MD5 Fast Processor Core

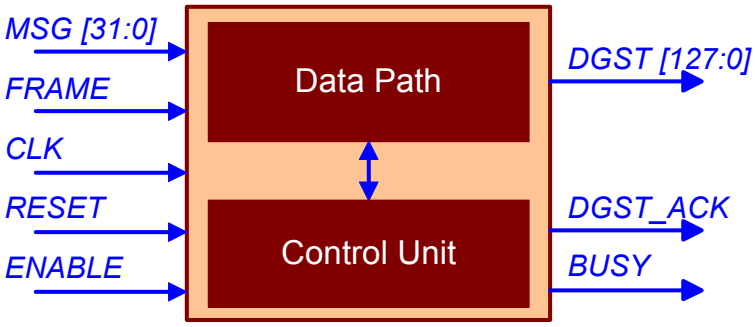
General information

MD5 is defined in RFC 1321. It is a strong one-way hash function that is being employed in various standards, algorithms and products (e.g. password storage, digital signature and authentication). Although MD5 is a strong cryptographic hash function, its operation on programmable processors is rather computational demanding, thus cause a performance bottleneck in the overall system. The Fast MD5 Processor Core with its high throughput can support critical network security system (e.g. digital signature in e-commerce, remote access etc).

Features

- *MD5 algorithm is implemented;*
- *Input data word length – 32 bit;*
- *Output digest length – 128 bit;*
- *Pipelined Data Processing;*
- *512 bit message is processed in 64 clocks*
- *Simple interface and timing;*
- *No dead clock cycles;*
- *Compliant with RFC 1321;*
- *Vendor independent VHDL model, netlist for target device.*

MD5 Fast Processor core pinout



Interface description

Pin	Activity	Description
CLK	Positive clock edge	Clock
RESET	HIGH	Asynchronous reset
ENABLE	HIGH	Clock enable
MSG[31:0]	-	Input message data
FRAME	HIGH	Input message data acknowledgment
DGST[127:0]	-	Output digest
DGST_ACK	HIGH	Output digest acknowledgment
BUSY	HIGH	Busy

Sample implementation

Device	Speed grade	Utilization	Performance	Synthesis and implementation tools	Availability
XILINX					
XC4036XLA	-09	1032 CLB	22.4 MHz	Synplify, Xilinx	***Now***, ver_1_1_1
XCV150	-6	972 Slices	48.19 MHz	Synplify, Xilinx	***Now***, ver_1_1_2
ALTERA					
EPF10K50E	-1	2438 LC	31.9 MHz	Synplify, Max+PlusII	***Now***, ver_1_1_3
EP20K60EFC324	-1X	2174 LE	39.58 MHz	Synplify, Quartus [1)]	***Now***, ver_1_1_4
EP2S15F484C3	3	1425 ALUTs	131.87 MHz	Quartus [2)]	***Now***, ver_1_1_5 [3)]
EP2S15F484C3	3	1324 ALUTs	124.72 MHz	Quartus [2)]	***Now***, ver_1_1_6 [4)]

1) Quartus – Altera Quartus II, ver 1.1;
2) Quartus – Altera Quartus II, ver 5.1;
3) – Speed optimized;
4) – Area optimized.

Synplify – Synplicity Synplify VHDL Compiler, version 6.1.3; ***Xilinx*** – Xilinx Foundation, version F2.1i Build 3.1.165;
Max+PlusII – Altera Max+PlusII, version 10.1.

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