IMPLEMENTING AES-256 ON FPGA

Thuan Hai Cong Ho
Student, Computer Engineering, University of Information Technology, HCMC, Vietnam
hohaicongthuan@gmail.com

***Abstract*—In the modern days, the amount of data grow exponentially, including classified and sensitive data that need to be kept secured. For this reason, many cryptographic techniques have been invented for the purpose. AES is one of them. It provides fast and secure data encryption which are the reasons this algorithm is chose for this project.**

The goal of this project is to implement a fully functional AES encryption and decryption system using 256-bit key on FPGA.

***Keywords*—AES-256; cryptography; data security; FPGA; encryption; decryption.**

1 INTRODUCTION

The Advanced Encryption Standard (AES), also known as *Rijndael* is a specification for encrypting electronic data first introduced by the *U.S. National Institute of Standards and Technology (NIST)* in 2001. It provides a fast and secure way to encrypt data and uses symmetric keys encryption which means both the encryption and decryption processes using the same key. The key length for AES could be 128, 192 and 256 bits. This paper concentrates on AES using 256-bit key which will be refered to as AES-256 for the rest of this paper.

1.1 Concepts used in AES-256

Key expansion	Routine used to generate a series of Round Keys from the Cipher Key.
State	Intermediate Cipher result that can be pictured as a rectangular array of bytes, having four rows and $\boldsymbol{Nb}$ columns.
S-box	Non-linear substitution table used in several byte substitution transformation and in the Key Expansion routine to perform a one-for-one substitution of a byte value.
Word	A group of 32 bits that is treated either as a single entity or as an array of 4 bytes.

1.2 Abbreviations and Symbols used in AES-256

$\boldsymbol{Nb}$	Number of columns (32-bit words) comprising the State. For this standard, $\boldsymbol{Nb} = 4$.
$\boldsymbol{Nk}$	Number of 32-bit words comprising the Cipher Key. For this standard, $\boldsymbol{Nk} = 8$.
$\boldsymbol{Nr}$	Number of rounds, which is a function of $\boldsymbol{Nk}$ and $\boldsymbol{Nb}$ (which is fixed). For this standard, $\boldsymbol{Nr} = 14$.
XOR	Exclusive-OR operation
$\oplus$	Exclusive-OR operation
$\otimes$	Multiplication of two polynomials (each with degree < 4) modulo $x^4 + 1$
$\bullet$	Finite field multiplication

2 MATHEMATICAL PRELIMINARIES

3 AES-256

4 IMPLEMENTATION

5 RESULTS

6 CONCLUSION

REFERENCES