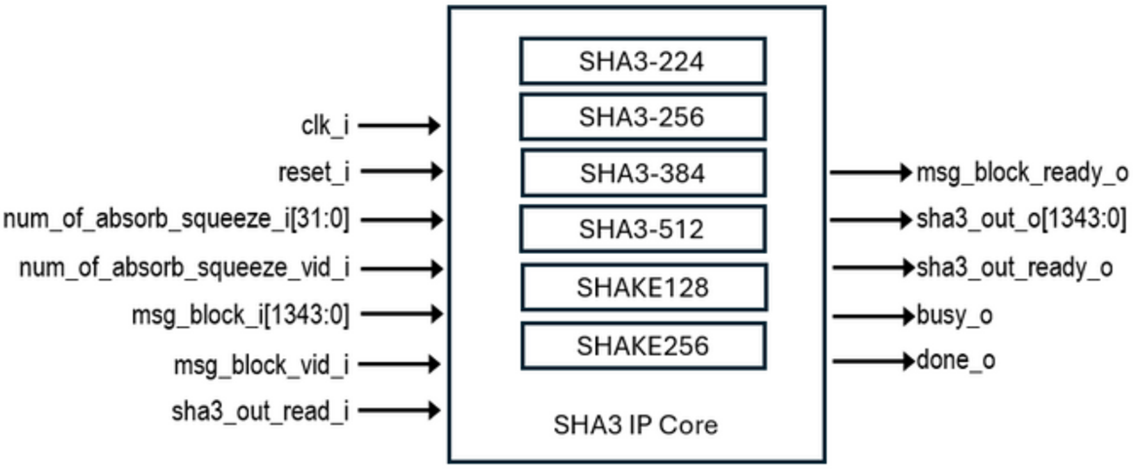
SHA3 IP Core
Datasheet

November 2024

OVERVIEW

SHA3 IP Cores perform cryptographic hashing in compliance with the SHA-3 (Secure Hash Algorithm 3) specifications defined in 'FIPS 202'. This standard specifies methods for generating secure hash values using the SHA-3 algorithm.

SHA3 IP Cores support the SHA3-224, SHA3-256, SHA3-384, SHA3-512, SHAKE128, and SHAKE256 functions, and are byte-oriented in their implementation. VHDL is used as the Hardware Description Language of the IP Core. AXI4-Stream interface can be designed and provided upon request.



DELIVERABLES

- Encrypted Netlist
- Synthesis Scripts
- Comprehensive Documentation
- SHA3 Validation SystemTestbenches in SystemVerilog

FEATURES LIST

SHA3 IP Core:

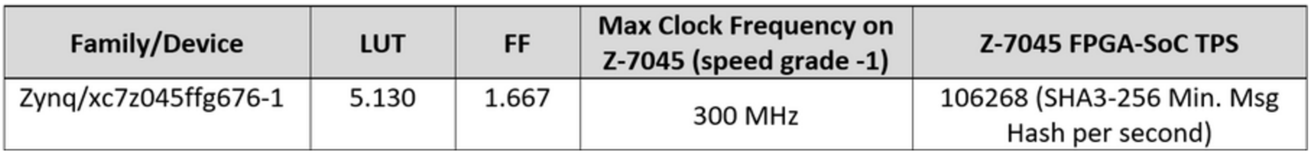
- supports hashing for functions listed below:
  - *SHA3-224*
  - *SHA3-256*
  - *SHA3-384*
  - *SHA3-512*
  - *SHAKE128*
  - *SHAKE256*
- is compliant with FIPS 202.
- is tested on Z-7015 Z-7020 Z-7045
- has fully stallable input and output interfaces.

Technology Partner

SHA3 IP Core

FPGA SYNTHESIS RESULTS

The FPGA resources requirements:



Family/Device	LUT	FF	Max Clock Frequency on Z-7045 (speed grade -1)	Z-7045 FPGA-SoC TPS
Zynq/xc7z045ffg676-1	5.130	1.667	300 MHz	106268 (SHA3-256 Min. Msg Hash per second)

LICENSING

A one-time license fee is paid with the initial IP purchase.

- Single project license
- Multi project license

MAINTENANCE & SUPPORT

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

ORDERING

- Purchase order shall include the product number EIP-13009.

Technology Partner