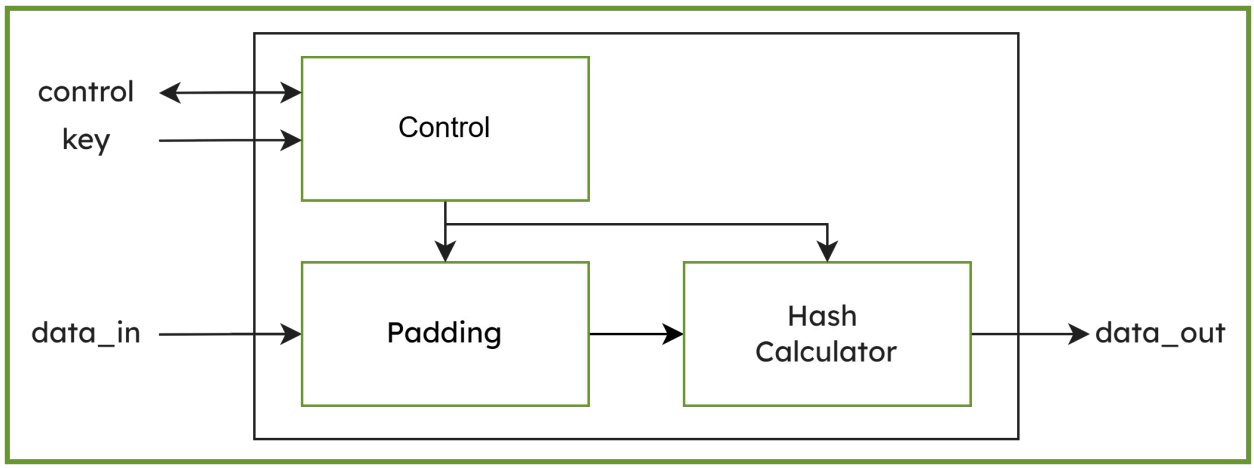
KiviHash-HMAC-SHA512

KiviCore

IP Core Product Brief 20260325

KiviHash-HMAC-SHA-512 | Secure Keyed-Hash Message Authentication Code IP Core

The HMAC SHA-512 IP core enables secure Keyed-Hash Message Authentication Code (HMAC) generation using the SHA-512 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 optionally 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 Keyed-Hash Message Authentication Code (HMAC) using SHA-512
- Supports HMAC for SHA-512, SHA-384, SHA-512/256
- Automatic padding
- High-speed design
- 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

Test and Verification

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

Applications

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

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	3415	157.3	2.52
Kintex 7	3418	267.5	4.28
Zync MPSoC Us+	3505	361.8	5.79
Versal AI Cores Series	3210	446.4	7.14

Efinix	Logic (XLR)	fmax (MHz)	Max. Throughput (Gbps)
Titanium	6018	285.1	4.56
Topaz	6018	198.7	3.18
Trion	6018	79.3	1.27