INVITED SPEAKER

MICHAEL PEHL (TUM EI SEC)

Michael Pehl received his Dr.-Ing. degree in 2012 from the Technical University of Munich. His thesis with title "Discrete Sizing of Analog Integrated Circuits" was carried out at the Institute for Electronic Design Automation and focused on the development of optimization algorithms for yield-aware analog sizing considering discrete design parameters. For this work he received the Kurt-Fischer Prize in 2013. Since 2012 he is researcher and teaching associate at the Institute for Security in Information Technology. The focus of his current research is on Physical Unclonable Functions. Further research interests include biometrics, side-channel analysis and tools to support secure design. He is member of IEEE and VDE.

TITLE

Physical Unclonable Functions – From Hardware-Intrinsic Features to Security

ABSTRACT

Physical Unclonable Functions are security primitives which can be used to derive secrets from hardware-intrinsic features. PUFs are used in two main applications: In challenge-response protocols, PUFs allow lightweight identification and authentication. For key-storage, PUFs are an alternative to the conventional way of storing a key in secure NVM. The research in this field until today now results in first products which use PUF primitives. However, deriving a secret from a PUF in a secure way is still a non-trivial task. Thus, it is crucial to analyze how secure a PUF is. Recent results from information theory can be used to derive theoretical bounds. Characterization and test of PUFs is required to analyze how close the reality is to such bounds, to find flaws in the design, and also to evaluate the quality of a PUF to enable certification in the future. Also, like every secure device, PUFs can be attacked in hardware, e.g., by side-channel analysis. So it is also crucial to find root causes for leakage and to protect the PUF and the required postprocessing against this class of attacks. This talk gives an overview over the mentioned topics and discusses where we stand.