ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

NGUYỄN HỒNG NHANH

SỬ DỤNG CÔNG NGHỆ CỨNG HÓA FPGA TRONG MÃ HÓA DỮ LIỆU

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

THÁI NGUYÊN, NĂM 2015

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

NGUYỄN HỒNG NHANH

SỬ DỤNG CÔNG NGHỆ CỨNG HÓA FPGA TRONG MÃ HÓA DỮ LIỆU

Chuyên ngành : Khoa học máy tính
Mã số : 60 48 01 01

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

HƯỚNG DẪN KHOA HỌC: TIẾN SỸ HỒ VĂN CANH

THÁI NGUYÊN, NĂM 2015

LỜI CAM ĐOAN

Tôi xin cam đoan, những nội dung liên quan tới đề tài được trình bày trong luận văn là do bản thân tự tìm hiểu, nghiên cứu dưới sự hướng dẫn khoa học của **Thầy giáo Tiến sỹ Hồ Văn Canh.**

Các nhận xét, kết luận được trích dẫn đầy đủ theo bản gốc.

Tôi xin chịu trách nhiệm trước pháp luật lời cam đoan của mình.

Học viên thực hiện

Nguyễn Hồng Nhanh

LỜI CẢM ƠN

Em xin gửi lời cảm ơn chân thành tới các Thầy thuộc Viện Công nghệ Thông tin/Viện Hàn lâm Khoa học và Công nghệ Việt Nam và Thầy Cô giáo của Trường Đại học Công nghệ Thông tin và Truyền thông/Đại học Thái Nguyên đã tận tình truyền đạt cho em những kiến thức quý báu trong suốt quá trình học tập tại Trường.

Em cũng xin gửi lời cảm ơn tới gia đình, bạn bè, đồng nghiệp và các đồng đội đã thường xuyên động viên, khích lệ giúp đỡ em trong suốt quá trình học tập cũng như hoàn thành luận văn của mình.

Đặc biệt, em xin gửi tới **Thầy giáo Tiến sỹ Hồ Văn Canh** - người đã giúp đỡ, tận tình chỉ bảo, hướng dẫn tỷ mỷ cho em trong quá trình làm đề tài với lòng biết ơn và lời cảm ơn sâu sắc. Trong thời gian làm việc với Thầy, em không những học hỏi được nhiều kiến thức bổ ích về các phương pháp mã hoá và tầm quan trọng của mã hoá dữ liệu trong thời đại ngày nay mà còn học được tinh thần làm việc, thái độ nghiên cứu khoa học nghiêm túc của thầy.

Mặc dù em đã cố gắng hoàn thành đề tài với tất cả nỗ lực của bản thân nhưng chắc chắn sẽ không tránh khỏi những thiếu sót. Em kính mong nhận được sự cảm thông và tận tình chỉ bảo của Quý Thầy Cô và các bạn.

Một lần nữa, em xin chân thành cảm ơn !

Thái Nguyên, tháng 10 năm 2015

Nguyễn Hồng Nhanh

MỤC LỤC

DANH MỤC CHỮ VIẾT TẮT

AES	Advanced Encryption Standard
ARK	AddRoundKey
ASIC	Application-Specific Integrated Circuit
ASSP	Application-Specific Standard Product
CLB	Configurable Logic Block
DES	Data Encryption Standard
DSP	Digital Signal Processor
EEPROM	Electrically Eraseable Programmable Read Only Memory
EPROM	Eraseable Programmable Read Only Memory
FPGA	Field-Programmable Gate Array
$GF(2^8)$	Trường Galois
GPP	General Purpose Processor
HDL	Hardware Description Language
IMC	InvMixColumns
ISB	InvSubBytes
ISR	InvShiftRows
MC	MixColumns
MCU	Microcontroller
MPGA	Mask-Programmable Gate Array
NIST	Institute of Standards and Technology
PAL	Programmable Array Logic
PLA	Programmable Logic Array
PLD	Programmable Logic Device
PROM	Programmable read-only Memory
RISC	Reduced Instruction Set Computer
SB	SubBytes
SR	ShiftRows
VHDL	Verilog Hardware Description Language

DANH MỤC BẢNG

DANH MỤC HÌNH