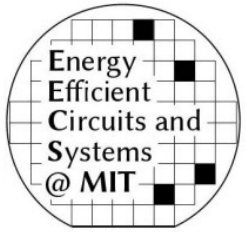
Attacking & Defending Embedded Neural Network Implementations against Power Side-Channel Attacks

Saurav Maji
Advisor: Prof. Anantha P. Chandrakasan



Self Introduction

- B.Tech. in Electronics & Electrical Communication Engineering, IIT Kharagpur, India (2017)
- S.M. in Electrical Engineering & Computer Science, MIT, 2019
- Currently working towards Ph.D. in MIT under Prof. Anantha P. Chandrakasan
- Interests: Hardware Security, Machine Learning Hardware, Biomedical Systems

Overview

- Motivation: Side-channel Security Concerns for Embedded Neural Network implementations.
- Hardware Defenses.
- Evaluation Results and Comparison.

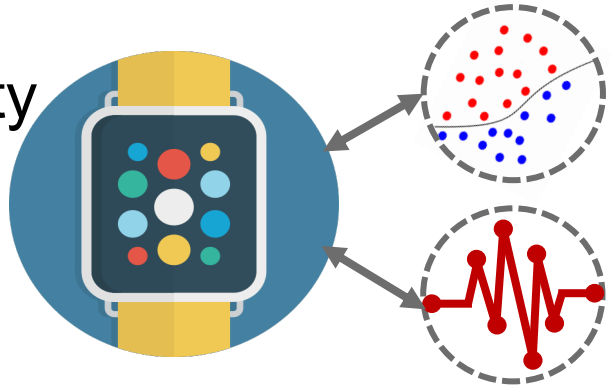
Security Concerns in Machine Learning

Embedded Machine Learning:

- Sensors collect private data and locally process them using ML models
- Data used for both training and diagnosis
- Fitness trackers, Health monitors, …

Security Concerns in Embedded ML:

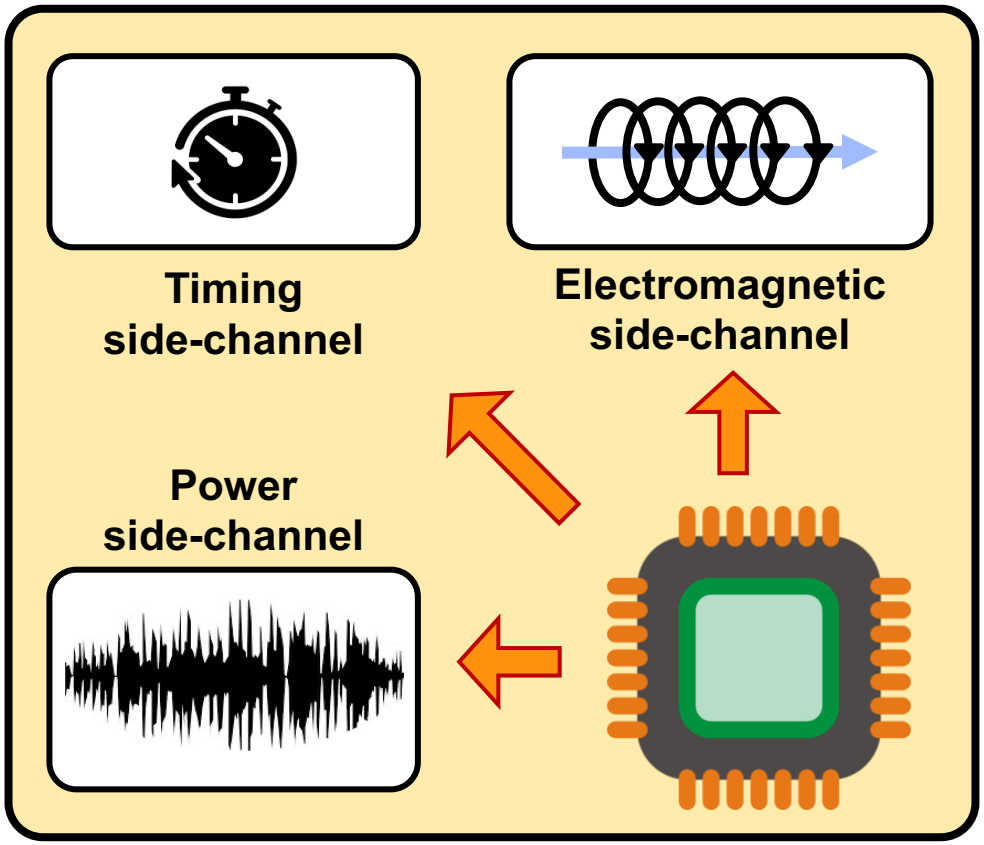
- ML models can be intellectual property
- Models leak training data
- Easier adversarial attacks
- Privacy concerns for user data



Opportunities:

- **New notions of security in embedded ML**
- **Need for <u>Secure Implementation by Design</u> !**

Side-Channel Attacks (SCA)



- **Information leakage through:**
  - Timing
  - Power consumption
  - EM emanations
- **Traditionally used to attack cryptographic algorithms.**
- **Side channels leak critical information in embedded ML**

Objectives:

- **Evaluation of side-channel leakages from embedded NN / ML implementations**
- **Side-channel countermeasures**

SCA on Embedded Neural Networks

Attacking Embedded Neural Networks:

- Exploits the timing and coarse-grained power information.
- Applicable to different precision networks: floating-point, fixed-point, binary networks.
- Platforms: AT328P, Cortex-M0+, RISC-V.

Defending Embedded Neural Networks:

- Purely software-based countermeasures have power and performance overheads due to architectural limitations
- Motivates the need for side-channel resistant hardware for optimal solutions

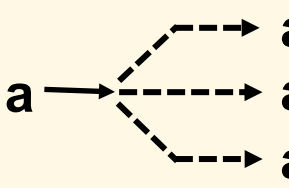
Reference: S. Maji, U. Banerjee and A. P. Chandrakasan, "Leaky Nets: Recovering Embedded Neural Network Models and Inputs Through Simple Power and Timing Side-Channels—Attacks and Defenses," in *IEEE Internet of Things Journal*, 2021.

Overview

- Motivation: Side-channel Security Concerns for Embedded Neural Network implementations.
- Hardware Defenses.
- Evaluation Results and Comparison.

Defense Methodology: Threshold Implementation-based Design

Boolean Masking: The data to be protected is split into random shares mask.

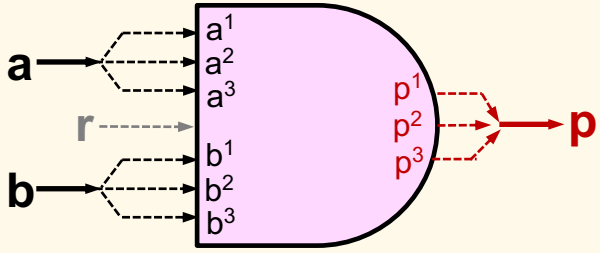


$a = a^1 \oplus a^2 \oplus a^3$

a^1, a^2 and a^3 are the 3 shares of **a**.

Threshold Implementation (TI): A Boolean-masking based Computation scheme.

- ❑ Provides provable against side-channel attacks.
- ❑ Operates over Boolean-shared inputs and generates Boolean-shared outputs.



$a = a^1 \oplus a^2 \oplus a^3$

$b = b^1 \oplus b^2 \oplus b^3$

$p = p^1 \oplus p^2 \oplus p^3$

$= (a \,\&\, b)$

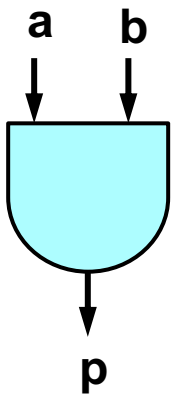
Threshold-based AND Computation

Reference: S. Nikova et. al, "Threshold Implementations Against Side-Channel Attacks and Glitches," *Information and Communications Security (ICICS)*, 2006.

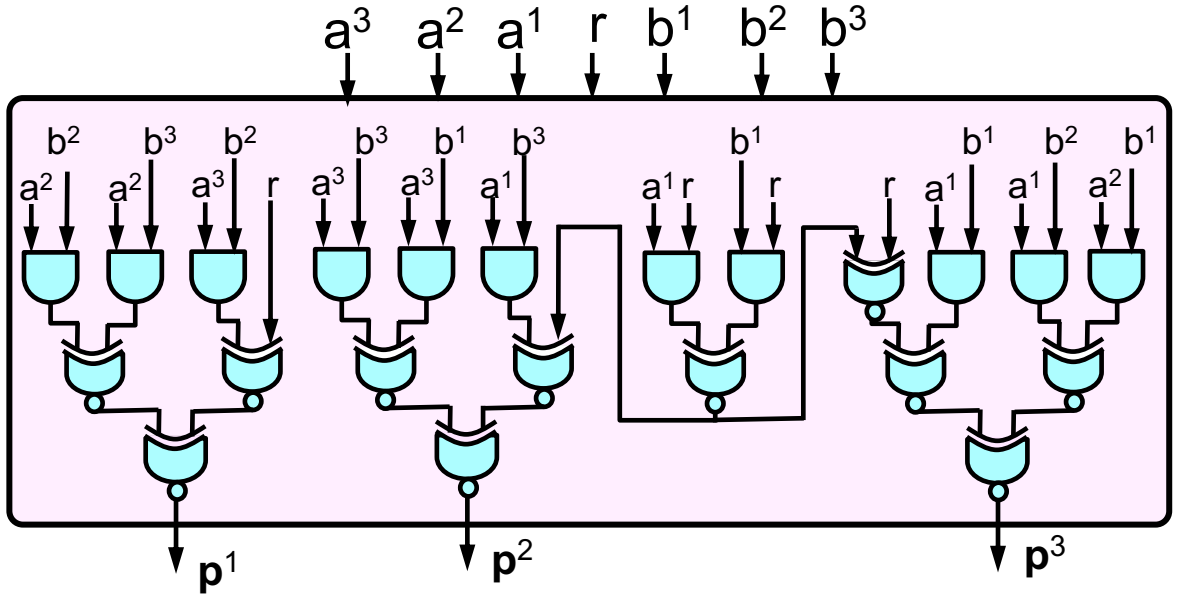
Threshold Implementation: Challenges

Energy Efficient Circuits and Systems @ MIT

Conventional AND



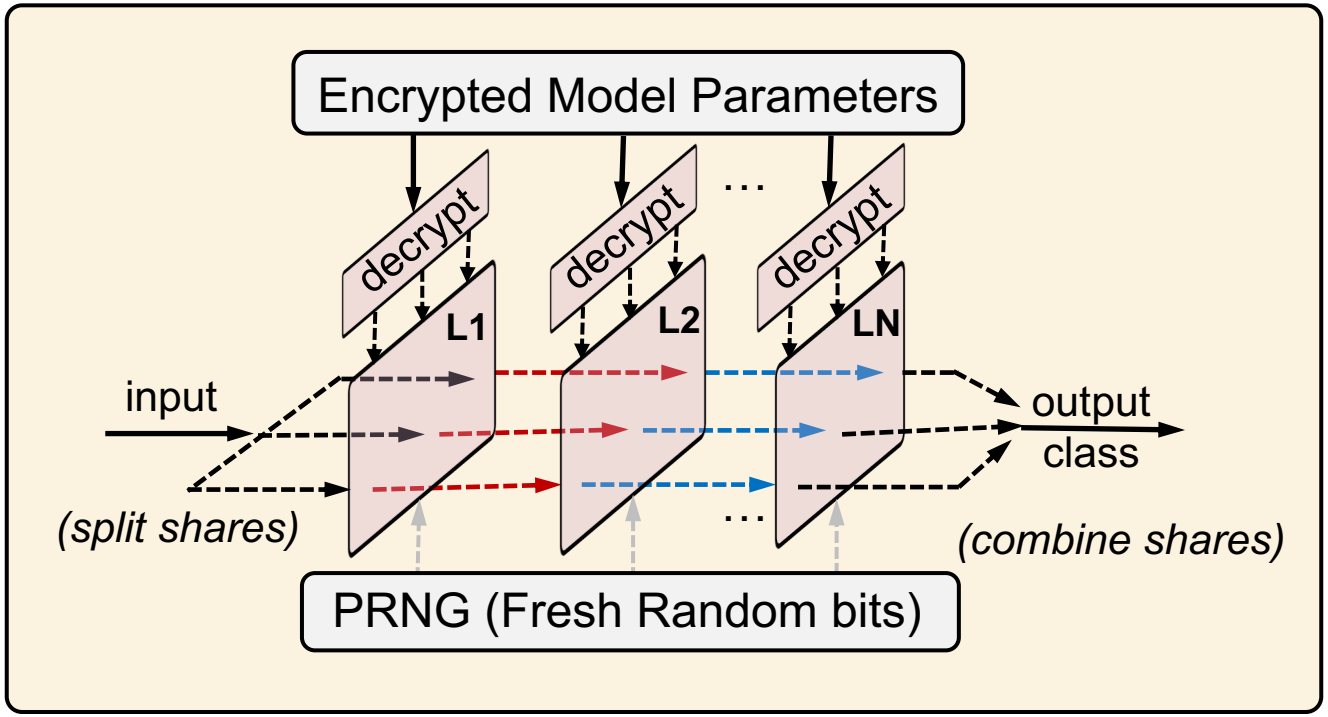
TI-based AND design using traditional gates



Challenges:

- ❑ Huge area & energy overheads.
- ❑ Huge increase in cycle latency.
- ❑ Requirement of fresh random bits.

Side-Channel Secure Neural Network Accelerator Design



Salient Features:

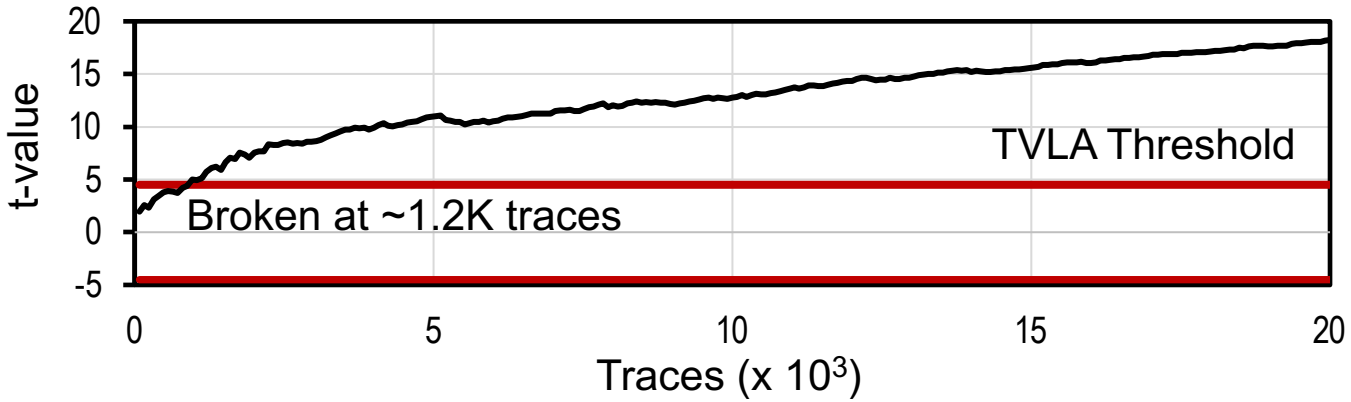
1. Side-channel secure model decryption unit.
2. TI-based Neural Network operation for protecting both the model parameters and the inputs.

Overview

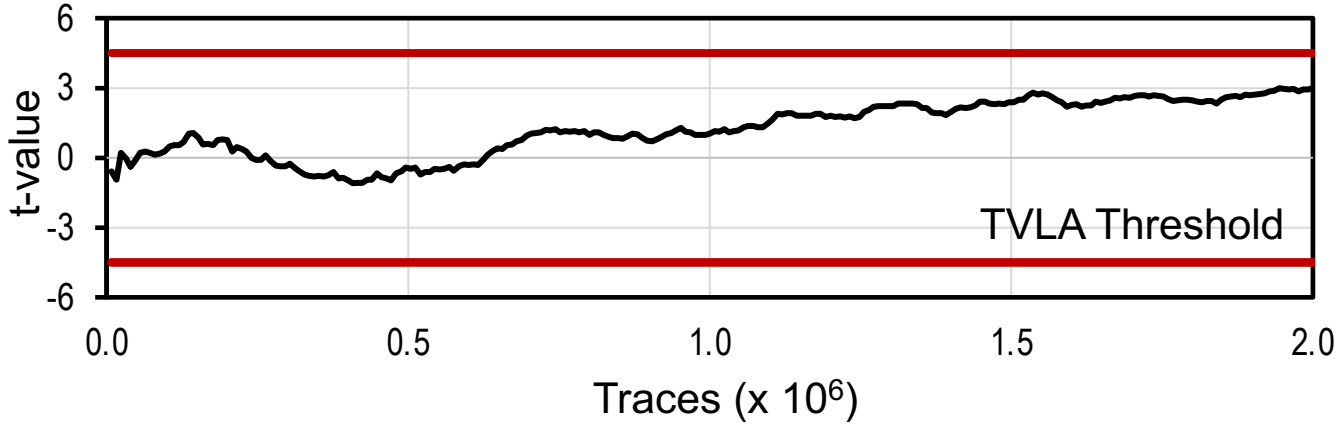
- Motivation: Side-channel Security Concerns for Embedded Neural Network implementations.
- Hardware Defenses.
- Evaluation Results and Comparison.

Side-Channel Leakage Evaluation Results

Test Vector Leakage Assessment (TVLA) Test:



(TVLA) Default MAC operation



(TVLA) Secure MAC operation

Comparison Results

Metric	HOST'20 [1]	ICCAD'20 [2]	CICC'19 [3]	This work
Platform	FPGA	FPGA	ASIC (55nm)	ASIC (28nm)
Defense Techniques	Arithmetic Masking	Boolean Masking	Homomorphic Enc./Dec.	Boolean Masking
Supply Voltage (V)	-	-	0.4	0.60 - 0.95
Frequency (MHz)	24	24	60	10 - 125
Latency Overhead [a]	2x	101x	-	1.4x
Energy / opn.	-	-	50.63 nJ/op. [b] 13.11 nJ/op.	2.1 pJ/op. (Traditional) [c] 11.5 pJ/op. (Secure)
Area Overhead	2.3x [d]	5.9x [d]	-	1.64x [e]
Configurability	No (MNIST)	No (MNIST)	-	Yes (MLP / 1D-CNN)
Model Details	Binarized	Binarized	-	Multibit
SCA Evaluation	CPA (>0.1M)	TVLA (>2M)	-	CPA , TVLA (>2M)
RNG Source	PRNG	Trivium (Traditional design)	-	Trivium (TI-based design)
Weights Encryption	No	No	Yes	Yes (Trivium Cipher)

[a] Calculated for 50 MAC operations.

[b] Energy reported for Enc and Dec. operations, respectively.

[c] Energy reported per MAC operations (averaged over 50 MAC operations).

[d] [4] and [5] reported the area overheads for the LUT and FF units.

[e] Our design has reported the overall area overhead (includes both the logic area and SRAM size increase).

Conclusion

- Side-channel Security concerns of Embedded Neural Networks implementations.
- Defense Technique – Threshold Implementation
- Side-channel evaluation results

Reference: S. Maji, U. Banerjee, S. H. Fuller, and A. P. Chandrakasan, "ShieldNN: A Threshold Implementation-based Neural Network Accelerator Securing Model Parameters and Inputs against Power Side-Channel Attacks," in *IEEE ISSCC*, 2022.

References

[1] A. Dubey, et al., "MaskedNet: The First Hardware Inference Engine Aiming Power Side-Channel Protection," *IEEE HOST*, 2020.

[2] A. Dubey, et al., "BoMaNet: Boolean Masking of an Entire Neural Network," *IEEE/ACM ICCAD*, 2020.

[3] I. Yoon, et al., "A 55nm 50nJ/encode 13nJ/decode Homomorphic Encryption Crypto-Engine for IoT Nodes to Enable Secure Computation on Encrypted Data," *IEEE CICC*, 2019.

Thanks !!!

Collaborators:

- Utsav Banerjee
- Samuel H. Fuller

Acknowledgements:

- Funding Support: Analog Devices Inc.
- Chip Fabrication Support: TSMC University Shuttle Program
- Alex Ji, Maitreyi Ashok, Miaorong Wang and Kyungmi Lee for helpful technical discussions.