BỘ GIÁO DỤC VÀ ĐÀO TẠO BỘ QUỐC PHÒNG

HỌC VIỆN KỸ THUẬT QUÂN SỰ

LƯU HỒNG DŨNG

NGHIÊN CỨU, PHÁT TRIỂN CÁC LƯỢC ĐỒ CHỮ KÝ SỐ TẬP THỂ

LUẬN ÁN TIẾN SỸ KỸ THUẬT

HÀ NỘI - 2013

BỘ GIÁO DỤC VÀ ĐÀO TẠO BỘ QUỐC PHÒNG

HỌC VIỆN KỸ THUẬT QUÂN SỰ

LƯU HỒNG DŨNG

NGHIÊN CỨU, PHÁT TRIỂN CÁC LƯỢC ĐỒ CHỮ KÝ SỐ TẬP THỂ

Chuyên ngành : KỸ THUẬT ĐIỆN TỬ

Mã số: 62 52 02 03

LUẬN ÁN TIẾN SỸ KỸ THUẬT

NGƯỜI HƯỚNG DẪN KHOA HỌC

1. TS Vũ Minh Tiến
2. TS Nguyễn Văn Liên

HÀ NỘI - 2013

LỜI CAM ĐOAN

Tôi xin cam đoan đây là công trình nghiên cứu của riêng tôi. Các kết quả trình bày trong Luận án là trung thực và chưa từng được công bố ở bất kỳ công trình nghiên cứu nào khác.

MỤC LỤC

DANH MỤC CÁC KÝ HIỆU, CÁC CHỮ VIẾT TẮT

Các ký hiệu

gcd(a,b)	Ước số chung lớn nhất của a và b
H(.)	Hàm băm
||	Toán tử nối/trộn 2 xâu
a|b	a là ước số của b
ID_i	Thông tin nhận dạng thực thể cuối U_i
M	Thông điệp dữ liệu
x_i	Khóa bí mật của thực thể ký U_i
y_i	Khóa công khai của thực thể ký U_i

Các chữ viết tắt

CA	Certificate Authority
CRL	Certificate Revocation List
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
EE	End Entity
LDAP	Lightweight Directory Access Protocol
ITU	Internet Telecommumications Union
ISO	International Organization for Standardization
PKC	Public Key Certificate
PKC^1	Public Key Cryptography
PKI	Public Key Infrastructure
RA	Registration Authority
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm

DANH MỤC CÁC HÌNH VẼ

MỞ ĐẦU

1. Tính cấp thiết của đề tài

Hiện nay, khi mà Chính phủ điện tử và Thương mại điện tử đã trở thành xu hướng tất yếu của hầu hết các quốc gia trên thế giới, trong đó có Việt Nam, thì chứng thực số [11] sẽ là một yếu tố không thể thiếu được và ngày càng trở nên quan trọng. Việc ra đời chứng thực số không những đảm bảo cho việc xây dựng thành công Chính phủ điện tử và Thương mại điện tử theo nhu cầu phát triển của xã hội mà còn có tác dụng rất to lớn trong việc phát triển các ứng dụng trên mạng Internet. Hạ tầng công nghệ của chứng thực số là Hạ tầng cơ sở khoá công khai (PKI - Public Key Infrastructure) [1] với nền tảng là mật mã khoá công khai (PKC[1] - Public Key Cryptography) [9] và chữ ký số (Digital Signature) [13].

Trong các giao dịch điện tử, chữ ký số được sử dụng nhằm đáp ứng yêu cầu chứng thực về nguồn gốc và tính toàn vẹn của thông tin. Chứng thực về nguồn gốc của thông tin là chứng thực danh tính của những thực thể (con người, thiết bị kỹ thuật,...) tạo ra hay có mối quan hệ với thông tin được trao đổi trong các giao dịch điện tử. Các mô hình ứng dụng chữ ký số hiện tại cho phép đáp ứng tốt các yêu cầu về chứng thực nguồn gốc thông tin được tạo ra bởi những thực thể có tính độc lập. Tuy nhiên, trong các mô hình hiện tại khi mà các thực thể tạo ra thông tin là thành viên hay bộ phận của một tổ chức (đơn vị hành chính, hệ thống kỹ thuật,...) thì nguồn gốc thông tin ở cấp độ tổ chức mà thực thể tạo ra nó là một thành viên hay bộ phận lại không được chứng thực. Nói cách khác, yêu cầu về việc chứng thực đồng thời danh tính của thực thể tạo ra thông tin và danh tính của tổ chức mà thực thể tạo ra thông tin là một thành viên hay bộ phận của nó không được đáp ứng trong các mô hình ứng dụng chữ ký số hiện tại. Trong khi đó, các yêu cầu như

thế ngày càng trở nên thực tế và cần thiết để bảo đảm cho các thủ tục hành chính trong các giao dịch điện tử. Mục tiêu của đề tài Luận án là nghiên cứu, phát triển một số lược đồ chữ ký số theo mô hình ứng dụng mới đề xuất nhằm bảo đảm các yêu cầu chứng thực về nguồn gốc và tính toàn vẹn cho các thông điệp dữ liệu trong các giao dịch điện tử mà ở đó các thực thể ký là thành viên hay bộ phận của các tổ chức có tư cách pháp nhân trong xã hội. Trong mô hình này, các thông điệp điện tử sẽ được chứng thực ở 2 cấp độ khác nhau: thực thể tạo ra nó và tổ chức mà thực thể tạo ra nó là một thành viên hay bộ phận của tổ chức này. Trong Luận án, mô hình ứng dụng chữ ký số với các yêu cầu đặt ra như trên được gọi là *mô hình chữ ký số tập thể* và các lược đồ chữ ký số xây dựng theo mô hình như thế được gọi là các *lược đồ chữ ký số tập thể*.

Một hướng nghiên cứu như vậy, có thể hiện tại chưa được đặt ra như một yêu cầu có tính cấp thiết, nhưng trong một tương lai không xa, khi Chính phủ điện tử và Thương mại điện tử cùng với hạ tầng công nghệ thông tin và truyền thông đã phát triển mạnh mẽ thì nhu cầu ứng dụng chữ ký số tập thể trong các dịch vụ chứng thực điện tử sẽ là tất yếu. Trước tình hình nghiên cứu trong và ngoài nước về chữ ký tập thể thì việc nghiên cứu, phát triển và từng bước đưa chữ ký tập thể ứng dụng vào thực tiễn xã hội là rất cần thiết.

Xuất phát từ thực tế đó, NCS đã chọn đề tài "**Nghiên cứu, phát triển các lược đồ chữ ký sô tập thể**" với mong muốn có những đóng góp vào sự phát triển khoa học và công nghệ chung của đất nước.

2. Đối tượng và phạm vi nghiên cứu

Đối tượng nghiên cứu của Luận án bao gồm:

- Cơ sở của các hệ mật khóa công khai và các lược đồ chữ ký số.
- Nguyên lý xây dựng các hệ mật khóa công khai và lược đồ chữ ký số.

- Các mô hình ứng dụng mật mã khóa công khai và chữ ký số.

Phạm vi nghiên cứu của Luận án bao gồm:

- Hệ mật khóa công khai RSA, hệ mật ElGamal, chuẩn chữ ký số GOST R34.10-94 của Liên bang Nga và các cơ sở toán học liên quan.
- Phương pháp mã hóa và giải mã, phương pháp hình thành và kiểm tra chữ ký số, chữ ký số tập thể.

3. Mục tiêu nghiên cứu

Mục tiêu nghiên cứu của Luận án bao gồm:

- Đề xuất mô hình ứng dụng chữ ký số nhằm đáp ứng các yêu cầu đặt ra khi triển khai một Chính phủ điện tử trong thực tế xã hội, áp dụng phù hợp cho đối tượng là các tổ chức, cơ quan hành chính, các doanh nghiệp,....
- Phát triển một số lược đồ chữ ký số theo mô hình đã đề xuất.

4. Phương pháp nghiên cứu

- Phát triển một số lược đồ cơ sở dựa trên các hệ mật và các chuẩn chữ ký số được đánh giá có độ an toàn cao, sử dụng các lược đồ này làm cơ sở để xây dựng các lược đồ chữ ký số theo mục tiêu nghiên cứu đặt ra.
- Xây dựng một số lược đồ chữ ký tập thể theo mô hình ứng dụng mới đề xuất có khả năng ứng dụng trong thực tiễn.

5. Nội dung nghiên cứu

Nội dung nghiên cứu của Luận án bao gồm:

- Các hệ mật RSA, hệ mật ElGamal và chuẩn chữ ký số GOST R34.10-94 của Liên bang Nga.
- Phát triển một số lược đồ cơ sở dựa trên hệ mật RSA, hệ mật ElGamal và chuẩn chữ ký số GOST R34.10-94.
- Xây dựng một số lược đồ chữ ký số dựa trên các lược đồ cơ sở theo mô