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:

```
EF_SHA256_WB INST (
        .clk_i(clk_i),
        .rst_i(rst_i),
        .adr_i(adr_i),
        .dat_i(dat_i),
        .dat_o(dat_o),
        .sel_i(sel_i),
        .cyc_i(cyc_i),
        .stb_i(stb_i),
        .ack_o(ack_o),
        .we_i(we_i),
        .IRQ(irq),
);
```

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 Interrupt Flags 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 OpenLane2 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

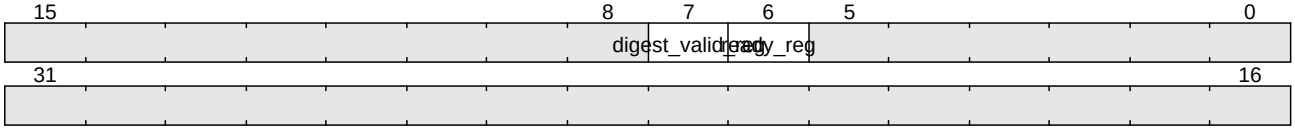
Registers

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	0008	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]

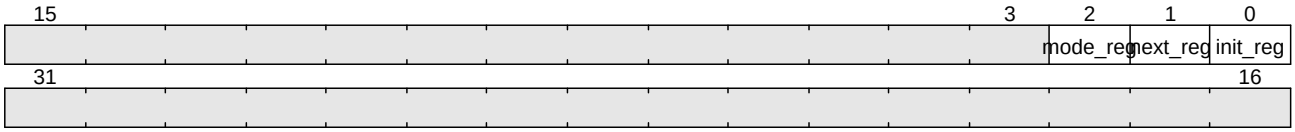
Status register bit 0: digest is valid , bit 1: ready



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]

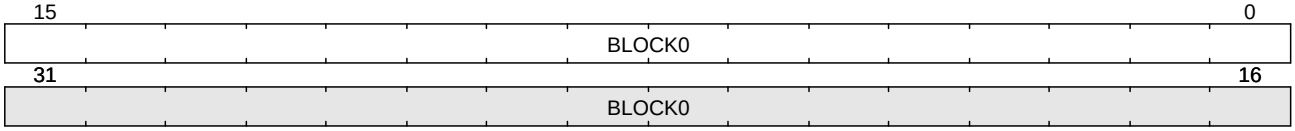
Control register bit 0: Initial bit (init) bit 1: Next bit , bit 2: Mode bit



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"

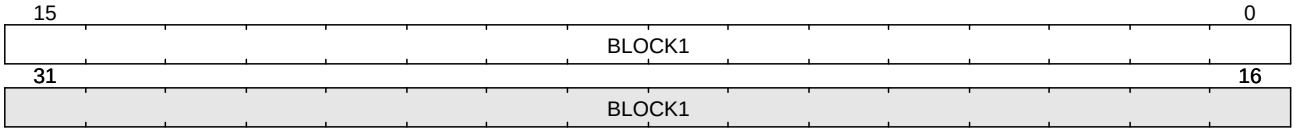
BLOCK0 Register [Offset: 0x8, mode: w]

Contains the bits 31-0 of the input block value



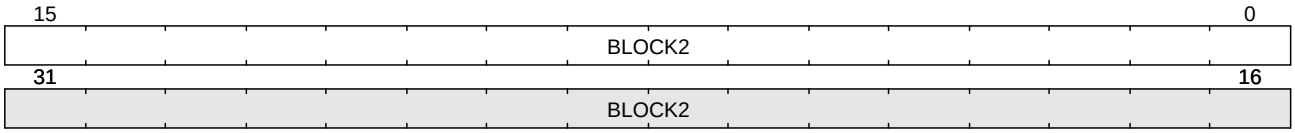
BLOCK1 Register [Offset: 0xc, mode: w]

Contains the bits 63-32 of the input block value



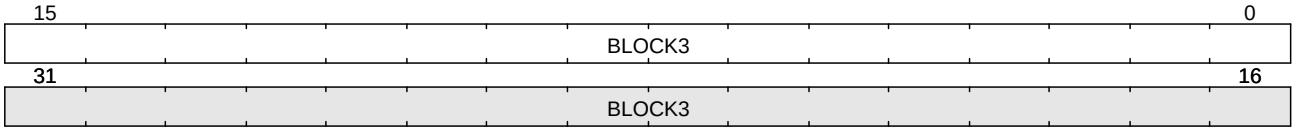
BLOCK2 Register [Offset: 0x10, mode: w]

Contains the bits 95-64 of the input block value



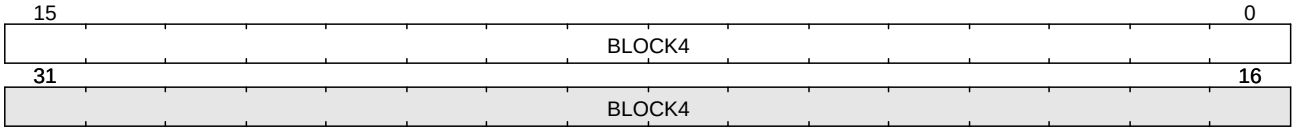
BLOCK3 Register [Offset: 0x14, mode: w]

Contains the bits 127-96 of the input block value



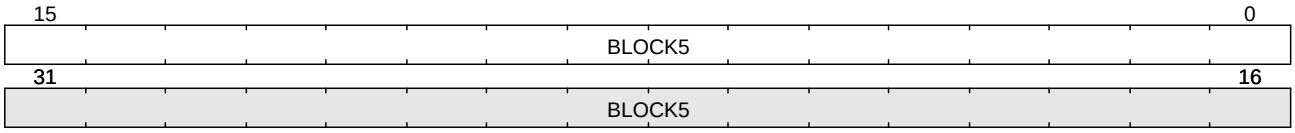
BLOCK4 Register [Offset: 0x18, mode: w]

Contains the bits 159-128 of the input block value



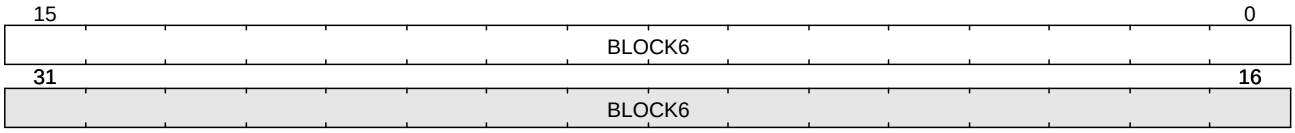
BLOCK5 Register [Offset: 0x1c, mode: w]

Contains the bits 191-160 of the input block value



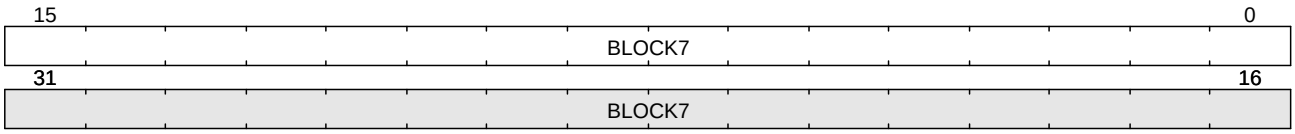
BLOCK6 Register [Offset: 0x20, mode: w]

Contains the bits 223-192 of the input block value



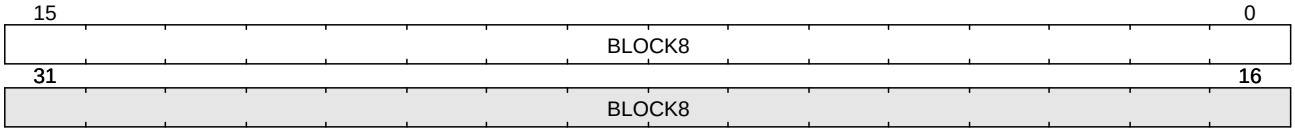
BLOCK7 Register [Offset: 0x24, mode: w]

Contains the bits 255-224 of the input block value



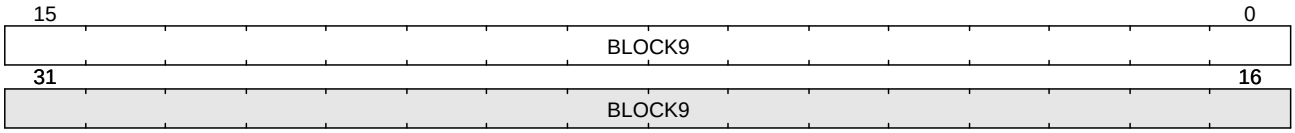
BLOCK8 Register [Offset: 0x28, mode: w]

Contains the bits 287-256 of the input block value



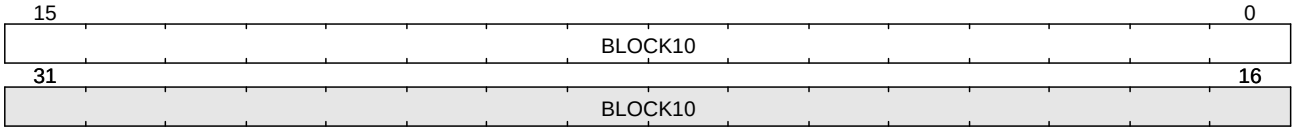
BLOCK9 Register [Offset: 0x2c, mode: w]

Contains the bits 319-288 of the input block value



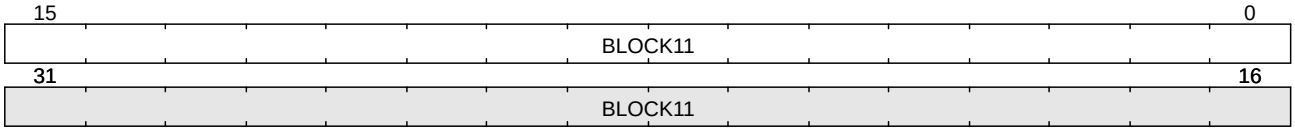
BLOCK10 Register [Offset: 0x30, mode: w]

Contains the bits 351-320 of the input block value



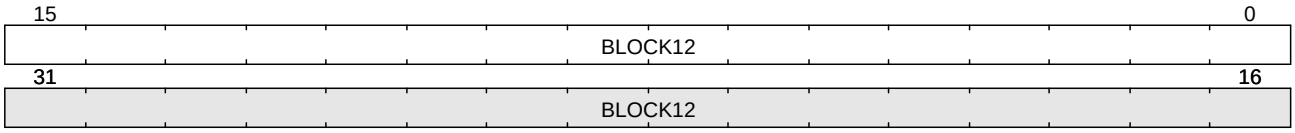
BLOCK11 Register [Offset: 0x34, mode: w]

Contains the bits 383-352 of the input block value



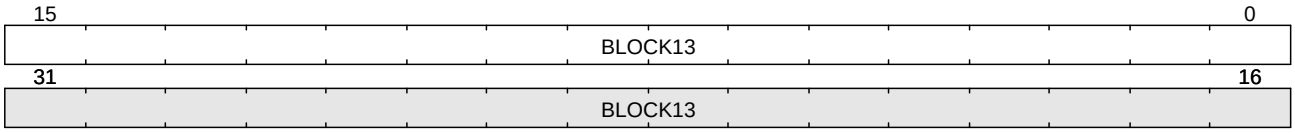
BLOCK12 Register [Offset: 0x38, mode: w]

Contains the bits 415-384 of the input block value



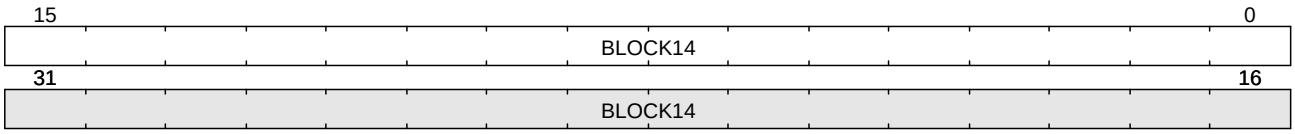
BLOCK13 Register [Offset: 0x3c, mode: w]

Contains the bits 447-416 of the input block value



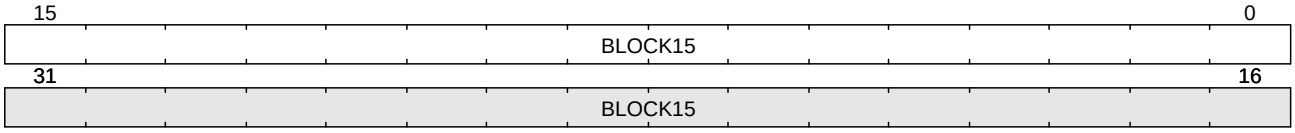
BLOCK14 Register [Offset: 0x40, mode: w]

Contains the bits 479-448 of the input block value



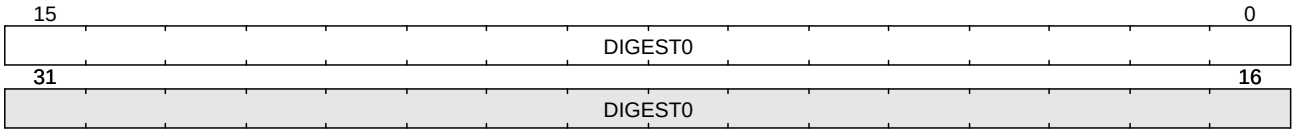
BLOCK15 Register [Offset: 0x44, mode: w]

Contains the bits 512-480 of the input block value



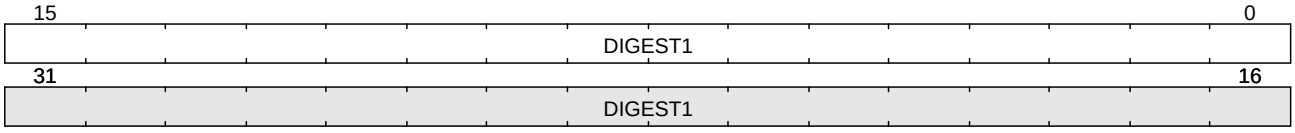
DIGEST0 Register [Offset: 0x48, mode: w]

Contains the bits 31-0 of the input digest value



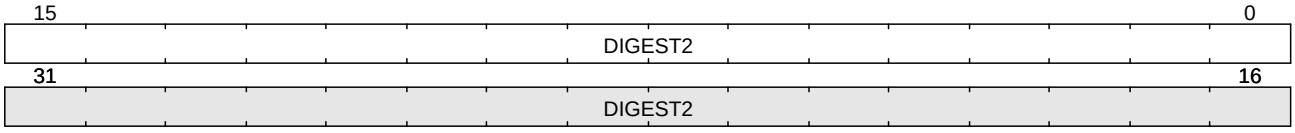
DIGEST1 Register [Offset: 0x4c, mode: w]

Contains the bits 63-32 of the input digest value



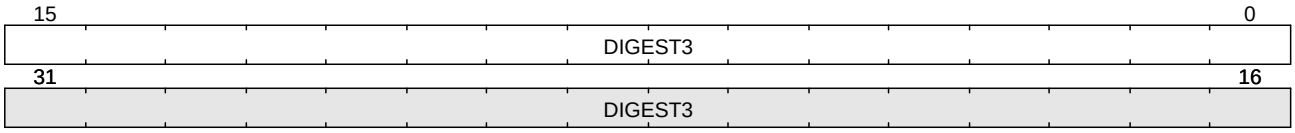
DIGEST2 Register [Offset: 0x50, mode: w]

Contains the bits 95-64 of the input digest value



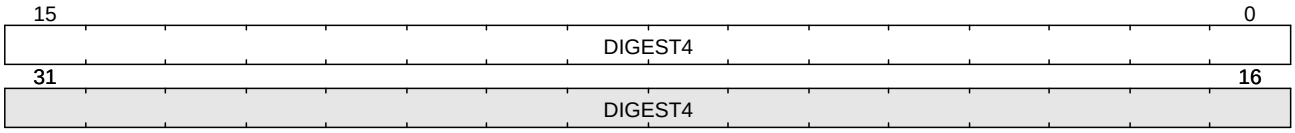
DIGEST3 Register [Offset: 0x54, mode: w]

Contains the bits 127-96 of the input digest value



DIGEST4 Register [Offset: 0x58, mode: w]

Contains the bits 159-128 of the input digest value

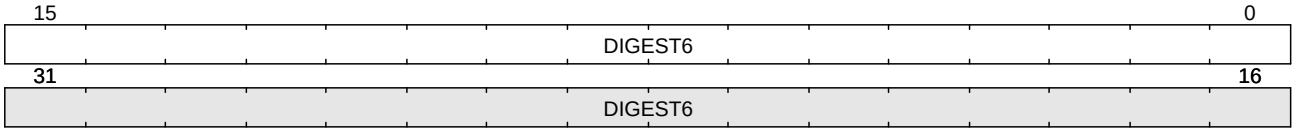


DIGEST5 Register [Offset: 0x5c, mode: w]

Contains the bits 191-160 of the input digest value

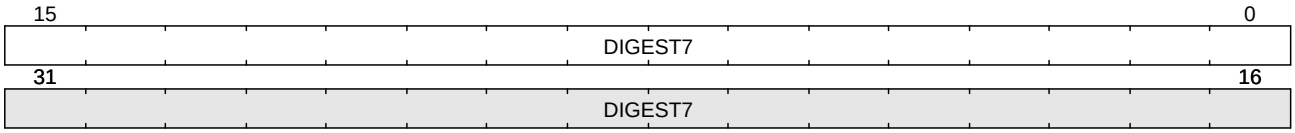
DIGEST6 Register [Offset: 0x60, mode: w]

Contains the bits 223-192 of the input digest value



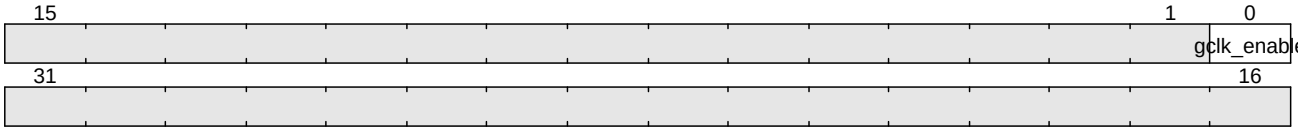
DIGEST7 Register [Offset: 0x64, mode: w]

Contains the bits 255-224 of the input digest value



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 OpenLane2 flow for implementation and would like to enable the clock gating feature, you need to add `CLKG_SKY130_HD` macro to the `VERILOG_DEFINES` 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 Drivers directory in the EFIS (Efabless Firmware Interface Standard) repo. EF_SHA256 driver documentation is available here. 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 .`

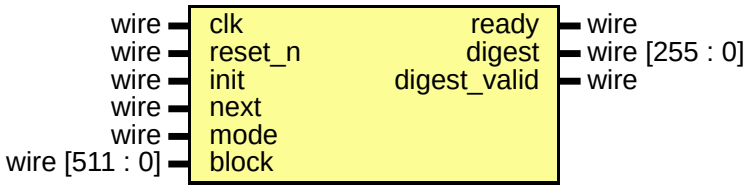
> **Note:** This method is recommended as it automatically installs EF_IP_UTIL as a dependency.

2. Cloning this repo:

- Clone EF_IP_UTIL repository, which includes the required modules from the common modules library, ef_util_lib.v.
  `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.



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