SHA-256 Secure Hash Function (SHA256)

September 14, 2007 Product Specification

CAST, Inc.
11 Stonewall Court
Woodcliff Lake, NJ 07677
USA
Phone: +1-201-391-8300
Fax: +1-201-391-8694
E-mail: info@cast-inc.com
URL: www.cast-inc.com

AllianceCORE™ Facts

Provided with Core	
Documentation	Design spec, Integration manual
Design File Formats	EDIF or NGC netlist, Verilog, VHDL
Constraints Files	sha256.ucf
Verification	Test Bench, Test Vectors
Instantiation Templates	VHDL, Verilog
Reference Designs & Application Notes	Example Design, Assembler programs
Additional Items	Software (C++) Bit-Accurate Model
Simulation Tool Used	
ModelTech's ModelSim, Cadence's NC-Sim	
Support	
Support Provided by CAST, Inc.	

Features

- Available under terms of the SignOnce IP License
- Compliant to the FIPS 180-2 specification for 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
- Robust verification environment includes bit-accurate software model

Table 1: Example Implementation Statistics for Xilinx® FPGAs

Family	Example Device	Fmax (MHz)	Slices[1]	IOB[2]	GCLK	BRAM	MULT/ DSP48	DCM / CMT	MGT	Design Tools
Spartan™-3	XC3S400-5	75	817	297	1	-	-	-	N/A	ISE™ 9.2.01i
Spartan™-3E	XC3S400E-5	95	1,007	297	1	-	-	-	N/A	ISE™ 9.2.01i
Virtex™- II	XC2V250-6	107	830	297	1	-	-	-	N/A	ISE™ 9.2.01i
Virtex™- II Pro	XC2VP2-7	120	815	297	1	-	-	-	N/A	ISE™ 9.2.01i
Virtex™-4	XC4VLX15-12	144	829	297	1	-	-	-	N/A	ISE™ 9.2.01i
Virtex™-5	XC5VLX30-3	175	433	297	1	-	-	-	N/A	ISE™ 9.2.01i

Notes:

1) Actual slice count dependent on percentage of unrelated logic – see Mapping Report File for details

2) Assuming all core I/Os and clocks are routed off-chip

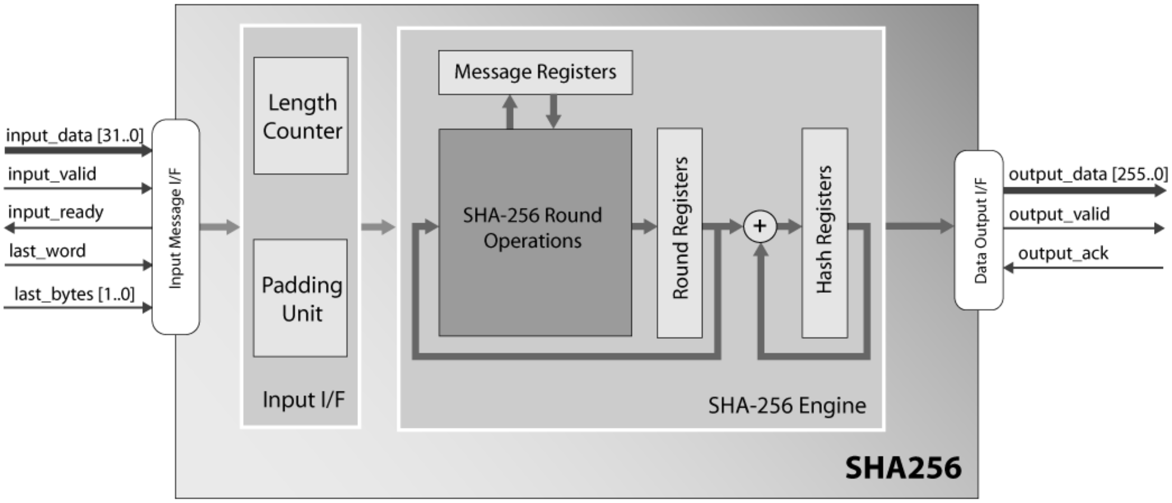

Figure 1: SHA256 Block Diagram

Applications

The high-performance SHA256 core is suitable for a variety of applications, including:

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

General Description

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. Representative results show that the core fits in a variety of Xilinx devices, requiring, for example, about 750 slices for Virtex-5. The complete deliverables feature comprehensive documentation, and a bit-accurate software model (BAM).

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.

Core Modifications

The core can easily be modified to support programmable Initial Vectors in place of the constants defined in the algorithm's specification. Contact CAST for more information.

Export Permits

Strong encryption technology is governed internationally by export regulations. Contact CAST to verify if your country qualifies for exportation of this technology.

Core I/O Signals

The core signal I/O have not been fixed to specific device pins to provide flexibility for interfacing with user logic. Descriptions of all signal I/O are provided in Table 2.

Table 2: Core I/O Signals.

Signal	Signal Direction	Description
clk	Input	Clock Input
enble	Input	Enable
clr	Input	Synchronous clear
rst	Input	Asynchronous reset
Message Data Input Interface		
msg_in	Input	Input Message data
msg_valid	Input	Masks valid input data on msg_in input bus
msg_ready	Output	Flag that shows if the core can accept input data on msg_in bus, in the current clock cycle
msg_last	Input	Marks the current word being written as the last word of the message
msg_size	Input	Provides the number of valid bytes in the msg_in input bus during the last message word transfer
Hash Value Output Interface		
hash_out	Output	Hash Value output bus
hash_valid	Output	Masks valid data on the hash_out bus
hash_ack	Input	Acknowledge signal indicating that the hash value was accepted

Verification Methods

The SHA256 core has been verified through extensive simulation and rigorous code coverage measurements. It has also been verified in a prototyping FPGA board platform.

Recommended Design Experience

The user must be familiar with HDL design methodology as well as instantiation of Xilinx netlists in a hierarchical design environment.

Ordering Information

This product is available directly from Xilinx Alliance Program member CAST under the terms of the SignOnce IP License. Please contact CAST for pricing and additional information about this product using the contact information on the front page of this datasheet. To learn more about the SignOnce IP License program, contact CAST or visit the web:

Email:	commonlicense@xilinx.com
URL:	www.xilinx.com/ipcenter/signonce

This product is available directly from Xilinx Alliance Program member CAST. Please contact CAST for pricing and additional information about this product using the contact information on the front page of this datasheet. The SHA256 core is licensed from Alma Technologies, S.A.

Related Information

Xilinx Programmable Logic

For information on Xilinx programmable logic or development system software, contact your local Xilinx sales office, or:

Xilinx, Inc.
2100 Logic Drive
San Jose, CA 95124
Phone: +1 408-559-7778
Fax: +1 408-559-7114
URL: www.xilinx.com