Aging and Side-channel EM Analysis

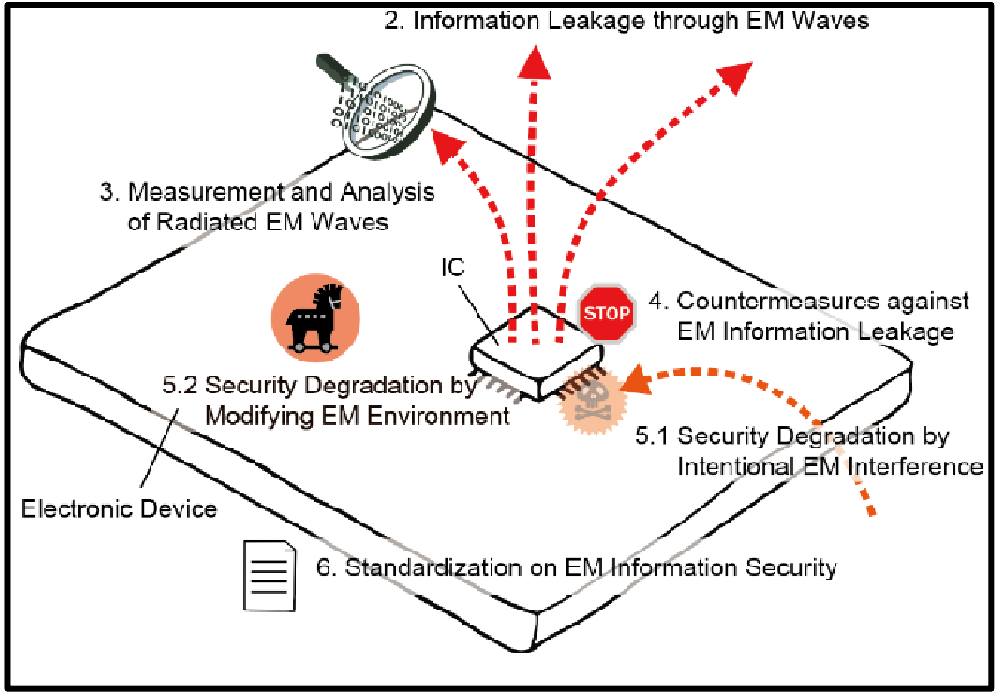
Ojas Kulkarni[1], Manoj Vutukuru[2], Rashmi Jha[2]

[1]Department of Electrical and Computer Engineering, University of Utah, Salt Lake City, UT 84096

[2]Department of Electrical and Computer Engineering, University of Cincinnati, Cincinnati, OH 45219

Introduction

[1]


2. Information Leakage through EM Waves
3. Measurement and Analysis of Radiated EM Waves
IC
STOP
4. Countermeasures against EM Information Leakage
5.2 Security Degradation by Modifying EM Environment
5.1 Security Degradation by Intentional EM Interference
Electronic Device
6. Standardization on EM Information Security

Hardware vulnerabilities:

- EM leakage

Impact of Hardware Vulnerabilities:

- Secret information can be retrieved
- Reliability can be compromised

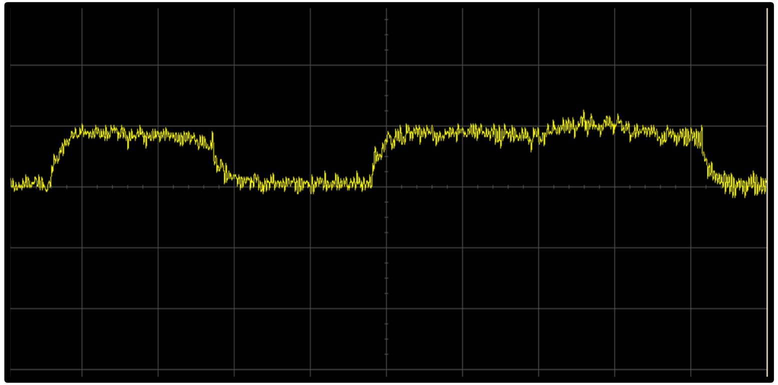
[1] Y. Hayashi and N. Homma, "Introduction to Electromagnetic Information Security," *IEICE Trans. Commun.*, vol. E102.B, no. 1, pp. 40–50, Jan. 2019, doi: 10.1587/transcom.2018EBI0001.

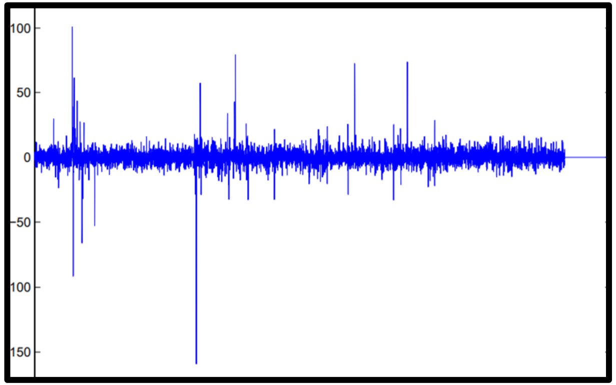
Side-Channel Electromagnetic Analysis

Computing platforms radiate EM fields

Can be measured using:

- Power (consumption) analysis
- EM analysis (our focus)

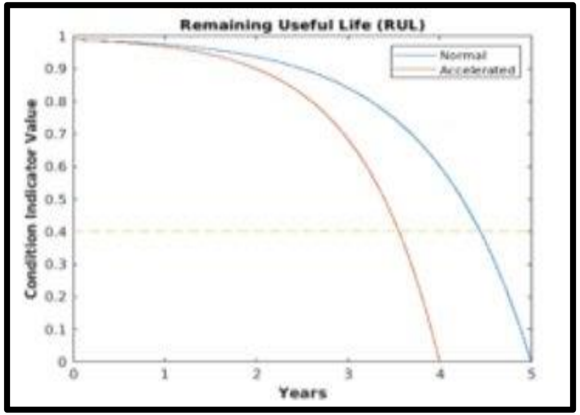


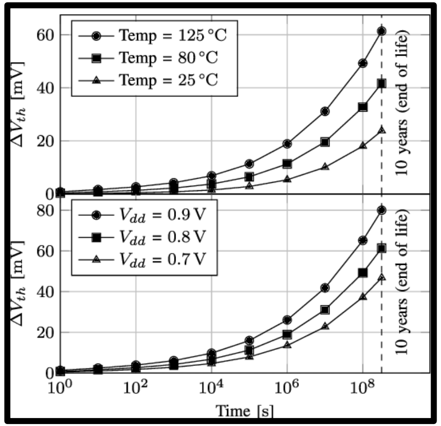


[1]

[1] D. Agrawal, B. Archambeault, J. R. Rao, P. Rohatgi, and P. O. Box, “The EM Side–Channel(s):Attacks and Assessment Methodologies”.

Aging





[1]

Transistors naturally age

- Hot-Carrier Injection
- Bias-Temperature Instability

Accelerate Aging to simulate lifetime conditions

- Hardware trojans etc.

[1] J. Lienig *et al.*, "Toward Security Closure in the Face of Reliability Effects ICCAD Special Session Paper," in *2021 IEEE/ACM International Conference On Computer Aided Design (ICCAD)*, Nov. 2021, pp. 1–9. doi: 10.1109/ICCAD51958.2021.9643447.

Motivation

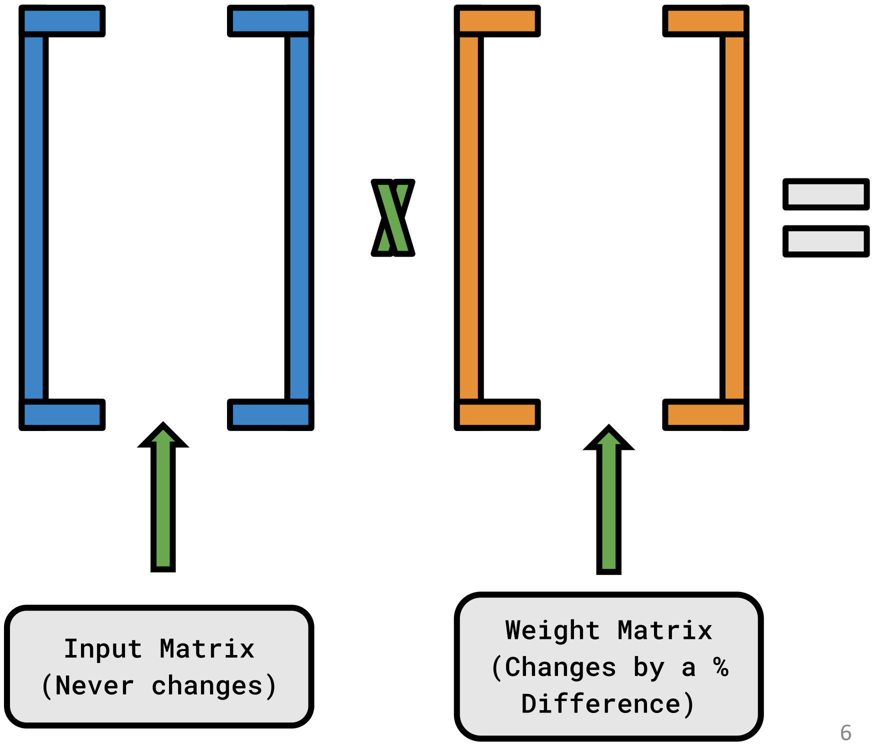
Matrix Multipliers are used in Machine Learning and thus security vulnerabilities need to be exploited

+

Side-Channel EM Analysis on FPGAs has taken a prevalence

Research Project Goal

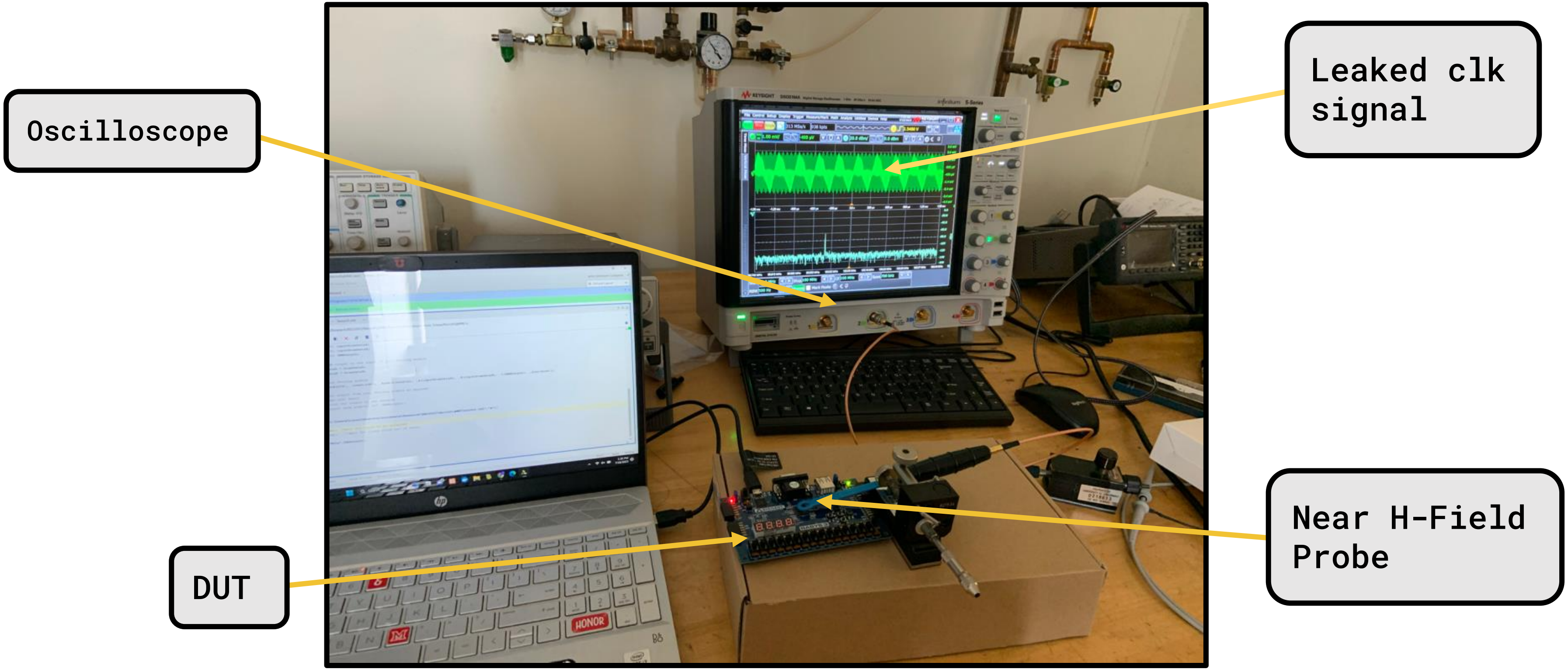
Evaluate the effect of aging onto FPGA based non-cryptographic circuit using side-channel EM analysis



Input Matrix (Never changes)

Weight Matrix (Changes by a % Difference)

Approach and Methods



Oscilloscope

Leaked clk signal

DUT

Near H-Field Probe

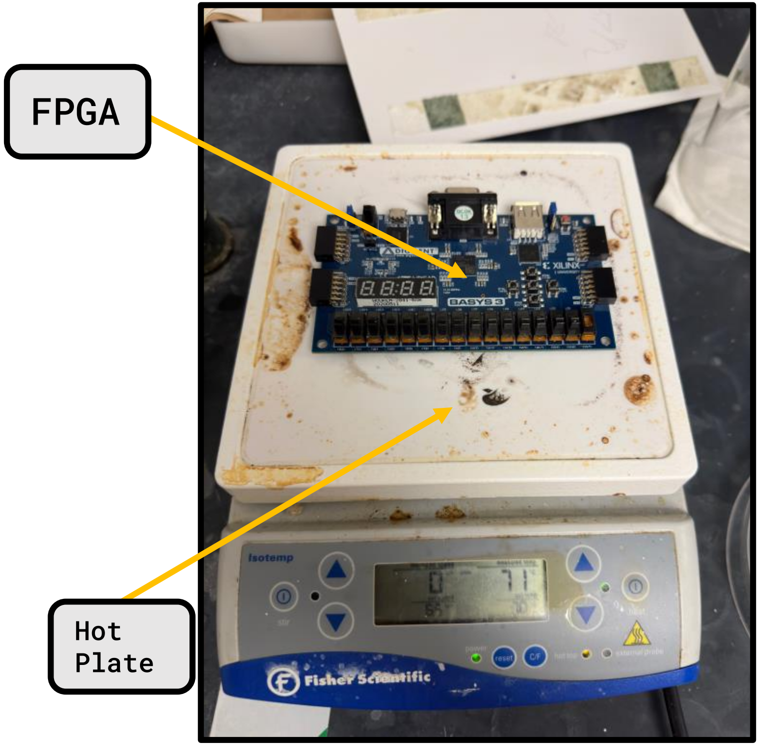
Methods for Accelerated Aging

Stress Test (~2 years):

- Let the Matrix Multiplier operate continuously for ~10 hours

Thermal Stress (~1 year):

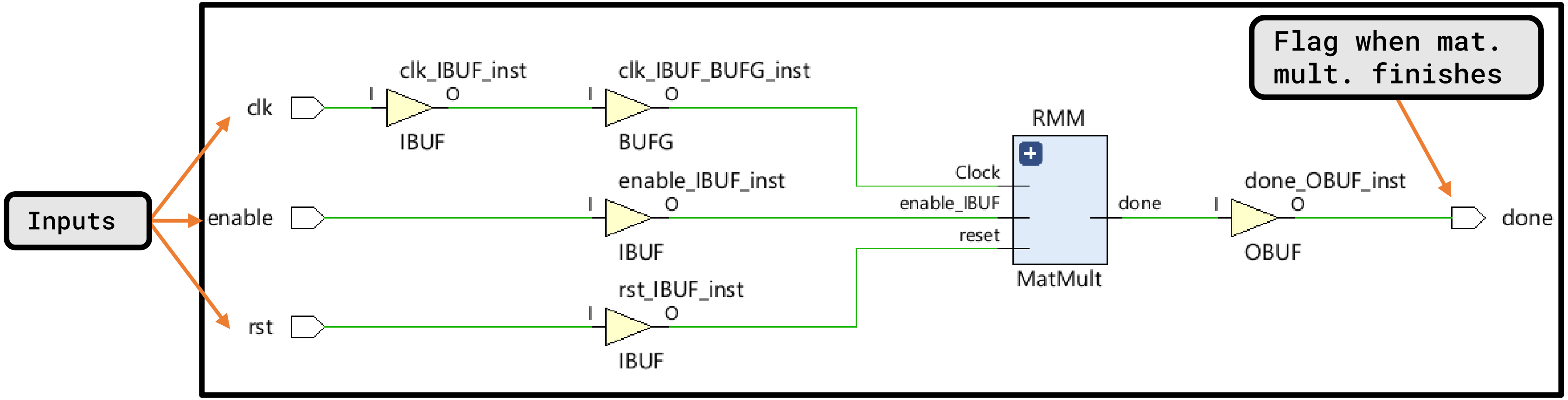
- 70°C for 3.5 hours
- Natural cooling



FPGA

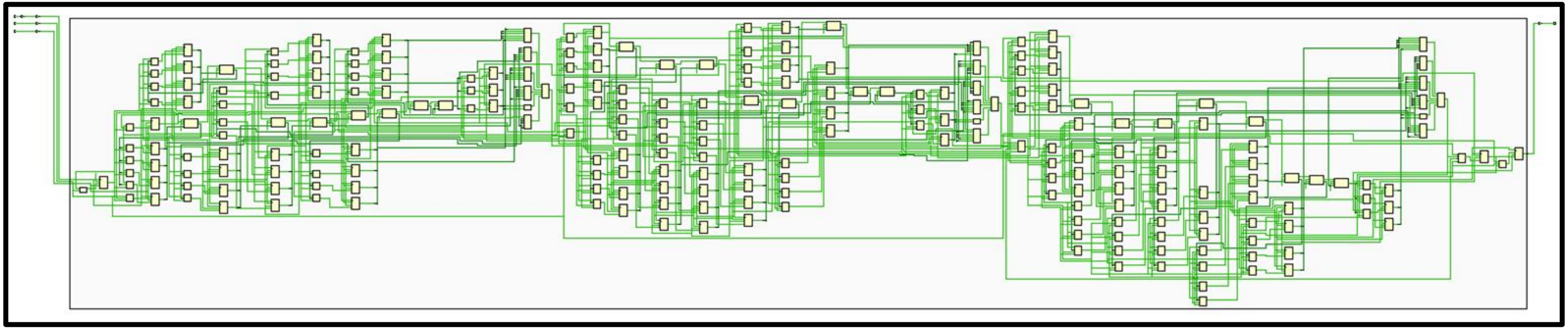
Hot Plate

Matrix Multiplier

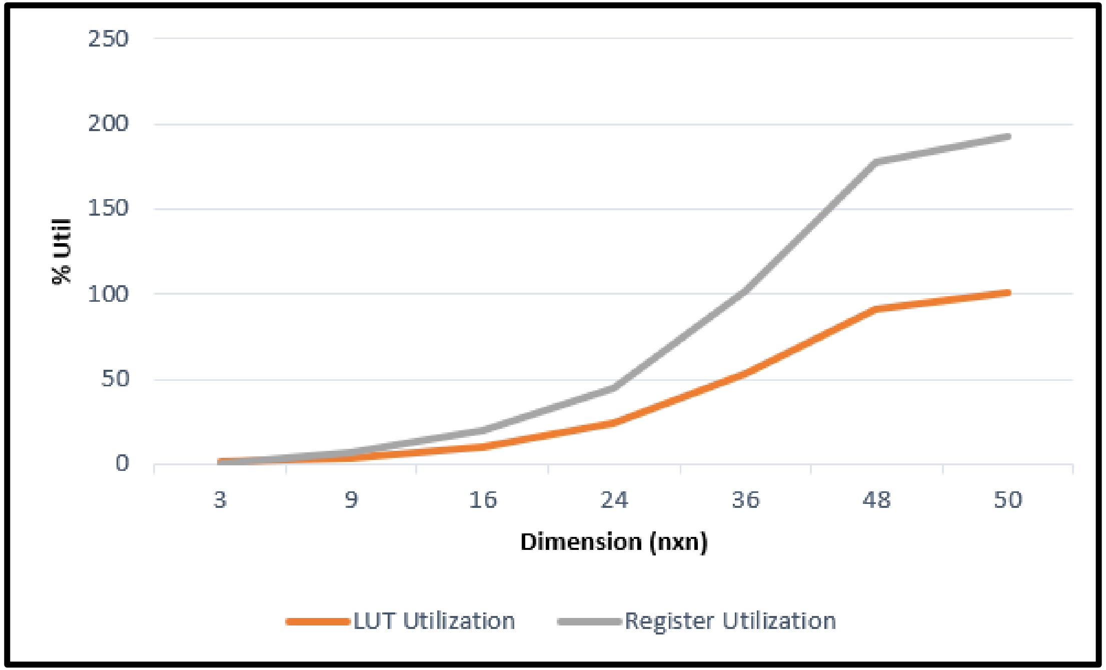


Inputs

Flag when mat. mult. finishes

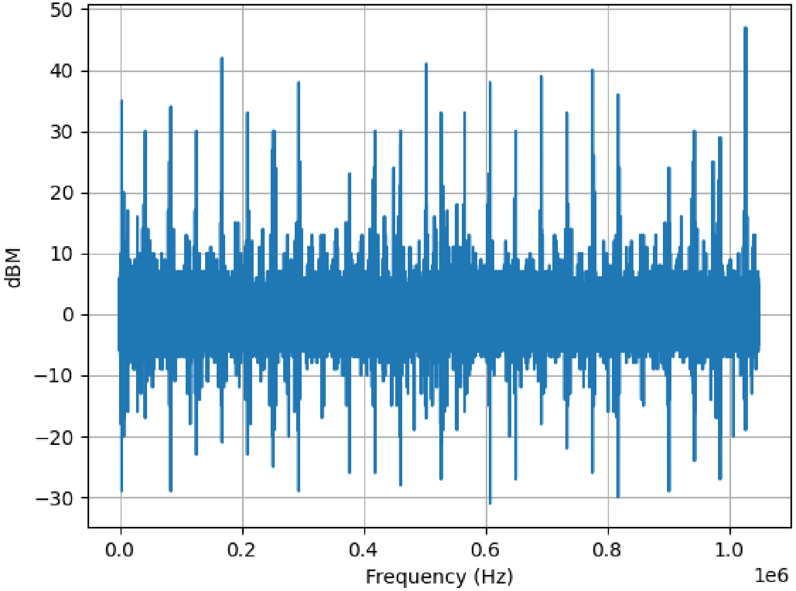


FPGA Limitations

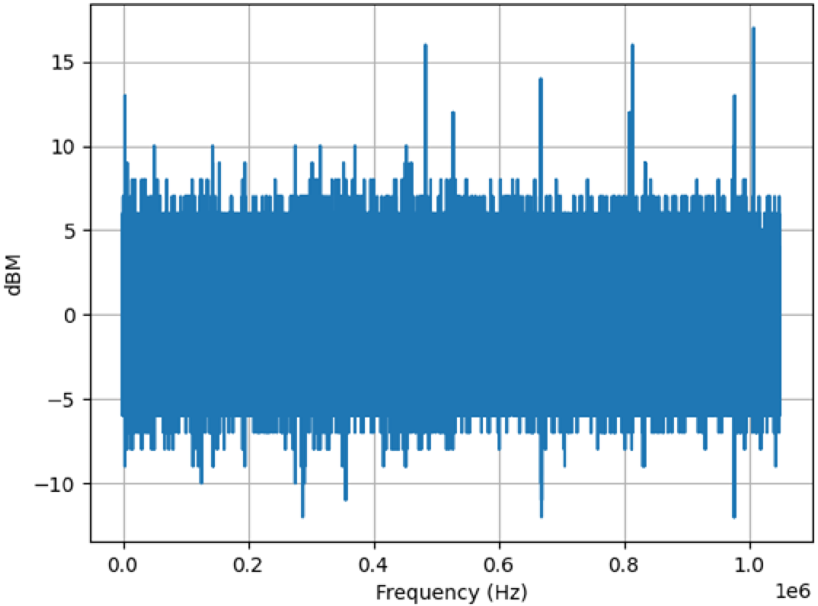


Simulated maximum of 50x50 arrays to max out resources aboard AMD Basys 3 board

Controls

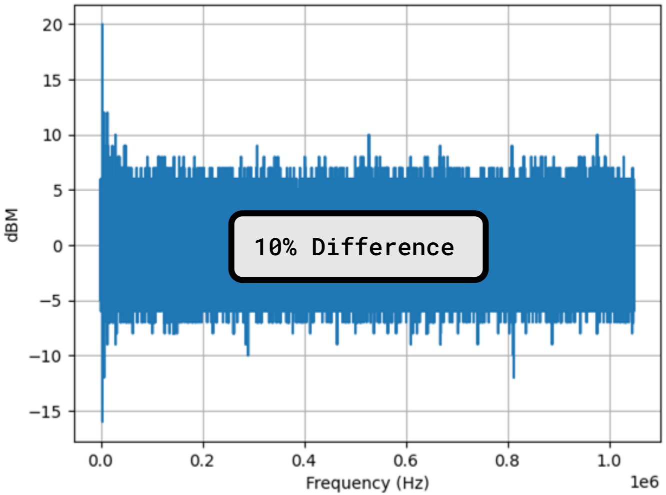


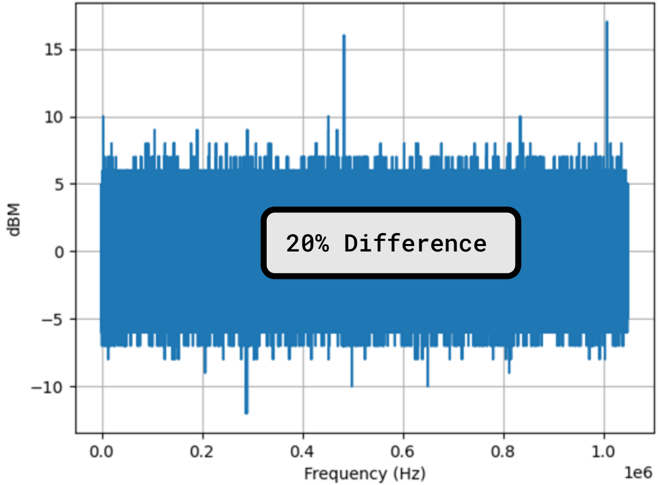
Weight values are all 0s

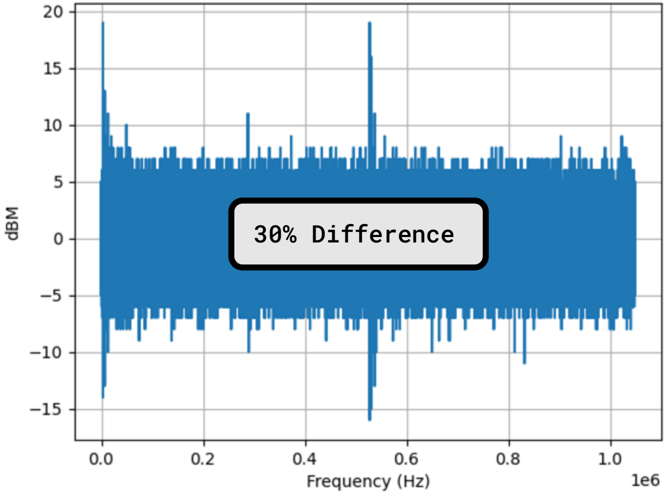


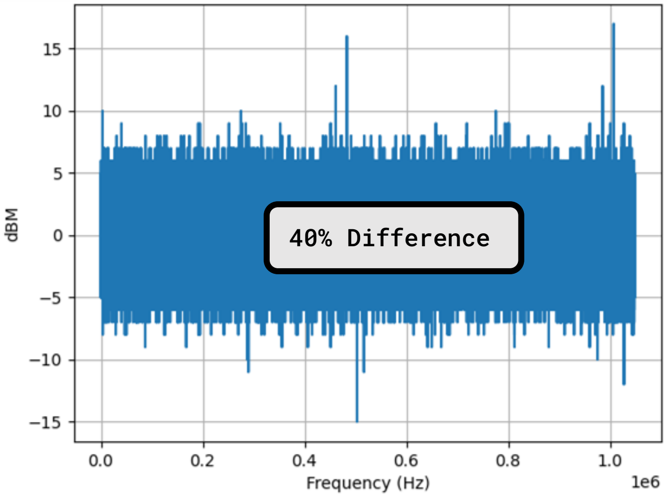
Weight values are all 1s

Unaged

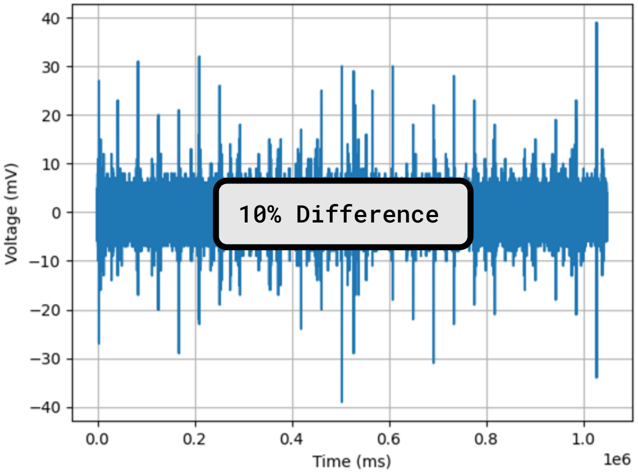

10% Difference
dBM
20
15
10
5
0
−5
−10
−15
0.0
0.2
0.4
0.6
0.8
1.0
Frequency (Hz)
1e6


20% Difference
dBM
15
10
5
0
−5
−10
0.0
0.2
0.4
0.6
0.8
1.0
Frequency (Hz)
1e6

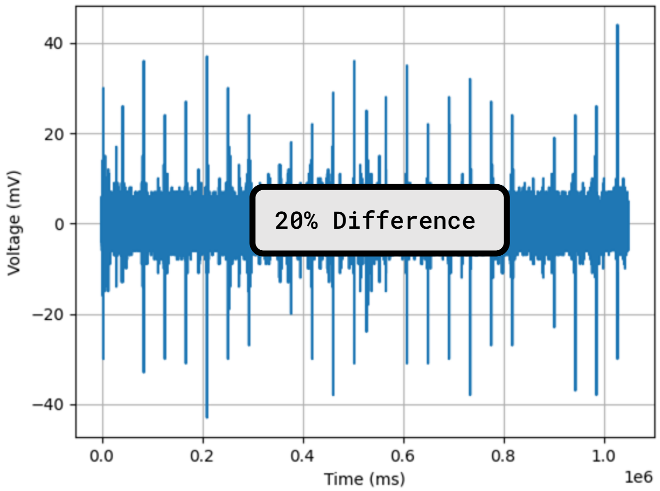

30% Difference
dBM
20
15
10
5
0
−5
−10
−15
0.0
0.2
0.4
0.6
0.8
1.0
Frequency (Hz)
1e6


40% Difference
dBM
15
10
5
0
−5
−10
−15
0.0
0.2
0.4
0.6
0.8
1.0
Frequency (Hz)
1e6

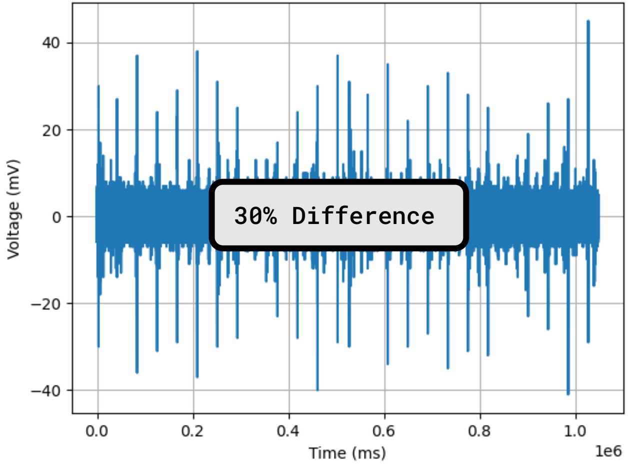
Stress Test



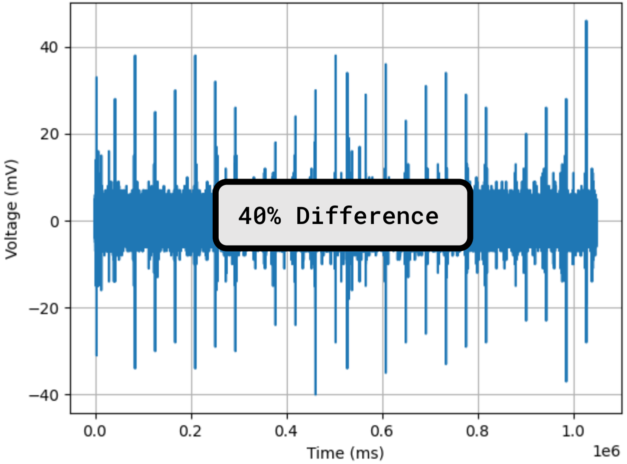
10% Difference



20% Difference

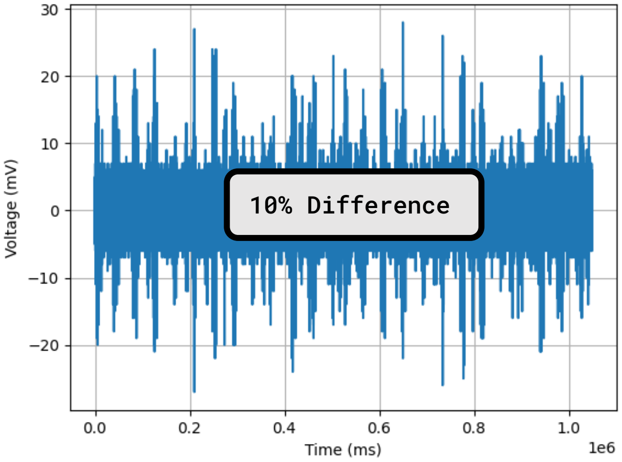


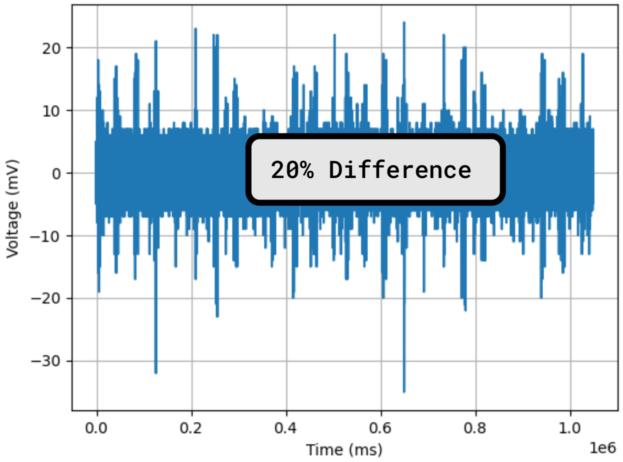
30% Difference

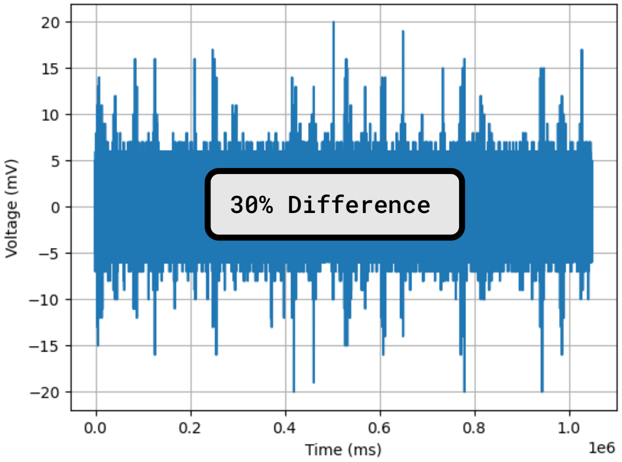


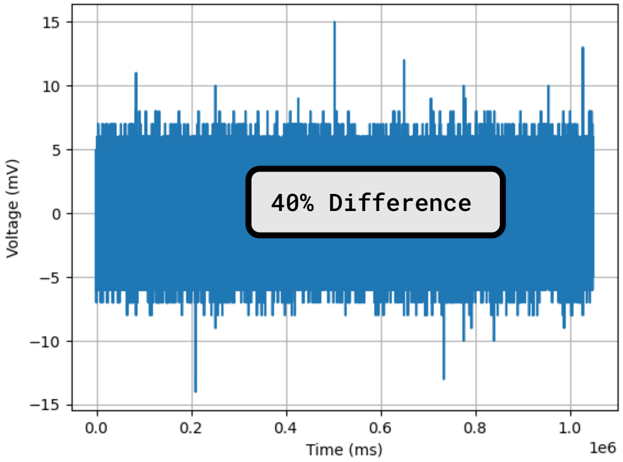
40% Difference

Thermal Stress

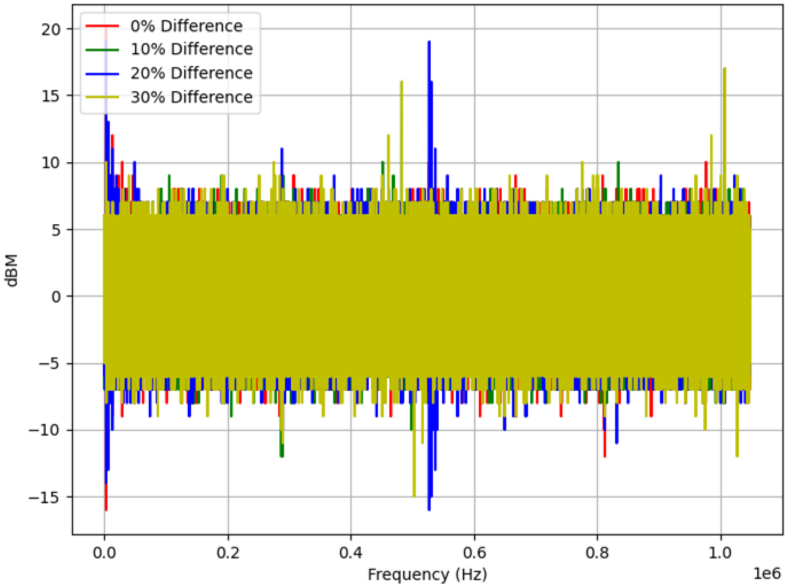


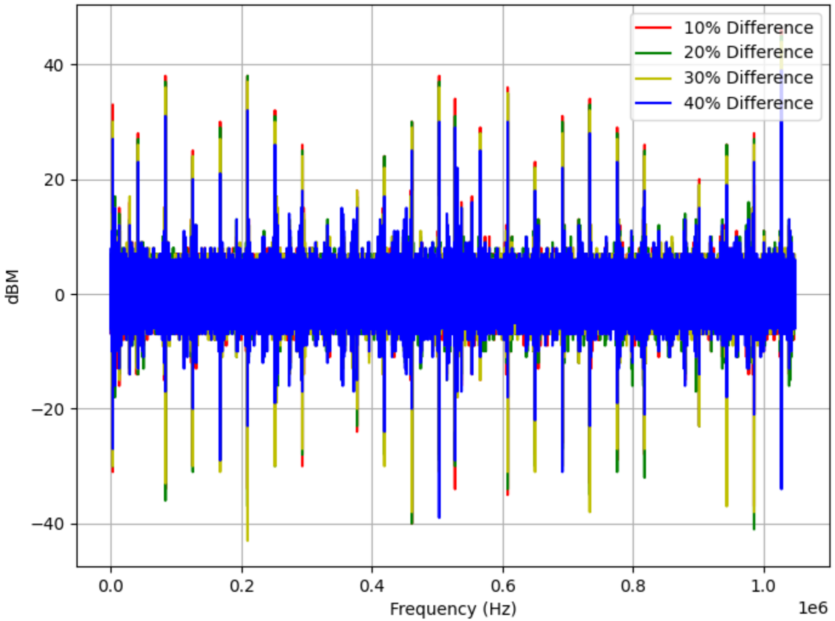






Outcome

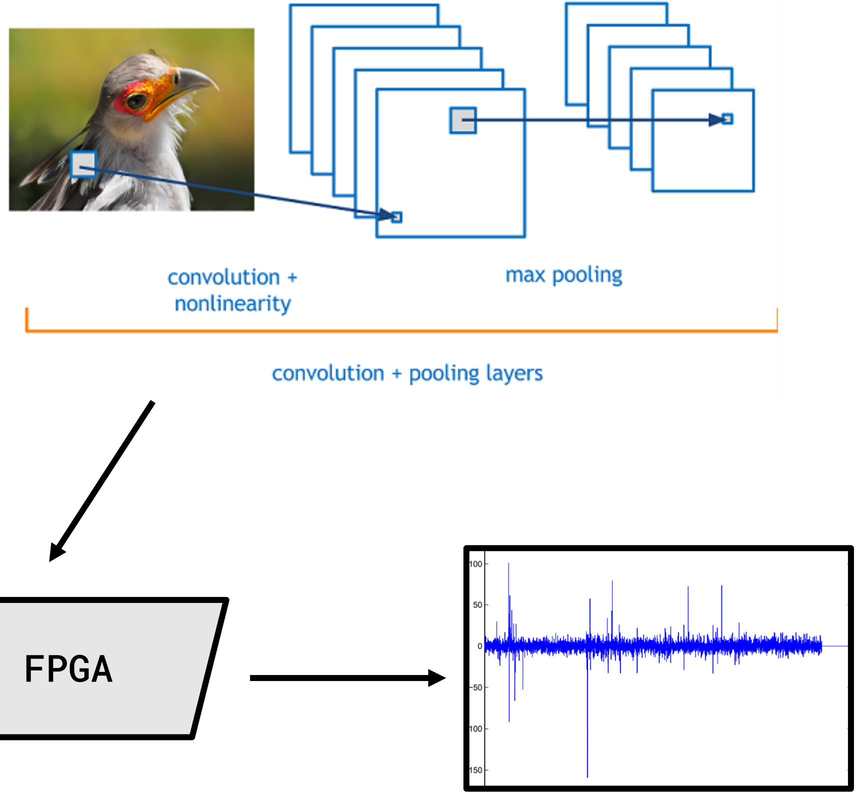

0% Difference
10% Difference
20% Difference
30% Difference
dBM
20
15
10
5
0
−5
−10
−15
0.0
0.2
0.4
0.6
0.8
1.0
Frequency (Hz)
1e6


10% Difference
20% Difference
30% Difference
40% Difference
dBM
40
20
0
−20
−40
0.0
0.2
0.4
0.6
0.8
1.0
Frequency (Hz)
1e6

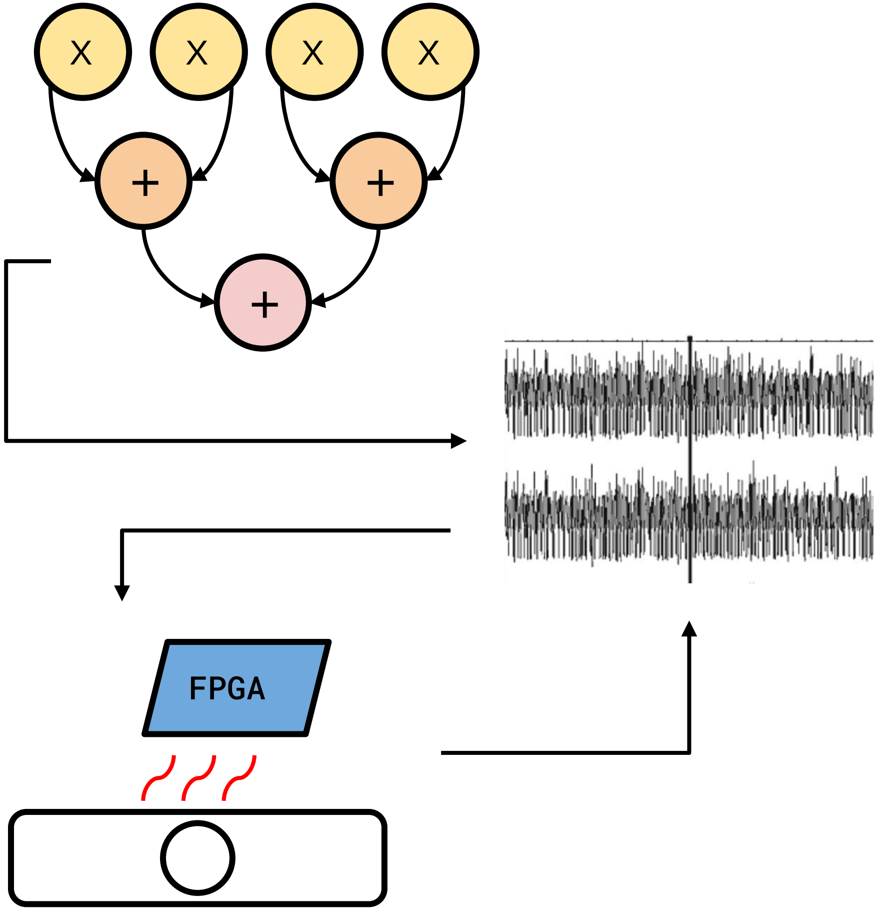
Future Work

Age the board much longer (~80°C for 2 weeks)

Attempt to run SCA on a traditional classifier



Conclusions



- Designed and implemented 38x38 (maximum) FPGA based matrix multiplier
- Performed aging and SCA
- Characterized SCA differences

Acknowledgements

NSF

#CNS-2150086

MIND

University of CINCINNATI

Thank You!