Friedrich-Alexander-Universität
Department Elektrotechnik-Elektronik-Informationstechnik

EEI-Kolloquium

Physical Unclonable Functions: Coded Modulation, Shaping, and Helper Data Schemes

Prof. Dr.-Ing. Robert Fischer
University of Ulm

Donnerstag, den 25.01.2024, 10:15 Uhr
Live: Raum 01.021, Cauerstraße 7, 91058 Erlangen.

Physical unclonable functions (PUFs) generate fingerprints by exploiting randomness that intrinsically occurs in integrated circuits due to uncontrollable variations in the manufacturing process of physical objects. Most of the literature deals with binary PUFs and employ binary hard-decision decoding to stabilize the response against environmental variations and readout errors.

It is of interest to i) increase the reliability by employing soft-decision decoding and ii) increase the size of the extracted key by resorting to higher-order alphabet or, even better, by applying methods from coded modulation and signal shaping.

In this talk, a suited model for studying PUFs with real-valued readout is presented. The transition from binary PUFs to schemes utilizing coded modulation and signal shaping will be discussed. The main item in PUFs is the so-called helper data scheme, which in the first place enables decoding. Suited schemes are presented, and it is shown how the helper data, which has to be independent of the PUF readout, can be designed to improve decodability.