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 LỀU 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 CÁM 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 cám 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 cám 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

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)