

Secure Hash Algorithm IP Core

The KiviHash-SHA-3 (secure hash algorithms) 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. 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 byte padding is included. It operates in a single clock domain and has been extensively verified.

Key Features

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

Easy Integration

- AMBA® AXI4 lite Interface
- Platform agnostic C source code HAL, API and software driver
- Software examples and software user guide included
- Integration examples included
- Comprehensive technical documentation

Applications

- Firmware Updates: Detecting tampered or corrupted update packages
- FPGA bitstreams: Ensuring only trusted configurations are loaded
- External memory integrity: Protecting stored data in flash or external RAM

Test And Verification

- NIST CAVS test vectors for SHA3 hash functions
- NIST CAVS test vectors for SHA3 XOF functions
- Extended verification through simulation
- FPGA integration and implementation tests
- Unity tests for driver and whole IP Core

Support and Maintenance

- Maintenance and updates of IP core included
- Rapid bug fix cycles
- Documentation and integration examples included
- Web based support with response times of 8 hours (Mo to Fri)

Product License Deliverables

- System Verilog RTL Source Code or Netlist format
- Testbenches
- Integration examples
- Simulation and synthesis scripts
- Software HAL & driver source code
- Software example source code
- Documentation

Evaluation License Deliverables

- Netlist format, time-bombed
- Testbenches
- Integration examples
- Software HAL & driver source code
- Software example source code
- Documentation

Evaluate KiviHash-SHA3

Register for the Evaluation Portal to access the evaluation package, technical documentation and integration resources.

[Get access](#)

FPGA Implementation Results

AMD (Xilinx)

Device	LUTs	max. Frequency (MHz)	max. Throughput (Gbps)
Spartan 7	7687	171.5	8.4
Kintex 7	7722	258.5	12.4
Zynq US+ MPSoC	7730	340.5	16.3
Versal AI Cores Series	7572	427.4	20.5

Efinix

Device	XLR	max. Frequency (MHz)	max. Throughput (Gbps)
Titanium	9246	375.7	18.0
Topaz	9246	234.6	11.3
Trion	9246	102.9	4.9

Contact

KiviCore GmbH
Gostritzer Straße 61
01217 Dresden
Germany

+49 351 871 9801
info@kivicore.com