MD5 IP Core with WISHBONE Slave Interface

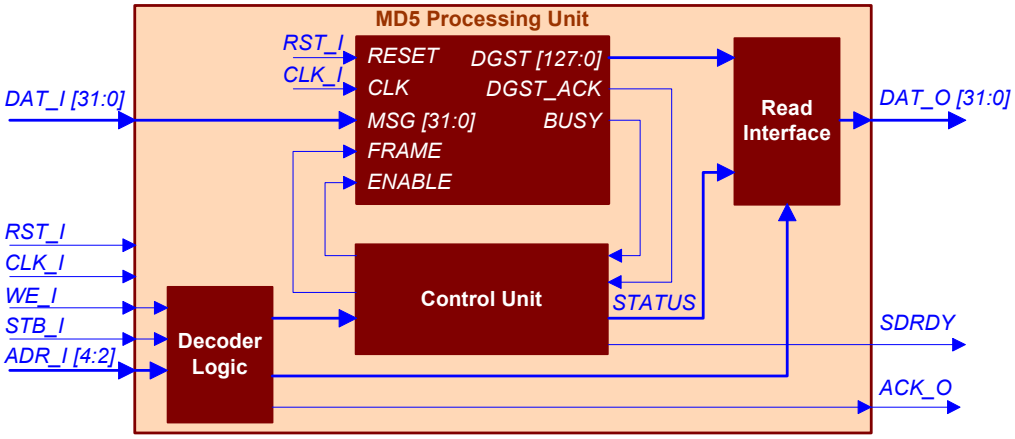
General information

MD5 IP CORE implements MD5 algorithm as defined in RFC1321. It is a strong one-way function that is being employed in various standards, algorithms and products (e.g. password storage, digital signature and authentication). The IP CORE is based on the INTRON's Fast MD5 processing unit that is designed for processing arbitrary length messages (up to 2^{64} bits). The IP CORE can be easily integrated into a WISHBONE-based SoC with Slave interface compliant with WISHBONE Specification (Rev.B.1) (single read/write cycles). No additional logic is required for processor integration.

Features

- *MD5 algorithm (RFC 1321) is implemented for arbitrary length messages (up to 264 bits).*
- *Interface is compliant with WISHBONE Slave Rev. B.1 interface with separated 32 bit input/output data buses.*
- *512 bit message block is processed in 66 clocks.*
- *Byte-based processing.*
- *Vendor independent VHDL model, netlist for target device.*

MD5 IP Core with WISHBONE Slave Interface pinout



Interface description

Pin	Activity	Description
RST_I	HIGH	Asynchronous reset
CLK_I	–	Clock input
ADR_I[4:2]	–	Subset of WISHBONE address bus
DAT_I[31:0]	–	Unidirectional WISHBONE write bus
WE_I	HIGH	WISHBONE bus access signal: HIGH for write transfer, LOW for read transfer
STB_I	HIGH	Strobe input indicated a valid data transfer cycle.
ACK_O	HIGH	Acknowledge output indicates the termination of a normal bus cycle
DAT_O[31:0]	–	Unidirectional WISHBONE read bus

Sample implementation

Device	Speed grade	Utilization	Performance	Synthesis and implementation tools	Availability
ALTERA Stratix II Device					
EP2S15F484C3	3	1512 ALUTs	***127.57*** MHz	Quartus[1)]	***Now***, ver_1_3_2[2)]
EP2S15F484C3	3	***1480*** ALUTs	122.41 MHz	Quartus[1)]	***Now***, ver_1_3_3[3)]

1) Quartus – Altera Quartus II, ver 5.1.
2) – Speed optimized;
3) – Area optimized.

http://www.intron-innovations.com
info@intron-innovations.com