SHA3

SHA3/KMAC/SHAKE Hash Cores

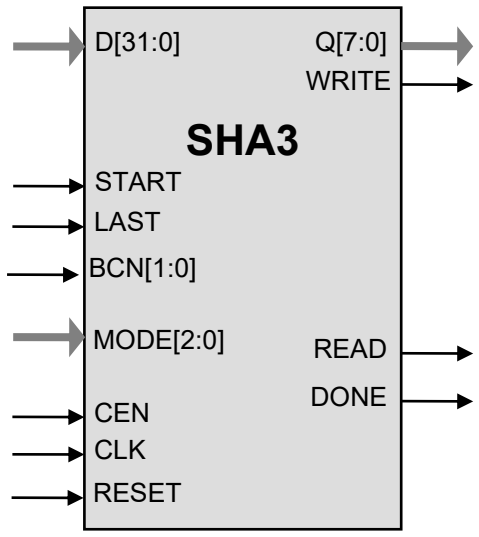
General Description

The SHA3 cores provide implementation of cryptographic hashes "Keccak" SHA-3 (cores SHA3-224, SHA3-256, SHA3-384 and SHA3-512) and (optionally) the corresponding hash-based HMAC, KMAC, and XOF (SHAKE) functions.

The cores utilize "flow-through" design that can be easily included into the data path of a communication system or connected to a microprocessor: the core reads the data via the D input and outputs the hash result via its Q output. Data buses for both D and Q are 32-bit wide; other configurations are available.

The design is fully synchronous and is available in both source and netlist form.

Symbol



Key Features

Completely self-contained; does not require external memory

SHA3-224, SHA3-256, SHA3-384, and SHA3-512 support SHA-3 algorithms per FIPS 202.

SHAKE128 / SHAKE256 XOF support is included.

Flow-through design; flexible data bus width

Test bench provided

Applications

- Post-quantum cryptography (PQC)
- Message digest and calculation
- Digital signature (DSA) algorithm of the Digital Signature Standard (DSS) per FIPS-186
- Key derivation function (HKDF per RFC RFC 9688)
- KMAC128 or KMAC256 as defined in Section 4.4 of NIST.SP.800-108r1-upd1
- Security protocols, including
  - S/MIME (PKCS #1, RFC 9688)
  - IPSec

Pin Description

Name	Type	Description
CLK	Input	Core clock signal
CEN	Input	Synchronous enable signal. When LOW the core ignores all its inputs and all its outputs must be ignored.
START	Input	HIGH starting input data processing
READ	Output	Read request for the input data word
DONE	Output	HIGH after the completion of the operation. Brought LOW by de-assertion of the **start**
RESET	Input	Asynchronous reset (for simulation purposes). Core will operate correctly if **reset** is never asserted.
LAST	Input	Marks the last byte of data
WRITE	Output	Write to the output interface
MODE[2:0]	Input	Mode of operation
D[31:0]	Input	Input Data
BCN[1:0]	Input	Number of bytes in the last word
Q[31:0]	Output	Output Hash Data

Function Description

The SHA-3 algorithms process data in block of different size that depends on the particular algorithm:

Hash	Block size ("bitrate")
SHA3-224	1152
SHA3-256	1088
SHA3-384	832
SHA3-512	576

The Secure Hash Standard (SHA-3) is a message digest standard as defined in the FIPS-202 publication http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf .

The core is designed for flow-through operation. The input data can contain any number of bytes up to 2^{29} (data padding is performed inside the core). The output data is the 224/256/384/512-bit hash or HMAC value.

Deliverables

HDL Source Licenses

- Synthesizable Verilog RTL source code
- Testbench (self-checking)
- Vectors for testbench
- Expected results
- User Documentation

Contact Information

IP Cores, Inc.
3731 Middlefield Rd.
Palo Alto, CA 94303, USA
Phone: +1 (650) 815-7996
E-mail: info@ipcores.com
www.ipcores.com