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.

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLK</td>
<td>Input</td>
<td>Core clock signal</td>
</tr>
<tr>
<td>CEN</td>
<td>Input</td>
<td>Synchronous enable signal. When LOW the core ignores all its inputs and all its outputs must be ignored.</td>
</tr>
<tr>
<td>START</td>
<td>Input</td>
<td>HIGH starting input data processing</td>
</tr>
<tr>
<td>READ</td>
<td>Output</td>
<td>Read request for the input data word</td>
</tr>
<tr>
<td>RESET</td>
<td>Input</td>
<td>Asynchronous reset (for simulation)</td>
</tr>
<tr>
<td>LAST</td>
<td>Input</td>
<td>Last word of data signal (triggers hash output after processing)</td>
</tr>
<tr>
<td>WRITE</td>
<td>Output</td>
<td>Write to the output interface</td>
</tr>
<tr>
<td>KEYWR</td>
<td>Input</td>
<td>Key write signal (for HMAC –SK option)</td>
</tr>
<tr>
<td>MODE</td>
<td>Input</td>
<td>Selection between hash and HMAC operations (for HMAC option)</td>
</tr>
<tr>
<td>D[ ]</td>
<td>Input</td>
<td>Input Data Word (8/16/32 bits wide, 64 bit option for SHA2-512)</td>
</tr>
<tr>
<td>Q[ ]</td>
<td>Output</td>
<td>Output Hash Data Word (8/16/32 bits wide, 64 bit option for SHA2-512)</td>
</tr>
</tbody>
</table>

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 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