**Dokumenttyp:** Konferenzbeitrag

**Art des Konferenzbeitrags:** Vortrag / Präsentation

**Autor(en) des Beitrags:** Jungk, Bernhard and Rodrigues Lima, Leandro and Hiller, Matthias

**Titel des Beitrags:** A Systematic Study of Lightweight Hash Functions on FPGAs

**Abstract:** Lightweight cryptography provides cryptographic algorithms for resource constrained devices and typically aims for low-cost ASIC applications like RFID tags. In addition, it also provides attractive performance–security trade-offs for FPGAs in scenarios with strict area constraints. This work presents FPGA implementations of the popular lightweight hash functions KECCAK-200 and KECCAK-400, PHOTON and SPONGENT, and gives a systematic analysis of size and throughput. The ratio between throughput and slices is a relative performance measure that enables a fair comparison among different algorithms and implementation strategies. The comparison shows that the size of the presented implementations differs over roughly one order of magnitude and the throughput over more than one order of magnitude. The SPONGENT implementation provided the highest throughput per area ratios.

**Stichworte:** Lightweight crypto, Hash function, Sponge construction, KECCAK, PHOTON, SPONGENT, FPGA