StealthSHA

SHA-2 and SHA-3 Hash, HMAC and KMAC Engine

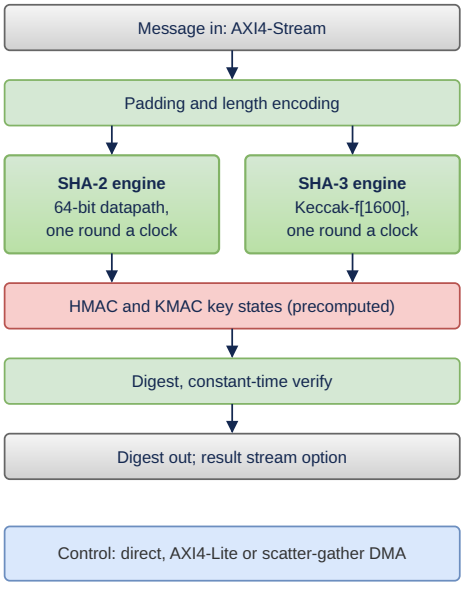
Every SHA-2 and SHA-3 hash function, SHAKE and cSHAKE, and HMAC and KMAC in hardware, in one compact core at one round per clock, with the same interfaces and DMA framework as StealthAES.

18.4 Gbps	4.68 Gbps	FIPS 180-4 · 202
Peak SHA3-256 Throughput	Peak SHA-512 Throughput	Complete SHA-2 and SHA-3 Families

All major FPGAs and ASICs. **AMD** Versal, UltraScale+, UltraScale and 7 Series · **Microchip** PolarFire, PolarFire SoC, SmartFusion 2 and IGLOO2 · **Altera** Agilex, Arria 10, Stratix 10 and Cyclone 10 · RTL optimized for ASIC implementation

Key Features

- **Complete SHA-2 Family**
  SHA-224/256/384/512, SHA-512/224 and /256
- **Complete SHA-3 Family**
  SHA3-224 to 512, SHAKE128/256 and cSHAKE
- **HMAC and KMAC in Hardware**
  Key state precomputed at key load
- **One Round per Clock**
  SHA-2 and SHA-3 at full rate per stream
- **Digest Verification**
  Constant-time compare with an expected MAC
- **Easy Integration**
  AXI4-Stream; direct, AXI4-Lite or DMA control
- **Zeroization**
  Key states and buffers, on command or reset
- **Configurable**
  SHA-2, SHA-3 or both; algorithm subsets



Applications

Secure Boot & Firmware
- Image hashing
- Firmware authentication
- Measured boot
- Update integrity

Protocols & Keys
- HMAC for IPsec and TLS
- KMAC message authentication
- Key derivation
- Custom protocols

Post-Quantum & Storage
- SHAKE expansion for PQC
- Bulk data integrity
- PCIe offload
- Storage authentication

StealthSHA Product Overview

Technical Specifications

Hash	SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256 (FIPS 180-4); SHA3-224, SHA3-256, SHA3-384, SHA3-512 (FIPS 202), selected per operation
XOF	SHAKE128, SHAKE256 (FIPS 202) and cSHAKE128, cSHAKE256 (SP 800-185)
MAC	HMAC (FIPS 198-1) and KMAC128, KMAC256 (SP 800-185), generation and constant-time verification
Throughput	One round per clock: up to 3.19 Gbps (SHA-256), 4.68 Gbps (SHA-512), 18.4 Gbps (SHA3-256) and 22.7 Gbps (SHAKE128) per stream
Interfaces	AXI4-Stream input and output; direct, AXI4-Lite or scatter-gather DMA control
Verification	A test suite including NIST CAVP test vectors

Area and Performance

		AMD Versal AI Edge		Microchip PolarFire SoC		Altera Agilex 5	
Algorithms	**Algorithm**	Throughput	Logic	Throughput	Logic	Throughput	Logic
SHA-224/256	SHA-256	3.19 Gbps	3454 LUT6	1.73 Gbps	5731 4LUT	2.09 Gbps	2707 ALM
SHA-384/512	SHA-512	4.68 Gbps	5904 LUT6	2.40 Gbps	9529 4LUT	2.72 Gbps	4278 ALM
SHA-2 family	SHA-512	4.11 Gbps	6410 LUT6	2.02 Gbps	11692 4LUT	2.53 Gbps	4639 ALM
SHA-3 family	SHA3-256	18.4 Gbps	7263 LUT6	8.16 Gbps	13432 4LUT	12.7 Gbps	6606 ALM
SHA-2 and SHA-3	SHA3-256	13.4 Gbps	12743 LUT6	6.80 Gbps	25248 4LUT	9.97 Gbps	9983 ALM

Post-place-and-route results for the core alone on a mid-range device of each family; results vary with device, tools and design.

Why Choose StealthCores?

Standards Verified
A test suite including NIST CAVP vectors for every algorithm family.

Seamless Integration
StealthAES's interfaces and DMA framework, Verilog and VHDL.

Expert Support
Decades of cryptographic experience, with dedicated integration support.

Mission-Critical Reliability
Designed for commercial, industrial, and defense applications.

Ready to Add Hashing and Authentication?

info@stealthcores.com | www.stealthcores.com | © 2026 StealthCores

Rev. 2026.1.0