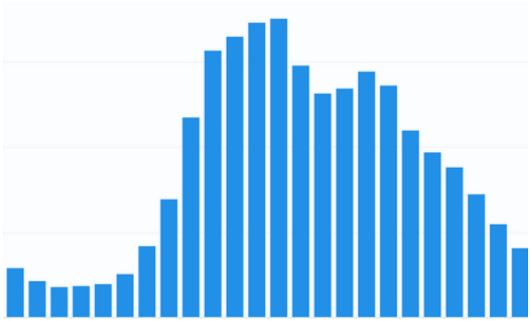
Parametric attack on a Physical Unclonable Function (PUF)



Physically unclonable functions (PUFs) are special hardware primitives that produce responses on challenges, which are unique for every PUF instance. PUFs are widely used for the integrated circuit (IC) identification and secret key generation. The special PUF behavior comes from the process variation phenomenon. Small variation in the electrical parameters between individual chips makes the same PUF design produce different results. Ideally, the PUF behavior cannot be modeled. In practice, various attacks on PUFs have been introduced, such as using machine learning to characterize the PUF behavior.

In this project, we are interested to learn about a parametric attack on PUFs mounted by a malicious manufacturing facility. In this attack, the adversary will tweak the process parameters in a way that the statistical assumptions on the process variations will not hold. This allows the adversary to introduce a statistical bias that alleviates the prediction attack.

To investigate this attack, the students will implement several classical PUF designs using analog design tools, tweak the device models to emulate a biased process, simulate the PUF design with the modified models to obtain their statistical properties. AT the next stage, the students will try to mount a prediction attack on the obtained results. The students will use analog design tools (Cadence Virtuoso), Spice simulations and statistical tools in this project.

Prerequisites: Logic Design, Linear Circuits, Lab 1.

Supervisor: Leonid Azriel (*leonida@technion.ac.il*)