

Data sheet for SHA 224/256/384/512 Core

Functional Description

This document describes the SHA2 family of cryptographic hash. For the SHA-224 or SHA-256, the algorithm takes as input a message of length which is a multiple of 512 bits and produces as output a 224-bit or 256-bit "fingerprint" of the input. For the SHA-384 or SHA-512, the input is a multiple of 1024 bits and the output is of width 384 or 512 bits respectively.

Features:

- Supports configurable clock rate
- Supports SHA-224, SHA-256, SHA-384, SHA-512 depending on the input parameter
- Takes 66 cycles for 512-bit data as in SHA-224 and SHA-256, and takes 82 cycles for 1024-bit data of SHA-384 and SHA-512
- Compliant with FIPS PUB 180-2

Block Diagram:

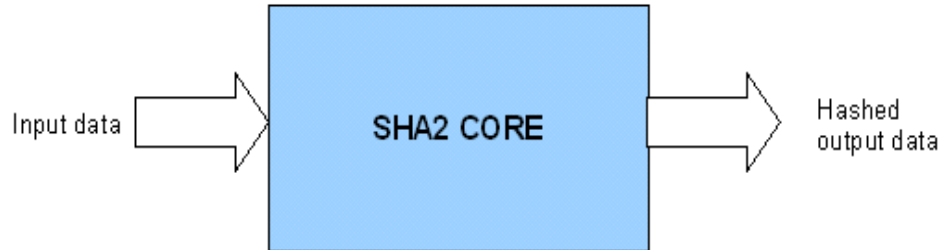


Figure 1: Block Diagram

Architectural Diagram:

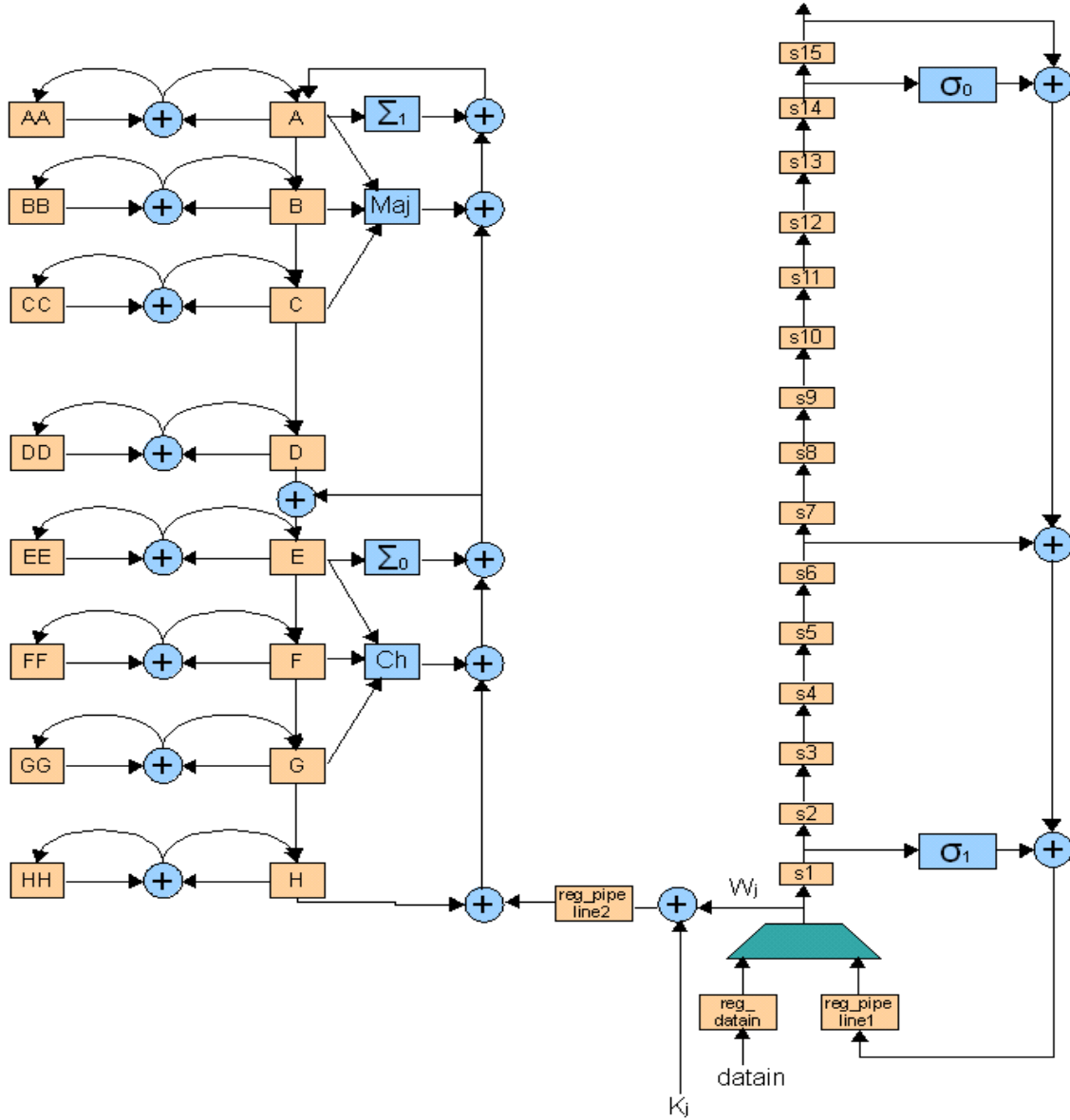


Figure 2: SHA2 Architecture Diagram

SHA2 Parameter Table

This table describes the general SHA2 parameters:

Parameter	Type	Description
SHA_METHOD	Integer	Decides the type of SHA2. SHA-224 for SHA_METHOD=224, SHA-256 for SHA_METHOD=256, SHA-384 for SHA_METHOD=384, SHA-512 for SHA_METHOD=512.

Signal Definition table:

Signal	Direction	Description
clock	IN	This is the system clock.
reset	IN	This is the system reset.
datain[31:0] or datain[63:0]	IN	This is the data input.
datain_valid	IN	This signal is held HIGH when data is being fed to the module. One chunk of data has 16 words of 32 bits each for SHA-224 or SHA-256 and has 16 words of 64 bits for SHA-384 or SHA-512. Thus this signal is HIGH for 16 consecutive cycles at one go.
start_data	IN	This signal is held HIGH for one cycle when the first data is given to the module.
end_data	IN	This signal is held HIGH for one cycle when the last 32-bit or 64-bit data is given to the module.
dataout[223:0] or dataout[255:0] or dataout[383:0] or dataout[511:0]	OUT	This is the output of the module. It is 224 bits for SHA-224, 256 bits for SHA-256, 384 bits for SHA-384 512 bits for SHA-512.
dataout_valid	OUT	This signal is HIGH for one cycle when the output is valid.
get_data	OUT	Data should be fed to the module one cycle after this signal goes HIGH. When this signal is HIGH an entire 512-bit chunk consisting of 16 32-bit words or 1024-bit chunk consisting of 16 64-bit words should be given.

Description:

1. Data is given to the SHA2 module when the 'get_data' signal is logic HIGH.
2. Sixteen words of 32 bits are given to the module if SHA-224 or SHA-256 and sixteen words of 64 bits are given if SHA-384 or SHA-512 in one single chunk, along with the 'datain_valid' signal.
3. When the first chunk of data is given to the SHA2 module, a start_data pulse is held HIGH for one cycle.
4. When the last chunk of data is being fed to the module an 'end_data' pulse is HIGH for one cycle when the last word is being written.
5. When the valid data is ready to be outputted, the 'dataout_valid' signal is HIGH for one cycle.
6. The SHA2 module takes 66 cycles to process one 512-bit chunk of data, and 82 cycles to process one 1024-bit chunk.

Schematic Symbol

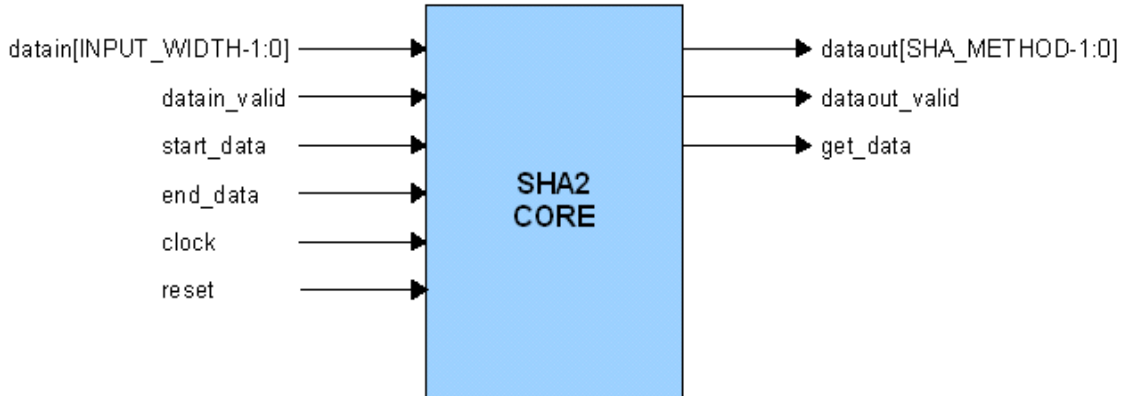


Figure 3: Schematic Symbol

Performance:

Hash Type	Device	Slice Register Count	Slice LUT Count	Frequency
SHA 224	Virtex-4 lx25 -10 ff668	754	1608	138 MHz.
	Virtex-5 lx30 - 3 ff676	753	1460	248 MHz.
SHA 256	Virtex-4 lx25 -10 ff668	754	1608	139 MHz.
	Virtex-5 lx30 - 3 ff676	753	1460	253 MHz.
SHA 384	Virtex-4 lx25 - 10 ff668	1495	3155	114 MHz.
	Virtex-5 lx30 - 3 ff676	1495	2886	203 MHz.
SHA 512	Virtex-4 lx25 - 10 ff668	1495	3155	115 MHz.
	Virtex-5 lx30 -3 ff676	1495	2886	204 MHz.

Verification:

The SHA2 module has been verified with following approaches:

- Comparison with the test-cases given in the FIPS PUB 180-2.
- Exhaustive Functional/Timing simulation.

Deliverables:

- Verilog RTL source code
- Test benches
- Synthesis and Simulation scripts.
- Detailed user documentation, including RTL source code documentation