Evaluation of the CAESAR Hardware API for Lightweight Implementations

ECE Ph.D. Seminar

by

Panasayya Yalla

Ph.D. Advisor:
Dr. Jens-Peter Kaps

Thursday, November, 30, 2017, 1:00PM–2:00PM
ENGR 3202

Abstract

The Competition for Authenticated Encryption: Security, Applicability, and Robustness (CAESAR) requires that all hardware implementations of candidate algorithms adhere to the CAESAR Hardware Application Programming Interface (API). The CAESAR Hardware API is supported by a development package which includes VHDL code for universal pre- and post-processors for high-speed and recently also for lightweight implementations. These processors are designed to make a cipher core compliant with the API. However, for lightweight implementations it is generally assumed that having generic pre-and post-processors increases the area consumption over merging their functionality with the cipher cores. We evaluate the lightweight package through two case studies. First, we verified that the lightweight package has a smaller area footprint than the high-speed package. Second, we show that the overhead of using the generic lightweight pre- and post-processors over integrating their functionality into the cipher core is negligible. As part of these case studies, we have developed the first lightweight implementations of Ketje-Sr, Ascon-128, and Ascon-128a.