

CAST

SHA1

SHA-1 Secure Hash Function Core

Features

- Compliant to the FIPS 180-1 specification for SHA-1.
- Bit padding.
- $2^{64}-1$ bits maximum message length.
- Supported Message lengths multiple of 8-bits.
- Initial values of Chaining Variables selected before synthesis.
- 82 processing cycles per message block.
- Fully stallable input and output interfaces, ideal for streaming applications.
- Optimized design for ASIC or FPGA implementations.
- Robust verification environment includes bit-accurate software model.
- Scan-ready design architecture.

The SHA1 core is a high-performance implementation of the SHA-1 Secure Hash message digest Algorithm. This one-way hash function conforms to the 1995 US Federal Information Processing Standard (FIPS) 180-1. It accepts a large, variable-length message and produces a fixed-length message authorization code.

The core is composed of two main modules, the SHA1 Engine Module and the Input Interface Module as shown in the block diagram. The SHA1 Engine Module applies the SHA1 loops on a single 512-bit message block, while the Input Interface Module performs the message padding. The processing of one 512-bit block is performed in 82 clock cycles, and the bit-rate achieved is 6.24Mbps/MHz on the input of the SHA1 core.

The SHA1 core is equipped with fully-stallable input and output interfaces. These enable the user's application to stop the input stream according to a data arrival rate, or to stop the output stream when the core is not able to receive data.

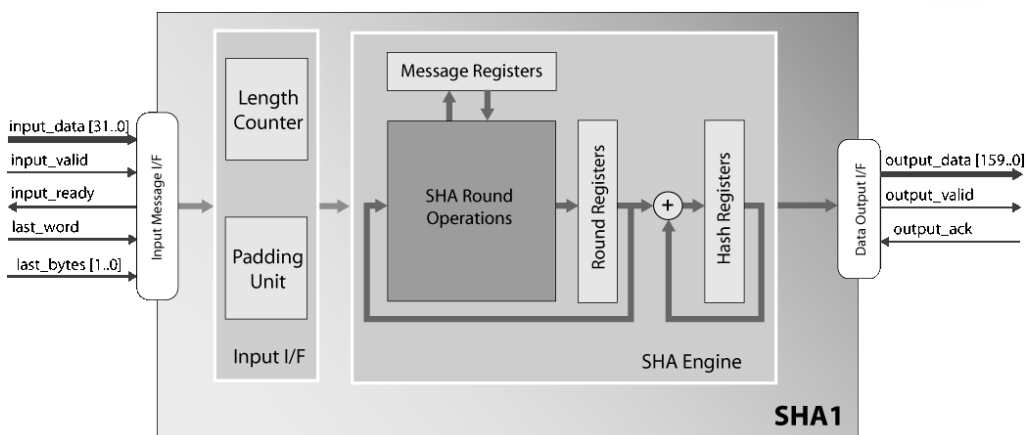
The core has been evaluated in a variety of technologies, and is available optimized for ASICs or FPGAs. Representative results show it to produce a competitive implementation, running at 350 MHz and requiring just 14,500 gates in a .18 μm ASIC process. The complete deliverables feature comprehensive documentation, and a bit-accurate software model (BAM).

Applications

The core is suitable for a variety of applications requiring digital signatures or other message origin authentication or tamper protection, including:

- E-commerce
- Data integrity
- Bulk Encryption
- High-speed networking equipment
- Secure wireless applications

Block Diagram



Functional Description

The input message data is passed in 32-bit words to the core, masked with the input_valid signal. As long as the input_ready signal is active, the external application should keep feeding input data to the core. When the core has received a complete message 512-bit packet, it pauses the input stream, and continues the message processing internally. When the message is processed and the core is ready for the next message, the core permits input data to be fed again. On the final message block, when the last 32-bit word is written, the last_word input must be activated, to indicate that a hash value has to be generated to the core's output. Along with the last_word, the last_bytes input must indicate how many bytes are valid in the last word, so that the padding unit knows how many bytes to pad.

The core can easily be modified to support programmable Initial Vectors for the Chaining Variables in place of the constants defined in the algorithm's specification.

Implementation Results

The following are representative ASIC results, with all I/Os assumed to be routed off-chip using I/O registers. Results are optimized for speed, with logic area excluding memory, and equivalent gate count using the smallest NAND2 gate available in the technology.

| ASIC Technology | Fmax (MHz) | Logic Area (μm^2) | Number of eq. gates ¹ |
|-------------------------|------------|--------------------------------|----------------------------------|
| UMC 0.18 μm | 350 | 176,856 | 14.5 K |
| TSMC 0.09 μm | 500 | 35,280 | 12.5 K |

1. Equivalent gate count uses the smallest NAND2 gate available in technology

Export Permits

This encryption technology is governed internationally by export regulations. Immediate export of the core is permitted to the following countries for uses not related to weapons of mass destruction:

| | | |
|------------------------------|-------------|---------------|
| Argentina | Japan | South Korea |
| Australia | New Zealand | Switzerland |
| Canada | Norway | Turkey |
| European Union Member States | Russia | Ukraine |
| | | United States |

Please contact CAST to discuss delivery to other destinations; approval is subject to the applicable export licenses being granted. The license can be generated from either the EU or the USA. Please note that licensees are responsible for complying with the applicable requirements for re-export of electronics containing strong encryption technology.

Support

The SHA1 core as delivered is warranted against defects for ninety days from purchase. Thirty days of phone and email technical support are included, starting with the first interaction. Additional maintenance and support options are available.

Verification

The SHA1 core has been verified through extensive simulation and rigorous code coverage measurements. It has also been verified in a prototyping FPGA board platform.

Deliverables

The SHA1 is available as a soft core (synthesizable HDL) for ASIC technologies and as a firm core (netlist) for FPGA technologies, and includes everything required for successful implementation. The Asic version includes:

- HDL (VHDL or Verilog) RTL source code.
- Synthesis scripts.
- Simulation script, vectors and expected results.
- Sophisticated self-checking Testbench (Verilog versions use Verilog 2001).
- Software (C++) Bit-Accurate Model.
- Comprehensive user documentation, including detailed specifications and a system integration guide.