TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN

KHOA KỸ THUẬT MÁY TÍNH

BÁO CÁO ĐỒ ÁN
THIẾT KẾ HỆ THỐNG SỐ HDL

ĐỀ TÀI

ADVANCED ENCRYPTION STANDARD

GV hướng dẫn: Ngô Hiếu Trường

Lớp: CE213.Q12

Nhóm sinh viên thực hiện:

Họ và Tên	*MSSV*
Vũ Thành Lam	**23520840**
Lê Trần Huỳnh Phong	**23521164**
Nguyễn Đức Toàn	**23521606**

Hồ Chí Minh, 2025

ACKNOWLEDGMENT

The author would like to thank the supervisor and all individuals who provided guidance and technical support during the completion of this work.

Mục lục

Danh sách hình vẽ

Danh sách bảng

Chương 1

GIỚI THIỆU

1.1 Tổng quan

1.1.1 AES là gì

AES (Advanced Encryption Standard) là một thuật toán mã hóa đối xứng dùng cùng một khóa để mã hóa và giải mã dữ liệu. AES hoạt động theo khối 128 bit và hỗ trợ các độ dài khóa 128, 192 hoặc 256 bit, mang lại tốc độ xử lý cao và mức độ bảo mật mạnh. Hiện nay, AES được sử dụng rộng rãi trong các ứng dụng bảo mật như HTTPS, VPN, và mã hóa dữ liệu trên thiết bị lưu trữ.

1.1.2 Lịch sử phát triển

()

1.1.3 Các đặc điểm của AES

()

1.2 Ứng dụng thực tế của AES

1.2.1 Bảo vệ dữ liệu cá nhân và tài khoản

()

1.2.2 Bảo về dữ liệu trong lĩnh vực y tế

()

1.2.3 Bảo vệ dữ liệu trong lĩnh vực tài chính

()

1.2.4 Bảo vệ dữ liệu trong thiết bị di động và ứng dụng di động

()

1.2.5 Bảo mật trong các hệ thống đám mây (Cloud Computing)

()

1.2.6 Bảo mật trong các Internet of Things (IoT)

()

1.2.7 Bảo mật trong các ứng dụng truyền thông và trò chơi điện tử

()

1.3 Nhiệm vụ đề tài

(Throughput, latency, CPU utilization, etc.)

1.4 Giới hạn đề tài

(Review previous works related to AES and FPGA implementation.)

1.5 Phân chia công việc nhóm

(Outline of remaining chapters.)

Chương 2

KIẾN TRÚC CỦA CHUẨN MÃ HÓA NÂNG CAO (AES256)

2.1 Quy trình mã hóa

2.1.1 Add Round Key

2.1.2 SubBytes Transformation

2.1.3 ShiftRows

2.1.4 MixColumns

2.1.5 Key Expansion

2.2 Kiến trúc Pipeline AES

Chương 3

TỔNG QUAN VỀ PHẦN MỀM MÔ PHỎNG VÀ PHẦN MỀM THIẾT KẾ

3.1 Tổng quan về phần mềm thiết kế và mô phỏng Vivado

3.2 Tổng quan về phần mềm tổng hợp Quartus

3.3 Tổng quan về phần mềm mô phỏng ModelSim

3.4 Tổng quan về ngôn ngữ Verilog

Chương 4

TRIỂN KHAI THIẾT KẾ PHẦN CỨNG AES256 VỚI KỸ THUẬT PIPELINE ĐỂ TĂNG THROUGHPUT

4.1 Triển khai kiến trúc Pipeline AES

4.1.1 Add Round Key

4.1.2 SubBytes Transformation

4.1.3 ShiftRows

4.1.4 MixColumns

4.1.5 Key Expansion

4.2 Kết quả tổng hợp của thiết kế

4.2.1 Mức độ sử dụng tài nguyên

4.2.2 Phân tích năng lượng tiêu thụ

4.3 Kết quả Simulation của thiết kế

4.3.1 Mô phỏng Pre-Simulation

4.3.2 Mô phỏng Post-Simulation

4.3.3 Kiểm tra kết quả mô phỏng với công cụ tính toán Online

4.4 Đánh giá thời gian hoạt động tĩnh của mạch

4.4.1 Kiểm tra độ trễ của mạch

4.4.2 Kiểm tra đồng bộ của mạch

This project successfully implements an AES encryption pipeline on FPGA, focusing on performance optimization and reduced logic utilization.

Chương 5

TỔNG KẾT VÀ ĐỊNH HƯỚNG PHÁT TRIỂN

5.1 Tổng kết

5.2 Định hướng phát triển

Future improvements could include ASIC-level implementation, additional optimization of sub-pipeline blocks, and developing a software interface for system testing.

Tài liệu tham khảo

[1] Author, *Title*, Publisher, Year.

[2] Another Author, *Another Title*, 2020.