Ascon Hash256/XOF128 IP Core

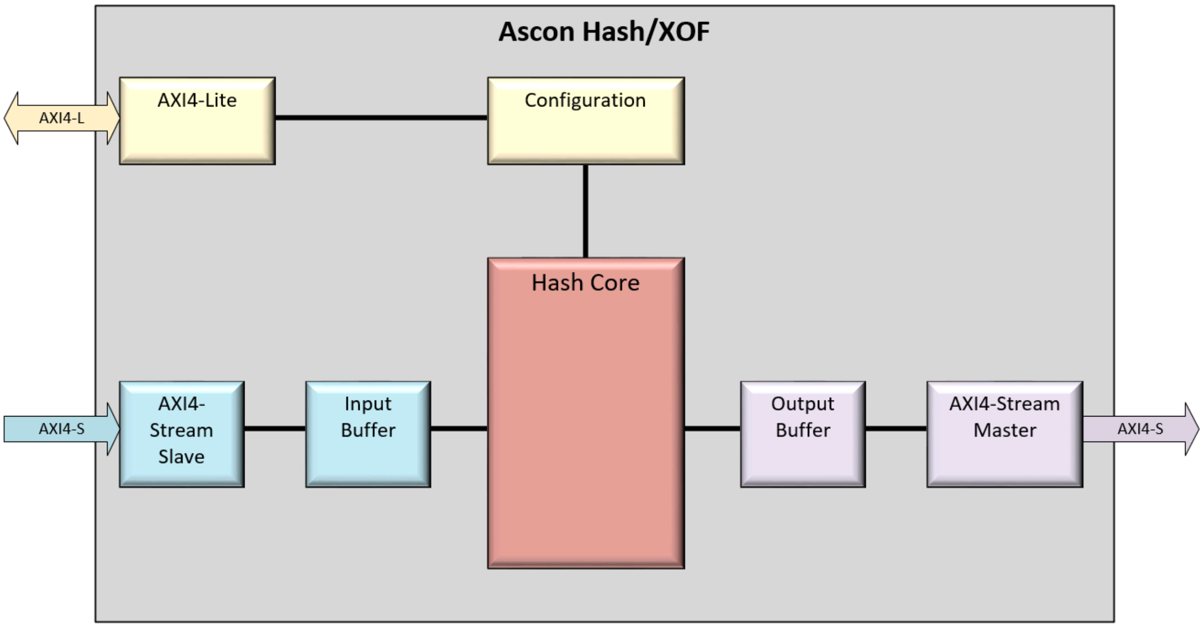
High-Efficiency, Lightweight Cryptographic Hashing for Secure Data Integrity Verification

Overview

The Ascon-HASH/XOF is a high-efficiency, silicon-proven hardware IP core that implements both the Ascon-HASH256 fixed-length hash algorithm and the Ascon-XOF128 extendable-output function (XOF), as specified in the NIST Lightweight Cryptography Standard (2023). Designed for seamless integration into System-on-Chip (SoC) architectures, this dual-mode core provides robust data integrity verification, collision-resistant cryptographic hashing, and variable-length output generation for high-speed data streams with minimal resource footprint and low latency.

It is the ideal solution for secure hash generation, digital signatures, and data integrity verification in constrained environments such as IoT edge devices, embedded systems, automotive networks, and aerospace applications, where performance, power, and area (PPA) are critical.

Block Diagram



Key Features & Benefits

Feature	Benefit
NIST Standard Compliance	Implements the certified, future-proof Ascon-128 algorithm, ensuring interoperability and regulatory acceptance.
AXI4-Stream Interfaces	Plug-and-play integration with modern SoC dataflow architectures. Simplifies connection to DMA controllers, communication IPs, and processors.
AXI4-Lite Control Interface	Standard, simple register programming model for easy CPU control and integration.
High Degree of Configurability	Tailor the IP to your exact performance, area, and security requirements. Optimize for your target technology node and application.
Side-Channel Resistance	Optional **Random Delay** feature disrupts timing patterns, providing a hardened layer of defense against simple power and timing analysis (SPA/STA).
Multi-Context Operation	Up to 4 independent configuration sets (Message length, Mode) allow instant switching between different security contexts or data streams without software overhead.
High-Throughput Task Queue	Submit up to 16 hash tasks in a single burst, freeing the software to perform other operations and maximizing data movement efficiency.
Small & Efficient	Exceptionally low resource utilization (see below) makes it suitable for the most area-sensitive designs without sacrificing performance.

Performance & Utilization Summary

The following resource utilization is for a minimally configured instance (prioritizing smallest area) synthesized for a typical FPGA target.

Resource Type	**Utilized**
Slice LUTs	1,060
Slice Registers	1,181
Bonded IOBs	162

Note: Utilization will scale with configuration choices (e.g., higher `RNDS_PER_CLK`). *The above figures demonstrate the core's inherently lightweight nature.*

Technical Specifications

Interfaces

- Data Plane: AXI4-Stream
    - Separate slave (input) and master (output) interfaces.
    - Configurable data width (`AXIS_DATA_WIDTH`): 32 or 64 bits.
    - Supports packetized data with `TLAST` signal.
- Control Plane: AXI4-Lite
    - Standard slave interface for CPU control.
    - Used to program the Message Length, and task queue.

Key Configuration Parameters (Pre-Synthesis)

Parameter	**Description**
`HASH_VARIANT`	Hash128 or XOF128
`LOG2_DATA/HASH_LEN`	Max length (in bits) for Message/Hash (when XOF128 variant is selected).
`SHADOW_REGS`	Defines the number of independent configuration register sets (1 to 4). Each set contains a complete configuration (Message Length, Control settings), enabling instant context switching for different data streams.
`MAX_TASKS`	Defines the depth of the internal encryption task queue (1 to 16). This allows the software to submit multiple hash tasks in a single burst, improving overall throughput and software efficiency.
`RNDS_PER_CLK`	Number of Ascon rounds computed per clock cycle. A higher value increases throughput at the cost of increased logic area. The optimal choice depends on the target device's speed and the area budget.
`RANDOM_DELAY`	Introduces random stalls to thwart side-channel attacks.
`INPUT/OUTPUT_BUF_LINES`	FIFO depth for clock domain crossing and rate matching.

Typical Use Cases

- IoT Device Authentication: Generating cryptographic fingerprints for sensor data, ensuring integrity in transmission from edge devices to cloud platforms.
- Automotive Data Integrity: Protecting critical vehicle data, such as diagnostic logs, sensor readings, and configuration files, against tampering in automotive Ethernet.
- Digital Evidence Chain-of-Custody: Creating immutable cryptographic hashes for digital forensic data, audit logs, and legal evidence storage systems.
- Healthcare Device Integrity: Verifying the integrity of medical device outputs, patient data records, and regulatory

compliance logs in portable medical equipment.

Why Choose This IP Core?

1. Proven Standard: Built on the NIST-selected Ascon algorithm, guaranteeing long-term viability and security.
2. Architectural Flexibility: From a tiny, sequential (`RNDS_PER_CLK=1`) core to a high-throughput, unrolled (`RNDS_PER_CLK=4`) version, you pay only for the performance you need.
3. Designed for Integration: Industry-standard AXI interfaces drastically reduce integration time and risk.
4. Security by Design: The optional Random Delay feature provides a tangible defense against a major class of physical attacks.
5. Superior System Efficiency: The integrated task queue decouples the processor from the encryption engine. Your software can queue a stream of data and return to other tasks, significantly reducing CPU overhead, leading to higher overall system performance.
6. Silicon-Efficient: The hierarchical utilization report confirms a lean and optimized design, preserving precious silicon real estate for your application logic.
7. Thoroughly Verified: 98% statement coverage, 91% branch coverage.

Getting Started

We provide the complete, synthesizable RTL source code (Verilog), a comprehensive testbench with verification suite, and detailed integration documentation.

Contact us today to discuss your specific requirements, request a datasheet for your target technology node, or to license the Ascon-HASH/XOF IP core.

Disclaimer: *Ascon is a NIST-standardized algorithm. This IP core is a hardware implementation of that algorithm. Performance and utilization figures are representative and will vary based on target technology, synthesis tools, and configuration settings.*