Side Channel Resistant MRAM Controller

**Background:**

DPA is an extremely powerful technique that uses power consumption as a source of leakage. For this, many power traces of execution of cryptographic algorithm are collected and processed. Machine learning techniques are then used to correlate between the power traces and the secret keys.

**Project Description:**

- Read Papers about DPA and Toggle MRAM
- Design MRAM Controller on FPGA
- Setup DPA attack according to architecture and technology
- Optimize the Controller by mean of Power analysis
- Evaluation of Immunity

**Perquisites:** Computer organization and Design

**Recommended:** Lab1

**Host:** VLSI Lab

Kunal, Eric 054-4946383, Lab718, ericherbelin@ee.Technion.ac.il

[http://asic2.group/](http://asic2.group/)