FPGA based SHA-256 for Digital Signature Generation

1 Objective

The primary objective of this project is to design and implement SHA-256 hardware unit on FPGA to generate digital signature of a given text file.
Digital signatures use a combination of two cryptographic techniques - HASH and asymmetric cryptography (RSA). The hex file of the text is first hashed using SHA-256, then the message digest is encrypted using RSA, the result is a digital signature.
SHA-256 being computationally intensive, is to be done on FPGA and RSA is to be done on NIOS softcore processor.

1.1 What is Hashing?

Cryptographic Hashing is the process of performing operations on raw text data such that that it cannot be reproduced back to its original form, hence considered as the 'signature' for a given text or a data file. Technically, hashing can be reversed, but the computational power needed to decrypt it makes decryption infeasible.
Hashing provides a secure and efficient way to verify data integrity. When you hash a piece of data, you can compare the resulting hash to a known or expected value to ensure the data has not been tampered with or corrupted. If the hash values match, you can be confident that the data has not been altered or modified since it was originally hashed. Hashing is widely used **to generate 'proof of work' in blockchain (cryptocurrency mining), digital signature generation, message authentication codes, key generation functions, password storage and verification etc.**

2 Weekly Milestones

- Week 1 :
  - Design and Verification of basic building blocks of SHA-256 on Modelsim with Gate level simulaiton.
  - Design of datapath of expansion algorithm.
  - Design of datapath of compression algorithm.
- Week 2 :
  - Design and verification of controller for the entire hardware.
  - Integration of datapath and controller and verifying SHA-256 unit on Modelsim with Gate level simulation.
- Week 3 :
  - Interfacing the SHA-256 unit with NIOS softcore processor.
  - Implementing RSA algorithm on NIOS.
  - Implementing the design on Max 10 FPGA.

3 References

1. Official documentation of SHA (Secure Hash Algorithm) - `https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf`

   This document contains all details of SHA-256 Algorithm.

2. To get an idea of hardware datapath of SHA-256 - Thi Hong Tran, Hoai Luan Pham, and Yasuhiko Nakashima. "A high- performance multi-mem sha-256 accelerator for society 5.0". IEEE Access, 9:39182–39192, 2021.

RA Incharge : K Akhilesh Rao (Roll No. - 213079018)