

BỘ GIÁO DỤC VÀ ĐÀO TẠO

BỘ QUỐC PHÒNG

VIỆN KHOA HỌC VÀ CÔNG NGHỆ QUÂN SỰ

HOÀNG VĂN QUÂN

**NGHIÊN CỨU GIẢI PHÁP NÂNG CAO HIỆU QUẢ
BẢO MẬT THÔNG TIN TRÊN MẠNG TRUYỀN SỐ LIỆU
ĐA DỊCH VỤ**

LUẬN ÁN TIẾN SĨ KỸ THUẬT

HÀ NỘI - 2016

BỘ GIÁO DỤC VÀ ĐÀO TẠO

BỘ QUỐC PHÒNG

VIỆN KHOA HỌC VÀ CÔNG NGHỆ QUÂN SỰ

HOÀNG VĂN QUÂN

**NGHIÊN CỨU GIẢI PHÁP NÂNG CAO HIỆU QUẢ
BẢO MẬT THÔNG TIN TRÊN MẠNG TRUYỀN SỐ LIỆU
ĐA DỊCH VỤ**

Chuyên ngành: Kỹ thuật điện tử
Mã số: 62 52 02 03

LUẬN ÁN TIẾN SĨ KỸ THUẬT

NGƯỜI HƯỚNG DẪN KHOA HỌC:

- 1. TS LÊU ĐỨC TÂN**
- 2. TS HOÀNG NGỌC MINH**

HÀ NỘI - 2016

LỜI CAM ĐOAN

Tôi xin cam đoan đây là công trình nghiên cứu của riêng tôi. Các nội dung, số liệu và kết quả trình bày trong luận án là hoàn toàn trung thực và chưa có tác giả nào công bố trong bất cứ một công trình nào khác, các dữ liệu tham khảo được trích dẫn đầy đủ.

Người cam đoan

Hoàng Văn Quân

LỜI CẢM ƠN

Luận án được thực hiện tại Viện Khoa học và Công nghệ Quân sự - Bộ Quốc phòng.

Tôi xin bày tỏ lòng biết ơn sâu sắc tới TS Lều Đức Tân và TS Hoàng Ngọc Minh, các thầy đã tận tình giúp đỡ, trang bị phương pháp nghiên cứu, kinh nghiệm, kiến thức khoa học và kiểm tra, đánh giá các kết quả trong suốt quá trình nghiên cứu luận án.

Xin trân trọng cảm ơn Viện Khoa học và Công nghệ Quân sự, Phòng Đào tạo, Viện Điện tử là cơ sở đào tạo và đơn vị quản lý, các đồng chí lãnh đạo, chỉ huy Cục Cơ yếu - Bộ Tổng Tham mưu – nơi tôi công tác đã tạo mọi điều kiện thuận lợi, hỗ trợ và giúp đỡ tôi trong suốt quá trình học tập, nghiên cứu thực hiện luận án. Xin chân thành cảm ơn các thầy, cô của Viện Khoa học và Công nghệ Quân sự, Viện Điện tử, các nhà khoa học, các đồng nghiệp thuộc Trung tâm Nghiên cứu Kỹ thuật Mật mã – Cục Cơ yếu, Viện Khoa học Công nghệ Mật mã/Ban Cơ yếu Chính phủ đã giúp đỡ, hỗ trợ tôi trong suốt thời gian qua.

Cuối cùng, tôi xin bày tỏ lòng thành kính và luôn ghi nhớ công ơn của cha mẹ, gia đình, những người thân và xin dành lời cảm ơn đặc biệt tới vợ con, những người đã luôn đồng hành, động viên và là chỗ dựa về mọi mặt giúp tôi vượt qua khó khăn để có được những kết quả nghiên cứu ngày hôm nay.

Tác giả

MỤC LỤC

| | Trang |
|---|-------|
| DANH MỤC CÁC KÝ HIỆU, CÁC CHỮ VIẾT TẮT..... | vi |
| DANH MỤC CÁC BẢNG..... | ix |
| DANH MỤC CÁC HÌNH VẼ..... | x |
| MỞ ĐẦU..... | 1 |
| Chương 1 TỔNG QUAN VỀ AN TOÀN VÀ BẢO MẬT TRONG MẠNG TRUYỀN SỐ LIỆU ĐA DỊCH VỤ..... | 8 |
| 1.1. Đặc điểm mạng truyền số liệu đa dịch vụ..... | 8 |
| 1.2. An toàn và bảo mật trong mạng truyền số liệu đa dịch vụ | 9 |
| 1.2.1. Một số khái niệm chung | 9 |
| 1.2.2. Các cơ chế an ninh dựa trên mật mã | 11 |
| 1.2.3. Vị trí đặt dịch vụ an ninh theo mô hình mạng phân tầng..... | 14 |
| 1.2.4. Ý nghĩa của việc sử dụng mật mã trong bảo mật tại tầng IP | 15 |
| 1.2.5. Bảo mật trong mạng truyền số liệu đa dịch vụ | 18 |
| 1.2.6. Giao thức bảo mật cho mạng truyền số liệu đa dịch vụ | 22 |
| 1.3. Giao thức bảo mật IPSec..... | 22 |
| 1.3.1. Kiến trúc của IPSec | 22 |
| 1.3.2. Module thiết lập SA | 24 |
| 1.3.3. Giao thức ESP | 24 |
| 1.3.4. Giao thức AH | 25 |
| 1.3.5. Giao thức trao đổi khóa IKEv2 trong IPSec | 26 |
| 1.4. Hạn chế của giải pháp bảo mật hiện tại và đề xuất hướng giải quyết..... | 27 |
| 1.4.1. Một số hạn chế của giải pháp bảo mật | 27 |
| 1.4.2. Đề xuất các nội dung nghiên cứu của luận án..... | 28 |
| 1.5. Giao thức trao đổi khóa Diffie-Hellman kết hợp ECC | 28 |

| | |
|---|----|
| 1.5.1. Đặt vấn đề..... | 28 |
| 1.5.2. Giao thức trao đổi khóa ECDH..... | 31 |
| 1.6. Công nghệ để cứng hóa mật mã..... | 34 |
| 1.7. Kết luận Chương 1 | 35 |
| Chương 2 NÂNG CAO HIỆU QUẢ THỰC HIỆN PHÉP NHÂN ĐIỂM CỦA ECC CHO GIAO THỨC TRAO ĐỔI KHÓA | 36 |
| 2.1. Phép nhân điểm trên đường cong elliptic | 36 |
| 2.1.1. Một số thuật toán nhân điểm elliptic trên trường $GF(2^n)$ | 36 |
| 2.1.2. Thuật toán nhân điểm Elliptic dựa trên triển khai một số nguyên theo NAF tính toán trực tiếp..... | 40 |
| 2.2. Xây dựng công thức tính số xung nhịp máy trung bình để cộng hai số nguyên khi thực hiện trên phần cứng..... | 43 |
| 2.2.1. Cơ sở đề xuất..... | 43 |
| 2.2.2. Mạch cộng hai số nguyên và phân phối xác suất của đại lượng $F(k)$ | 43 |
| 2.2.3. Kết quả tính toán số $AAF(k)$ và $AAF(k,M)$ | 51 |
| 2.2.4. Ứng dụng của kết quả..... | 55 |
| 2.3. Thực hiện thuật toán nhân điểm trên phần cứng FPGA | 55 |
| 2.3.1. Phương pháp thiết kế chung..... | 55 |
| 2.3.2. Lựa chọn đường cong elliptic | 56 |
| 2.3.3. Mô hình cứng hóa thuật toán nhân điểm..... | 56 |
| 2.3.4. Kết quả thực hiện | 71 |
| 2.4. Kết luận Chương 2 | 74 |
| Chương 3 NÂNG CAO HIỆU QUẢ THỰC HIỆN THUẬT TOÁN MÃ HÓA DỮ LIỆU TRONG BẢO MẬT MẠNG TRUYỀN SỐ LIỆU | 76 |
| 3.1. Cơ sở lý thuyết | 76 |
| 3.1.1. Các mã khối có cấu trúc SPN..... | 76 |

| | |
|---|-----|
| 3.1.2. Các tiêu chí đánh giá và xây dựng tầng tuyến tính hiệu quả, an toàn cho mã khối có cấu trúc SPN..... | 78 |
| 3.2. Chuẩn mã hóa dữ liệu AES..... | 81 |
| 3.3. Đánh giá một số ma trận MDS trong các mã pháp dạng AES..... | 85 |
| 3.3.1. Một số định nghĩa..... | 85 |
| 3.3.2. Đánh giá một số ma trận MDS sử dụng trong mã pháp dạng AES..... | 87 |
| 3.4. Đề xuất ma trận MDS mới để cải tiến tầng tuyến tính cho các mã pháp dạng AES..... | 91 |
| 3.4.1. Đề xuất ma trận MDS mới và đánh giá hiệu quả hoạt động..... | 92 |
| 3.4.2. Phân tích cài đặt các ma trận theo quan điểm phần mềm..... | 96 |
| 3.4.3. Điểm bất động của tầng tuyến tính theo ma trận đề xuất..... | 99 |
| 3.4.4. Kết quả cài đặt thực nghiệm trên FPGA..... | 100 |
| 3.4.5. Kết quả cài đặt AES chuẩn và AES với ma trận MDS đề xuất ... | 102 |
| 3.5. Kết luận Chương 3..... | 103 |
| KẾT LUẬN..... | 105 |
| DANH MỤC CÁC CÔNG TRÌNH KHOA HỌC ĐÃ CÔNG BỐ..... | 107 |
| TÀI LIỆU THAM KHẢO..... | 108 |

DANH MỤC CÁC KÝ HIỆU, CÁC CHỮ VIẾT TẮT

| | |
|-----------------------|---|
| E | Ký hiệu đường cong elliptic |
| O | Điểm vô cực của đường cong elliptic |
| G | Một điểm trên E sinh ra một nhóm cyclic cấp N |
| K_A | Khóa bí mật A |
| K_B | Khóa bí mật B |
| $\mathbb{F}_p, GF(p)$ | Ký hiệu cho trường hữu hạn chứa p phần tử với p là số nguyên tố |
| $\#(X, Y)$ | Lực lượng của tập X, Y |
| $\#(a)$ | Lực lượng của a |
| $\#(b)$ | Lực lượng của b |
| x_1, y_1 | Tọa độ điểm P trên đường cong E |
| x_2, y_2 | Tọa độ điểm Q trên đường cong E |
| x_3, y_3 | Tọa độ điểm R trên đường cong E |
| $Rank(A)$ | Hạng của ma trận A |
| ATM1 | An toàn mạng 1 |
| ATM2 | An toàn mạng 2 |
| AES | Chuẩn mã hóa dữ liệu mở rộng (Advanced Encryption Standard) |
| AH | Giao thức tiêu đề xác thực (Authentication Header) |
| ASIC | Mạch tích hợp cho các ứng dụng đặc biệt (Application Specific Integrated Circuit) |
| ATM | Phương thức truyền tải không đồng bộ (Asynchronous Transfer Mode) |
| DLP | Bài toán logarith rời rạc (Discrete Logarithm Problem) |
| DoS | Tấn công từ chối dịch vụ (Denial of Service) |
| DDoS | Tấn công từ chối dịch vụ phân tán (Distributed Denial of Service) |
| DTLS | Bảo mật gói dữ liệu tầng giao vận (Datagram Transport Layer Security) |
| DH | Diffie-Hellman (Elliptic Curve) |

| | |
|-------|--|
| EC | Đường cong elliptic |
| ECADD | Phép cộng hai điểm khác nhau (Elliptic Curve ADD) |
| ECC | Hệ mật Elliptic (Elliptic Curve Cryptosystem) |
| ECDBL | Phép nhân đôi (phép cộng hai điểm giống nhau - EC Double) |
| ECDH | Bài toán Diffie-Hellman trên Elliptic (Elliptic Curve Diffie-Hellman) |
| ECDLP | Bài toán logarith rời rạc trên đường cong elliptic (Elliptic Curve Discrete Logarithm Problem) |
| ECDSA | Thuật toán chữ ký số Elliptic (Elliptic Curve Digital Signature Algorithm) |
| ESP | Encapsulating Security Payload |
| FPGA | Mảng cổng lập trình dạng trường (Field Programmable Gate Array) |
| GCD | Tìm ước số chung lớn nhất (Greatest Common Divisor) |
| IP | Giao thức liên mạng (Internet Protocol) |
| IDPS | Hệ thống phát hiện và ngăn chặn truy cập (Intrusion Detection Pevention System) |
| IPSec | Giao thức bảo mật (IP Security Protocol) |
| IKE | Trao đổi khóa (Internet Key Exchange) |
| ISO | Tổ chức Tiêu chuẩn quốc tế (International Organization for Standardization) |
| MPLS | Chuyển mạch nhãn đa giao thức (Multi Protocol Label Switching) |
| MDS | Phân tách có khoảng cách cực đại (Maximum Distance Separable) |
| NAF | Dạng không liền kề (Non Adjacent Form) |
| LAN | Mạng cục bộ (Local Area Network) |
| LC | Tế bào logic (Logic Cell) |
| LE | Phần tử logic (Logic Element) |
| MPPE | Mã hóa điểm tới điểm (Microsoft Point to Point Encryption) |

| | |
|------|--|
| OSI | Mô hình tương tác giữa các hệ thống mở (Open Systems Interconnection) |
| SPN | Mạng thay thế - hoán vị (Substitution Permutation Network) |
| RSA | Thuật toán mã khóa công khai của Rivest, Shamir và Adleman |
| VPN | Mạng riêng ảo (Virtual Private Network) |
| VHDL | Ngôn ngữ mô tả phần cứng (Verilog Hardware Description Language) |