

**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 mỉ 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

<b>LỜI CAM ĐOAN</b>	<b>Trang</b> i
<b>LỜI CẢM ƠN</b>	ii
<b>MỤC LỤC</b>	iii
<b>DANH MỤC CHỮ VIẾT TẮT</b>	vi
<b>DANH MỤC BẢNG</b>	vii
<b>DANH MỤC HÌNH</b>	viii
<b>MỞ ĐẦU</b>	1
<b>Chương 1</b>	
<b>TỔNG QUAN VỀ MỘT SỐ HỆ MẬT MÃ HIỆN ĐẠI</b>	4
<b>1.1. Cơ sở khoa học của hệ mật mã</b>	4
1.1.1. Yêu cầu cơ bản đối với hệ mã hóa	5
1.1.2. Các thành phần cơ bản của hệ mã hóa	5
1.1.3. Vai trò của mã hóa	6
<b>1.2. Hệ mã hoá khoá đối xứng</b>	7
1.2.1. Chuẩn mã hoá dữ liệu DES	7
1.2.1.1. Lịch sử ra đời	7
1.2.1.2. Tổng quát	8
1.2.1.3. Tạo khóa	10
1.2.1.4. Hoán vị khởi đầu	12
1.2.1.5. Mã hóa chi tiết một vòng	12
1.2.1.6. Hoán vị cuối cùng	17
1.2.1.7. Giải mã DES	17
1.2.1.8. Độ an toàn của thuật toán	17
1.2.2. Chuẩn mã hoá nâng cao AES	19
1.2.2.1. Tổng quan mã hóa AES	19
1.2.2.2. Phép biến đổi SubBytes và InvSubBytes	22
1.2.2.3. Phép biến đổi ShiftRows và InvShiftRows	24
1.2.2.4. Phép biến đổi MixColumns và InvMixColumns	25
1.2.2.5. Key scheduling	27
1.2.2.6. Quy trình giải mã	28

<b>1.3. Hệ mã hoá khoá công khai</b>	29
1.3.1. Hệ mã hóa RSA	30
1.3.1.1. Khái quát	30
1.3.1.2. Mô tả hệ mã hoá RSA	30
1.3.1.3. Tạo khóa	31
1.3.1.4. Mã hóa	32
1.3.1.5. Giải mã	32
1.3.1.6. Một số phương pháp tấn công	33
1.3.1.6.1. Phương pháp sử dụng $\varphi(n)$	33
1.3.1.6.2. Áp dụng thuật toán phân tích ra thừa số	33
1.3.1.6.3. Bẻ khóa dựa trên tấn công lặp lại	34
1.3.1.7. Đánh giá chung	34
1.3.2. Hệ mã hóa Elgamal	35
1.3.2.1. Quá trình tạo khoá, lập mã và giải mã	35
1.3.2.2. Đánh giá độ an toàn	36
<b>1.4. Kết luận chương</b>	37

## Chương 2

### TỔNG QUAN VỀ CÔNG NGHỆ FPGA

<b>2.1. Cơ sở khoa học của các thiết bị khả trình</b>	39
<b>2.2. Khái quát về một số công nghệ cứng hóa hiện nay</b>	40
2.2.1. Công nghệ ASIC	40
2.2.2. Công nghệ ASSP	41
2.2.3. Công nghệ Configurable Processor	42
2.2.4. Công nghệ DSP	42
2.2.5. Công nghệ MCU	43
2.2.6. Công nghệ RISC/GP	44
<b>2.3. Công nghệ FPGA</b>	46
2.3.1. Giới thiệu chung về FPGA	46
2.3.2. Tổng quan về FPGA	47
2.3.2.1. Cấu trúc các FPGA	47
2.3.2.2. Các khối logic cấu hình (Configurable logic Block)	48
2.3.2.3. Các nguồn kết nối (Routes)	48
2.3.2.4. Phân loại FPGA	48
2.3.3. Các công nghệ lập trình FPGA	49
2.3.3.1. Công nghệ lập trình dùng RAM tĩnh	50
2.3.3.2. Các thiết bị lập trình cầu chì nghịch (Anti-fuse)	51
2.3.3.3. Công nghệ lập trình dùng EPROM và EEROM	53
2.3.3. Các ứng dụng của FPGA	54
2.3.3.1. FPGA sử dụng cho các mạch tích hợp có ứng dụng đặc biệt	55
2.3.3.2. FPGA dùng cho thiết kế mạch ngẫu nhiên	55
2.3.3.3. FPGA thay thế các chip SSI trong mạch ngẫu nhiên	55

2.3.3.4. FPGA ứng dụng cho chế tạo mẫu	55
2.3.3.5. FPGA ứng dụng cho chế tạo máy tính	55
2.3.3.6. FPGA ứng dụng trong các thiết bị tái cấu hình	56
2.3.4. Thiết kế và lập trình cho FPGA	56
2.3.5. Tấn công đối với FPGA	57
2.3.5.1. Tấn công kiểu hộp đen	57
2.3.5.2. Tấn công kiểu đọc lại	58
2.3.5.3. Tấn công kiểu nhái lại	58
2.3.5.4. Tấn công kiểu thám ngược thiết kế chuỗi bit	58
2.3.5.5. Tấn công vật lý	59
2.3.5.6. Tấn công side channel	59
2.3.6. Nhận xét chung về FPGA	59
<b>2.4. Kết luận chương</b>	<b>61</b>

### **Chương 3**

<b>GIẢI PHÁP TRIỂN KHAI THUẬT TOÁN AES TRÊN NỀN FPGA</b>	<b>62</b>
<b>3.1. Giải pháp tổng quát về triển khai thuật toán AES trên nền FPGA</b>	<b>62</b>
3.1.1. Mô tả lưu đồ tổng quát của bộ mã hóa và giải mã AES	62
3.1.2. Khối Data của bộ mã hóa	63
3.1.3. Khối KeyExpansion	64
3.1.4. Khối CPU và khối Data của bộ giải mã	65
3.1.5. Thiết kế chi tiết các khối chức năng của bộ mã hóa	67
3.1.6. Thiết kế các khối chức năng của bộ giải mã	70
3.1.7. Thiết kế chi tiết cho khối KeyExpansion	72
3.1.8. Khối CPU - điều khiển bộ giải mã	73
3.1.9. Khối giao tiếp với máy tính	75
3.1.10. Sử dụng chế độ cài đặt ECB cho giải pháp	75
<b>3.2. Các yêu cầu của giải pháp và đánh giá</b>	<b>78</b>
3.2.1. Tốc độ và tài nguyên	78
3.2.2. Cấu trúc phần cứng FPGA để thực hiện AES	79
<b>3.4. Chương trình DEMO thuật toán mã hoá AES</b>	<b>82</b>
<b>3.4. Kết luận chương</b>	<b>83</b>

<b>KẾT LUẬN</b>	<b>84</b>
-----------------	-----------

<b>TÀI LIỆU THAM KHẢO</b>	<b>86</b>
---------------------------	-----------

### **PHỤ 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 Erasable Programmable Read Only Memory
EPROM	Erasable 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**

<b>Bảng 1.1.</b> Các giai đoạn mã hoá của DES	8
<b>Bảng 1.2.</b> Số bit được loại bỏ khi đi qua PC1	11
<b>Bảng 1.3.</b> Số bit dịch chuyển	11
<b>Bảng 1.4.</b> PC2 (hoán vị nén)	11
<b>Bảng 1.5.</b> Bảng hoán vị khởi đầu IP	12
<b>Bảng 1.6.</b> Hộp E	14
<b>Bảng 1.7.</b> Các hộp S	15
<b>Bảng 1.8.</b> Hoán vị cuối cùng $IP^{-1}$	17
<b>Bảng 1.9.</b> Bảng thế s-box của AES	24
<b>Bảng 1.10.</b> Tóm tắt các bước tạo khoá, mã hoá và giải mã hệ Enganmal	36
<b>Bảng 2.1.</b> So sánh xử lý tín hiệu thời gian thực	45
<b>Bảng 2.2.</b> Các đặc tính của công nghệ lập trình	54

## DANH MỤC HÌNH

<b>Hình 1.1.</b> Mô hình mã hóa	6
<b>Hình 1.2.</b> Minh họa hệ mã hóa khoá đối xứng	7
<b>Hình 1.3.</b> Sơ đồ tổng quát mã hóa DES	9
<b>Hình 1.4.</b> Sơ đồ tạo khóa	10
<b>Hình 1.5.</b> Biểu diễn dãy 64 bit $x$ chia thành 2 thành phần $L_0, R_0$	12
<b>Hình 1.6.</b> Sơ đồ chi tiết một vòng	13
<b>Hình 1.7.</b> Sơ đồ hoạt động của hàm $f$	13
<b>Hình 1.8.</b> Hoán vị mở rộng	14
<b>Hình 1.9.</b> Lưu đồ cấu trúc lặp của thuật toán mã hóa AES	20
<b>Hình 1.10.</b> Mô tả State trong thuật toán mã hóa AES được biểu diễn dạng ma trận $4 \times 4$	20
<b>Hình 1.11.</b> Lưu đồ mã hóa và giải mã một vòng của thuật toán mã hóa AES	21
<b>Hình 1.12.</b> Lưu đồ thực hiện SB và ISB	22
<b>Hình 1.13.</b> Biến đổi SubBytes đối với mảng trạng thái	23
<b>Hình 1.14.</b> Lưu đồ thực hiện SR	25
<b>Hình 1.15.</b> Quá trình xử lý MixColumns	25
<b>Hình 1.16.</b> Mô tả bước trong Key scheduling	27
<b>Hình 1.17.</b> Mã hoá với khóa mã và giải mã khác nhau	29
<b>Hình 1.18.</b> Sơ đồ thuật toán RSA	31
<b>Hình 2.1.</b> Mô hình FPGA	47
<b>Hình 2.2.</b> Bốn loại FPGA trên thực tế	49
<b>Hình 2.3.</b> Công nghệ lập trình RAM tĩnh	50
<b>Hình 2.4.</b> Công nghệ lập trình cầu chì nghịch PLICE	51
<b>Hình 2.5.</b> Công nghệ lập trình cầu chì nghịch ViaLink	52
<b>Hình 2.6.</b> Công nghệ lập trình EPROM transistor	53
<b>Hình 2.7.</b> Minh họa khả năng cấu hình lại của FPGA	60
<b>Hình 3.1.</b> Sơ đồ khối tổng quát hệ thống AES	62
<b>Hình 3.2.</b> Sơ đồ thuật toán khối data của bộ mã hóa	63