AISS Alpha Release Document (03/01/2021)

Security IP: Secure Hash Algorithm 2 (HW Acc.)

[Category] For <update following field> template v1.0
TDD ID: TA1.1.5 Task 5
Name: Security IP (BAA Track C)
Version: <a change will replicate through-out the document>1.0
Author(s): Tanvir Rahman, Fahim Rahman
Date: <automatically updated> March 1, 2021

ABSTRACT

This document contains the alpha release information of the hardware cryptographic implementation of secure hash algorithm (SHA-2). This IP is intended to be used within the cryptographic boundary of the security engine.

DATA RIGHTS

Document Revision History:

Version	Date	Author	Change Description
1.0	3/1/2021	FR	Initial version

Table of Contents

List of Figures

List of Tables

1. Introduction

1.1 Purpose

The purpose of this document is to inform AISS program performers and the DARPA IV&V team of the alpha release information to implement and enable the hardware cryptographic implementation of secure hash algorithm 2 (SHA-2) within the cryptographic boundary of the security engine of the developed system-on-chip design.

1.2 Scope

This document outlines the functional and design description for the current alpha release of the developed IP of to meet the Phase 1 functional goals of the AISS program. It also lists necessary assumptions, dependencies, test results, and next release target goals.

2. Solution Description: Hardware Secure Hash Algorithm 2 (SHA-2)

2.1 Phase 1 Functional Goals

Secure hash algorithm 2 (SHA-2) is a cryptographic hash function by NIST. A hardware SHA-2 module is developed to perform target operations in hardware within the cryptographic boundary of the security engine in addition to the software operation to be performed by the host/SE processor. The Phase 1 functional goals for this task is to provide **hardware operations of SHA-2 algorithm for bit sizes of 256b, 384b, and 512b**.

2.2 Release Highlights

In accordance with our milestone and deliverables timeline (as established in previous quarters), we summarize the current release deliverables as follows.

Table 1: Release Highlights of RSA

Subtask	Timeline (Target)	Deliverables	Status	Current Release
1.5.6.1 IP Draft Design	03/01/2021	High-level design schematics and high-level state machine flow diagram	Done	Yes
1.5.6.2 Base version of IP in HDL SHA-2 (256b)	03/01/2021	Base IP in HDL to perform secure hashing operation	Done	Yes

1.5.6.3 Functional Verification of base IP	03/01/2021	Verified base IP including simulation results	Done	Yes
1.5.6.4 Base SHA-2 IP in HDL with expanded key size (384b, 512b)	03/01/2021	Base IP in HDL to perform secure hashing operation	Done	Yes
1.5.6.5 Functional Verification of base IP (256b, 384b, 512b)	03/01/2021	Verified base IP including simulation results	Done	Yes

2.3 Description

2.3.1 Design Description

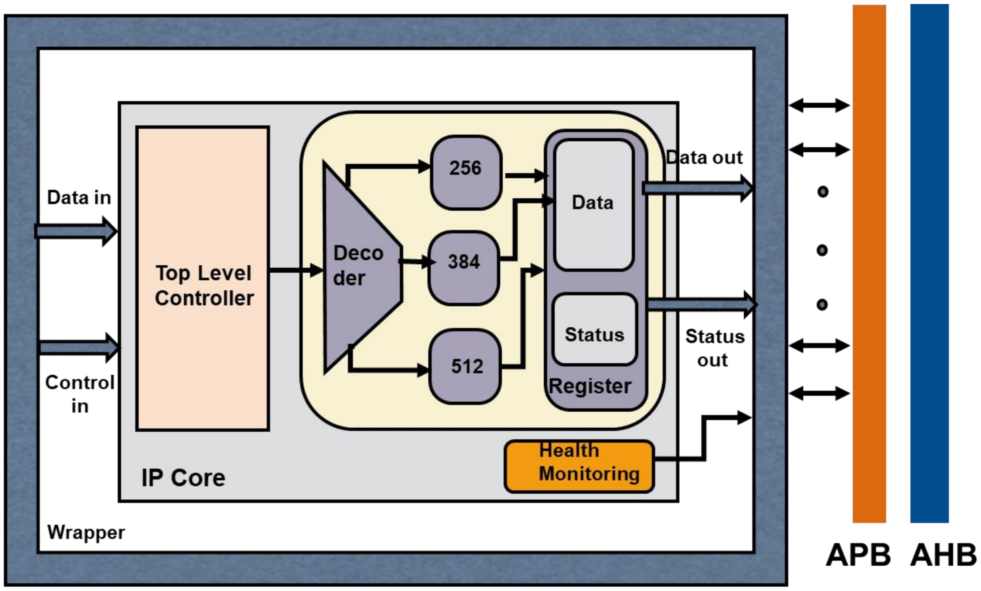

Figure 1: SHA-2 IP Design Schematics

The goal of developing SHA-2 hardware IP is to provide secure hashing of any input message. Figure 1 shows all the blocks/entities of the SHA-2 hashing IP. In this submission we are only developing the base version of IP, so the health monitoring block is not present, rather it will be included in our next phase where we will develop the advanced version of IP.

Wrapper: The wrapper module takes care of all the IP communication with the Master through the bus. As the size requirements of data and control i/o signals can be larger than the bus capacity, the wrapper module is going to take care of this limitation. The design and working principle of the wrapper is out of the scope of this work and submission.

Top-level controller: This controller takes all the basic input control and data signals required for the proper IP functionality. This controller controls the proper functional states within the IP and communicates with an outside entity (wrapper/ master) with necessary outputs or status.

2.3.2 Functional Description

To start the IP user needs to input a clock to the block and general guidelines would be to reset the system before use.

Data will be read in windows of 1024 bits. This will be stored in the data register that is only available when the write enable is active. This is to prevent starting an operation before another operation completes.

Function Bits register (not shown in the block diagram) will work the same as input data. This is to protect the integrity of the operation.

Next, the master will need to send the ‘go’ signal to start an operation from the controller. The controller will then send a logic ‘1’ signal to the Decoder which will use the function_bits register to start the correct function.

When the function completes, the data will be stored in a 512b register array and the bus will receive a “Done” signal to know that data is ready to be read. The bus/wrapper then needs to read and then send read_en.

All the output data and status bits are registered. All the specific data and control signals (input/output) and their sizes are listed in table 2.

Table 2:List of I/O signals and their specifications of SHA-2 IP

Signal Name	Signal Type	Size	Description
Reset	Control (in)	1 bit	Resets the SHA-2 block
Go	Control (in)	1 bit	Activates the SHA-2 block
Function_bit	Control (in)	2 bit	Modes of SHA-2 o/p
Flag	data (out)	1 bit	Any runtime status (advanced version)
Read_complete	Control (in)	1 bit	The master device must acknowledge the data read being complete

Busy	Data (out)	1 bit	SHA-2 block is busy
Output	Data (out)	512b	Output Data
Data_in	Data (in)	1024b	Input data
Clock	Data (in)	Clock pulse (1/0)	Required clock
Done	Control(out)	1 bit	Current o/p is complete
Read_en	Control (out)	1 bit	Data can be sent out to the wrapper
Write_en	Control (in)	1 bit	This stores the input data to the input register

2.3.3 Simulation Results

A sample snippet of the simulation result of the developed SHA-2 IP is Shown in Figure 2. A detailed testbench and simulation results are provided in the shared files.

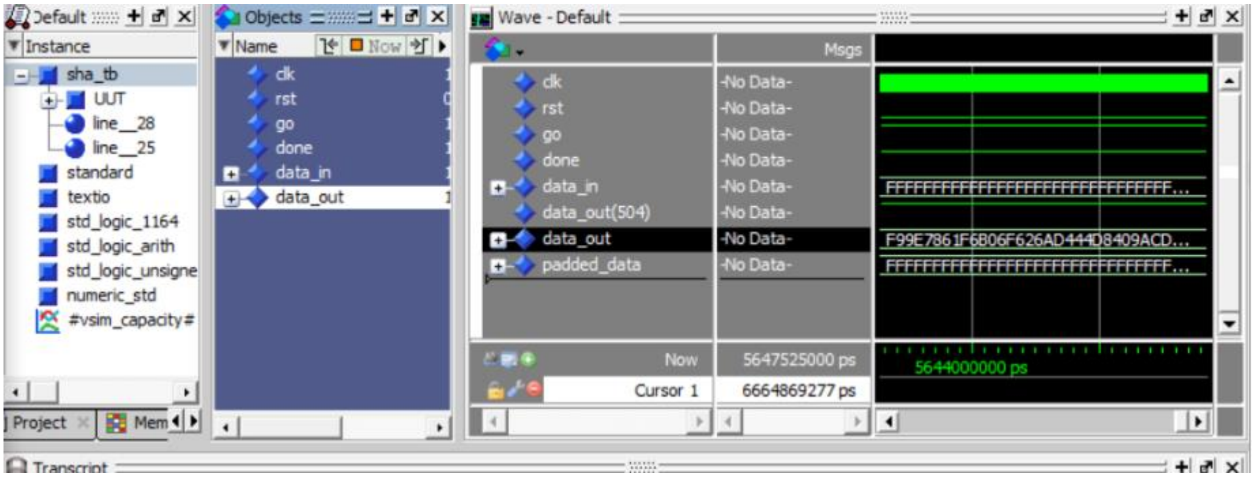

Figure 2: Simulation result for SHA-2 IP

2.4 Delivered Materials:

The delivered material is one zip file that contains SHA-2 IP and associated materials (SHA2_all_v01.zip). The zip file contains all the HDL codes along with the test bench, readme.txt, and simulation screenshot. This IP supports the functionality of SHA-2 256b, 384b and 512b.

3. Target features/deliverables for next release

Target deliverables of the next release for the RSA IP are listed in table 3.

Table 3: Target deliverables of the SHA-2 IP

Subtask	Timeline	Deliverable Format
1.5.6.6 Implementing base reusable SHA-2 IP for user interaction (256b, 384b, 512b)	06/01/2021	Executable SHA-2 IP in RTL (per user-provided selection of specs within design limit)
1.5.6.7 Mitigated SHA-2 IP Draft Design	06/01/2021	High-level design schematics and high-level state machine flow diagram of the mitigated SHA-2 IP
1.5.6.8 Implementing mitigated version/s of SHA-2 IP (V1)	06/01/2021	Power and side-channel attack resistant standalone version/s of H/W SHA-2 IP in HDL

4. Assumptions

1. IP will receive the input data to match with the exact bit sizes as defined by the table.
2. Wrapper will take care of the communication between bus and IP and other external modules.
3. Base version of IP will not exhibit any mitigation capabilities.

5. Limitations

1. Variables in the HDL code provided will not exactly match with the names presented in the schematic in few cases, however, the working principle and concept presented here remain perfectly aligned between the HDL code and schematics design.
2. All three blocks of SHA-2 hashing functionality are going to produce an output of 512b. In the case of 256b/384b hashing function selection, the output will be zero-padded to make 512b of output, so Wrapper or Master can ignore those padded zeros in case the hashing function is selected to be 256b/384b. The reason is, currently, our top-level design supports only one output data size (512b).
3. Currently the design is not optimized for performance.

6. Library and Environment

- IEEE standard HDL library

7. IP Rights

As determined by Synopsys and University of Florida.

8. References

- N/A

9. Appendix

Video of the IP runtime simulation can be found at
https://youtu.be/eB8x4tNMSGA