Abstract

Invaluable benchmarking efforts have been made to measure the performance of eSTREAM portfolio stream ciphers and SHA-3 hash function candidates on multiple architectures. In this thesis we contribute to these efforts; we evaluate the performance of *all* eSTREAM ciphers and *all* second-round SHA-3 candidates on NVIDIA Graphics Processing Units (GPUs).

Complementarity, we present the first implementation of the cube attack in a multi-GPU setting. Our framework proves useful in the practical analysis of algorithms by providing a generic black box interface and speedup factors over 100×. Demonstrating its use we analyze two eSTREAM stream ciphers, MICKEY v2 and Trivium. We find that MICKEY is not susceptible to low-degree cube attacks, while our Trivium analysis confirms previous results, in addition to several new equations applicable to a partial key recovery.

We also extend the linear differential cryptanalysis framework introduced by Brier, Khazaei, Meier and Peyrin at ASIACRYPT 2009 using two new trail search algorithms, and several optimizations. We find several collision and second preimage attacks on simplified and round-reduced variants of BLAKE and CubeHash, two SHA-3 second round candidates. Using the extended framework we also present improved collision attacks on CubeHash, when compared to previous results. In combination with the condition function concept, our new trail search algorithms lead to much faster collision attacks. We demonstrate this by providing a real collision for CubeHash-5/96. Additionally our randomized trail search finds highly probable linear differential trails and leads to significantly better attacks for up to eight rounds of CubeHash.