

May 2026

OVERVIEW

The Keccak IP core supports Keccak-based hash functions, including the SHA3 and SHAKE families. It is fully compliant with the NIST's SHA3 standard and incorporates countermeasures against Side-Channel Analysis attacks (e.g., masking).

FEATURES LIST

- i. FIPS-202 compliant.
- ii. Algorithms supported (but not limited to):
 - SHA3-224
 - SHA3-256
 - SHA3-448
 - SHA3-512
 - SHAKE128
 - SHAKE256
 - cSHAKE
 - KMAC
- iii. Run-time configurable rate (Keccak's parameter).
- iv. Multiple context support (parallel hash computations).
 - v. Design-time configurable area-time trade-off parameter.
- vi. Improved parallelism with FIFO.
- vii. Optional Side-Channel Analysis and Fault Injection attacks countermeasures (e.g., masking)
- viii. AXI4 interface for system integration and drivers available upon request.

DELIVERABLES

- Encrypted Netlist.
- Synthesis Scripts.
- Comprehensive Documentation.
- Drivers upon request.

MAINTENANCE & SUPPORT

- M&S fee of 15% is mandatory for the first year.
- Telephone and email support is included under M&S agreement.
- IP Core updates are included in M&S.

Technology Partner



Keccak IP Core

LICENSING

Following licensing models are available:

- Encrypted Netlist
- Encrypted RTL

ORDERING

Purchase order shall include the product number EIP-30010001.

FPGA SYNTHESIS RESULT

Family/Device	SCA+FI Countermeasures	LUT	FF	DSP	BRAM
Zynq/xc7z020clg400-1	No	4792	3455	0	0
	Yes	9777	7626	0	0

BLOCK DIAGRAM

