# EF SHA256

APB, AHBL and wishbone wrappers for the SHA-256 cryptographic hash function which is implemented in Verilog in the secworks/sha256 repository.

## The wrapped IP

APB, AHBL, and Wishbone wrappers are provided. All wrappers provide the same programmer's interface as outlined in the following sections.

#### **Wrapped IP System Integration**

Based on your use case, use one of the provided wrappers or create a wrapper for your system bus type. For an example of how to integrate the wishbone wrapper:

## Wrappers with DFT support

Wrappers in the directory /hdl/rtl/bus\_wrappers/DFT have an extra input port sc\_testmode to disable the clock gate whenever the scan chain testmode is enabled.

## **Interrupt Request Line (irq)**

This IP generates interrupts on specific events, which are described in the <u>Interrupt Flags</u> section bellow. The IRQ port should be connected to the system interrupt controller.

# Implementation example

The following table is the result for implementing the EF\_SHA256 IP with different wrappers using Sky130 HD library and <a href="OpenLane2">OpenLane2</a> flow.

Module	Number of cells	Max. freq		
EF_SHA256	TBD	TBD		
EF_SHA256_APB	TBD	TBD		
EF_SHA256_AHBL	TBD	TBD		
EF_SHA256_WB	TBD	TBD		

# The Programmer's Interface

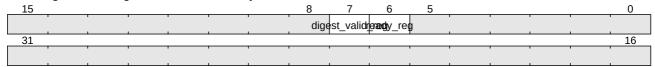
# Registers

Name	Offset	Reset Value	Access Mode	Description
STATUS	0000	0x00000000	r	Status register bit 0: digest is valid , bit 1: ready
CTRL	0004	0x00000000	w	Control register bit 0: Initial bit (init) bit 1: Next bit , bit 2: Mode bit
BLOCK0	8000	0x00000000	w	Contains the bits 31-0 of the input block value
BLOCK1	000c	0x00000000	w	Contains the bits 63-32 of the input block value
BLOCK2	0010	0x00000000	w	Contains the bits 95-64 of the input block value
BLOCK3	0014	0x00000000	w	Contains the bits 127-96 of the input block value
BLOCK4	0018	0x00000000	W	Contains the bits 159-128 of the input block value
BLOCK5	001c	0x00000000	W	Contains the bits 191-160 of the input block value
BLOCK6	0020	0x00000000	W	Contains the bits 223-192 of the input block value
BLOCK7	0024	0x00000000	w	Contains the bits 255-224 of the input block value
BLOCK8	0028	0x00000000	w	Contains the bits 287-256 of the input block value
BLOCK9	002c	0x00000000	w	Contains the bits 319-288 of the input block value
BLOCK10	0030	0x00000000	w	Contains the bits 351-320 of the input block value
BLOCK11	0034	0x00000000	w	Contains the bits 383-352 of the input block value
BLOCK12	0038	0x00000000	w	Contains the bits 415-384 of the input block value
BLOCK13	003c	0x00000000	w	Contains the bits 447-416 of the input block value
BLOCK14	0040	0x00000000	w	Contains the bits 479-448 of the input block value
BLOCK15	0044	0x00000000	w	Contains the bits 512-480 of the input block value
DIGEST0	0048	0x00000000	w	Contains the bits 31-0 of the input digest value
DIGEST1	004c	0x00000000	w	Contains the bits 63-32 of the input digest value
DIGEST2	0050	0x00000000	w	Contains the bits 95-64 of the input digest value
DIGEST3	0054	0x00000000	w	Contains the bits 127-96 of the input digest value
DIGEST4	0058	0x00000000	w	Contains the bits 159-128 of the input digest value
DIGEST5	005c	0x00000000	w	Contains the bits 191-160 of the input digest value
DIGEST6	0060	0x00000000	w	Contains the bits 223-192 of the input digest value
DIGEST7	0064	0x00000000	w	Contains the bits 255-224 of the input digest value
IM	ff00	0x00000000	W	Interrupt Mask Register; write 1/0 to enable/disable interrupts; check the interrupt flags table for more details
RIS	ff08	0x00000000	w	Raw Interrupt Status; reflects the current interrupts status; check the interrupt flags table for more details

Name	Offset	Reset Value	Access Mode	Description
MIS	ff04	0x00000000	W	Masked Interrupt Status; On a read, this register gives the current masked status value of the corresponding interrupt. A write has no effect; check the interrupt flags table for more details
IC	ff0c	0x00000000	w	Interrupt Clear Register; On a write of 1, the corresponding interrupt (both raw interrupt and masked interrupt, if enabled) is cleared; check the interrupt flags table for more details
GCLK	ff10	0x00000000	w	Gated clock enable; 1: enable clock, 0: disable clock

# STATUS Register [Offset: 0x0, mode: r]

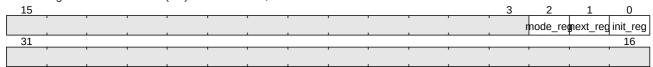
Status register bit 0: digest is valid , bit 1: ready



bit	field name	width	description
6	ready_reg	1	Ready to start
7	digest_valid_reg	1	Digest is valid

# CTRL Register [Offset: 0x4, mode: w]

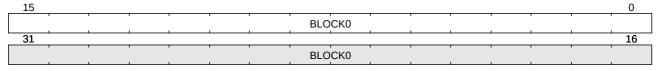
Control register bit 0: Initial bit (init) bit 1: Next bit , bit 2: Mode bit



bit	field name	width	description
0	init_reg	1	Initial bit
1	next_reg	1	Next bit
2	mode_reg	1	Mode bit; "0" means SHA224 "1" means SHA256"

## BLOCK0 Register [Offset: 0x8, mode: w]

Contains the bits 31-0 of the input block value



# BLOCK1 Register [Offset: 0xc, mode: w]

15			block va	iiao					
1 1	T.	· 	·	1		1	-	-	1 1
31				1	BLOCK1				
'	1	•	•	-	BLOCK1	,	1	1	1
	,				' '		<u> </u>		
OCK2 Re	aister (C	)ffset:	0x10. r	mode:	w1				
	_								
tains the bits 5	s 95-64 of t	he input	block va	lue					
<del>-</del> ,	1	•	ı	-	BLOCK2	,	1	-	, ,
1		-	-					-	
	,				BLOCK2		•		
OCK3 Re	gister [C	ffset:	0x14, r	mode:	w]				
ains the bits	: 127-96 of	the innu	t hlock v	alue					
5	3 127 30 01	пе пра	t block v	uiuc					
					BLOCK3		· 		
1	•		•	•	BLOCK3	•	•	•	
				1	BLOCK3				
ains the bits	_				w]				
tains the bits	_				w]	, ,	,		
OCK4 Retains the bits	_				BLOCK4		<u>,                                     </u>		<u> </u>
tains the bits	_				_				
tains the bits	s 159-128 (	of the inp	ut block	value	BLOCK4				
tains the bits 5 1  OCK5 Re	gister [C	of the inp	ox1c, r	value mode:	BLOCK4		,		
cains the bits  DCK5 Recains the bits	gister [C	of the inp	ox1c, r	value mode:	BLOCK4				
cains the bits  DCK5 Recains the bits	gister [C	of the inp	ox1c, r	value mode:	BLOCK4				
DCK5 Retains the bits	gister [C	of the inp	ox1c, r	value mode:	BLOCK4  BLOCK5				
tains the bits	gister [C	of the inp	ox1c, r	value mode:	BLOCK4  BLOCK4				
CALCARD TO THE SECOND TO THE S	gister [C	Offset:	0x1c, r	value  mode: value	BLOCK4  BLOCK5  BLOCK5				
CALCARD TO THE SECOND TO THE S	gister [C	Offset:	0x1c, r	value  mode: value	BLOCK4  BLOCK5  BLOCK5				
DCK5 Recains the bits  1  DCK6 Recains the bits	gister [C	Offset:	0x1c, r ut block	value  mode: value  mode: value	BLOCK4  BLOCK5  BLOCK5		,		
DCK5 Recains the bits  DCK6 Recains the bits	gister [C	Offset:	0x1c, r ut block	value  mode: value  mode: value	BLOCK4  BLOCK5  BLOCK5				
DCK5 Recains the bits  1  CK6 Recains the bits  1	gister [C	Offset:	0x1c, r ut block	value  mode: value  mode: value	BLOCK4  BLOCK5  BLOCK5				
DCK5 Recains the bits  1  CK6 Recains the bits  1	gister [C	Offset:	0x1c, r ut block	value  mode: value  mode: value	BLOCK4  BLOCK5  BLOCK5  BLOCK5				
DCK5 Recains the bits  1  CK6 Recains the bits  1	gister [C	Offset:	0x1c, r ut block	value  mode: value  mode: value	BLOCK4  BLOCK5  BLOCK5  BLOCK5				
DCK5 Retains the bits  1  CK6 Retains the bits  1	gister [C gister [C s 191-160 (	Offset: Of the inp	Ox1c, r ut block  Ox20, r ut block	value  mode:  value  value	BLOCK4  BLOCK5  BLOCK5  BLOCK6  BLOCK6				
DCK5 Retains the bits  1  CK6 Retains the bits  1	gister [C gister [C s 191-160 (	Offset: Of the inp	Ox1c, r ut block  Ox20, r ut block	value  mode:  value  value	BLOCK4  BLOCK5  BLOCK5  BLOCK6  BLOCK6				
DCK5 Retains the bits	gister [C	Offset: Offset: Offset:	0x1c, r ut block  0x20, r ut block	value  mode: value  value  mode: value	BLOCK4  BLOCK5  BLOCK5  BLOCK6  BLOCK6				

BLOCK7

BLOCK8 Register [Offset: 0x28, mode: w]

Contains the bit	s 287-256 o	f the input b	olock value					0
15				BLOCK8	, ,			0
31	1		,	BLOCK8			1	16
1 1			· · · · · · · · · · · · · · · · · · ·	1 1			<u>'</u>	
BLOCK9 Re	gister [O	ffset: 0x2	2c, mode:	w]				
Contains the bit	s 319-288 o	f the input k	olock value					
15	·		·	BLOCK9	1 1	<u> </u>		0
31			1	BLOCK9	1 1			16
	,			BLOCKS				
BLOCK10 R	egister [(	Offset: 0	x30, mode	: w]				
Contains the bit	s 351-320 o	f the input k	olock value					
15				PLOCK10			1 1	0
31				BLOCK10				16
				BLOCK10				
	ogiotor [(	Officet. O	v24 mode	. wal				
BLOCK11 R				: vv]				
Contains the bit	s 383-352 o	f the input b	olock value					0
				BLOCK11		,	1 1	10
31				BLOCK11				16
	·		·		·	·		
BLOCK12 R	egister [0	Offset: 0	x38, mode	: w]				
Contains the bit	s 415-384 o	f the input b	olock value					
15	-		1	BLOCK12	1 1	1	1	, 0
31				BLOCK12			-	16
	,		,	BLOCKIZ				
BLOCK13 R	egister [0	Offset: 0:	x3c, mode	: w]				
Contains the bit	_			-				
15		- i i i i i i i i i i i i i i i i i i i			, ,			0
31	-		-	BLOCK13				16
,	<u>'</u>	' '	'	BLOCK13		<u>'</u>		,
DI 001/11 -		officer of						
BLOCK14 R	egister [C	חנ: 0Σ	x4u, mode	: w]				
Contains the bit	s 479-448 o	f the input b	olock value					0
			1	BLOCK14		,		
31	,	'		BLOCK14	,		, ,	16
	1		1	22001121	1	1		1

BLOCK15 Register [Offset: 0x44, mode: w]

IGEST0 Register [Offset: 0x48, mode: w]  Intains the bits 31-0 of the input digest value  IDEST0  IGEST1 Register [Offset: 0x4c, mode: w]  IDEST1  IDEST2  IDEST2  IDEST2  IDEST2  IDEST3  IDEST4  IDEST6  IDEST6  IDEST7  IDE	15	512-480 of the input bloc	A Value			0
GEST0 Register [Offset: 0x48, mode: w]  Intains the bits 31-0 of the input digest value  15  DIGEST0  GEST1 Register [Offset: 0x4c, mode: w]  Intains the bits 63-32 of the input digest value  15  DIGEST1  GEST2 Register [Offset: 0x50, mode: w]  Intains the bits 95-64 of the input digest value  15  DIGEST2  GEST3 Register [Offset: 0x54, mode: w]  Intains the bits 127-96 of the input digest value  15  DIGEST3  GEST4 Register [Offset: 0x58, mode: w]  Intains the bits 159-128 of the input digest value  15  DIGEST3  GEST4 Register [Offset: 0x58, mode: w]  Intains the bits 159-128 of the input digest value  15  DIGEST3  GEST5 Register [Offset: 0x58, mode: w]  Intains the bits 159-128 of the input digest value  15  DIGEST4  GEST5 Register [Offset: 0x5c, mode: w]  Intains the bits 191-160 of the input digest value  15  DIGEST4  DIGEST5  DIGEST5			BLOCK15			
GEST0 Register [Offset: 0x48, mode: w]  ontains the bits 31-0 of the input digest value  15  DIGEST0  31  DIGEST0  GEST1 Register [Offset: 0x4c, mode: w]  ontains the bits 63-32 of the input digest value  15  DIGEST1  31  DIGEST1  GEST2 Register [Offset: 0x50, mode: w]  ontains the bits 95-64 of the input digest value  15  DIGEST2  GEST3 Register [Offset: 0x54, mode: w]  ontains the bits 127-96 of the input digest value  15  DIGEST3  GEST4 Register [Offset: 0x58, mode: w]  ontains the bits 159-128 of the input digest value  15  DIGEST3  GEST5 Register [Offset: 0x58, mode: w]  ontains the bits 159-128 of the input digest value  15  DIGEST3  GEST5 Register [Offset: 0x5c, mode: w]  ontains the bits 159-126 of the input digest value  15  DIGEST4  GEST5 Register [Offset: 0x5c, mode: w]  ontains the bits 191-160 of the input digest value  15  DIGEST5  DIGEST5	31		BI OCK15	1 1	1 1 1	<u> </u>
Intains the bits 31-0 of the input digest value    15			5200110	- '		
Intains the bits 31-0 of the input digest value    15	GESTO Rec	uister [Offset: Ny48	mode: wl			
15  DIGESTO  31  DIGESTO  GEST1 Register [Offset: 0x4c, mode: w]  Intains the bits 63-32 of the input digest value  15  DIGEST1  GEST2 Register [Offset: 0x50, mode: w]  Intains the bits 95-64 of the input digest value  15  DIGEST2  GEST3 Register [Offset: 0x54, mode: w]  Intains the bits 127-96 of the input digest value  15  DIGEST3  GEST4 Register [Offset: 0x58, mode: w]  Intains the bits 159-128 of the input digest value  15  DIGEST3  GEST4 Register [Offset: 0x58, mode: w]  Intains the bits 159-128 of the input digest value  15  DIGEST4  GEST5 Register [Offset: 0x5c, mode: w]  Intains the bits 191-160 of the input digest value  15  DIGEST4  DIGEST4  DIGEST5		<u>-</u>	<u>-</u>			
GEST1 Register [Offset: 0x4c, mode: w]  ntains the bits 63-32 of the input digest value  15  DIGEST1  31  DIGEST1  31  DIGEST1  GEST2 Register [Offset: 0x50, mode: w]  ntains the bits 95-64 of the input digest value  15  DIGEST2  31  DIGEST2  GEST3 Register [Offset: 0x54, mode: w]  ntains the bits 127-96 of the input digest value  15  DIGEST3  GEST4 Register [Offset: 0x58, mode: w]  ntains the bits 159-128 of the input digest value  15  DIGEST3  GEST4 Register [Offset: 0x58, mode: w]  ntains the bits 159-128 of the input digest value  15  DIGEST4  GEST5 Register [Offset: 0x5c, mode: w]  ntains the bits 191-160 of the input digest value  15  DIGEST5  DIGEST4		31-0 of the input digest v	alue			C
GEST1 Register [Offset: 0x4c, mode: w]  ntains the bits 63-32 of the input digest value  15  DIGEST1  31  DIGEST1  GEST2 Register [Offset: 0x50, mode: w]  ntains the bits 95-64 of the input digest value  15  DIGEST2  GEST3 Register [Offset: 0x54, mode: w]  ntains the bits 127-96 of the input digest value  15  DIGEST3  GEST4 Register [Offset: 0x58, mode: w]  ntains the bits 159-128 of the input digest value  15  DIGEST3  GEST4 Register [Offset: 0x58, mode: w]  ntains the bits 159-128 of the input digest value  15  DIGEST4  GEST5 Register [Offset: 0x5c, mode: w]  ntains the bits 191-160 of the input digest value  15  DIGEST4  GEST5 Register [Offset: 0x5c, mode: w]  ntains the bits 191-160 of the input digest value  15  DIGEST5	1 1		DIGEST0	1 1	1 1	
GEST1 Register [Offset: 0x4c, mode: w]  ntains the bits 63-32 of the input digest value  15  DIGEST1  GEST2 Register [Offset: 0x50, mode: w]  ntains the bits 95-64 of the input digest value  15  DIGEST2  31  DIGEST2  31  DIGEST3  GEST3 Register [Offset: 0x54, mode: w]  ntains the bits 127-96 of the input digest value  15  DIGEST3  GEST4 Register [Offset: 0x58, mode: w]  ntains the bits 159-128 of the input digest value  15  DIGEST3  GEST4 Register [Offset: 0x58, mode: w]  ntains the bits 159-128 of the input digest value  15  DIGEST4  GEST5 Register [Offset: 0x5c, mode: w]  ntains the bits 191-160 of the input digest value  15  DIGEST5  DIGEST4	31					1
ntains the bits 63-32 of the input digest value  15  DIGEST1  GEST2 Register [Offset: 0x50, mode: w]  Intains the bits 95-64 of the input digest value  15  DIGEST2  GEST3 Register [Offset: 0x54, mode: w]  Intains the bits 127-96 of the input digest value  15  DIGEST3  GEST3 Register [Offset: 0x54, mode: w]  Intains the bits 127-96 of the input digest value  15  DIGEST3  GEST4 Register [Offset: 0x58, mode: w]  Intains the bits 159-128 of the input digest value  15  DIGEST4  GEST5 Register [Offset: 0x5c, mode: w]  Intains the bits 191-160 of the input digest value  15  DIGEST4  GEST5 Register [Offset: 0x5c, mode: w]  Intains the bits 191-160 of the input digest value  15  DIGEST5  DIGEST5	1		DIGEST0			
ntains the bits 63-32 of the input digest value  15  DIGEST1  GEST2 Register [Offset: 0x50, mode: w]  Intains the bits 95-64 of the input digest value  15  DIGEST2  GEST3 Register [Offset: 0x54, mode: w]  Intains the bits 127-96 of the input digest value  15  DIGEST3  GEST3 Register [Offset: 0x54, mode: w]  Intains the bits 127-96 of the input digest value  15  DIGEST3  GEST4 Register [Offset: 0x58, mode: w]  Intains the bits 159-128 of the input digest value  15  DIGEST4  GEST5 Register [Offset: 0x5c, mode: w]  Intains the bits 191-160 of the input digest value  15  DIGEST4						
DIGEST1  DIGEST1  GEST2 Register [Offset: 0x50, mode: w]  Intains the bits 95-64 of the input digest value  DIGEST2  DIGEST2  GEST3 Register [Offset: 0x54, mode: w]  Intains the bits 127-96 of the input digest value  DIGEST3  GEST4 Register [Offset: 0x58, mode: w]  Intains the bits 159-128 of the input digest value  DIGEST3  GEST4 Register [Offset: 0x58, mode: w]  Intains the bits 159-128 of the input digest value  DIGEST4  GEST5 Register [Offset: 0x5c, mode: w]  Intains the bits 191-160 of the input digest value  DIGEST5  DIGEST4	GEST1 Reg	Jister [Offset: 0x4c	, mode: wj			
DIGEST1  DIGEST1  DIGEST1  GEST2 Register [Offset: 0x50, mode: w]  ntains the bits 95-64 of the input digest value  15  DIGEST2  DIGEST2  JUSEST2  GEST3 Register [Offset: 0x54, mode: w]  ntains the bits 127-96 of the input digest value  15  DIGEST3  GEST4 Register [Offset: 0x58, mode: w]  ntains the bits 159-128 of the input digest value  15  DIGEST3  GEST4 Register [Offset: 0x58, mode: w]  ntains the bits 159-128 of the input digest value  15  DIGEST4  GEST5 Register [Offset: 0x5c, mode: w]  ntains the bits 191-160 of the input digest value  15  DIGEST4	ntains the bits	63-32 of the input digest	value			
GEST2 Register [Offset: 0x50, mode: w]  ntains the bits 95-64 of the input digest value  15  DIGEST2  31  DIGEST2  GEST3 Register [Offset: 0x54, mode: w]  ntains the bits 127-96 of the input digest value  15  DIGEST3  GEST4 Register [Offset: 0x58, mode: w]  ntains the bits 159-128 of the input digest value  15  DIGEST3  GEST4 Register [Offset: 0x58, mode: w]  ntains the bits 159-128 of the input digest value  15  DIGEST4  GEST5 Register [Offset: 0x5c, mode: w]  ntains the bits 191-160 of the input digest value  15  DIGEST4	15				1	, (
GEST2 Register [Offset: 0x50, mode: w]  Intains the bits 95-64 of the input digest value  15  DIGEST2  31  DIGEST2  GEST3 Register [Offset: 0x54, mode: w]  Intains the bits 127-96 of the input digest value  15  DIGEST3  GEST4 Register [Offset: 0x58, mode: w]  Intains the bits 159-128 of the input digest value  15  DIGEST3  GEST4 Register [Offset: 0x58, mode: w]  Intains the bits 159-128 of the input digest value  15  DIGEST4  GEST5 Register [Offset: 0x5c, mode: w]  Intains the bits 191-160 of the input digest value  15  DIGEST4	31		DIGEST1			1
ntains the bits 95-64 of the input digest value    DIGEST2	, ,		DIGEST1	1	, ,	, -
ntains the bits 95-64 of the input digest value  DIGEST2  DIGEST2  GEST3 Register [Offset: 0x54, mode: w]  ntains the bits 127-96 of the input digest value  DIGEST3  DIGEST3  DIGEST3  DIGEST3  GEST4 Register [Offset: 0x58, mode: w]  ntains the bits 159-128 of the input digest value  DIGEST4  DIGEST4  GEST5 Register [Offset: 0x5c, mode: w]  ntains the bits 191-160 of the input digest value  DIGEST4	<u> </u>					
ntains the bits 95-64 of the input digest value    DIGEST2	GEST2 Red	uister (Offset: 0x50	mode: wl			
DIGEST2  31  DIGEST2  GEST3 Register [Offset: 0x54, mode: w]  Intains the bits 127-96 of the input digest value 15  DIGEST3  DIGEST3  GEST4 Register [Offset: 0x58, mode: w]  Intains the bits 159-128 of the input digest value 15  DIGEST4  GEST5 Register [Offset: 0x5c, mode: w]  Intains the bits 191-160 of the input digest value 15  DIGEST4  DIGEST4	OLOTZ Neg	ister [Oliset: 0x30	, mode. Wj			
IGEST3 Register [Offset: 0x54, mode: w]  Intains the bits 127-96 of the input digest value  15  DIGEST3  IGEST4 Register [Offset: 0x58, mode: w]  Intains the bits 159-128 of the input digest value  15  DIGEST4  IGEST5  DIGEST4  IGEST5 Register [Offset: 0x5c, mode: w]		95-64 of the input digest	value			_
IGEST3 Register [Offset: 0x54, mode: w]  Intains the bits 127-96 of the input digest value  15  DIGEST3  IGEST4 Register [Offset: 0x58, mode: w]  Intains the bits 159-128 of the input digest value  15  DIGEST4  IGEST5  DIGEST4  IGEST5 Register [Offset: 0x5c, mode: w]  INTAIN DIGEST4  IGEST5 Register [Offset: 0x5c, mode: w]  INTAIN DIGEST5  DIGEST5  DIGEST5  DIGEST5  DIGEST5	15		DIGEST2	- t	T T	, (
IGEST3 Register [Offset: 0x54, mode: w]  Intains the bits 127-96 of the input digest value  IDIGEST3  IDIGEST3  IDIGEST3  IDIGEST4  IDIGEST4  IDIGEST4  IDIGEST4  IDIGEST4  IDIGEST5  IDIGEST5  IDIGEST5  IDIGEST6  IDIGEST7  IDIG	31		5.02012			1
ntains the bits 127-96 of the input digest value  DIGEST3  DIGEST3  DIGEST3  GEST4 Register [Offset: 0x58, mode: w]  ntains the bits 159-128 of the input digest value  DIGEST4  DIGEST4  GEST5 Register [Offset: 0x5c, mode: w]  ntains the bits 191-160 of the input digest value  DIGEST5  DIGEST5			DIGEST2			·
ntains the bits 127-96 of the input digest value  DIGEST3  DIGEST3  DIGEST3  GEST4 Register [Offset: 0x58, mode: w]  ntains the bits 159-128 of the input digest value  DIGEST4  DIGEST4  GEST5 Register [Offset: 0x5c, mode: w]  ntains the bits 191-160 of the input digest value  DIGEST5  DIGEST5						
DIGEST3  31  DIGEST3  GEST4 Register [Offset: 0x58, mode: w]  ntains the bits 159-128 of the input digest value  15  DIGEST4  31  DIGEST4  GEST5 Register [Offset: 0x5c, mode: w]  ntains the bits 191-160 of the input digest value  15  DIGEST5	GEST3 Reg	jister [Offset: 0x54	, mode: w]			
DIGEST3  31  DIGEST3  DIGEST3  DIGEST4  DIGEST4  DIGEST4  DIGEST4  DIGEST4  DIGEST4  DIGEST4  DIGEST4  DIGEST4  DIGEST5	entaine the hite	127 06 of the input diges	t value			
GEST4 Register [Offset: 0x58, mode: w]  Intains the bits 159-128 of the input digest value  DIGEST4  DIGEST4  GEST5 Register [Offset: 0x5c, mode: w]  Intains the bits 191-160 of the input digest value  DIGEST5  DIGEST5		127-90 of the input diges	t value			(
GEST4 Register [Offset: 0x58, mode: w]  Intains the bits 159-128 of the input digest value  15  DIGEST4  31  DIGEST4  GEST5 Register [Offset: 0x5c, mode: w]  Intains the bits 191-160 of the input digest value  15  DIGEST5		<u> </u>	DIGEST3	<u> </u>	· · · ·	<u> </u>
GEST4 Register [Offset: 0x58, mode: w]  ontains the bits 159-128 of the input digest value  15  DIGEST4  31  DIGEST4  GEST5 Register [Offset: 0x5c, mode: w]  ontains the bits 191-160 of the input digest value  15  DIGEST5	31		DIOFCTO			
ntains the bits 159-128 of the input digest value  DIGEST4  DIGEST4  GEST5 Register [Offset: 0x5c, mode: w]  ntains the bits 191-160 of the input digest value  DIGEST5			DIGESTS			
ntains the bits 159-128 of the input digest value  DIGEST4  DIGEST4  GEST5 Register [Offset: 0x5c, mode: w]  ntains the bits 191-160 of the input digest value  DIGEST5  DIGEST5	050545	1-1				
DIGEST4  31  DIGEST4  GEST5 Register [Offset: 0x5c, mode: w]  Intains the bits 191-160 of the input digest value  15  DIGEST5	GES14 Reg	Jister [Offset: 0x58	, mode: wj			
DIGEST4  31  DIGEST4  DIGEST4  DIGEST5 Register [Offset: 0x5c, mode: w]  Ontains the bits 191-160 of the input digest value  15  DIGEST5	ontains the bits	159-128 of the input dige	est value			
DIGEST4  DIGEST4  DIGEST5 Register [Offset: 0x5c, mode: w]  Ontains the bits 191-160 of the input digest value  15  DIGEST5	15	<del></del>	<del></del>	<del></del>	<del> </del>	(
DIGEST4  GEST5 Register [Offset: 0x5c, mode: w]  Intains the bits 191-160 of the input digest value  15  DIGEST5	21		DIGEST4			1
GEST5 Register [Offset: 0x5c, mode: w] Intains the bits 191-160 of the input digest value  DIGEST5	<u>, , , , , , , , , , , , , , , , , , , </u>	1 1	DIGEST4	1	, ,	, 1
ntains the bits 191-160 of the input digest value  15  DIGEST5			2.02011	1		
ntains the bits 191-160 of the input digest value  15  DIGEST5		iotor [Offoot: 0:-	modo, wl			
15 DIGEST5	CECTE Das	Jister [Uliset: UX5C	, mode: wj			
15 DIGEST5	GEST5 Reg	_				
		<u>-</u>	est value			
	ontains the bits	<u>-</u>	1 1			(

DIGEST5

DIGEST6 Register [Offset: 0x60, mode: w]

Contains the bits 223-192 of the input digest value

15									0
				DIGE	ST6				
31									16
				DIGE	ST6				

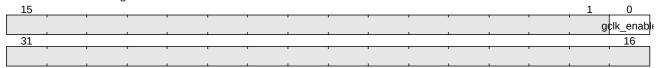
## DIGEST7 Register [Offset: 0x64, mode: w]

Contains the bits 255-224 of the input digest value

15									0
				DIGE	ST7				
31									16
				DIGE	ST7				

## GCLK Register [Offset: 0xff10, mode: w]

Gated clock enable register



bit	field name	width	description
0	gclk_enable	1	Gated clock enable; 1: enable clock, 0: disable clock

## **Interrupt Flags**

The wrapped IP provides four registers to deal with interrupts: IM, RIS, MIS and IC. These registers exist for all wrapper types.

Each register has a group of bits for the interrupt sources/flags.

- IM [offset: 0xff00]: is used to enable/disable interrupt sources.
- RIS [offset: 0xff08]: has the current interrupt status (interrupt flags) whether they are enabled or disabled.
- MIS [offset: 0xff04]: is the result of masking (ANDing) RIS by IM.
- IC [offset: 0xff0c]: is used to clear an interrupt flag.

The following are the bit definitions for the interrupt registers:

Bit	Flag	Width	Description
0	VALID	1	Digest is valid
1	READY	1	Ready to start

#### **Clock Gating**

The IP includes a clock gating feature that allows selective activation and deactivation of the clock using the GCLK register. This capability is implemented through the ef\_util\_gating\_cell module, which is part of the common modules library, ef\_util\_lib.v. By default, the clock gating is disabled. To enable behavioral implmentation clock gating, only for simulation purposes, you should define the CLKG\_GENERIC macro. Alternatively, define the CLKG\_SKY130\_HD macro if you wish to use the SKY130 HD library clock gating cell, sky130\_fd\_sc\_hd\_dlclkp\_4.

**Note:** If you choose the <a href="OpenLane2">OpenLane2</a> flow for implementation and would like to enable the clock gating feature, you need to add <a href="CLKG\_SKY130\_HD">CLKG\_SKY130\_HD</a> macro to the <a href="VERILOG\_DEFINES">VERILOG\_DEFINES</a> configuration variable. Update OpenLane2 YAML configuration file as follows:

```
VERILOG_DEFINES:
- CLKG_SKY130_HD
```

#### **Firmware Drivers:**

Firmware drivers for EF\_SHA256 can be found in the <u>Drivers</u> directory in the <u>EFIS</u> (Efabless Firmware Interface Standard) repo. EF\_SHA256 driver documentation is available <u>here</u>. You can also find an example C application using the EF\_SHA256 drivers here.

#### Installation:

You can install the IP either by cloning this repository or by using IPM.

### 1. Using IPM:

- [Optional] If you do not have IPM installed, follow the installation guide here
- After installing IPM, execute the following command ipm install EF\_SHA256.

Note: This method is recommended as it automatically installs **EF\_IP\_UTIL** as a dependency.

#### 2. Cloning this repo:

- Clone <u>EF\_IP\_UTIL</u> repository, which includes the required modules from the common modules library, <u>ef\_util\_lib.v.</u> git clone https://github.com/efabless/EF\_IP\_UTIL.git
- Clone the IP repository git clone github.com/efabless/SW\_SHA256

#### The Wrapped IP Interface

**NOTE:** This section is intended for advanced users who wish to gain more information about the interface of the wrapped IP, in case they want to create their own wrappers.

```
wire [255 : 0]
         wire -
                 clk
                                        ready
                                        digest
         wire -
                  reset n
         wire =
                 init
                                  digest_valid
                                                 - wire
         wire -
                 next
         wire -
                 mode
wire [511:0] =
                 block
```

#### **Ports**

Port	Direction	Width	Description
init	input	1	Initial bit
next	input	1	Next bit
mode	input	1	Mode bit; '0' means SHA224 '1' means SHA256
block	input	512	block value
ready	output	1	ready to start

Port	Direction	Width	Description
digest	output	256	digest value
digest_valid	output	1	digest is valid