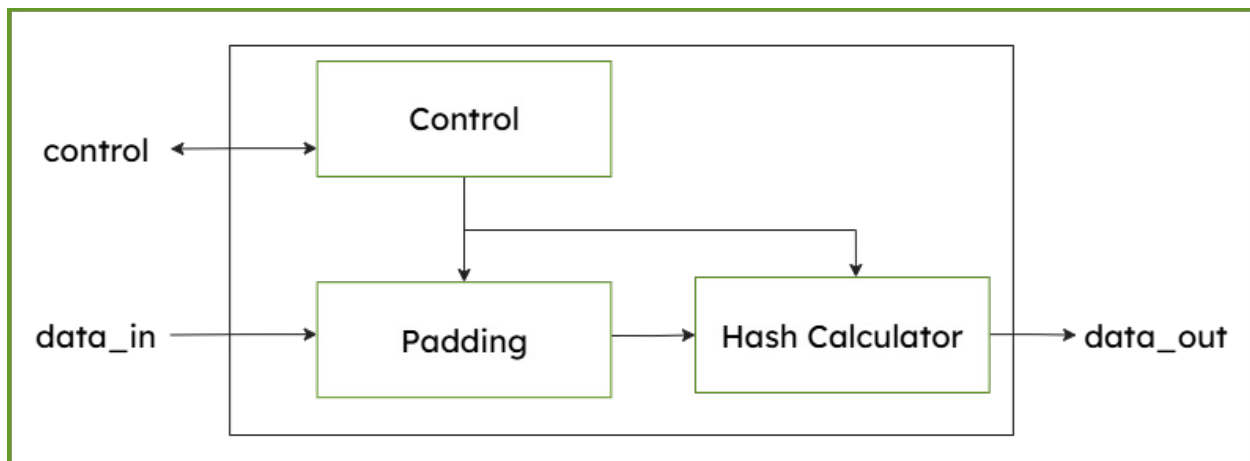


## KiviHash-SHA3 Secure Hash Algorithm (256)

KiviHash-SHA-256 is an IP core implementing the SHA-256 cryptographic algorithm, an one-way hash function compliant to NIST's FIPS 180-4 standard. It is optimized for high speed designs and easy integration with any FPGA and ASIC designs. Automatic byte padding is included. It features a standard AMBA® AXI4-Lite interface for straightforward hardware integration and HAL, and software driver (C-code, platform independent) for simple software integration.



### Key Features

- NIST FIPS 180-4 compliant
- Supports cryptographic hashing for SHA-256 mode
- Automatic padding
- High-speed design
- AMBA® AXI4-Lite interface
- Fully synchronous design
- HAL and software driver (C-code, platform independent)
- For any FPGA and ASIC

### Applications

- Firmware Updates: Detecting tampered or corrupted update packages
- FPGA bitstreams: Ensuring only trusted configurations are loaded
- Communication protocols: TLS, IPsec, MAC-based authentication
- External memory integrity: Protecting stored data in flash or external RAM

## Test and Verification

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

## Licensing & Services

- Product license
  - One-time license fee
  - Single or multi project license
- Evaluation license available
- Technical support by email
- Maintenance & updates

## Easy integration

- AMBA® AXI4-Lite interface
- Platform agnostic C source code HAL, API and software driver
- Software examples included
- Software user guide

## Deliverables

- Product license
  - System Verilog RTL Source Code or Netlist format
- Evaluation license
  - Netlist format, time bombed
- Testbenches
- Integration examples
- Software HAL & driver source code
- Software example source code

## FPGA Implementation Results

AMD	Logic (LUTs)	fmax (MHz)	Max. Throughput (Gbps)
Spartan 7	1685	191.4	1.53
Kintex 7	1689	308.6	2.47
Zync MPSoC Us+	1822	473.7	3.79
Versal AI Cores Series	1761	496.8	3.97

Efinix	Logic (XLR)	fmax (MHz)	Max. Throughput (Gbps)
Titanium	3067	404.9	3.24
Topaz	3067	286.5	2.29
Trion	3067	116.2	0.93