

CAST

MD5

MD5 Hash Function Core

The MD5 core is a high performance implementation of the MD5 Message Digest algorithm, a one-way hash function, compliant with RFC1321. The core is composed of two main modules, the MD5 Engine Module and the Input Interface Module as shown in the block diagram. The MD5 Engine Module applies the MD5 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 MD5 engine.

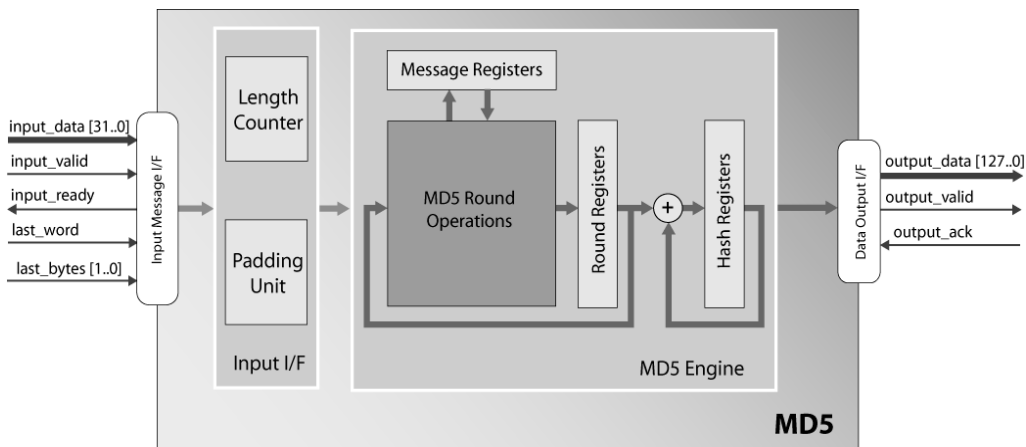
The MD5 core is equipped with easy to use fully stallable interfaces both for input and output. These are designed to permit the user's application to stop the data stream from the core when it is not able to receive data or to stop the input stream towards the core according to data arrival rate.

Applications

The high-performance MD5 core is suitable for a variety of applications, including:

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

Block Diagram



Features

- Compliant to the RFC1321 specification of MD5.
- 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.
- Scan-ready design architecture.

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 equivalent gate count using the smallest NAND2 gate available in the technology.

ASIC Technology	Fmax (MHz)	Logic Area (um ²)	Number of eq. gates
UMC 0.18 μm	280	134,170	11 K
TSMC 0.09 μm	500	28,220	10 K

1. Excluding memory (512 bits)
2. 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 MD5 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 MD5 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 MD5 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.

CAST
info@cast-inc.com
www.cast-inc.com

CAST, Inc. 11 Stonewall Court
Woodcliff Lake, NJ 07677 USA
tel 201-391-8300 fax 201-391-8694
Copyright © CAST, Inc. 2010, All Rights Reserved.
Contents subject to change without notice.
Trademarks are the property of their respective owners.

 **Alma
Technologies**
The MD5 core is sourced from
Technology Partner Alma Technologies.