BỘ GIÁO DỤC VÀ ĐÀO TẠO BỘ QUỐC PHÒNG

VIỆN KHOA HỌC VÀ CÔNG NGHỆ QUÂN SỰ

Hoàng Văn Thức

HỆ TIÊU CHUẨN THAM SỐ AN TOÀN CHO HỆ MẬT RSA VÀ ỨNG DỤNG

LUẬN ÁN TIẾN SĨ TOÁN HỌC

Hà Nội - 2011

BỘ GIÁO DỤC VÀ ĐÀO TẠO BỘ QUỐC PHÒNG

VIỆN KHOA HỌC VÀ CÔNG NGHỆ QUÂN SỰ

Hoàng Văn Thức

HỆ TIÊU CHUẨN THAM SỐ AN TOÀN CHO HỆ MẬT RSA VÀ ỨNG DỤNG

Chuyên ngành : Bảo đảm toán học cho máy tính và hệ thống tính toán.

Mã số : 62 46 35 01

LUẬN ÁN TIẾN SĨ TOÁN HỌC

NGƯỜI HƯỚNG DẪN KHOA HỌC:

1. TS. LỀU ĐỨC TÂN
2. PGS.TS. BẠCH NHẬT HỒNG

Hà Nội - 2011

LỜI CAM ĐOAN

Tôi xin cam đoan, đây là công trình nghiên cứu của riêng tôi. Các 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.

Người cam đoan

Hoàng Văn Thức

LỜI CẢM ƠN

Luận án này 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 Tiến sĩ Lều Đức Tân, Phó giáo sư - Tiến sĩ Bạch Nhật Hồng đã tận tình hướng dẫn và giúp đỡ tôi trong suốt quá trình học tập, nghiên cứu và hoàn thành luận án này.

Tôi xin cám ơn Viện Khoa học và Công nghệ Quân sự là cơ sở đào tạo và đơn vị quản lý đã tạo mọi điều kiện, hỗ trợ, giúp đỡ tôi trong quá trình học tập, nghiên cứu.

Xin cám ơn Ban Cơ yếu Chính phủ, Học viện Kỹ thuật Mật mã, Phân viện Nghiên cứu Khoa học Mật mã đã động viên, hỗ trợ, tạo điều kiện cho tôi được học tập, nghiên cứu.

Tôi luôn luôn ghi nhớ công ơn của bố mẹ, gia đình và xin dành lời cảm ơn đặc biệt tới vợ con, những người đã luôn ở bên cạnh, động viên và là chỗ dựa về mọi mặt giúp tôi vượt qua khó khăn để hoàn thành các nội dung nghiên cứu.

Lời cuối cùng, cho tôi bày tỏ lòng biết ơn chân thành tới các thầy, các cô của Viện Khoa học và Công nghệ Quân sự, các nhà khoa học, đặc biệt là những nhà khoa học có thâm niên nghiên cứu lâu năm về lĩnh vực luận án đang nghiên cứu cùng bạn bè, đồng nghiệp đã luôn động viên, chia sẻ, giúp đỡ tôi trong suốt thời gian qua.

Tác giả

MỤC LỤC

DANH MỤC CÁC KÝ HIỆU, CÁC CHỮ VIẾT TẮT

Các ký hiệu

d:	Số mũ bí mật RSA.
e:	Số mũ công khai RSA.
$\mathbb{F}_p$:	Trường các số nguyên với phép cộng và phép nhân được rút gọn theo modulo p.
$\mathbb{F}_p^*$:	Nhóm nhân cực đại của $\mathbb{F}_p$.
$\gcd(a,b)$:	Ước số chung lớn nhất của a và b.
$\text{lmc}(a,b)$:	Bội số chung nhỏ nhất của a và b.
$O(B)$:	Vô cùng lớn cỡ B, $x = O(B)$ tồn tại một hằng số dương c sao cho $x \le cB$.
$ord_N a$:	Bậc của phần tử a trong nhóm nhân $\mathbb{Z}_N^*$.
$\mathbb{N}$:	Tập các số tự nhiên.
N:	RSA modulus.
$nlen$:	Độ dài RSA modulus tính theo bít.
n_0:	Độ dài p_0 tính theo bít.
n_1:	Độ dài p_1 tính theo bít.
n_2:	Độ dài p_2 tính theo bít.
n_3:	Độ dài q_1 tính theo bít.
n_4:	Độ dài q_2 tính theo bít.
n_5:	Độ dài p_{11} tính theo bít.
n_6:	Độ dài q_{11} tính theo bít.
p, q:	Các số nguyên tố.
p_0:	Ước nguyên tố lớn nhất của $\lvert p - q \rvert$.
p_1:	Ước nguyên tố lớn nhất của $p - 1$.

p_2: Ước nguyên tố lớn nhất của $p + 1$.

p_{11}: Ước nguyên tố lớn nhất của $p_1 - 1$.

q_1: Ước nguyên tố lớn nhất của $q - 1$.

q_2: Ước nguyên tố lớn nhất của $q + 1$.

q_{11}: Ước nguyên tố lớn nhất của $q_1 - 1$.

plen: Độ dài số nguyên tố *p* tính theo bít.

qlen: Độ dài số nguyên tố *q* tính theo bít.

Proof(*p*): Chứng nhận tính nguyên tố của *p*.

Prob{*x* : *y*}: Xác suất xảy ra biến cố *y* với giả thiết *x*.

x modulo *p*: Phần dư khi chia *x* cho *p*.

$x \| y$: Chuỗi kết quả của việc nối chuỗi *y* vào chuỗi *x*.

$\lceil x \rceil$: số nguyên *m* nhỏ nhất sao cho $m \geq x$.

$\lfloor x \rfloor$: số nguyên *m* lớn nhất sao cho $m \leq x$.

$\mathbb{Z}$: Tập các số nguyên.

$\mathbb{Z}_N$: Vành số nguyên với phép cộng và phép nhân rút gọn theo modulo *N*.

$\mathbb{Z}_N^*$: Nhóm nhân cực đại của vành $\mathbb{Z}_N$.

$\lambda(N)$: Bậc (order) lớn nhất của các phần tử trong nhóm $\mathbb{Z}_N^*$.

$\varphi(N)$: Số các số nguyên $0 \leq a < N$ thỏa mãn $\gcd(a, N) = 1$.

Các chữ viết tắt

AES (*Advanced Encryption Standard*): Chuẩn mã hoá tiên tiến.

ANSI (*American National Standard Institute*): Viện tiêu chuẩn quốc gia Mỹ

CA (*Certificate Authority*): Thẩm quyền chứng thực.

CBC (*Cipher Block Chaining*): Chế độ mã móc xích trong mã khối.

ECDSA (*Elliptic Curve Digital Signature Algorithm*): Thuật toán chữ ký số đường cong elliptic.

DES (*Data Encryption Standard*): Chuẩn mã hoá dữ liệu.

DH (*Diffie-Hellman*): Tên một thuật toán trao đổi khoá.

DPA (*Differential Power Analysis*): Phân tích năng lượng sai khác.

DSS (*Digital Signature Standard*): Chuẩn chữ ký số.

ECM (*Elliptic Curve Method*): Phương pháp phân tích số dựa trên đường cong elliptic.

FIPS (*Ferderal Infomation Processing Standard*): Tiêu chuẩn xử lý thông tin liên bang (Mỹ).

FTP (*File Transfer Protocol*): Giao thức truyền tệp tin.

IE (*Internet Explorer*): Tên một trình duyệt Web của hãng Microsoft.

IETF (*Internet Engineering Task Force*): Nhóm đặc trách về kỹ thuật Internet.

IFC (*Integer Factorization Cryptography*): Mật mã dựa trên bài toán phân tích số nguyên.

IIS (*Internet Information Server*): Tên một phần mềm Web server của hãng Microsoft.

ISO/IEC (*Internatinal Organization for Standardization/International Electrotechnical Comission*): Tổ chức ban hành chuẩn quốc tế/Uỷ ban điện tử quốc tế.

MD5 (*Message Digest*): Tên một hàm băm mật mã.

MAC (*Message Authentication Code*): Mã xác thực thông báo.

NFS (*Number Field Sieve*): Sàng trường số.

NIST (*National Institute of Standard and Technology*): Viện các tiêu chuẩn và công nghệ quốc gia (Mỹ).

NSS (*Network Security Service*): Dịch vụ bảo mật mạng.