EE-214
Digital Circuits Lab Project
RA In-Charge –
Naef Ahmad (WEL – 3rd year RA) - 213079015

Implementation of

128-bit AES (Advanced Encryption Standard)

In ECB (Electronic Codebook) mode on XEN-10 FPGA

INTRODUCTION

The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called plaintext. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits.

AES has primarily 2 modes

1. ECB (Electronic Code Book) - Each packet of 128 bits is encrypted by the same key. ECB doesn't work well if the input has repetitive patterns. Encrypted data can display different but consistent patterns, thus giving away some information.
2. CBC – Cipher Block Chaining, where each packet is encrypted by the key as well as output data from previous blocks. This mitigates the shortcoming of ECB.

Reference to Official NIST-AES Document: AES-NIST Official Documentation Link

DELIVERABLES:

- Week - 1
  - Designing Sub-Bytes, Shift-Rows, Mix-Columns, Add Round-Key blocks
  - Writing your own **Testbench** to verify blocks at each step.
  - Encryption of 128-bit packet along with the Datapath and controller FSM
  - Verification using Online AES Calculator
- Week – 2
  - Providing Plain Text and Key sequentially as number of I/O pins are limited on Xen10
  - Performing Encryption on huge data.
  - Encryption of "**Penguin Image**" (or similar image) to demonstrate ECB Shortcomings

Note: Each step must be verified with RTL & Scan chain method

Note: Since XEN10 doesn't offer Gate Level Simulation, students can select some other FPGA (such as CYCLONE GX IV) to verify using Gate Level Simulation.

Note: Students don't need to learn the whole encryption theory. Just the implementation part would suffice

REFERENCES

- AES Documentation - https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf
- Online Cipher and Decipher text Calculator - https://www.hanewin.net/encrypt/aes/aes-test.htm
- Penguin AES - https://github.com/robertdavidgraham/ecb-penguin