SHA-1 Fast Processor Core

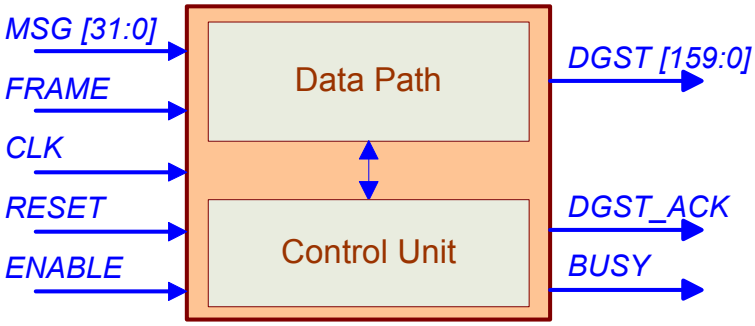
General information

SHA-1 is defined in FIPS180-1. 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 SHA-1 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 SHA-1 Processor Core with its high throughput can support critical network security system (e.g. digital signature in e-commerce, remote access etc).

Features

- *SHA-1 algorithm is implemented;*
- *Input data word length – 32 bit;*
- *Output digest length – 160 bit;*
- *Pipelined data processing;*
- *512 bit message is processed in 84 clocks*
- *Simple interface and timing;*
- *No dead clock cycles;*
- *Compliant with FIPS180-1;*
- *Vendor independent VHDL model, netlist for target device.*

SHA-1 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[159:0]	-	Output digest
DGST_ACK	HIGH	Output digest acknowledgment
BUSY	HIGH	Busy

Sample implementation

Device	Speed grade	Utilization	Performance	Synthesis and implementation tools	Availability
XILINX					
XC4028XLA	-09	783 CLBs	36.9 MHz	Synplify, Xilinx	***Now***, ver_1_2_1
XCV150	-6	716 Slices	70.56 MHz	Synplify, Xilinx	***Now***, ver_1_2_2
ALTERA					
EPF10K50E	-1	1943 LCs	51 MHz	Synplify, Max+PlusII	***Now***, ver_1_2_3
EP20K100EFC324	-1X	1521 LEs	61.89 MHz	Synplify, Quartus (1)	***Now***, ver_1_2_4
EP2S15F484C3	3	1454 ALUTs	157.46 MHz	Quartus (2)	***Now***, ver_1_2_5

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;
Quartus (1) – Altera Quartus II, ver 1.1; ***Quartus (2)*** – Altera Quartus II, ver 5.1.

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