

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

NGUYỄN THỊ CHUNG THỦY

NGHIÊN CỨU MỘT SỐ KỸ THUẬT AN TOÀN
THÔNG TIN DÙNG TRONG KIỂM PHIẾU ĐIỆN TỬ

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

THÁI NGUYÊN - 2015

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

NGUYỄN THỊ CHUNG THỦY

**NGHIÊN CỨU MỘT SỐ KỸ THUẬT AN TOÀN
THÔNG TIN DÙNG TRONG KIỂM PHIẾU ĐIỆN TỬ**

Chuyên ngành: Khoa học máy tính

Mã số: 60 48 01 01

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

Người hướng dẫn khoa học: PGS.TS TRỊNH NHẬT TIẾN

THÁI NGUYÊN - 2015

LỜI CAM ĐOAN

Tôi xin cam đoan luận văn này của tự bản thân tôi tìm hiểu, nghiên cứu dưới sự hướng dẫn của PGS.TS Trịnh Nhật Tiến. Các chương trình thực nghiệm do chính bản thân tôi lập trình, các kết quả là hoàn toàn trung thực. Các tài liệu tham khảo được trích dẫn và chú thích đầy đủ.

TÁC GIẢ LUẬN VĂN

Nguyễn Thị Chung Thủy

LỜI CẢM ƠN

Em xin bày tỏ lời cảm ơn chân thành tới tập thể các thầy cô giáo Viện công nghệ thông tin - Viện Hàn lâm Khoa học và Công nghệ Việt Nam, các thầy cô giáo Trường Đại học Công nghệ thông tin và truyền thông - Đại học Thái Nguyên đã dạy dỗ chúng em trong suốt quá trình học tập chương trình cao học tại trường.

Đặc biệt em xin bày tỏ lòng biết ơn sâu sắc tới thầy giáo PGS.TS Trịnh Nhật Tiến, Trường Đại học Công nghệ - Đại học Quốc gia Hà Nội đã quan tâm, định hướng và đưa ra những góp ý, gợi ý, chỉnh sửa quý báu cho em trong quá trình làm luận văn tốt nghiệp.

Cuối cùng, em xin chân thành cảm ơn các bạn bè đồng nghiệp, gia đình và người thân đã quan tâm, giúp đỡ và chia sẻ với em trong suốt quá trình làm luận văn tốt nghiệp.

Thái Nguyên, ngày tháng năm 2015

HỌC VIÊN

Nguyễn Thị Chung Thủy

MỤC LỤC

LỜI CAM ĐOAN.....	i
LỜI CẢM ƠN	ii
MỤC LỤC.....	iii
DANH MỤC CÁC HÌNH.....	vii
MỞ ĐẦU	1
1. Lý do lựa chọn đề tài.....	1
2. Mục đích nghiên cứu.....	2
3. Đối tượng và phạm vi nghiên cứu.....	2
4. Tóm tắt luận điểm cơ bản.....	2
5. Phương pháp nghiên cứu.....	3
6. Nội dung luận văn	3
Chương 1. TỔNG QUAN VỀ BỎ PHIẾU ĐIỆN TỬ VÀ MỘT SỐ BÀI TOÁN TRONG KIỂM PHIẾU ĐIỆN TỬ	4
1.1. Tổng quan về bỏ phiếu điện tử.....	4
1.1.1. Khái niệm bỏ phiếu.....	4
1.1.2. Khái niệm bỏ phiếu điện tử.....	4
1.1.3. So sánh bỏ phiếu từ xa với bỏ phiếu truyền thống	5
1.1.4. Các thành phần trong hệ thống bỏ phiếu điện tử	6
1.1.5. Các giai đoạn bỏ phiếu điện tử	7
1.1.6. Thực trạng bỏ phiếu điện tử ở Việt Nam và trên Thế giới	14
1.2. Một số bài toán phát sinh trong giai đoạn kiểm phiếu điện tử.....	15
1.2.1. Phòng tránh thành viên ban kiểm phiếu thông gian: sửa đổi nội dung lá phiếu.....	15
1.2.2. Phòng tránh cử tri bán phiếu bầu cho ứng cử viên	16
1.2.3. Giải mã lá phiếu để kiểm phiếu	17
1.3. Vấn đề mã hóa.....	18
1.3.1. Mã hóa khóa đối xứng (mã hóa khóa riêng).....	20

1.3.2. Mã hóa khóa bất đối xứng (mã hóa khóa công khai)	21
Chương 2. MỘT SỐ KỸ THUẬT BẢO ĐẢM AN TOÀN THÔNG TIN	
ỨNG DỤNG TRONG KIỂM PHIẾU ĐIỆN TỬ	24
2.1. Kỹ thuật mã khóa trên đường cong Elliptic	24
2.1.1. Hệ mã hóa Elgamal cổ điển	24
2.1.2. Hệ mã hóa trên đường cong Elliptic	25
2.2. Kỹ thuật chia sẻ bí mật.....	33
2.2.1. Khái niệm “Chia sẻ bí mật”	33
2.2.2. Ví dụ về “Chia sẻ bí mật”	33
2.2.3. Sơ đồ “Chia sẻ bí mật” Shamir	34
2.3. Kỹ thuật chứng minh không tiết lộ thông tin	37
2.3.1. Khái niệm “Chứng minh không tiết lộ thông tin” và Giao thức Σ	37
2.3.2. Chứng minh tính hợp lệ của lá phiếu (x, y) (Giao thức 1)	38
2.3.3. Chứng minh quyền sở hữu giá trị bí mật β (Giao thức 2).....	41
2.3.4. Giai đoạn cử tri chuyển lá phiếu tới ban kiểm phiếu với phương án 2	43
Chương 3. ỨNG DỤNG TRONG KIỂM PHIẾU ĐIỆN TỬ	45
3.1. Ứng dụng hệ mã hóa trên đường cong Elliptic trong bầu cử điện tử.....	45
3.1.1. Các đối tượng của hệ thống bầu cử	45
3.1.2. Thiết lập	45
3.1.3. Bỏ phiếu	46
3.1.4. Mở phiếu bầu	46
3.2. Ứng dụng sơ đồ chia sẻ bí mật Shamir trong kiểm phiếu điện tử.....	47
3.3. Chương trình thử nghiệm.....	49
3.3.1. Môi trường cài đặt và thử nghiệm	49
3.3.2. Phát biểu bài toán.....	49
3.3.3. Thiết kế phần mềm	50
3.3.4. Giao diện chương trình và kết quả thử nghiệm	51
3.3.5. Đánh giá	59

KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN ĐỀ TÀI	61
TÀI LIỆU THAM KHẢO	63

DANH MỤC CÁC BẢNG

Bảng 3.1: Bảng so sánh về độ dài khóa của EC- Elgamal và Elgamal..... 61

DANH MỤC CÁC HÌNH

Hình 1.1:	Sơ đồ giai đoạn đăng ký bỏ phiếu	9
Hình 1.2:	Sơ đồ giai đoạn bỏ phiếu	10
Hình 1.3:	Sơ đồ giai đoạn kiểm phiếu	12
Hình 1.4:	Sơ đồ tổng quan quy trình Bỏ phiếu điện tử	13
Hình 1.5:	Sơ đồ kỹ thuật mã hóa hai tầng	16
Hình 1.6:	Quy trình tính kết quả bầu cử	17
Hình 1.7:	Sơ đồ mã hóa dữ liệu	19
Hình 1.8:	Sơ đồ hoạt động của mã hóa khóa đối xứng	21
Hình 1.9:	Sơ đồ hoạt động của mã hóa khóa bất đối xứng	22
Hình 2.1:	Phép cộng trên đường cong Elliptic	28
Hình 2.2:	Phép nhân đôi trên đường cong Elliptic	29
Hình 2.3:	Sơ đồ giai đoạn cử tri chuyển lá phiếu tới ban kiểm phiếu	39
Hình 3.1:	Sơ đồ chia sẻ ngưỡng A (t,m) trong giai đoạn kiểm phiếu	49
Hình 3.2:	Giao diện chính của chương trình	51
Hình 3.3:	Ban bầu cử đăng nhập vào hệ thống lưu trữ khóa	52
Hình 3.4:	Giao diện chính của hệ thống lưu trữ khóa	53
Hình 3.5:	Thông báo tạo cơ sở dữ liệu cho ban kiểm phiếu thành công	53
Hình 3.6:	Thông báo tạo dữ liệu cho cử tri thành công	54
Hình 3.7:	Bảng danh sách cử tri	54
Hình 3.8:	Danh sách cử tri sau khi được ban bầu cử tạo cơ sở dữ liệu	54
Hình 3.9:	Cử tri đăng nhập hệ thống	55
Hình 3.10:	Giao diện cử tri bỏ phiếu	56
Hình 3.11:	Giao diện ban kiểm phiếu đăng nhập hệ thống	57
Hình 3.12:	Giao diện mảnh khóa	57
Hình 3.13:	Kết quả cuộc bầu cử	58
Hình 3.14:	Kết quả cuộc bầu cử trên cơ sở dữ liệu của hệ thống	59

