ES1005 – MD5 Hashing Core

Introduction

The es1005 hash fully implements the MD5 (Message Digest Algorithm RFC 1321). The core can be used for data authentication in digital broadband, wireless or multimedia system. The MD5 core processes the input message in 512-bit blocks and produce message digest of 128-bit (for md5). The output data is referred to as a “digital signature” or “fingerprint” or “message digest” of input messages

Features

- ✓ Supports MD5 Secure Hash Algorithm described in RFC 1321.
- ✓ High speed operation. One clock per hash step. Full MD5 is computed in 64+1 cycles.
- ✓ Supports message padding
- ✓ Allows Time Division Multiplexing (TDM) of several data streams.
- ✓ Simple external interface
- ✓ Simple 32 bit I/O interface
- ✓ Outputs message digest from every input block of data (512-bit block size)
- ✓ Supports user input initialization vectors.
- ✓ Minimal gate count.
- ✓ Support 1.6 Gb/s of data rate for MD5 at 200 MHz.
- ✓ Available in ASIC and FPGA Technologies.

Applications

- Secure corporate communications

  - Virtual Private Networks (VPN)
  - Storage Area Networks (SAN)
  - Video conferencing
  - Voice services

- Secure electronic transactions

  - Medical files
  - Financial files
  - Securities exchange
  - eCommerce
  - Point-of-Sale

- Personal mobile communications

  - Video phones
  - PDA
  - Point-to-Point Wireless

Pin Description

Name	I/O	Width	Description
clk	Input	1	System Clock input
rst_n	Input	1	Asynchronous active low reset
DataVld	Input	1	Input data port DataIn is sampled every clock when DataVld is asserted.
DataIn	Input	32	32-bit message data input
DataFirst	Input	1	When asserted, indicates first 32 bit of message. This is used to load initialization vector
DataLast	Input	1	When asserted, indicates last 32 bit of message for respective session.
DataNumb	Input	5	This signal indicates how many bits of the data at DataIn are to be sampled as message data when DataLast is asserted. This signal is ignored if DataLast is not asserted.
DataLast	Input	1	When asserted, indicates last 32 bit of message for respective session.
InitVec	Input	1	When asserted indicates that data presently sampled at DataIn port is initialization vector. For MD5 initialization vector is 160-bit, so this signal should be valid for 5 cycles before feeding the message data for a respective session.
MsgDgstVld	Output	1	Message Digest ready signal, when asserted signifies the message digest for current block is presented at MsgDigest output port.
MsgDigest	Output	32	Message digest output data. Most significant 32 bits of data are presented first.
DataBusy	Output	1	When asserted indicates that the core is busy computing message digest. Message input data should not be presented to DataIn.

Functional Description

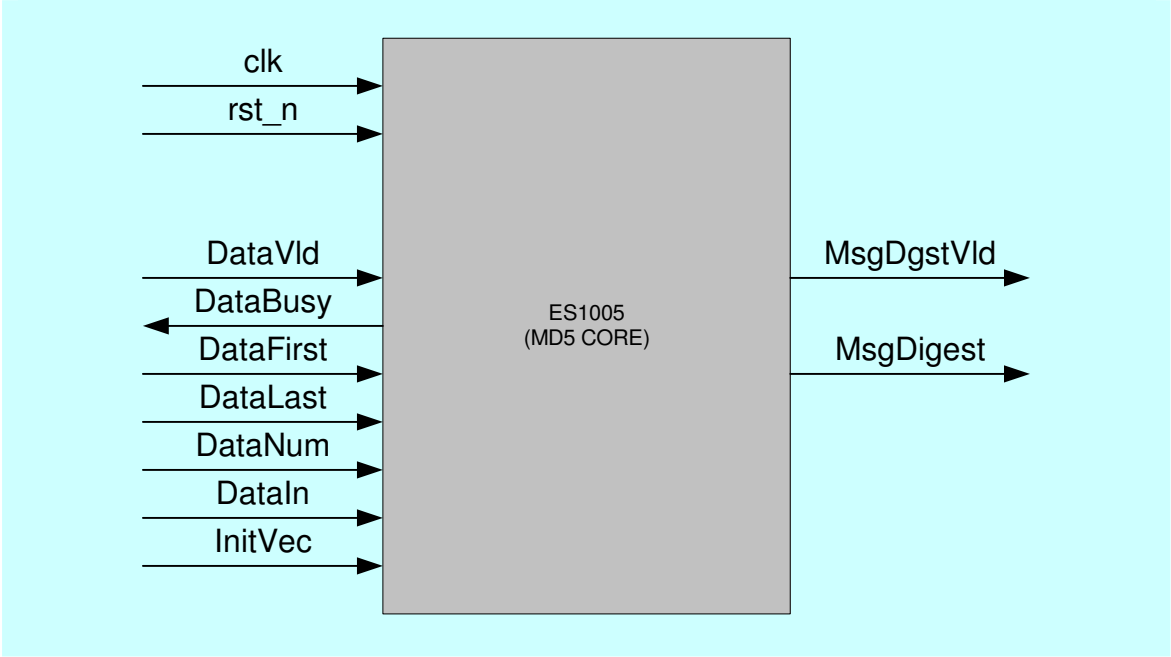

Figure 1. ES1005 Symbol

ES1005 fully implements Message Digest (MD5) function described in RFC 1321. It accepts any length of packet data up to 2^64 Bits and computes the 128-bit message digest value. Input data is fed into the core using DataVld, DataFirst and DataLast signals. At the end of MD5 computation, a 128-bit message digest is generated on MsgDigest[31:0]. The result is extracted from the core in 4 consecutive cycles.

Figure 2 depicts the top level functional timing diagrams of ES1005.

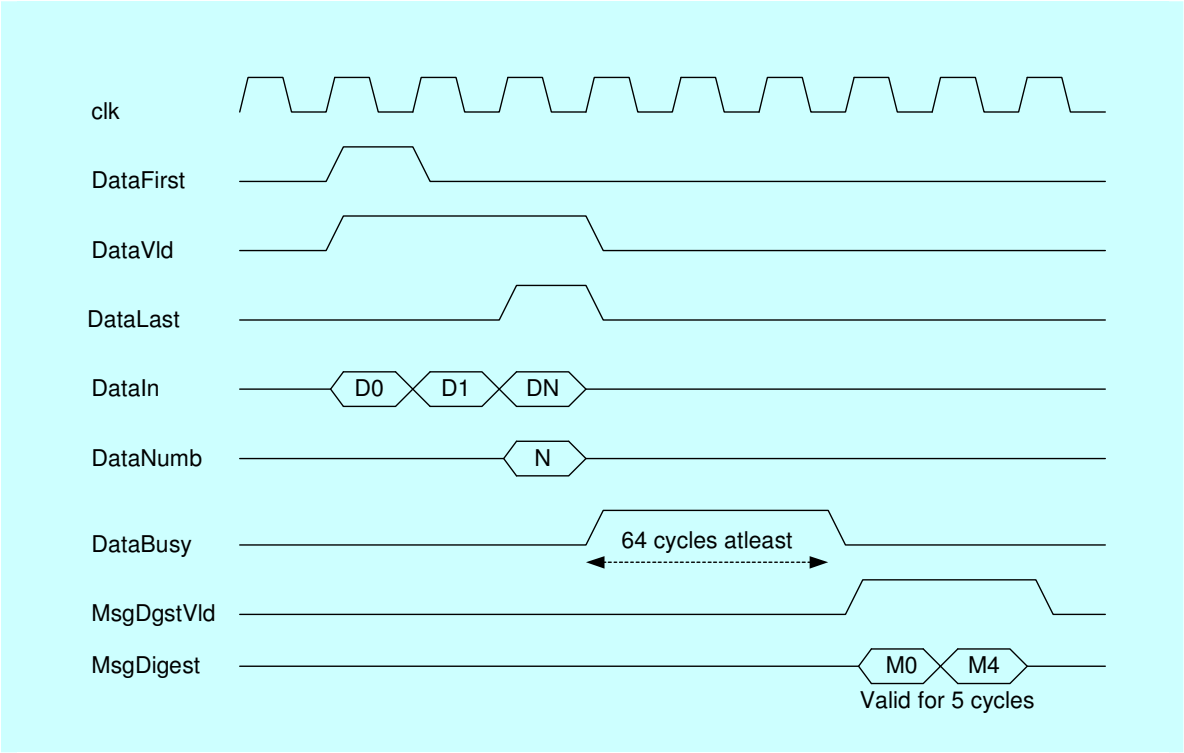

Figure 2. ES1005 Interface Timing Diagram

The core also pads the data if the input data is not multiple congruent of 448 bits. This makes the usage very simple and no extra hardware is needed to support MD5 padding. The core also allows to load initialization vector using InitVec valid signal and this can be used to implement HMAC like function.

Deliverables

- ✓ Synthesizable Verilog RTL source code
- ✓ Simulation scripts
- ✓ Self-checking Test environment
  - ➢ Test-bench
  - ➢ Test-vectors
  - ➢ Expected results
- ✓ Synthesis scripts
- ✓ User Documentation

Sales Representatives

For pricing information:

Esencia Technologies Inc.
2041 Mission College Blvd., Suite #100
Santa Clara CA, 95054
Tel: (408) 736-8284
Web: www.esenciatech.com
E-mail: sales@esenciatech.com

About Esencia

Esencia Technologies is a leading provider of pre-verified virtual components for consumer electronics and communication markets at competitive prices.