NTHU- EE525500 Design of Chip Security- Spring 2025

Lab03 FPGA Demonstration

Objective

Learn how to pack your design into AXI IP for a CPU system to accelerate the demonstration environment setup of your design on FPGA

Prior Knowledge

1. Design flow with Xilinx EDA tool (Vivado & SDK).
2. Secure Hash Algorithm Standard (SHA) (FIPS 180-4).

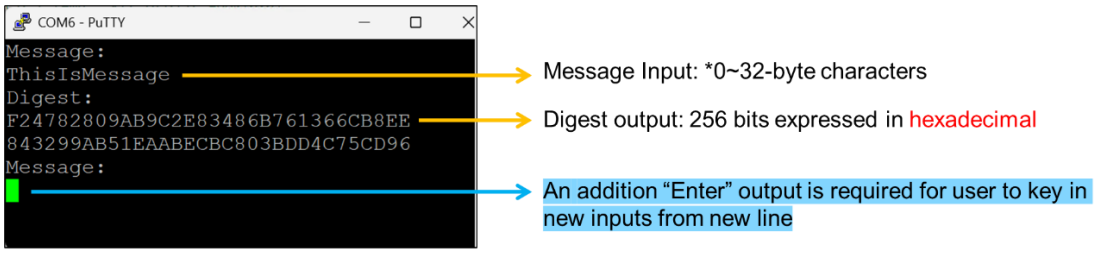
Submission Content

1. Deliver a demonstration environment with your SHA-256 module in Lab02 with these functions below:
    a. Let user enter message via keyboard, and then corresponding digest should be calculated by your SHA-256 module and shown on SDK terminal.
    b. Function "a." should be repeatable without reset or power-cycling.
2. Slides for presentation (6 minutes for your presentation)
    a. Block diagram of your entire design in FPGA.
    b. Total number of registers that you used and the corresponding purpose in packing your SHA2-256 module.
    c. Resource usage summary table (in Vivado -->IMPLEMENTATION-->Report Utilization)
    d. Flow chart of your C code for fulfilling the requirements in 1.
    e. Problems you encounter/solve.
    f. Others.

Demonstration Format Specification

1. SDK Terminal reconfiguration for UART:
    - Baud (rate): 115200 bit per second
    - Data bits: 8
    - Stop bits: 1
    - Parity: None

2. Input/output order on SDK terminal:



Reference Environment

- nthu_sys_lcm_only.tar

Submit

- lab03_xxxxxxx.pdf (xxxxxxx is your student ID)
  This is the slide for your Lab 03 presentation

Credit

- Demonstration (70%)
- Items should be included in your slides (25%):
  - Block diagram
  - AXI registers plan
  - Utilization report
  - Flow chart of your C program
  - Others
- Presentation performance (5%)