SHA2-IP Demo Instruction

SHA2-IP Demo Instruction

Rev1.00 22-Apr-2025

This document provides instructions for demonstrating the operation of SHA2-IP on the KCU116 Evaluation Board. In this demonstration, users can test the functionality of SHA2-IP using custom input messages and evaluate its performance via the serial console. The following sections detail the environment setup, test menu and results.

1 Environment Setup

To operate SHA2-IP demo, please prepare following test environment.

1) FPGA development board (KCU116 Evaluation Board).
2) Test PC.
3) Micro USB cable for JTAG connection between FPGA board and Test PC.
4) Micro USB cable for UART connection between FPGA board and Test PC.
5) Vivado tool for programming FPGA installed on Test PC.
6) Serial console software such as TeraTerm installed on PC. The setting on the console is Baudrate=115,200, Data=8-bit, Non-parity and Stop=1.
7) Demo configuration file (To download this file, please visit our website at www.design-gateway.com).

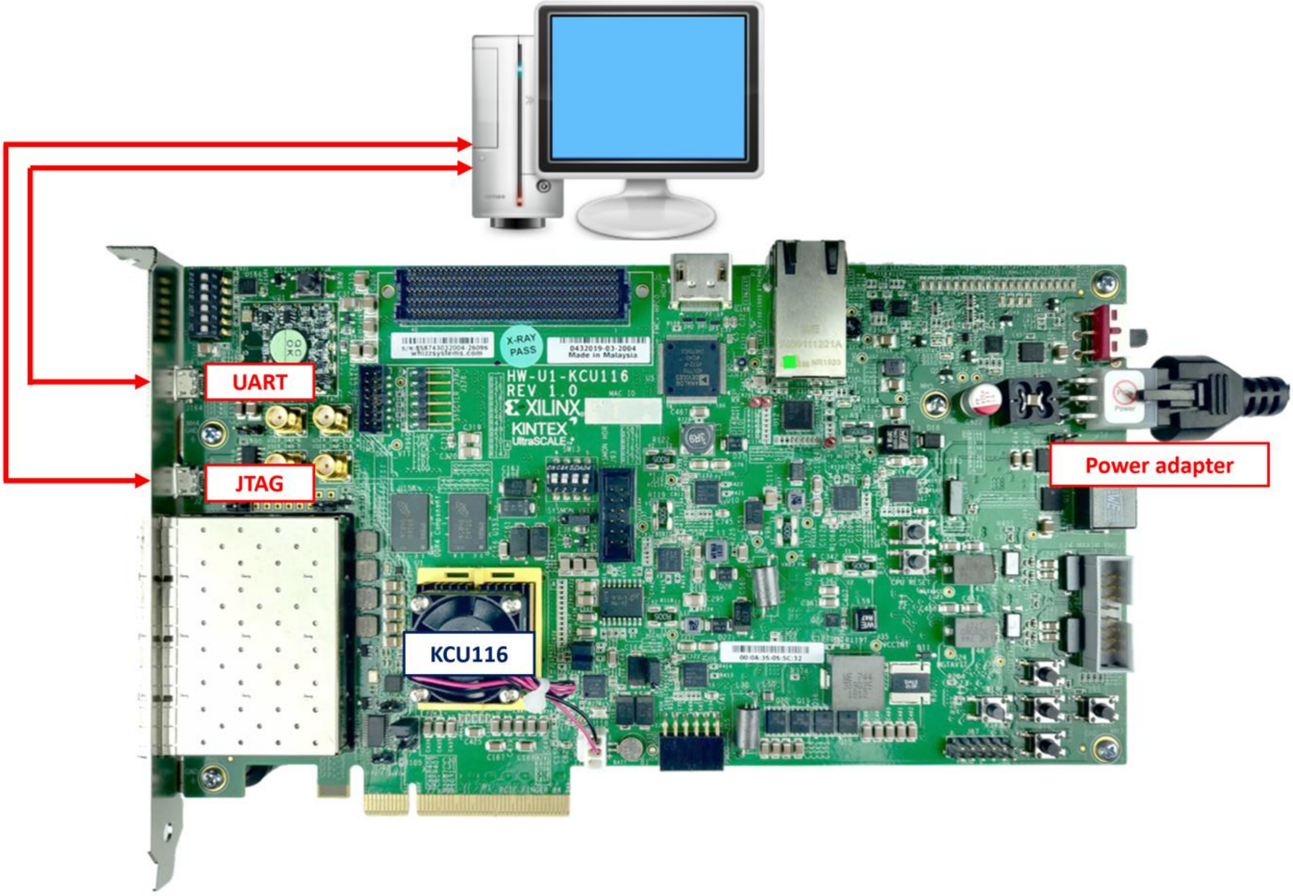
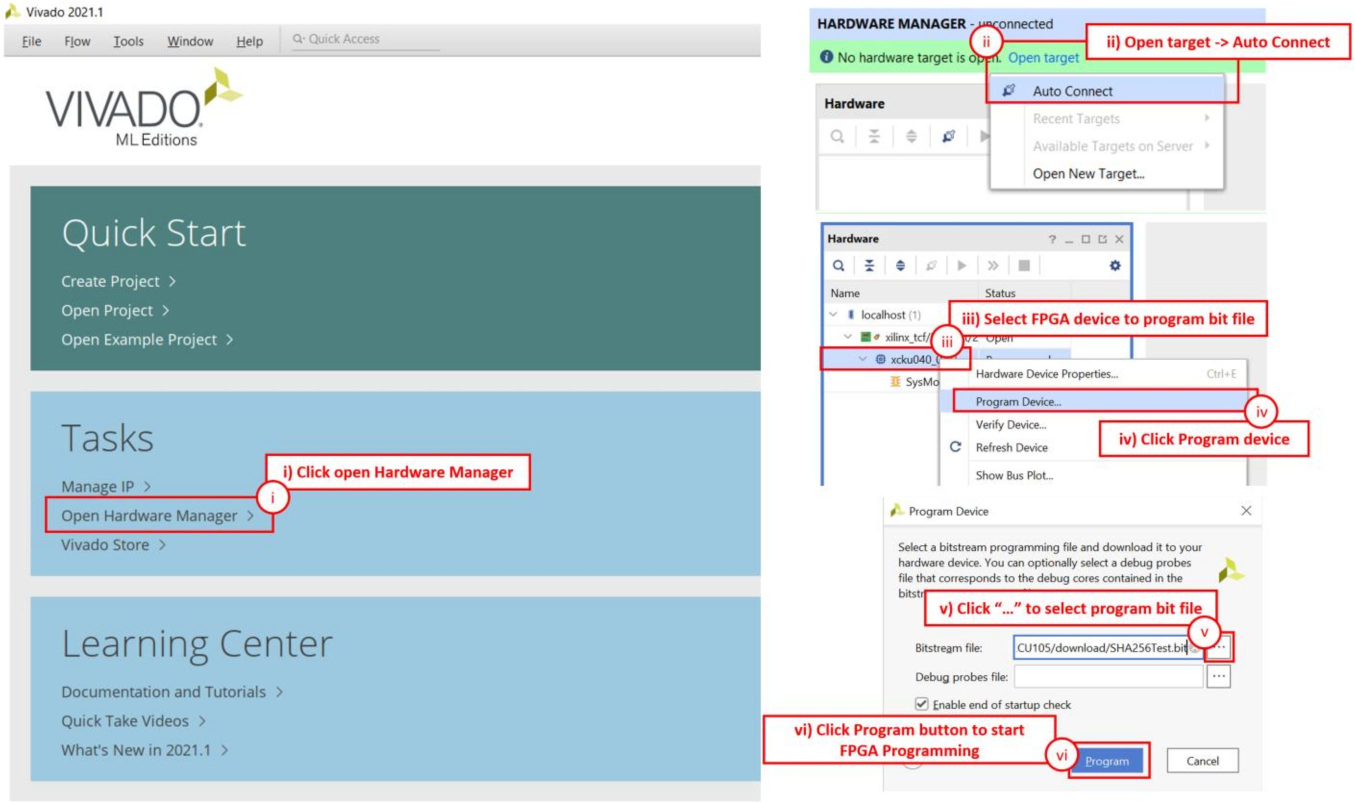


Figure 1 SHA2-IP demo environment on KCU116 board

2 FPGA Development Board Setup

1) Make sure the power switch is off and connect the power supply to KCU105 development board.
2) Connect USB cable between PC to JTAG micro-USB port.
3) Power on the system.
4) Open Vivado Hardware Manager to program FPGA by following steps.
5) Click open Hardware Manager.
   a) Open target -> Auto Connect.
   b) Select FPGA device to program bit file.
   c) Click Program device.
   d) Click "…" to select program bit file.
   e) Click Program button to start FPGA Programming.



i) Click open Hardware Manager

ii) Open target -> Auto Connect

iii) Select FPGA device to program bit file

iv) Click Program device

Select a bitstream programming file and download it to your hardware device. You can optionally select a debug probes file that corresponds to the debug cores contained in the bitstr

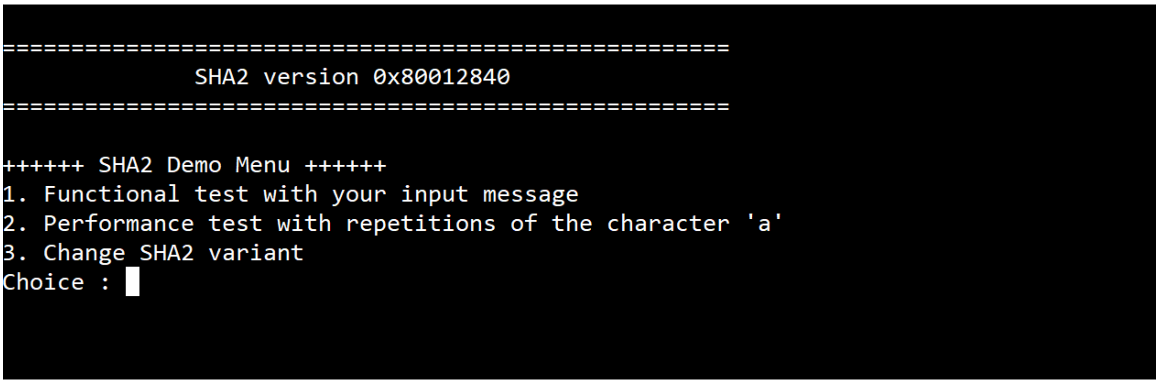
v) Click "…" to select program bit file

vi) Click Program button to start FPGA Programming

Figure 2 Program Device

3 Serial Console

Users can test and monitor the functionality and performance of SHA2-IP via the serial console. When the configuration is complete, the SHA2-IP demo test menu will be displayed, as shown in Figure 3. Details of each menu are described in topic 4.



```
=====================================================
              SHA2 version 0x80012840
=====================================================

++++++ SHA2 Demo Menu ++++++
1. Functional test with your input message
2. Performance test with repetitions of the character 'a'
3. Change SHA2 variant
Choice :
```

Figure 3 Serial Console

4 Test Menu and Results

4.1 Functional Test

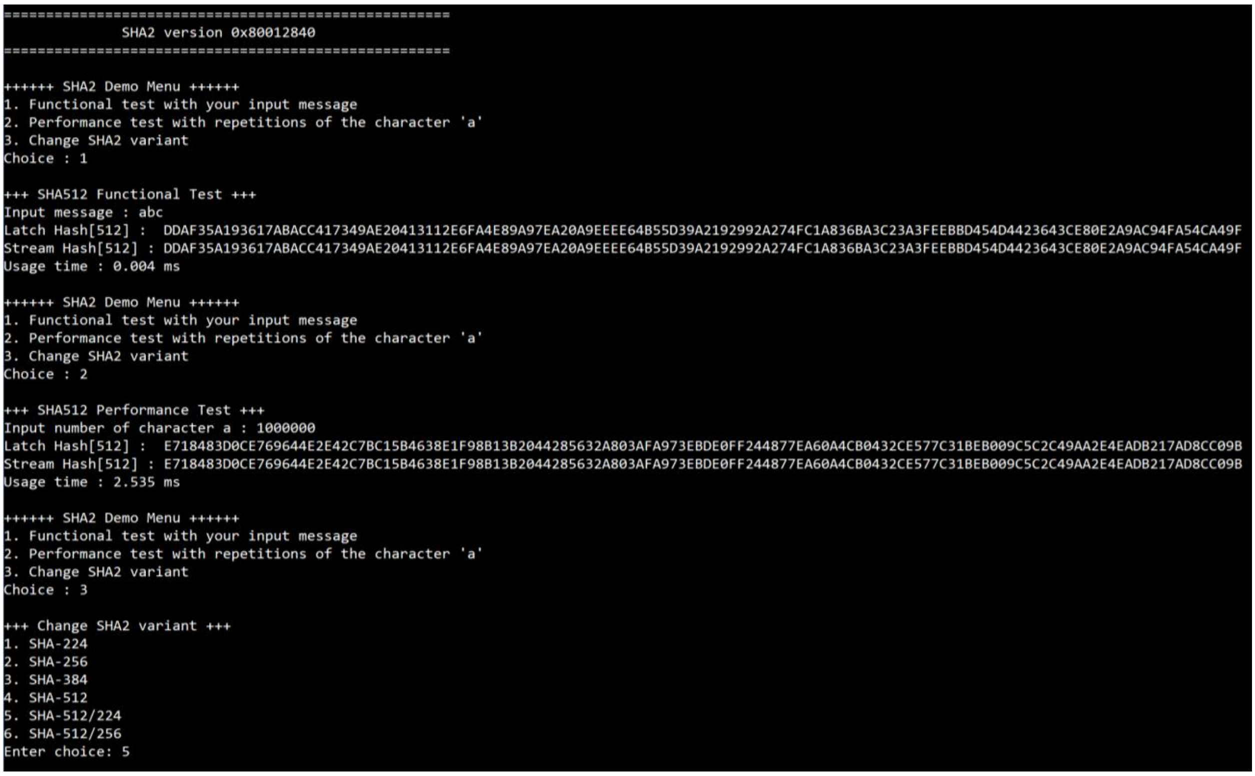
The functional test evaluates the SHA2-IP to generate a hash from a given input. Users can input a message, which is then processed by SHA2-IP to produce a corresponding hash value. The maximum length of the input message is 2047 characters. Additionally, the execution time required for this operation is recorded.

4.2 Performance Test

The performance test evaluates the computational efficiency of the SHA2-IP when processing large volumes of data. Users can enter the length of repeated ‘a’ character, and then the SHA2-IP computes its hash. The execution time is measured to analyze the processing capability under high data loads.

4.3 SHA2 Variant Selection

SHA2-IP supports multiple variants: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, and SHA-512/256. Users can switch between these variants to hash different messages. The default setting is SHA-512.



```
====================================================
              SHA2 version 0x80012840
====================================================

++++++ SHA2 Demo Menu ++++++
1. Functional test with your input message
2. Performance test with repetitions of the character 'a'
3. Change SHA2 variant
Choice : 1

+++ SHA512 Functional Test +++
Input message : abc
Latch Hash[512] :  DDAF35A193617ABACC417349AE20413112E6FA4E89A97EA20A9EEEE64B55D39A2192992A274FC1A836BA3C23A3FEEBBD454D4423643CE80E2A9AC94FA54CA49F
Stream Hash[512] : DDAF35A193617ABACC417349AE20413112E6FA4E89A97EA20A9EEEE64B55D39A2192992A274FC1A836BA3C23A3FEEBBD454D4423643CE80E2A9AC94FA54CA49F
Usage time : 0.004 ms

++++++ SHA2 Demo Menu ++++++
1. Functional test with your input message
2. Performance test with repetitions of the character 'a'
3. Change SHA2 variant
Choice : 2

+++ SHA512 Performance Test +++
Input number of character a : 1000000
Latch Hash[512] :  E718483D0CE769644E2E42C7BC15B4638E1F98B13B2044285632A803AFA973EBDE0FF244877EA60A4CB0432CE577C31BEB009C5C2C49AA2E4EADB217AD8CC09B
Stream Hash[512] : E718483D0CE769644E2E42C7BC15B4638E1F98B13B2044285632A803AFA973EBDE0FF244877EA60A4CB0432CE577C31BEB009C5C2C49AA2E4EADB217AD8CC09B
Usage time : 2.535 ms

++++++ SHA2 Demo Menu ++++++
1. Functional test with your input message
2. Performance test with repetitions of the character 'a'
3. Change SHA2 variant
Choice : 3

+++ Change SHA2 variant +++
1. SHA-224
2. SHA-256
3. SHA-384
4. SHA-512
5. SHA-512/224
6. SHA-512/256
Enter choice: 5
```

Figure 4 SHA2-IP functional and performance test results.

5 Revision History

Revision	Date (D-M-Y)	Description
1.00	22-Apr-25	Initial version release