ASCON-F

ASCON Authenticated Encryption & Hashing Engine

The ASCON-F IP core is a compact, high-throughput hardware engine implementing the lightweight authenticated encryption with associated data (AEAD) and hashing algorithms described in the Ascon v1.2 specification.

A single instance of the ASCON-F IP core can encrypt or decrypt data using the Ascon-128 and Ascon-128a functions or perform Cryptographic hashing Hash per the Ascon-Hash and Ascon-Hasha functions. The mode of operation (encryption or decryption, and Ascon function), as well as the encryption key and nonce values, are run-time programmable and can be changed per block of input data. The core uses simple input and output interfaces, that can be optionally bridged to AXI4-Stream, or to AXI4 Memory Mapped master or slave ports using bridges separately available from CAST.

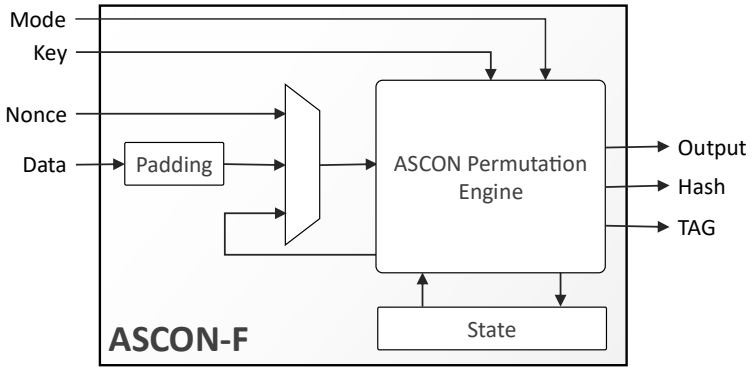
The core synthesizes to approximately 11k gates and is able to run at frequencies exceeding 2 GHz in modern ASIC technologies. Ignoring overheads related to input padding and core initialization, the throughput ranges from 5.3 to 16 bits/cycle depending on the mode and function, which at 2 GHz translates to 10.6 to 32 Gbps. The processing throughput can be further scaled by instantiating the core multiple times.

The core is designed for ease of use and integration and adheres to industry-best coding and verification practices. Technology mapping and timing closure are trouble-free, as the core contains no multi-cycle or false paths and uses only rising-edge-triggered D-type flip-flops, no tri-states, no SRAMs, and a single-clock/reset domain.

About ASCON

The ASCON family of algorithms was developed by Graz University of Technology, Infineon Technologies, Lamarr Security Research, and Radboud University and was selected in February 2023 by the US National Institute of Standards and Technology (NIST) as the new standard for lightweight cryptography. Learn more online at NIST, Wikipedia, and the Ascon website by Graz University of Technology.

Block Diagram



FEATURES

- Authenticated Encryption and Hashing per NIST submitted specification Ascon v1.2
  - Ascon-128 and Ascon-128a authenticated encryption/decryption
  - Ascon-Hash & Ascon-Hasha hash functions
  - Ascon-Xof, Ascon-Xofa, and Ascon-80pq on request
- Run-time selectable operation mode, encryption key and nonce

Compact and Fast

- Approximately 11,000 eq. gates
- More than 2GHz on modern ASIC technologies
- Throughput without any initialization and padding overhead:
  - Ascon-128: 10.6 bits/cycle
  - Ascon-128a: 16 bits/cycle
  - Ascon-Hash: 5.3 bits/cycle
  - Ascon-Hasha: 8 bits/cycle

Easy to integrate & implement.

- Fully synchronous, uses only the rising clock-edge, single-clock domain, no false or multicycle timing paths, scan-ready, LINT-clean
- Simple input and output interface, optionally bridged to AMBA® interfaces or integrated with a DMA engine.
- Available VHDL or Verilog source code format, or as a targeted FPGA
- Soft, technology-agnostic IP core directly synthesizes to any FPGA or ASIC technology

Deliverables

The core is available in RTL source or as a targeted FPGA netlist. It is delivered with everything required for a successful implementation, including a sophisticated, self-checking HDL Testbench, a behavioral C Model & test vector generator, and comprehensive documentation.

Export Permits

This core implements encryption functions and as such it is subject to export control regulations. Export to your country may or may not require a special export license. Please contact CAST to determine what applies in your specific case.

Applications

Implementing the Ascon family of lightweight authenticated ciphers and hash functions, the core can be used to protect edge IoT devices, secure communications or video surveillance systems, and encrypt data storage.

Implementation Results

The ASCON-F IP core can be mapped to any ASIC technology or FPGA device. The following are sample ASIC pre-layout results reported from synthesis with a silicon vendor design kit under typical conditions, with all core I/Os assumed to be routed on-chip.

ASIC Technology	Logic (eq. gates)	Memory (bits)	Freq. (MHz)
TSMC 7nm	10,544	0	2,300
TSMC 16nm	10,584	0	2,150
TSMC 28nm HPC	11,283	0	1,900

The provided figures do not represent the higher speed or smaller area for the core. Please contact CAST to get characterization data for your target configuration and technology.