SHA2-IP Demo Instruction

SHA2-IP Demo Instruction

Rev1.00 23-Apr-2025

This document provides instructions for demonstrating the operation of SHA2-IP on the FPGA 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
   - Agilex7 I-series development kit. or
   - Arria10 SoC Development board.
2) Test PC.
3) Micro USB cable for JTAG connection between FPGA board and Test PC.
4) Quartus programmer for programming FPGA and Nios II command shell, installed on PC.
5) Demo configuration file (To download this file, please visit our web site at www.design-gateway.com).

Figure 1 SHA2-IP demo environment on Agilex7 I-series board

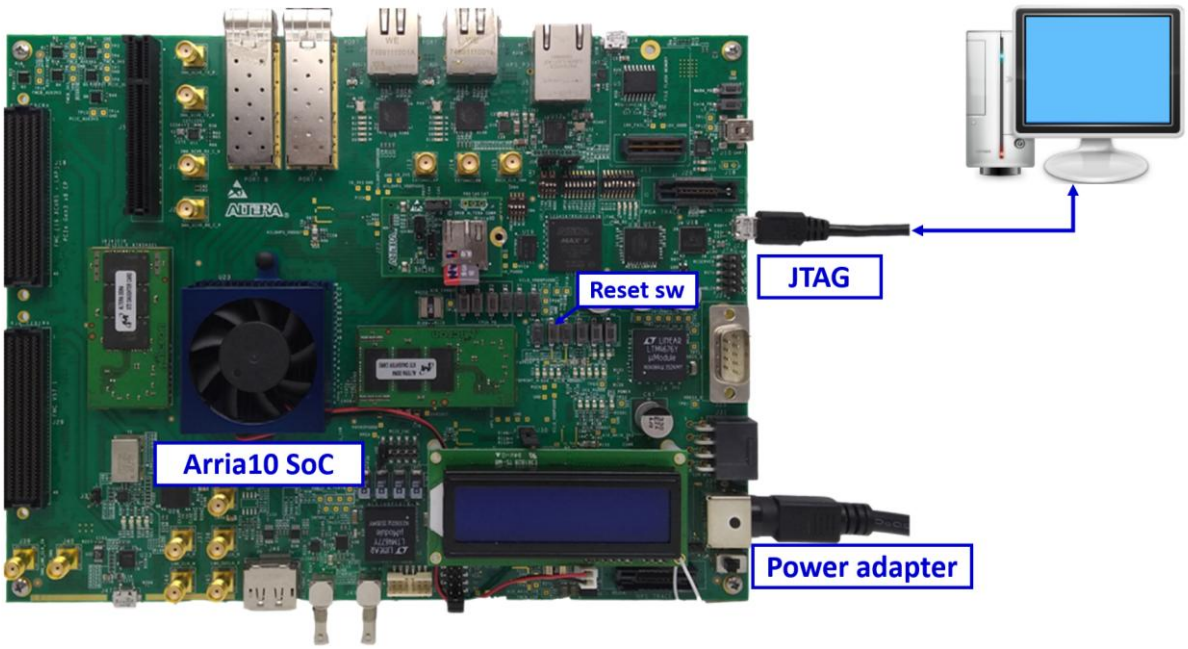

Figure 2 SHA2-IP demo environment on Arria10 SoC board

2 FPGA Development Board Setup

1) Make sure power switch is off and connect power supply to FPGA development board.
2) Connect USB cables between FPGA board and PC via micro-USB ports.
3) Turn on power switch for FPGA board.
4) Open Quartus Programmer to program FPGA through USB-1 by following step.
   i). Click “Hardware Setup…” to select
      - AGI FPGA Development Kit [USB-1] for Agilex7 I-series
      - USB-BlasterII [USB-1] for Arria10 SoC
   ii). Click “Auto Detect” and select FPGA number.
   iii). Select FPGA device icon.
   iv). Click “Change File” button, select SOF file in pop-up window and click “open” button.
   v). Check “program”.
   vi). Click “Start” button to program FPGA.
   vii). Wait until Progress status is equal to 100%.

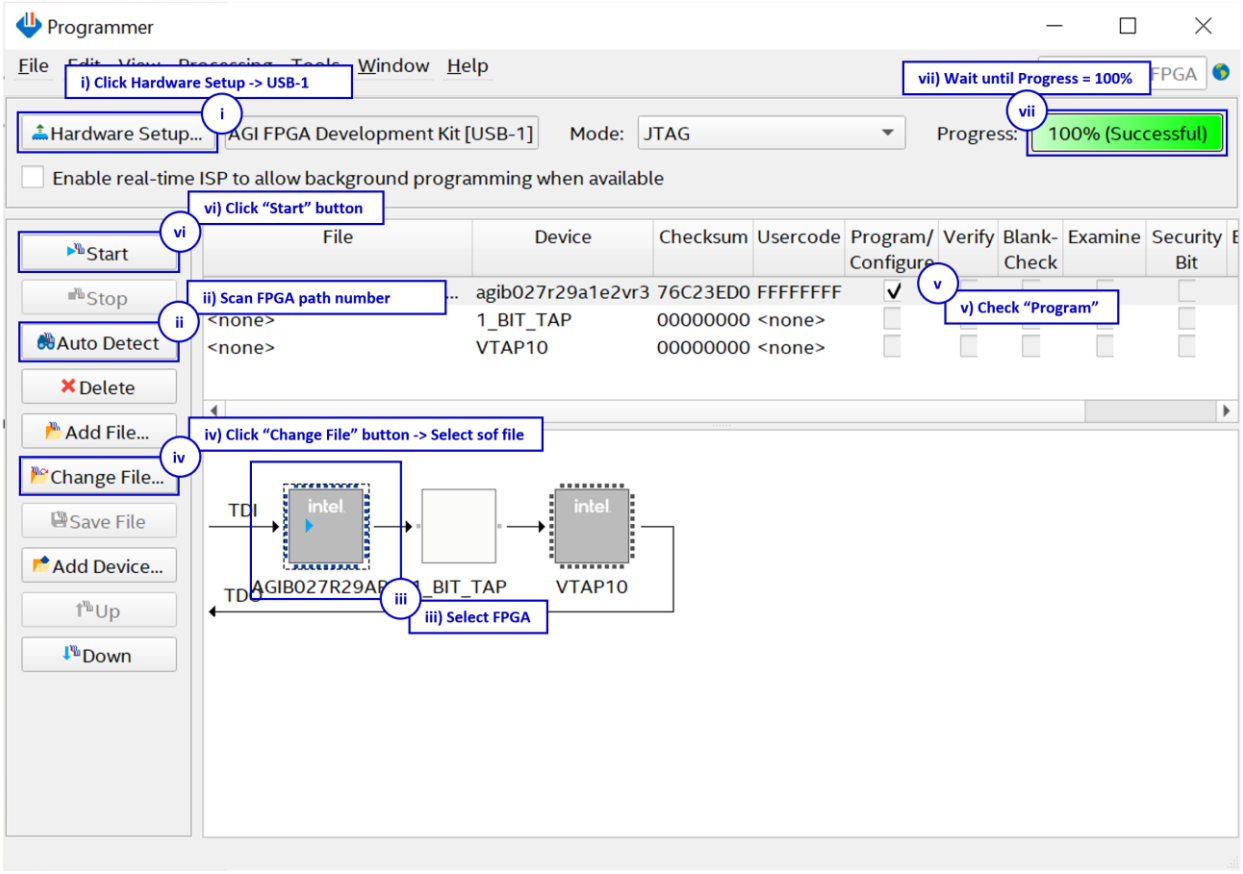

Figure 3 Program Device

For A10SoC after program SOF file complete, Quartus Prime will show popup message of Intel FPGA IP Evaluation Mode Status as shown in Figure 4. Please do not press cancel button.

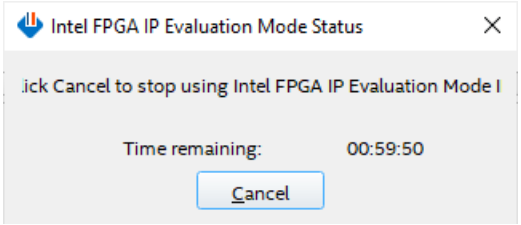

Figure 4 Intel FPGA IP Evaluation Mode Status

3 Nios II Command Shell

Users can test and monitor the functionality and performance of SHA2-IP via Nios II Command Shell. When the configuration is complete, the SHA2-IP demo test menu will be displayed, as shown in Figure 5. Details of each menu are described in topic 4.

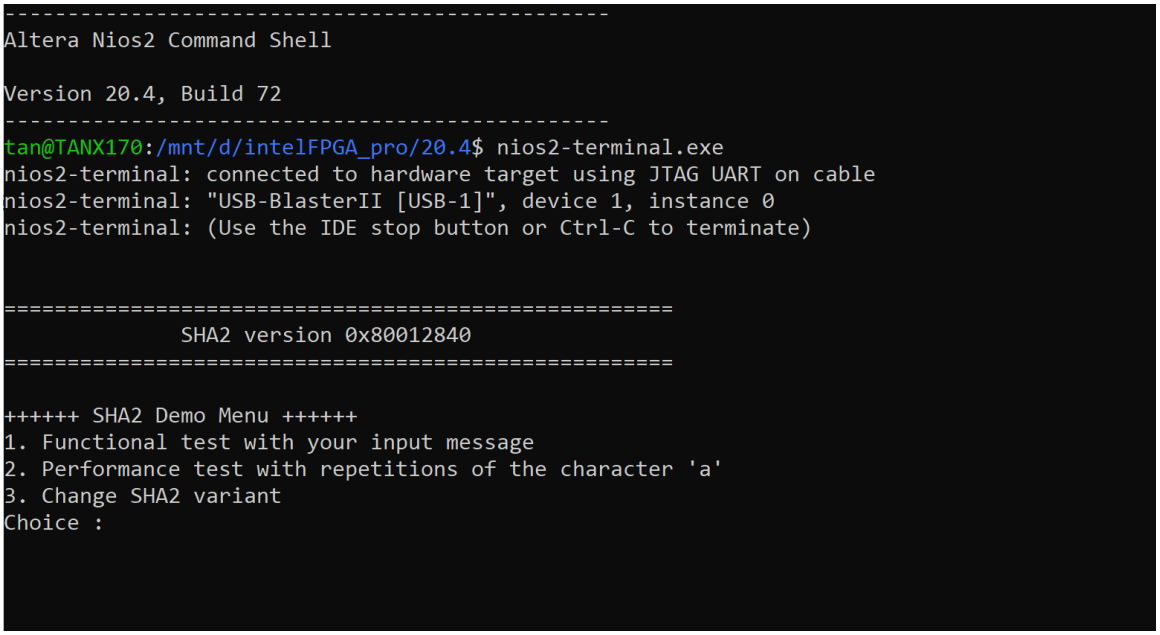

Figure 5 Nios II Command Shell

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.

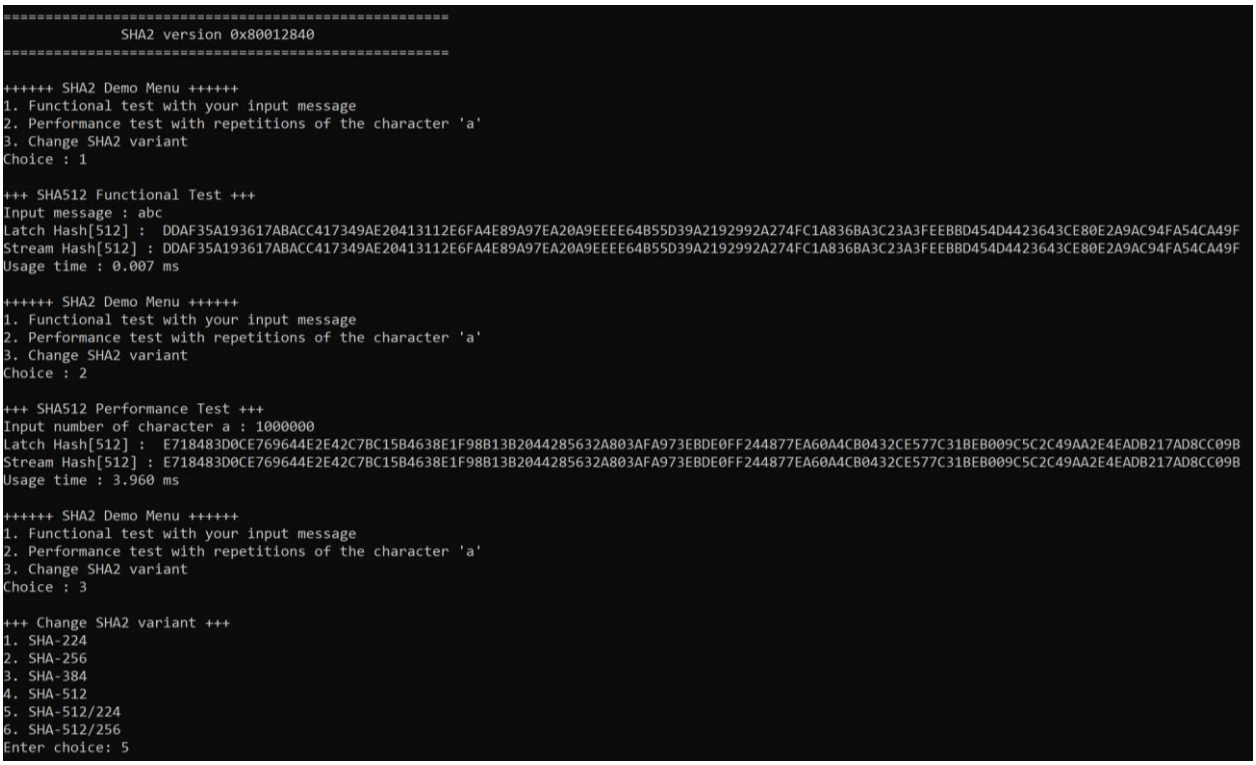

Figure 6 SHA2-IP functional and performance test results.

5 Revision History

Revision	Date (D-M-Y)	Description
1.00	23-Apr-25	Initial version release

