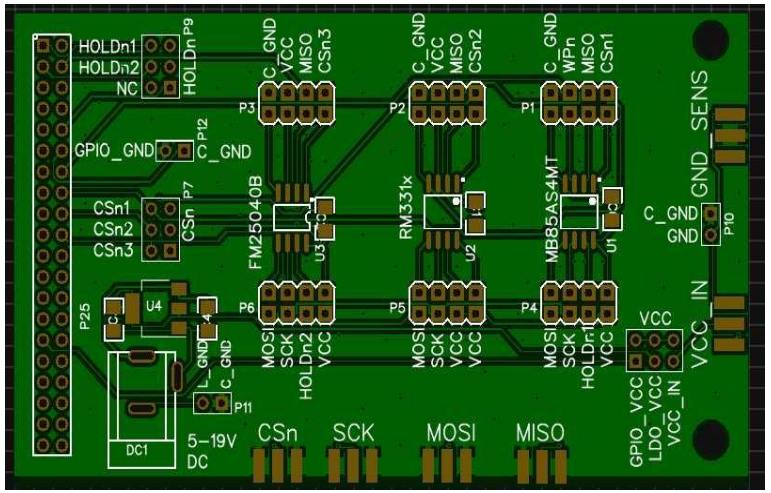
Differential Power Analysis (DPA) of emerging technology memories

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.*

ReRAM, FeRAM and CBRAM are emerging memory technologies.



Project Description:

- Read Papers about DPA and AES (Advanced Encryption Standard)
- Implement SPI I/F on FPGA board
- Design AES Module
- Setup DPA attack
- Collect and Process Traces

Perquisites: Computer organization and Design

Recommended: Lab1

Host: VLSI Lab

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

http://asic2.group/

ASIC² ARCHITECTURES SYSTEMS INTELLIGENT COMPUTING INTEGRATED CIRCUITS