

# IMPLEMENT AES-256 ALGORITHM 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 important and sensitive data that need to be kept secured. For this reason, many cryptographic algorithms 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

## 2 MATHEMATICAL PRELIMINARIES

## 3 AES-256 ALGORITHM

## 4 IMPLEMENTATION

## 5 RESULTS

## 6 CONCLUSION

## REFERENCES