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

Features
• RFC 1321 compliant
• Suitable for data authentication applications
• Fully synchronous design
• Available as fully functional and synthesizable VHDL or Verilog soft-core
• Test benches provided
• Available under terms of the SignOnce IP License

Applications
• Electronic funds transfer
• Authenticated electronic data transfers
• Encrypted data storage

Table 1: Core Implementation Data

<table>
<thead>
<tr>
<th>Supported Family</th>
<th>Device Tested</th>
<th>Fmax (MHz)</th>
<th>CLB Slices¹,²</th>
<th>IOBs²</th>
<th>GCLK</th>
<th>BRAM</th>
<th>MULT</th>
<th>DCM</th>
<th>MGT</th>
<th>PPC</th>
<th>Design Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spartan-3</td>
<td>XC3S200-4</td>
<td>41</td>
<td>535</td>
<td>167</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>N/A</td>
<td>N/A</td>
<td>ISE 5.2i</td>
</tr>
<tr>
<td>Spartan-IIE</td>
<td>XC2S50E-7</td>
<td>46</td>
<td>544</td>
<td>167</td>
<td>1</td>
<td>1</td>
<td>N/A</td>
<td>0</td>
<td>N/A</td>
<td>N/A</td>
<td>ISE 5.2i</td>
</tr>
<tr>
<td>Virtex-II Pro</td>
<td>XC2VP2-7</td>
<td>74</td>
<td>605</td>
<td>167</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>ISE 5.2i</td>
</tr>
<tr>
<td>Virtex-II</td>
<td>XC2V250-6</td>
<td>65</td>
<td>525</td>
<td>167</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>N/A</td>
<td>N/A</td>
<td>ISE 5.2i</td>
</tr>
</tbody>
</table>

Notes:
1. Actual slice count may vary depending on percentage of unrelated logic – see Mapping Report File for details
2. Assuming all core I/Os are routed off-chip
3. Optimized for speed; smaller implementations possible when optimized for area
MD5 Message Digest Algorithm

General Description
This core is a fully compliant hardware implementation of the Message Digest Algorithm MD5, suitable for a variety of applications. It computes a 120-bit message digest for messages of up to \((2^{64} - 1)\) bits.

The MD5 algorithm is an improved version of the MD4, created by Professor Ronald L. Rivest of MIT and is closely modeled after that algorithm. It operates on message blocks of 512 bits for which a 128-bit (4 x 32-bit words) digest is produced. Corresponding 32-bit words of the digest from consecutive message blocks are added to each other to form the message of the whole message.

Functional Description
The MD5 core is partitioned into modules as shown in Figure 1. The modules are described below.

Pad Words
This module pads the incoming data with the appropriate number of bits. According to the MD5 algorithm all data to be processed must be a multiple of 512 bits.

Length Counter
This module counts the number of bits being input. This information is also used to pad the incoming data to digest.

16x32 Register Array
Main storage for the 512 bits to be digested.

Compute A, B, C, D
This is a group of non-linear functions used by the MD5 algorithm to digest the data.

4x32 Registers Arrays
These two arrays are used to compute the intermediate and the final results of the message digest.

Pinout
The pinout of the C8051 core has not been fixed to specific FPGA I/O, thereby allowing flexibility with a user’s application. Signal names are shown in Figure 1 and described in Table 2.

Table 2: Core Signal Pinout

<table>
<thead>
<tr>
<th>Signal</th>
<th>Direction</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSTN</td>
<td>Input</td>
<td>Asynchronous reset, active low</td>
</tr>
<tr>
<td>EN</td>
<td>Input</td>
<td>Clock enable signal, active high</td>
</tr>
<tr>
<td>INIT</td>
<td>Input</td>
<td>Initialize message digest calculation</td>
</tr>
<tr>
<td>DIN[31:0]</td>
<td>Input</td>
<td>Input data</td>
</tr>
<tr>
<td>ACK</td>
<td>Input</td>
<td>Input data acknowledge</td>
</tr>
<tr>
<td>LAST</td>
<td>Input</td>
<td>Last input data word indication</td>
</tr>
<tr>
<td>REQ</td>
<td>Output</td>
<td>Requests input data</td>
</tr>
<tr>
<td>READY</td>
<td>Output</td>
<td>Output data valid</td>
</tr>
<tr>
<td>A[31:0]</td>
<td>Output</td>
<td>First message digest word</td>
</tr>
<tr>
<td>B[31:0]</td>
<td>Output</td>
<td>Second message digest word</td>
</tr>
<tr>
<td>C[31:0]</td>
<td>Output</td>
<td>Third message digest word</td>
</tr>
<tr>
<td>D[31:0]</td>
<td>Output</td>
<td>Fourth message digest word</td>
</tr>
</tbody>
</table>
Core Modifications
AMBA interface support. Contact CAST for modification.

Verification Methods
The core’s functionality was verified by means of extensive software simulation.

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 AllianceCORE product is available from Xilinx AllianceCORE partner, CAST, Inc. under terms of the SignOnce IP License. To learn about the SignOnce IP License program, contact CAST, Inc., visit www.xilinx.com/ipcenter/signonce.htm, or write to commonlicense@xilinx.com.

Please contact CAST, Inc. for pricing and additional information about this AllianceCORE product.

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: 408-559-7778
  Fax: 408-559-7114
  URL: www.xilinx.com

For AllianceCORE™ specific information: