eSi-SHA-256

1 Contents

2 Overview

The eSi-SHA-256 core can be used to calculate the SHA-256 hash value of a block of data. It supports the following features:

- FIPS 180-4 compliant SHA-256 hash engine.
- Integrated DMA – zero CPU overhead and low bus utilisation.
- AMBA 3 AHB-lite slave interface for control register access.
- AMBA 3 AHB-lite master interface for data transfers.

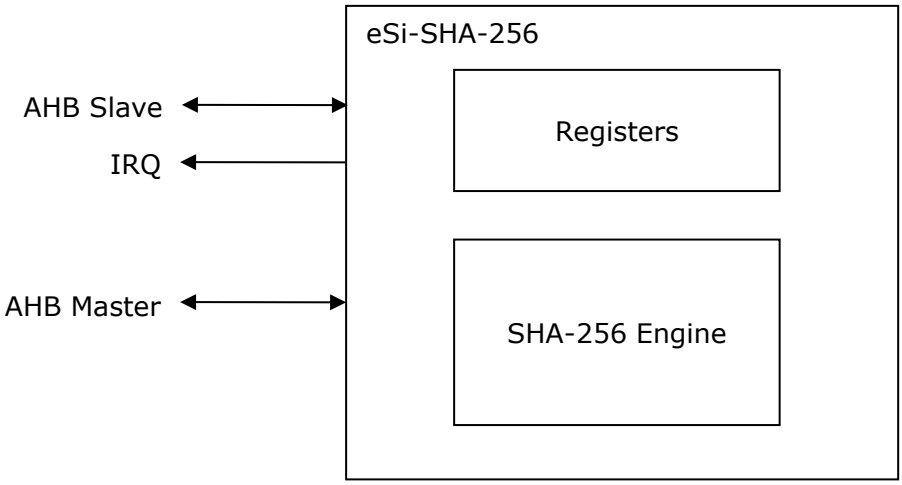

Figure 1: eSi-SHA-256

3 Hardware Interface

Module Name	cpu_ahb_sha_256
HDL	Verilog
Technology	Generic
Source Files	cpu_ahb_sha_256.v, cpu_sha_256.v

Port	Type	Description
write_enable	Integer	Specifies whether writing the hash to memory is supported

Table 1: Parameters

Port	Direction	Width	Description
clk	Input	1	Hashing clock. Must be synchronous to m_hclk
s_hclk	Input	1	Slave interface, AHB clock
s_hresetn	Input	1	Slave interface, AHB reset, active-low
s_haddr	Input	BITS	Slave interface, AHB address
s_hburst	Input	3	Slave interface, AHB burst type
s_hmastlock	Input	1	Slave interface, AHB locked transfer
s_hprot	Input	4	Slave interface, AHB protection
s_hsize	Input	3	Slave interface, AHB size
s_htrans	Input	2	Slave interface, AHB transfer type
s_hwdata	Input	BITS	Slave interface, AHB write data
s_hwrite	Input	1	Slave interface, AHB write
s_hready	Input	1	Slave interface, AHB ready
s_hsel	Input	1	Slave interface, AHB select
s_hready	Output	1	Slave interface, AHB ready
s_hrdata	Output	BITS	Slave interface, AHB read data
s_hresp	Output	1	Slave interface, AHB response
m_hclk	Input	1	Master interface, AHB clock. Must be the same frequency and synchronous to s_hclk
m_hresetn	Input	1	Master interface, AHB reset, active-low
m_hready	Input	1	Master interface, AHB ready
m_hrdata	Input	BITS	Master interface, AHB read data
m_hresp	Input	1	Master interface, AHB response
m_haddr	Output	BITS	Master interface, AHB address
m_hburst	Output	3	Master interface, AHB burst type
m_hmastlock	Output	1	Master interface, AHB locked transfer
m_hprot	Output	4	Master interface, AHB protection
m_hsize	Output	3	Master interface, AHB size
m_htrans	Output	2	Master interface, AHB transfer type
m_hwdata	Output	BITS	Master interface, AHB write data
m_hwrite	Output	1	Master interface, AHB write
interrupt_n	Output	1	Interrupt request, active-low
clk_cactive	Output	1	Clock active. When deasserted, clk can be gated.
m_hclk_cactive	Output	1	Clock active. When deasserted, m_hclk can be gated.

Table 2: I/O Ports

For complete details of the AHB signals, please refer to the AMBA 3 AHB-Lite Protocol v1.0 Specification available at http://www.arm.com/products/solutions/AMBAHomePage.html

4 Software Interface

4.1 Register Map

Register	Address offset	Access	Description
src_address	0x00	R/W	Source address register
dst_address	0x04	R/W	Destination address register
count	0x08	R/W	Count register
status	0x0c	R/W	Status register
control	0x10	R/W	Control register
hash[31:0]	0x20	R	Calculated hash, least significant bits
hash[63:32]	0x24	R	Calculated hash
hash[95:64]	0x28	R	Calculated hash
hash[127:96]	0x2c	R	Calculated hash
hash[159:128]	0x30	R	Calculated hash
hash[191:160]	0x34	R	Calculated hash
hash[223:192]	0x38	R	Calculated hash
hash[255:224]	0x3c	R	Calculated hash, most significant bits

Table 3: Register Map

4.1.1 Source Address Register

The source address register contains the base address of the data to calculate the hash value for.

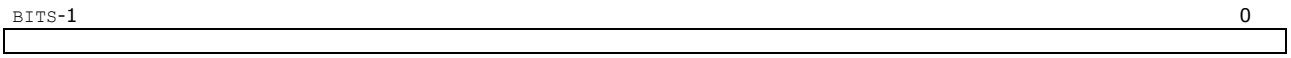

Figure 2: Format of the src_address register

4.1.2 Destination Address Register

The destination address register contains the base address to store the computed hash value to. The dst_address register is only implemented if the write_enable parameter is 1.

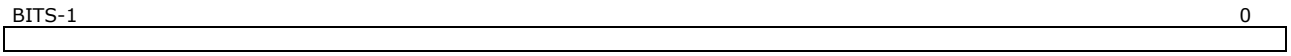

Figure 3: Format of the dst_address register

4.1.3 Count Register

The count register contains the number of bytes of data to read.

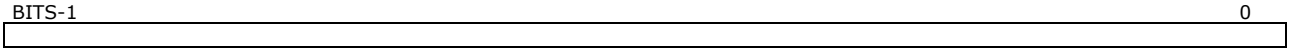

Figure 4: Format of the count register

4.1.4 Status Register

The status register contains a selection of flags that indicate the current status of the eSi-SHA-256 module.

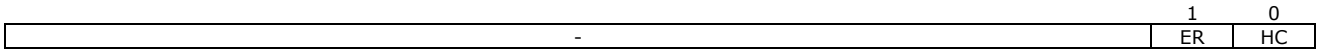

Figure 5: Format of the `status` register

Register	Values	Description
HC	0 - Not complete 1 – Complete	Hash complete. Read only
ER	0 – No error 1 – Error	Indicates an error occurred. Sticky

Table 4: Fields of the `status` register

4.1.5 Control Register

The control register contains a selection of flags that control the operation of the eSi-SHA-256 core.

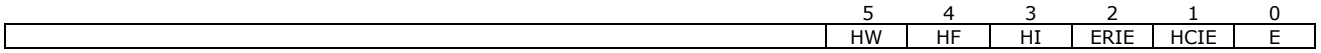

Figure 6: Format of the `control` register

Register	Values	Description
E	0 - Disabled 1 - Enabled	Enables the hash module, reading `count` bytes from `src_address`
HCIE	0 – Disabled 1 – Enabled	Hash complete interrupt enable
ERIE	0 – Disabled 1 – Enabled	Error interrupt enable
HI	0 – Do not initialise 1 – Initialise hash	Disables hash initialisation
HF	0 – Do not finalise 1 – Finalise hash	Finalises the hash calculation by adding padding and bit length
HW	0 – Do not write hash 1 – Write hash	Writes the hash to memory at the address specified by `dst_address`. This is only supported if `write_enable` parameter is 1.

Table 5: Fields of the `control` register

4.2 Interrupts

The eSi-SHA-256 core supports the following interrupts.

- Hash complete interrupt
- Error interrupt

The `HC` flag in the `status` register will be set 1 when `count` bytes of data have been read from `src_address`, the hash value has been calculated and, if requested, written to memory. When the `HC` flag in the `status` register is set to 1 and the `HCIE` flag in the `control` register is set to 1, the hash complete interrupt will be asserted.

The error interrupt will be raised then the `ER` flag in the `status` register is 1 and the `ERIE` flag in the `control` register is set to 1. This indicates an error was detected while reading data from memory or writing the hash to memory.

5 Revision History

Hardware Revision	Software Release	Description
1	3.3.9	Initial release

Table 6: Revision History

