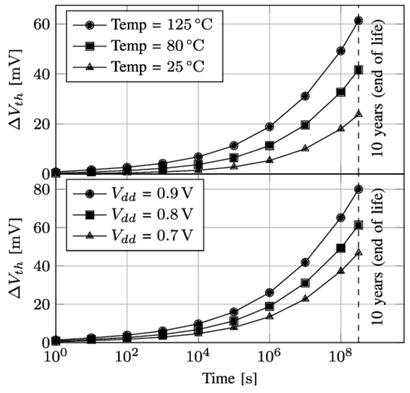
Impact of Aging on EM Side-Channel Analysis of FPGA based Matrix Multiplier

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

[1]Department of Electrical and Computer Engineering, University of Utah, Salt Lake City, UT, 84112
[2]Department of Electrical and Computer Engineering, University of Cincinnati, Cincinnati, OH, 45219

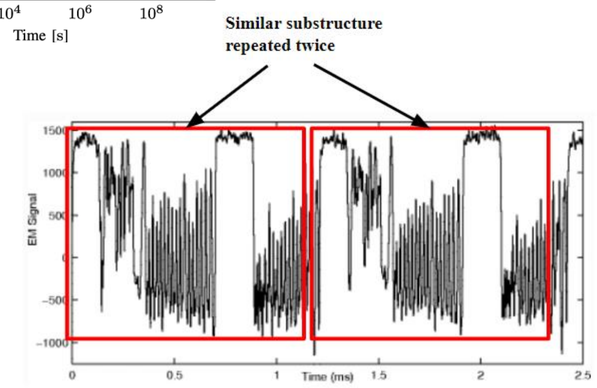
Introduction

- CMOS devices undergo damage as they naturally age
  - Causes increase in threshold voltage leading to increased switching times
- EM Side-Channel Analysis exploits EM leakage to extract sensitive information
- Matrix Multipliers are widespread as AI/ML Acceleration techniques



DECREASES REMAINING USEFUL LIFE

2 rounds of RSA encryption are shown here

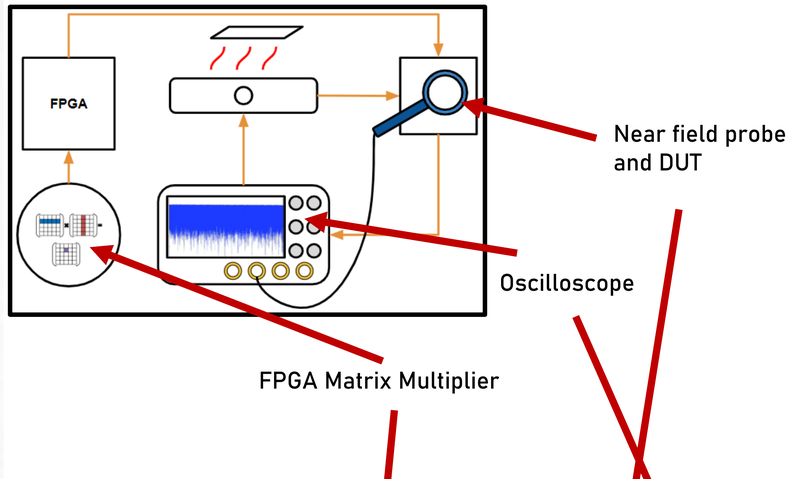


Objective

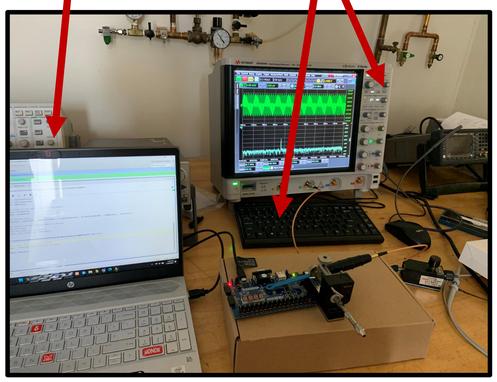
FPGA MMU → Aging FPGA → SEMA

Test the impact of AGING on MATRIX MUTIPLIERS using EM SIDE CHANNEL analysis

Methodology



1) Implement largest MM
2) EM analysis – UNAGED
3) Change weights – 10%, 20%, 30%, 40%
4) EM analysis – MODERATELY AGED
5) CHANGE WEIGHTS
6) EM Analysis – HEAVILY AGED



Initial Results & Control

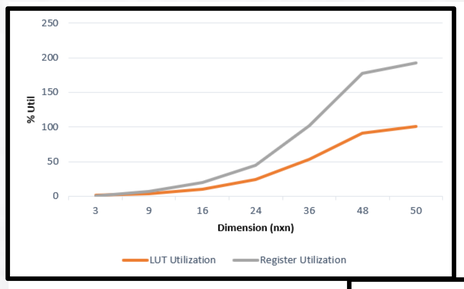
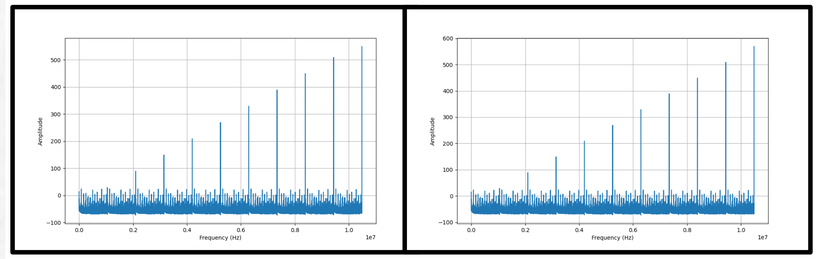


Fig. 5: FPGA Resource utilization wrt matrix dimension

Fig. 6: Control with 0% difference in the weights

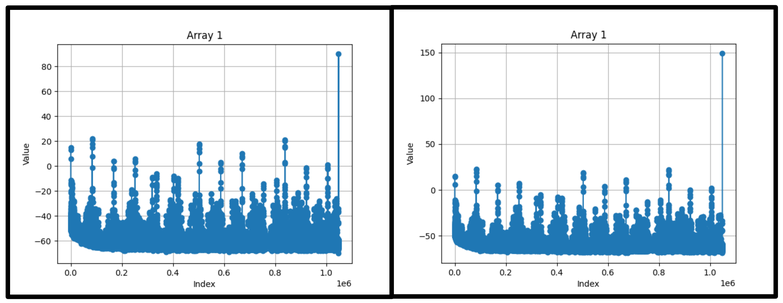
Experimental Results

UNAGED



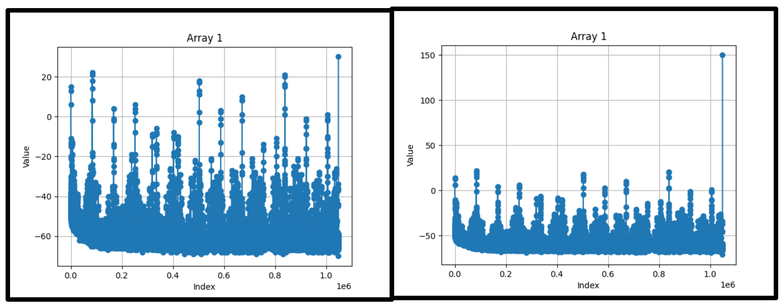
10% Difference | 30% Difference

MODERATELY AGED



10% Difference | 30% Difference

HEAVILY AGED



10% Difference | 30% Difference

Acknowledgements

This work was supported by NSF Award ID #CNS-2150086 under the Research Experience for Undergraduate in Hardware