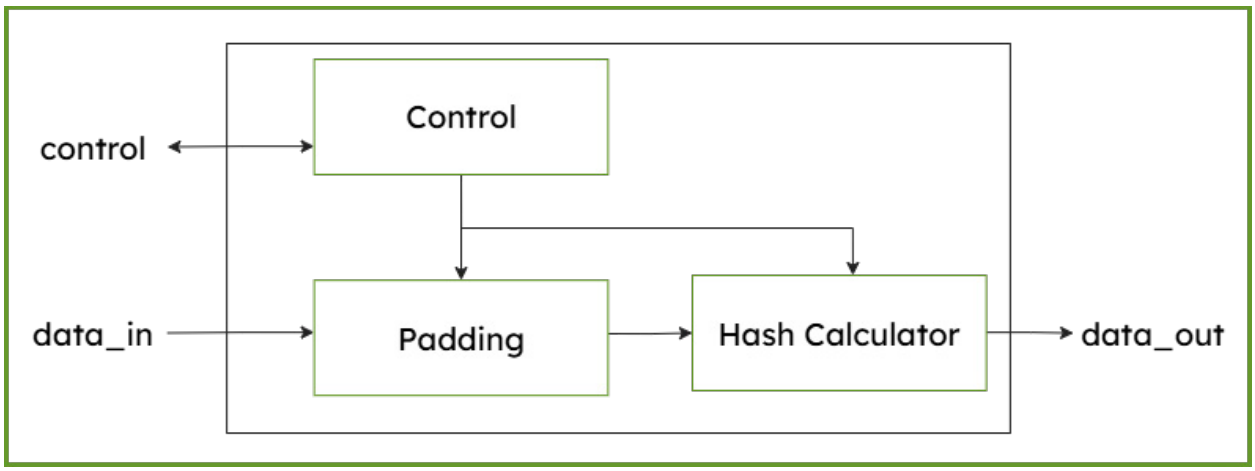
# KiviHash-SHA3

KiviCore

IP Core Product Brief 20260318

## KiviHash-SHA3 Secure Hash Algorithm (224/256/384/512 )

The KiviHash-SHA3 (secure hash algorithms) is a hardware accelerator for cryptographic hashing functions. It is an area efficient, 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
- HAL and software driver (C-code, platform independent)
- For any FPGA and ASIC

### Applications

- Boot chains: Verifying firmware integrity from root of trust to application
- 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

## 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 source code
- Software user guide

## Deliverables

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

## FPGA Implementation Results

| Efinix | Logic (XLR) | fmax (MHz) | Max. Throughput (Gbps) |
|---|---:|---:|---:|
| Titanium | 9246 | 375.7 | 18.0 |
| Topaz | 9246 | 234.6 | 11.3 |
| Trion | 9246 | 102.9 | 4.9 |