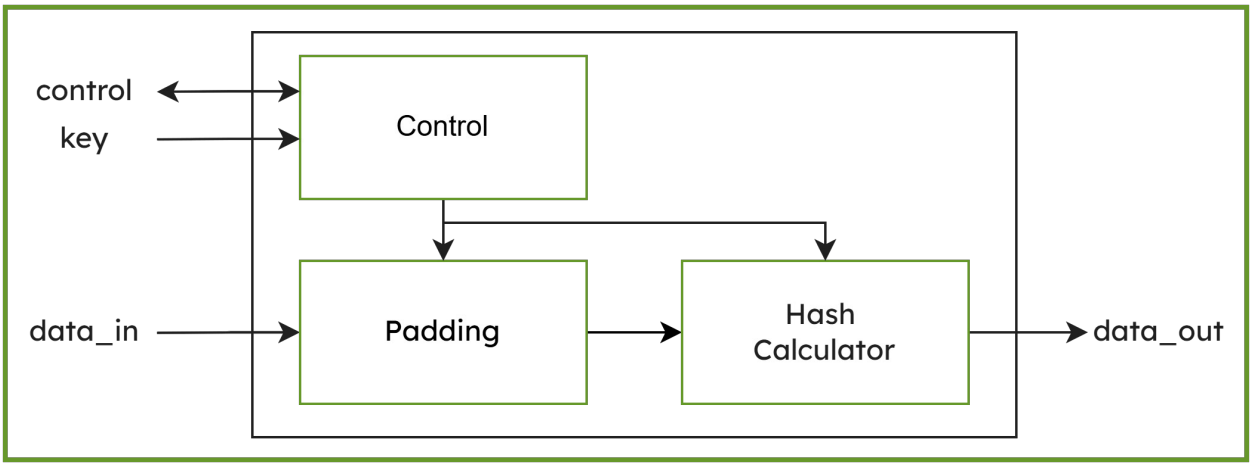
KiviHash-HMAC-SHA256

KiviCore

IP Core Product Brief 20260325

KiviHash-HMAC-SHA256 | Secure Keyed-Hash Message Authentication Code IP Core

The HMAC SHA-256 IP core enables secure Keyed-Hash Message Authentication Code (HMAC) generation using the SHA-256 algorithm. The IP core is compliant to NIST FIPS 198-1 and NIST SP 800-224. It features automatic padding and a high-speed architecture optimized for efficient processing in embedded systems. The core is designed as a fully synchronous module and supports integration via an AMBA® AXI4-Lite interface. To simplify system integration, it is delivered with a hardware abstraction layer (HAL) and platform-independent C-based software drivers. The design can be deployed on a wide range of FPGA and ASIC platforms.



Key Features

- NIST FIPS 198-1 and NIST SP 800-224 compliant
- Supports HMAC using SHA-256
- 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

Easy integration

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

Applications

- Boot chains: Verifying firmware integrity from root of trust to application
- Firmware Updates: Protection against unauthorized updates

Test and Verification

- Extended verification through simulation
- FPGA integration and implementation tests
- Unity tests for driver and whole IP Core

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
- Documentation

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