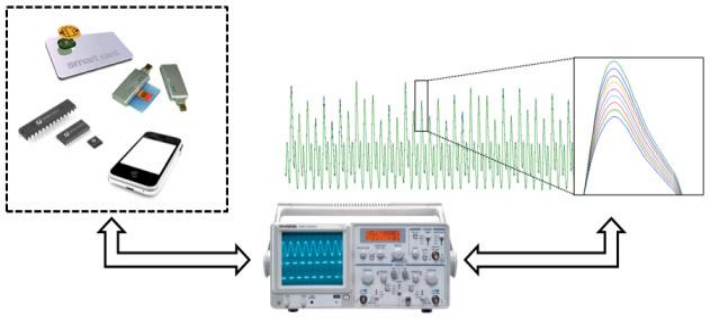
Design and Security Analysis of an AES encryption module

Background: *Side Channel Analysis is a group of attacks that utilize side effects of implementations of cryptographic hardware to gain access to secrets. One of such attacks is a Differential Power Analysis (DPA). 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. It was first published in 1996, and since then hundreds of works have been published on successful DPA attacks of different types and on protection methods.*



Project Description: In this project, we will apply a basic DPA attack to an implementation of a most popular encryption algorithm today – AES (Advanced Encryption Standard). For this purpose, we will first implement the AES algorithm on an FPGA device. At the next stage, the FPGA device will be connected to an oscilloscope or a data acquisition device for collecting traces. The traces will then be processed and analyzed for finding a key. Finally, protection techniques will be evaluated.

The project phases will include:

- Design of the AES module on an FPGA
- Verification of the design
- Setting up the DPA experiment
- Collecting & Processing traces using signal processing techniques
- Implementing and testing the protection

Leonid Azriel, leonid.azriel@gmail.com
Eric Herbelin ericherbelin@ee.Technion.ac.il

דרישות קדם: תכן לוגי, מעבדה

ASIC² ARCHITECTURES SYSTEMS INTELLIGENT COMPUTING INTEGRATED CIRCUITS