ALSHA Core

Application Note

Rev. [6/2012]

6-19-2012

Table of Contents

General Information

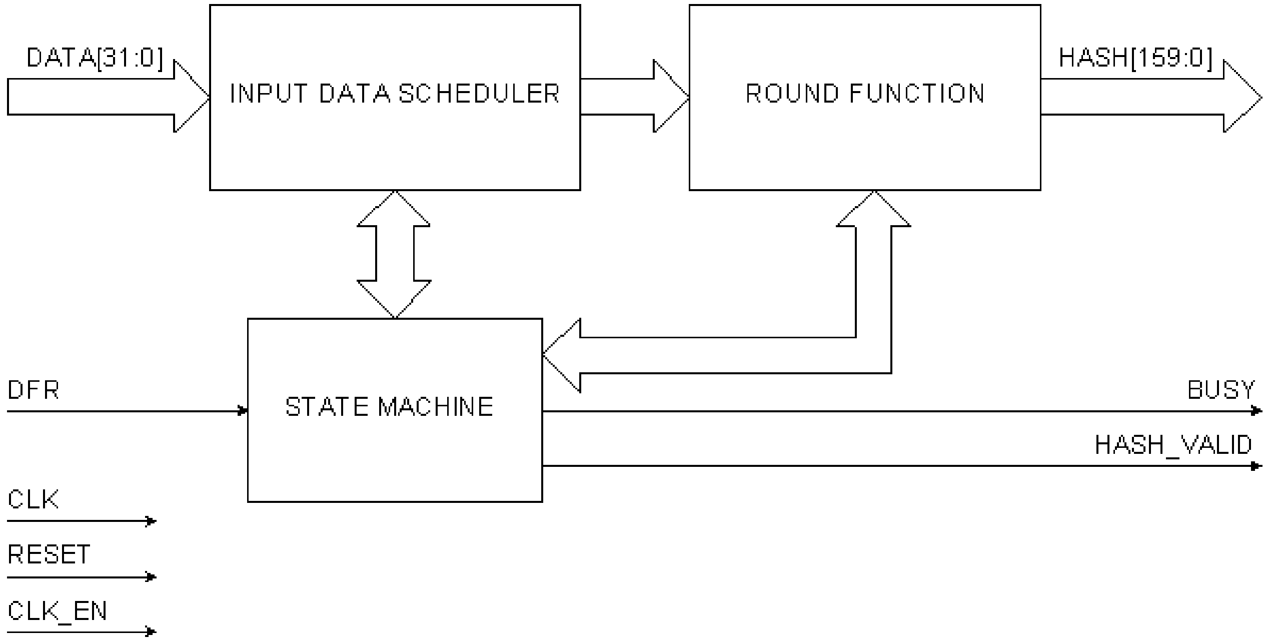
The ALSHA core is the VHDL model of the processor that performs SHA-1 hash function calculation. The model is fully compliant with FIPS180-1.

Features

- Byte oriented hash calculation
- Hash value of 512-bit message is calculated in 81 clock cycles
- Suitable for fast Digital Signature Algorithm implementations
- No dead clock cycles
- Simple interface and timing
- Fully synchronous design

Block Diagram

The basic structure of the ALDES core is shown below:



Contents

Synthesizable

See the Deliverables section of this document for further details.

Test Vectors

See the Deliverables section of this document for further details.

Interface

The pinout of the ALSHA core has not been fixed to specific FPGA I/O, allowing flexibility with a user's application. Signal names are shown in the table.

Signal Name	Signal Direction	Polarity	Description
CLK	IN	-	Clock input
RESET	IN	HIGH	Asynchronous reset
CLK_EN	IN	HIGH	Clock enable
DFR	IN	HIGH	Data frame: 1- data are loaded, 0 – end of data
DATA[31:0]	IN	-	Input data
HASH_VALID	OUT	HIGH	Hash ready signal
BUSY	OUT	-	Busy signal, 1 - processor is busy, 0 - data can be loaded
HASH[159:0]	OUT	-	Output hash data

Data processing begins with DFR setting to HIGH. When CLK_EN is set to HIGH then core reacts on CLK signal. While data are processed by ALSHA core BUSY signal indicates that processor is busy. If set LOW, then the input data signal IN_DATA can be changed, when set HIGH, the processor will not load input data to itself. Result of calculation appears at the HASH output and it is followed by HASH_VALID signal in HIGH.

Implementation Data

The core has been synthesized and implemented to different types of reprogrammable devices. The model has been verified using the simulation environment and tested on the real hardware.

Software				
Synthesis Tool	Synopsys FPGA Express™ build 2.1.3.3220			
Implementation Tools	Xilinx Foundation™ 2.1i SP6, Altera MAX+plusII™ 9.4, Quartus™ 2000.02			
Verification Tool	Active-HDL™ 4.1			
Hardware				
Vendor	Xilinx		Altera	
Device Family	4K	Virtex™	FLEX™ 10K	APEX™ 20K
Target Device	XC4044XL-09	XCV300-6	EPF10K50-1	EP20K100-1
Area	704CLBs	1016Slices	1947LCs	1413LCs
System Clock fmax	23MHz	52MHz	27MHz	64MHz

Deliverables

After you request the desired compiled synthesizable core, Aldec delivers the following files:

- Technology-dependent EDIF (ALSHA.EDF) and VHDL (ALSHA.VHD) netlists
- Test vectors and patterns
- User-Guide and Application Notes
- Sample designs
- Software emulator of ALSHA core

Usually Aldec delivers both EDIF and VHDL netlists for customers who order the synthesizable model. The EDIF netlist is used for the place and route process and VHDL is the post-synthesis netlist used for the simulation only. Of course, both netlists are technology-dependent, because they are created after the synthesis where the customer needs to specify a vendor, target family, etc.

Software emulator of ALSHA core is intended to use as «golden» source for patterns from user-provided set of data.

Aldec can provide also a set of VHDL test benches for their cores. Usually they are sold at the additional charge.

Source codes are sold on a case-by-case basis.