30.37	66.92
7%	45.34	50.02	94.75	46.03	47.27	89.99	47.76	37.31	78.10	47.07	29.89	66.51
10%	48.97	47.51	94.20	51.55	43.97	89.06	50.17	33.85	77.88	50.34	29.53	65.73
15%	43.79	43.29	93.13	48.62	39.89	88.68	49.31	31.45	76.54	50.52	27.55	64.79
20%	46.90	40.91	93.11	45.52	35.93	87.96	46.03	28.04	76.08	46.21	26.20	65.11
Avg.	47.18	47.54	94.39	47.44	44.19	89.72	47.96	34.79	78.15	48.08	29.24	66.28

methods	Total area (μm^2)	Total power (mW)
Proposed methods	**69412.32**	**17.2917**
LRC	273247.08	52.3496
ROC	2102.70	0.8465

- High accuracy, Up to 96% accuracy;
- Good anti-noise capacity, 93% accuracy when 20% V_{dd} noise;
- High sensitivity to small R_{sca}, up to 81% accuracy with 0.2 ohm R_{sca}.
- Low resource consumption, 75% in circuit area and 68% in power consumption can be saved

Area consumption

metrics	value (μm^2)
Number of ports	10150
Number of nets	26082
Number of cells	15353
Number of combinational cells	10197
Number of sequential cells	4736
Number of macros/black boxes	0
Number of buf/inv	1751
Number of references	5
Combinational area	27649.079983
Buf/Inv area	1918.800076
Noncombinational area	41568.840114
Macro/Black Box area	0.000000
Net Interconnect area	0.000000
Total cell area	69217.920097
Total area	69217.920097

Power consumption

metrics	value (mW)
Cell Internal Power	0.6312
Net Switching Power	0.1095
Total Dynamic Power	0.7407
Cell Leakage Power	0.0561

In this experiment, standard cells of TSMC 65nm process were used for logic synthesis, with a module clock frequency of 50MHz (i.e., 20ns). Considering the design margin, the synthesis clock period was set to 18ns.

➢ Conclusion

- To address the issue of low detection accuracy when power side-channel information is mixed with circuit noise, a method based on a voltage comparator has been proposed to assess the voltage drop caused by PAA;
- For the problem of low detection accuracy under small resistance value intrusion by PAA, this paper has designed a real-time PAA detection model based on a linear SVM according to the proposed voltage comparison strategy;
- A hardware circuit for an on-chip real-time detection system with low area, power consumption overhead, and high detection efficiency has been designed for the proposed PAA detection method.

THE END