The SHA-3 - secure hash algorithms - crypto engine is a hardware accelerator for cryptographic hashing functions. It is an area efficient and high throughput design and compliant to NIST's FIPS 202 standard. Additionally it supports all SHA-3 hash functions - SHA-3-224, SHA-3-256, SHA-3-384 and SHA-3-512 - as well as extendable output functions (XOF) - SHAKE-128 and SHAKE-256. It provides full protection against time-based side channel attacks (SCA). Automatic bit and byte padding is included.
The SHA-3 crypto engine is an IP core and built with a focus on simplicity and seamless integration, while also following coding and verification practices in the industry. It operates in a single clock domain and has been extensively verified.
The SHA-3 IP core offers a versatile solution for maintaining data integrity and verifying authentication across various applications. Its applications span a wide range, including Message Authentication Codes (MAC), IPsec and TLS/SSL protocol engines, secure boot engines, encrypted data storage, e-commerce platforms, financial transaction systems, blockchain, or pseudo random bit generation.

Key Features

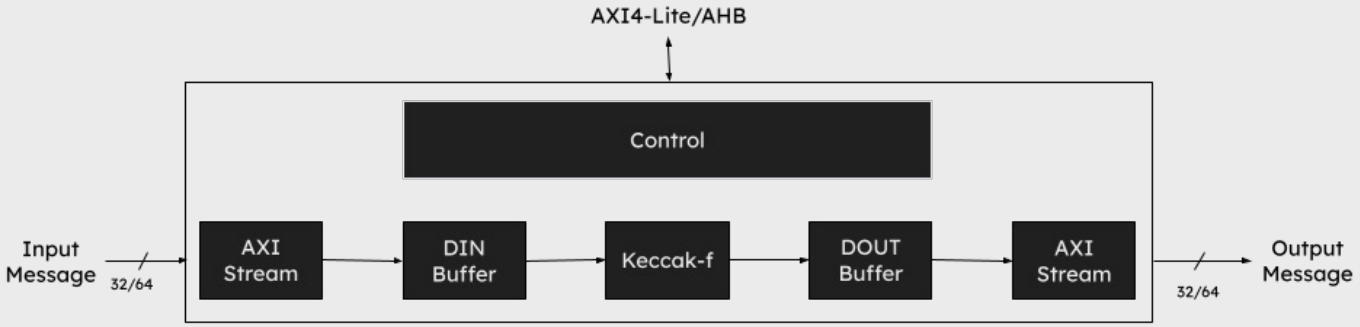
- FIPS 202 compliant
- Supports cryptographic hashing for SHA-3 in 224/256/384/512 mode
- Extendable-Output Functions for SHAKE 128/256
- AMBA® AXI4-Stream
- Fully synchronous design
- For any FPGA and ASIC

Deliverables

- System Verilog RTL Source Code
- Testbenches
- Integration examples
- Software example source code
- Documentation

Licensing

- One-time license fee
- Single or multi project license



Block Diagram

Device	Logic	FF	fmax	Max. Throughput
AMD Spartan 7	8165 LUTs	2810	174 MHz	11.4 Gbps
AMD Kintex-7 series	8151 LUTs	2811	258 MHz	16.5 Gbps
AMD Zynq MPSoC US+	8152 CLBs	2811	331 MHz	21.2 Gbps
Efinix Titanium	8459 LUT4	2778	391 MHz	25.0 Gbps
Effinix Trion	8459 LUT4	2778	90 MHz	5.8 Gbps
Lattice Avant E	11301 LUT4	2790	131 MHz	8.4 Gbps
Lattice CertusPro-NX	11948 LUT4	2804	149 MHz	9.5 Gbps
Lattice Certus-NX	11948 LUT4	2804	149 MHz	9.5 Gbps

Utilization and Performance

KiviCore GmbH
Gostritzer Straße 611
01217 Dresden
Germany
info@kivicore.com
+49 351 871 9801