SHA1, SHA2

Cryptographic Hash Cores

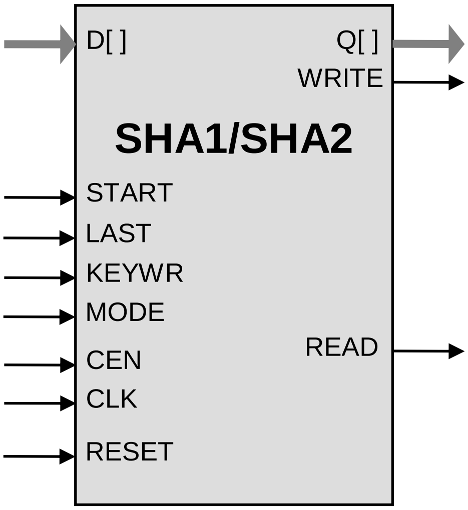
General Description

The SHA cores provide implementation of cryptographic hashes SHA-1 (core SHA1), SHA-2 (cores SHA2-256 and SHA2-512).

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 bus widths for both D and Q are parameterized.

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

SHA1 supports SHA-1 per FIPS 180-1, SHA2-256 and SHA2-512 support SHA-2 per FIPS 180-2.

HMAC option is available with flow-through and microprocessor-friendly (-SK) interfaces for the key input.

Flow-through design; flexible data bus width

Test bench provided

Applications

- Message digest calculation
- Digital signature (DSA) algorithm of the Digital Signature Standard (DSS) per FIPS-186
- Security protocols, including
  - TLS (RFC 2246, RFC 4346)
  - SSL v3
  - PGP (RFC 2440)
  - SSH (RFC 4251)
  - S/MIME (PKCS #7, RFC 3852)
  - IPSec (RFC 2404, RFC 4301)

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
RESET	Input	Asynchronous reset (for simulation)
LAST	Input	Last word of data signal (triggers hash output after processing)
WRITE	Output	Write to the output interface
KEYWR	Input	Key write signal (for HMAC –SK option)
MODE	Input	Selection between hash and HMAC operations (for HMAC option)
D[ ]	Input	Input Data Word (8/16/32 bits wide, 64 bit option for SHA2-512)
Q[ ]	Output	Output Hash Data Word (8/16/32 bits wide, 64 bit option for SHA2-512)

Function Description

The SHA algorithms process data in 512-bit blocks (SHA1, SHA2-256) or 1024-bit blocks (SHA2-512) and produce message digests consisting of 160 (SHA1), 256 (SHA2-256), and 512 bits (SHA2-512).

The Secure Hash Standard (SHA) is a message digest standard as defined in the FIPS-180-2 publication http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf .

The core is designed for flow-through operation, with flexible-width input and output interfaces.

Export Permits

The cores are subject to the US export regulations. See the IP Cores, Inc. licensing basics page, http://ipcores.com/exportinformation.htm, for links to US government sites and licensing details.

Deliverables

HDL Source Licenses

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

Netlist Licenses

- Post-synthesis EDIF
- Testbench (self-checking)
- Vectors for testbenches
- Expected results

Contact Information

IP Cores, Inc.
3731 Middlefield Rd.
Palo Alto, CA 94303, USA
Phone: +1 (650) 814-0205
E-mail: info@ipcores.com
www.ipcores.com