

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC CNTT&TT THÁI NGUYÊN

NGUYỄN HẢI TRƯỜNG

NGHIÊN CỨU KẾT HỢP SƠ ĐỒ CHIA SẺ BÍ MẬT
SHAMIR VÀ HỆ MÃ HÓA ELGAMAL, ỨNG DỤNG
TRONG BỎ PHIẾU ĐIỆN TỬ

LUẬN VĂN THẠC SỸ KHOA HỌC MÁY TÍNH

THÁI NGUYÊN, 2014

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC CNTT&TT THÁI NGUYÊN

NGUYỄN HẢI TRƯỜNG

**NGHIÊN CỨU KẾT HỢP SƠ ĐỒ CHIA SẺ BÍ MẬT
SHAMIR VÀ HỆ MÃ HÓA ELGAMAL, ỨNG DỤNG
TRONG BỎ PHIẾU ĐIỆN TỬ**

Chuyên ngành: Khoa học máy tính

Mã số: 60 48 01

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

NGƯỜI HƯỚNG DẪN KHOA HỌC

TS. VŨ MẠNH XUÂN

THÁI NGUYÊN, 2014

LỜI CAM ĐOAN

Tên tôi là: Nguyễn Hải Trường

Sinh ngày: 05/11/1980

Học viên lớp cao học CHK11G - Trường Đại học Công nghệ thông tin và Truyền thông – Đại học Thái Nguyên.

Hiện đang công tác tại: Trường THPT Ý La

Xin cam đoan: Đề tài “*Nghiên cứu kết hợp sơ đồ chia sẻ bí mật Shamir và hệ mã hóa Elgamal, ứng dụng trong bỏ phiếu điện tử*” do Thầy giáo TS. Vũ Mạnh Xuân hướng dẫn là công trình nghiên cứu của riêng tôi. Tất cả tài liệu tham khảo đều có nguồn gốc, xuất xứ rõ ràng.

Tác giả xin cam đoan tất cả những nội dung trong luận văn đúng như nội dung trong đề cương và yêu cầu của thầy giáo hướng dẫn. Nếu sai tôi hoàn toàn chịu trách nhiệm trước hội đồng khoa học và trước pháp luật.

Thái Nguyên, ngày .. tháng .. năm 2014

TÁC GIẢ LUẬN VĂN

LỜI CẢM ƠN

Sau sáu tháng nghiên cứu và làm việc nghiêm túc, được sự động viên, giúp đỡ và hướng dẫn tận tình của Thầy giáo hướng dẫn TS. Vũ Mạnh Xuân, luận văn với đề tài “*Nghiên cứu kết hợp sơ đồ chia sẻ bí mật Shamir và hệ mã hóa Elgamal, ứng dụng trong bảo phiếu điện tử*” đã hoàn thành.

Tôi xin bày tỏ lòng biết ơn sâu sắc đến:

Thầy giáo hướng dẫn TS. Vũ Mạnh Xuân đã tận tình chỉ dẫn, giúp đỡ tôi hoàn thành luận văn này.

Trường THPT Ý La đã tạo điều kiện về mặt thời gian giúp tôi yên tâm học tập.

Khoa sau Đại học Trường Đại học công nghệ thông tin và truyền thông đã giúp đỡ tôi trong quá trình học tập cũng như thực hiện luận văn.

Tôi xin chân thành cảm ơn bạn bè, đồng nghiệp và gia đình đã động viên, khích lệ, tạo điều kiện giúp đỡ tôi trong suốt quá trình học tập, thực hiện và hoàn thành luận văn này.

TÁC GIẢ LUẬN VĂN

MỤC LỤC

LỜI CAM ĐOAN	i
LỜI CẢM ƠN.....	ii
DANH MỤC HÌNH VẼ	iii
DANH MỤC BẢNG BIỂU.....	v
MỞ ĐẦU	1
CHƯƠNG 1. BỔ PHIẾU ĐIỆN TỬ	4
1.1. Tổng quan về bổ phiếu điện tử	4
1.1.1. Khái niệm về bổ phiếu	4
1.1.2. Khái niệm bổ phiếu điện tử.....	4
1.1.3. Các thành phần trong hệ thống bổ phiếu điện tử	5
1.1.4. Các giai đoạn bổ phiếu điện tử	5
1.2. Mật mã trong bổ phiếu điện tử	6
1.2.1. Kiểm tra tổng các phiếu bầu thay vì kiểm tra từng lá phiếu	6
1.2.2. Mật mã ngưỡng giúp đạt tính phân quyền trong kiểm phiếu.....	9
1.2.3. Mã hóa xác suất giúp giữ vững tính ẩn danh của phiếu bầu.....	9
1.2.4. Chứng minh tương tác để chống việc bán phiếu bầu.....	10
Kết luận chương 1	11
CHƯƠNG 2. CƠ SỞ LÝ THUYẾT	13
2.1. Tổng quan về an toàn và bảo mật thông tin.....	13
2.1.1. Sự cần thiết của bảo đảm an toàn thông tin	13
2.1.2. Khái niệm an toàn thông tin.....	13
2.1.3. Các phương pháp bảo vệ thông tin	15
2.1.4. An toàn thông tin bằng mật mã.....	16
2.1.5. Vai trò của hệ mật mã	17
2.1.6. Phân loại hệ mật mã.....	18
2.1.7. Tiêu chuẩn đánh giá hệ mật mã	19

2.2. Cơ sở toán học của mật mã.....	19
2.2.1. Nhóm , vành và không gian Z_p	19
2.2.2. Bài toán logarit rời rạc	20
2.3. Mã hóa	21
2.3.1. Mã hóa dữ liệu	21
2.3.2. Phân loại.....	24
2.3.3. Ưu khuyết điểm của hai phương pháp	28
Kết luận chương 2	29
CHƯƠNG 3. ỨNG DỤNG HỆ MẬT ELGAMAL SƠ ĐỒ CHIA SẺ BÍ MẬT	
TRONG BỎ PHIẾU ĐIỆN TỬ	30
3.1. Hệ mật mã khóa công khai	30
3.1.1. Tổng quan về hệ mật mã khóa công khai	30
3.1.2. Hệ mật Elgamal.....	31
3.2. Chia sẻ khóa bí mật	33
3.2.1. Kỹ thuật Chia sẻ khóa bí mật (Secret Sharing).....	33
3.2.2. Các sơ đồ chia sẻ bí mật:	34
3.3. Ứng dụng hệ mã hóa đồng cấu Elgamal và sơ đồ chia sẻ bí mật Shamir trong một số bài toán bỏ phiếu điện tử	38
3.3.1. Ứng dụng hệ mã hóa Elgamal cho bỏ phiếu đồng ý /không đồng ý.....	38
3.3.2. Sơ đồ chia sẻ bí mật Shamir kết hợp với hệ mã hóa Elgamal cho bài toán loại bỏ phiếu chọn L trong K.	40
3.4. Khảo sát thực trạng tại Văn phòng UBND Tỉnh Tuyên Quang	44
3.4.1. Giới thiệu chung về Văn phòng UBND Tỉnh Tuyên Quang	44
3.4.2. Thực trạng các cuộc bỏ phiếu/bầu cử tại VP UBND Tỉnh	46
3.4.3. Một số mẫu biểu liên quan.....	46
3.5. Xây dựng chương trình bỏ phiếu điện tử.....	50
3.5.1. Khảo sát thực trạng và phát biểu bài toán.....	50
3.5.2. Chương trình demo	51
3.5.3. Một số kết quả đạt được.....	54
Kết luận chương 3	59
KẾT LUẬN	61
TÀI LIỆU THAM KHẢO	62

DANH MỤC HÌNH VẼ

Hình 2.1	Mã hoá với khoá mã và khoá giải giống nhau	18
Hình 2.2	Quy trình mã hóa dữ liệu.....	22
Hình 2.3	Sơ đồ mã hóa và giải mã	23
Hình 2.4	Sơ đồ mã hóa và giải mã bằng khóa riêng	25
Hình 2.5	Sơ đồ mã hóa và giải mã bằng khóa công khai.....	26
Hình 3.1	Sơ đồ mã hóa công khai	30
Hình 3.2	Sơ đồ bỏ phiếu đồng ý/ không đồng ý	39
Hình 3.3	Sơ đồ bỏ phiếu chọn L trong K.....	42
Hình 3.4	Sơ đồ tổ chức Văn phòng UBND Tỉnh Tuyên Quang	45
Hình 3.5	Thủ tục qui trình bầu cử hội đồng nhân dân cấp tỉnh.....	49
Hình 3.6	Mẫu danh sách cử tri	50
Hình 3.7	Giao diện chương trình chính.....	55
Hình 3.8	Giao diện chương trình bỏ phiếu có/không đồng ý.....	56
Hình 3.9	Giao diện chương trình bỏ phiếu chọn L trong K.....	58

DANH MỤC BẢNG BIỂU

Bảng 2.1	Các ưu khuyết điểm của hệ thống khóa bí mật (khóa đối xứng)	28
Bảng 2.2	Các ưu khuyết điểm của hệ thống mã hóa khóa công khai	28
Bảng 3.1	Một số ví dụ về mã hóa và giải mã	32
Bảng 3.2	Các file chính để minh họa Bài toán bỏ phiếu có/không đồng ý	52
Bảng 3.3	Các file chính để minh họa Bài toán bỏ phiếu “chọn L trong K”	54

MỞ ĐẦU

1. Tính khoa học và cấp thiết của đề tài

Trong những năm gần đây, sự phát triển, hội tụ và tương tác các xu thế công nghệ đã mở ra nhiều cơ hội phát triển cho Chính phủ điện tử. Một trong những phương diện mới đánh dấu sự phát triển của Chính phủ điện tử và đã được kiểm chứng ở một số nước phương Tây là *bỏ phiếu điện tử*.

Phương thức bỏ phiếu truyền thống gặp phải một số hạn chế: với những cử tri ở vùng sâu vùng xa, khoảng cách về địa lý sẽ bị hạn chế việc thực hiện được quyền bỏ phiếu của mình; tính độc lập, cá nhân và quyền riêng tư của cử tri sẽ bị ảnh hưởng lớn; tính minh bạch, niềm tin vào số lần bỏ phiếu của một cử tri; việc đảm bảo an ninh cho bầu cử, tính minh bạch kết quả bầu cử, sự tham gia và thái độ tham gia của những cử tri trẻ đối với cuộc bầu cử; tính an ninh của những lá phiếu trong quá trình vận chuyển và kiểm phiếu. Cùng với đó là quá trình chuẩn bị cơ sở vật chất, đào tạo nhân lực phục vụ cho cuộc bầu cử. Đây quả là những khó khăn, thách thức vô cùng lớn.

Trong khi đó, với hình thức bỏ phiếu điện tử, mọi người dân đều có thể tự tay bỏ những lá phiếu của mình cho dù họ đang ở đâu, làm gì. Hơn nữa, nó còn đảm bảo được tính cá nhân và quyền riêng tư trong lá phiếu của mình, đảm bảo an ninh do không mất quá trình vận chuyển “thủ công” hòm phiếu từ nhiều địa điểm khác nhau mà nó đã được lưu trữ ngay lập tức vào hệ thống cơ sở dữ liệu. Thay vì đào tạo một đội ngũ cán bộ khổng lồ để phục vụ cho công tác bầu cử, việc bỏ phiếu điện tử sẽ gián tiếp tới mức tối đa về nhân lực. Và một điều đặc biệt, hình thức bỏ phiếu này sẽ đáp ứng nhu cầu bầu cử theo cách của những người trẻ đó có thể là bầu cử trực tuyến, có thể là bầu cử qua điện thoại hoặc bầu cử thông qua Facebook, Twiter, Youtube... Thông qua hệ thống Internet và những thiết bị thông minh, chính phủ có thể dễ dàng kết nối tất cả quá trình trước, trong và sau bầu cử nhanh, gọn, nhẹ; thu hút được đông đảo cử tri và không phân biệt đối tượng, vị trí địa lý. Điều này chắc chắn sẽ giảm bớt sức nặng tối đa cho cuộc bầu cử và mang lại thành công cho nó. Qua đó cũng thấy được tính ưu việt của hình thức bỏ phiếu điện tử. Với chính phủ, bỏ phiếu điện tử là một bước cụ thể hóa của chính phủ điện tử và được đánh giá là giải pháp hữu hiệu cho việc bầu cử của các quốc gia.

Trên thế giới, khái niệm bỏ phiếu điện tử (e-voting) không còn xa lạ gì đối với các nước phát triển, nhất là ở Bắc Mỹ và Châu Âu. Tại Châu Á, chỉ có ba nước đã từng thử nghiệm hệ thống bầu cử điện tử, đó là Hàn Quốc, Nhật Bản và

Ấn Độ, những nước có trình độ công nghệ phát triển cao. Tuy nhiên bầu cử điện tử tại ba nước này vẫn chưa được xem là thực sự thành công khi kết quả thu được từ những lá phiếu điện tử vẫn còn nhiều nghi vấn. Vấn đề lớn nhất chính là tính bảo mật của toàn hệ thống.

Tại Việt Nam bỏ phiếu điện tử mới chỉ dừng ở mục đích bầu chọn, bình chọn (bầu chọn Vịnh Hạ Long là di sản Thiên nhiên thế giới, bình chọn bài hát hay trên sóng truyền hình..) song chưa thể triển khai vào bầu cử Quốc hội do còn nhiều hạn chế (vấn đề ngân sách, giáo dục ý thức cho người dân, quá trình phổ biến, huấn luyện phương thức thực hiện cho các cấp, các bộ phận liên quan..). Đây rõ ràng là một khoảng trống khá lớn, nhất là việc kinh phí lắp đặt hệ thống máy bầu cử hay trở ngại trong khoảng cách vùng miền.

Để hoạt động bỏ phiếu hay bỏ phiếu phát huy đúng tác dụng thì cần đảm bảo hai yêu cầu về *tính kiểm tra được* và *tính tự do trong lựa chọn* [1], [2], [9]. Điều này chỉ có thể được thực hiện nhờ mật mã. Người đầu tiên đặt nền móng cho việc xây dựng các hệ bỏ phiếu tích hợp các phương pháp mật mã là Chaum vào năm 1981 [3]. Kể từ đó đến nay, các công trình công bố trên thế giới đều tập trung vào xây dựng ba mô hình bỏ phiếu cơ bản là: mô hình xáo trộn phiếu [3], mô hình chữ ký mù [4] và mô hình sử dụng mã hóa đồng cấu [6],[7],[9]. Trong đó, do tính ưu việt trong giải quyết vấn đề tính kiểm tra được và tính tự do trong lựa chọn mà gần đây, mô hình mã hóa đồng cấu được tập nghiên cứu nhiều nhất. Hiện tại ở Việt Nam, các công trình như [1], [2] mới chỉ dừng lại ở việc đề xuất áp dụng các mô hình bỏ phiếu mà chưa thực sự triển khai trên một ứng dụng cụ thể.

Chính vì vậy, được sự hướng dẫn của Thầy giáo, TS. Vũ Mạnh Xuân, tác giả lựa chọn đề tài luận văn tốt nghiệp “*Nghiên cứu kết hợp sơ đồ chia sẻ bí mật Shamir và hệ mã hóa Elgamal, ứng dụng trong bỏ phiếu điện tử*” với mong muốn áp dụng các kiến thức đã được học, xây dựng thử nghiệm mô hình bỏ phiếu điện tử tại văn phòng ủy ban nhân dân tỉnh Tuyên Quang.

2. Mục tiêu, đối tượng và phạm vi nghiên cứu của đề tài

Qua việc phân tích, khảo sát và đánh giá thực trạng bỏ phiếu điện tử tại Việt Nam cũng như thế giới, kết hợp với nghiên cứu các kỹ thuật, phương pháp, thuật toán mã hóa, mục tiêu của luận văn được xác định là: Ứng dụng tính chất đồng cấu của hệ mã hóa khóa công khai Elgamal và kỹ thuật chia sẻ khóa bí mật để giải quyết hai bài toán