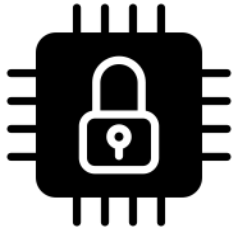
Improving Side-channel Leakage Assessment using Pre-silicon Leakage Models

Dillibabu Shanmugam and Patrick Schaumont

WPI

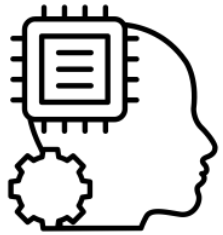
14th International workshop of Constructive Side-Channel Analysis and Secure Design(COSADE)
TUM, Germany, April 3-4, 2023

Introduction



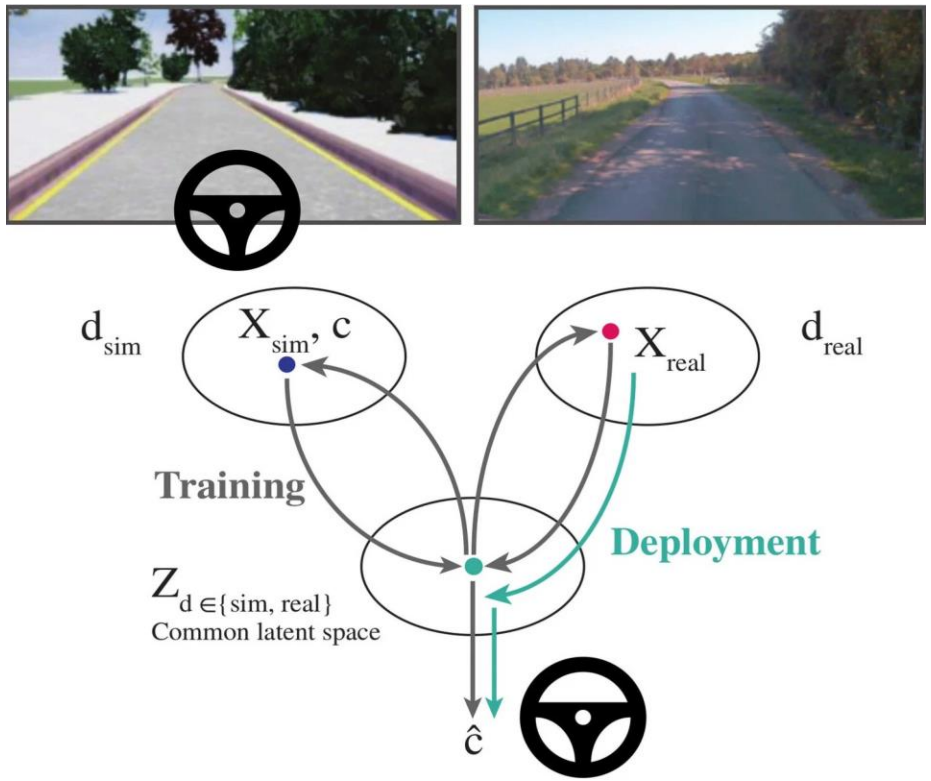
Evaluating power side-channel vulnerability of complex SoC is non-trivial

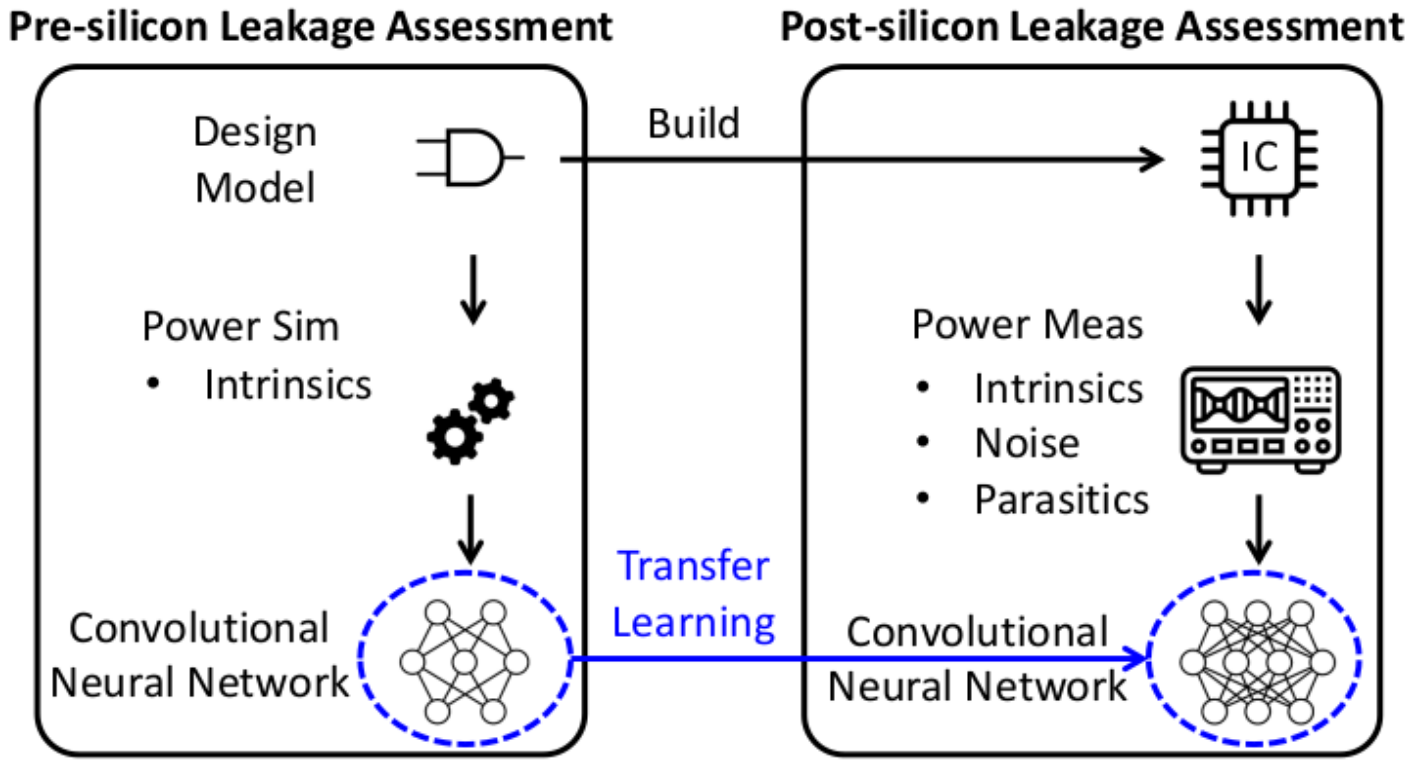
Machine learning techniques improved side-channel leakage assessment lot



How to improve machine learning techniques further

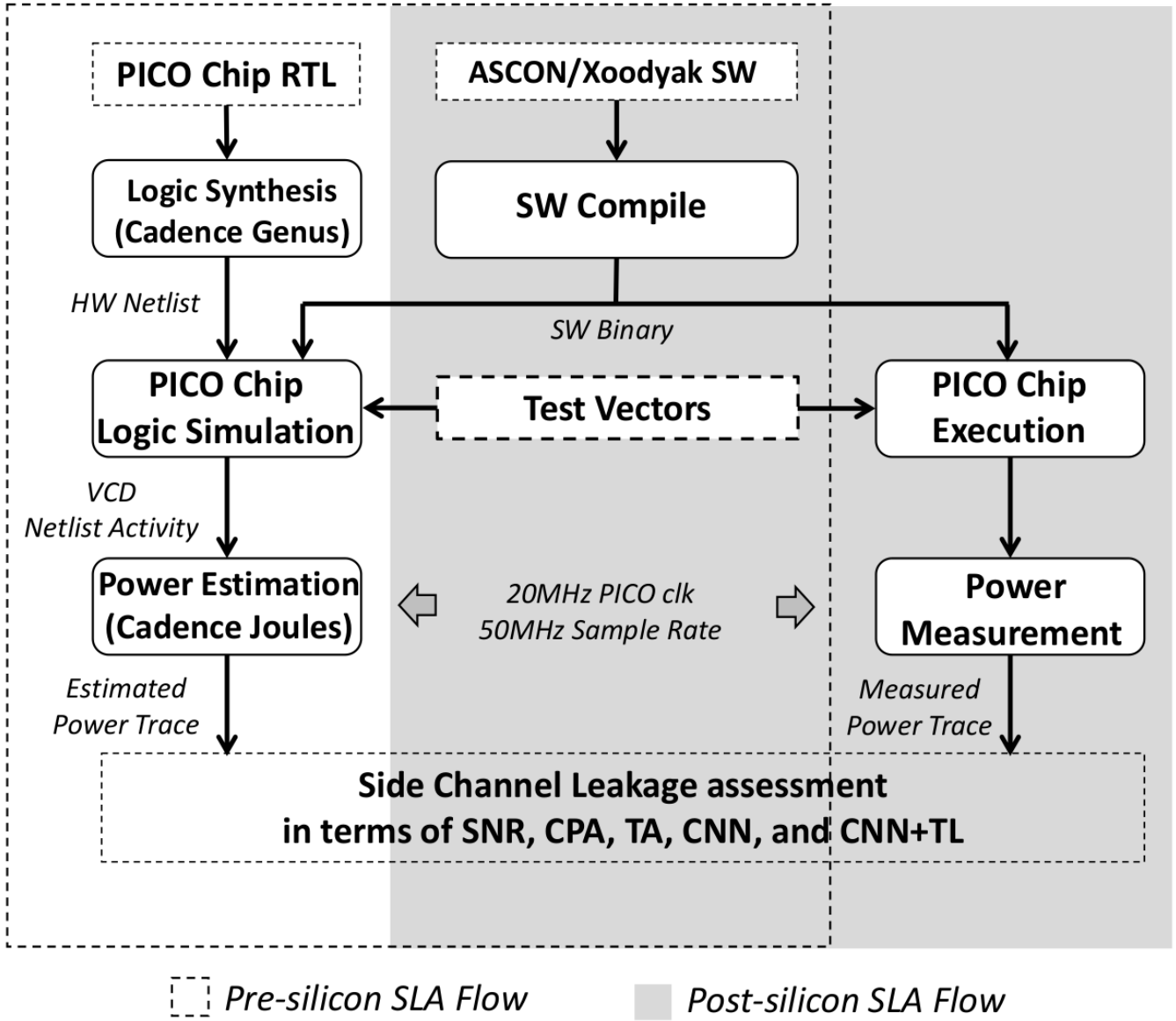
Pre-and post-silicon leakage assessment





Impact: Better threat model for evaluation

Side-channel Leakage Assessment flow (pre- and post-silicon)



Traditional assessment of ASCON

Point of interest : X = (X3 ^ X4) ^ (255 ^ (X0 ^ X4)) & X1)

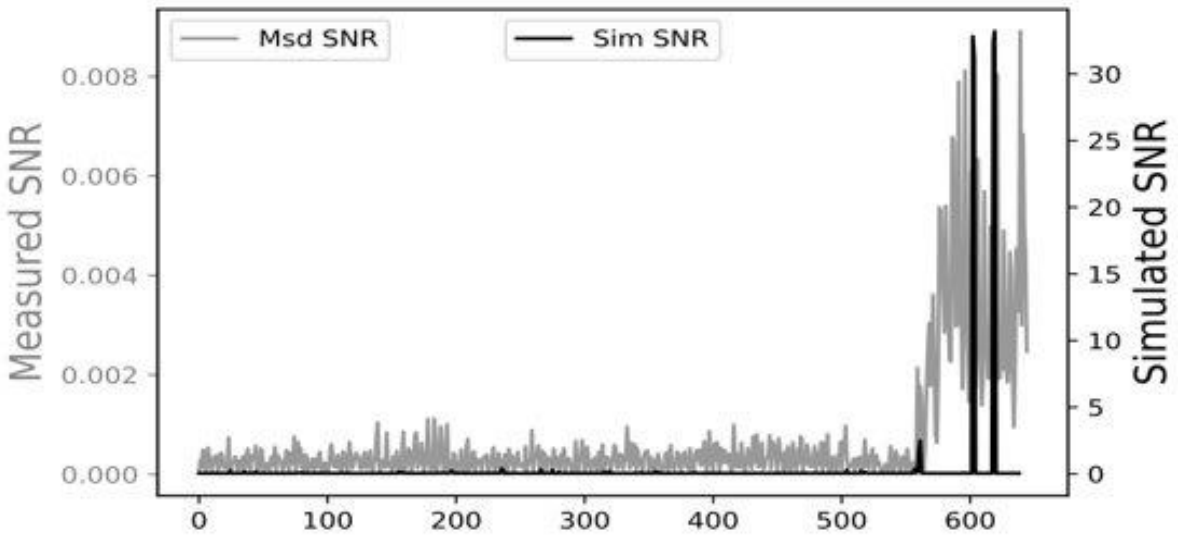
```
1  lui     a5,0x30005
2  addi    a5,a5,8
3  li      a4,1
4  sw      a4,0(a5)          // GPIO trigger up
5  lbu     a4,-52(s0)
6  lbu     a5,-60(s0)
7  xor     a5,a5,a4          // a4 <- X3^X4
8  andi    a4,a5,255
9  lbu     a3,-28(s0)
10 lbu     a5,-52(s0)
11 xor     a5,a5,a3          // a5 <- (X4^X0)
12 andi    a5,a5,255
13 not     a5,a5             // a5 <- (255^(X4^X0))
14 andi    a3,a5,25
15 lbu     a5,-36(s0)
16 and     a5,a5,a3          // a5 <- (255^(X4^X0))&X1
17 andi    a5,a5,255
18 xor     a5,a5,a4          // a5 <- (X3^X4)^(255^(X4^X0))&X1
19 andi    a5,a5,255
20 sb      a5,-52(s0)        // store X4
21 lui     a5,0x3000
22 addi    a5,a5,8
23 sw      zero,0(a5)        //  GPIO trigger down
```

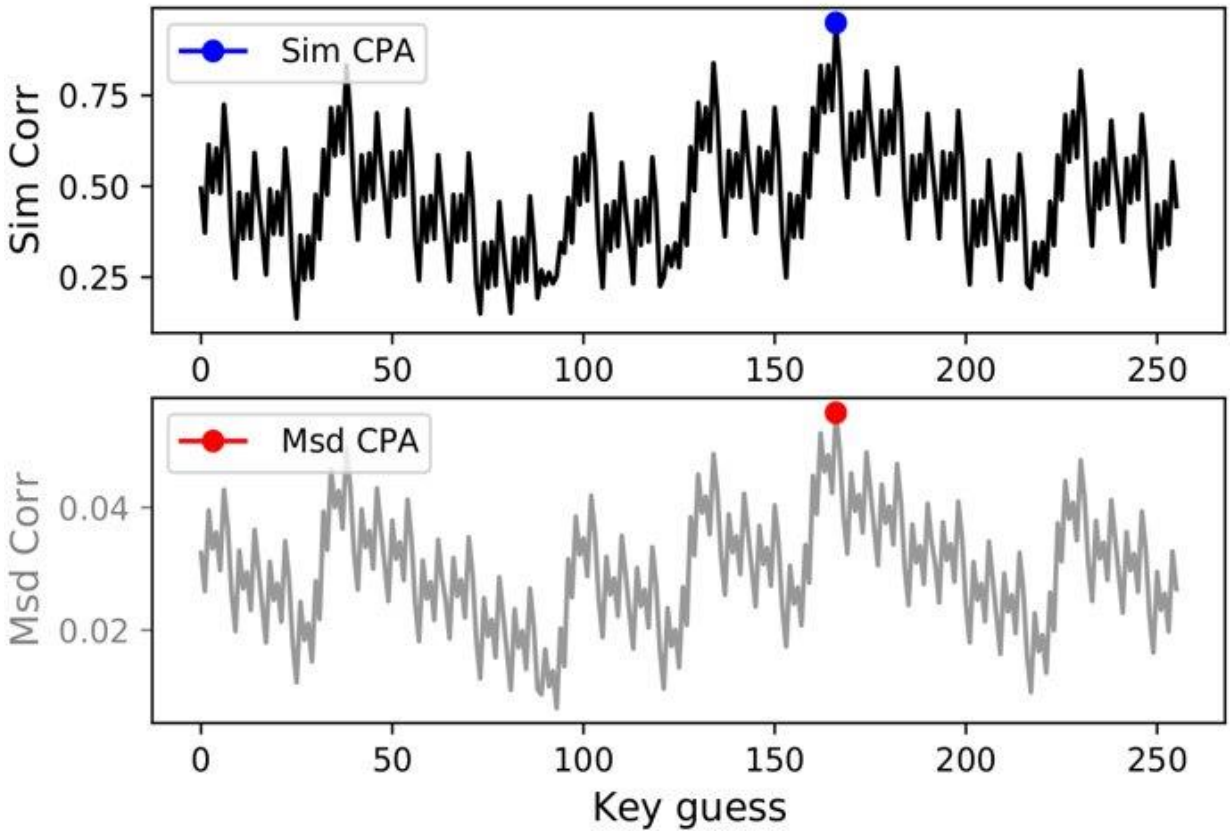
Listing: Ascon S-box assembly code

Related works	Platform	Traces
Samwel et al	Spartan 6	40k
Ramazanpour et al	Artix-7	24k
Our work	**RISCV**	**2k**

Point of interest : Y = (X1 ^ (255 ^ ((X2 ^ X1) & X3))) ^ ((X0 ^ X4) ^ ((255^ X1) & (X2^X1)))

Traditional assessment of ASCON





Both simulation and measured has 640 samples

CPA:

- Simulated : 8 traces
- Measured : 2000 traces

WPI

Convolutional Neural Network(CNN)

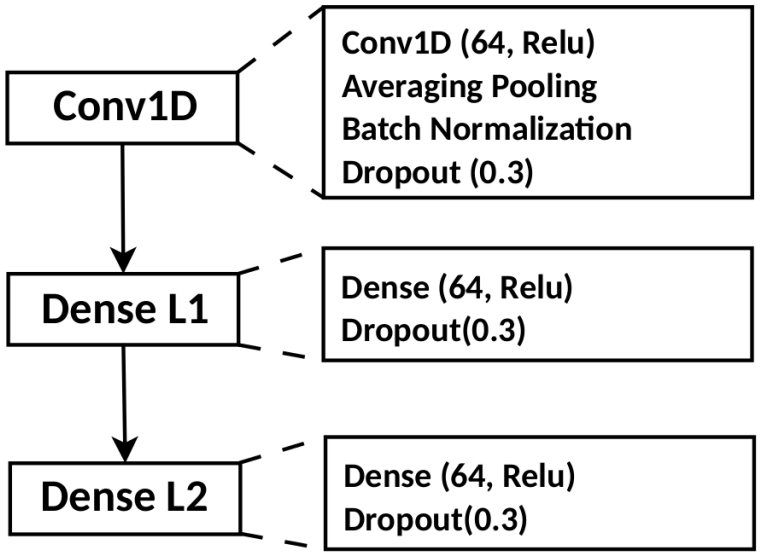


Figure: Network architecture

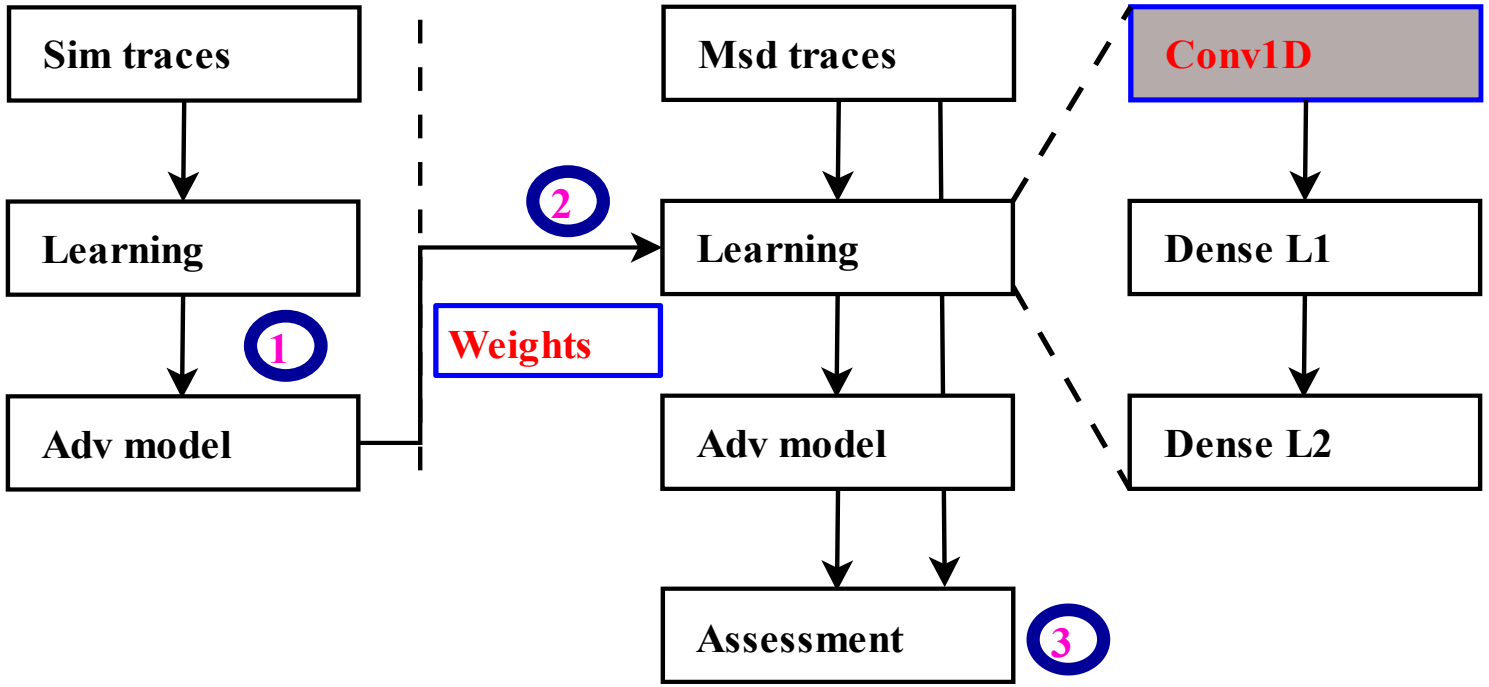
Network architecture and hyperparameters play an important role in a successful adversarial threat model.

64 power samples and intermediate value(label) as input to the network. It extracts features and has 256-class classifier.

Adopted ASCAD[1] network and optimized using random search for the specific target

[1]https://github.com/ANSSI-FR/ASCAD

Transfer learning



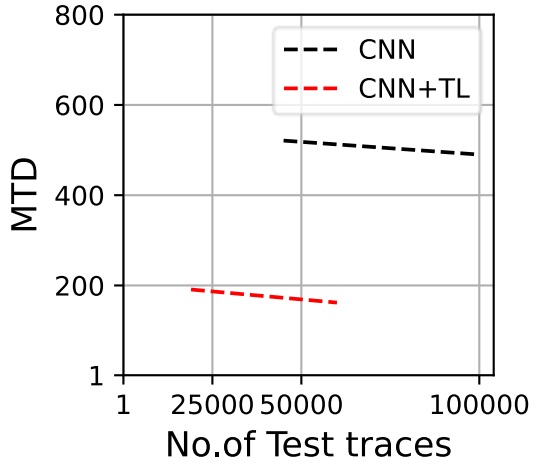
Impact: Reduce learning time and assessment effort

Transfer part of the pre-silicon threat model to the post-silicon threat model.

Pre-silicon traces are noiseless. Therefore, the threat model is more accurate when transferring the model for post-silicon analysis.

Summary of Results : ASCON

SLA of S-box X4	Measured(CNN)		
	Profiling	MTD	Accuracy
Test case_1	45,000	521	80%
Test case_2	100,000	490	82%



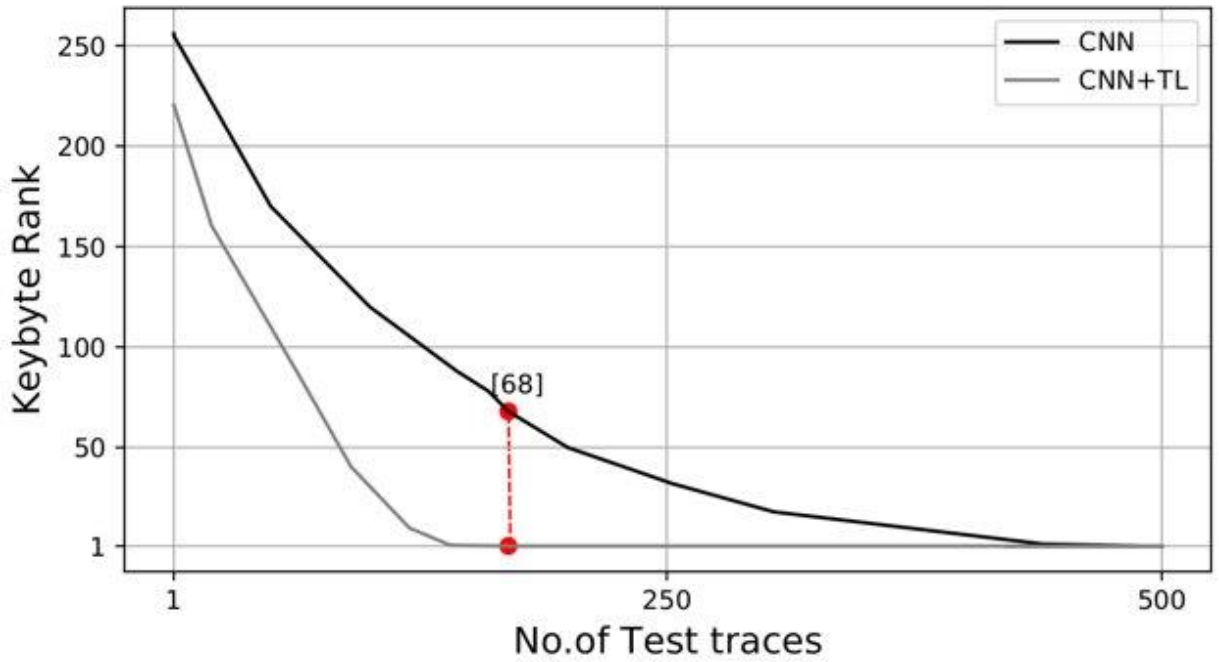
SLA of S-box X4	Simulated			Transfer(CNN+TL)		
	Profiling	MTD	Accuracy	Profiling	MTD	Accuracy
Test case_1	5,000	11	94%	19,000	191	80%
Test case_2	20,000	2	94%	60,000	162	81%

- TL needs fewer traces to access the design. TL requires 1.97 and 2.87 times fewer profile and test traces.

WPI

Accuracy for simulated, transfer, and measured are 94%, 81%, and 82% respectively.

Observation



- TL converges **68 rank faster** compares to measured CNN
- TL models **gain 5 to 7 bits** in guessing entropy

WPI

Summary of Results

Primitive	SLA Flow	CPA (MTD)	Template		CNN	
			Profiling (x 1,000)	MTD	Profiling (x 1,000)	MTD
ASCON	Simulated	8	9	2	9	2
	Measured	2000	90	573	90	500
	Transfer	-	-	-	19	176

WPI

Performance comparison : Assessment complexity

The proposed TL method outperforms all other assessment

Assessment	Relative Assessment Gain on CPA
CPA	1
Template	3.4
CNN	4
TL	11.4

- Ratio of chosen assessment over CPA.
- CNN+TL is less sensitive to distortions from the measurement setup than any other assessment

Assessment	Relative Assessment Loss over Simulation
CPA	250
Template	136
CNN	250
TL	88

- Increase in the number of traces for an assessment from simulated traces to measured traces.
- CNN+TL shows less relative assessment loss

Performance comparison: Time complexity

Primitive	SLA Flow	CPA		Template			CNN		
				# (x 1,000)	LT	AT	#(x 1,000)	LT	AT
ASCON	Simulated	8	<1m	9	10m	5m	9	50m	10m
	Measured	2000	<10m	90	30m	20m	90	6hr	20m
	Transfer	-		-	-		19	60m	15m

Performed all simulation and SLA experiments on Intel Xeon 6248 server.

Difference between simulated and measured trace capturing time:

- To simulate a trace requires 30sec, whereas measurement required 0.15sec. Measurement is 200 times faster

Cost of SLA on the collected traces:

- TL completes the task in 60+50 minutes as opposed to 6 hours by CNN

Conclusion

Transfer learning threat model evaluates the cryptographic design with 2.87 times lesser number of traces compare to CNN

Side channel leakage assessment on Xoodyak also shows similar results

Pre-silicon side-channel leakage assessment is a powerful tool for security validation

References

- Buhan, I., Batina, L., Yarom, Y., Schaumont, P.: SoK: Design Tools for Side-Channel-Aware Implementations. In: Suga, Y., Sakurai, K., Ding, X., Sako, K. (eds.) ASIA CCS '22: ACM Asia Conference on Computer and Communications Security, Nagasaki, Japan, 30 May 2022 - 3 June 2022. pp. 756–770. ACM (2022). https://doi.org/10.1145/3488932.3517415

- Picek, S., Perin, G., Mariot, L., Wu, L., Batina, L.: SoK: Deep Learning-based Physical Side-channel Analysis. IACR Cryptol. ePrint Arch. p. 1092 (2021), https://eprint.iacr.org/2021/1092

- Thapar, D., Alam, M., Mukhopadhyay, D.: Deep Learning assisted Cross-Family Profiled Side-Channel Attacks using Transfer Learning. In: 22nd International Symposium on Quality Electronic Design, ISQED 2021, Santa Clara, CA, USA, April 7-9, 2021. pp. 178–185. IEEE (2021). https://doi.org/10.1109/ISQED51717.2021.9424254

- Das, D., Golder, A., Danial, J., Ghosh, S., Raychowdhury, A., Sen, S.: X-DeepSCA: Cross-Device Deep Learning Side Channel Attack. In: Proceedings of the 56th Annual Design Automation Conference 2019, DAC 2019, Las Vegas, NV, USA, June 02-06, 2019. p. 134. ACM (2019). https://doi.org/10.1145/3316781.3317934

Thank you for your attention

dshanmugam@wpi.edu

Further reading: "Improving Side-channel Leakage Assessment using Pre-silicon Leakage Models,"
D. Shanmugam, P. Schaumont, 14th International Workshop on Constructive Side-channel Analysis and Secure Design (COSADE 2023), Munich, Germany, April 2023.