

CAST



SHA256

SHA-256 Hash Function Core

Features

- Compliant to FIPS 180-2 specification of SHA-256.
- Bit padding.
- $2^{64}-1$ bits maximum message length.
- Supported Message lengths multiple of 8-bits.
- Initial values of Chaining Variables selected before synthesis.
- 66 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.

The SHA256 core is a high-performance implementation of the SHA-256 Secure Hash message digest Algorithm. This one-way hash function conforms to the 1995 US Federal Information Processing Standard (FIPS) 180-2. It accepts a large, variable-length message and produces a fixed-length message authorization code.

The core is composed of two main modules, the SHA256 Engine Module and the Input Interface Module as shown in the block diagram. The SHA256 Engine Module applies the SHA256 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 66 clock cycles and the bit-rate achieved is 7.75Mbps / MHz on the input of the SHA256 core.

The SHA256 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.

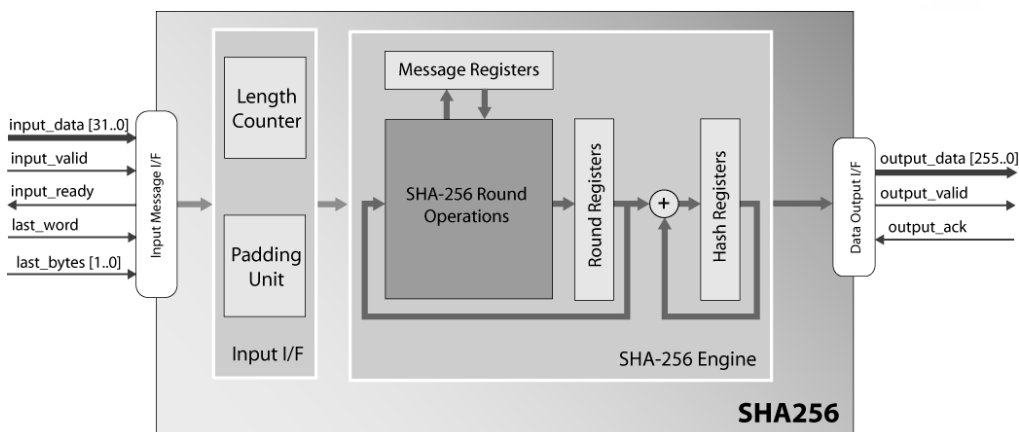
The core has been evaluated in a variety of technologies, and is available optimized for ASICs or FPGAs. Indicative results show that the core fits in a variety of Xilinx devices, requiring, for example, about 290 slices for Virtex-6. The complete deliverables feature comprehensive documentation, and 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 sample Xilinx results with all I/Os assumed to be routed off-chip.

Xilinx Device	Slices	Fmax (MHz)	I/O	BRAM	Special Features	ISE
Spartan-3 3S1000-5	1,222	66	334	1 RAMB16	-	12.2
Spartan-6 6SLX45-3	640	115	334	1 RAMB16	-	12.2
Virtex-5 5VLX30-3	480	160	334	1 RAMB36	-	12.2
Virtex-6 6VLX75T-3	287	250	334	-	-	12.2

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 SHA256 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 SHA256 core has been verified through extensive synthesis, place and route and simulation runs. It has also been verified in a prototyping FPGA board platform.

Deliverables

The SHA256 is available in ASIC (synthesizable HDL) and FPGA (netlist) forms, and includes everything required for successful implementation. The Xilinx version includes:

- Post-synthesis EDIF or NGC netlist
- Sophisticated self-checking Testbench (Verilog versions use Verilog 2001)
- Software (C++) Bit-Accurate Model and test vector generator
- Simulation scripts, test vectors and expected results
- Place and route scripts
- Comprehensive user documentation, including detailed specifications and a system integration guide