Lehrstühle und Professuren

Dokumenttyp: Verschiedenes

Author: Patrick Karl and Michael Tempelmeier

Titel: A Detailed Report on the Overhead of Hardware APIs for Lightweight

Abstract: The “Competition for Authenticated Encryption: Security, Applicability, and Robustness” (CAESAR) was the first cryptographic competition that required designers to use a mandatory hardware API for their implementations. Recently, a similar hardware API for the NIST Lightweight Cryptography (LWC) project was proposed. Both APIs feature an accompanying development package to help designers implementing the API. In this paper, we have an in-depth look on these packages. We analyze the features of both packages, discuss their resource utilization, and demonstrate their impact on Ascon128, SpoC-64, and Gimli implementations on a modern Artix-7 FPGA. Finally, we provide some tweaks and enhancements to further optimize the development package for the LWC API.

Publiziert als: Cryptology ePrint Archive, Report 2020/112

Monat: Jan

Jahr: 2020

https://eprint.iacr.org/2020/112

TUM-Einrichtung: Lehrstuhl Sicherheit in der Informationstechnik