MSc project idea:

Debiasing in memory-based PUFs

Memory-based PUFs (Physical Unclonable Functions) such as SRAM-PUFs make use of uncontrollable and unique manufacturing variations in digital memory chips to derive inbuilt identifiers/keys from the hardware. For example, cell arrays in uninitialised SRAM memory have a unique 0/1 startup pattern. An essential step in key derivation is error correction, since PUF readout yields noise values. A complication occurs in the "more noise than entropy" regime, when the cell values are very biased, such that the entropy of the noise exceeds the entropy of the PUF pattern. It is still possible to derive a key, namely using *debiasing* techniques.

https://www.iacr.org/archive/ches2015/92930497/92930497.pdf
https://eprint.iacr.org/2016/241.pdf
https://pure.tue.nl/ws/portalfiles/portal/160359845/20200911_Kusters.pdf

The assignment is to analyse the performance of these techniques, especially in the "more noise than entropy" regime, and possibly to construct improved versions.

Please contact Boris Škorić if you are interested,
MF 6.059
040-247 4870
b.skoric@tue.nl

[March 2021]