PUFs for Bitstream Protection

Physical Unclonable Functions derive secrets from chip-individual manufacturing variations. One idea, proposed in the last years, was to use PUFs to protect an FPGA bitstream, e.g. [1]. This concept utilizes delay variation in circuits like suggested in [2].

For this seminar topic, the used protection mechanism, including the principle of the PUF, should be described. Possible security threats and the feasibility/infeasibility of possible attacks should be analyzed and discussed.


Contact

Request Topic

Advisors

Michael Pehl