**Evaluation of the CAESAR Hardware API for Lightweight Implementations**

**Panasya Yalla, Jens-Peter Kaps**

Department of Electrical and Computer Engineering, George Mason University, Fairfax, Virginia 20304, USA

## Abstract

The Competition for Authenticated Encryption: Security, Applicability, and Robustness (CAESAR) requires that all hardware implementations of candidate algorithms adhere to the CAESAR Hardware API [1]. 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. In this work we verify that the lightweight package has a smaller area footprint than the high-speed package. We also 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.

## Introduction and Motivation

- **CAESAR** evaluates candidates for a final portfolio of new Authenticated Encryption with Associated Data (AEAD) algorithms.
- All candidates must adhere to the CAESAR hardware (HW) Application Programming Interface (API).
- The HW API is a component which enables a fair comparison among algorithms.
  - Independent FIFO inputs for public data (PDI) and secret data (SDI) and FIFO outputs (ODI).
  - Independent control for commands and data types using a simple protocol.
  - CAESAR HW API is supported by an implementer’s guide and development package [2].
  - Includes VHDL code for high-speed (HS) and lightweight (LW) implementations.
  - Pre- and PostProcessor separate protocol from cryptographical algorithms.
  - By using FIFOs and burst modes, header information to PostProcessor.
  - It is generally assumed that having generic pre- and post-processors increases the area consumption over merging their functionality with the cipher cores.

## Differences between HS vs. LW Packages

**High-Speed**
- Supports bus width
  - **32 ≤ w ≤ 256** in multiples of 8.
  - PreProcessor expands PDI and SDI data to full block size for CipherCore.
  - PreProcessor stores one block of PDI and SDI data.
  - PreProcessor contains universal padding unit.
  - Tag comparison has to be performed in CipherCore.

**Lightweight**
- Supports bus width of w, 16, and 32.
- PreProcessor, CipherCore, Bypass FIFO, and PostProcessor have equal bus width.
- PreProcessor has no data storage.
- Assumes padding is performed in CipherCore.
- PostProcessor supports tag comparison.

## Case Study 1: Integrated vs. LW Package

**CAESAR High-Speed Block Diagram**

**CAESAR Lightweight Block Diagram**

**Case Study 1: Integrated vs. LW Package**

**Protocol: Instruction**

**States for Processing Instruction**

**Protocol: Segment Header**

**With w=8, 16, and 16**

**States for Processing Header**

**sdi_valid sdi_ready sdi_valid sdi_data**

**msg_auth_valid msg_auth_ready msg_auth_valid msg_auth**

**bdo_type bdo_valid bdo_valid bdo_bytes**

**Key comparison has to be performed in CipherCore.**

## Conclusions

- **The graph shows implementation results of Ketje-Sr on Spartan-6.**
  - Using the CAESAR LW Package leads to a small area increase over integrated designs.
  - This small increase can easily be mitigated.

- **The graph shows the overhead incurred for implementations of Ascon on Spartan-6.**
  - Using the CAESAR LW Package leads to a much larger area increase than the LW Package as it expands the data and key buses to the full block size.

- **CAESAR LW Package allows for bus widths of 8 and 16 bits, which are not currently supported by CAESAR HS Package.**
  - The CAESAR LW-Package reduces the design time for LW implementations.
  - The CAESAR LW Package will be included in the next release of the Development Package for the CAESAR Hardware API.
  - The usage will be documented in the next release of the Implementer’s Guide to the CAESAR Hardware API.

## Acknowledgment

The CAESAR Lightweight Support Package was developed in collaboration with Fabio De Santis and Michael Tempelmeyer from Technische Universität München.

## References