Low Latency Primitives and Beyond

Gregor Leander

Ruhr University Bochum, Germany

In this talk I will give a survey on low latency block ciphers first and then look into dedicated applications that might allow for interesting alternatives due to the attacker model, e.g. cache encryption. In the last part of the talk, I will discuss security aspects of the sum-of-two-permutations construction of a pseudo random function and how to related its security to the composition of the two permutations.