HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

NGUYỄN TẤN ĐỨC

NGHIÊN CỨU PHÁT TRIỂN MỘT SỐ LƯỢC ĐỒ CHỮ KÝ SỐ MÙ, CHỮ KÝ SỐ TẬP THỂ MÙ DỰA TRÊN CÁC CHUẨN CHỮ KÝ SỐ

LUẬN ÁN TIẾN SĨ KỸ THUẬT

HÀ NỘI – NĂM 2020

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

NGUYỄN TẤN ĐỨC

NGHIÊN CỨU PHÁT TRIỂN MỘT SỐ LƯỢC ĐỒ CHỮ KÝ SỐ MÙ, CHỮ KÝ SỐ TẬP THỂ MÙ DỰA TRÊN CÁC CHUẨN CHỮ KÝ SỐ

Chuyên ngành: Kỹ thuật máy tính

Mã số: 9.48.01.06

LUẬN ÁN TIẾN SĨ KỸ THUẬT

NGƯỜI HƯỚNG DẪN KHOA HỌC:

1. PGS.TS. Nguyễn Hiếu Minh

2. TS. Ngô Đức Thiện

HÀ NỘI – NĂM 2020

LỜI CAM ĐOAN

Tôi xin cam đoan các kết quả nghiên cứu được trình bày trong luận án là các công trình nghiên cứu của tôi dưới sự hướng dẫn của cán bộ hướng dẫn, các kết quả nghiên cứu là trung thực và chưa được công bố trong bất kỳ công trình nào khác. Các dữ liệu tham khảo được trích dẫn đầy đủ.

Hà Nội, ngày tháng 12 năm 2020

Tác giả

Nguyễn Tấn Đức

LỜI CẢM ƠN

Trong quá trình học tập, nghiên cứu và thực hiện luận án, Nghiên cứu sinh đã nhận được sự định hướng, giúp đỡ, các ý kiến đóng góp quý báu và những lời động viên khích lệ chân thành của các nhà khoa học, các thầy cô, các đồng tác giả nghiên cứu, đồng nghiệp và gia đình.

Có được kết quả hôm nay, trước hết, nghiên cứu sinh xin bày tỏ lời cảm ơn chân thành tới các thầy hướng dẫn, cùng các nhóm nghiên cứu các công trình nghiên cứu đã công bố. Xin chân thành cảm ơn các thầy, cô ở khoa Đào tạo Sau Đại học và các thầy, cô ở Học viện Công nghệ Bưu chính Viễn thông đã giúp đỡ nghiên cứu sinh trong suốt thời gian thực hiện luận án.

Nghiên cứu sinh chân thành cảm ơn Ban Giám đốc Học viện Công nghệ Bưu chính Viễn thông đã tạo điều kiện thuận lợi để nghiên cứu sinh hoàn thành nhiệm vụ nghiên cứu.

Cuối cùng, nghiên cứu sinh bày tỏ lời cảm ơn tới đồng nghiệp, gia đình, và bạn bè đã luôn động viên, chia sẻ, ủng hộ, khuyến khích và giúp đỡ nghiên cứu sinh trong suốt quá trình học tập và nghiên cứu vừa qua.

NCS Nguyễn Tấn Đức

MỤC LỤC

LỜI CAM ĐOAN i
LỜI CẢM ƠN ii
MỤC LỤC iii
DANH MỤC CÁC THUẬT NGỮ, CHỮ VIẾT TẮT viii
DANH MỤC CÁC HÌNH VẼ x
DANH MỤC CÁC BẢNG xi
MỞ ĐẦU 1
CHƯƠNG 1. TỔNG QUAN VỀ CHỮ KÝ SỐ VÀ VẤN ĐỀ NGHIÊN CỨU 7
1.1. TỔNG QUAN VỀ CHỮ KÝ SỐ 7
1.1.1. Khái niệm chữ ký số 7
1.1.2. Lược đồ chữ ký số 8
1.1.3. Tạo và xác thực chữ ký số 9
1.1.4. Chức năng của chữ ký số 10
1.1.5. Phân loại tấn công chữ ký số 11
1.1.6. Các dạng phá vỡ lược đồ chữ ký số 12
1.2. CHỮ KÝ SỐ TẬP THỂ 12
1.3. CHỮ KÝ SỐ MÙ 14
1.4. CHỮ KÝ SỐ TẬP THỂ MÙ 17
1.5. MÔ HÌNH ĐÁNH GIÁ TÍNH AN TOÀN CỦA LƯỢC ĐỒ CHỮ KÝ SỐ - MÔ HÌNH TIÊN TRI NGẪU NHIÊN (ROM) 21
1.6. CƠ SỞ TOÁN HỌC ỨNG DỤNG TRONG CÁC LƯỢC ĐỒ CHỮ KÝ SỐ 22
1.6.1. Bài toán phân tích thừa số một số nguyên lớn (IFP) 22

1.6.2. Bài toán logarit rời rạc (DLP) 23

1.6.3. Bài toán logarit rời rạc trên đường cong elliptic (ECDLP) 25

1.7. MỘT SỐ CHUẨN CHỮ KÝ SỐ VÀ LƯỢC ĐỒ CHỮ KÝ SỐ PHỔ BIẾN SỬ DỤNG TRONG LUẬN ÁN 27

1.7.1. Lược đồ chữ ký số RSA 27

1.7.2. Lược đồ chữ ký số Schnorr 28

1.7.3. Lược đồ chữ ký số EC-Schnorr.....28

1.7.4. Chuẩn chữ ký số GOST R34.10-94 29

1.7.5. Chuẩn chữ ký số GOST R34.10-2012 30

1.8. MỘT SỐ LƯỢC ĐỒ CHỮ KÝ ĐƯỢC SỬ DỤNG ĐÁNH GIÁ, SO SÁNH TRONG LUẬN ÁN.....31

1.8.1. Một số lược đồ chữ ký số được sử dụng để so sánh với các lược đồ đề xuất trong luận án. 31

1.8.2. Một số nghiên cứu liên quan trong nước gần đây.....37

1.9. PHÂN TÍCH MỘT SỐ CÔNG TRÌNH NGHIÊN CỨU VỀ CHỮ KÝ SỐ ĐÃ CÔNG BỐ GẦN ĐÂY VÀ VẤN ĐỀ CẦN GIẢI QUYẾT TRONG LUẬN ÁN.....39

1.10. KẾT LUẬN CHƯƠNG 1 46

CHƯƠNG 2. PHÁT TRIỂN MỘT SỐ LƯỢC ĐỒ CHỮ KÝ SỐ TẬP THỂ MÙ DỰA TRÊN CÁC CHUẨN CHỮ KÝ SỐ VÀ LƯỢC ĐỒ CHỮ KÝ SỐ PHỔ BIẾN 47

2.1. ĐỀ XUẤT LƯỢC ĐỒ CHỮ KÝ SỐ TẬP THỂ MÙ DỰA TRÊN CHUẨN CHỮ KÝ SỐ GOST R34.10-94 VÀ LƯỢC ĐỒ CHỮ KÝ SỐ SCHNORR 47

2.1.1. Lược đồ chữ ký số tập thể mù dựa trên chuẩn GOST R34.10-94 48

2.1.2. Lược đồ chữ ký số tập thể mù dựa trên lược đồ Schnorr.....53

2.1.3. Đánh giá độ phức tạp thời gian của các lược đồ đề xuất 58

2.2. ĐỀ XUẤT LƯỢC ĐỒ CHỮ KÝ SỐ TẬP THỂ MÙ DỰA TRÊN CHUẨN CHỮ KÝ SỐ GOST R34.10-2012 VÀ LƯỢC ĐỒ EC-SCHNORR 62
2.2.1. Lược đồ chữ ký số tập thể mù dựa trên chuẩn GOST R34.10-2012 62
2.2.2. Lược đồ chữ ký số tập thể mù dựa trên lược đồ EC-Schnorr 67
2.2.3. Đánh giá độ phức tạp thời gian của các lược đồ đề xuất 72
2.3. ĐỘ PHỨC TẠP VỀ THỜI GIAN CỦA CÁC LƯỢC ĐỒ ĐỀ XUẤT ..75
2.3.1. Thực nghiệm 75
2.3.2. Đánh giá các lược đồ chữ ký số tập thể mù đề xuất 78
2.4. KẾT LUẬN CHƯƠNG 2 79
CHƯƠNG 3. PHÁT TRIỂN LƯỢC ĐỒ CHỮ KÝ SỐ MÙ VÀ CHỮ KÝ SỐ TẬP THỂ MÙ DỰA TRÊN HAI BÀI TOÁN KHÓ 80
3.1. ĐÁNH GIÁ MỘT SỐ LƯỢC ĐỒ CHỮ KÝ SỐ MÙ DỰA TRÊN VIỆC KẾT HỢP CỦA HAI BÀI TOÁN KHÓ 80
3.2. LƯỢC ĐỒ CHỮ KÝ SỐ MÙ, CHỮ KÝ SỐ TẬP THỂ MÙ DỰA TRÊN SỰ KẾT HỢP LƯỢC ĐỒ CHỮ KÝ SỐ RSA VÀ SCHNORR.85
3.2.1. Xây dựng lược đồ cơ sở 85
3.2.2. Lược đồ chữ ký số mù dựa trên lược đồ cơ sở.....86
3.2.3. Lược đồ chữ ký số tập thể mù dựa trên lược đồ cơ sở.....88
3.2.4. Đánh giá các lược đồ chữ ký số đề xuất 89
3.2.5. Đánh giá độ phức tạp thời gian của lược đồ chữ ký số đề xuất 92
3.3. ĐỀ XUẤT LƯỢC ĐỒ KÝ SỐ DỰA TRÊN NHÓM CON HỮU HẠN KHÔNG VÒNG HAI CHIỀU.....95
3.3.1. Tổng quan về lược đồ đề xuất.....95
3.3.2. Thiết lập các nhóm con hữu hạn không vòng hai chiều.....95
3.3.3. Xây dựng lược đồ ký số cơ sở dựa trên bài toán khó mới đề xuất .101

3.3.4. Xây dựng lược đồ chữ ký số mù dựa trên lược đồ chữ ký số cơ sở103
3.3.5. Xây dựng lược đồ ký số tập thể mù mới 105
3.3.6. Đánh giá các lược đồ đề xuất 107
3.4. KẾT LUẬN CHƯƠNG 3 114
CHƯƠNG 4. ỨNG DỤNG LƯỢC ĐỒ CHỮ KÝ SỐ TẬP THỂ MÙ ĐỀ XUẤT VÀO LƯỢC ĐỒ BẦU CỬ ĐIỆN TỬ 115
4.1. GIỚI THIỆU 115
4.2. TỔNG QUAN VỀ HỆ THỐNG BẦU CỬ ĐIỆN TỬ 117
4.3. CÁC LƯỢC ĐỒ CHỮ KÝ SỐ SỬ DỤNG TRONG LƯỢC ĐỒ BẦU CỬ ĐIỆN TỬ ĐỀ XUẤT 118
4.3.1. Lược đồ chữ ký số tập thể mù dựa trên Schnorr 119
4.3.2. Lược đồ chữ ký số tập thể mù dựa trên EC-Schnorr 121
4.3.3. Chữ ký số trên token được làm mù 122
4.3.4. Chữ ký trên phiếu bầu được làm mù 123
4.3.5. Xác thực thông tin dựa trên thông tin ẩn danh 123
4.4. LƯỢC ĐỒ BẦU CỬ ĐIỆN TỬ SỬ DỤNG LƯỢC ĐỒ CHỮ KÝ SỐ TẬP THỂ MÙ ĐỀ XUẤT DỰA TRÊN SCHNORR VÀ EC-SCHNORR124
4.4.1. Cấu hình của lược đồ đề xuất 124
4.4.2. Các tầng hoạt động của lược đồ đề xuất 129
4.5. ĐÁNH GIÁ VÀ PHÂN TÍCH 135
4.6. ĐÁNH GIÁ ĐỘ AN TOÀN CỦA LƯỢC ĐỒ BẦU CỬ ĐỀ XUẤT ..137
4.7. KẾT LUẬN CHƯƠNG 4 138
KẾT LUẬN 140
CÁC CÔNG TRÌNH KHOA HỌC ĐÃ CÔNG BỐ 144
TÀI LIỆU THAM KHẢO 145

DANH MỤC CÁC KÝ HIỆU

Ký hiệu	Nghĩa của các ký hiệu
$\{0,1\}^*$	Ký hiệu chuỗi bit có độ dài bất kỳ
$\{0,1\}^k$	Ký hiệu chuỗi bit có độ dài k
2^∞	Tập tất cả các Oracle
$\phi(n)$	Hàm phi Euler của n
ε	Hàm nhỏ không đáng kể
$H(M)$	Giá trị băm của M
pk	Khóa công khai (Public Key)
sk	Khóa bí mật (Secret Key)
Z	Tập số nguyên
Z_p^*	Nhóm nhân hữu hạn
Sig	Thủ tục ký
Ver	Thủ tục xác thực
Gen	Thủ tục tạo khóa

DANH MỤC CÁC THUẬT NGỮ, CHỮ VIẾT TẮT

Từ viết tắt	Nghĩa tiếng Anh	Nghĩa tiếng Việt
ACMA	Adaptive Chosen Message Attack	Tấn công văn bản được lựa chọn thích ứng
	Blind MultiSignature	Chữ ký số tập thể mù
CNTT	Information Technology	Công nghệ thông tin
DCMA	Directed Chosen Message Attack	Tấn công văn bản được lựa chọn trực tiếp
DLP	Discrete Logarithm Problem	Bài toán logarit rời rạc
DS	Digital Signature	Chữ ký số
DSA	Digital Signature Algorithm	Thuật toán chữ ký số
DSS	Digital Signature Standard	Chuẩn chữ ký số
EC	Elliptic Curve	Đường cong elliptic
ECC	Elliptic Curve Cryptography	Mã hóa trên đường cong elliptic
ECDLP	Elliptic Curve Discrete Logarithm Problem	Bài toán logarit rời rạc trên đường cong elliptic
ECDSA	Elliptic Curve Digital Signature Algorithm	Thuật toán chữ ký số dựa trên đường cong elliptic
GCMA	Generic Chosen Message Attack	Tấn công văn bản được lựa chọn tổng quát
IFP	Integer Factorization Problem	Bài toán phân tích thừa số nguyên tố
KMA	Known Message Attack	Tấn công văn bản được biết
KOA	Key Only Attacks	Tấn công vào khoá
MA	Message Attacks	Tấn công vào văn bản

NFS	Number Field Sieve	Thuật toán sàng trường số
QS	Quadratic Sieve	Thuật toán sàng bậc hai
ROM	Random Oarcle Model	Mô hình tiên tri ngẫu nhiên
TB	Total Break	Phá vỡ hoàn toàn
TTP	Trusted Third Party	Bên thứ ba tin cậy
UCLN		Ước số chung lớn nhất

DANH MỤC CÁC HÌNH VẼ

Hình 1.1. Quy trình tạo chữ ký số 9
Hình 1.2. Quy trình xác thực chữ ký số 10
Hình 1.3. Luồng cấu trúc chữ ký số mù 16
Hình 1.4. Tiến trình của chữ ký số tập thể mù 18
Hình 2.1. Tóm tắt thuật toán ký số của LĐ 2.01 50
Hình 2.2. Tóm tắt thuật toán ký số của LĐ 2.02 55
Hình 2.3. Tóm tắt thuật toán ký số của LĐ 2.03 64
Hình 2.4. Tóm tắt thuật toán ký số của LĐ 2.04 69
Hình 3.1. Tóm tắt thuật toán ký số của lược đồ chữ ký số mù đề xuất 105
Hình 3.2. Tóm tắt thuật toán ký số của lược đồ ký số tập thể mù đề xuất 107
Hình 4.1. Kiến trúc tổng quan của lược đồ bầu cử điện tử đề xuất 124
Hình 4.2. Sơ đồ luồng dữ liệu của tầng cấp phát token 129
Hình 4.3. Sơ đồ luồng dữ liệu của tầng đăng ký 131
Hình 4.4. Sơ đồ luồng dữ liệu của tầng bỏ phiếu 133
Hình 4.5. Thủ tục tạo phiếu bầu ở tầng bỏ phiếu 134
Hình 4.6. Sơ đồ luồng dữ liệu của tầng kiểm phiếu 134

DANH MỤC CÁC BẢNG

Bảng 2.1. Độ phức tạp thời gian của lược đồ LĐ 2.01 59

Bảng 2.2. Độ phức tạp thời gian của lược đồ [73].....59

Bảng 2.3. So sánh độ phức tạp thời gian của lược đồ LĐ 2.01 và lược đồ [73].....60

Bảng 2.4. Độ phức tạp thời gian của lược đồ LĐ 2.02 60

Bảng 2.5. Độ phức tạp thời gian của lược đồ [72].....61

Bảng 2.6. So sánh độ phức tạp thời gian của lược đồ LĐ 2.02 và lược đồ [72].....61

Bảng 2.7. Chi phí thời gian của LĐ 2.01 và LĐ 2.02 62

Bảng 2.8. Độ phức tạp thời gian của lược đồ LĐ 2.03 73

Bảng 2.9. So sánh độ phức tạp thời gian của lược đồ LĐ 2.03 và lược đồ [73].....73

Bảng 2.10. Độ phức tạp thời gian của lược đồ LĐ 2.04 74

Bảng 2.11. Độ phức tạp thời gian của lược đồ [79].....74

Bảng 2.12. So sánh chi phí thời gian của LĐ 2.04 và lược đồ [73] và [79] 74

Bảng 2.13. So sánh chi phí thời gian của LĐ 2.03 và lược đồ LĐ 2.04 75

Bảng 2.14. Chi phí thời gian của lược đồ đề xuất theo chuẩn GOST (mili giây).....76

Bảng 2.15. Chi phí thời gian của lược đồ đề xuất theo Schnorr (mili giây) 77

Bảng 2.16. So sánh chi phí thời gian các lược đồ chữ ký số tập thể mù đề xuất.....78

Bảng 3.1. So sánh độ phức tạp thời gian của lược đồ chữ ký số tập thể mù đề xuất và lược đồ [45] và [CT4] (Thủ tục sinh chữ ký).....93

Bảng 3.2. So sánh độ phức tạp thời gian của lược đồ chữ ký mù đề xuất và lược đồ [CT4], [45] (Thủ tục kiểm tra chữ ký) 93

Bảng 3.3. So sánh độ phức tạp tính toán các pha của lược đồ đề xuất và [CT4].....94

Bảng 3.4. Chi phí thời gian của lược đồ đề xuất và lược đồ [69], [93] 112

Bảng 3.5. Chi phí thời gian của lược đồ đề xuất và lược đồ [69], [93] 112

Bảng 3.6. Chi phí thời gian của lược đồ đề xuất và lược đồ [70], [72] 113

Bảng 3.7. Kích thước chữ ký của lược đồ đề xuất và [69], [70], [72], [93] 113

Bảng 4.1. Bảng danh sách cử tri (*danhsachcutri*).....126

Bảng 4.2. Bảng danh sách token (*danhsachtoken*) 127

Bảng 4.3. Bảng danh sách phiếu bầu đã làm mù (*bangphieubau*).....128

Bảng 4.4. Bảng danh sách phiếu bầu đã được giải mù (*bangkiemphieu*) 128

Bảng 4.5. Chi phí thời gian yêu cầu cho các tầng của lược đồ bầu cử 136

MỞ ĐẦU

1. Tính cấp thiết của đề tài

Cách mạng công nghiệp lần thứ 4 còn có thể gọi là cuộc cách mạng số sẽ chuyển hóa thế giới thực thành thế giới số, thúc đẩy phát triển chính phủ số và kinh tế số. Theo đó, hầu hết dữ liệu của nền kinh tế và Chính phủ sẽ được lưu trữ, trao đổi và xác thực qua môi trường mạng sẽ đặt ra thách thức là làm thế nào để đảm bảo an toàn cho các giao dịch điện tử đó. Sử dụng chữ ký số là một trong những câu trả lời hiệu quả nhất hiện nay, là một trong các giải pháp xác thực an toàn được ứng dụng phổ biến ở nhiều nước trên thế giới và ở Việt Nam hiện nay. Chữ ký số giúp đảm bảo an toàn cho các giao dịch trên môi trường mạng, giải quyết vấn đề về toàn vẹn dữ liệu, là bằng chứng để ngăn chặn việc chối bỏ trách nhiệm trên nội dung đã ký, giúp các doanh nghiệp, tổ chức, cá nhân có thể yên tâm khi giao dịch trên mạng.

Khái niệm chữ ký số đầu tiên được đề xuất vào năm 1976 bởi hai nhà mật mã học nổi tiếng Whitfield Diffie và Martin Hellman dựa trên mật mã khóa công khai, đã cho thấy những đặc tính nổi bật và vô cùng quan trọng trong việc đảm bảo an toàn cho các giao dịch trao đổi thông tin qua mạng. Cho đến nay, chữ ký số đã có những bước phát triển mạnh mẽ và trở thành bộ phận cấu thành quan trọng của ngành mật mã học. Dựa vào các tiêu chí khác nhau có thể chia lược đồ chữ ký số thành nhiều loại như chữ ký số nhóm, chữ ký số tập thể, chữ ký số đại diện, chữ ký số ngưỡng, hay các loại chữ ký số mù,...

Trong các loại chữ ký số thì chữ ký số mù là một loại chữ ký số đặc biệt được phát minh bởi Chaum [13] vào năm 1983, chữ ký này được ứng dụng nhiều trong các hệ thống yêu cầu đảm bảo tính riêng tư của các bên tham gia. Hiện nay, lược đồ chữ ký số mù đang được nghiên cứu, phát triển và ứng dụng trong nhiều hệ thống như thương mại điện tử, thanh toán trực tuyến hay bầu cử điện tử. Hơn nữa, với việc sử dụng ngày càng nhiều giao dịch trực tuyến như hiện nay thì vai trò của lược đồ chữ ký số mù trong việc đảm bảo an toàn và tính riêng tư của khách hàng lại càng trở nên quan trọng hơn bao giờ hết.

Có thể thấy rằng, từ khi David Chaum đề xuất lược đồ chữ ký số mù đầu tiên dựa trên chữ ký số RSA, sau đó có rất nhiều nghiên cứu về lược đồ chữ ký số mù, chữ ký số tập thể mù được công bố. Có thể chia thành các hướng nghiên cứu như: (1) Lược đồ dựa trên các chuẩn, lược đồ phổ biến để kế thừa tính an toàn và hiệu quả của chúng. Tuy nhiên có nhiều lược đồ chủ yếu dựa trên một bài toán khó nên xác suất bị phá vỡ là cao, để tăng cường tính an toàn thì cần phải phát triển các lược đồ thực sự dựa trên nhiều bài toán khó, điều này sẽ làm cho việc tấn công trở nên khó khăn hơn khi phải giải đồng thời nhiều bài toán khó. Ngoài ra cũng có các lược đồ dựa trên hai bài toán khó nhưng chưa được chứng minh trong mô hình chuẩn hoặc mô hinh ROM nên cần cải tiến thêm. (2) Lược đồ không dựa trên chuẩn, có hai loại là dựa trên một bài toán khó hoặc hai bài toán khó. Tuy nhiên, mặc dù các tác giả có chứng minh tính an toàn nhưng do không dựa trên các chuẩn và cũng chưa được kiểm nghiệm bởi các tổ chức về tiêu chuẩn nên còn phải tiếp tục nghiên cứu thêm.

Cơ sở toán học cho các loại lược đồ chữ ký số hiện nay cơ bản dựa trên 3 bài toán khó nổi tiếng và được xem là không thể giải được trong thời gian đa thức là bài toán phân tích thừa số một số nguyên lớn (IFP), bài toán logarit rời rạc (DLP) và bài toán logarit rời rạc trên đường cong elliptic (ECDLP). Tuy nhiên, với sự phát triển nhanh chóng của công nghệ tính toán thì việc giải các bài toán khó trên chỉ còn là vấn đề thời gian nhất là khi máy tính lượng tử được phát triển, nên việc nghiên cứu các cơ sở toán học cho các lược đồ chữ ký số mới nhằm tăng độ an toàn hơn là điều rất quan trọng trong thời điểm hiện nay, nhất là trong bối cảnh Chính phủ Việt Nam đang rất quyết tâm thực hiện chuyển đổi số trong thời gian tới.

Từ phân tích trên, việc ứng dụng các chuẩn chữ ký số, lược đồ chữ ký số đã được đánh giá là hiệu quả và an toàn làm cơ sở để xây dựng các lược đồ ký số mù, đồng thời nghiên cứu các giao thức ký số mới là vấn đề có tính thời sự và thực tiễn. Xuất phát từ thực tế đó, nghiên cứu sinh đã chọn đề tài "***Nghiên cứu phát triển một số lược đồ chữ ký số mù, chữ ký số tập thể mù dựa trên các chuẩn chữ ký số*** " với mong muốn có những đóng góp vào sự phát triển khoa học và công nghệ trong lĩnh

vực đảm bảo an toàn và tính riêng tư cho các giao dịch trực tuyến trên môi trường mạng.

2. Đối tượng và phạm vi nghiên cứu của luận án

Đối tượng nghiên cứu:

- Cơ sở của các hệ mật khóa công khai và các lược đồ chữ ký số.
- Các mô hình ứng dụng hệ mật khóa công khai và chữ ký số.
- Lược đồ chữ ký số mù, chữ ký số tập thể mù.

Phạm vi nghiên cứu:

- Hệ mật khóa công khai RSA, Schnorr, EC-Schnorr, chuẩn chữ ký số GOST R34.10-94, GOST R34.10-2012.
- Các cơ sở toán học liên quan như bài toán IFP, DLP, ECDLP.
- Cơ sở lý thuyết về phát triển chữ ký số.
- Cơ sở, mô hình chữ ký số mù, chữ ký số tập thể mù.
- Mô hình ứng dụng chữ ký số mù.

3. Mục tiêu nghiên cứu

Mục tiêu nghiên cứu của luận án là cung cấp một số đảm bảo toán học cho một số phiên bản lược đồ chữ ký số mù, chữ ký số tập thể mù được xây dựng từ các chuẩn chữ ký số và chữ ký số phổ biến đã được chứng minh về tính hiệu quả và an toàn. Đồng thời nghiên cứu thêm giao thức ký số mới làm cơ sở xây dựng lược đồ chữ ký số mù có kích thước khoá ngắn hơn trong khi vẫn đảm bảo mức độ an toàn như các lược đồ đã công bố.

4. Phương pháp nghiên cứu

Nghiên cứu sinh sử dụng phương pháp nghiên cứu là tham khảo các công trình, bài báo và sách, tài liệu chuyên ngành về mật mã, chữ ký số, chữ ký số tập thể, chữ ký số mù và chữ ký số tập thể mù, từ đó đề xuất lược đồ mới giải quyết

một số vấn đề còn tồn tại. Sử dụng các lý thuyết về các hệ mật phổ biến để xây dựng các giao thức và lược đồ chữ ký số mù mới. Chứng minh tính đúng đắn của các lược đồ đề xuất trong mô hình ROM. Đồng thời kết hợp với việc đánh giá thời gian tính toán các thuật toán của các lược đồ đề xuất bằng cách so sánh với các lược đồ đã công bố trước đó. Ngoài ra, còn tiến hành thực nghiệm trên máy tính để đánh giá thời gian tính toán một số lược đồ đề xuất.

5. Nội dung nghiên cứu của luận án

- Hệ mật khóa công khai RSA, Schnorr, EC-Schnorr và các chuẩn chữ ký số GOST R34.10-94, GOST R34.10-2012.

- Đề xuất các lược đồ chữ ký số tập thể mù dựa trên các chuẩn chữ ký số GOST R34-10.94 và lược đồ Schnorr. Chuẩn GOST R34-10.2012 và lược đồ EC-Schnorr.

- Xây dựng lược đồ chữ ký số cơ sở và lược đồ chữ ký số mù, tập thể mù dựa trên hai bài toán khó IFP và DLP (lược đồ RSA và Schnorr).

- Xây dựng bài toán khó mới dựa trên hai vấn đề khó về tính toán, trên cơ sở đó xây dựng lược đồ ký số mù mới có kích thước chữ ký được rút ngắn và dựa trên độ khó tính toán của bài toán DLP modulo một hợp số n và sử dụng các nhóm con hữu hạn không vòng hai chiều.

- Xây dựng lược đồ bầu cử điện tử ứng dụng chữ ký số mù đề xuất.

6. Ý nghĩa khoa học và thực tiễn

Việc cải tiến và phát triển các lược đồ chữ ký số nhằm đảm bảo khó bị phá vỡ, chữ ký số được rút ngắn nhưng vẫn đảm bảo tính an toàn, đồng thời khả thi để có thể triển khai trong thực tế là yêu cầu luôn được đặt ra cho các nhà nghiên cứu. Nghiên cứu của nghiên cứu sinh đóng góp cho khoa học và thực tiễn một số kết quả sau:

- Xây dựng một số lược đồ chữ ký số tập thể mù mới dựa trên các chuẩn và lược đồ chữ ký số phổ biến đã được chứng minh về tính an toàn và hiệu quả, đã

được áp dụng trong thực tế. Các lược đồ đề xuất được xem là có độ phức tạp về thời gian thấp hơn một số lược đồ đã được công bố.

- Xây dựng một số lược đồ chữ ký số mù, tập thể mù dựa trên hai bài toán khó, là các lược đồ phổ biến để đảm bảo tính an toàn và hiệu quả của các lược đồ đề xuất. Để phá vỡ các lược đồ này yêu cầu phải giải đồng thời hai bài toán khó, do đó việc phá vỡ lược đồ yêu cầu nhiều thời gian hơn.

- Xây dựng bài toán khó mới. Trên cơ sở đó, xây dựng lược đồ ký số mù mới có kích thước được rút ngắn hơn một số lược đồ đã công bố cùng hướng nghiên cứu nhưng vẫn đảm bảo mức độ an toàn tương đương các lược đồ đó, có thể sử dụng được trong các hệ thống có hạ tầng công nghệ thông tin thấp như khả năng lưu trữ, xử lý, năng lượng,…

7. Bố cục của luận án

Ngoài phần mở đầu giới thiệu tính cấp thiết, mục tiêu, phương pháp, đối tượng, phạm vi nghiên cứu, các đóng góp, ý nghĩa khoa học, thực tiễn và phần kết luận của luận án, luận án được chia thành 4 chương với bố cục như sau:

Chương 1: Tổng quan về chữ ký số và vấn đề nghiên cứu

Nội dung chương 1 trình bày các khái niệm, định nghĩa liên quan được sử dụng trong luận án và ba bài toán khó được sử dụng nhiều trong các nghiên cứu về chữ ký số và trình bày các lược đồ phổ biến, các chuẩn đang được ứng dụng trong thực tế làm cơ sở để nghiên cứu, đề xuất các lược đồ chữ ký số mới.

Chương 2: Phát triển một số lược đồ chữ ký số tập thể mù dựa trên các chuẩn chữ ký số

Nội dung chương 2 trình bày kết quả nghiên cứu mới của luận án. đó là dựa trên một số chuẩn và lược đồ chữ ký số phổ biến để đề xuất bốn lược đồ chữ ký số tập thể mù mới. Các lược đồ mới kế thừa những ưu điểm về tính an toàn và hiệu năng của các chuẩn và lược đồ phổ biến. Tính an toàn của các lược đồ đề xuất được chứng minh trong mô hình tiên tri ngẫu nhiên ROM.

Chương 3: Phát triển lược đồ chữ ký số mù và chữ ký số tập thể mù dựa trên hai bài toán khó

Nội dung chương 3 trình bày kết quả nghiên cứu mới của luận án, đó là đề xuất lược đồ chữ ký số mù, chữ ký số tập thể mù mới dựa trên hai bài toán khó IFP và DLP.

Đồng thời xây dựng lược đồ ký số mới dựa trên bài toán khó mới đề xuất. Bài toán khó mới được thiết kế trên cơ sở sử dụng các nhóm con hữu hạn không vòng hai chiều. Xây dựng lược đồ chữ ký số mù, chữ ký số tập thể mù có kích thước được rút ngắn dựa trên lược đồ ký số mới.

Chương 4: Ứng dụng lược đồ chữ ký số tập thể mù đề xuất vào lược đồ bầu cử điện tử

Nội dung chương 4 trình bày về lược đồ bầu cử điện tử sử dụng các lược đồ chữ ký số tập thể mù dựa trên lược đồ Schnorr và lược đồ chữ ký số tập thể mù dựa trên lược đồ EC-Schnorr đề xuất trong chương 2.

CHƯƠNG 1. TỔNG QUAN VỀ CHỮ KÝ SỐ VÀ VẤN ĐỀ NGHIÊN CỨU

Chương 1 trình bày một số khái niệm cơ bản về chữ ký số, lược đồ chữ ký số, vấn đề liên quan đến nghiên cứu của luận án và cơ sở toán học liên quan như: khái niệm về chữ ký số, lược đồ chữ ký số, chữ ký số mù và các dạng tấn công chữ ký số,… Ba bài toán khó là bài toán phân tích thừa số một số nguyên lớn (IFP), bài toán logarit rời rạc (DLP) và bài toán logarit rời rạc trên đường cong elliptic (ECDLP); Các lược đồ chữ ký số phổ biến và các chuẩn chữ ký số đang được ứng dụng nhiều trong thực tế như RSA, Schnorr, EC-Schnorr, GOST R34.10-94 và GOST R34.10-2012.

Đồng thời trình bày một số lược đồ chữ ký số mù, chữ ký số tập thể mù đã được công bố và được lựa chọn để so sánh với các công trình nghiên cứu được đề xuất trong luận án. Phần cuối chương trình bày hướng nghiên cứu của luận án.

1.1. TỔNG QUAN VỀ CHỮ KÝ SỐ

1.1.1. Khái niệm chữ ký số

Hiện nay có nhiều định nghĩa về chữ ký số theo khía cạnh và quan điểm nghiên cứu khác nhau. Tuy nhiên, theo Nghị Định 130/2018/NĐ-CP, ngày 27/9/2018 của Chính phủ Việt Nam, chữ ký số được định nghĩa là một loại chữ ký điện tử, được tạo bằng sự chuyển đổi thông điệp dữ liệu sử dụng một hệ thống mật mã không đối xứng, theo đó người có được thông điệp dữ liệu ban đầu và khóa công khai của người ký có thể xác định được chính xác:

+ Việc biến đổi nêu trên được tạo ra bằng đúng khóa bí mật tương ứng với khóa công khai trong cùng một cặp khóa;

+ Sự toàn vẹn nội dung của thông điệp dữ liệu kể từ khi thực hiện việc biến đổi nêu trên.

Cho đến nay, chữ ký số đã có những bước phát triển mạnh mẽ và trở thành bộ phận cấu thành quan trọng của ngành mật mã học. Hiện nay, đã có nhiều các lược đồ chữ ký số khác nhau được nghiên cứu và phát triển dựa trên các chuẩn chữ ký số và các lược đồ chữ ký số phổ biến như GOST R34.10-94, GOST R34.10-2012, RSA, Rabin, Schnorr, EC-Schnorr,... Gần 40 năm qua, dựa vào các tiêu chí khác nhau có thể chia các lược đồ chữ ký số thành nhiều loại như chữ ký số nhóm, chữ ký số tập thể, chữ ký số đại diện, chữ ký số mù,... Chữ ký số cũng đã được ứng dụng rộng rãi trong thực tiễn và đã được đưa thành chuẩn và được triển khai ở hơn 40 quốc gia trên thế giới như FIPS của Mỹ, GOST của Liên bang Nga,…

1.1.2. Lược đồ chữ ký số

Năm 1976, trong bài báo "*New Directions in Cryptography*" [23], Whitfield Diffie và Martin Hellman mô tả về một lược đồ chữ ký số, họ chỉ phỏng đoán rằng những lược đồ này tồn tại dựa trên những hàm toán học một chiều mà chưa đưa ra được lược đồ chữ ký số nào. Sau đó, năm 1978, trong công bố " *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*", R.Rivest, A.Shamir, và L.Adleman lần đầu tiên đưa ra lược đồ chữ ký số dựa trên bài toán IFP được gọi là RSA và được sử dụng cho đến ngày nay [83].

Lược đồ chữ ký số gồm ba thành phần (*Gen, Sig, Ver*) lần lược gọi là bộ sinh khóa, thuật toán ký, thuật toán xác thực. Các thành phần của lược đồ chữ ký số có thuật toán thực hiện trong thời gian đa thức, trong đó thuật toán đầu tiên là theo xác suất, thuật toán thứ hai cũng thường là theo xác suất và thuật toán thứ ba là mang tính chất khẳng định.

Với đầu vào là 1^k bộ sinh khóa sẽ cho đầu ra là cặp khóa công khai và bí mật *(pk,sk).* Để ký thông điệp *M,* tạo ra chữ ký *s* thực hiện như sau: $s \leftarrow Sig^R(sk, M)$.

Để xác thực chữ ký của *M,* thực hiện phép tính $Ver^R(pk, M, s) \in \{0,1\}$. Ở đây $Ver^R(pk, M, s) = 1$ với mọi $s \in [Sig^R(sk, M)]$. Kẻ tấn công có thuật toán *F* có khả năng truy cập tới *R* (nguồn Oracle). Đầu ra của *F* là cặp *(M,s)* sao cho *M* không phải

được truy vấn từ nguồn Oracle. Lược đồ được cho là an toàn nếu với mọi hàm F của kẻ tấn công thì hàm $\varepsilon(k)$ được định nghĩa là:

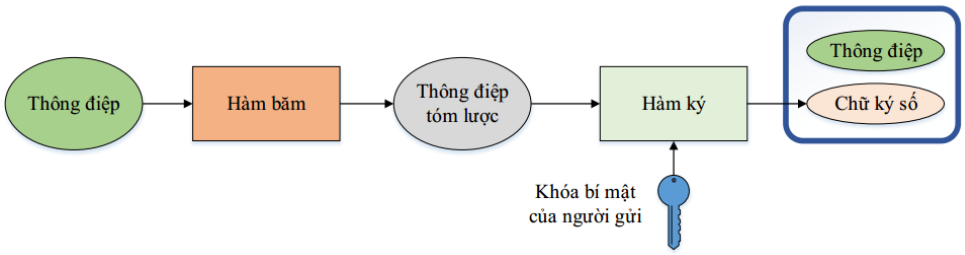
$$\varepsilon(\mathrm{k}) = \Pr[R \leftarrow 2^{\infty}; (pk, sk \leftarrow Gen(1^{k}); (M, s) \leftarrow F^{R, Sig^{R}(pk, M)}(pk) : Ver^{R}(pk, M, s) = 1]$$

là một hàm có giá trị không đáng kể. Chúng ta nói kẻ tấn công thực hiện tấn công thành công nếu có F cho ra (M,s) thỏa mãn $Ver^{R}(pk, M, s) = 1$.

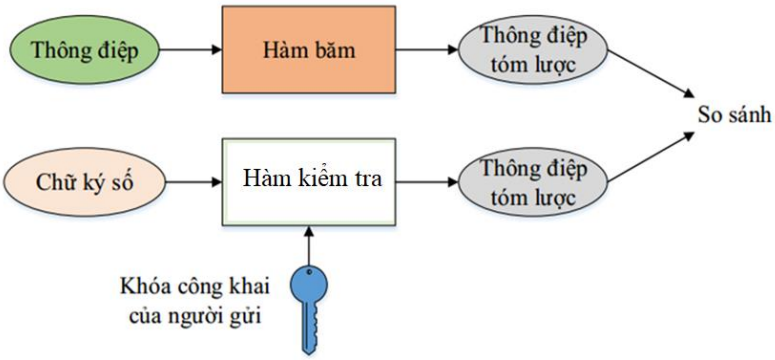
Do thông điệp cần ký thường có chiều dài khá dài nên có một biện pháp để ký là chia thông điệp ra các đoạn nhỏ và sau đó ký lên từng đoạn và ghép lại. Nhưng phương pháp này có nhược điểm là: (i) chữ ký lớn, (ii) quá trình ký bị chậm vì hàm ký là các hàm mũ, (iii) chữ ký có thể bị đảo lộn các vị trí nên không đảm bảo tính nguyên vẹn của thông điệp. Do đó, khi ký thì người ký thường không ký lên thông điệp gốc mà ký lên giá trị hàm băm của thông điệp, vì giá trị của hàm băm luôn cho chiều dài xác định.

1.1.3. Tạo và xác thực chữ ký số

Một lược đồ chung và đơn giản cho việc tạo và xác thực một chữ ký số được trình bày như trên hình 1.1 và 1.2. Một hàm băm được áp dụng cho thông điệp để tạo ra một bảng mã thông điệp có kích thước cố định.



Hình 1.1. Quy trình tạo chữ ký số



Hình 1.2. Quy trình xác thực chữ ký số

Một hình thức ký số đơn giản đó là mã hóa thông điệp sử dụng khóa riêng của người gửi. Khi đó, cả thông điệp và chữ ký số có thể được gửi cho người nhận. Thông điệp được giải mã và có thể đọc được bởi bất kỳ ai nhưng chữ ký thì đảm bảo tính xác thực của người gửi. Ở phía người nhận, một hàm nghịch đảo với hàm ký được áp dụng để khôi phục lại bản mã thông điệp ban đầu. Thông điệp nhận được cũng sẽ được đưa vào cùng hàm băm như bên gửi và tạo ra bản mã thông điệp. Việc tạo ra bản mã thông điệp được so sánh với bản mã thông điệp vừa được khôi phục từ chữ ký số. Nếu chúng giống nhau thì có thể đảm bảo rằng thông điệp đã được gửi bởi đúng người gửi và nó không hề bị thay đổi trong quá trình truyền chữ ký số và thông điệp trên mạng.

1.1.4. Chức năng của chữ ký số

1) Xác thực được nguồn gốc thông điệp: Tùy thuộc vào từng thông điệp mà có thể thêm các thông tin nhận dạng như tên tác giả, nhãn thời gian,…

2) Tính toàn vẹn của thông điệp: Khi có sự thay đổi bất kỳ vô tình hay cố ý lên thông điệp thì giá trị hàm băm sẽ bị thay đổi và kết quả kiểm tra sẽ cho kết quả không đúng hay nói rằng thông điệp không toàn vẹn.

3) Chống từ chối thông điệp: Vì chỉ có chủ thông điệp mới có khóa riêng để ký lên thông điệp nên người ký không thể chối bỏ thông điệp của mình.

1.1.5. Phân loại tấn công chữ ký số

Goldwasser trong [34] mô tả các loại tấn công chữ ký số. Ký hiệu B là người ký bị tấn công. Có hai dạng tấn công chữ ký số:.

1) Tấn công vào khóa (KOA): Kẻ tấn công chỉ biết khóa công khai.

2) Tấn công vào văn bản (MA): Tấn công dạng này là kẻ tấn công có thể kiểm tra một số chữ ký số tương ứng với các văn bản đã biết hoặc được lựa chọn… Tùy theo cách kẻ tấn công quan sát thấy hoặc lựa chọn văn bản, có thể phân loại tiếp thành 04 loại tấn công vào văn bản như sau:

i) Tấn công văn bản được biết (KMA): Kẻ tấn công có thể truy cập đến chữ ký của các văn bản $M_1, M_2, ..., M_n$ nhưng không được tự ý lựa chọn.

ii) Tấn công văn bản được lựa chọn tổng quát (GCMA): ở đây kẻ tấn công được xem là có thể truy cập được các chữ ký hợp lệ của người ký ***B*** cho danh sách văn bản được lựa chọn $M_1, M_2, ..., M_n$ trước khi cố gắng phá vỡ lược đồ chữ ký số của ***B***. các bản văn bản này được chọn bởi kẻ tấn công và không phụ thuộc vào khóa công khai của ***B*** (ví dụ M_i được chọn ngẫu nhiên). Đây là kiểu tấn công không thích ứng: toàn bộ danh sách văn bản được lập từ trước khi bất ký chữ ký nào được nhìn thấy. Tấn công dạng này được gọi là tổng quát vì không phụ thuộc vào khóa công khai của ***B***, đây là hình thức tấn công có thể thực hiện đối với bất kỳ ai.

iii) Tấn công văn bản được lựa chọn trực tiếp (DCMA): Tấn công dạng này cũng tương tự tấn công lựa chọn tổng quát, có điều khác là danh sách văn bản được tạo ra sau khi được biết khóa công khai của B nhưng danh sách đó được tạo ra trước khi quan sát được bất kỳ chữ ký nào. Đây vẫn là tấn công không thích ứng, và cũng chỉ tấn công được với người ký B nào đó mà không phải là tất cả.

iv) Tấn công văn bản được lựa chọn thích ứng (ACMA): Kẻ tấn công có thể sử dụng B như là nguồn Oracle. Văn bản được chọn không chỉ sau khi được biết khóa công khai của B mà còn cả sau khi quan sát được các chữ ký được tạo ra trước đó.

Cả bốn loại tấn công văn bản được liệt kê theo mức độ tăng dần của tính nghiêm trọng. Các lược đồ chữ ký số khi đưa ra công khai phải chịu được tấn công văn bản lựa chọn thích ứng.

1.1.6. Các dạng phá vỡ lược đồ chữ ký số

Goldwasser trong [34] mô tả đầy đủ các dạng phá vỡ lược đồ chữ ký số. Khi nói rằng kẻ tấn công phá vỡ được lược đồ chữ ký số của B thì có nghĩa là cuộc tấn công có thể thực hiện được với một xác suất không phải là hàm không đáng kể $\varepsilon(k)$, với k là tham số về tính an toàn của hệ thống.

1) Phá vỡ hoàn toàn (TB): Khi kẻ tấn công biết được thông tin bí mật (cửa sập) của người ký B.

2) Giả mạo tổng quát (UF): Kẻ tấn công có thể tìm được thuật toán ký số có chức năng tương đương thuật toán ký của người ký B (có thể dựa trên thông tin cửa sập khác nhưng tương đương cửa sập của người ký B).

3) Giả mạo có lựa chọn (SF): Kẻ tấn công có thể tìm được chữ ký của thông điệp cụ thể được lựa chọn có ưu tiên theo cách của kẻ tấn công.

4) Giả mạo có tồn tại (EF): Giả mạo được chữ ký của ít nhất một văn bản. Kẻ tấn công có thể không kiểm soát toàn bộ quá trình sinh ra chữ ký, nhưng có thể tạo ra chữ ký một cách ngẫu nhiên không chủ định trước.

Các dạng tấn công và phá vỡ lược đồ chữ ký số được trình bày ở trên về cơ bản được áp dụng cho tất cả các lược đồ chữ ký số, tuy nhiên có những loại hình tấn công và phá vỡ lược đồ chữ ký theo đặc thù của từng loại lược đồ ký số.

1.2. CHỮ KÝ SỐ TẬP THỂ

Thực tế hiện nay, nhiều khi một thực thể ký (con người, thiết bị kỹ thuật,...) là thành viên hay bộ phận của một tổ chức (đơn vị hành chính, hệ thống kỹ thuật,...) và thông điệp dữ liệu (bản tin, thông báo, tài liệu,...) được thực thể ký tạo ra với tư cách là một thành viên hay bộ phận của tổ chức đó. Vấn đề ở đây là, thông tin cần

phải được chứng thực về nguồn gốc và tính toàn vẹn ở hai cấp độ: cấp độ cá nhân thực thể ký và cấp độ tổ chức mà thực thể ký là thành viên hay bộ phận của nó. Các mô hình ứng dụng chữ ký số đơn mới chỉ đảm bảo tốt cho nhu cầu chứng thực thông tin ở cấp độ cá nhân, còn việc chứng thực đồng thời ở cả hai cấp độ như thế vẫn chưa đáp ứng. Do đó, mô hình chữ ký số tập thể nhằm đáp ứng cho các yêu cầu chứng thực thông tin ở nhiều cấp độ khác nhau đang được quan tâm nghiên cứu và ứng dụng.

Chữ ký số tập thể dựa trên RSA lần đầu tiên được K.Nakamura và K.Itakura [75] đưa ra vào năm 1983. Lược đồ chữ ký số tập thể cho phép nhiều người tham gia ký văn bản và người xác thực có thể xác thực đối với từng thành viên trong tập thể người ký đó. Cách đơn giản nhất để tạo nên chữ ký số tập thể là ghép tất cả các chữ ký số đơn của các thành viên với nhau. Tuy nhiên với cách như vậy thì độ dài của chữ ký và độ phức tạp tính toán tăng tỷ lệ với số lượng người ký.

Trải qua hơn 35 năm phát triển, chữ ký số tập thể ngày càng có nhiều ứng dụng thực tiễn trong thương mại điện tử và Chính phủ điện tử. Ví dụ, chính sách phân chia chức năng, nhiệm vụ quyền hạn trong nội bộ một cơ quan, mỗi bộ phận có một người quản lý, những người này phải hợp tác với nhau. Lược đồ chữ ký số tập thể cho phép việc phân chia chức năng, quyền hạn của các bộ phận trong nội bộ của cơ quan một cách có hiệu quả. Mỗi người quản lý có một khoá bí mật riêng của mình sử dụng để ký vào thông điệp.

Các thành phần của lược đồ chữ ký số tập thể:

1) Giao thức sinh khóa: Giao thức này thường được thực hiện một lần ban đầu cho tất cả các thành viên trong tập thể người ký. Mỗi thành viên nhận được như đầu vào thông tin về nhóm **U**, đó là danh sách và định danh của các thành viên trong tập thể người ký. Giao thức sinh khóa sẽ sinh cho mỗi thành viên một cặp khóa bí mật và khóa công khai tương ứng (sk_i, pk_i).

2) Thuật toán ký tập thể: Các thành viên trong tập thể người ký tham gia ký, kết quả là chữ ký tập thể có thể được đưa ra bởi một trong các thành viên đó hoặc bên thứ ba tin cậy TTP.

3) Thuật toán kiểm tra chữ ký: Thuật toán này có thể thực hiện bởi một người khác (không nằm trong nhóm **U**), đầu vào là thông tin về **U**, thông điệp *M* và chữ ký số tập thể. Thuật toán cho đầu ra là "ĐÚNG" hoặc "SAI".

Các thuộc tính cơ bản của chữ ký số tập thể:

1) Độ dài của chữ ký số tập thể là không thay đổi, bằng độ dài chữ ký số riêng lẻ của từng người ký.

2) Chữ ký số tập thể có thể được kiểm tra theo phương thức thông thường như chữ ký số đơn thay vì phải kiểm tra tất cả các chữ ký số riêng lẻ.

3) Khoá công khai của lược đồ chữ ký số tập thể được tạo ra bởi sự kết hợp của tất cả các khoá công khai riêng lẻ.

4) Giả sử có *n* thành viên tham gia ký vào một văn bản. Khi đó $n - 1$ thành viên không thể ký thay cho người còn lại.

Thuộc tính (1) tối thiểu hoá chi phí bộ nhớ dành cho việc lưu trữ chữ ký số tập thể trong truyền thông. Thuộc tính (2) tăng tốc độ của quá trình kiểm tra chữ ký. Thuộc tính (3) giảm tài nguyên của thư mục hoặc ổ đĩa dùng để lưu trữ khoá công khai vì chỉ cần lưu trữ khoá công khai của mỗi người là đủ.

1.3. CHỮ KÝ SỐ MÙ

Chaum đưa ra khái niệm chữ ký số mù đầu tiên vào năm 1983 [13], cho phép khách hàng mua hàng nặc danh trong các hệ thống thương mại điện tử. Trong chữ ký này, người ký văn bản nhưng lại không được biết nội dung văn bản đó, và không thể xác định được mình đã ký văn bản đó khi nào, cho ai (*mặc dù người ký có thể xác thực được chữ ký đó*). Câu hỏi đặt ra là tại sao người ký lại không được biết nội dung văn bản mà mình ký? nhưng quan niệm này lại rất hữu ích trong các vấn đề đòi hỏi sự nặc danh, như là bỏ phiếu trực tuyến hay thương mại điện tử. Khi tham

gia bỏ phiếu trực tuyến, không ai biết rằng cử tri đã bỏ phiếu cho ai. Tương tự với lĩnh vực thương mại điện tử, có thể người mua hàng không muốn ai đó biết mình là ai khi mua một món hàng nào đó. Khi các đồng tiền điện tử đã được ký mù thì người mua hàng có thể mua hàng nặc danh.

Theo như Chaum trình bày thì lược đồ chữ ký số mù là một loại lược đồ mà người yêu cầu nhận một chữ ký $Sig(M)$ cho thông điệp *M* của mình từ một người ký, người này chỉ có nhiệm vụ ký mà không biết thông tin gì về thông điệp. Sau này, khi người ký nhận được cặp thông điệp – chữ ký $(M, Sig(M))$, người ký chỉ có thể xác thực là chữ ký đó có đúng hay không mà không thể tìm ra mối liên kết giữa cặp thông điệp – chữ ký với trường hợp xác định của lược đồ ký số đã được sử dụng để sinh ra chữ ký đó. Như vậy, lược đồ chữ ký số mù được xem như là hệ thống chữ ký số hai khóa kết hợp với một hệ thống khóa công khai kiểu giao hoán, đó là:

+ Hàm ký Sig chỉ được biết bởi người ký và hàm nghịch đảo Sig' tương ứng được công khai, theo đó $Sig'(Sig(M)) = M$ và Sig' không mang một manh mối nào cho việc tìm ra Sig.

+ Hàm giao hoán f và nghịch đảo f' của nó chỉ được biết đến bởi người yêu cầu, theo đó $f'(Sig(f(M))) = Sig(M)$, $f(m)$ và *s* không đưa ra manh mối nào cho việc tìm ra *M*.

Dựa trên các hàm này, một lược đồ chữ ký số mù bao gồm 4 pha:

+ Pha làm mù: Người yêu cầu làm mù thông điệp để người ký không thể nhìn thấy nội dung thật sự của thông điệp bằng cách nhân thông điệp với một số ngẫu nhiên hay mã hóa nó với một vài khóa hoặc cũng có thể sử dụng hàm băm để băm thông điệp: Người yêu cầu chọn thông điệp *M* một cách ngẫu nhiên, tính $f(M)$ và gửi nó cho người ký.

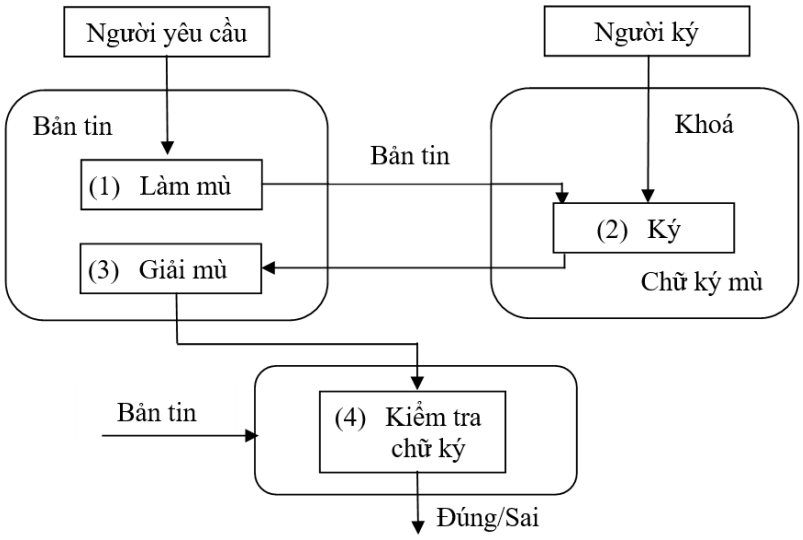
+ Pha ký số: Kế tiếp, người ký sẽ ký vào thông điệp mặc dù không biết nội dung thật sự của thông điệp. Người ký sẽ ký mù lên thông điệp đã được gửi đến bởi người yêu cầu: Người ký sẽ ký trên $f(M)$ bằng cách sử dụng hàm *Sig* và trả về

thông điệp đã được ký $Sig(f(M))$ cho người yêu cầu.

+ Pha giải mù: Kế đến, người yêu cầu tiến hành giải mù thông điệp có chữ ký của người ký gửi tới bằng cách áp dụng f' để bóc tách $Sig(f(M))$ và thu được $f'(Sig(f(M))) = Sig(M)$.

+ Pha xác thực: Người xác thực nhận được chữ ký và xác thực chữ ký đó bằng cách kiểm tra theo biểu thức xác thực: Bất kỳ ai cũng có thể kiểm tra thông tin đã được bóc tách $Sig(M)$ bằng cách áp dụng hàm nghịch đảo công khai Sig' của người ký và kiểm tra xem biểu thức $Sig'(Sig(M)) = M$ có thỏa mãn hay không.

Hình 1.3 mô tả tóm tắt về luồng cấu trúc của chữ ký số mù với hai bên tham gia là người yêu cầu và người ký, các thành phần khác không thể hiện trong hình này.



Hình 1.3. Luồng cấu trúc chữ ký số mù

Các thuộc tính của chữ ký số mù: Chữ ký số mù là một loại chữ ký số đặc biệt, vì vậy chữ ký số mù thừa hưởng tất cả các thuộc tính chung của chữ ký số nói chung, ngoài ra chữ ký số mù còn có thêm các thuộc tính đặc trưng riêng như sau:

1) Tính mù: Nội dung thông điệp bị làm mù đối với người ký.

2) Tính không truy vết: Người ký không thể truy lại mối quan hệ giữa chữ ký và thông điệp, ngay cả khi chữ ký đã được công bố công khai.

3) Tính chống giả mạo: Với bất kỳ thuật toán hiệu năng cao trong thời gian đa thức nào của kẻ tấn công thì xác suất giả mạo chữ ký thành công là vô cùng bé.

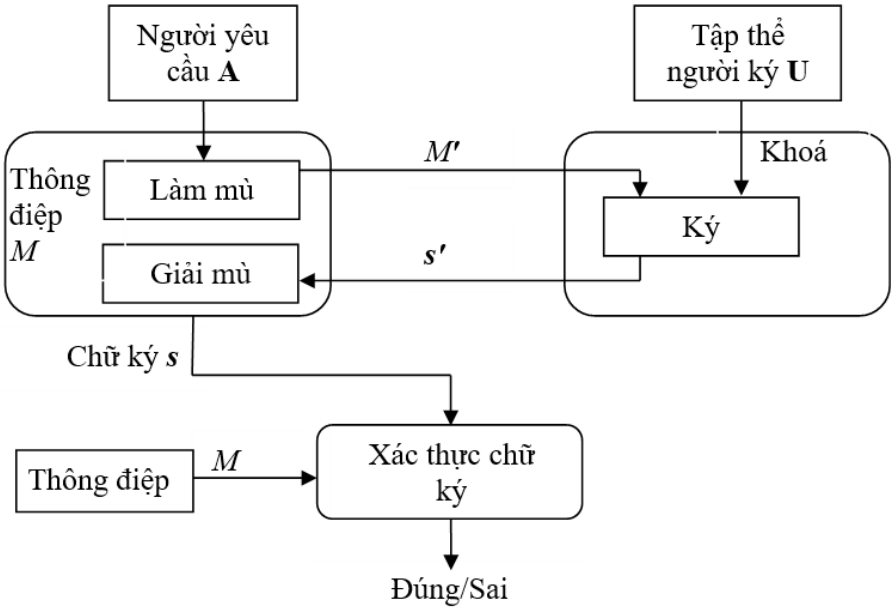
Các thuộc tính này có thể được sử dụng trong các ứng dụng trên mạng cần bảo vệ tính riêng tư của khách hàng,…

1.4. CHỮ KÝ SỐ TẬP THỂ MÙ

Lược đồ chữ ký số tập thể mù cho phép nhiều người ký trên cùng một thông điệp đã được làm mù. Trong lược đồ chữ ký số tập thể mù, người yêu cầu **A** là người muốn nhận một chữ ký số từ nhiều người ký, do vậy mỗi người ký sẽ không biết mối quan hệ giữa thông điệp đã bị làm mù, thông điệp chưa bị làm mù và các tham số của chữ ký. Điều này có nghĩa là họ không thể nhận dạng được chữ ký về sau này, ngay cả khi họ thỏa hiệp lại với nhau.

Một giải pháp đơn giản cho lược đồ chữ ký số tập thể mù đó là mỗi người ký sẽ ký thông điệp sử dụng lược đồ chữ ký số thông thường. Phương pháp này có một nhược điểm là dữ liệu bị lớn lên theo số lượng người ký. Năm 1995, Horster và các cộng sự công bố trong [42] là công trình đầu tiên về chữ ký số tập thể mù được đề xuất cho việc sử dụng trong bầu cử điện tử sử dụng hệ mật dựa trên bài toán logarit rời rạc.

Tiến trình của một chữ ký số tập thể mù được mô tả như trong hình 1.5 gồm có hai thành phần chính là người yêu cầu và tập thể người ký, các thành phần trung gian khác không thể hiện trong hình này. Trong đó, người yêu cầu **A** cần tập thể **U** ký cho thông điệp *M*, **A** không đưa *M* cho **U** ký mà làm "mù" *M* thành M'. Sau đó A đưa M' cho **U** ký. Sau khi nhận được chữ ký trên M', **A** xóa mù để thu được chữ ký trên *M*. Như vậy **A** vẫn có chữ ký của **U** trên *M* mà **U** không biết thông tin gì về *M*.



Hình 1.4. Tiến trình của chữ ký số tập thể mù

Tính an toàn của lược đồ chữ ký số tập thể mù:

Tính an toàn của lược đồ chữ ký số tập thể mù được xác định thông qua tính mù và tính chống giả mạo [21], [25].

Tính mù: nghĩa là với bất kỳ thuật toán hiệu năng cao trong thời gian đa thức nào của kẻ tấn công có vai trò như người ký thì xác suất có thể biết được nội dung bản tin *M*, đồng thời có thể liên kết các bản tin để biết được thông tin người yêu cầu là vô cùng bé.

Tính chống giả mạo: Với bất kỳ thuật toán hiệu năng cao trong thời gian đa thức nào của kẻ tấn công thì xác suất giả mạo chữ ký thành công là vô cùng bé.

Có thể mô phỏng việc chống giả mạo như sau: Một kẻ tấn công với thuật toán hiệu năng cao cố gắng giả mạo bằng cách sinh ra $\lambda+1$ cặp giá trị hợp lệ của thông điệp và chữ ký với các thông điệp khác nhau sau λ lần tương tác với người ký hợp pháp, khi đó $\lambda+1$ cặp có thể xác định phù hợp bởi kẻ tấn công trong thời gian tấn công. Để xác định phiên hoàn thành, giả định rằng người ký hợp pháp trả về ký hiệu là *"Đúng"* khi giao thức cuối cùng được thực hiện để hoàn tất chữ ký.

Định nghĩa 1.1 (Tính mù) [21]: Với mọi thuật toán thời gian đa thức của kẻ tấn công B đóng vai trò như người ký thì xác suất thành công của thực nghiệm dưới đây là một hàm vô cùng nhỏ.

- Gọi (U_0, U_1) là 2 người yêu cầu tin cậy, (U_0, U_1) tham gia lược đồ chữ ký số tập thể mù với B trên thông điệp (M_{1-b}, M_b) và đầu ra là chữ ký (s_{1-b}, s_b) tương ứng với $b \in \{0,1\}$ được chọn ngẫu nhiên.

- Gửi ($M_{1-b}, M_b, s_{1-b}, s_b$) đến B và B cho đầu ra là $b' \in \{0,1\}$. Với tất cả B, U_0, U_1 và một hằng số c bất kỳ và một số nguyên tố p đủ lớn thì xác suất thành công của thực nghiệm là nhỏ không đáng kể: $|\Pr[b = b'] - \frac{1}{2}| < \frac{1}{p^c}$.

Định nghĩa 1.2 (Tính chống giả mạo) [21], [49]: Một kẻ tấn công **B** với thuật toán xác định có được bộ $(\varepsilon, t, q_h, q_e, q_s)$ gọi là giả mạo. Nếu trong khoảng thời gian t nó có thể hoàn thành các truy vấn (q_h, q_e, q_s) với khả năng ít nhất là ε, trong đó (q_h, q_e, q_s) lần lượt là số truy vấn của hàm băm, trích xuất và ký.

Một lược đồ $(\varepsilon, t, q_h, q_e, q_s)$ được gọi là an toàn với kẻ tấn công **B** theo cách là không thể giả mạo chống lại dạng tấn công thông điệp đã được lựa chọn nếu kẻ giả mạo $(\varepsilon, t, q_h, q_e, q_s)$ không tồn tại.

Công trình [49] chứng minh tính chất chống giả mạo của lược đồ chữ ký số dựa trên bài toán DLP, còn công trình [21] thì dựa vào công trình [49] để chứng minh tính chất chống giả mạo của lược đồ chữ ký số đối với bài toán ECDLP.

Theo Liu trong công trình [49], một lược đồ chữ ký số chống được giả mạo chữ ký phải thỏa mãn tính chất sau:

Tính chất: Lược đồ chữ ký số có bộ tham số $(\varepsilon, t, q_h, q_e, q_s)$ gọi là an toàn trong ROM nếu tồn tại (ε', t') -DL trong G, với:

$$\varepsilon' = (1 - \frac{q_h(q_e + q_s)}{q})(1 - \frac{1}{q})(\frac{1}{q_h})\varepsilon; \quad t' = t + O(q_e + q_s)E$$

Trong đó, (q_h, q_e, q_s) lần lượt là số truy vấn của hàm băm, trích xuất và tạo chữ ký mù; E là thời gian thực hiện các phép tính luỹ thừa modulo.

Chứng minh: Giả sử tồn tại một kẻ giả mạo **A**, xây dựng thuật toán **B** để giúp **A** giải bài toán DLP. **B** có nhóm nhân *G* với phần tử sinh *g* và có bậc *q*, và $\rho \in G$, B được yêu cầu phải tìm $\alpha \in Z_q$ sao cho $\rho = g^{\alpha}$. Chứng minh như sau:

Thiết lập: **B** chọn hàm băm thông điệp $H : \{0,1\}^* \rightarrow Z_q$ cư xử như là một tiên tri ngẫu nhiên. **B** có trách nhiệm mô phỏng như nhà tiên tri ngẫu nhiên này. **B** $X \leftarrow \rho$ và gửi tham số công khai $(G, q, g, \mathrm{X}, \mathrm{H})$ tới **A**.

Trích xuất Oracle: **A** được phép truy vấn tới phần truy xuất oracle để có một *ID*. **B** mô phỏng oracle như sau: Chọn hai số *a,b* ngẫu nhiên, với $(a,b) \in Z_q$ và thiết lập: $R \leftarrow X^a g^b; s \leftarrow b; H(R, ID) \leftarrow (-a)$, với (R, s) là khóa bí mật tương ứng với *ID* và lưu trữ bộ $(R, s, H(R, ID, ID)$ trong bảng dữ liệu.

Ký Oracle: **A** truy vấn tới phần ký oracle của thông điệp *m* và số định danh *ID*. Đầu tiên, **B** kiểm tra xem *ID* đã được truy vấn tiên tri ngẫu nhiêu *H* hay đã được trích xuất oracle trước chưa. Nếu có, **B** khôi phục $(R, s, H(R, ID, ID)$ từ bảng và sử dụng các giá trị này để ký thông điệp theo thuật toán ký được mô tả trong lược đồ. Đầu ra là chữ ký (Y, R, z) của thông điệp *m* và lưu $H(Y, R, m)$ trong bảng hàm băm. Nếu *ID* chưa được truy vấn thì **B** thực hiện lại mô phỏng phần trích xuất oracle và sử dụng khóa bí mật tương ứng để ký thông điệp.

Tính toán kết quả: Cuối cùng, **A** tạo ra chữ ký số giả mạo là $\sigma^*_{(1)} = (Y^*, R^*, z^*_{(1)})$ trên *m* bởi khoá bí mật ID^*. **B** thực hiện lại phần truy vấn tới $H(Y^*, R^*, m^*)$ và cung cấp với giá trị khác, **A** cho ra chữ ký khác là $\sigma^*_{(2)} = (Y^*, R^*, z^*_{(2)})$. **B** lặp lại lần nữa và thu được $\sigma^*_{(3)} = (Y^*, R^*, z^*_{(3)})$, trong đó (Y^*, R^*) là giống nhau cho các lần truy vấn. Gọi (c_1, c_2, c_3) là đầu ra của truy vấn tiên tri ngẫu nhiên $H(Y^*, R^*, m^*)$ cho các lần một, hai và ba.

Với $(x, y, z) \in Z_q$, bây giờ việc biểu thị logarit rời rạc của (R, X, Y) tương ứng là: $g^r = R; g^x = X; g^y = Y$. Từ phương trình kiểm tra $g^z = YR^h X^{hH(R,ID)}$, tính được:

$$z_{(i)}^* = y + rc_i + xc_i H(R^*, ID) \bmod q, i = 1,2,3$$

Trong các phương trình đó, **B** không biết (x, y, z), **B** phải giải các phương trình tuyến tính độc lập ở trên để tìm *x* hay phải giải bài toán DLP.

Phân tích xác suất: Việc mô phỏng trích xuất oracle lỗi nếu phép gán ngẫu nhiên $H(R, ID)$ gây ra sự không nhất quán, xảy ra với xác suất lớn nhất là $\frac{q_h}{q}$. Do đó việc mô phỏng thành công trong $(q_e + q_s)$ lần (*vì* $H(R, ID)$ *cũng có thể được truy vấn trong phần ký oracle, nếu ID chưa được truy vấn trong phần trích xuất oracle*) với xác suất ít nhất là:

$$(1 - \frac{q_h}{q})^{q_e + q_s} \geq 1 - \frac{q_h(q_e + q_s)}{q}.$$

Do tính ngẫu nhiên lý tưởng của mô hình ROM nên tồn tại truy vấn $H(Y^*, R^*, m^*)$ với xác suất ít nhất là $(1 - \frac{1}{q})$. **B** đoán đúng điểm quay lại phần truy vấn với xác suất là ít nhất là $1/q_h$. Vì vậy mà xác suất thành công chung là $\varepsilon' = (1 - \frac{q_h(q_e + q_s)}{q})(1 - \frac{1}{q})\frac{1}{q_h}\varepsilon$, và độ phức tạp về thời gian của thuật toán B dựa trên hàm mũ được thực hiện chủ yếu trong pha trích xuất và pha ký, và là $t' = t + O(q_e + q_s)E$.

1.5. MÔ HÌNH ĐÁNH GIÁ TÍNH AN TOÀN CỦA LƯỢC ĐỒ CHỮ KÝ SỐ - MÔ HÌNH TIÊN TRI NGẪU NHIÊN (ROM)

Bài toán trong các hệ mật (giả sử bài toán RSA) được coi là không tồn tại thuật toán hiệu quả thời gian đa thức. Cho nên để khẳng định một lược đồ ký số là an toàn, người ta thường chứng minh rằng khả năng giả mạo nó là khó tương đương

với độ khó của bài toán khó tương ứng. Tức là nếu như lược đồ ký số RSA bị tấn công thành công thì sẽ giải được bài toán RSA. Người ta giả sử lược đồ bị tấn công theo cấp độ mạnh nhất (cấp độ 4), nhưng chỉ cần thu được thành công thấp nhất (*có nghĩa là chỉ cần tìm được chữ ký giả mạo*) thì lược đồ ký số đã bị coi là không an toàn.

Để có được mô hình mà lược đồ có thể bị tấn công theo cấp độ 4, năm 1993 Phillip Rogaway và Mathir Bellare đề xuất ra mô hình tiên tri ngẫu nhiên ROM [9]. Trong ROM chỉ có một khác biệt duy nhất so với phương pháp thông thường đó là hàm băm được sử dụng trong quá trình mã hoá (Encoding) là hàm có giá trị được lấy ngẫu nhiên. Khi đó các mã băm sẽ phân bố đều trên toàn miền giá trị của nó. Có thể mô tả cách thức lấy mã băm của các hàm băm trong ROM như sau: Khi lần đầu lấy mã băm của thông điệp, hàm băm sẽ lấy ngẫu nhiên một giá trị trong miền giá trị và coi đó là mã băm. Ngoài ra, hàm băm phải có cách thức "ghi nhớ" để về sau nếu lại yêu cầu lấy mã băm của *M* thì hàm băm sẽ đưa lại mã băm đã lấy trước đó. Như vậy trong mô hình ROM và với các lược đồ ký dựa trên RSA, người ta có quyền lấy mã băm và chữ ký của bất kỳ thông điệp nào mà họ muốn. Và việc lấy các giá trị đó được thực hiện như các lời tiên tri (Oracle). Khi ấy, việc một lược đồ được coi là không an toàn nếu người tấn công có thể giả mạo chữ ký nào đó mà chưa từng được lấy chữ ký.

Mô hình ROM là công cụ mạnh được sử dụng để chứng minh tính an toàn một cách nghiêm ngặt cho các giao thức mã hoá cơ sở xác định. Điển hình là hàm băm được chứng minh theo mô hình ROM.

1.6. CƠ SỞ TOÁN HỌC ỨNG DỤNG TRONG CÁC LƯỢC ĐỒ CHỮ KÝ SỐ

1.6.1. Bài toán phân tích thừa số một số nguyên lớn (IFP)

Định nghĩa bài toán [49], [87]: Bài toán phân tích thừa số của một số nguyên được phát biểu như sau: cho một hợp số n được tạo bởi hai số nguyên tố lớn p và q, hãy tìm giá trị của p và q.

Trong khi việc tìm các số nguyên tố lớn là một nhiệm vụ khá dễ dàng, thì bài toán phân tích thừa số của các số như vậy được xem như là không thể tính toán được nếu như các số nguyên tố được lựa chọn một cách cẩn thận. Dựa trên độ khó của bài toán này, Rivest, Shamir và Adleman đã phát triển hệ mật khóa công khai RSA [83]. Một hệ mật khóa công khai khác sở hữu khả năng bảo mật dựa trên tính không thể giải của bài toán IFP đó là Rabin [80] và Williams [105].

Hiện tại, các thuật toán phân tích thừa số nguyên tố có thể giải bài toán với số nguyên dương có khoảng 130 chữ số thập phân. Mã hóa RSA được xây dựng trên cơ sở độ khó của bài toán phân tích thừa số nguyên tố.

Các hình thức tấn công trong bài toán IFP:

Về cơ bản, có hai dạng thuật toán phân tích thừa số là các thuật toán chuyên dụng và các thuật toán đa dụng. Các thuật toán chuyên dụng cố gắng khai thác các thuộc tính đặc biệt của số nguyên *n* đang được phân tích. Ngược lại, thời gian thực hiện của các thuật toán đa dụng chỉ phụ thuộc vào kích thước của số nguyên *n.*

Chỉ trước khi phát triển hệ mật RSA, thuật toán phân tích thừa số đa dụng tốt nhất là thuật toán chia liên tiếp, thuật toán này có thể phân tích các số đến 40 chữ số thập phân (133 bit). Thuật toán này dựa trên ý tưởng sử dụng thừa số cơ sở của các số nguyên tố và tạo một tập các phương trình tuyến tính liên kết với nhau mà nghiệm cuối cùng của nó dẫn tới việc phân tích ra các thừa số. Thuật toán này có cùng ý tưởng chính như các thuật toán đa dụng đã được sử dụng ngày nay: Thuật toán sàng bậc hai (quadratic sieve – QS) và sàng trường số (number field sieve – NFS). Cả hai thuật toán này có thể được tiến hành song song để cho phép thực hiện việc phân tích thừa số trên mạng phân tán. Vì vậy các máy tính lớn (mainframe) hay các siêu máy tính không còn là yếu tố nòng cốt quyết định đến việc giải bài toán phân tích các số nguyên lớn.

1.6.2. Bài toán logarit rời rạc (DLP)

Định nghĩa bài toán [87]: Nếu *p* là một số nguyên tố, thì $\mathbb{Z}_p$ là ký hiệu của tập

các số nguyên $\{0,1,2,...,p-1\}$, ở đây phép cộng và phép nhân được thực hiện qua phép modulo *p*. Khi đó rõ ràng tồn tại một phần tử $g \in \mathbb{Z}_p \neq 0$ sao cho mỗi phần tử khác 0 trong $\mathbb{Z}_p$ có thể được viết dưới dạng lũy thừa của *g*. Phần tử *g* như vậy được gọi là phần tử sinh của $\mathbb{Z}_p$.

Bài toán DLP được phát biểu như sau: cho một số nguyên tố *p*, một phần tử sinh *g* của $\mathbb{Z}_p^*$ và một phần tử $\beta \in \mathbb{Z}_p^*$, $\beta \neq 0$, tìm số nguyên duy nhất *l* sao cho $0 \leq l \leq p-2$ và $\beta \equiv g^l \bmod p$. Số nguyên *l* được gọi là logarit rời rạc của β cơ số *g*.

Một cách phát biểu khác: Cho *p* là một số nguyên tố và là phần tử sinh *g* của nhóm $\mathbb{Z}_p^*$, khi đó bài toán logarit rời rạc trên trường $\mathbb{Z}_p$ hay còn gọi là bài toán $DLP_{(p,g)}$ được phát biểu như sau: Với mỗi số nguyên dương $y \in \mathbb{Z}_p^*$, hãy tìm *x* thỏa mãn phương trình $g^x \bmod p = y$.

Trong một hệ thống giao dịch điện tử ứng dụng chứng thực số để xác thực nguồn gốc và tính toàn vẹn thông tin cho các thông điệp dữ liệu, bài toán $DLP_{(p,g)}$ là khó theo nghĩa không thể thực hiện được trong thời gian thực. Ở đó, mỗi thành viên của hệ thống tự chọn cho mình khóa bí mật *x* thỏa mãn $1 < x < p-1$, tính và công khai tham số $y = g^x \bmod p$.

Trong hơn 40 năm qua, DLP đã được các nhà toán học nghiên cứu một cách rộng rãi. Hiện nay, bài toán DLP vẫn được xem là khó do chưa có giải thuật thời gian đa thức giải được, do vậy mà có nhiều lược đồ chữ ký số được xây dựng dựa trên bài toán này.

Các hình thức tấn công trong bài toán DLP:

Giống như với bài toán phân tích số nguyên, có hai loại thuật toán để giải bài toán logarit rời rạc. Các thuật toán chuyên dụng cố gắng khai thác các thuộc tính đặc biệt của số nguyên tố *p*. Ngược lại, thời gian thực hiện của các thuật toán đa dụng chỉ phụ thuộc vào kích thước của giá trị *p*.

Các thuật toán đa dụng nhanh nhất đã được biết đến để giải bài toán DLP dựa trên một phương pháp gọi là index–calculus. Theo phương pháp này, một cơ sở dữ liệu các số nguyên tố và logarit tương ứng của nó được xây dựng sẵn, sau đó có thể dễ dàng tìm được logarit của các phần tử của một trường bất kỳ. Điều này giống như phương pháp thừa số cơ sở (factor base) cho bài toán phân tích một số nguyên lớn. Vì nguyên nhân này mà nếu có những cải tiến trong các thuật toán hoặc IFP hoặc DLP được tìm thấy, thì gần như ngay lập tức sau đó có thể mong chờ một cải tiến tương tự được tìm thấy trong thuật toán còn lại. Như với các phương pháp phân tích thừa số, các thuật toán index–calculus có thể dễ dàng được thực hiện theo phương thức song song.

1.6.3. Bài toán logarit rời rạc trên đường cong elliptic (ECDLP)

Trong vài thập kỷ gần đây, đường cong elliptic đóng vai trò quan trọng đối với lý thuyết số và mật mã. Mật mã đường cong elliptic (ECC) được giới thiệu lần đầu vào năm 1991 bởi các công trình nghiên cứu độc lập của Neals Koblitz và Victor Miller [53], [68]. Tính an toàn của ECC dựa vào bài toán logarit rời rạc trên nhóm các điểm của đường cong elliptic.

Mật mã ECC có độ dài khoá nhỏ hơn nhiều lần trong khi vẫn đảm bảo an toàn tương đương với các hệ mật khóa công khai truyền thống. Điều đó có nghĩa là việc cài đặt ECC sử dụng tài nguyên hệ thống ít hơn, năng lượng tiêu thụ nhỏ hơn... Với ưu thế về độ dài khóa nhỏ, ECC được ứng dụng rộng rãi trong nhiều lĩnh vực.

Đường cong elliptic (EC) trong luận án nghiên cứu dưới dạng sau:

$$y^2 = x^3 + ax + b \bmod p$$

Trong đó *a, b* là các hằng số, giá trị *x, y, a, b* thuộc trường $\mathbb{Z}_p$ và

$$4a^3 + 27b^2 \neq 0 \bmod p$$

Ngoài ra EC có thể được xác định bằng *J(E)* với:

$$J(E) = 1728\frac{4a^3}{4a^3 + 27b^2} \bmod p$$

Các hằng số *a, b* có thể được xác định dựa vào *J(E)* như sau:

$$a = 2k \bmod p; b = 3k \bmod p$$

Với $k = \frac{J(E)}{1728 - J(E)} \bmod p; J(E) \neq 0; J(E) \neq 1728$

Một số ký hiệu sử dụng cho bài toán trên đường cong elliptic sử dụng trong luận án này là: *p* là một số nguyên tố lớn tạo trường *GF(p)* của đường cong elliptic (EC); *m* là nhóm điểm của EC thỏa mãn: $p+1-2\sqrt{p} \le m \le p+1+2\sqrt{p}$; *q* là một số nguyên tố chỉ số lượng nhóm con của EC và được xác định như sau: *m=nq*; *G* là điểm khác gốc *O* của EC với toạ độ (x_G, y_G) thỏa mãn: $q \times G \equiv O \bmod p$; *g* là phần tử sinh thuộc $\mathbb{Z}_p^*$ thỏa mãn $g^q \bmod p \equiv 1 \bmod p$; *H(M)* là giá trị hàm băm thông điệp *M*; *d* là khóa riêng của người sử dụng, với $1 < d < q$;

Định nghĩa bài toán [53], [68]: Nếu *q* có số mũ là một số nguyên tố, thì F_q ký hiệu cho trường hữu hạn chứa *q* phần tử. Trong các ứng dụng, cụ thể *q* là lũy thừa của 2 (2^m) hoặc là một số nguyên tố lẻ *p*.

Bài toán ECDLP được phát biểu như sau [53], [68]: Cho đường cong *EC* trên trường hữu hạn *GF(p)*, điểm $G \in E(GF(p))$ với bậc *n* ($n \times G \equiv O \equiv \infty$) và điểm $P \in E(GF(p))$, tìm số nguyên $k \in [0, n-1]$ sao cho $P = k \times G$. Số nguyên *k* được gọi là logarithm rời rạc của *P* với cơ sở *G* và thường viết tắt là $k = \log_G P$.

Dựa trên độ khó của bài toán này, vào năm 1985, Koblitz [53] và Miller [68] đã đưa ra các đề xuất sử dụng nhóm các điểm trên đường cong elliptic được xác định trên một trường hữu hạn để thực hiện rất nhiều các hệ mật DLP. Một giao thức mật mã như vậy hiện đang được chuẩn hóa là DSA trên đường cong elliptic, được gọi là ECDSA.

Các hình thức tấn công trong bài toán ECDLP:

Bất kỳ một hệ mật khóa công khai nào cũng phải sử dụng một bài toán khó để xây dựng hàm một chiều. Ý nghĩa một chiều ở đây có nghĩa là tính thuận thì dễ (*thuật toán giải trong thời gian đa thức*) và tính ngược thì khó (*thuật toán giải với thời gian không phải là đa thức - thường là hàm mũ*). Các tham số của hệ mật ECC cần phải được lựa chọn cẩn thận để tránh được các tấn công đối với bài toán ECDLP. Thuật toán vét cạn để giải bài toán ECDLP là lần lượt tính thử các điểm *G, 2G, 3G, ...* cho đến khi điểm mới tính được đúng bằng điểm *P*. Trong trường hợp xấu nhất phải cần đến *n* bước thử, trung bình thường là $\frac{n}{2}$ bước thử là đạt được điểm *P*, do đó cần phải chọn *n* đủ lớn để bài toán vét cạn là không khả thi $n \geq 2^{160}$.

Thuật toán tốt nhất hiện nay để tấn công bài toán ECDLP là sự kết hợp của thuật toán Pohlih-Hellman và Pollard's rho [40], thuật toán này có thời gian tính là $O\left(\sqrt{p}\right)$, với *p* là ước số nguyên tố lớn nhất của *n* do đó phải chọn số *n* sao cho nó chia hết số nguyên tố *p* lớn nhất có $\sqrt{p}$ đủ lớn để giải bài toán này là không khả thi.

1.7. MỘT SỐ CHUẨN CHỮ KÝ SỐ VÀ LƯỢC ĐỒ CHỮ KÝ SỐ PHỔ BIẾN SỬ DỤNG TRONG LUẬN ÁN

1.7.1. Lược đồ chữ ký số RSA

Tạo khóa: Quá trình tạo khóa cho chữ ký số RSA [83] được mô tả như sau:

Người ký:

+ Chọn cặp số nguyên tố đủ lớn *p* và *q*, tính *n=pq*;

+ Chọn số nguyên *e* thỏa mãn *UCLN*(*e*, $\phi(n)$) = 1, với $\phi(n) = (p-1)(q-1)$;

+ Tính số nguyên *d*, thỏa mãn phương trình $d \equiv e^{-1} \bmod \phi(n)$;

+ Khoá bí mật là *d* và các giá trị công khai là (*n, e*).

Tạo chữ ký: Để tạo ra chữ ký của thông điệp $M \in Z_n$, người ký tính giá trị *s* như sau: $s = Sig_{(n,d)}(H(M)) \leftarrow H(M)^d \bmod n$. Trong đó *H* là hàm băm, *s* là chữ ký.

Xác thực chữ ký: Để xác thực chữ ký *s* có phải của người ký hay không thì người nhận kiểm tra bằng thủ tục: $Ver_{(n,e)}(H(M),s) = TRUE$ nếu như $H(M) = s^e \bmod n$.

Quá trình tạo chữ ký và kiểm tra chữ ký giống với quá trình mã hoá và giải mã của hệ mật RSA chỉ khác là quá trình tạo chữ ký thì người ký dùng khóa riêng còn quá trình kiểm tra thì người nhận dùng khóa công khai.

1.7.2. Lược đồ chữ ký số Schnorr

Lược đồ chữ ký số Schnorr [56] được phát triển dựa trên bài toán DLP và được mô tả như sau:

Tham số sử dụng: tham số miền là (*p, q, g*); số nguyên tố lớn ngẫu nhiên *q*; số nguyên tố lớn ngẫu nhiên *p* thoả mãn (*p*-1) chia hết cho *q*; phần tử sinh $g = h^{(p-1)/q} \bmod p$ với h bất kỳ và $(1 < h < p-1)$, chọn lại nếu *g*=1; Khoá bí mật $d \in Z_q^*$; thông điệp cần ký *M*.

Tạo khoá:

- Tính khóa công khai $\rho = g^d \bmod p$;

Tạo chữ ký: Tính các thành phần của chữ ký

- Người ký chọn giá trị ngẫu nhiên *k* với $(1 < k < q)$ và tính $c = g^k \bmod p$;

- Tính thành phần đầu tiên $r = H(M,c) \bmod q$, nếu *r* = 0 thì chọn lại *k;*

- Tính $s = (k - rd) \bmod q$, nếu s = 0 thì quay lại phần chọn *k* và tính *c*;

- Đầu ra là cặp (r,s) là chữ ký số trên thông điệp *M*.

Xác thực chữ ký:

- Tính $c' = g^s \rho^r \bmod p$ và $r' = H(M,c')$;

- Nếu $r' = r$ thì chữ ký được chấp nhận, ngược lại không được chấp nhận.

1.7.3. Lược đồ chữ ký số EC-Schnorr

Lược đồ chữ ký số EC-Schnorr [28] được phát triển dựa trên bài toán ECDLP và được mô tả như sau:

Tham số sử dụng: Đường cong ellip EC với p là một số nguyên tố lớn tạo trường G của đường cong EC; q là một số nguyên tố chỉ số lượng nhóm con của EC; G là điểm khác gốc O của EC với toạ độ (x_G, y_G) thỏa mãn: $q \times G \equiv O \bmod p$; g là phần tử sinh thuộc $\mathbb{Z}_p^*$ thỏa mãn $g^q \bmod p \equiv 1 \bmod p$; *H(M)* là giá trị hàm băm thông điệp M; d là khóa riêng của người sử dụng, với $1 < d < q$.

Tạo khoá:

- Tính điểm khóa công khai $P = d \times G \bmod p$;

Tạo chữ ký: Tính các thành phần của chữ ký

- Người ký chọn giá trị ngẫu nhiên k với $(1 < k < q)$ và tính $C = k \times G \bmod p$;

- Tính $r = H(M, x_C) \bmod q$, với x_C là hoành độ của điểm C, nếu $r = 0$ thì quay lại chọn k;

- Tính $s = (k - rd) \bmod q$, nếu $s = 0$ thì quay lại phần chọn k và tính C;

- Đầu ra của thuật toán là cặp (r, s), là chữ ký số trên thông điệp M.

Xác thực chữ ký:

- Tính $C' = s \times G + r \times P \bmod p$ và $r' = H(M, x_{C'})$;

- Nếu $r' = r$ thì chữ ký được chấp nhận, ngược lại không được chấp nhận.

1.7.4. Chuẩn chữ ký số GOST R34.10-94

Chữ ký số chuẩn GOST R34.10-94 [35] mô tả như sau:

Tham số sử dụng: tham số miền là (p, q, g); hai số nguyên tố p, q với $q|(p-1)$; g là một phần tử sinh của nhóm con thuộc nhóm nhân $\mathbb{Z}_p^*$ bậc q (tức là $g^q \bmod p \equiv 1 \bmod p$); khoá bí mật là d với $1 < d < q$; thông điệp cần ký M;

Tạo khoá:

- Người ký tính khoá công khai $\rho = g^d \bmod p$;

Tạo chữ ký: Tính các thành phần của chữ ký

- Người ký chọn giá trị ngẫu nhiên *k* sao cho $(1 < k < q)$ và tính $c = g^k \bmod p$;

- Tính phần đầu tiên của chữ ký là $r = c \bmod q$ và tính $h = H(M) \bmod q$, nếu *r* = 0 thì chọn lại *k*;

- Tính $s = (kh + rd) \bmod q$, nếu s = 0 thì quay về phần chọn *k*;

- Đầu ra của thuật toán là cặp (r, s), là chữ ký số trên thông điệp *M*.

Xác thực chữ ký:

- Kiểm tra chữ ký: Tính $r' = (\mathrm{g}^{s/h}\ \rho^{-r/h} \bmod p) \bmod q$;

- Nếu $r' = r$ thì chữ ký được chấp nhận, ngược lại không được chấp nhận.

1.7.5. Chuẩn chữ ký số GOST R34.10-2012

Chữ ký số chuẩn GOST R34.10-2012 [24] mô tả như sau:

Tham số sử dụng: Như phần Lược đồ chữ ký số EC-Schnorr

Tạo khoá:

- Tính giá trị điểm khóa công khai $P = d \times G \bmod p$;

Tạo chữ ký: Tính các thành phần của chữ ký

- Người ký chọn giá trị ngẫu nhiên *k* sao cho $(1 < k < q)$ và tính $C = k \times G \bmod p$;

- Tính giá trị băm $H(M)$ của thông điệp *M;*

- Tính phần đầu tiên của chữ ký số là $r = x_C \bmod q$, với x_C là hoành độ của điểm *C*, nếu $r = 0$ thì quay lại chọn *k*

- Tính $e = H(M) \bmod q$ và $s = (ke + rd) \bmod q$, nếu $s = 0$ thì quay về phần chọn *k*;

- Đầu ra của thuật toán là cặp (r, s), là chữ ký số trên thông điệp *M*.

Xác thực chữ ký:

- Tính $C' = (se^{-1} \bmod q) \times G - (re^{-1} \bmod q) \times P$ và $r' = x \times C' \bmod q$;

- Nếu $r' = r$ thì chữ ký được chấp nhận, ngược lại không được chấp nhận.

1.8. MỘT SỐ LƯỢC ĐỒ CHỮ KÝ ĐƯỢC SỬ DỤNG ĐÁNH GIÁ, SO SÁNH TRONG LUẬN ÁN

1.8.1. Một số lược đồ chữ ký số được sử dụng để so sánh với các lược đồ đề xuất trong luận án.

Phần này trình bày một số lược đồ liên quan được lựa chọn so sánh với các lược đồ đề xuất trong luận án.

1.8.1.1. Lược đồ chữ ký số trong [45]

Năm 2008, Ismail, Tahat và Amad đề xuất lược đồ chữ ký số dựa trên bài toán IFP và DLP. Lược đồ này được sử dụng so sánh với lược đồ đề xuất ở chương 3. Lược đồ được trình bày như sau:

Lược đồ chữ ký số cơ sở: Gọi $h(.)$ là hàm băm với đầu ra là t bits (giả sử như t=128). p là số nguyên tố lớn và n là tích của hai số nguyên tố an toàn, $\phi(n)$ là hàm Euler. Một số nguyên g là phần tử sinh của nhóm cấp n và thỏa mãn $g^n \equiv 1 (\bmod p)$. Lược đồ chữ ký số cơ sở được mô tả như sau:

Tạo khóa: chọn ngẫu nhiên số nguyên $e \in Z_n^* = \{1, 2, ..., n-1\}$ sao cho $UCLN(e,n)$=1. Tính số nguyên d thỏa mãn $ed = 1 \bmod(\phi(n))$. Chọn số nguyên x từ Z_p^* và tính $y = g^x (\bmod p)$. Khóa công khai là (y, e) và khóa bí mật là (x, d).

Tạo chữ ký: Để tạo chữ ký cho thông điệp m, người ký chọn ngẫu nhiên số nguyên bí mật $1 < r < n$, sau cho $UCLN(r,n)$=1. Và tính $k = g^r (\bmod p)$ và $s = h(m)x + kr (\bmod n)$ và tính $u = s^d (\bmod n)$. Người ký gửi (k,u) với bản tin m như là chữ ký cho người kiểm tra.

Xác thực chữ ký: Người kiểm tra có thể kiểm tra chữ ký bằng cách tính $g^{u^e} = y^{h(m)} k^k (\bmod p)$. Nếu thỏa mãn thì chữ ký số được xác thực, ngược lại thì chữ ký là không được xác thực.

Lược đồ chữ ký số mù dựa trên lược đồ chữ ký số cơ sở được mô tả qua các pha giao tiếp như sau:

+ Người ký chọn số nguyên $1 < r' < n$, sao cho $UCLN(r', n) = 1$. Và tính $k' = g^{r'} (\text{mod } p)$. Nếu $UCLN(k', n) = 1$ thì thực hiện tiếp bước sau, còn không thì chọn lại $1 < r' < n$.

+ Tiếp theo người ký gửi cho người yêu cầu ký bản tin m giá trị k'.

+ Người yêu cầu ký nhận k' và kiểm tra $UCLN(k', n) = 1$. Nếu đúng thì chọn giá trị của hai nhân tố làm mù $(\alpha, \beta) \in Z_n^*$ và tính $k = k'^{\alpha} g^{\beta} (\text{mod } p)$. Và kiểm tra $UCLN(k, n) = 1$, nếu không đúng thì quay lại bước chọn nhân tố mù, và nếu đúng thì tính và gửi cho người ký giá trị

+ Người ký tính và gửi cho người yêu cầu giá trị: $s' = h(m')x + k'r' (\text{mod } n)$.

+ Người yêu cầu tính và gửi cho người ký giá trị: $s = (\alpha s' k k'^{-1} + \beta k)(s'^{-1})^e (\text{mod } n)$.

+ Người ký tính và gửi người yêu cầu giá trị: $u' = s^d (\text{mod } n)$.

+ Người yêu cầu cuối cùng tính: $u = u's' (\text{mod } n)$.

(*k*,*u*) là chữ ký số mù hợp lệ trên thông điệp *m*. Việc xác thực chữ ký số được thực hiện như phương trình trong lược đồ cơ sở.

1.8.1.2. Lược đồ chữ ký số trong [72]

Năm 2010, Nikolay A.Moldovyan và Alexander A.Moldovyan đề xuất lược đồ ký số tập thể mù dựa trên bài toán khó DLP. Lược đồ đề xuất dựa trên mô hình chữ ký số tập thể được trình bày trong [71] và thiết kế lược đồ chữ ký số tập thể mù. Lược đồ này được sử dụng so sánh với lược đồ đề xuất ở chương 2. Lược đồ được trình bày như sau:

Gọi *p* là số nguyên tố lớn sao cho *q* là ước của (*p*-1) và *g* là phần tử sinh bậc *q* trong $\mathbb{Z}_p^*$. $Y = g^x \bmod p$ là khóa công khai, với *x* là khóa riêng.

Tạo chữ ký:

1) Vòng 1 (tập thể người ký **B**) : Mỗi thành viên trong tập thể người ký **B** chọn một số ngẫu nhiên $t_i < q$ và tính $R_i = g^{t_i} \bmod p$ và gửi cho tất cả các thành viên còn lại trong tập thể người ký để tính $R = \prod_{i=1}^{n} R_i \bmod p$ và gửi cho **A**.

2) Vòng 2 (người yêu cầu **A**): chọn hai số ngẫu nhiên $(\tau, \varepsilon) < q$ và tính $R' = RY^{\tau} g^{\varepsilon} \bmod p$. Sau đó **A** tính $E' = H(M \,||\, R')$ (là tham số thứ nhất của chữ ký), và tính $E = E' + \tau \bmod q$ và gửi E tới tất cả những người ký.

3) Vòng 3 (tập thể người ký **B**) : Mỗi thành viên nhóm **B** sử dụng (t_i, x_i) riêng của mình để tính $S_i = t_i + x_i E \bmod q$ và tính $S = \sum_{i=1}^{n} S_i \bmod q$ và gửi S cho **A**

4) Vòng 4 (người yêu cầu **A**): tính thành phần thứ hai của chữ ký số mù là $S' = S + \varepsilon \bmod q$

Cặp (E', S') là chữ ký số mù của thông điệp M.

Kiểm tra chữ ký: Chữ ký được kiểm tra như sau:

Bước 1: Tính $R^* = g^S Y^{-E} \bmod p$

Bước 2: Tính $E^* = H(M \,||\, R^*)$

So sánh: Nếu $E^* = E'$ thì chữ ký số được chấp nhận, ngược lại chữ ký không được chấp nhận.

1.8.1.3. Lược đồ chữ ký số trong [73]

Năm 2011, Nikolay A.Moldovyan đề xuất lược đồ ký số tập thể mù dựa trên chuẩn GOST R34.10-94, lược đồ sử dụng độ khó của bài toán logarit rời rạc, sử dụng các phương trình tạo chữ ký số khác với lược đồ đề xuất và chưa được đánh giá độ an toàn trong mô hình đánh giá độ an toàn chuẩn như ROM,… Ngoài ra, lược đồ [73] sử dụng bốn tham số làm mù nên độ phức tạp tính toán cao hơn lược đồ NCS đề xuất. Lược đồ được trình bày như sau:

Gọi *p, q* là các số nguyên tố lớn và *g* là phần tử sinh bậc *q* trong $\mathbb{Z}_p^*$. Khóa công khai của mỗi người ký là $Y_i = g^{x_i} \bmod p$, với x_i là khóa riêng người ký thứ *i*. *Y* là khóa công khai của tập thể người ký.

Tạo chữ ký:

1) Vòng 1 (tập thể người ký **B**) : Mỗi thành viên trong tập thể người ký **B** chọn một số ngẫu nhiên k_i và tính $\rho_i = g^{k_i} \bmod p$ và gửi cho tất cả các thành viên còn lại trong tập thể người ký để tính $\rho = \prod_{i=1}^{n} \rho_i \bmod p$ và gửi cho **A**.

2) Vòng 2 (người yêu cầu **A**): tính $h' = H(M)$; chọn số ngẫu nhiên $(\tau, \mu, \varepsilon, \delta) \in \{1, 2, ..., q-1\}$ và tính $h = \tau h'$, $\rho' = \rho^{1/\delta} Y^{\mu} g^{\varepsilon} \bmod p$, $r' = \rho' \bmod q$ và tính $r = \tau\delta(r' + \mu h') \bmod q$, r' là thành phần thứ nhất của chữ ký. Gửi (*r*, *h*) tới tất cả những người ký.

3) Vòng 3 (tập thể người ký **B**) : Mỗi thành viên trong tập thể người ký **B** tính $s_i = k_i h + x_i r \bmod q$ và tính $s = \sum_{i=1}^{n} s_i \bmod q$ và gửi *s* cho **A**.

4) Vòng 4 (người yêu cầu **A**): tính thành phần thứ hai của chữ ký số mù là $s' = (\tau^{-1}\delta^{-1}s + \varepsilon h') \bmod q$

Cặp (r', s') là chữ ký số mù của thông điệp *M*.

Kiểm tra chữ ký: Chữ ký được kiểm tra như sau:

Bước 1: Tính $h = H(M)$

Bước 2: Tính $r^* = (g^{s/h} Y^{-r/h} \bmod p) \bmod q$

So sánh: Nếu $r^* = r$ thì chữ ký số được chấp nhận, ngược lại chữ ký không được chấp nhận.

1.8.1.4. Lược đồ chữ ký số trong [70]

Năm 2017, Minh và cộng sự đề xuất lược đồ ký số mù mới dựa trên độ khó của việc khai căn bậc *k* modulo một số nguyên tố *p* lớn với trường hợp *k* là số nguyên tố và thỏa mãn $k^2 | (p-1)$ [55]. Các lược đồ được đề xuất tạo ra chữ ký (E', S'), trong đó E' có giá trị 160 bit và S' có giá trị là 1024 bit. Lược đồ này được sử dụng so sánh với lược đồ đề xuất ở chương 3. Lược đồ chữ ký số tập thể mù được trình bày như sau:

Gọi $\{B_1, B_2, ..., B_n\}$ là tập thể người ký thông điệp *M* cho người yêu cầu **A**

Tạo khoá:

1) Gọi $x_1, x_2, ..., x_n$ là khoá riêng của tập thể người ký với $1 < x_i < p$, $x_i (i = 1, 2, ..., n)$ được chọn ngẫu nhiên và chỉ thành viên B_i biết.

2) Gọi $y_1, y_2, ..., y_n$ là khoá công khai của tập thể người ký với $y_i = x_i^k \bmod p$ được tính và công khai bởi thành viên B_i.

3) Khoá công khai chung của nhóm là : $Y = \prod_{i=1}^{n} y_i^{y_i} \bmod p$

Tạo chữ ký: có 4 vòng

1) Vòng 1 (tập thể người ký **B**) : Mỗi thành viên của tập thể người ký **B** chọn một số ngẫu nhiên $t_i < p$ và tính $r_i = t_i^k \bmod p$ và gửi cho tất cả các thành viên còn lại trong tập thể người ký để tính $R = \prod_{i=1}^{n} r_i \bmod p$ và gửi cho **A.**

2) Vòng 2 (người yêu cầu **A**): chọn một số ngẫu nhiên $\varepsilon < Nk$ với *N* là số nguyên chẵn và *k* không chia hết cho ε, và chọn một số ngẫu nhiên $\sigma < p$ và tính $R' = RY^{\varepsilon}\sigma^k \bmod p$. Sau đó **A** tính $E' = H(M \,||\, R')$ (là tham số thứ nhất của chữ ký), và tính $E = E' + \varepsilon \bmod N'$ với $N' = Nk$ và gửi *E* tới tất cả những người ký.

3) Vòng 3 (Tập thể người ký **B**) : Mỗi thành viên nhóm B sử dụng (t_i, x_i) riêng của mình để tính $s_i = x_i^{Ey_i} t_i \bmod p$ và tính $S = \prod_{i=1}^{n} s_i \bmod p$ và gửi S cho A

4) Vòng 4 (người yêu cầu A): tính thành phần thứ hai của chữ ký số mù là $S' = S\sigma \bmod p$

Cặp (E', S') là chữ ký số mù của thông điệp *M*.

Kiểm tra chữ ký: Chữ ký được kiểm tra như sau:

Bước 1: Tính $R^* = S'^k Y^{-E'} \bmod p$

Bước 2: Tính $E^* = H(M \,||\, R^*)$

So sánh: Nếu $E^* = E'$ thì chữ ký được chấp nhận, ngược lại không chấp nhận.

1.8.1.5. Lược đồ chữ ký số trong [8]

Công trình "Security of blind digital signature" của nhóm tác giả Ari Juels, Michael Luby, và Rafail Ostrovsky trình bày hai khái niệm về độ an toàn cho chữ ký số, đó là chứng minh độ an toàn dựa trên độ phức tạp (*Complexity-based proofs*) và chứng minh độ an toàn dựa trên mô hình tiên tri ngẫu nhiên ROM (*Proofs based on random oracle model*). Các tác giả cũng chỉ ra rằng việc chứng minh độ an toàn dựa trên sự phức tạp được ưu tiên sử dụng so với việc chứng minh dựa trên ROM. Tuy nhiên đến nay, đa số các công trình nghiên cứu là chứng minh độ an toàn dựa trên mô hình ROM và nhóm tác giả trình bày lược đồ chữ ký mù đầu tiên với việc chứng minh độ an toàn dựa trên độ phức tạp.

Công trình đưa ra hai đóng góp là: (1) Các khái niệm mù và an toàn có thể được chính thức hóa đồng thời (2) đưa ra cấu trúc chứng minh của sự tồn tại của một lược đồ chữ ký số mù đáp ứng các yêu cầu mạnh nhất theo giả định phức tạp chung và chạy trong thời gian đa thức (*điều này là khá phức tạp và không hiệu quả*).

Tuy nhiên, theo nghiên cứu của NCS thì công trình [8] chủ yếu là tập trung vào xây dựng mô hình chữ ký số mù mà chưa đưa ra lược đồ hay thuật toán ký mù cụ thể nào. Ngoài ra các mô hình đề xuất được chứng minh dựa trên độ phức tạp. Trong khi các tiêu chí cần đạt được của luận án là xây dựng các lược đồ chữ ký số tập thể mù dựa trên các chuẩn và các lược đồ phổ biến và chứng minh độ an toàn trong mô hình ROM. Qua đó có thể ứng dụng các giải thuật của lược đồ đề xuất vào xây dựng các phần mềm ứng dụng,…và như vậy có thể sử dụng được trong các ứng dụng thực tế như bầu cử điện tử,…

1.8.2. Một số nghiên cứu liên quan trong nước gần đây

Luận án tiến sĩ của Lưu Hồng Dũng (năm 2013) về nghiên cứu, phát triển các lược đồ chữ ký số tập thể [1].

Luận án đề xuất mô hình chữ ký số tập thể đáp ứng yêu cầu xác thực nguồn gốc và tính toàn vẹn cho các thông điệp dữ liệu ở nhiều cấp độ khác nhau, ứng dụng phù hợp trong các tổ chức xã hội, các cơ quan hành chính nhà nước, các doanh nghiệp,... Cụ thể, giới thiệu hai mô hình chữ ký số gồm mô hình dựa trên tính khó của bài toán khai căn một số nguyên trên vành $Z_n = pq$, trong đó p, q là các số nguyên tố phân biệt. Mô hình thứ hai được cải tiến từ mô hình chữ ký số GOST R34.10.94. Chứng minh được tính đúng đắn và tính an toàn của các lược đồ đề xuất. Trên cơ sở các mô hình đề xuất, phát triển 9 lược đồ chữ k ý số tập thể theo mô hình mới đề xuất.

Tuy nhiên, luận án chỉ đề xuất lược đồ chữ ký số tập thể mà chưa phát triển thành các lược đồ chữ ký số mù, nghiên cứu luận án này khác với hướng nghiên cứu của NCS là về chữ ký số mù.

Luận án tiến sĩ của Đặng Minh Tuấn (năm 2017) nghiên cứu xây dựng một số dạng lược đồ mới cho chữ ký số tập thể [7]

Luận án đã xây dựng mô hình chữ ký số tập thể đa thành phần, ở đó mỗi thành viên có thể ký vào nhiều thành phần khác nhau của văn bản và một phần của văn

bản có thể ký bởi nhiều người. Trên cơ sở đó, triển khai cho 03 hệ mật tiêu biểu và sự kết hợp mô hình mới đề xuất với các mô hình đã có như mô hình chữ ký số ủy nhiệm và chữ ký số mù.

Cụ thể, luận án đề xuất mô hình chữ ký số tập thể đa thành phần tổng quát và triển khai trên hệ mật như: (i) xây dựng lược đồ chữ ký số tập thể đa thành phần dựa trên hệ mật đường cong elliptic; (ii) xây dựng lược đồ chữ ký số tập thể đa thành phần dựa trên hệ mật DLP; (iii) xây dựng lược đồ chữ ký số tập thể đa thành phần dựa trên cặp song tuyến. Đồng thời, luận án cũng đã đưa ra mô hình chữ ký số ủy nhiệm đa thành phần và chữ ký số tập thể mù đa thành phần.

Luận án này có hướng nghiên cứu về chữ ký số tập thể mù khác với hướng nghiên cứu về chữ ký số tập thể mù của NCS đó là: Luận án này nghiên cứu về chữ ký số tập thể mù đa thành phần theo mô hình tự đề xuất, nghĩa là trong quá trình ký tập thể mù, mỗi người ký có thể ký nhiều phần của văn bản và mỗi phần của văn bản có thể được ký bởi nhiều người. Còn theo hướng nghiên cứu về chữ ký số tập thể mù của NCS là nghiên cứu đề xuất các lược đồ chữ ký số tập thể mù dựa trên các chuẩn chữ ký số và chữ ký số phổ biến, đồng thời phương thức ký tập thể là ký song song, hay mỗi người ký chỉ ký một thành phần văn bản.

Luận án tiến sĩ của Đào Tuấn Hùng (năm 2017) về nghiên cứu, phát triển một số lược đồ chữ ký số hướng tới nhóm [6]

Luận án xây dựng lược đồ chữ ký số tập thể hoàn toàn mới có phân biệt trách nhiệm dựa trên tính khó của bài toán DLP và tính khó của bài toán tính căn modulo của số nguyên tố. Luận án đề xuất hai lược đồ chữ ký số tập thể có cấu trúc song song và hai lược đồ chữ ký số tập thể có cấu trúc tuần tự, trong đó hai lược đồ ký đa thành phần nhằm đáp ứng các lớp bài toán ký với số lượng thành viên ký và số văn bản không cố định, cung cấp khả năng một người tham gia xác thực nhiều văn bản. Các lược đồ này minh chứng rõ ràng về trách nhiệm của người ký và cho phép giảm chi phí tính toán cũng như truyền tin. Ngoài ra, luận án còn xây dựng một lược đồ

chữ ký số nhóm dựa trên bài toán DLP trên đường cong elliptic cho phép giảm chiều dài chữ ký số và tăng hiệu quả của thủ tục tạo chữ ký,...

Tuy nhiên, luận án chỉ đề xuất các dạng lược đồ chữ ký số tập thể mà chưa phát triển thành các lược đồ chữ ký số mù, khác với hướng nghiên cứu của NCS.

Nhìn chung, trong thời gian gần đây ở trong nước có nhiều luận án tiến sĩ nghiên cứu về chữ ký số, chữ ký số tập thể và tập thể mù. Tuy nhiên như trình bày ở trên, các hướng nghiên cứu trên là khác với hướng nghiên cứu của NCS.

1.9. PHÂN TÍCH MỘT SỐ CÔNG TRÌNH NGHIÊN CỨU VỀ CHỮ KÝ SỐ ĐÃ CÔNG BỐ GẦN ĐÂY VÀ VẤN ĐỀ CẦN GIẢI QUYẾT TRONG LUẬN ÁN

Có thể thấy rằng, từ khi David Chaum đề xuất lược đồ chữ ký số mù đầu tiên, sau đó có rất nhiều nghiên cứu về lược đồ chữ ký số mù, chữ ký số tập thể mù được công bố. Trong các lược đồ thuộc loại chữ ký số mù được công bố, có thể chia thành các hướng nghiên cứu như sau:

1) Dựa trên các chuẩn, các lược đồ phổ biến đã được chứng minh về tính an toàn và hiệu quả và được ứng dụng nhiều trong thực tế, như các chuẩn và lược đồ GOST R34.10-94, GOST R34.10-2012, RSA, Rabin, Schnorr, EC-Schnorr,… để kế thừa tính an toàn và hiệu quả của chúng vì chúng đã được chuẩn hóa hoặc được đưa vào các hệ thống tiêu chuẩn.

Tuy nhiên, việc phát triển các lược đồ chữ ký số mù dựa trên chuẩn GOST và các lược đồ phổ biến như RSA, Rabin, Schnorr, EC-Schnorr, Elgamal thì được nhiều nhà nghiên cứu quan tâm. Việc phát triển chữ ký số mù dựa trên chuẩn DSA thì theo tìm hiểu của NCS là phương trình ký của DSA không mở rộng để xây dựng các lược đồ chữ ký số mù được (theo công trình nghiên cứu [66]). Và thực thế hiện nay theo NCS tìm hiểu cũng chưa thấy có lược đồ chữ ký số mù đề xuất được công bố dựa trên DSA.

Các lược đồ chữ ký số mù dựa trên các chuẩn GOST 34.10 và các lược đồ phổ biến như trên có thể phân tiếp thành hai loại nhỏ hơn như sau:

(i) Lược đồ xây dựng mới chỉ dựa trên các bài toán đơn như IFP, DLP và ECDLP: Có thể thấy, các lược đồ chỉ dựa trên một bài toán khó [5], [11], [13], [20], [47], [73], do đó chỉ đảm bảo tính an toàn trong ngắn hạn. Giả thiết rằng trong tương lai, khi các bài toán khó lần lượt bị phá giải, các lược đồ này sẽ không còn an toàn nữa.

Hiện nay, tuy có một số lược đồ đề xuất dựa trên hai bài toán khó nhưng chỉ cần giải được một bài toán khó thì lược đồ bị phá vỡ. Một số lược đồ dựa trên nền tảng hai bài toán IFP và DLP như: năm 1998, Shao [88] và Li-Xiao [62] đã đề xuất các lược đồ chữ ký số dựa trên IFP và DLP. Sau đó, năm 1999 Lee [57] chứng minh rằng lược đồ chữ ký của Shao là không an toàn như báo cáo. Để khắc phục nhược điểm lược đồ chữ ký của Shao, năm 2001, He [103] đề xuất một lược đồ chữ ký số cũng dựa vào bài toán IFP và DLP sử dụng cùng modulo và một tập số mũ và các khóa bí mật. Vào năm 2002, Hung Min Sun [44] chỉ ra rằng các lược đồ đó chỉ dựa trên bài toán DLP. Năm 2003, Wang, Lin và Chang [100] đề xuất một lược đồ chữ ký số dựa trên cả hai bài toán khó và lược đồ này vẫn chưa bị phá vỡ. Năm 2007, Wei [101] đưa ra hai lược đồ cải tiến từ lược đồ của Shao và Li-Xiao nhằm chống lại những tấn công vào hai lược đồ này. Năm 2009, Lin, Gun và Chen [63] cho rằng các lược đồ của Wei vẫn không an toàn do có thể giả mạo chữ ký của một thông điệp bằng cách sử dụng phương pháp của Pollard [78] và Schnorr.

Ngoài ra còn có các nghiên cứu liên quan gần đây như: năm 2010, Nikolay A. Moldovyan và Alexander A. Moldovyan công bố bài báo "*Lược đồ chữ ký số tập thể mù dựa trên bài toán DLP*" [72]. Bài báo xây dựng lược đồ chữ ký số tập thể mù dựa trên lược đồ Schnorr. Trong lược đồ đề xuất, chữ ký được hình thành đồng thời bởi tất cả những người ký, do đó mà lược đồ có thể sử dụng cho các ứng dụng dạng như ký hợp đồng điện tử, đây là một dạng mới của lược đồ chữ ký số tập thể có thể dùng để ký đồng thời một gói các hợp đồng khác nhau bởi các tập thể người ký khác nhau, và còn có thể gọi là lược đồ chữ ký số hỗn hợp. Năm 2011, Nikolay A. Moldovyan công bố nghiên cứu [73] "*Xây dựng lược đồ ký mù dựa trên chuẩn chữ ký số*". Bài báo xây dựng lược đồ ký số mù dựa trên chuẩn chữ ký số của Nga

và đây là lược đồ đầu tiên dựa trên chuẩn chữ ký số, công trình cũng đề xuất lược đồ chữ ký số tập thể mù dựa trên chuẩn chữ ký số và là lược đồ ký số tập thể mù đầu tiên sử dụng các phương trình trong chuẩn chữ ký số để xác minh chữ ký.

Năm 2013, nhóm tác giả Lưu Hồng Dũng và cộng sự công bố bài báo "*Phát triển một dạng lược đồ chữ ký số mới*" [2]. Bài báo đề xuất một dạng lược đồ chữ ký số mới dựa trên bài toán phân tích số và khai căn trên vành Z_n. Mức độ an toàn của các lược đồ đề xuất được đánh giá qua một số dạng tấn công đã được biết đến trong thực tế, cho thấy các lược đồ mới này có thể sử dụng trong các ứng dụng thực tế nếu các tham số hệ thống được lựa chọn hợp lý. Tuy nhiên, để sử dụng được trong thực tế, các lược đồ này cần được cải tiến và đánh giá kỹ càng hơn cả về mức độ an toàn cũng như khía cạnh hiệu quả thực hiện. Năm 2014, nhóm tác giả Nguyễn Tiền Giang và cộng sự công bố bài báo "*Lược đồ chữ ký số mù xây dựng trên bài toán khai căn*" [5]. Bài báo đề xuất việc phát triển lược đồ chữ ký số mù từ một dạng lược đồ chữ ký số mới xây dựng dựa trên tính khó của bài toán khai căn trên vành $Z_{n=pq}$, với *p, q* là các số nguyên tố lớn. Ưu điểm của lược đồ chữ ký số mù này là khả năng chống lại kiểu tấn công làm lộ nguồn gốc thông điệp được ký so với các lược đồ chữ ký số mù đã được biết trước đó. Ribarski và cộng sự công bố nghiên cứu các lược đồ chữ ký số mù dựa trên định danh trên cơ sở các cặp trên đường cong elliptic để xây dựng chữ ký số mù như một phần của lược đồ bỏ phiếu điện tử. Các tác giả cũng so sánh về chi phí tính toán của các phép toán số học và so sánh băng thông trực tiếp của giao thức tương tác trong thuật toán ký của các lược đồ chữ ký số mù [82]. Năm 2015, nhóm tác giả Lưu Hồng Dũng và cộng sự công bố bài báo "*Một dạng lược đồ chữ ký số xây dựng trên bài toán phân tích số*" [3]. Bài báo đề xuất một dạng lược đồ chữ ký số mới dựa trên bài toán phân tích số. Mức độ an toàn của lược đồ mới được đánh giá bằng độ khó giải của bài toán phân tích số. Dạng lược đồ mới này có thể sử dụng cho các ứng dụng thực tế nếu các tham số hệ thống và các phương trình kiểm tra tính hợp lệ của chữ ký được lựa chọn hợp lý. Tuy nhiên các lược đồ này cần được đánh giá kỹ càng cả về mức độ an toàn cũng như khía cạnh hiệu quả thực hiện. Fuchsbauer và cộng sự công bố nghiên cứu xây

dựng một cấu trúc chữ ký số mù tối ưu trong mô hình chuẩn, và được mở rộng thành chữ ký số mù một phần và chữ ký số mù trên các vectơ bản tin, điều này tạo ra thông tin ẩn danh trong mô hình chuẩn [30].

Năm 2016, Guo và cộng sự trong bài báo [36] trình bày một lược đồ multi-proxy ký mù lượng tử. Trong lược đồ này, một người ký ban đầu ủy quyền phần ký của mình cho một nhóm người có thẩm quyền ký bằng cách sử dụng lệnh bảo đảm. Verma và cộng sự đề xuất hai lược đồ chữ ký số mù công bằng trên cơ sở định danh dựa trên một phương pháp cắt gọn và dựa trên giao thức chuyển giao không nhớ. Các lược đồ đề xuất có thể là một giải pháp thay thế để loại bỏ việc lạm dụng các giao thức mật mã và vấn đề quản lý khóa trong các giao thức mã hóa khóa công khai [97]. Năm 2017, nhóm tác giả Hieu Minh và cộng sự công bố bài báo [70] "*Xây dựng lược đồ ký số mù mới dựa trên bài toán khó mới*". Công trình đề xuất một lược đồ chữ ký mù và hai loại lược đồ chữ ký tập thể mù mới, các lược đồ đó dựa trên độ khó của việc tìm căn bậc *k* modulo một số nguyên tố lớn. Verma và cộng sự đề xuất một lược đồ proxy ký mù với khả năng phục hồi bản tin để rút ngắn kích thước chữ ký số trên bản tin và giảm chi phí thời gian tính toán [96]. Banerjee đề xuất một lược đồ chữ ký mù và một proxy mù an toàn dựa trên ID từ các cặp song tuyến, lược đồ đáp ứng các thuộc tính bảo mật của cả lược đồ chữ ký số mù và proxy mù [84]. James và cộng sự đề xuất lược đồ chữ ký số mù mới với việc khôi phục thông điệp trong phần thiết lập trên cơ sở định danh sử dụng cặp song tuyến trên các đường cong elliptic, lược đồ đề xuất với giả định rằng bài toán Diffie-Hellman là khó [46]. Kumar và cộng sự trong [55] đề xuất một lược đồ chữ ký số mù bằng cách sử dụng hệ thống mật mã dựa trên định danh, lược đồ sử dụng kết hợp lược đồ chữ ký số mù Bolyreva và chữ ký dựa trên định danh của Cha-Chaon. Các tác giả chứng minh là lược đồ đề xuất phù hợp với hệ thống bỏ phiếu điện tử hơn so với các lược đồ chữ ký mù dựa trên định danh khác. M. Kumar và cộng sự đề xuất một lược đồ chữ ký số mù mới sử dụng hệ thống mật mã dựa trên định danh trên cơ sở độ khó của bài toán ECDLP, các tác giả cũng cho rằng lược đồ đề xuất là hiệu quả hơn đáng kể về chi phí tính toán và chi phí băng thông so với

các lược đồ khác dựa trên ghép cặp song tuyến [54]. Muthanna đề xuất một lược đồ chữ ký số mù an toàn mới, mà để bảo mật chữ ký số mù, lược đồ này tạo ra hai chữ ký số mù. Mỗi chữ ký số mù có các yếu tố mù riêng. Ngoài ra, người yêu cầu cũng mã hóa thông tin được gửi cho người ký bằng một khóa được tạo bởi hệ thống mật mã El-Gamal, khóa này làm tăng thêm độ an toàn cho thông điệp được ký [74].

Năm 2018, Tahat và cộng sự trong bài báo "*Partially blind signature scheme based on chaotic maps and factoring problems*" đã đề xuất một lược đồ với chi phí tính toán thấp dựa trên cả hệ thống mật mã và hệ thống hỗn hợp. Tính an toàn của lược đồ phụ thuộc vào độ linh hoạt của bài toán IFP và DLP của đa thức Chebyshev. Lược đồ được chứng minh có chi phí kênh truyền thấp, đây là lược đồ chữ ký số mù một phần đầu tiên dựa trên các ánh xạ ngẫu nhiêu và IFP [94]. Verma và cộng sự đề xuất lược đồ chữ ký số mù ghép khôi phục thông điệp trên cơ sở định danh. Trong lược đồ này, thông điệp không được truyền với chữ ký và được khôi phục trong giai đoạn xác minh, tổng chiều dài chữ ký của thông điệp là thấp và lược đồ có chi phí tính toán thấp nhất, sử dụng băng thông thấp và độ an toàn cao [98]. Zhu và cộng sự đề xuất một lược đồ proxy ký mù dựa trên định danh và không phụ thuộc vào hạ tầng khóa công khai. Độ an toàn của lược đồ đề xuất phụ thuộc bài toán giải pháp số nguyên vòng nhỏ trên mạng đơn vị nghiên cứu định lý số [110]. Zhang và cộng sự đề xuất một lược đồ chữ ký số sử dụng bên tin cậy thứ ba để tránh việc chối bỏ của người nhận. Người nhận kiểm tra chữ ký thông quan bên thứ 3 trong lược đồ. Lược đồ sử dụng các đặc tính vật lý của cơ học lượng tử để làm mù thông điệp, ủy quyền, ký và xác minh chữ ký [108].

Qua phân tích trên, để tăng cường tính an toàn cho các lược đồ chữ ký số, cần phải phát triển các lược đồ thực sự dựa trên nhiều bài toán khó, điều này sẽ làm cho việc tấn công trở nên khó khăn hơn khi phải giải đồng thời các bài toán khó.

(ii) Lược đồ đề xuất dựa trên hai bài toán khó nhưng chưa chứng minh trong mô hình chuẩn và mô hình ROM [29], [30], [73], [107] và tính hiệu quả của các lược đồ này có thể cần cải tiến thêm như giảm độ phức tạp về thời gian,...

Chứng minh tính an toàn của các lược đồ chữ ký số mù mà không dựa vào mô hình ROM cũng đang được các nhà nghiên cứu quan tâm hiện nay. Fuchsbauer và Vergnaud trong [29] đã đưa ra lược đồ chữ ký số mù đầu tiên mà việc chứng minh tính an toàn không dựa vào mô hình ROM, lược đồ này cung cấp một lược đồ bầu cử điện tử và có thể được sử dụng cho mô hình chữ ký nhóm ẩn danh. Phương pháp chứng minh tính an toàn áp dụng trong [29] sử dụng các hệ thống chứng minh không tiết lộ thông tin, chữ ký tự động và mã hóa dựa trên thẻ. Trong [73] và [107] cũng đã nghiên cứu đề xuất các lược đồ chữ ký số mà việc chứng minh tính an toàn không dựa vào mô hình ROM, tuy nhiên các kỹ thuật này cần được nghiên cứu thêm và phải được các viện nghiên cứu đánh giá mới có thể triển khai trong thực tế.

2) Lược đồ không dựa trên chuẩn: Một số lược đồ công bố chưa được kiểm nghiệm về tính an toàn và hiệu quả do không dựa trên các chuẩn [2], [3], [4], [45], [63], [93]. Các lược đồ dựa trên các bài toán khó đơn như IFP, DLP, ECDLP hoặc trên hai bài toán khó. Mặc dù các tác giả có chứng minh tính an toàn nhưng do không dựa trên các chuẩn và cũng chưa được kiểm nghiệm bởi các tổ chức về tiêu chuẩn trên thế giới nên còn phải tiếp tục nghiên cứu thêm. Một số lược đồ công bố có chứng minh hiệu năng, tuy nhiên có thể nghiên cứu để tối ưu thêm để có thể ứng dụng trong thực tế, nhất là đối với các thiết bị có khả năng xử lý hạn chế như thiết bị IoT hiện nay.

Ngày nay, khi mà chữ ký số mù được áp dụng rộng rãi trong nhiều ứng dụng yêu cầu tính ẩn danh như bầu cử điện tử, thương mại điện tử và tiền điện tử,… [15], [18], [106]. Để đảm bảo chất lượng các dịch vụ này, một số lược đồ chữ ký mù được đề xuất. Năm 1995, Camenisch [11] đề xuất lược đồ chữ ký mù mới dựa trên bài toán DLP. Sau đó, Harn [39] tuyên bố rằng chữ ký mù trong [11] có thể bị truy vết bởi người ký. Tuy nhiên, Horster [41] mô phỏng rằng người ký không thể truy

ngược lại chủ sở hữu chữ ký. Dựa vào các kỹ thuật phân tích mật mã trong [39], Lee [15] chứng minh rằng lược đồ của Camenisch không thỏa mãn tính không thể truy vết. Để khắc phục điểm yếu này, họ đã đề xuất một lược đồ chữ ký mù mới dựa trên DLP. Cuối cùng, vào năm 2005, Wu và Wang [106] đã chứng minh tính không thể truy vết của lược đồ Camenisch, họ cũng tuyên bố rằng lược đồ của Lee và cộng sự là không thể truy vết được, nhưng chứng minh của họ về tính không thể truy vết đó là sai. Họ đã sửa chữa việc chứng minh tính không thể truy vết của lược đồ của Lee và kết luận rằng lược đồ của Camenisch vẫn nhiều hiệu quả hơn của Lee. Sau đó, Jena và cộng sự [18] và [19] đề xuất hai lược đồ chữ ký mù mới, tuy nhiên họ không chứng minh lược đồ của họ là đảm bảo tính đúng của chữ ký số mù.

Gần đây, Fan và cộng sự trong [27] đã thực hiện tấn công vào các lược đồ của [15] và [106] bằng cách chỉ thực hiện một vòng lược đồ ký thì người yêu cầu ký có thể đạt được nhiều hơn một chữ ký hợp lệ. Họ kết luận rằng, một lược đồ chữ ký số mù an toàn và mới cần phải được quan tâm nghiên cứu. Các lược đồ chữ ký số mù đề xuất trong luận án này nhằm góp phần thực hiện các xu hướng nghiên cứu đó.

Từ phân tích trên, NCS đã chọn hướng nghiên cứu là dựa trên các chuẩn GOST 34.10 của Liên bang Nga và các lược đồ phổ biến, đồng thời xây dựng các lược đồ dựa trên sự kết hợp của hai bài toán khó. Xây dựng bài toán khó mới mà để phá vỡ phải giải đồng thời hai vấn đề khó dạng IFP và DLP, sau đó xây dựng lược đồ chữ ký số mù có độ dài được rút ngắn. Cụ thể như sau:

1) Dựa trên một bài toán khó: Nghiên cứu xây dựng các lược đồ chữ ký số tập thể mù mới dựa trên chuẩn và lược đồ phổ biến đã được chứng minh về tính an toàn và hiệu quả trong thực tế nhằm kế thừa tính an toàn và hiệu quả của chúng, đó là GOST R34.10-94 và GOST R34.10-2012, Schnorr, EC-Schnorr, RSA.

2) Dựa trên hai bài toán khó và các lược đồ phổ biến: Xây dựng lược đồ chữ ký số mù, chữ ký số tập thể mù dựa trên hai bài toán khó là IFP và DLP. Sau đó mở rộng để xây dựng lược đồ chữ ký mù đơn và tập thể mù, mà để phá vỡ lược đồ này yêu cầu phải giải đồng thời hai bài toán khó. Lược đồ mới đề xuất dựa trên lược đồ

RSA và Schnorr để kế thừa tính an toàn và hiệu quả của chúng.

3) Xây dựng bài toán khó mới sử dụng nhóm con hữu hạn không vòng hai chiều mà để phá vỡ chúng phải giải đồng thời hai vấn đề tính toán khó dạng bài toán IFP và DLP. Trên cơ sở bài toán khó mới, xây dựng lược đồ chữ ký số mù, chữ ký số tập thể mù có độ dài được rút ngắn. Đây là lược đồ chữ ký số mù đầu tiên sử dụng nhóm con hữu hạn không vòng hai chiều.

1.10. KẾT LUẬN CHƯƠNG 1

Chương 1 trình bày tổng quan về lược đồ chữ ký số, chữ ký số tập thể, chữ ký số mù, chữ ký số tập thể mù và các tính chất, chức năng và tính an toàn của các lược đồ chữ ký số. Đồng thời cũng trình bày về mô hình đánh giá độ an toàn của các lược đồ chữ ký số là mô hình tiên tri ngẫu nhiên (ROM).

Chương 1 cũng giới thiệu tổng quan về ba bài toán khó là IFP, DLP và ECDLP. Trình bày các chuẩn và lược đồ phổ biến đang được ứng dụng trong thực tế như RSA, Schnorr, EC-Schnorr, GOST R34.10-94 và GOST R34.10-2012. Trình bày khái quát một số các công trình nghiên cứu liên quan gần đây trong nước, chỉ ra các hướng nghiên cứu và nêu định hướng hướng nghiên cứu của NCS.

Chương 1 cũng tập trung phân tích một số lược đồ chữ ký số mù liên quan đã được công bố. Qua phân tích, NCS phân loại các hướng nghiên cứu trong thời gian qua và chỉ ra những vấn đề cần phải cải tiến hoặc nghiên cứu thêm,... Qua đó, NCS đã chọn hướng nghiên cứu là: dựa trên các chuẩn và các lược đồ phổ biến để xây dựng các lược đồ chữ ký số mù, tập thể mù mới nhằm kế thừa tính an toàn và hiệu quả của chúng, đồng thời có cải tiến để có thể ứng dụng được trong thực tế. Đề xuất một số lược đồ chữ ký số mù dựa trên sự kết hợp của hai bài toán khó. Đề xuất bài toán khó mới sử dụng các nhóm con hữu hạn không vòng hai chiều, trên cơ sở đó xây dựng lược đồ chữ ký số mù, chữ ký số tập thể mù. Các lược đồ đề xuất dựa trên hai bài toán khó giúp tăng thêm tính an toàn của các lược đồ chữ ký số theo thời gian khi ứng dụng trong thực tế.

CHƯƠNG 2. PHÁT TRIỂN MỘT SỐ LƯỢC ĐỒ CHỮ KÝ SỐ TẬP THỂ MÙ DỰA TRÊN CÁC CHUẨN CHỮ KÝ SỐ VÀ LƯỢC ĐỒ CHỮ KÝ SỐ PHỔ BIẾN

Đã có một số lược đồ chữ ký số tập thể mù được đề xuất, nhưng lược đồ dựa trên các chuẩn chữ ký số hay các lược đồ phổ biến thì chưa được đề cập nhiều trong các nghiên cứu như đã phân tích ở chương 1. Chương này đề xuất một số lược đồ chữ ký số tập thể mù mới dựa trên một số chuẩn chữ ký số và một số lược đồ chữ ký số phổ biến. Các lược đồ mới tận dụng những ưu điểm về tính an toàn và hiệu năng của các lược đồ đã được chứng minh trong thực tế. Tính an toàn của các lược đồ đề xuất được chứng minh trong mô hình ROM.

Chương 2 xây dựng 02 lược đồ dựa trên chuẩn GOST R34.10-94 và lược đồ Schnorr, và 02 lược đồ dựa trên chuẩn GOST R34.10-2012 và lược đồ EC-Schnorr. Sau đó so sánh độ phức tạp thời gian của chúng và đề xuất hướng ứng dụng trong thực tế. Kết quả nghiên cứu công bố tại công trình [CT2] và [CT3].

2.1. ĐỀ XUẤT LƯỢC ĐỒ CHỮ KÝ SỐ TẬP THỂ MÙ DỰA TRÊN CHUẨN CHỮ KÝ SỐ GOST R34.10-94 VÀ LƯỢC ĐỒ CHỮ KÝ SỐ SCHNORR

Phần này đề xuất 2 lược đồ chữ ký số tập thể mù mới dựa trên chuẩn GOST R34.10-94 và lược đồ Schnorr, là các lược đồ dựa trên bài toán DLP. Đồng thời so sánh với các lược đồ đã công bố cùng hướng nghiên cứu để chứng minh khả năng ứng dụng trong thực tế của các lược đồ đề xuất.

Chuẩn chữ ký số GOST R34.10-94 và lược đồ Schnorr mô tả các lược đồ chữ ký số đơn. Cải tiến ở đây là dựa trên chuẩn và lược đồ phổ biến này, đề xuất phương pháp để xây dựng các lược đồ chữ ký số tập thể mù hiệu quả từ chữ ký số đơn. Qua đó có thể sử dụng được trong các ứng dụng yêu cầu nhiều người ký (dạng

chữ ký tập thể) và cần tính ẩn danh (tính mù). Các lược đồ đề xuất mới được mô tả như sau:

Tham số sử dụng trong lược đồ đề xuất: tham số miền là (*p, q, g*); hai số nguyên tố *p, q* với $q|(p-1)$; *g* là một phần tử sinh của nhóm con thuộc nhóm nhân Z_p^* bậc *q* (tức là $g^q \bmod p \equiv 1 \bmod p$); và khoá bí mật là *d* với $1 < d < q$.

Giả sử rằng có một người yêu cầu **A** yêu cầu tập thể người ký **B** (gồm *n* thành viên) có thẩm quyền ký để ký trên thông điệp *M*. Người yêu cầu không muốn tập thể người ký **B** biết nội dung của thông điệp *M*. Đầu tiên, người yêu cầu làm mù thông điệp *M* thành M', gửi M' đến **B**. Tập thể **B** ký lên M' và gửi lại cho người yêu cầu. Người yêu cầu xóa mù trên M' thành *M* và kiểm tra chữ ký thu được. Nếu chữ ký hợp lệ thì người yêu cầu đã có chữ ký hợp lệ trên thông điệp *M*.

Gọi TTP là bên thứ 3 tin cậy, TTP có thể là người đại diện của tập thể người ký hoặc có thể do một cơ quan chuyên trách đảm nhiệm.

2.1.1. Lược đồ chữ ký số tập thể mù dựa trên chuẩn GOST R34.10-94

2.1.1.1. Xây dựng lược đồ

Phần này đề xuất lược đồ chữ ký số tập thể mù dựa trên GOST R34.10-94, được ký hiệu là LĐ 2.01. Lược đồ được trình bày như sau:

1) Cài đặt: Mỗi người ký trong tập thể người ký **B** tính khoá công khai ρ_i của mình và gửi cho TTP để tính khoá công khai ρ của tập thể **B** như sau:

$$\rho_i = g^{d_i} \bmod p,\ i = 1, 2, ..., n;\quad \rho = \prod_{i=1}^{n} \rho_i \bmod p$$

2) Trích xuất: Mỗi người ký trong **B** chọn một giá trị ngẫu nhiên k_i với $k_i \in Z_q$, tính c_i và gửi tới TTP để tính $\overline{c}$. TTP gửi $\overline{c}$ tới A, với:

$$c_i = g^{k_i} \bmod p,\ i = 1, 2, ..., n;\quad \overline{c} = \prod_{i=1}^{n} c_i \bmod p = g^{\sum_{i=1}^{n} k_i \bmod q} \bmod p$$

3) Làm mù: Người yêu cầu **A** chọn hai giá trị ngẫu nhiên (*hay còn gọi là nhân tố làm mù*) $\alpha, \beta \in \{1, 2, ..., q\text{-}1\}$, tính $h = H(M)$ và tính $(\overline{r}, \overline{h})$ như sau:

$$\begin{cases} \overline{h} = \alpha h \bmod p \\ c = \overline{c}^{\beta} g^{\alpha} \bmod p \\ r = c \bmod q \\ \overline{r} = (r\beta^{-1}\alpha) \bmod q \end{cases}$$

Người yêu cầu **A** gửi cặp $(\overline{r}, \overline{h})$ tới mỗi người ký trong **B**.

4) Tạo chữ ký: Mỗi người ký trong **B** nhận cặp $(\overline{r}, \overline{h})$ từ **A**, mỗi người ký tính s_i và gửi cho TTP để tính $\overline{s}$ và gửi lại cho người yêu cầu, với:

$$s_i = k_i \overline{h} + d_i \overline{r} \bmod q; \quad \overline{s} = \sum_{i=1}^{n} s_i \bmod q$$

5) Giải mù: Người yêu cầu **A** giải mù $\overline{s}$ bằng cách tính *s* theo công thức: $s = (\beta\alpha^{-1}\overline{s} + \alpha h) \bmod q$

Cặp (r, s) là chữ ký số của tập thể **B** trên thông điệp *M*.

6) Kiểm tra chữ ký: Tính r' theo công thức (2.1) và so sánh r' với *r*, nếu $r' = r$ thì chữ ký được chấp nhận, ngược lại thì chữ ký không được chấp nhận, với:

$$r' = (g^{s/h} \rho^{-r/h} \bmod p) \bmod q \qquad (2.1)$$

Thật vậy, có thể chứng minh như sau:

$$\begin{cases} g^{s_i} = g^{k_i \overline{h} + d_i \overline{r}} \bmod p \Rightarrow g^{\sum_{i=1}^{n} s_i} = g^{\overline{h} \sum_{i=1}^{n} k_i} g^{\overline{r} \sum_{i=1}^{n} d_i} \bmod p \\ g^{\overline{s}} = \overline{c}^{\overline{h}} \rho^{\overline{r}} \bmod p \Rightarrow \overline{c} = g^{\overline{s}/\overline{h}} \rho^{-\overline{r}/\overline{h}} \bmod p \end{cases}$$

$$\overline{r} = (r\beta^{-1}\alpha) \bmod q \Rightarrow r = \overline{r}\beta\alpha^{-1} \bmod q$$

Thay vào phương trình kiểm tra (2.1), tính được:

$$
\begin{aligned}
r' &= (\mathrm{g}^{s/h}\ \rho^{-r/h} \bmod p) \bmod q \\
&= (\mathrm{g}^{(\beta\alpha^{-1}\overline{s}+\alpha h)/h}\ \rho^{-(\overline{r}\beta\alpha^{-1})/h} \bmod p) \bmod q \\
&= (g^{(\beta\overline{s})/\overline{h}+\alpha}\ \rho^{-(\beta\overline{r})/\overline{h}} \bmod p) \bmod q \\
&= (\overline{c}^{\beta} g^{\alpha} \bmod p) \bmod q \\
&= c \bmod q \\
&= r
\end{aligned}
$$

Vậy $r' = r$ đã được chứng minh hay chữ ký đã được xác thực.

Người yêu cầu **A** (M)	Dữ liệu	Tập thể người ký **B** ($p,\ q,\ \rho, \overline{c}$)
		Công khai ($p,\ q,\ \rho, \overline{c}$)
Chọn: $\alpha, \beta \in \{1, 2, ..., q-1\}$ $\overline{h} = \alpha h \bmod p$ $c = \overline{c}^{\beta} g^{\alpha} \bmod p$ $r = c \bmod q$ $\overline{r} = (r\beta^{-1}\alpha) \bmod q$	$\overline{h}, \overline{r}$ →	$s_i = k_i \overline{h} + d_i \overline{r} \bmod q$ $\overline{s} = \sum_{i=1}^{n} s_i \bmod q$
$s = (\beta\alpha^{-1}\overline{s} + \alpha h) \bmod q$ Chữ ký số là cặp: (r,s)	← $\overline{s}$	

Hình 2.1. Tóm tắt thuật toán ký số của LĐ 2.01

2.1.1.2. Đánh giá tính an toàn của lược đồ đề xuất

Lược đồ chữ ký số tập thể mù an toàn và được xác định bởi hai đặc trưng là tính mù và tính không thể giả mạo.

1) Tính mù: Các lược đồ chữ ký số tập thể mù đề xuất đảm bảo tính mù.

Chứng minh: Sử dụng các điều kiện trong định nghĩa 1.1 của chương 1 để chứng minh tính mù của lược đồ đề xuất.

Lấy bộ chữ ký $(M, r, s) \in \{(M_0, r_0, s_0), (M_1, r_1, s_1)\}$ là một trong hai bộ chữ ký số được gửi đến tập thể người ký **B**. Gọi $(\overline{h}, \overline{r}, \overline{s})$ là dữ liệu được lưu trong các lược

đồ chữ ký số được phát hành từ **B**. Sẽ tồn tại hai giá trị ngẫu nhiên α, β liên kết $(\bar{h},\bar{r},\bar{s})$ tới (M,r,s).

Từ mô tả trong các lược đồ, có các liên kết sau:

$\bar{h} = \alpha h \bmod p$; $s = (\beta\alpha^{-1}\bar{s} + \alpha h) \bmod q$ và $\bar{r} = (r\beta^{-1}\alpha) \bmod q$

Theo các liên kết trên tính được: $\alpha = \bar{h}h^{-1}$ và $\beta = (s - \bar{h})\bar{h}h^{-1}\bar{s}^{-1}$

Thay α, β vừa tính ở trên vào phương trình tính $\bar{r}$, thu được *r* như sau:

$$\bar{r} = (r\beta^{-1}\alpha) \bmod q \Rightarrow r = \bar{r}(s - \bar{h})\bar{s}^{-1} \bmod q \qquad (2.2)$$

Từ (2.2) cho thấy, *r* luôn có mối quan hệ xác định là hằng số và không phụ thuộc vào hai hệ số α, β. Do đó, khi chọn $(M,r,s) \in \{(M_0,r_0,s_0),(M_1,r_1,s_1)\}$ với dữ liệu lưu trữ trong lược đồ phát hành của **B** là $(\bar{h}_i,\bar{r}_i,\bar{s}_i)$ (với *i*=0,1) thì luôn tồn tại cặp α, β thỏa mãn điều kiện.

Với xác suất lớn nhất lựa chọn đúng để $b' = b$ trong tập chữ ký phát hành lựa chọn $(M,r,s) \in \{(M_0,r_0,s_0),(M_1,r_1,s_1)\}$ là $\frac{1}{2}$, hay $\Pr[b = b'] = \frac{1}{2}$, tức là biểu thức $\left|\Pr[b = b'] - \frac{1}{2}\right| < \frac{1}{p^c}$ là đúng, thỏa mãn điều kiện trong định nghĩa 1.1. Do đó, các lược đồ đề xuất là mù vô điều kiện.

Hay có thể nói rằng người ký thông điệp không thể biết nội dung thông điệp vì thông điệp được băm ra và kết hợp với giá trị ngẫu nhiên α được lựa chọn bởi người yêu cầu như là $h = H(M)$ và $\bar{h} = \alpha h \bmod p$. Do đó mà bên ký không biết gì về nội dung thông điệp đã ký.

2) Tính chống giả mạo: Lược đồ chữ ký số tập thể mù đề xuất có bộ tham số $(\varepsilon, t, q_h, q_e, q_s)$ gọi là an toàn trong ROM nếu tồn tại (ε', t')-DL trong Z_p, với:

$$\varepsilon' = (1 - \frac{q_h(q_e + q_s)}{q})(1 - \frac{1}{q})\frac{1}{q_h}\varepsilon; \quad t' = t + O(q_e + q_s)E$$

Trong đó, (q_h, q_e, q_s) lần lượt là số truy vấn của hàm băm, trích xuất và tạo chữ ký mù; E là thời gian thực hiện các phép tính luỹ thừa modulo.

Chứng minh: Sử dụng các kết quả trình bày trong định nghĩa 1.2 của chương 1 để chứng minh.

Giả sử tồn tại một kẻ giả mạo **A**, xây dựng thuật toán B để giúp **A** giải bài toán DLP với phần tử sinh *g*, số nguyên tố *p* và $\rho' \in Z_p$, **B** được yêu cầu phải tìm $x \in Z_q$ sao cho $\rho' = g^x \bmod p$.

B thực hiện như sau: Chọn hàm băm thông điệp $h = H \in \{0,1\}^* \to Z_q$, gửi tham số công khai (p, q, g, ρ', h) tới **A**. **B** chọn hai giá trị ngẫu nhiên (*k′,d′*) và tính *c**:

$$c^* = (\rho')^{k'} g^{d'} \bmod p. \qquad (2.3)$$

d′ được xem như là khoá riêng của người ký, *k′* là giá trị được chọn ngẫu nhiên và *(k′,d′,c*)* là kết quả đầu ra. ***A*** được phép truy vấn tới phần truy xuất oracle để có một khoá riêng *d′* của thông điệp *M*. Đầu tiên ***B*** kiểm tra xem *d′* đã được sử dụng cho truy vấn trong các phần cài đặt trước chưa, nếu *d′* đã được sử dụng rồi thì ***B*** lấy bộ *(c*,k′,d′,h)* từ bảng được lưu để ký thông điệp *M* theo pha tạo chữ ký được mô tả trong lược đồ, đầu ra của thuật toán ký là $(M, \vec{r}', \vec{s}')$. Nếu *d′* chưa được sử dụng trong phần cài đặt trước thì B thực hiện lại các mô phỏng và chọn lại khoá bí mật *d′* cho đến khi thỏa mãn.

Cuối cùng, **A** tạo ra chữ ký số giả mạo là $s_1^* = (h, \vec{r}', \vec{s}_1')$ trên M bởi khoá bí mật *d′*. B lại thực hiện lần nữa bằng cách giữ nguyên $(h, \vec{r}')$ và lại yêu cầu **A** ký tiếp và thu được $s_2^* = (h, \vec{r}', \vec{s}_2')$. **A** có được s_j^* (với *j*=1,2) được tính như sau:

Từ $c^* = g^{s_j^*/h} \rho^{-r/h} \bmod p$ với $\rho = g^{d'} \bmod p$, thay vào (2.3), tính được:

$$(\rho')^{k'} g^{d'} \bmod p = g^{s_j^*/h} \rho^{-r/h} \bmod p$$
$$\Rightarrow g^{xk'+d'} = g^{s_j^* h^{-1} - rh^{-1}d'}$$
$$\Rightarrow xk' + d' = s_j^* h^{-1} - rh^{-1}d'$$
$$\Rightarrow s_j^* = h(xk' + d') + rd'$$

Thuật toán **B** chưa biết (*x*, *r*) trong các phương trình trên nên để thu được *x* thì B phải giải phương trình tuyến tính có hai ẩn số hoặc phải giải bài toán DLP.

Phân tích xác suất: Xác suất thực hiện không thành công lớn nhất việc gán giá trị hàm băm $h = H \in \{0,1\}^* \to Z_q$ bằng $\frac{q_h}{q}$ được mô phỏng thực hiện trong $(q_e + q_s)$ lần. Hay $(1 - \frac{q_h}{q})^{q_e+q_s} \geq 1 - \frac{q_h(q_e+q_s)}{q}$.

B có thể xác định chính xác vị trí giá trị hàm băm là $\frac{1}{q_h}$. Do tính ngẫu nhiên lý tưởng của mô hình ROM nên tồn tại chữ ký *s* với xác suất ít nhất là $(1 - \frac{1}{q})$. Như vậy, xác suất thành công là $\varepsilon' = (1 - \frac{q_h(q_e+q_s)}{q})(1 - \frac{1}{q})\frac{1}{q_h}\varepsilon$, và độ phức tạp về thời gian của thuật toán B dựa trên hàm mũ được thực hiện chủ yếu trong pha trích xuất và tạo chữ ký, và là $t' = t + O(q_e + q_s)E$.

2.1.2. Lược đồ chữ ký số tập thể mù dựa trên lược đồ Schnorr

2.1.2.1. Xây dựng lược đồ

Phần này đề xuất lược đồ chữ ký số tập thể mù dựa trên lược đồ chữ ký số đơn Schnorr, được ký hiệu là LĐ 2.02. Lược đồ được trình bày như sau:

1) Thiết lập: Mỗi người ký trong tập thể người ký **B** tính khoá công khai ρ_i của mình và gửi cho TTP để tính khoá công khai tập thể ρ như sau:

$$\rho_i = g^{d_i} \bmod p, i = 1,2,...,n; \quad \rho = \prod_{i=1}^{n} \rho_i \bmod p$$

2) Trích xuất: Mỗi người ký trong **B** chọn một giá trị ngẫu nhiên k_i với $k_i \in Z_q^*$, tính c_i và gửi tới TTP để tính $\overline{c}$, $\overline{c}$ được gửi tới người yêu cầu **A**, với:

$$c_i = g^{k_i} \bmod p, i = 1,2,...,n; \quad \overline{c} = \prod_{i=1}^{n} c_i \bmod p = g^{\sum_{i=1}^{n} k_i \bmod q} \bmod p$$

3) Làm mù: Người yêu cầu **A** chọn hai giá trị ngẫu nhiên $\alpha, \beta \in \{1,2,...,q\text{-}1\}$ và tính $h = H(M \| c)$ và $\overline{r}$ như sau:

$$c = \overline{c} g^{\alpha} \rho^{\beta} \bmod p; r = h \bmod q; \overline{r} = (r - \beta) \bmod q$$

Người yêu cầu gửi $\overline{r}$ tới mỗi người ký trong **B**.

4) Tạo chữ ký: Mỗi người ký trong **B** nhận $\overline{r}$ từ **A** và tính chữ ký riêng của mình là s_i: $s_i = k_i - d_i \overline{r} \bmod q$, và gửi tới TTP để tính chữ ký số chung của tập thể **B** là $\overline{s}$: $\overline{s} = \sum_{i=1}^{n} s_i \bmod q$, và gửi $\overline{s}$ tới **A**.

5) Giải mù: Người yêu cầu **A** tính *s* theo công thức: $s = (\overline{s} + \alpha) \bmod q$

Cặp (r, s) là chữ ký số của tập thể người ký **B** trên thông điệp *M*.

6) Kiểm tra chữ ký: Tính c' và r' theo công thức (2.4) và so sánh r' với *r*, nếu $r' = r$ thì chữ ký được chấp nhận, ngược lại thì chữ ký không được chấp nhận.

$$c' = g^s \rho^r \bmod p; \quad r' = H(M \| c') \bmod q \qquad (2.4)$$

Thật vậy, có thể chứng minh như sau:

$$
\begin{aligned}
c' &= g^{s}\rho^{r} \bmod p \\
&= g^{\bar{s}+\alpha}\rho^{\bar{r}+\beta} \bmod p = g^{\bar{s}+\alpha}\rho^{\bar{r}+\beta} \bmod p \\
&= g^{\sum_{i=1}^{n}(k_i - d_i\bar{r})+\alpha} \; g^{\bar{r}\sum_{i=1}^{n} d_i}\rho^{\beta} \bmod p \\
&= g^{\sum_{i=1}^{n}(k_i - d_i\bar{r})+\alpha+\bar{r}\sum_{i=1}^{n} d_i}\rho^{\beta} \bmod p \\
&= \bar{c}g^{\alpha}\rho^{\beta} \bmod p = c \\
\Rightarrow r' &= H(M\|c') = r
\end{aligned}
$$

Vậy $r' = r$ đã được chứng minh hay chữ ký đã được xác thực.

Người yêu cầu **A** (M)	Dữ liệu	Tập thể người ký **B** (p, q, $\rho, \bar{c}$)
Chọn: $\alpha, \beta \in \{1, 2, ..., q-1\}$ $h = H(M\|c)$; $c = \bar{c}g^{\alpha}\rho^{\beta} \bmod p$ $r = h \bmod q$ $\bar{r} = (r - \beta) \bmod q$ $s = (\bar{s} + \alpha) \bmod q$ Chữ ký số là cặp: (r,s)	← Công khai (p, q, $\rho, \bar{c}$) $\bar{r}$ → $\bar{s}$ ←	$s_i = k_i - d_i\bar{r} \bmod q$ $\bar{s} = \sum_{i=1}^{n} s_i \bmod q$

Hình 2.2. Tóm tắt thuật toán ký số của LĐ 2.02

2.1.2.2. Đánh giá tính an toàn của lược đồ đề xuất

Lược đồ chữ ký số tập thể mù an toàn và được xác định bởi hai đặc trưng là tính mù và tính không thể giả mạo.

1) Tính mù: Các lược đồ chữ ký số tập thể mù đề xuất đảm bảo tính mù.

Chứng minh: Sử dụng các điều kiện trong định nghĩa 1.1 của chương 1 để chứng minh.

Lấy bộ chữ ký $(M, r, s) \in \{(M_0, r_0, s_0), (M_1, r_1, s_1)\}$ là một trong hai bộ chữ ký số được gửi đến người ký B. Gọi $(\bar{r}, \bar{s})$ là dữ liệu được lưu trong các lược đồ chữ

ký số được phát hành từ B. Sẽ tồn tại hai giá trị ngẫu nhiên α, β liên kết $(\overline{r}, \overline{s})$ tới (M, r, s). Từ mô tả trong các lược đồ, có các liên kết sau:

$\overline{r} = (r - \beta) \bmod q$; $s = (\overline{s} + \alpha) \bmod q$; $c = \overline{c} g^{\alpha} \rho^{\beta} \bmod p$ và $r = h \bmod q$

Theo các liên kết trên thì tính được: $\beta = r - \overline{r}$ và $\alpha = s - \overline{s}$

Thay α, β vừa tính ở trên vào phương trình tính c, thu được:

$$c = \overline{c} g^{s-\overline{s}} \rho^{r-\overline{r}} \bmod p \qquad (2.5)$$

Từ $r = H(M \,||\, c) \bmod q$ và (2.5), có thể nhận thấy là r luôn có mối quan hệ xác định là hằng số và không phụ thuộc vào hai hệ số α, β. Do đó mà khi chọn $(M, r, s) \in \{(M_0, r_0, s_0), (M_1, r_1, s_1)\}$ với dữ liệu lưu trữ trong lược đồ phát hành của B là $(\overline{r_i}, \overline{s_i})$ (với i=0,1) thì luôn tồn tại cặp α, β thỏa mãn điều kiện.

Với xác suất lớn nhất lựa chọn đúng để $b' = b$ trong tập chữ ký phát hành lựa chọn $(M, r, s) \in \{(M_0, r_0, s_0), (M_1, r_1, s_1)\}$ là $\frac{1}{2}$, hay $\Pr[b = b'] = \frac{1}{2}$, tức là biểu thức $\left|\Pr[b = b'] - \frac{1}{2}\right| < \frac{1}{p^c}$ là đúng, thỏa mãn điều kiện trong định nghĩa 1.1. Do đó, các lược đồ đề xuất là mù vô điều kiện.

Hay có thể nói rằng người ký thông điệp không thể biết nội dung thông điệp vì thông điệp được băm ra và kết hợp với các giá trị ngẫu nhiên (α, β) được lựa chọn bởi người yêu cầu như là $r = H(M \,||\, c)$ và $c = \overline{c} g^{\alpha} \rho^{\beta} \bmod p$. Do đó mà bên ký không biết gì về nội dung thông điệp đã ký.

2) Tính chống giả mạo: Lược đồ chữ ký số tập thể mù đề xuất có bộ tham số $(\varepsilon, t, q_h, q_e, q_s)$ gọi là an toàn trong ROM nếu tồn tại (ε', t')-DL trong Z_p, với:

$$\varepsilon' = (1 - \frac{q_h(q_e + q_s)}{q})(1 - \frac{1}{q})\frac{1}{q_h}\varepsilon; \quad t' = t + O(q_e + q_s)E$$

Trong đó, (q_h, q_e, q_s) lần lượt là số truy vấn của hàm băm, trích xuất và tạo chữ ký mù; E là thời gian thực hiện các phép tính luỹ thừa modulo.

Chứng minh: Sử dụng các kết quả trình bày trong định nghĩa 1.2 của chương 1 để chứng minh.

Giả sử là tồn tại một kẻ giả mạo **A**, xây dựng thuật toán **B** để giúp **A** giải bài toán DLP với phần tử sinh *g*, số nguyên tố *p* và $\rho' \in Z_p$, **B** được yêu cầu phải tìm $x \in Z_q$ sao cho $\rho' = g^x \bmod p$.

B thực hiện như sau: chọn hàm băm thông điệp $r' = H \in \{0,1\}^* \to Z_q$, gửi tham số công khai (p, q, g, ρ', r') tới **A**. **B** chọn hai số ngẫu nhiên (*k′,d′*) và tính *c**:

$$c^* = \rho' \rho^{k'} g^{d'} \bmod p \qquad (2.6)$$

d' được xem như là khoá riêng của người ký, k' là giá trị được chọn ngẫu nhiên và *(k′,d′,c*)* là kết quả đầu ra. ***A*** được phép truy vấn tới phần truy xuất oracle để có một khoá riêng d' của thông điệp *M*. Đầu tiên ***B*** kiểm tra xem d' đã được sử dụng cho truy vấn trong các phần cài đặt trước chưa, nếu d' đã được sử dụng rồi thì ***B*** lấy bộ (c^*, k', d', r') từ bảng được lưu để ký thông điệp *M* theo pha tạo chữ ký được mô tả trong lược đồ, đầu ra của thuật toán ký là $(M, \vec{r}', \vec{s}')$. Nếu d' chưa được sử dụng trong phần cài đặt trước thì B thực hiện lại các mô phỏng và chọn lại khoá bí mật d' cho đến khi thỏa mãn.

Cuối cùng, **A** tạo ra chữ ký số giả mạo là $s_1^* = (r', \vec{s}_1')$ trên M bởi khoá bí mật d'. **B** lại thực hiện lần nữa bằng cách giữ nguyên r' và lại yêu cầu **A** ký tiếp và thu được $s_2^* = (r', \vec{s}_2')$.

s_j^* $(j = 1, 2)$ được tính như sau:

Từ: $c^* = g^s \rho^r \bmod p$ với $\rho = g^{d'} \bmod p$, thay vào (2.6), tính được:

$$\rho'\rho^{k'} g^{d'} \bmod p = g^{s_j^*} \rho^r \bmod p$$
$$\Rightarrow g^{x+d'k'+d'} = g^{s_j^*+rd'}$$

$$\Rightarrow x + d'k' + d' = s_j^* + rd'$$
$$\Rightarrow s_j^* = x + k'd' + d' - rd'$$

Thuật toán **B** chưa biết (*x*, *r*) trong các phương trình trên. Để thu được *x* thì **B** phải giải phương trình tuyến tính có hai ẩn số hoặc phải giải bài toán DLP.

Phân tích xác suất: Xác suất thực hiện không thành công lớn nhất việc gán giá trị hàm băm $r' = H \in \{0,1\}^* \to Z_q$ bằng $\frac{q_h}{q}$ được mô phỏng thực hiện trong $(q_e + q_s)$ lần. Ta có $(1-\frac{q_h}{q})^{q_e+q_s} \geq 1-\frac{q_h(q_e+q_s)}{q}$.

B có thể xác định chính xác vị trí chọn giá trị hàm băm là $(1/q_h)$. Do tính ngẫu nhiên lý tưởng của mô hình ROM, nên tồn tại chữ ký *s* với xác suất ít nhất là $(1-\frac{1}{q})$. Như vậy, xác suất thành công là $\varepsilon' = (1-\frac{q_h(q_e+q_s)}{q})(1-\frac{1}{q})\frac{1}{q_h}\varepsilon$, và độ phức tạp về thời gian của thuật toán **B** dựa trên hàm mũ được thực hiện chủ yếu trong pha trích xuất và tạo chữ ký, và là $t' = t + O(q_e + q_s)E$.

2.1.3. Đánh giá độ phức tạp thời gian của các lược đồ đề xuất

Phần này so sánh độ phức tạp thời gian của lược đồ LĐ 2.01 với lược đồ [73] và lược đồ LĐ 2.02 với lược đồ [72] với giả định là các lược đồ đó được tính toán với cùng tham số an toàn trong Z_p và số thành viên của tập thể người ký là *n*. NCS lựa chọn lược đồ chữ ký số tập thể mù trong [73] để so sánh với lược đồ đề xuất do lược đồ trong [73] cũng xây dựng bằng cách sử dụng độ khó của bài toán logarit rời rạc, dựa trên chuẩn chữ ký số GOST R34.10, tuy nhiên sử dụng các phương trình tạo chữ ký số khác với lược đồ đề xuất và chưa được đánh giá độ an toàn trong mô hình đánh giá độ an toàn chuẩn như ROM,… (*lược đồ đề xuất của NCS được chứng minh độ an toàn trong mô hình ROM*). Ngoài ra, lược đồ [73] sử dụng bốn tham số

làm mù nên độ phức tạp tính toán cao hơn lược đồ NCS đề xuất (*sử dụng hai tham số mù*). Kết quả so sánh được trình bày bên dưới.

Trong phần so sánh này, quy ước ký hiệu: T_h là chi phí thời gian thực hiện hàm băm; T_{inv} là chi phí thời gian thực hiện phép nghịch đảo; T_m là chi phí thời gian thực hiện phép nhân modulo; T_e là chi phí thời gian thực hiện phép luỹ thừa; tất cả thực hiện trong Z_p.

Theo [26], có ước lượng: $T_h \approx T_m$; $T_{inv} \approx 240T_m$; $T_e \approx 21T_m$, trên cơ sở các phép tính trong các phương trình của lược đồ đề xuất và lược đồ được trình bày trong [73] quy đổi về độ phức tạp thời gian của phép tính nhân T_m tại các bảng 2.1, 2.2 và có các kết quả so sánh như trong các bảng 2.3 bên dưới.

Bảng 2.1. Độ phức tạp thời gian của lược đồ LĐ 2.01

Loại phép tính	Lược đồ dựa trên chuẩn GOST R34.10-94 (LĐ 2.01)			
	Làm mù	Tạo chữ ký	Giải mù	Kiểm tra
Phép tính luỹ thừa	2			1
Phép tính nghịch đảo	1		1	1
Phép tính hàm băm	1			
Phép tính nhân	4	$2n$	3	3
Quy đổi ra T_m	$287T_m$	$2nT_m$	$243T_m$	$264T_m$
Tổng chi phí thời gian	$(794+2n)T_m$			

Bảng 2.2. Độ phức tạp thời gian của lược đồ [73]

Loại phép tính	Lược đồ [73]			
	Làm mù	Tạo chữ ký	Giải mù	Kiểm tra
Phép tính luỹ thừa	3			1
Phép tính nghịch đảo	1		2	1
Phép tính hàm băm	1			
Phép tính nhân	6	$2n$	3	1
Quy đổi ra T_m	$310T_m$	$2nT_m$	$483T_m$	$264T_m$
Tổng chi phí thời gian	$(1057+2n)T_m$			

Bảng 2.3. So sánh độ phức tạp thời gian của lược đồ LĐ 2.01 và lược đồ [73]

	Lược đồ LĐ 2.01	[73]
Làm mù	$287T_m$	$310T_m$
Tạo chữ ký	$2nT_m$	$2nT_m$
Giải mù	$243T_m$	$483T_m$
Kiểm tra chữ ký	$264T_m$	$264T_m$
Tổng cộng	$(794+2n)T_m$	$(1057+2n)T_m$

Từ bảng 2.3 cho thấy độ phức tạp thời gian của lược đồ chữ ký số tập thể mù dựa trên chuẩn GOST R34.10-94 là thấp hơn trong [73].

Phần này so sánh lược đồ LĐ 2.02 với lược đồ [72]. NCS chọn lược đồ chữ ký số tập thể mù trong [72] để so sánh với lược đồ đề xuất do lược đồ trong [72] cũng xây dựng bằng cách sử dụng độ khó của bài toán logarit rời rạc, sử dụng hai tham số làm mù giống như lược đồ đề xuất, tuy nhiên sử dụng các phương trình tạo chữ ký số khác với lược đồ đề xuất. Kết quả so sánh được trình bày như bên dưới.

Bảng 2.4. Độ phức tạp thời gian của lược đồ LĐ 2.02

Loại phép tính	Lược đồ dựa trên lược đồ Schnorr (LĐ 2.02)			
	Làm mù	Tạo chữ ký	Giải mù	Kiểm tra
Phép tính luỹ thừa	2			2
Phép tính nghịch đảo				
Phép tính hàm băm	1			1
Phép tính nhân	2	n		1
Quy đổi ra T_m	$45T_m$	nT_m	Không đáng kể	$44T_m$
Tổng chi phí thời gian	$(89+n)T_m$			

Bảng 2.5. Độ phức tạp thời gian của lược đồ [72]

Loại phép tính	Lược đồ [72]			
	Làm mù	Tạo chữ ký	Giải mù	Kiểm tra
Phép tính luỹ thừa	2			2
Phép tính nghịch đảo				1
Phép tính hàm băm	1			
Phép tính nhân		n		1
Quy đổi ra T_m	$45T_m$	nT_m	Không đáng kể	$262T_m$
Tổng chi phí thời gian	$(307+n)T_m$			

Bảng 2.6. So sánh độ phức tạp thời gian của lược đồ LĐ 2.02 và lược đồ [72]

	Lược đồ dựa trên Schnorr (LĐ 2.02)	[72]
Làm mù	$45T_m$	$45T_m$
Tạo chữ ký	nT_m	nT_m
Giải mù	Không đáng kể	Không đáng kể
Kiểm tra chữ ký	$44T_m$	$262T_m$
Tổng cộng	$(89+n)T_m$	$(307+n)T_m$

Bảng 2.6 cho thấy độ phức tạp thời gian của lược đồ chữ ký số tập thể mù dựa trên Schnorr thấp hơn trong [72].

Tiếp theo là phần so sánh độ phức tạp tính toán của hai lược đồ đề xuất cùng dựa trên độ khó của bài toán DLP là LĐ 2.01 và LĐ 2.02.

Theo bảng 2.7 thì độ phức tạp thời gian của lược đồ chữ ký số tập thể mù dựa trên chuẩn GOST R34.10-94 là cao hơn các lược đồ chữ ký số dựa trên Schnorr. Phát hiện này phù hợp với các đánh giá so sánh giữa chuẩn GOST R34.10-94 và lược đồ chữ ký số Schnorr, nên có thể nghiên cứu ứng dụng trong các ứng dụng có yêu cầu phần cứng tính toán thấp như thiết bị IoT,…

Bảng 2.7. Chi phí thời gian của LĐ 2.01 và LĐ 2.02

	LĐ 2.01	LĐ 2.02
Làm mù	$287T_m$	$45T_m$
Tạo chữ ký	$2nT_m$	nT_m
Giải mù	$243T_m$	Không đáng kể
Kiểm tra chữ ký	$264T_m$	$44T_m$
Tổng cộng	$(794+2n)T_m$	$(89+n)T_m$

2.2. ĐỀ XUẤT LƯỢC ĐỒ CHỮ KÝ SỐ TẬP THỂ MÙ DỰA TRÊN CHUẨN CHỮ KÝ SỐ GOST R34.10-2012 VÀ LƯỢC ĐỒ EC-SCHNORR

Ưu điểm của hệ mật ECC so với các hệ mật khóa công khai khác là ECC cung cấp các thuộc tính an toàn có thể so sánh với các hệ mật khóa công khai truyền thống mặc dù độ dài khóa nhỏ hơn gấp nhiều lần. Do đó, việc cài đặt ECC tiêu tốn ít tài nguyên hệ thống và năng lượng hơn. Do lợi thế về độ dài khóa nhỏ, ECC đã được áp dụng rộng rãi trong nhiều lĩnh vực.

Trong phần này đề xuất 2 lược đồ chữ ký số tập thể mù dựa trên chuẩn GOST R34.10-2012 và lược đồ EC-Schnorr. Sau đó so sánh với một số lược đồ đã công bố, qua đó đề xuất hướng ứng dụng cho các lược đồ đề xuất.

Chuẩn chữ ký số GOST R34.10-2012 và lược đồ EC-Schnorr mô tả các lược đồ chữ ký số đơn. Cải tiến ở đây là dựa trên chuẩn và lược đồ phổ biến này, đề xuất phương pháp để xây dựng các lược đồ chữ ký số tập thể mù hiệu quả từ chữ ký số đơn. Qua đó có thể sử dụng được trong các ứng dụng yêu cầu nhiều người ký (dạng chữ ký tập thể) và cần tính ẩn danh (tính mù). Lược đồ đề xuất được mô tả như sau:

2.2.1. Lược đồ chữ ký số tập thể mù dựa trên chuẩn GOST R34.10-2012

2.2.1.1. Xây dựng lược đồ

Phần này đề xuất lược đồ chữ ký số tập thể mù dựa trên chuẩn GOST R34.10-2012, được ký hiệu là LĐ 2.03. Lược đồ được trình bày như sau:

1) Cài đặt: Mỗi người ký trong tập thể **B** tính khóa công khai của mình và gửi đến TTP để tính khóa công khai tập thể *P* như sau:

$$P_i = d_i \times G\,;\, P = P_1 + P_2 + ... + P_n = \sum_{i=1}^{n} d_i \times G \text{ với } i=1,2,...,n$$

Mỗi người ký trong **B** chọn ngẫu nhiên giá trị k_i với $k_i \in Z_q$ và tính C_i sau đó gửi đến TTP để tính $\overline{C}$ như sau: $C_i = k_i \times G \text{ với } i=1,2...n$ và $\overline{C} = \sum_{i=1}^{n} C_i = \sum_{i=1}^{n} k_i \times G$, và gửi $\overline{C}$ đến người yêu cầu **A**.

2) Làm mù: **A** chọn ngẫu nhiên 2 giá trị $\alpha, \beta \in \{1,2,...,q-1\}$ và tính:

$$\begin{cases} h = H(M); e = h \bmod q; \overline{e} = \alpha e \bmod q \\ C = \beta \times \overline{C} + \alpha \times G \\ r = x_C \bmod q; \overline{r} = (r\beta^{-1}\alpha) \bmod q \end{cases}$$

A gửi $(\overline{r}, \overline{e})$ tới **B**.

3) Tạo chữ ký: Mỗi người ký trong **B** tính s_i và gửi TTP để tính $\overline{s}$ và gửi tới **A** như: $s_i = k_i\overline{e} + d_i\overline{r} \bmod q;\ \overline{s} = \sum_{i=1}^{n} s_i \bmod q$.

4) Giải mù: Người yêu cầu **A** tính *s*: $s = (\beta\alpha^{-1}\overline{s} + \alpha e) \bmod q$

Cặp (r, s) là chữ ký số tập thể mù của tập thể **B** trên thông điệp *M*.

5) Kiểm tra chữ ký: Tính C', r' và so sánh, nếu $r' = r$ thì chữ ký được chấp nhận, ngược lại thì chữ ký không được chấp nhận, với:

$$C' = (se^{-1} \bmod q) \times G - (re^{-1} \bmod q) \times P \text{ và } r' = x_{C'} \bmod q$$

Thật vậy, có thể chứng minh như sau:

Với $s_i \times G = ((k_i\overline{e} + d_i\overline{r}) \bmod q) \times G$, tính $C_i, \overline{C}$ như sau:

$$C_i = k_i \times G = (s_i \overline{e}^{-1} \bmod q) \times G - (d_i \overline{re}^{-1} \bmod q) \times G;$$

$$\overline{C} = \sum_{i=1}^{m} C_i = \overline{e}^{-1} \sum_{i=1}^{m} (s_i \bmod q) \times G - \overline{re}^{-1} \sum_{i=1}^{m} (d_i \bmod q) \times G;$$

$$= (\overline{se}^{-1} \bmod q) \times G - (\overline{re}^{-1} \bmod q) \times P$$

Từ: $\overline{r} = (r\beta^{-1}\alpha) \bmod q \Rightarrow r = \overline{r}\beta\alpha^{-1} \bmod q$, thay vào biểu thức tính C':

$$C' = (se^{-1} \bmod q) \times G - (re^{-1} \bmod q) \times P;$$

$$= ((\alpha e + \beta \overline{s} \alpha^{-1}) e^{-1} \bmod q) \times G - ((\overline{r}\beta\alpha^{-1}e^{-1}) \bmod q) \times P;$$

$$= \beta((\overline{se}^{-1} \bmod q) \times G - (\overline{re}^{-1} \bmod q) \times P) + (\alpha \bmod q) \times G;$$

$$= \beta \times \overline{C} + \alpha \times G = C$$

Hay $r' = r$, vậy $r' = r$ đã được chứng minh hay chữ ký đã được xác thực.

Người yêu cầu **A** (M)	Dữ liệu	Tập thể người ký **B** (p, q, G, P, $\overline{C}$)
Chọn: $\alpha, \beta \in \{1, 2, ..., q-1\}$	←	Công khai (p, q, G, P, $\overline{C}$)
$h = H(M)$		
$e = h \bmod q$		
$\overline{e} = \alpha e \bmod q$		
$C = \beta \times \overline{C} + \alpha \times G$		
$r = x_C \bmod q$		
$\overline{r} = (r\beta^{-1}\alpha) \bmod q$	$\overline{e}, \overline{r}$ →	$s_i = k_i \times \overline{e} + d_i \times \overline{r} \bmod q$
		$\overline{s} = \sum_{i=1}^{n} s_i \bmod q$
	$\overline{s}$ ←	
$s = (\beta\alpha^{-1}\overline{s} + \alpha e) \bmod q$		
Chữ ký số là cặp: (r, s)		

Hình 2.3. Tóm tắt thuật toán ký số của LĐ 2.03

2.2.1.2. Đánh giá tính an toàn của các lược đồ đề xuất

1) Tính mù: Các lược đồ chữ ký số tập thể mù đề xuất đảm bảo tính mù.

Chứng minh: Sử dụng các điều kiện trong định nghĩa 1.1 của chương 1 để chứng minh.

Lấy bộ chữ ký $(M,r,s) \in \{(M_0,r_0,s_0),(M_1,r_1,s_1)\}$ là một trong hai bộ chữ ký số được gửi đến người ký B. Gọi $(\overline{e},\overline{r},\overline{s})$ là dữ liệu được lưu trong các lược đồ chữ ký số được phát hành từ **B**. Sẽ tồn tại hai giá trị ngẫu nhiên *α, β* liên kết $(\overline{e},\overline{r},\overline{s})$ tới (M,r,s). Từ mô tả trong các lược đồ, có các liên kết sau:

$\overline{e} = \alpha e \bmod q$, $\overline{r} = (r\beta^{-1}\alpha) \bmod q$ và $s = (\beta\alpha^{-1}\overline{s} + \alpha e) \bmod q$

Theo các liên kết trên tính được: $\alpha = \overline{e}e^{-1}$ và $\beta = (s-\overline{e})\overline{e}e^{-1}\overline{s}^{-1}$

Thay α, β vừa tính ở trên vào phương trình tính $\overline{r}$, thu được *r* như sau:

$$\overline{r} = (r\beta^{-1}\alpha) \bmod q \Rightarrow r = \overline{r}(s-\overline{e})\overline{s}^{-1} \bmod q \qquad (2.7)$$

Từ (2.7) cho thấy là *r* luôn có mối quan hệ xác định là hằng số và không phụ thuộc vào hai hệ số α, β, nên khi chọn $(M,r,s) \in \{(M_0,r_0,s_0),(M_1,r_1,s_1)\}$ với dữ liệu lưu trữ trong lược đồ phát hành của **B** là $(\overline{e}_i,\overline{r}_i,\overline{s}_i)$ (với *i*=0,1) thì luôn tồn tại cặp α, β thỏa mãn điều kiện.

Với xác suất lớn nhất lựa chọn đúng để $b' = b$ trong tập chữ ký phát hành lựa chọn $(M,r,s) \in \{(M_0,r_0,s_0),(M_1,r_1,s_1)\}$ là $\frac{1}{2}$, hay $\Pr[b = b'] = \frac{1}{2}$, tức là biểu thức $\left|\Pr[b = b'] - \frac{1}{2}\right| < \frac{1}{p^c}$ là đúng, thỏa mãn điều kiện trong định nghĩa 1.1. Do đó, các lược đồ đề xuất là mù vô điều kiện.

Hay có thể nói rằng, đối với các lược đồ chữ ký số tập thể mù dựa trên chuẩn GOST R34.10-2012, người ký không thể biết nội dung thông điệp vì thông điệp được băm ra và kết hợp với các giá trị (α,β) được lựa chọn ngẫu nhiên bởi người yêu cầu như là $h = H(M)$, $e = h \bmod q$, $\overline{e} = \alpha e \bmod q$. Do vậy mà bên ký không thể biết nội dung thông điệp mà mình đã ký.

2) Tính chống giả mạo: Lược đồ chữ ký số tập thể mù đề xuất có bộ tham số $(\varepsilon, t, q_h, q_e, q_s)$ được gọi là an toàn trong ROM nếu tồn tại (ε', t')-ECDL trong trường *GF*(*p*), với:

$$\varepsilon' = (1 - \frac{q_h(q_e + q_s)}{q})(1 - \frac{1}{q})\frac{1}{q_h}\varepsilon; \quad t' = t + O(q_e + q_s)E$$

Trong đó, (q_h, q_e, q_s) lần lượt là số truy vấn của hàm băm, trích xuất và tạo chữ ký mù; E là thời gian thực hiện các phép tính luỹ thừa modulo trong *GF*(*p*).

Chứng minh: Sử dụng các kết quả trình bày trong định nghĩa 1.2 của chương 1 để chứng minh.

Giả sử là tồn tại một kẻ giả mạo **A**, xây dựng thuật toán **B** để giúp **A** giải bài toán logarit rời rạc. **B** được cho là một nhóm nhân *G* trong *GF*(*p*) với thành phần *G*, số nguyên tố *q* và điểm *Q* trên đường cong elliptic. **B** được yêu cầu tìm giá trị $x \in Z_q$ sao cho $Q = x \times G$.

B tiến hành như sau: chọn hàm băm thông điệp $e = H \in \{0,1\}^* \to Z_q$, gửi các tham số công khai (p, G, Q, e) tới **A**. **B** chọn hai số ngẫu nhiên (*k′,d′*) và tính *C**:

$$C^* = k' \times Q + d' \times G \qquad (2.8)$$

d′ được xem như là khoá riêng của người ký, *k′* là giá trị được chọn ngẫu nhiên và *(k′,d′,C*)* là kết quả đầu ra. **A** truy vấn tập Oracle của chữ ký số với thông điệp *M* và khoá riêng *d′*. Đầu tiên, **B** kiểm tra xem *d′* đã được sử dụng cho truy vấn trong các phần cài đặt trước chưa. Nếu *d′* đã được sử dụng rồi thì **B** lấy bộ (C^*, k', d', e) *(C*,k′,d′,e)* từ bảng được lưu để ký thông điệp *M* theo pha tạo chữ ký được mô tả trong lược đồ. Đầu ra của thuật toán ký là $(M, \vec{r}', \vec{s}')$. Nếu d' chưa được sử dụng trong các phần cài đặt trước thì **B** thực hiện lại các mô phỏng và chọn lại khoá bí mật *d′* cho đến khi thỏa mãn.

Cuối cùng, **A** tạo ra chữ ký số giả mạo là $s_1^* = (e, \overline{r}', \overline{s}_1')$ trên M bởi khoá bí mật d'. **B** lại thực hiện lần nữa bằng cách giữ nguyên $(e, \overline{r}')$ và lại yêu cầu **A** ký tiếp và thu được $s_2^* = (e, \overline{r}', \overline{s}_2')$.

Với $C^* = (se^{-1} \bmod q) \times G - (re^{-1} \bmod q) \times P;\ P = d \times G$

Thay vào (2.8), tính được:

$$k' \times Q + d' \times G = (s_j^* e^{-1} \bmod q) \times G - (re^{-1} \bmod q) \times P$$
$$\Rightarrow k'x \times G + d' \times G = (s_j^* e^{-1} \bmod q) \times G - (re^{-1} \bmod q) d' \times G$$
$$\Rightarrow s_j^* = e(k'x + d') + rd'$$

với j=1,2.

Thuật toán **B** chưa biết (x, r) nên để thu được x thì **B** phải giải phương trình tuyến tính có hai ẩn số hoặc phải giải bài toán ECDLP.

Phân tích xác suất: Xác suất thực hiện thành công việc lựa chọn đúng giá trị hàm băm $h = H \in \{0,1\}^* \to Z_q$ là $1 - \frac{q_h}{q}$ và được mô phỏng thực hiện trong $(q_e + q_s)$ lần. Ta có $(1 - \frac{q_h}{q})^{q_e + q_s} \geq 1 - \frac{q_h(q_e + q_s)}{q}$ nên **B** có thể xác định chính xác điểm nghiêm ngặt để chọn lại giá trị hàm băm là $\frac{1}{q_h}$. Do tính ngẫu nhiên lý tưởng trong ROM nên xác suất tồn tại chữ ký s là $\frac{1}{q}$. Như vậy, xác suất thành công là $\varepsilon' = (1 - \frac{q_h(q_e + q_s)}{q})(1 - \frac{1}{q})\frac{1}{q_h}\varepsilon$, và độ phức tạp về thời gian của thuật toán **B** dựa trên hàm mũ được thực hiện trong pha hình thành khoá và ký, và là $t' = t + O(q_e + q_s)E$.

2.2.2. Lược đồ chữ ký số tập thể mù dựa trên lược đồ EC-Schnorr

2.2.2.1. Xây dựng lược đồ chữ ký số

Phần này đề xuất lược đồ chữ ký số tập thể mù dựa trên lược đồ EC-Schnorr, ký hiệu là LĐ 2.04. Lược đồ được trình bày như sau:

1) Thiết lập: Mỗi người ký trong tập thể **B** tính giá trị khóa công khai P_i của mình và gửi đến TTP để tính giá trị khóa công khai tập thể *P* như sau.

$$P_i = d_i \times G\,;\, P = P_1 + P_2 + ... + P_n = \sum_{i=1}^{n} d_i \times G \text{ với } i=1,2...n$$

Mỗi người ký chọn ngẫu nhiên giá trị k_i với $k_i \in Z_q$ và tính C_i sau đó gửi đến TTP để tính $\overline{C}$ như: $C_i = k_i \times G \text{ với } i=1,2,...,n$ và $\overline{C} = \sum_{i=1}^{n} C_i = \sum_{i=1}^{n} k_i \times G$ và gửi $\overline{C}$ đến người yêu cầu **A**.

2) Làm mù: **A** chọn ngẫu nhiên 2 giá trị $\alpha, \beta \in \{1,2,...,q\text{-}1\}$ và tính:

$$C = \overline{C} + \alpha \times G + \beta \times P$$
$$r = H(M, x_C) \bmod q$$
$$\overline{r} = (r - \beta) \bmod q$$

Người yêu cầu gửi $\overline{r}$ tới mỗi người ký trong **B**.

3) Tạo chữ ký: Mỗi người ký tính s_i và gửi đến TTP để tính $\overline{s}$ và gửi tới **A**, với: $s_i = k_i - d_i \overline{r} \bmod q;\ \overline{s} = \sum_{i=1}^{n} s_i \bmod q$.

4) Giải mù: Người yêu cầu tính *s:* $s = (\overline{s} + \alpha) \bmod q$, cặp (*r*,*s*) là chữ ký số tập thể mù của tập thể người ký lên thông điệp *M* .

5) Kiểm tra chữ ký: Tính các giá trị: $C' = s \times G + r \times P$ và $r' = H(M, x_{C'})$.

So sánh*:* nếu $r' = r$ thì chữ ký được chấp nhận, ngược lại không chấp nhận.

Thật vậy, có thể chứng minh như sau:

Với $C' = s \times G + r \times P$

Thay công thức tính *s* và *r* ở trên vào, tính được:

$$C' = (\overline{s} + \alpha) \times G + (\overline{r} + \beta) \times P$$
$$= (\alpha \times G + \beta \times P + \sum_{i=1}^{n} (k_i - \overline{r} d_i) \times G + \overline{r} \sum_{i=1}^{n} d_i \times G)$$
$$= \overline{C} + \alpha \times G + \beta \times P$$
$$= C$$
$$\Rightarrow r' = H(M, x_{C'})$$
$$= H(M, x_C) = r$$

Vậy $r' = r$ đã được chứng minh hay chữ ký đã được xác thực.

Người yêu cầu **A** (*M*)	Dữ liệu	Tập thể người ký **B** (*p, q, G, P,* $\overline{C}$)
Chọn: $\alpha, \beta \in \{1, 2, ..., q-1\}$ $C = \overline{C} + \alpha \times G + \beta \times P$ $r = H(M, x_C) \bmod q$ $\overline{r} = (r - \beta) \bmod q$	←	Công khai (*p, q, G, P,* $\overline{C}$)
	$\overline{r}$ →	$s_i = k_i - d_i \overline{r} \bmod q$
$s = (\overline{s} + \alpha) \bmod q$ Chữ ký số là cặp: (*r,s*)	$\overline{s}$ ←	$\overline{s} = \sum_{i=1}^{n} s_i \bmod q$

Hình 2.4. Tóm tắt thuật toán ký số của LĐ 2.04

2.2.2.2. Đánh giá tính an toàn của các lược đồ đề xuất

1) Tính mù: Các lược đồ chữ ký số tập thể mù đề xuất đảm bảo tính mù.

***Chứng minh**:* Sử dụng các điều kiện trong định nghĩa 1.1 của chương 1 để chứng minh.

Lấy bộ chữ ký $(M, r, s) \in \{(M_0, r_0, s_0), (M_1, r_1, s_1)\}$ là một trong hai bộ chữ ký số được gửi đến người ký B. Gọi $(\overline{r}, \overline{s})$ là dữ liệu được lưu trong các lược đồ chữ ký số được phát hành từ B. Sẽ tồn tại hai giá trị ngẫu nhiên *α, β* liên kết $(\overline{r}, \overline{s})$ tới (M, r, s). Từ mô tả trong các lược đồ, có các liên kết sau:

$\bar{r} = (r - \beta) \bmod q$, $s = (\bar{s} + \alpha) \bmod q$

Theo các liên kết trên tính được: $\alpha = s - \bar{s}$ và $\beta = (r - \bar{r})$

Thay α, β vừa tính ở trên vào phương trình tính *C*, tính được:

$$C = \bar{C} + \alpha \times G + \beta \times P = \bar{C} + (s - \bar{s}) \times G + (r - \bar{r}) \times P \quad (2.9)$$

Từ (2.9) có thể nhận thấy là *r* luôn có mối quan hệ xác định là hằng số với *M* và $(s, \bar{r}, \bar{s})$ và không phụ thuộc vào hai hệ số α, β. Do đó mà khi chọn $(M, r, s) \in \{(M_0, r_0, s_0), (M_1, r_1, s_1)\}$ với dữ liệu lưu trữ trong lược đồ phát hành của B là $(\bar{r}, \bar{s})$ thì luôn tồn tại cặp α, β thỏa mãn.

Với xác suất lớn nhất lựa chọn đúng để $b' = b$ trong tập chữ ký phát hành lựa chọn $(M, r, s) \in \{(M_0, r_0, s_0), (M_1, r_1, s_1)\}$ là $\frac{1}{2}$, hay $\Pr[b = b'] = \frac{1}{2}$, tức là biểu thức $\left|\Pr[b = b'] - \frac{1}{2}\right| < \frac{1}{p^c}$ là đúng, thỏa mãn điều kiện trong định nghĩa 1.1. Do đó, các lược đồ đề xuất là mù vô điều kiện.

Do người ký không thể biết nội dung thông điệp vì thông điệp được băm và kết hợp với hoành độ điểm *C* với $r = H(M, x_C) \bmod q$ và $C = \bar{C} + \alpha \times G + \beta \times P$. Do vậy mà bên ký không thể biết được nội dung thông điệp mà mình đã ký.

2) Tính chống giả mạo: Lược đồ chữ ký số tập thể mù đề xuất có bộ tham số $(\varepsilon, t, q_h, q_e, q_s)$ được gọi là an toàn trong ROM nếu tồn tại (ε', t')-ECDL trong trường *GF*(*p*), với:

$$\varepsilon' = (1 - \frac{q_h(q_e + q_s)}{q})(1 - \frac{1}{q})\frac{1}{q_h}\varepsilon; \quad t' = t + O(q_e + q_s)E$$

Trong đó, (q_h, q_e, q_s) lần lượt là số truy vấn của hàm băm, trích xuất và tạo chữ ký mù; *E* là thời gian thực hiện các phép tính luỹ thừa modulo trong *GF*(*p*).

Chứng minh: Sử dụng các kết quả trình bày trong định nghĩa 1.2 của chương 1 để chứng minh.

Giả sử tồn tại một kẻ giả mạo **A**, xây dựng thuật toán **B** để giúp **A** giải bài toán logarit rời rạc. **B** được cho là một nhóm nhân *G* trong *GF*(*p*) với thành phần *G*, số nguyên tố *q* và điểm *Q* trên đường cong elliptic. B được yêu cầu tìm giá trị $x \in Z_q$ sao cho $Q = x \times G$.

B tiến hành như sau: chọn hàm băm thông điệp $r' = H \in \{0,1\}^* \to Z_q$, gửi tham số công khai (p, G, Q, r') tới **A**. **B** chọn hai giá trị ngẫu nhiên (*k′,d′*) và tính *C**:

$$C^* = Q + d' \times G + k' \times P' \qquad (2.10)$$

d' được xem như là khoá riêng của người ký, k' là giá trị được chọn ngẫu nhiên và *(k′,d′,C*)* là kết quả đầu ra. **A** truy vấn tập Oracle của chữ ký số với thông điệp *M* và khoá riêng *d′*. Đầu tiên, **B** kiểm tra xem *d′* đã được sử dụng cho truy vấn trong các phần cài đặt trước chưa. Nếu d' đã được sử dụng rồi thì B lấy bộ (C^*, k', d') từ bảng được lưu để ký thông điệp *M* theo pha tạo chữ ký được mô tả trong lược đồ. Đầu ra của thuật toán ký là $(M, r', \vec{s}')$. Nếu d' chưa được sử dụng trong các phần cài đặt trước thì **B** thực hiện lại các mô phỏng và chọn lại khoá bí mật *d′* cho đến khi thỏa mãn. Cuối cùng, **A** tạo ra chữ ký số giả mạo là $s_1^* = (r', \vec{s}_1')$ trên *M* bởi khoá bí mật *d′*. **B** lại thực hiện lần nữa bằng cách giữ nguyên (r) và lại yêu cầu **A** ký tiếp và thu được $s_2^* = (r', \vec{s}_2')$.

Từ $C^* = s \times G + r \times P$

Thay vào (2.10), tính được:

$$Q + k'd' \times G + d' \times G = s_j^* \times G + r \times P$$
$$\Rightarrow x \times G + k'd' \times G + d' \times G = s_j^* \times G + rd' \times G$$
$$\Rightarrow s_j^* = x + d'k' - rd' + d'$$

với j=1,2.

Thuật toán B chưa biết (x,r) nên để thu được x thì **B** phải giải phương trình tuyến tính có hai ẩn số hoặc phải giải bài toán ECDLP.

Phân tích xác suất: Xác suất thực hiện thành công việc lựa chọn đúng giá trị hàm băm $h = H \in \{0,1\}^* \to Z_q$ là $1-\frac{q_h}{q}$ và được mô phỏng thực hiện trong $(q_e + q_s)$ lần. Ta có $(1-\frac{q_h}{q})^{q_e+q_s} \geq 1-\frac{q_h(q_e+q_s)}{q}$ nên **B** có thể xác định chính xác điểm nghiêm ngặt để chọn lại giá trị hàm băm là $1/q_h$.

Do tính ngẫu nhiên lý tưởng trong ROM nên xác suất tồn tại chữ ký s là $1/q$. Như vậy, xác suất thành công là $\varepsilon' = (1-\frac{q_h(q_e+q_s)}{q})(1-\frac{1}{q})\frac{1}{q_h}\varepsilon$. Độ phức tạp về thời gian của thuật toán **B** dựa trên hàm mũ được thực hiện trong pha hình thành khoá và ký số, và là $t' = t + O(q_e + q_s)E$.

2.2.3. Đánh giá độ phức tạp thời gian của các lược đồ đề xuất

Theo [26], có ước lượng: $T_h \approx T_m$; $T_{inv} \approx 240T_m$; $T_s \approx 29T_m$, trên cơ sở các phép tính trong các phương trình của lược đồ đề xuất và lược đồ được trình bày trong [79], quy đổi về độ phức tạp thời gian của phép tính nhân T_m, các kết quả so sánh như trình bày bên dưới.

Phần này so sánh độ phức tạp thời gian của các lược đồ LĐ 2.03 với lược đồ được mô tả trong [73] với giả định là các lược đồ đó phải được tính toán với cùng tham số an toàn trong Z_p và số thành viên của tập thể người ký là n.

Bảng 2.8. Độ phức tạp thời gian của lược đồ LĐ 2.03

Loại phép tính	Lược đồ dựa trên chuẩn GOST R34.10-2012 (LĐ 2.03)			
	Làm mù	Tạo chữ ký	Giải mù	Kiểm tra
Phép tính luỹ thừa				
Phép tính nghịch đảo	1		1	2
Phép tính hàm băm	1			
Phép tính nhân vô hướng	2			
Phép tính nhân modulo	3	$2n$	3	2
Quy đổi ra T_m	$302T_m$	$2nT_m$	$243T_m$	$482T_m$
Tổng chi phí thời gian	$(1027+2n)\ T_m$			

Bảng 2.9. So sánh độ phức tạp thời gian của lược đồ LĐ 2.03 và lược đồ [73]

	Lược đồ LĐ 2.03	[73]
Làm mù	$302T_m$	$310T_m$
Tạo chữ ký	$2nT_m$	$2nT_m$
Giải mù	$243T_m$	$243T_m$
Kiểm tra chữ ký	$540T_m$	$482T_m$
Tổng cộng	$(1027+2n)T_m$	$(1057+2n)T_m$

Bảng 2.9 cho thấy độ phức tạp thời gian của lược đồ chữ ký số tập thể mù dựa trên chuẩn GOST R34.10-2012 là gần như tương đương với lược đồ trong [73], tuy nhiên do lược đồ LĐ 2.03 dựa trên bài toán ECDLP, trong khi [73] dựa trên bài toán DLP nên độ dài khóa của LĐ 2.03 nhỏ hơn nhiều so với độ dài khóa trong [73] khi có cùng mức độ an toàn.

Phần tiếp theo so sánh độ phức tạp thời gian của các lược đồ LĐ 2.04 với hai lược đồ được mô tả trong [73] và [79] với giả định là các lược đồ đó phải được tính toán với cùng tham số an toàn trong Z_p và số thành viên của tập thể người ký là n.

Bảng 2.10. Độ phức tạp thời gian của lược đồ LĐ 2.04

Loại phép tính	Lược đồ dựa trên EC-Schnorr (LĐ 2.04)			
	Làm mù	Tạo chữ ký	Giải mù	Kiểm tra
Phép tính luỹ thừa				
Phép tính nghịch đảo				
Phép tính hàm băm	1			
Phép tính nhân vô hướng	2			2
Phép tính nhân modulo		n		
Quy đổi ra T_m	$59T_m$	nT_m	Không đáng kể	$58T_m$
Tổng chi phí thời gian	$(117+n)\ T_m$			

Bảng 2.11. Độ phức tạp thời gian của lược đồ [79]

Loại phép tính	Lược đồ [79]			
	Làm mù	Tạo chữ ký	Giải mù	Kiểm tra
Phép tính luỹ thừa				
Phép tính nghịch đảo	1			
Phép tính hàm băm	1			
Phép tính nhân vô hướng				
Phép tính nhân modulo	3	n	1	1
Quy đổi ra T_m	$245T_m$	nT_m	T_m	T_m
Tổng chi phí thời gian	$(247+n)\ T_m$			

Bảng 2.12. So sánh chi phí thời gian của LĐ 2.04 và lược đồ [73] và [79]

	(LĐ 2.04)	[73]	[79]
Làm mù	$59T_m$	$310T_m$	$245T_m$
Tạo chữ ký mù	nT_m	$2nT_m$	nT_m
Giải mù	Không đáng kể	$243T_m$	T_m
Kiểm tra chữ ký	$58T_m$	$482T_m$	T_m
Tổng cộng	$\mathbf{(117+n)}\ T_m$	$\mathbf{(1057+2n)}T_m$	$\mathbf{(247+n)}\ T_m$

Bảng 2.12 cho thấy độ phức tạp thời gian của lược đồ chữ ký số tập thể mù dựa trên lược đồ EC-Schnorr là thấp hơn [73] và [79], Tuy nhiên do LĐ 2.04 dựa trên bài toán ECDLP, trong khi [73] dựa trên bài toán DLP nên độ dài khóa của LĐ 2.04 nhỏ hơn nhiều so với độ dài khóa trong [73] khi có cùng mức độ an toàn. Đối với lược đồ [79] thì lược đồ LĐ 2.04 và lược đồ [79] cùng dựa trên bài toán ECDLP nên với cùng độ dài khóa thì độ phức tạp về thời gian của LĐ 2.04 thấp hơn khoảng hai lần so với [79] nên có thể nghiên cứu tính toán ứng dụng được trong thực tế.

Tiếp theo là phần so sánh độ phức tạp thời gian của các lược đồ LĐ 2.03 và LĐ 2.04 là hai lược đồ đề xuất dựa trên bài toán khó ECDLP.

Bảng 2.13. So sánh chi phí thời gian của LĐ 2.03 và lược đồ LĐ 2.04

	LĐ 2.03	**LĐ 2.04**
Làm mù	$302T_m$	$59T_m$
Tạo chữ ký mù	$2nT_m$	nT_m
Giải mù	$243T_m$	Không đáng kể
Kiểm tra chữ ký	$540T_m$	$58T_m$
Tổng cộng	$(1027+2n)T_m$	$(117+n)\ T_m$

Bảng 2.13 cho thấy, độ phức tạp thời gian của lược đồ chữ ký số tập thể mù dựa trên chuẩn GOST R34.10-2012 là cao hơn lược đồ chữ ký số dựa trên EC-Schnorr. Phát hiện này phù hợp với các đánh giá so sánh giữa chuẩn GOST R34.10-2012 và lược đồ chữ ký số EC-Schnorr.

2.3. ĐỘ PHỨC TẠP VỀ THỜI GIAN CỦA CÁC LƯỢC ĐỒ ĐỀ XUẤT

2.3.1. Thực nghiệm

Phần này chạy thực nghiệm tính thời gian của các pha trong các lược đồ đề xuất. Thời gian tính toán cho các pha làm mù, ký số, giải mù và kiểm tra là các trình quản lý độc lập, tức là không dựa trên ứng dụng nào được phát triển trong môi trường thực tế. Do đó tất cả thời gian tính toán không bao gồm thời gian giao tiếp.

Ngoài ra, phần này được giả định rằng các yếu tố gây mù, số nguyên bí mật, số nguyên tố,… của các thực thể liên quan được chuẩn bị trước. Đồng thời, các hoạt động không liên quan đến mật mã không được xem xét.

Phần thực nghiệm sử dụng máy tính ảo hóa trên nền VMWare đặt tại trung tâm dữ liệu tỉnh Tây Ninh, với cấu hình máy chủ là: Processor Intel Xeon Silver 4216 2.1G, 16C/32T, 9.6GT/s, 22M Cache, Turbo, HT (100W) DDR4-2400; Memory 16GB; Microsoft Windows 10 (10.0) Professional 64-bit; java version "1.8.0_201" (JAVA 8); NetBeans 8.2. Các tham số đầu vào sử dụng khóa 1024 bit cho các lược đồ dựa trên bài toán DLP và 192 bit cho các lược đồ dựa trên bài toán ECDLP, sử dụng hàm băm là SHA-256, số thành viên ký trong lược đồ ký tập thể là n=3. Kết quả được tính trung bình 1000 lần chạy và được chỉ ra như bên dưới.

Bảng 2.14 cho thấy, nếu sử dụng độ dài khóa cho các lược đồ dựa trên bài toán DLP là 1024 bit và sử dụng độ dài khóa cho các lược đồ dựa trên bài toán ECDLP là 192 bit (*khi đó độ dài khóa của DLP gấp khoảng 5.3 lần ECDLP*) thì thời gian tính toán của các lược đồ chữ ký số tập thể mù dựa trên chuẩn GOST R34.10-94 (bài toán DLP) là 29.1965 mili giây và lược đồ chữ ký số tập thể mù dựa trên chuẩn GOST R34.10-2012 (bài toán ECDLP) là 43.9465 mili giây, tức là thời gian tính toán của LĐ 2.03 khoảng 1.5 lần thời gian của LĐ 2.01.

Bảng 2.14. Chi phí thời gian của lược đồ đề xuất theo chuẩn GOST (mili giây)

	(LĐ 2.01)		**(LĐ 2.03)**	
	Lý thuyết	Thực nghiệm	Lý thuyết	Thực nghiệm
Làm mù	$287T_m$	11.2791	$302T_m$	13.7003
Tạo chữ ký	$2nT_m$	0.2463	$2nT_m$	0.2509
Giải mù	$243T_m$	8.1671	$243T_m$	8.7312
Kiểm tra chữ ký	$264T_m$	9.5040	$540T_m$	21.2641
Tổng thời gian	$(794+2n)T_m$	**29.1965**	$(1027+2n)T_m$	**43.9465**

Bảng 2.15. Chi phí thời gian của lược đồ đề xuất theo Schnorr (mili giây)

	(LĐ 2.02)		**(LĐ 2.04)**	
	Lý thuyết	Thực nghiệm	Lý thuyết	Thực nghiệm
Làm mù	$45T_m$	1.8551	$59T_m$	2.9692
Tạo chữ ký	nT_m	0.1232	nT_m	0.1932
Giải mù	Không đáng kể	0.0004	Không đáng kể	0.0005
Kiểm tra chữ ký	$44T_m$	1.6584	$58T_m$	2.3191
Tổng thời gian	$(89+n)T_m$	**3.6371**	$(117+n)\ T_m$	**5.4920**

Bảng 2.15 cho thấy, thời gian tính toán của các lược đồ chữ ký số tập thể mù dựa trên lược đồ Schnorr (LĐ 2.02) là 3.6371 mili giây và lược đồ chữ ký số tập thể mù dựa trên lược đồ EC-Schnorr (LĐ 2.04) là 5.4920 mili giây, tức là thời gian tính toán của lược đồ LĐ 2.04 khoảng 1.5 lần thời gian của LĐ 2.02.

Như vậy, kết quả thực nghiệm cho thấy thời gian tính toán của các lược đồ chữ ký số tập thể mù dựa trên bài toán DLP là thấp hơn các lược đồ dựa trên bài toán ECDLP (khoảng 1.5 lần), trong khi độ dài khóa của các lược đồ dựa trên bài toán ECDLP là thấp hơn các lược đồ dựa trên bài toán DLP (khoảng 5.3 lần). Ngoài ra theo Sharon Levy trong bài báo [89] thì khi yêu cầu độ an toàn tăng thêm thì thời gian tính toán của lược đồ dựa trên bài toán DLP tăng rất nhanh so với thời gian tính toán của lược đồ dựa trên ECDLP. Ví dụ: khi độ an toàn yêu cầu là 571 bit cho ECDLP và 15.360 bit cho DLP thì độ dài bit của DLP lớn hơn gấp 26.9 lần ECDLP, đồng thời thì thời gian tính toán của pha tạo chữ ký của lược đồ dựa trên DLP cũng cao hơn gấp 2.99 lần lược đồ dựa trên ECDLP.

Ngoài ra cũng có thể thấy rằng, với cùng một mức độ an toàn yêu cầu thì các lược đồ dựa trên bài toán ECDLP sẽ có độ dài khóa nhỏ hơn nhiều lần so với các lược đồ dựa trên bài toán DLP nên giúp giảm không gian lưu trữ, tiêu thụ năng lượng, năng lực xử lý và băng thông [48]. Do đó, có thể sử dụng được trong các

mạng có năng lực xử lý thấp như tốc độ đường truyền, khả năng lưu trữ và năng lực tính toán của hệ thống như ứng dụng trong các thiết bị IoT, thẻ thông minh,…

2.3.2. Đánh giá các lược đồ chữ ký số tập thể mù đề xuất

Phần này đánh giá độ phức tạp về thời gian của bốn lược đồ đề xuất trong chương 2, qua đó đề xuất hướng ứng dụng các lược đồ đề xuất trong thực tế.

Bảng 2.16 thể hiện độ phức tạp thời gian của bốn lược đồ đề xuất theo đối tượng tham gia vào lược đồ là người yêu cầu, người ký và người kiểm tra.

Bảng 2.16. So sánh chi phí thời gian các lược đồ chữ ký số tập thể mù đề xuất

	LĐ 2.01	LĐ 2.02	LĐ 2.03	LĐ 2.04
Thực hiện bởi người yêu cầu	$530T_m$	$45T_m$	$545T_m$	$59T_m$
Thực hiện bởi người ký	$44nT_m$	$43nT_m$	$61nT_m$	$61nT_m$
Thực hiện bởi người kiểm tra	$264T_m$	$44T_m$	$540T_m$	$58T_m$

Trong hầu hết các ứng dụng sử dụng chữ ký số mù, người ký (tập thể người ký) thường phải xử lý nhiều phép tính hơn người yêu cầu, trong khi khả năng tính toán phía người yêu cầu và người kiểm tra thường bị hạn chế trong một số tình huống xác định như sử dụng thiết bị di động, IoT,... nên để bảo đảm chất lượng của các dịch vụ phổ biến dựa trên chữ ký số mù thì điều cấp bách hiện nay là giảm tải tính toán cho phía người yêu cầu so với người ký (tập thể người ký). Các lược đồ chữ ký số mù đề xuất trong chương 2 đáp ứng xu thế đó nên hoàn toán có thể nghiên cứu ứng dụng trong thực tế.

Ngoài ra, khi so sánh các lược đồ theo chuẩn GOST và lược đồ Schnorr thì kết quả cho thấy các lược đồ chữ ký số tập thể mù dựa trên lược đồ Schnorr có độ phức tạp thời gian ở phía người yêu cầu và người kiểm tra thấp hơn ở phía người ký, đặc biệt là khi số lượng người trong tập thể ký lớn, nên các lược đồ này có nhiều hiệu quả khi sử dụng trong các ứng dụng mà yêu cầu khả năng lưu trữ, khả năng xử lý và băng thông đường truyền thấp ở phía người yêu cầu như bầu cử điện tử trên hệ

thống di động, thanh toán trực tuyến không truy vết, và các ứng dụng sử dụng thiết bị IoT,…

2.4. KẾT LUẬN CHƯƠNG 2

Chương 2 đề xuất 4 lược đồ chữ ký số tập thể mù mới dựa trên các chuẩn chữ ký số là GOST R34.10-94, GOST R34.10-2012 và các lược đồ phổ biến như Schnorr và EC-Schnorr. Đóng góp trong chương 2 là dựa trên các chuẩn và các lược đồ phổ biến (*các chuẩn và lược đồ phổ biến sử dụng ở chương này được mô tả như các lược đồ chữ ký số đơn*), NCS thực hiện cải tiến là đề xuất phương pháp để xây dựng các lược đồ chữ ký số tập thể mù hiệu quả từ chữ ký số đơn. Qua đó có thể sử dụng được trong các ứng dụng yêu cầu nhiều người ký (dạng chữ ký tập thể) và cần tính ẩn danh (tính mù).

Do dựa theo chuẩn và lược đồ phổ biến nên lược đồ đề xuất đã kế thừa các ưu điểm về tính an toàn và hiệu quả của các chuẩn và lược đồ đã được kiểm chứng trong thực tế (*đây là hướng nghiên cứu thứ 1 đã được đề cập trong chương 1*). Việc dựa trên chuẩn và trên lược đồ phổ biến với cơ sở toán học là dựa trên độ khó của bài toán logarit rời rạc và bài toán logarit rời rạc trên đường cong elliptic giúp cho các lược đồ đề xuất có khả năng ứng dụng cao, nhất là đối với các bài toán ECDLP sẽ cho độ dài khóa thấp hơn nhiều so với các bài toán IFP và DLP, và do đó sẽ ứng dụng tốt hơn trong các ứng dụng mà có thiết bị có năng lực xử lý thấp. Kết quả này đã được công bố tại công trình [CT2], [CT3].

Kết quả thực nghiệm ở chương 2 cũng cho thấy, các lược đồ chữ ký số tập thể mù dựa trên lược đồ Schnorr có nhiều hiệu quả khi sử dụng trong các ứng dụng mà yêu cầu khả năng lưu trữ, khả năng xử lý và băng thông đường truyền thấp ở phía người yêu cầu như bầu cử điện tử trên hệ thống di động, thanh toán trực tuyến không truy vết, và các ứng dụng sử dụng thiết bị IoT,…

Trên cơ sở so sánh các lược đồ chữ ký số tập thể mù đề xuất trong chương 2, sẽ chọn hai lược đồ có thời gian tính toán tốt nhất để ứng dụng thiết kế lược đồ bầu cử điện tử sẽ trình bày trong chương 4 [CT6].

CHƯƠNG 3. PHÁT TRIỂN LƯỢC ĐỒ CHỮ KÝ SỐ MÙ VÀ CHỮ KÝ SỐ TẬP THỂ MÙ DỰA TRÊN HAI BÀI TOÁN KHÓ

Chương 3 đề xuất lược đồ chữ ký số mù, tập thể mù dựa trên các lược đồ phổ biến như Schnorr và RSA để đảm bảo được tính an toàn và hiệu quả. Đồng thời đề xuất lược đồ chữ ký số mù, chữ ký số tập thể mù mới dựa trên bài toán khó mới do NCS tự phát triển, mà để phá vỡ lược đồ phải giải được hai vấn đề khó về tính toán như tìm logarit rời rạc modulo số nguyên tố và phân tích hợp số n chứa hai số nguyên tố chưa được biết. Lược đồ ký số mới rút ngắn được kích thước của chữ ký số đề xuất. Kết quả nghiên cứu đã được công bố tại công trình [CT1] và [CT5].

3.1. ĐÁNH GIÁ MỘT SỐ LƯỢC ĐỒ CHỮ KÝ SỐ MÙ DỰA TRÊN VIỆC KẾT HỢP CỦA HAI BÀI TOÁN KHÓ

Đã có nhiều các lược đồ chữ ký số được đề xuất dựa trên một trong các bài toán khó như IFP, DLP hoặc ECDLP, tuy nhiên các lược đồ này chỉ bảo đảm tính an toàn trong thời gian ngắn. Để tăng cường tính an toàn của các lược đồ chữ ký số thì các lược đồ cần phải được xây dựng dựa trên nhiều bài toán khó kết hợp, điều này làm cho việc tấn công các lược đồ chữ ký số sẽ trở nên khó khăn hơn vì kẻ tấn công phải giải đồng thời nhiều bài toán khó, hay có thể kéo dài thời gian lược đồ có thể đảm bảo an toàn. Mặc dù các lược đồ chữ ký số dựa trên một bài toán khó có độ phức tạp tính toán thấp hơn các lược đồ chữ ký số dựa trên hai bài toán khó, tuy nhiên do chỉ dựa trên một bài toán khó nên thời gian để các lược đồ có thể bị phá vỡ sẽ nhanh hơn các lược đồ dựa trên hai bài toán khó, vì khi giải được một bài toán khó thì chưa phá vỡ được lược đồ mà phải giải được cả bài toán khó còn lại thì lược đồ đó mới bị phá vỡ, do đó mà các lược đồ dựa trên hai bài toán khó đang được quan tâm nghiên cứu, nhất là trong thời đại hiện nay, nhiều máy tính năng lực xử lý rất cao nên việc giải được các bài toán khó cũng là rất khả thi trong thời gian ngắn.

Đã có một số lược đồ dựa trên hai bài toán khó IFP và DLP được công bố như [45], [95], [102]. Tuy nhiên, đa số các lược đồ đã công bố được chứng minh là không an toàn như [62], [89], [109]. Vì vậy, việc nghiên cứu phát triển thêm nhiều lược đồ chữ ký số an toàn mới dựa trên hai bài toán khó là một trong những hướng nghiên cứu đang được quan tâm gần đây.

Năm 1994, L. Harn đề xuất lược đồ chữ ký số dựa trên hai bài toán khó là IFP và DLP [38], lược đồ này kết hợp giữa RSA và ElGamal cùng một số cải tiến nhằm nâng cao hiệu năng tính toán. Sau đó, năm 1996, Lee và T.Hwang trong [59] đã chỉ ra rằng chỉ cần giải một bài toán DLP là có thể giải được lược đồ của Harn.

Năm 2009, Dernova đề xuất lược đồ chữ ký số dựa trên hai bài toán khó là IFP và DLP [22]. Lược đồ được tóm tắt như sau:

Các ký hiệu sử dụng trong lược đồ: H là hàm băm của thông điệp M cần ký, g là phần tử nguyên thủy bậc q của Z_p^* thỏa điều kiện $g^q \equiv 1 \bmod p$; λ là độ dài bit của q, q là một số nguyên tố lớn và là thừa số của n. Khóa công khai là (p, g, λ), khóa bí mật là q.

Thủ tục sinh chữ ký:

1) Tính $r = H(g^k \bmod p)$, k là giá trị ngẫu nhiên bí mật, với $1 < k \le q - 1$

2) Phương trình tính S là : $S = k\left(Hr\right)^{-1} mod\, q$

Chữ ký số là cặp giá trị (r, S), với $|S| \le \lambda$

Khi sử dụng số nguyên tố p có độ dài khoảng 1024 bit, hàm băm H có kích thước là t bit và giả sử là t = 160 bit, thì độ dài của chữ ký sẽ là:

$|H| + |q| \approx 160 + 512 \approx 672$ bit.

Thủ tục xác thực chữ ký: Kiểm tra điều kiện $|S| \le \lambda$, nếu điều kiện thỏa mãn thì tính theo phương trình kiểm tra $r = H\left(g^{HSr} \bmod p\right)$ và chữ ký được chấp nhận, ngược lại chữ ký bị từ chối.

Yếu tố quan trọng trong thủ tục xác thực chữ ký là điều kiện $|S| \le \lambda$, vì chữ ký (r, S') với thành phần thứ 2 có kích thước $|S'| \approx 1023$ bit (nếu $|p| \approx 1024$ bit) có thể dễ dàng sinh ra mà không cần biết giá trị bí mật *q*. Và chữ ký (r, S') như vậy vẫn phù hợp với phương trình kiểm tra. Tuy nhiên, chữ ký (r, S') sẽ không thỏa mãn với điều kiện $|S'| \le \lambda$. Vì vậy, để giả mạo chữ ký thì (r, S') phải thỏa mãn cả phương trình kiểm tra và điều kiện $|S'| \le \lambda$, khi không biết *q* sẽ không dễ hơn bài toán phân tích $n = (p-1)/2$. Thoạt nhìn, tính an toàn của lược đồ này được dựa trên hai bài toán khó IFP và DLP. Tuy nhiên, thực tế thì có thể chứng minh được rằng tính an toàn của nó chỉ dựa trên một bài toán khó (IFP hoặc DLP).

Một lược đồ khác được phát triển từ lược đồ chữ ký số Schnorr [85], sử dụng số nguyên tố có dạng $p = 2n+1$. Khóa công khai của lược đồ bao gồm 4 giá trị (p, g, λ, y) với *p* được chọn như trong [22] và *y* được tính theo công thức $y = g^x \bmod p$, với *x* là khóa bí mật. Lược đồ được tóm tắt như sau:

***Thủ tục sinh chữ ký*:**

1) Tính $R = g^k \bmod p$, *k* là giá trị ngẫu nhiên bí mật và $1 < k \le q-1$

2) Tính $E = H\left(M \,||\, R\right)$

3) Tính $S = k - xE \bmod q$, sao cho $R = g^S y^E \bmod p$

Chữ ký số là cặp số (*R*, *S*).

Thủ tục xác thực chữ ký: Nếu $|S| \le \lambda$, thì tính $R^* = g^S y^E \bmod p$. Ngược lại, chữ ký số bị từ chối.

Tính $E^* = H\left(M \,||\, R^*\right)$, nếu $E^* = E$ thì chữ ký được chấp thuận.

Việc phá vỡ lược đồ này có thể thực hiện bằng cách giải đồng thời 2 bài toán khó. Giải bài toán DLP sẽ tìm khóa bí mật *x* và giải bài toán IFP sẽ tính được *q* (*q* được yêu cầu để tính *S* với độ dài của *S* không vượt quá $\lambda = |q|$). Tuy nhiên, việc giải đồng thời hai bài toán khó để phá vỡ lược đồ này là không cần thiết vì các tham số bí mật của lược đồ này có thể được tìm ra bởi việc chỉ giải bài toán DLP.

Có thể thực hiện việc tìm tham số bí mật như sau:

Chọn một số nguyên bất kỳ *t* sao cho độ dài bit của *t* không vượt quá $\lambda - 1$. Sau đó tính $Z = g^t \bmod p$.

Tiếp theo, áp dụng thuật toán tìm logarit của Z theo cơ số *g* và thuật toán tính chỉ số (index calculus algorithm) sẽ tính ra được số T, T được tính theo modul $n = (p-1)/2$. Với xác suất gần bằng 1, kích thước của T là $|T| \approx |n| > |t|$.

Do g là số có bậc *q* trong Z_p^* và vì $t = T \bmod q$ nên *q* sẽ là giá trị chia giữa của $(T-t)$. Nhờ việc phân tích $(T-t)$ có thể tìm được tham số bí mật *q*. Xác suất để thực hiện phân tích thành công $(T-t)$ là khá cao. Điều này có nghĩa là thực hiện thủ tục trên vài lần có thể tìm được giá trị giữa của $(T-t)$, và như vậy *q* có thể dễ dàng được phân tích. Hay để phá vỡ lược đồ trên, chỉ cần giải một bài toán DLP.

Năm 2012, S. Vishnoi và V. Shrivastava đề xuất lược đồ ký số mới dựa trên hai bài toán khó IFP và DLP [99]. Lược đồ sử dụng số nguyên tố *p* cho bài toán DLP, số *n* là tích của hai số nguyên tố lớn q, q' với $p < n$, *g* là phần tử nguyên thủy trong Z_p^*. Lược đồ được trình bày như sau:

Tạo khóa:

1) Tính $\phi(n) = (q-1)(q'-1)$

2) Chọn hai giá trị ngẫu nhiên *k* và *v* sao cho $1 < k, v < p-1$

3) Chọn ngẫu nhiên (x,r,b) sao cho $1<x,r,b<n-1$ và $UCLN(x,\phi(n))=1$

4) Tìm c sao cho $cb^x=1 \bmod n$

5) Tính u, w, t, y : $u=g^k \bmod p$; $w=g^v \bmod p$; $t=u^w \bmod p$; $y=r^x \bmod n$

Khóa công khai là (x, c, g) và khóa bí mật là (k, v, u, w, b, r).

Tạo chữ ký: Để tạo chữ ký cho thông điệp M, người ký thực hiện như sau:

1) Chọn số nguyên z thỏa mãn $1<z<p-1$ và $UCLN(z,p-1)=1$

2) Tính $h=g^z \bmod p$

3) Tính $\gamma=tw^h \bmod p$

4) Tính $f=rb^{H(M)} \bmod n$

5) Tính $s=((H(M)-kw-hv+yz)z^{-1}) \bmod(p-1)$; Trong đó (-kw) và (-hv) là nghịch đảo cộng của kw và hv. Nếu t=0 hoặc f=0 hoặc s=0 thì lặp lại các bước trên.

Chữ ký số là cặp giá trị (γ,h,f,s).

Xác thực chữ ký: Nếu $g^{H(M)}h^{(f^x c^{H(M)} \bmod n)}=\gamma h^s \bmod p$ thì chữ ký số được xác thực đúng, ngược lại thì chữ ký là không đúng.

Đến năm 2013, Shin-Yan Chiou và Yi-Xuan He [92] đã chứng minh lược đồ của S.Vishnoi và V.Shrivastava là không an toàn trước các cuộc tấn công giả mạo chữ ký. Phương pháp tấn công mô tả như sau:

+ Chọn số nguyên z' thỏa mãn $1<z'<p-1$ và $UCLN(z',p-1)=1$

+ Tính $h'=g^{z'} \bmod p$

+ Chọn f' sao cho $1<f'<n-1$

+ Tính $\gamma'=h'^{(f')^x c^{H(M')} \bmod n} \bmod p$

+ Tính $s'=H(M')z'^{-1} \bmod(p-1)$

Chữ ký của thông điệp giả M' là (γ', h', f', s')

Người nhận sẽ xác thực theo biểu thức: $g^{H(M)}h^{(f^x c^{H(M)} \bmod n)} = \gamma h^s \bmod p$

Với chữ ký của thông điệp giả thì $g^{H(M')}g^{z'(f'^x c^{H(M')} \bmod n)} = g^{H(M')+(z'(f'^x c^{H(M')} \bmod n))}$

Tương tự thì phương trình dưới đây thỏa mãn phương trình xác thực,

$$\gamma h^s = h'^{(f'^x c^{H(M')} \bmod n)} g^{z'H(M')z'^{-1}} \bmod p$$
$$= g^{H(M')}g^{z'(f'^x c^{H(M')} \bmod n)}$$
$$= g^{H(M')+z' f'^x c^{H(M')} \bmod n}$$

Có thể thấy rằng người tấn công không cần giải bài toán khó nào cũng có thể giả mạo chữ ký. Như vậy, với các lược đồ dựa trên hai bài toán khó trên đây, thực chất chỉ cần giải một bài toán khó là có thể phá vỡ được lược đồ.

3.2. LƯỢC ĐỒ CHỮ KÝ SỐ MÙ, CHỮ KÝ SỐ TẬP THỂ MÙ DỰA TRÊN SỰ KẾT HỢP LƯỢC ĐỒ CHỮ KÝ SỐ RSA VÀ SCHNORR

Phần này đề xuất lược đồ chữ ký số mù và tập thể mù dựa trên hai lược đồ phổ biến là RSA và Schnorr. Việc dựa trên các lược đồ chữ ký số đơn (*RSA và Schnorr*) để xây dựng các lược đồ chữ ký số mù và tập thể mù có thể sử dụng trong các ứng dụng yêu cầu cao về tính an toàn (*phải giải hai bài toán khó*) và yêu cầu nhiều người ký ẩn danh (*tập thể mù*). Kết quả này được công bố tại [CT5].

3.2.1. Xây dựng lược đồ cơ sở

Phần này thực hiện cải tiến như sau: sử dụng số nguyên tố p có cấu trúc $p = 2n+1$, tham số g có bậc n modulo p, sử dụng thêm phần tử e cho khoá công khai, phần tử d cho khoá bí mật. Trong phương trình kiểm tra chữ ký thì sử dụng S^e thay thế S, các phần tử e và d được tạo ra giống như trong RSA, e được chọn có kích thước trong khoảng 16 đến 32 bits, $\phi(n) = (q-1)(q'-1)$, d thỏa mãn $d = e^{-1} \bmod \phi(n)$. Lược đồ được mô tả như sau:

a) Tạo khoá

1) Chọn giá trị nguyên ngẫu nhiên $e \in Z_n$ sao cho $UCLN(e, \phi(n)) = 1$ và tính d sao cho $ed \equiv 1 \bmod \phi(n)$

2) Chọn giá trị ngẫu nhiên bí mật x với $x \in Z_p^*$ và tính $y = g^x \bmod p$

Khoá công khai là (e, g, y) và khoá bí mật là (x, d)

b) Tạo chữ ký

1) Tính $R = g^k \bmod p$ với k là giá trị bí mật ngẫu nhiên thỏa mãn $1 < k \le n-1$

2) Tính $E = H(M \,||\, R)$

3) Tính S sao cho $S^e = k - xE \bmod n$ hay $S = (k - xE)^d \bmod n$

4) Tính $R = g^{S^e} y^E \bmod p$

Chữ ký là cặp (E, S).

c) Kiểm tra chữ ký

Tính $R^* = g^{S^e} y^E \bmod p$ và $E^* = H(M \,||\, R^*)$, nếu $E^* = E$ thì chữ ký hợp lệ, ngược lại thì chữ ký không hợp lệ.

Giải bài toán DLP trong Z_p^* là không đủ để phá vỡ lược đồ đề xuất mà yêu cầu phải biết thừa số của n. Giải bài toán DLP sẽ tính được khoá bí mật x và có thể tính được $S^* = (k - xE) \bmod n$. Tuy nhiên, để tính được chữ ký số S thì yêu cầu phải khai căn bậc e modulo n từ S^e, nghĩa là phải phân tích được thừa số của n hay phải giải được bài toán IFP.

3.2.2. Lược đồ chữ ký số mù dựa trên lược đồ cơ sở

Lược đồ chữ ký số cơ sở sử dụng hai bài toán khó được trình bày ở mục 3.2.1 được sử dụng làm cơ sở để xây dựng lược đồ chữ ký số mù. Phương pháp này được sử dụng để phát triển lược đồ chữ ký số mù yêu cầu giải đồng thời hai bài toán khó. Có 6 vòng trong lược đồ ký mù. Trong đó M là thông điệp đã được làm mù. Tham

gia vào lược đồ ký số là người ký **B** và người yêu cầu **A**. Lược đồ được mô tả như sau:

a) Tạo khoá

1) Chọn giá trị nguyên ngẫu nhiên $e \in Z_n$ sao cho $UCLN(e,\phi(n)) = 1$ và tính d sao cho $ed \equiv 1 \bmod \phi(n)$

2) Chọn giá trị ngẫu nhiên bí mật x với $x \in Z_p^*$ và tính $y = g^x \bmod p$

Khoá công khai là (e, g, y) và khoá bí mật là (x, d).

b) Tạo chữ ký

1) Vòng 1 (người ký **B**):

+ Chọn ngẫu nhiên k với $1 < k \le n-1$

+ Tính $R = g^k \bmod p$ và cho **A**

2) Vòng 2 (người yêu cầu **A**):

+ Chọn hai giá trị ngẫu nhiên (ε, τ) có kích thước khoảng 16 bit

+ Tính $R' = Rg^{\varepsilon} y^{\tau} \bmod p$, $E' = H\left(M \| R'\right)$, $E = E' - \tau$ và gửi E cho **B**

3) Vòng 3 (người ký **B**):

Tính $D = k - xE \bmod n$ sao cho $R = g^D y^E \bmod p$ và gửi D cho **A**

4) Vòng 4 (người yêu cầu **A**):

Chọn ngẫu nhiên $\mu < n$, tính $D' = \mu^e (D + \varepsilon) \bmod n$ và gửi D' cho **B**

5) Vòng 5 (người ký **B**):

Tính $D'' = D'^d = \mu^{ed} (D + \varepsilon)^d = \mu (D + \varepsilon)^d \bmod n$ và gửi D'' cho **A**

6) Vòng 6 (người yêu cầu **A**):

Tính $E' = E + \tau$ và $S' = \dfrac{D^{"}}{\mu \bmod n}$

Chữ ký số mù là cặp (E', S').

c) Kiểm tra chữ ký

Tính $R'^{*} = g^{S'^{e}} y^{E'} \bmod p$ và $E'^{*} = H\left(M \,||\, R'^{*}\right)$, nếu $E'^{*} = E'$ thì chữ ký hợp lệ, ngược lại chữ ký không hợp lệ.

3.2.3. Lược đồ chữ ký số tập thể mù dựa trên lược đồ cơ sở

Giả sử tập thể người ký **B** có *m* thành viên, lược đồ được mô tả như sau:

a) Tạo khoá:

1) Chọn giá trị nguyên ngẫu nhiêu $e \in Z_n$ sao cho $UCLN(e, \phi(n)) = 1$ và tính *d* sao cho $ed \equiv 1 \bmod \phi(n)$

2) Chọn giá trị ngẫu nhiên bí mật x_i với $x_i \in Z_p^*$ và tính $y_i = g^{x_i} \bmod p$

3) Gửi TTP tính khóa công khai chung của tập thể: $y = \prod_{i=1}^{m} y_i \bmod p, i = 1, 2...m.$

Khoá công khai là (*e*, *g*, *y*). Khoá bí mật là $\left(x_i, d\right)$

b) Tạo chữ ký

Vòng 1 (mỗi thành viên trong **B**):

+ Chọn k_i ngẫu nhiên sao cho $1 < k_i \le n - 1$

+ Tính $R_i = g^{k_i} \bmod p$

+ Gửi TTP tính giá trị: $\overline{R} = \prod_{i=1}^{m} R_i \bmod p = g^{\sum_{i=1}^{m} k_i \bmod p} \bmod p$

Vòng 2 (người yêu cầu **A**):

+ Chọn hai giá trị ngẫu nhiên (ε, τ) có kích thước khoảng 16 bit

+ Tính $R' = \overline{R} g^{\varepsilon} y^{\tau} \bmod p$, $E' = H\left(M \| R'\right)$, $E = E' - \tau$ và gửi E cho **B**.

Vòng 3 (mỗi thành viên trong **B**):

+ Tính $D_i = k_i - x_i E \bmod n$, sao cho $R_i = g^{D_i} y_i^{E} \bmod p$

+ Gửi TTP tính: $\overline{D} = \sum_{i=1}^{m} D_i \bmod n$ và gửi $\overline{D}$ cho **A**

Vòng 4 (người yêu cầu **A**):

Chọn ngẫu nhiên $\mu < n$, tính $D' = \mu^{e}\left(\overline{D} + \varepsilon\right) \bmod n$ và D' cho **B**

Vòng 5 (tập thể người ký **B**):

Tính $D'' = D'^{d} = \mu^{ed}\left(\overline{D} + \varepsilon\right)^{d} = \mu\left(\overline{D} + \varepsilon\right)^{d} \bmod n$ và gửi D'' cho **A**

Vòng 6 (người yêu cầu **A**):

Tính $E' = E + \tau$ và $S' = \dfrac{D''}{\mu \bmod n}$

Chữ ký mù là cặp (E', S').

c) Kiểm tra chữ ký:

Tính $R'^{*} = g^{S'^{e}} y^{E'} \bmod p$ và $E'^{*} = H\left(M \| R'^{*}\right)$, nếu $E'^{*} = E'$ thì chữ ký hợp lệ, ngược lại chữ ký không hợp lệ.

3.2.4. Đánh giá các lược đồ chữ ký số đề xuất

Định lý 3.1: Chữ ký số mù (E', S') là hợp lệ tương ứng với thông điệp *M*.

Chứng minh: Thật vậy, từ các vòng 4, 5, 6, tính được:

$$S'^{e} = \frac{D''^{e}}{\mu^{e}} = \frac{D'}{\mu^{e}} = \frac{\mu^{e}\left(D + \varepsilon\right)}{\mu^{e}} = D + \varepsilon \bmod n$$

Sử dụng điều kiện $S'^{e} = D + \varepsilon \bmod n$ để chứng minh tính đúng của phương trình xác thực như sau:

$$\begin{aligned} R'^{*} &= g^{S'^{e}} y^{E'} = g^{D+\varepsilon} y^{E+\tau} \\ &= g^{D} y^{E} g^{\varepsilon} y^{\tau} \\ &= R g^{\varepsilon} y^{\tau} \left(\bmod p\right) \\ \Rightarrow E'^{*} &= E' \end{aligned}$$

Định lý 3.2: Chữ ký số tập thể mù (E', S') là hợp lệ của *m* người ký tương ứng với thông điệp *M*.

Chứng minh: Thật vậy, từ các vòng 4, 5, 6, tính được:

$$S'^{e} = \frac{D''^{e}}{\mu^{e}} = \frac{D'}{\mu^{e}} = \frac{\mu^{e}\left(\bar{D} + \varepsilon\right)}{\mu^{e}} = \bar{D} + \varepsilon \bmod n$$

Sử dụng điều kiện $S'^{e} \equiv \bar{D} + \varepsilon \bmod n$ để chứng minh tính đúng của phương trình xác thực như sau:

$$\begin{aligned} R'^{*} &= g^{S'^{e}} y^{E'} = g^{\bar{D}+\varepsilon} y^{E+\tau} \\ &= g^{\bar{D}} y^{E} g^{\varepsilon} y^{\tau} \\ &= \bar{R} g^{\varepsilon} y^{\tau} \left(\bmod p\right) \\ \Rightarrow E'^{*} &= E' \end{aligned}$$

Định lý 3.3: Lược đồ chữ ký số mù đề xuất bảo đảm thuộc tính không truy vết khi thông điệp *M* và chữ ký (E', S') được chuyển cho người ký.

Chứng minh: Với xác suất bằng nhau của mỗi người yêu cầu và những người tham gia vào các lược đồ ký mù có thể cung cấp một chữ ký trên một thông điệp *M*. Điều này chứng tỏ bộ ba $\left(R, D, E\right)$ được hình thành từ người ký có thể liên kết chữ ký số (E', S') với thông điệp *M*. Thực tế khi $R = g^{D} y^{E} \bmod p$ và $R' = g^{S'^{e}} y^{E'} \bmod p$ thì mối quan hệ $\frac{R'}{R} = g^{S'^{e}-D} y^{E'-E} = g^{\varepsilon} y^{\tau} \left(\bmod p\right)$. Vì vậy, khi chọn ngẫu nhiên giá

trị (ε,τ) thì chữ ký (E',S') với xác suất bằng nhau có thể được tạo ra với mọi người yêu cầu trong quá trình ký mù.

Định lý 3.4: Lược đồ chữ ký số tập thể mù đề xuất bảo đảm thuộc tính không truy vết khi thông điệp *M* và chữ ký (E',S') được chuyển cho người ký.

Chứng minh*:* Với xác suất bằng nhau của mỗi người yêu cầu và người ký, những người tham gia vào các lược đồ ký mù có thể cung cấp một chữ ký trên một thông điệp *M*. Điều này chứng tỏ bộ ba $\left(R_i,D_i,E\right)$ được hình thành từ mỗi người ký có thể liên kết chữ ký (E',S') với thông điệp *M*. Thực tế khi $\bar{R}=g^{\bar{D}}y^{E} \bmod p$ và $R'=g^{S'^{e}}y^{E'} \bmod p$ thì mối quan hệ $\frac{R'}{\bar{R}}=g^{S'^{e}-\bar{D}}y^{E'-E}=g^{\varepsilon}y^{\tau}\left(\bmod p\right)$. Vì vậy, khi chọn ngẫu nhiên giá trị (ε,τ) thì chữ ký (E',S') với xác suất bằng nhau có thể được tạo ra với mọi người yêu cầu trong quá trình ký mù.

Định lý 3.5: Chỉ có người ký mới có thể tạo ra được chữ ký hợp lệ.

Tấn công 1 (tấn công bởi bên ngoài): Kẻ tấn công cố gắng dò tìm chữ ký (E',S') đối với thông điệp *M* bằng cách chọn một số nguyên cố định và tìm các số còn lại. Chẳng hạn, kẻ tấn công lựa chọn E' và cố gắng tìm ra giá trị S' thỏa mãn phương trình $R'\equiv g^{S'^{e}}y^{E'}\left(\bmod p\right)$ và ngược lại. Để làm điều này, kẻ tấn công đầu tiên chọn ngẫu nhiên một số nguyên R' rồi tính $S'^{e}=\log_g R'y^{-E'}\left(\bmod p\right)$ và chỉ thực hiện được nếu giải được hai bài toán khó.

Tấn công 2 (tấn công bởi người yêu cầu): Người yêu cầu có thể biết được những chữ ký riêng lẻ nhưng không thể phá vỡ được tính an toàn của lược đồ. Nếu người yêu cầu không thể tính toán được chữ ký số mù (chữ ký số tập thể mù) chính xác từ những chữ ký riêng lẻ thì phương trình kiểm tra chữ ký số mù (chữ ký số tập thể mù) sẽ không thể thỏa mãn. Loại tấn công này có thể phát hiện bởi quá trình kiểm tra chữ ký.

Tấn công 3 (Tấn công bởi người ký hoặc tập thể người ký): Kẻ tấn công không thể tính khóa của tập thể người ký và xác thực khóa người ký và thay thế người ký gốc. Vì người ký chọn giá trị $1 < k_i \le n-1$ và tính toán $R_i = g^{k_i} \bmod p$ và gửi R_i cho **A**. Giá trị k_i từ R_i không thể tính toán được (xác định k_i là phải giải bài toán DLP). Thực tế trong lược đồ đề xuất, kẻ tấn công không thể tìm giá trị k_i ngẫu nhiên tương ứng với chữ ký.

3.2.5. Đánh giá độ phức tạp thời gian của lược đồ chữ ký số đề xuất

Phần này so sánh độ phức tạp thời gian của lược đồ chữ ký số tập thể mù đề xuất với lược đồ chữ ký số tập thể mù trình bày trong [CT4] và [45]. [CT4] thiết kế lược đồ chữ ký số tập thể mù dựa trên lược đồ Rabin và Schnorr sử dụng S^3 thay cho S, còn lược đồ này sử dụng S^e thay cho S trong phần kiểm tra chữ ký số.

Lược đồ [45] được trình bày chi tiết ở chương 1, được sử dụng để so sánh với lược đồ đề xuất cũng dựa trên hai bài toán khó là IFP và DLP. Ở phần tạo tham số cũng giống như lược đồ đề xuất, tuy nhiên ở phần tạo chữ ký và xác thực, [45] sử dụng tới hai tham số ngẫu nhiên (*lược đồ đề xuất chỉ sử dụng một tham số ngẫu nhiên*) và phương trình xác thực của [45] cũng phức tạp hơn lược đồ đề xuất nên tăng độ phức tạp về thời gian so với lược đồ đề xuất, trong khi tính an toàn của lược đồ thì xem như tương đương nhau vì cùng dựa trên hai bài toán khó IFP và DLP. Kết quả so sánh như dưới đây.

Bảng 3.1. So sánh độ phức tạp thời gian của lược đồ chữ ký số tập thể mù đề xuất và lược đồ [45] và [CT4] (Thủ tục sinh chữ ký)

Các phép tính	Thực hiện bởi người yêu cầu			Thực hiện bởi người ký		
	Lược đồ đề xuất	[45]	[CT4]	Lược đồ đề xuất	[45]	[CT4]
Số phép tính lũy thừa	3	7	2	2	1	1
Số phép tính nghịch đảo	1	4	1	0	0	0
Số phép tính hàm băm	1	3	1	0	1	0
Số phép tính nhân	3	11	5	2	2	1
Số phép tính căn bậc 3	0	0	0	0	0	1
Số lượng số ngẫu nhiên	3	2	3	1	1	1

Bảng 3.2. So sánh độ phức tạp thời gian của lược đồ chữ ký mù đề xuất và lược đồ [CT4], [45] (Thủ tục kiểm tra chữ ký)

Số phép tính	Thực hiện xác minh		
	Lược đồ đề xuất	[45]	[CT4]
Số phép tính lũy thừa	3	4	2
Số phép tính băm	1	1	1
Số phép tính nhân	1	2	3

Các kết quả tại bảng 3.1 và bảng 3.2 đã chỉ ra rằng, lược đồ chữ ký mù đề xuất và lược đồ trong [CT4] có độ phức tạp thời gian thấp hơn lược đồ trong [45]. Mặc dù lược đồ đề xuất có độ phức tạp thời gian gần như tương đương lược đồ trong [CT4] đối với phần người yêu cầu và kiểm tra. Tuy nhiên đối với người ký thì lược đồ đề xuất thực hiện dễ dàng hơn vì không yêu cầu tính căn bậc 3 khi tính giá trị D'' (D'' *được sử dụng để tính chữ ký số mù* S'), và vì vậy mà lược đồ này dễ sử dụng hơn.

Còn khi so sánh với [45] thì độ phức tạp thời gian của lược đồ đề xuất thấp hơn ở phần người yêu cầu và người kiểm tra. Thực tế, để đảm bảo chất lượng các

dịch vụ cần phải giảm phần tính toán cho phía người yêu cầu ký hơn là người ký vì điều kiện hạ tầng tính toán của phía người ký thường cao hơn phía người yêu cầu. Lược đồ đề xuất đáp ứng yêu cầu đó nên có thể sử dụng trong các ứng dụng thực tế nếu được tính toán và lựa chọn các tham số đầu vào một cách cẩn thận.

Tiếp theo là phần so sánh lược đồ đề xuất với lược đồ trong [CT4] theo các pha trong lược đồ. Trong đó T_r là ký hiệu chi phí thời gian tính căn bậc 3.

Bảng 3.3. So sánh độ phức tạp tính toán các pha của lược đồ đề xuất và [CT4]

	Lược đồ đề xuất	[CT4]
Làm mù	$45T_m$	$45T_m$
Ký số	$(43+m)T_m$	$(3+m)T_m + T_r$
Giải mù	$241T_m$	$241T_m$
Kiểm tra chữ ký	$65T_m$	$65T_m$
Tổng cộng	$(394+m)T_m$	$(354+m)T_m + T_r$

Bảng 3.3 chỉ ra rằng, nếu tính độ phức tạp thời gian theo các pha là làm mù, tạo chữ ký, giải mù và kiểm tra thì lược đồ chữ ký tập thể mù đề xuất và lược đồ trong [CT4] có độ phức tạp thời gian gần như nhau ở các pha, riêng pha tạo chữ ký thì lược đồ đề xuất thực hiện dễ dàng hơn vì không yêu cầu tính căn bậc 3 khi tính giá trị D'' như trong [CT4] nên có thể dễ ứng dụng trong thực tế đối với các ứng dụng mà hiệu năng của thiết bị người ký cũng không cao.

Như vậy, phần này đã xây dựng lược đồ chữ ký số mù, chữ ký số tập thể mù dựa trên hai bài toán khó là IFP và DLP. Việc dựa trên các lược đồ phổ biến như Schnorr và RSA để đảm bảo được tính an toàn và hiệu quả (*đây là hướng nghiên cứu thứ 2 đã được đề cập trong chương 1*). Do lược đồ dựa trên hai bài toán khó nên để phá vỡ lược đồ sẽ mất rất nhiều thời gian để phải phá vỡ hai bài toán khó. Vì vậy mà lược đồ đề xuất này có thể sử dụng trong các ứng dụng yêu cầu thời gian lưu trữ kết quả đủ lâu. Kết quả này được công bố trong công trình [CT5].

3.3. ĐỀ XUẤT LƯỢC ĐỒ KÝ SỐ DỰA TRÊN NHÓM CON HỮU HẠN KHÔNG VÒNG HAI CHIỀU

3.3.1. Tổng quan về lược đồ đề xuất

Trong các hệ thống sử dụng lược đồ ký số khoá công khai để ký số các tài liệu điện tử, tính an toàn của lược đồ ký số thường dựa trên hai yếu tố, thứ nhất là thuật toán nổi tiếng để việc giả mạo chữ ký số là không khả thi về mặt tính toán, và thứ hai là xác suất xuất hiện các thuật toán mới để phá vỡ lược đồ ký số đó là không đáng kể. Trong thực tế, các lược đồ chữ ký số phổ biến dựa trên độ khó của bài toán logarit rời rạc [67] có kích thước chữ ký số là 4ρ-bit sẽ cung cấp độ an toàn ρ-bit (tức là để làm giả một chữ ký số thành công yêu cầu phải thực hiện 2^{ρ} phép toán luỹ thừa). Còn các lược đồ chữ ký số dựa trên cơ sở độ khó của bài toán IFP thường có kích thước chữ ký số lớn hơn nhiều [67], [83].

Phần này xây dựng một lược đồ ký số mù với kích thước chữ ký là 3ρ-bit nhưng cung cấp độ an toàn ρ-bit. Các lược đồ đề xuất là dựa trên độ khó của bài toán DLP modulo một hợp số và sử dụng nhóm con hữu hạn không vòng G của nhóm nhân Z_n^*, và còn được gọi là nhóm con hữu hạn không vòng hai chiều, tức là nhóm con được tạo ra bởi phần tử sinh gồm hai thành phần có cùng bậc là r (r là số nguyên tố), nhóm con như vậy chứa r^2 phần tử.

Phần sau trình bày phương pháp xác suất và tất định để thiết lập các nhóm hữu hạn.

3.3.2. Thiết lập các nhóm con hữu hạn không vòng hai chiều

3.3.2.1. Phương pháp tất định

Phần này xây dựng một nhóm con hữu hạn không vòng G của nhóm nhân Z_n^* của vòng hữu hạn Z_n, trong đó $n = pq$ với p, q là hai số nguyên tố lớn có kích thước tương ứng là $|q| \approx \lambda\ bit, |p| \approx 2\lambda\ bit$ [13]. Tham số λ được chọn phụ thuộc vào mức độ an toàn yêu cầu, ví dụ với $\lambda \approx 512\ bit$ có độ an toàn 80-bit và

$\lambda \approx 1232\,bit$ cung cấp độ an toàn 128-bit. Số q và p là số bí mật và có cấu trúc $p = N_p r + 1$ và $q = N_q r + 1$, trong đó N_p và N_q là hai số chẵn lớn, r là một số nguyên tố ρ-bit (ρ = 80 cung cấp độ an toàn yêu cầu bằng 2^{80} phép tính luỹ thừa).

Nhóm con G có bậc r^2 được tạo ra bởi hai số nguyên α và β là hai nhóm con cyclic khác nhau của Z_n^* có bậc r. Sử dụng thuật toán tất định dưới đây để tìm α, β

Thuật toán 3.1

1) Tạo giá trị γ có bậc r modulo p

2) Tạo giá trị δ có bậc r modulo q

3) Chọn các giá trị ngẫu nhiên $0 < h < r$ và $0 < k < r$ và tìm giá trị α thỏa mãn hệ phương trình đồng dư sau đây:

$$\begin{cases} \alpha \equiv \gamma^k \bmod p \\ \alpha \equiv \delta^h \bmod q \end{cases} \tag{3.1}$$

4) Chọn các giá trị ngẫu nhiên $0 < g < r$ và $0 < m < r$ thỏa mãn $gh \neq km \bmod r$ và tính giá trị β theo hệ phương trình đồng dư sau đây:

$$\begin{cases} \beta \equiv \gamma^g \bmod p \\ \beta \equiv \delta^m \bmod q \end{cases} \tag{3.2}$$

Các kết quả đầu ra α và β thuộc các nhóm con cyclic khác nhau có bậc r, do đó các phép nhân (modulo n) của tất cả các phép luỹ thừa có thể của α và β tạo thành một nhóm con cơ bản có bậc là r^2. Bậc của mỗi giá trị α và β là r theo các công thức dưới đây:

$$\left\{\left\{\alpha^r \equiv \gamma^{kr} \equiv 1 \bmod p\right\} \cup \left\{\alpha^r \equiv \delta^{hr} \equiv 1 \bmod q\right\}\right\} \Rightarrow \alpha^r \equiv 1 \bmod n \tag{3.3}$$

$$\left\{\left\{\beta^r \equiv \gamma^{gr} \equiv 1 \bmod p\right\} \cup \left\{\beta^r \equiv \delta^{mr} \equiv 1 \bmod q\right\}\right\} \Rightarrow \beta^r \equiv 1 \bmod n \tag{3.4}$$

Mệnh đề 3.1: Thuật toán 3.1 tạo ra các giá trị α và β và bất đẳng thức $\alpha \neq \beta^d \bmod n$ đúng với mọi $d \in \{1,2,...,r\}$

Chứng minh: Rõ ràng bất đẳng thức $\alpha \neq \beta^d \bmod n$ là đúng. Giả sử với mọi giá trị $d \in \{1,2,...,r\}$ thì đẳng thức $\alpha = \beta^d \bmod n$ là đúng.

Từ (3.1) tính được:

$\{\beta^d \equiv \gamma^k \bmod p\} \Rightarrow \{\beta \equiv \gamma^{k/d} \bmod p\}$

$\{\beta^d \equiv \delta^h \bmod q\} \Rightarrow \{\beta \equiv \gamma^{h/d} \bmod q\}$

Từ (3.2) tính được:

$\{\gamma^g \equiv \gamma^{k/d} \bmod p\} \Rightarrow \{g \equiv k/d \bmod r\}$

$\{\delta^m \equiv \delta^{h/d} \bmod q\} \Rightarrow \{m \equiv h/d \bmod r\}$

Vì vậy mà $\{d \equiv (k/g) \bmod r\}$ và $\{d \equiv (h/m) \bmod r\}$, do đó $km \equiv hg \bmod r$. Kết quả này mâu thuẫn với điều kiện $gh \neq km \bmod r$ được sử dụng tại bước thứ 4 của thuật toán khi chọn *g* và *m*. Vì vậy, khẳng định trên đã được chứng minh.

Từ mệnh đề 3.1 cho thấy rằng phép nhân (mod *n*) của tất cả các phép luỹ thừa có thể của α và β tạo ra r^2 giá trị khác nhau theo công thức dạng $\alpha^i \beta^j \bmod n$, mỗi giá trị có bậc *r*: $\left(\alpha^i \beta^j\right)^r \equiv \alpha^{ir} \beta^{jr} \equiv 1.1 \equiv 1 \bmod n.$

3.3.2.2. Phương pháp xác suất

Phần này xây dựng nhóm con hữu hạn không vòng *G* của nhóm nhân Z_n^* của vòng hữu hạn Z_n, trong đó $n = pq$ với *p, q* là hai số nguyên tố lớn có kích thước là $|q| \approx |p| \approx 512\ bit$. *q* và *p* là số bí mật và có cấu trúc $p = N_p r^2 + 1$ và $q = N_q r^2 + 1$, trong đó N_p và N_q là hai số chẵn lớn có chứa một ước số nguyên tố lớn, *r* là số nguyên tố ρ-bit. Nhóm nhân Z_n^* của vòng hữu hạn Z_n được tạo trên cơ sở hai phần

tử. Kết quả dưới đây có được từ thực tế là giá trị của hàm Euler tổng quát của *n* là $L(n)$ nhỏ hơn giá trị của hàm Euler $\phi(n)$ của *n*.

$$\begin{aligned}\phi(n) &= (q-1)(p-1)\\ &= UCLN(q-1, p-1)\,\text{BCNN}[q-1, p-1]\\ &= UCLN(q-1, p-1)L(n) \geq r^2 L(n)\end{aligned}$$

Phần này sử dụng nhóm con *G* có bật r^2 của nhóm nhân Z_n^*, là nhóm con hữu hạn không vòng hai chiều và được tạo bởi hai thành phần có giá trị α và β có bậc là số nguyên tố *r*. Tất cả các phần tử của nhóm con *G*, trừ phần tử sinh đều có bậc là *r*. Giá trị của hai thành phần cơ bản có giá trị α và β được tạo bởi các thuật toán xác suất như sau:

Thuật toán 3.2

1) Chọn số ngẫu nhiên *b* sao cho $1 < b < n$

2) Tính $\gamma = L(n)/r$ và $z = b^{\gamma} \bmod n$

3) Nếu $z \neq 1,$ thì giá trị α (β) được tính từ z, ngược lại lặp lại bước 1-3

Tính đúng của thuật toán trên dễ dàng được chứng minh.

Thật vậy, nếu $z \neq 1$ đạt được khi tính *z* thì $z = b^{L(n)/r} \bmod n$, và vì vậy theo định lý Fermat tổng quát thì $z^{r-} \equiv b^{L(n)} \equiv 1 \bmod n,$ tức là bậc của *z* là *r* (cũng có thể xem là nếu $z^r \equiv 1 \bmod n$ giữ bậc của *z* chia *r* , vì *r* là ước số nguyên tố của $L(n)$ nên *r* là bậc của một số các số modulo *n*). Khi thực hiện thủ tục này hai lần thì có thể tính được hai giá trị ngẫu nhiên bậc *r* mod *n*.

Xác suất để hai giá trị như thế thuộc cùng một nhóm con cyclic là tỷ số của số phần tử không phải là phần tử sinh trong nhóm con cyclic của số nguyên tố bậc *r* với số phần tử có bậc *r* và được chứa trong Z_n^*. Nhóm Z_n^* chứa nhóm con cơ sở bậc r^2 và được tạo bởi hai phần tử có bậc *r*. Nhóm con cơ sở như vậy chứa $r^2 - 1$ phần tử có bậc *r*. Do đó, xác suất được xác định trước đó là $\frac{r}{r^2-1} \approx \frac{1}{r} \approx 2^{-80}$. Xác suất

này có thể được bỏ qua vì thời gian sử dụng trong thủ tục kiểm tra việc tạo ra giá trị α và β thuộc cùng một nhóm con cyclic có bậc r không cần phải thực hiện.

Xác suất này có thể được giảm tới $\approx 2^{-160}$ khi tạo ra giá trị α và β theo thuật toán thay đổi dưới đây:

Thuật toán 3.3

1) Chọn giá trị ngẫu nhiên b, sao cho $1 < b < n$

2) Tính $\gamma = L(n)/r^2$ và $z = b^{\gamma} \bmod n$

3) Nếu $z \neq 1$, và giá trị $\alpha'(\beta') = z^r \bmod n \neq 1$, thì α (β) lấy giá trị $\alpha'^r \bmod n$ ($\beta'^r \bmod n$). Ngược lại thì lặp lại bước 1-3

Việc giảm xác suất đạt được là bởi vì những giá trị được tạo trước có bậc r^2, số này được tăng tới luỹ thừa r và kết quả được lấy là các giá trị α (β).

Nếu các giá trị α', β' có bậc r^2 thuộc các nhóm con cyclic khác nhau G_{r^2} thì các giá trị α và β sẽ cũng thuộc các nhóm con cyclic khác nhau. Xác suất $\Pr(\alpha, \beta \in G_{r^2})$ mà α và β cùng chung nhóm con cyclic là tỷ số của số phần tử có bậc r^2 trong một nhóm con cyclic với số phần tử có bậc r^2 trong Z_n^*. Với sự có mặt của nhóm con cơ sở trong Z_n^* được tạo ra bởi hai phần tử có bậc r^2 thì việc thể hiện số phần tử của các nhóm cơ sở đó theo xác suất được ước lượng như sau:

$$\Pr(\alpha, \beta \in G_{r^2}) = \frac{r(r-1)}{r^2(r^2-1)} \approx \frac{1}{r^2} \approx 2^{-160} \qquad (3.5)$$

Vì vậy, thuật toán thứ hai tạo ra hai giá trị ngẫu nhiên α và β được ưu tiên vì nó giảm thiểu đáng kể xác suất tạo ra α và β thuộc cùng một nhóm con cyclic là xấp xỉ với 2^{80}.

Để tạo ra số nguyên tố p có cấu trúc $p = Nr + 1$ và có kích thước $\approx \lambda$, trong đó r là số nguyên tố ρ-bit đã cho, có thể sử dụng thuật toán sau:

Thuật toán 3.4

1) Tạo một số nguyên tố ngẫu nhiên π có kích thước $\lambda - \rho$ và tính $p = 2\pi r + 1$

2) Thiết lập bộ đếm có $i = 0$

3) Tạo giá trị nguyên ngẫu nhiên $\mu < p$

4) Nếu 4 điều kiện sau đạt là: $\mu^{2\pi r} = 1 \bmod p$, $\mu^{\pi r} \neq 1 \bmod p$, $\mu^{2\pi} \neq 1 \bmod p$ và $\mu^{2r} \neq 1 \bmod p$ thì tới bước 6, ngược lại thì tới bước 5

5) Nếu $i < 20$ thì về lại bước 3, ngược lại thì về lại bước 1

6) Kết quả đầu ra là số nguyên tố $p = 2\pi r + 1$

Để tạo số nguyên tố *p* có cấu trúc $p = Nr^2 + 1$ và kích thước $\approx \lambda$, trong đó *r* là số nguyên tố ρ-bit đã cho, có thể sử dụng thuật toán sau:

Thuật toán 3.5

1) Tạo số nguyên tố ngẫu nhiên π có kích thước là $\lambda - 2\rho$ và tính $p = 2\pi r^2 + 1$

2) Thiết lập bộ đếm $i = 0$

3) Tạo giá trị nguyên ngẫu nhiên $\mu < p$

4) Nếu 4 điều kiện sau đạt là: $\mu^{2\pi r^2} = 1 \bmod p$, $\mu^{\pi r^2} \neq 1 \bmod p$, $\mu^{2\pi r} \neq 1 \bmod p$ và $\mu^{2r^2} \neq 1 \bmod p$, thì tới bước 6, ngược lại thì tới bước 5

5) Nếu $i < 20$ thì về lại bước 3, ngược lại thì về lại bước 1

6) Kết quả đầu ra là số nguyên tố $p = 2\pi r + 1$.

Thuật toán 3.4 và 3.5 làm việc chính xác, vì việc thực hiện các điều kiện chỉ ra ở bước 4 có nghĩa là giá trị μ có bậc $\omega_p = p - 1 \bmod p$. Thật vậy do định lý Euler nên với bất kỳ hợp số *n* nào cũng không tồn tại các số có bậc là $n - 1 \bmod n$.

Có thể thay đổi thuật toán trên để giảm đáng kể thời gian yêu cầu để tạo ra số nguyên tố có kích thước lớn, tuy nhiên thuật toán 3.4 là đủ áp dụng trong thực tế, do những số nguyên tố có dạng $p = 2\pi r + 1$ chỉ được tạo ra ở giai đoạn tạo khoá riêng và khoá công khai.

3.3.3. Xây dựng lược đồ ký số cơ sở dựa trên bài toán khó mới đề xuất

a) Tạo khoá

Phần này xây dựng một lược đồ chữ ký số 240-bit và được sử dụng như thuật toán ký số cơ sở khi thiết kế lược đồ ký số mù.

Trong lược đồ cơ sở này, giả sử các tham số (n, α, β, r) được tạo ra bởi một bên tin cậy sử dụng các số nguyên tố lớn *p* và *q* được chọn ngẫu nhiên và có kích thước theo mức độ an toàn yêu cầu. Sau khi tính các tham số (n, α, β, r) thì các số bí mật *p* và *q* sẽ bị hủy.

Người yêu cầu tạo khoá riêng của mình là cặp số nguyên ngẫu nhiên *x* và *w* với $(1 < x < r; 1 < w < r)$ và tính khoá công khai *y* theo công thức $y = \alpha^x \beta^w \bmod n$.

Khi tạo chữ ký số, người ký chỉ sử dụng số bí mật *x* và *w*. Do đó, để giả mạo chữ ký, kẻ tấn công phải tính toán được *x* và *w* từ khoá công khai *y* đã biết và các giá trị cơ sở là α và β. Đây được xem là bài toán DLP trên cơ sở đa chiều. Trong trường hợp xem xét là hai chiều, bài toán DLP modulo *n* được cho bên dưới và chỉ ra rằng bài toán DLP có cùng độ khó như bài toán IFP. Nếu có một thuật toán đa thức hiệu quả để tính toán bài toán DLP hai chiều thì nó có thể được chuyển đổi thành thuật toán đa thức để phân tích thừa số modulo *n*. Bởi vì bài toán IFP và DLP modulo số nguyên là những bài toán khó nên bài toán DLP và IFP là những bài toán rất khác nhau.

Trường hợp đặc biệt: Là trường hợp giải bài toán DLP modulo một hợp số với cấu trúc đặc biệt. Chọn số $n = pq$ với *p* và *q* là hai số nguyên tố lớn và $(p-1)$ và $(q-1)$ chứa hệ số nguyên tố lớn *r*. Trong trường hợp này, một nhóm hữu hạn của

các số nghịch đảo modulo *n* được tạo ra bởi thành phần cơ sở chứa hai thành phần có giá trị α và β, bậc của nó chứa ước số *r*. Giả sử là *y* chứa trong nhóm này và được yêu cầu tính giá trị *x* và *w* theo công thức:

$$y = \alpha^x \beta^w \bmod n \tag{3.6}$$

Bài toán này có thể được gọi là bài toán DLP hai chiều hoặc DLP trên cơ sở hai chiều. Bài toán này có thể được giảm tới bài toán DLP thông thường.

Từ (3.6), có được hệ đồng dư thức như sau:

$$\begin{cases} y = \alpha^x \beta^w \equiv g^c \bmod p \\ y = \alpha^x \beta^w \equiv g'^{c'} \bmod q \end{cases} \tag{3.7}$$

g và g' tương ứng là căn nguyên thuỷ modulo *p* và *q*. Giải bài toán DLP thông thường nhiều lần, tính được *c*, c', *u*, *v*, u' và v' như sau:

$$\begin{cases} \alpha = g^u \bmod p, \beta = g^v \bmod p \\ \alpha = g'^u \bmod q, \beta = g'^v \bmod q \end{cases}$$

Sử dụng các giá trị đã được tính là *c*, c', *u*, *v*, u' và v', hệ đồng dư thức có thể được viết như sau:

$$\begin{cases} g^{ux+vw} \equiv g^c \bmod p \\ g'^{u'x+v'w} \equiv g'^{c'} \bmod q \end{cases} \tag{3.8}$$

Từ (3.8) tính được:

$$\begin{cases} ux + vw \equiv c \bmod (p-1) \\ u'x + v'w \equiv c' \bmod (q-1) \end{cases} \tag{3.9}$$

Từ hai hệ đồng dư tuyến tính này, có thể tính giá trị chưa biết *x* và *w* , nó xác định toạ độ của các giá trị logarit rời rạc hai chiều yêu cầu.

b) Tạo chữ ký

1) Chọn giá trị ngẫu nhiên $1 < k < r$ và $1 < t < r$ và tính $R = \alpha^k \beta^t \bmod n$

2) Tính thành phần ρ-bit đầu tiên: $E = H(M \| R) \bmod r$ (sử dụng hàm băm 2ρ-bit đặc biệt $H(M)$ [52])

3) Tính thành phần ρ-bit thứ hai: $S = (k + xE) \bmod r$

4) Tính thành phần ρ-bit thứ ba: $U = (t + xE) \bmod r$

Bộ ba (E, S, U) là chữ ký của thông điệp *M*. Kích thước của chữ ký là cố định và bằng 3ρ. Hai tham số ρ và λ được chọn phụ thuộc vào mức độ an toàn yêu cầu của lược đồ. Để cung cấp mức độ an toàn 80-bit (hoặc 128-bit), sử dụng tham số $\rho \geq 80$ (hoặc $\rho \geq 128$) và $\lambda \geq 512$ (hoặc $\lambda \geq 1232$).

c) Kiểm tra chữ ký

Tính $\tilde{R} = y^{-E} \alpha^{S} \beta^{U} \bmod n$ và $\tilde{E} = H\left(M \| \tilde{R}\right) \bmod r$, nếu $\tilde{E} = E$ thì chữ ký hợp lệ, ngược lại thì chữ ký không hợp lệ.

3.3.4. Xây dựng lược đồ chữ ký số mù dựa trên lược đồ chữ ký số cơ sở

Lược đồ chữ ký số mù đề xuất bao gồm ba pha và hai bên tham gia là người yêu cầu **A** và người ký **B**. Lược đồ ký số mù mới dựa trên lược đồ cơ sở được trình bày trong 3.3.3 và được mô tả như sau:

a) Tạo khoá

Người ký **B** tạo khoá riêng của mình là cặp số nguyên ngẫu nhiên *x* và *w* với $(1 < x < r; 1 < w < r)$ và tính khoá công khai *y* theo công thức: $y = \alpha^{x} \beta^{w} \bmod n.$

b) Tạo chữ ký

Có 4 vòng trong lược đồ ký số mù. Người ký thực hiện ký một thông điệp *M* đã được làm mù như sau:

1) Vòng 1 (người ký **B**):

+ Chọn giá trị ngẫu nhiên $1 < k < r$ và $1 < t < r$ và tính $\bar{R} = \alpha^{k} \beta^{t} \bmod n$

+ Gửi $\bar{R}$ tới người yêu cầu A.

2) Vòng 2 (người yêu cầu **A**):

+ Bước 1: Tạo 3 giá trị ngẫu nhiên (ε, μ, τ) sao cho $(1 < \varepsilon, \mu, \tau < r)$

+ Bước 2: Tính

$$R = \bar{R}^{\varepsilon} y^{\mu} \alpha^{\tau} \bmod n,\ \tilde{E} = H\left(M \| \tilde{R}\right) \bmod r,\ \bar{E} = \varepsilon^{-1}(E + \mu) \bmod r$$

Nếu $\bar{E} = 0$ thì lặp lại bước 2 với những tham số mù ngẫu nhiên mới. Ngược lại, gửi $\bar{E}$ tới người ký B.

Lưu ý: *E* là thành phần đầu tiên của chữ ký trên *M* (xem hình 3.1).

3) Vòng 3 (người ký **B**):

Sử dụng giá trị *t*, *k* riêng và khoá bí mật *x*, *w* của mình tính: $\bar{S} = (k + x\bar{E}) \bmod r$ và $\bar{U} = (t + w\bar{E}) \bmod r$ và gửi $\bar{U}$, $\bar{S}$ tới người yêu cầu A.

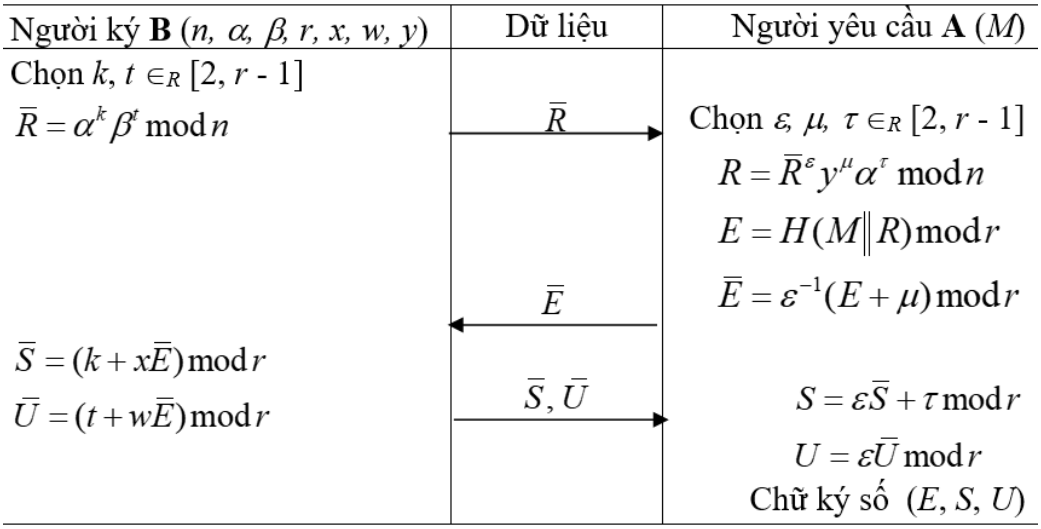
4) Vòng 4 (người yêu cầu **A**): tính thành phần thứ 2 và thứ 3 của chữ ký số mù là: $S = \varepsilon\bar{S} + \tau \bmod r$ và $U = \varepsilon\bar{U} \bmod r$.

Bộ 3 các giá trị (E, S, U) là chữ ký số mù trên thông điệp *M*, và kích thước chữ ký số là $|E| + |S| + |U| \approx 3|r| \approx 240$ bit.

c) Kiểm tra chữ ký

1) Sử dụng các giá trị của chữ ký số mù (*E, S, U*) để tính: $\tilde{R} = y^{-E} \alpha^{S} \beta^{U} \bmod n$ và $\tilde{E} = H\left(M \| \tilde{R}\right) \bmod r$

2) So sánh: nếu $\tilde{E} = E$ thì chữ ký hợp lệ, ngược lại là không hợp lệ.



Hình 3.1. Tóm tắt thuật toán ký số của lược đồ chữ ký số mù đề xuất

3.3.5. Xây dựng lược đồ ký số tập thể mù mới

Lược đồ ký số mù đề xuất trong phần 3.3.4 có thể được sử dụng để thiết kế lược đồ ký số tập thể mù mới. Lược đồ bao gồm 3 pha là: pha tạo khoá, pha tạo chữ ký và pha kiểm tra. Giả sử rằng tập thể người ký **B** là $\{B_1, B_2, ..., B_m\}$ muốn tạo ra chữ ký số tập thể mù cho thông điệp *M* được đề xuất bởi người yêu cầu **A**.

a) Tạo khoá

Tập thể người ký **B** tạo các tham số sau:

1) $(x_1, x_2, ..., x_m)$ và $(w_1, w_2, ..., w_m)$ là các khoá bí mật của tập thể người ký sao cho $1 < x_i < p$ và $1 < w_i < p$, x_i, w_i với $(i = 1, 2, ..., m)$ được chọn ngẫu nhiên và chỉ có người ký B_i biết.

2) $(y_1, y_2, ..., y_m)$ là các khoá công khai của tập thể người ký sao cho $y_i = \alpha^{x_i} \beta^{w_i} \bmod n$ được công khai bởi tập thể người ký B_i.

3) Khoá công khai tập thể *y* được tính như là sự kết hợp của các khoá công khai riêng lẻ y_i của tất cả các người ký: $Y = \prod_{i=1}^{m} y_i \bmod n$.

b) Tạo chữ ký

Có 4 vòng trong lược đồ ký số tập thể mù. Tập thể người ký **B** ký thông điệp được làm mù *M* như sau:

1) Vòng 1 (mỗi người ký B_i):

+ Tạo hai giá trị ngẫu nhiên $1 < k_i < r; 1 < t_i < r$ và tính $r_i = \alpha^{k_i}\beta^{t_i} \bmod n$

+ Gửi r_i tới tất cả những người ký khác tính giá trị ngẫu nhiên chung là $\bar{R} = \prod_{i=1}^{m} r_i \bmod n,$ gửi $\bar{R}$ cho người yêu cầu **A**

2) Vòng 2 (người yêu cầu **A**):

+ Bước 1: tạo 3 giá trị ngẫu nhiên (ε, μ, τ) sao cho $1 < \varepsilon, \mu, \tau < r$

+ Bước 2: Tính

$R = \bar{R}^{\varepsilon} y^{\mu} \alpha^{\tau} \bmod n,\ E = H(M \| R) \bmod r\ ,\ \bar{E} = \varepsilon^{-1}(E + \mu) \bmod r$

Nếu $\bar{E} = 0$ thì lặp lại bước 2 với các tham số mù ngẫu nhiên mới, ngược lại gửi $\bar{E}$ tới người ký B_i (xem hình 3.2).

3) Vòng 3 (mỗi người ký B_i):

+ Sử dụng các tham số t_i, k_i và khoá bí mật x_i, w_i riêng của mình và tính $s_i = (k_i + x_i\bar{E}) \bmod r$ và $u_i = (t_i + w_i\bar{E}) \bmod r$

+ Gửi (s_i, u_i) tới tất cả những người ký khác và tính các tham số chung của tập thể: $\bar{S} = \sum_{i=1}^{m} s_i = (\sum_{i=1}^{m} k_i + \bar{E}\sum_{i=1}^{m} x_i) \bmod r$ và $\bar{U} = \sum_{i=1}^{m} u_i = (\sum_{i=1}^{m} t_i + \bar{E}\sum_{i=1}^{m} w_i) \bmod r$

+ Gửi $(\bar{U}, \bar{S})$ tới người yêu cầu A

4) Vòng 4 (người yêu cầu A): tính hai thành phần còn lại của chữ ký số tập thể mù là: $S = \varepsilon\bar{S} + \tau \bmod r$ và $U = \varepsilon\bar{U} \bmod r.$

Bộ 3 giá trị (*E, S, U*) là chữ ký số tập thể mù của thông điệp *M*, và kích thước chữ ký là $|E|+|S|+|U| \approx 3|r| \approx 240$ bit. Kích thước không phụ thuộc số người ký và là 3ρ.

c) Kiểm tra chữ ký

1) Sử dụng các giá trị của chữ ký số tập thể mù (E,S,U) để tính các giá trị: $\tilde{R} = Y^{-E}\alpha^{S}\beta^{U} \bmod n$ và $\tilde{E} = H\left(M \| \tilde{R}\right) \bmod r$.

2) So sánh: nếu $\tilde{E} = E$ thì chữ ký hợp lệ, ngược lại chữ ký không hợp lệ.

Người ký $\mathbf{B_i}$ $(n, \alpha, \beta, r, x_i, w_i, y)$	Dữ liệu	Người yêu cầu **A** (M)
Chọn $k_i, t_i \in_R [2, r-1]$ $r_i = \alpha^{k_i}\beta^{t_i} \bmod n$		
$\bar{R} = \prod_{i=1}^{m} r_i \bmod n$	$\bar{R}$ →	Chọn $\varepsilon, \mu, \tau \in_R [2, r-1]$ $R = \bar{R}^{\varepsilon} y^{\mu}\alpha^{\tau} \bmod n$ $E = H(M \| R) \bmod r$
$s_i = (k_i + x_i\bar{E}) \bmod r$ $u_i = (t_i + w_i\bar{E}) \bmod r$	← $\bar{E}$	$\bar{E} = \varepsilon^{-1}(E+\mu) \bmod r$
$\bar{S} = \sum_{i=1}^{m} s_i = (\sum_{i=1}^{m} k_i + \bar{E}\sum_{i=1}^{m} x_i) \bmod r$		
$\bar{U} = \sum_{i=1}^{m} u_i = (\sum_{i=1}^{m} t_i + \bar{E}\sum_{i=1}^{m} w_i) \bmod r$	$\bar{S}, \bar{U}$ →	$S = \varepsilon\bar{S} + \tau \bmod r$ $U = \varepsilon\bar{U} \bmod r$ Chữ ký số (E, S, U)

Hình 3.2. Tóm tắt thuật toán ký số của lược đồ ký số tập thể mù đề xuất

3.3.6. Đánh giá các lược đồ đề xuất

3.3.6.1. Tính đúng

Định lý 3.6 (chữ ký số cơ sở): Bộ 3 giá trị (*E, S, U*) là chữ ký số hợp lệ tương ứng với thông điệp *M*.

***Chứng minh*:** Thay thế các giá trị *y, U* và *S* vào bên phải của phương trình kiểm tra $\tilde{R} = y^{-E}\alpha^{S}\beta^{U} \bmod n$:

$$\tilde{R} = y^{-E}\alpha^{S}\beta^{U} \bmod n = \left(\alpha^{x}\beta^{w}\right)^{-E}\alpha^{S}\beta^{U} \bmod n$$
$$= \alpha^{-Ex}\beta^{-Ew}\alpha^{(k+xE)}\beta^{(t+wE)} \bmod n$$
$$= \alpha^{-Ex}\beta^{-Ew}\alpha^{k}\alpha^{xE}\beta^{t}\beta^{wE} \bmod n$$
$$= \alpha^{k}\beta^{t} \bmod n$$
$$= R$$
$$\Rightarrow \tilde{E} = H(M \,||\, \tilde{R}) = H(M \,||\, R) = E.$$

Kết quả cho thấy lược đồ đảm bảo tính đúng của lược đồ ký số cơ sở.

Định lý 3.7 (chữ ký số mù): Bộ 3 giá trị (*E*, *S*, *U*) là chữ ký số mù hợp lệ tương ứng với thông điệp *M*.

Chứng minh: Thay thế các giá trị *E*, *U* và *S* vào bên phải của phương trình kiểm tra $\tilde{R} = y^{-E}\alpha^{S}\beta^{U} \bmod n$:

$$\tilde{R} = y^{-E}\alpha^{S}\beta^{U} \bmod n$$
$$= y^{-\varepsilon\bar{E}+\mu}\alpha^{\varepsilon\bar{S}+\tau}\beta^{\varepsilon\bar{U}} \bmod n$$
$$= y^{-\varepsilon\bar{E}}y^{\mu}\alpha^{\varepsilon\bar{S}}\alpha^{\tau}\beta^{\varepsilon\bar{U}} \bmod n$$
$$= (y^{-\bar{E}}\alpha^{\bar{S}}\beta^{\bar{U}})^{\varepsilon}\, y^{\mu}\alpha^{\tau} \bmod n$$
$$= \bar{R}^{\varepsilon}\, y^{\mu}\alpha^{\tau} \bmod n$$
$$= R$$
$$\Rightarrow \tilde{E} = H(M \,||\, \tilde{R}) = H(M \,||\, R) = E.$$

Kết quả cho thấy, lược đồ đảm bảo tính đúng và chữ ký số (*E*, *S*, *U*) được biết bởi **A** mà không được biết bởi **B**.

Định lý 3.8 (chữ ký số tập thể mù): Bộ 3 giá trị (*E*, *S*, *U*) là chữ ký số tập thể mù hợp lệ tương ứng với thông điệp *M*.

Chứng minh: phần chứng minh này sử dụng khoá công khai của tập thể người ký *Y*. Thay thế các giá trị *E*, *U* và *S* vào bên phải của phương trình kiểm tra $\tilde{R} = Y^{-E}\alpha^{S}\beta^{U} \bmod n$:

$$\tilde{R} = Y^{-E}\alpha^{S}\beta^{U} \bmod n = Y^{-\varepsilon\bar{E}+\mu}\alpha^{\varepsilon\bar{S}+\tau}\beta^{\varepsilon\bar{U}} \bmod n$$
$$= Y^{-\varepsilon\bar{E}}Y^{\mu}\alpha^{\varepsilon\bar{S}}\alpha^{\tau}\beta^{\varepsilon\bar{U}} \bmod n$$
$$= (Y^{-\bar{E}}\alpha^{\bar{S}}\beta^{\bar{U}})^{\varepsilon}Y^{\mu}\alpha^{\tau} \bmod n$$
$$= (Y^{-\bar{E}}\alpha^{\sum_{i=1}^{m}s_i}\beta^{\sum_{i=1}^{m}u_i})^{\varepsilon}Y^{\mu}\alpha^{\tau} \bmod n$$
$$= (Y^{-\bar{E}}\alpha^{\sum_{i=1}^{m}s_i}\beta^{\sum_{i=1}^{m}u_i})^{\varepsilon}Y^{\mu}\alpha^{\tau} \bmod n$$
$$= \left(\prod_{i=1}^{m} y_i^{-\bar{E}}\alpha^{s_i}\beta^{u_i}\right)^{\varepsilon} Y^{\mu}\alpha^{\tau} \bmod n$$
$$= \left(\prod_{i=1}^{m} r_i\right)^{\varepsilon} Y^{\mu}\alpha^{\tau} \bmod n$$

$$= \bar{R}^{\varepsilon}Y^{\mu}\alpha^{\tau} \bmod n$$
$$= R$$
$$\Rightarrow \tilde{E} = H(M \,||\, \tilde{R}) = H(M \,||\, R) = E$$

Kết quả cho thấy, lược đồ đảm bảo tính đúng và chữ ký số tập thể mù (*E, S, U*) được biết đến đối với **A** và không được biết đối với mỗi người ký B_i.

3.3.6.2. Tính không thể truy vết

Định lý 3.9 (chữ ký số mù): Lược đồ đề xuất bảo đảm không thể truy vết khi thông điệp *M* và chữ ký (*E, S, U*) được chuyển cho người ký.

Chứng minh: Gọi $(\bar{E}_1, \bar{S}_1, \bar{U}_1)$ và $(\bar{E}_2, \bar{S}_2, \bar{U}_2)$ là hai bộ chữ ký số mù khác nhau và được lưu trữ bởi người ký B. Theo phương trình của thủ tục tạo chữ ký, có được mối liên hệ như sau:

$$\varepsilon = U/\bar{U} \bmod r;\ \tau = S - U\bar{S}/U \bmod r \text{ và } U = U\bar{E}/U - E \bmod r.$$

Điều đó chỉ ra rằng chữ ký (*E, S, U*) có thể được tạo ra bởi người yêu cầu $\mathbf{A}_1$ từ bộ ba $(\bar{E}_1, \bar{S}_1, \bar{U}_1)$ (trong trường hợp giả sử A_1 sử dụng các giá trị ε_1, τ_1 và σ_1) và chữ ký như vậy cũng có thể được tạo ra bởi người yêu cầu A_2 từ người ký B là bộ ba $(\bar{E}_2, \bar{S}_2, \bar{U}_2)$ (trong trường hợp giả sử A_2 đã sử dụng các giá trị ε_2, τ_2 và σ_2). Do

các giá trị (ε, τ và σ) được chọn ngẫu nhiên nên chữ ký số có thể được tạo ra từ mỗi cặp bộ ba được xem xét cũng như từ mỗi các bộ ba trong cơ sở dữ liệu, tức là lược đồ đảm bảo thuộc tính không truy vết (hay đảm bảo tính mù).

Định lý 3.10 (chữ ký số tập thể mù): Lược đồ đề xuất đảm bảo thuộc tính không thể truy vết khi thông điệp *M* và chữ ký (*E, S, U*) được chuyển tới tất cả hoặc tới một người ký.

Chứng minh: Giả sử rằng có nhiều người yêu cầu khác nhau trình thông điệp *M* tới một số tập thể người ký xác định và những người ký đã lưu tất cả bộ ba $(\bar{E}, \bar{S}, \bar{U})$ chữ ký số trong thủ tục ký số tập thể mù.

Gọi $(\bar{E}_1, \bar{S}_1, \bar{U}_1)$ và $(\bar{E}_2, \bar{S}_2, \bar{U}_2)$ là hai bộ ba chữ ký số. Theo cấu trúc của lược đồ ký số tập thể mù, các thành phần của bộ ba chữ ký số đầu tiên thỏa mãn biểu thức sau:

$$\varepsilon = U / \bar{U} \bmod r;\ \tau = S - U\bar{S} / U \bmod r \text{ và } U = U\bar{E} / U - E \bmod r$$

Mối liên hệ đó chỉ rằng, chữ ký (*E, S, U*) có thể được tạo ra bởi người yêu cầu A_1 từ bộ ba $(\bar{E}_1, \bar{S}_1, \bar{U}_1)$ (trong trường hợp giả sử A_1 đã sử dụng các giá trị ε_1, τ_1 và σ_1) và chữ ký như vậy cũng có thể được tạo ra bởi người yêu cầu A_2 với một số người ký B_i từ bộ ba chữ ký $(\bar{E}_2, \bar{S}_2, \bar{U}_2)$ (trong trường hợp giả sử A_2 đã sử dụng các giá trị ε_2, τ_2 và σ_2). Vì các giá trị ($\varepsilon, \tau, \sigma$) được chọn ngẫu nhiên nên chữ ký số có thể được tạo ra từ mỗi cặp bộ ba được xem xét cũng như là từ mỗi những bộ ba trong cơ sở dữ liệu, tức là thuộc tính không truy vết được cung cấp bởi lược đồ.

3.3.6.3. Tính không thể giả mạo

Tính không thể giả mạo chỉ ra rằng chỉ có người ký (tập thể người ký) mới có thể tạo ra chữ ký hợp lệ

Tấn công 1 (tấn công bởi bên ngoài): Kẻ tấn công cố gắng dò tìm chữ ký (*E, S, U*) của thông điệp *M* đã cho bằng cách chọn cố định một trong những giá trị *R, E,*

S và U và tìm các giá trị khác còn lại, ở đây $R = y^{-E}\alpha^{S}\beta^{U} \bmod n$ và $E = H(M \| R) \bmod r$. Chẳng hạn, kẻ tấn công chọn R và cố gắng tìm các giá trị còn lại là E, S và U thỏa mãn công thức $R = y^{-E}\alpha^{S}\beta^{U} \bmod n$ và ngược lại. Kẻ tấn công đầu tiên chọn ngẫu nhiên R và sau đó tính các giá trị S và U, và chỉ thực hiện được nếu bài toán DLP modulo một hợp số bị phá vỡ. Hoặc là kẻ tấn công đầu tiên chọn giá trị ngẫu nhiên E và sau đó tính R, giả sử là lược đồ sử dụng một hàm băm an toàn, do đó kẻ tấn công không thể tính được giá trị R từ giá trị E được chọn đặc biệt. Tương tự, đầu tiên kẻ tấn công có thể chọn giá trị ngẫu nhiên S (hoặc U) và sau đó tính E và U (hoặc S), và cũng chỉ thực hiện được nếu bài toán DLP modulo một hợp số bị phá vỡ.

Tấn công 2 (tấn công bởi người yêu cầu): Người yêu cầu có thể biết được những chữ ký riêng lẻ nhưng không thể phá vỡ được tính an toàn của lược đồ. Nếu người yêu cầu không thể tính toán được chữ ký số mù (chữ ký số tập thể mù) chính xác từ những chữ ký riêng lẻ thì phương trình kiểm tra chữ ký số mù (chữ ký số tập thể mù) sẽ không thể thỏa mãn. Loại tấn công này có thể phát hiện bởi quá trình kiểm tra chữ ký.

Tấn công 3 (tấn công bởi người ký hoặc tập thể người ký): Giả sử rằng có $(m-1)$ người ký là những kẻ tấn công cố gắng tính khoá bí mật của người ký m. Khi chia sẻ chữ ký tập thể $(\bar{E}, \bar{S}, \bar{U})$ với người ký m, những kẻ tấn công đó biết (r_m, s_m, u_m) được tạo bởi m và thỏa mãn phương trình $r_m = y_m{}^{-\bar{E}}\alpha^{s_m}\beta^{u_m} \bmod n$, trong đó $\bar{E}$ nằm ngoài tầm kiểm soát của những kẻ tấn công. Do đó, việc tính toán khoá bí mật của người ký m yêu cầu phải giải bài toán DLP modulo một hợp số.

3.3.6.4. Đánh giá độ phức tạp thời gian các lược đồ đề xuất

Phần này đánh giá độ phức tạp thời gian của các lược đồ đề xuất dựa trên số phép tính nhân, số phép tính hàm băm, số ngẫu nhiên phát sinh, số phép tính nghịch đảo và số phép tính luỹ thừa.

Bảng 3.4 và bảng 3.5 so sánh độ phức tạp thời gian thực hiện bởi người yêu cầu, người ký và người kiểm tra giữa các lược đồ ký số mù đề xuất và các lược đồ trong [69] và [93].

Bảng 3.4. Chi phí thời gian của lược đồ đề xuất và lược đồ [69], [93]

Loại phép tính	Thực hiện bởi người yêu cầu			Thực hiện bởi người ký		
	Lược đồ đề xuất	[69]	[93]	Lược đồ đề xuất	[69]	[93]
Phép tính luỹ thừa	3	3	7	2	2	2
Phép tính nghịch đảo	1	1	4	0	0	0
Phép tính hàm băm	1	1	3	0	0	1
Phép tính nhân	5	4	11	3	1	2
Số lượng số ngẫu nhiên	3	2	2	2	1	1

Bảng 3.5. Chi phí thời gian của lược đồ đề xuất và lược đồ [69], [93]

Loại phép tính	Thực hiện bởi người kiểm tra		
	Lược đồ đề xuất	[69]	[93]
Phép tính luỹ thừa	3	3	4
Phép tính hàm băm	1	1	1
Phép tính nhân	2	1	1
Phép tính nghịch đảo	1	0	0

Bảng 3.6 so sánh độ phức tạp thời gian được thực hiện bởi người yêu cầu và người kiểm tra giữa lược đồ ký số tập thể mù đề xuất và lược đồ trong [70] và [72].

Bảng 3.4, 3.5, 3.6 cho thấy độ phức tạp thời gian của lược đồ chữ ký số tập thể mù đề xuất thì hầu như là bằng với lược đồ [69], [70], [72], [93]. Trong đó, lược đồ trong [69] và [93] là lược đồ chữ ký số tập thể mù dựa trên hai bài toán khó là IFP và DLP giống như lược đồ đề xuất ở phần này. Tuy nhiên, lược đồ trong [69] và

[93] dựa trên nhóm cyclic, trong khi lược đồ đề xuất dựa trên bài toán khó mới đề xuất là dựa trên nhóm con hữu hạn không vòng hai chiều.

Bảng 3.6. Chi phí thời gian của lược đồ đề xuất và lược đồ [70], [72]

Loại phép tính	Thực hiện bởi người yêu cầu			Thực hiện bởi người kiểm tra		
	Lược đồ đề xuất	[70]	[72]	Lược đồ đề xuất	[70]	[72]
Phép tính luỹ thừa	3	2	2	3	2	2
Phép tính nghịch đảo	1	0	0	1	1	1
Phép tính hàm băm	1	1	1	1	1	1
Phép tính nhân	5	3	2	2	1	1
Số lượng số ngẫu nhiên	3	2	2	0	0	0

Lược đồ được sử dụng so sánh trong [70] là dựa trên bài toán khó mới do các tác giả trong [70] đề xuất, trong khi lược đồ trong [72] thì chỉ dựa trên bài toán DLP. Kết quả cho thấy lược đồ mới dựa trên bài toán khó mới do NCS đề xuất khi so sánh với các lược đồ dựa trên hai bài toán khó, một bài toán khó hay bài toán khó do tác giả đề xuất trong [70] đều cho độ phức tạp thời gian là gần như tương đương. Tuy nhiên, lược đồ đề xuất có kích thước chữ ký số ngắn hơn nhiều so với các lược đồ trong [69], [70], [72], [93], và do đó có thể ứng dụng nhiều hơn trong thực tế, nhất là ở các hạ tầng triển khai ứng dụng có tài nguyên thấp. Kết quả so sánh được thể hiện trong bảng 3.7.

Bảng 3.7. Kích thước chữ ký của lược đồ đề xuất và [69], [70], [72], [93]

Kích thước chữ ký	Các lược đồ đề xuất	[69]	[93]	[70]	[72]
Số bit	240	1,184	2,048	1,184	320

3.4. KẾT LUẬN CHƯƠNG 3

Chương 3 xây dựng lược đồ chữ ký số mù, chữ ký số tập thể mù dựa trên lược đồ phổ biến là Schnorr và RSA để kế thừa tính an toàn và hiệu quả (*đây là hướng nghiên cứu thứ 2 đã được đề cập trong chương 1*). Do lược đồ dựa trên hai bài toán khó nên để phá vỡ lược đồ sẽ mất rất nhiều thời gian để giải hai bài toán khó. Vì vậy mà lược đồ đề xuất này có thể sử dụng trong các ứng dụng yêu cầu thời gian lưu trữ kết quả đủ lâu. Kết quả này được công bố trong công trình [CT5].

Phần kế tiếp của chương 3 là phần quan trọng nhất của chương này cũng như của luận án này là đề xuất bài toán khó mới dựa trên nhóm con hữu hạn không vòng hai chiều. Trên cơ sở đó xây dựng lược đồ chữ ký số mù mới dựa trên độ khó của bài toán DLP modulo một hợp số nguyên $n = p*q$. Lược đồ đề xuất có tính an toàn cao do giảm xác suất phá vỡ tiềm năng vì yêu cầu giải pháp tiềm năng phải giải được hai vấn đề khó về tính toán như tìm logarit rời rạc modulo số nguyên tố và phân tích hợp số n chứa hai số nguyên tố chưa được biết. Khi chọn các tham số có độ an toàn 80-bit thì chữ ký số trong lược đồ ký số mù đề xuất có kích thước 240 bits (và không phụ thuộc vào số người ký). Kết quả này được công bố trong công trình [CT1].

Trong hầu hết các ứng dụng dựa trên các chữ ký số mù, người ký (tập thể người ký) thường phải xử lý nhiều phép tính hơn người yêu cầu, trong khi khả năng tính toán của người yêu cầu có thể bị hạn chế trong một số tình huống xác định như sử dụng thiết bị di động,... nên để bảo đảm chất lượng của các dịch vụ dựa trên chữ ký số mù thì điều qua trọng là giảm tải tính toán cho phía người yêu cầu so với người ký (tập thể người ký). Các lược đồ đề xuất trong phần này đáp ứng xu thế đó. Các chứng minh về tính hiệu quả và an toàn của các lược đồ chữ ký số đề xuất thể hiện rằng, nếu việc lựa chọn các tham số cẩn thận trong thực tế sẽ giúp cho việc sử dụng các lược đồ đề xuất trong các ứng dụng thực tế là hoàn toàn khả thi.

CHƯƠNG 4. ỨNG DỤNG LƯỢC ĐỒ CHỮ KÝ SỐ TẬP THỂ MÙ ĐỀ XUẤT VÀO LƯỢC ĐỒ BẦU CỬ ĐIỆN TỬ

4.1. GIỚI THIỆU

Hiện nay, trong khi xã hội hiện đại hoàn toàn dựa vào CNTT cho các hoạt động của Chính phủ, kinh doanh, công việc và giải trí…, thì việc sử dụng CNTT để ra quyết định dân chủ vẫn còn ở giai đoạn nghiên cứu và hoàn thiện. Đã có một số nước sử dụng bầu cử điện tử để người dân thực hiện quyền dân chủ của mình, tuy nhiên thách thức chính trong các hệ thống bầu cử điện tử hiện có là vấn đề bảo đảm tính bảo mật và tính ẩn danh cho cử tri. Cho đến nay, nhiều giải pháp thiết kế hệ thống bầu cử điện tử đã được đề xuất. Tuy nhiên, không có một giải pháp nào hoàn chỉnh trong cả lý thuyết và thực tiễn. Vì vậy, các nhà nghiên cứu cố gắng dựa trên các hệ mật cơ bản để xây dựng các chương trình bầu cử điện tử với hiệu quả cao để đáp ứng các yêu cầu đó.

Bầu cử điện tử đã thu hút nhiều sự quan tâm gần đây và có nhiều lược đồ đã được đề xuất. Các lược đồ có thể được chia thành ba cách tiếp cận chính là (i) dựa trên các lược đồ chữ ký mù [14], [104], (ii) các lược đồ dựa trên mã hóa đồng cấu [10], [40], [60] và (iii) các lược đồ dựa trên mạng hỗn hợp [37], [61], [76]. Đồng thời cũng có một số lược đồ dựa trên cơ sở lai ghép giữa mã hóa đồng cấu và mạng hỗn hợp [50], [86]. Ngoài ra cũng có một số công bố gần đây như đề xuất các yêu cầu, thiết kế và thực hiện khi thiết kế hệ thống bầu cử điện tử [33], đề xuất chữ ký số mù an toàn ứng dụng cho bầu cử điện tử [77], hệ thống bầu cử điện tử dựa trên nền tảng android [81], hệ thống bầu cử điện tử sử dụng cho điện thoại di động android [65], ứng dụng bầu cử điện tử cải tiến sử dụng hạ tầng android [32], cơ chế kiểm tra bầu cử sử dụng mã hóa mới cho hệ thống bầu cử điện tử trên cơ sở cam kết bit và chữ ký số mù [17], sử dụng chữ ký số mù dựa trên định danh sử dụng cho hệ thống bầu cử điện tử [64] và lược đồ bầu cử điện tử không truy vết dựa trên cặp chữ ký số [52].

Trong các loại tiếp cận trên thì việc ứng dụng chữ ký số mù vào hệ thống bầu cử điện tử đang là một hướng nghiên cứu được các nhà nghiên cứu quan tâm vì nó bảo đảm được tính ẩn danh của cử tri khi đi bầu giống như bỏ phiếu truyền thống, vì không một cử tri nào muốn việc mình bỏ phiếu cho ai bị người khác biết được. Ngoài ra, vì mọi phiếu bầu đều được làm mù và giải mù chỉ bởi cử tri tương ứng nên có thể được xác minh một cách công khai, rộng rãi [43], [51].

Một lược đồ bầu cử điện tử an toàn phải đảm bảo đáp ứng các tính chất sau đây đã được đề xuất trong [31].

+ Tính riêng tư của cử tri: Phải đảm bảo rằng các cử tri đủ điều kiện bỏ phiếu đều có thể bỏ phiếu, nhưng không thể kết nối danh tính cử tri với nội dung phiếu bầu của họ và cử tri có thể bỏ phiếu nặc danh.

+ Không lộ thông tin bầu cử: người bỏ phiếu không thể có được bất kỳ thông tin nào để chứng minh cho người cưỡng chế rằng cử tri đã bỏ phiếu như thế nào. Thuộc tính này nhằm ngăn chặn việc mua hoặc bán phiếu bầu.

+ Chống cưỡng chế: Một lược đồ bầu cử được cho là ngăn chặn việc cưỡng ép nếu cử tri không thể hợp tác với người cưỡng chế để chứng minh với họ rằng cử tri đã bỏ phiếu như thế nào và cũng chống việc mua bán phiếu bầu.

+ Tính chính xác: Chỉ những cử tri đủ điều kiện mới có thể bỏ phiếu. Không ai có thể bỏ phiếu nhiều lần. Phiếu bầu đã gửi không thể thay đổi. Tất cả các phiếu hợp lệ đều được kiểm đếm.

+ Công bằng: Không bên tham gia nào có thể biết được thông tin gì về việc bỏ phiếu ngoại trừ phiếu bầu của mình, không có bất cứ phần kết quả nào được tiết lộ trước giai đoạn kiểm phiếu.

+ Khả năng kiểm chứng: phiếu bầu phải được kiểm chứng độc lập bởi cử tri khi đã được đưa vào kiểm phiếu và phải được kiểm đếm chính xác.

+ Dân chủ: mỗi cử tri đủ điều kiện có quyền bỏ phiếu của mình và không được phép yêu cầu bất cứ ai bỏ phiếu theo ý mình.

+ Tính mạnh mẽ: lược đồ bỏ phiếu phải được bảo mật và không bị xâm phạm bởi những ứng viên nhằm ngăn chặn mọi hành vi gây hại cho cử tri bởi chính quyền hoặc người lạ.

Tuy nhiên, đạt được tất cả các yêu cầu trên là một thách thức lớn. Chương này đề xuất một lược đồ bỏ phiếu điện tử mới sử dụng 2 chữ ký của cơ quan có thẩm quyền bầu cử. Một chữ ký trên phiếu bầu đã được cử tri làm mù được tạo ra bởi nhiều thành viên của cơ quan có thẩm quyền để đảm bảo tính chính xác của việc xây dựng phiếu bầu. Ngoài ra, còn có một chữ ký khác trên mỗi cử tri như là ký trên token chứa thông tin đã được làm mù cho phép cử tri thực hiện bầu cử trong các giai đoạn bầu cử ẩn danh. Đồng thời, để cho phép một cử tri đăng ký được ẩn danh, sử dụng lược đồ thông qua chứng chỉ dựa trên thông tin ẩn danh được đề xuất trong [91]. Lược đồ bầu cử đề xuất sử dụng lược đồ chữ ký số tập thể mù và các lược đồ này đã được chứng minh là mù vô điều kiện. Ngoài ra, do có nhiều cơ quan có thẩm quyền độc lập và mỗi cơ quan gồm nhiều người tham gia trong lược đồ bầu cử nên lược đồ bầu cử hoàn toàn tin cậy, trừ khi tất cả các thành viên trong mỗi cơ quan và tất cả các cơ quan liên kết với nhau để phá hoại cuộc bầu cử.

4.2. TỔNG QUAN VỀ HỆ THỐNG BẦU CỬ ĐIỆN TỬ

Một hệ thống bầu cử thường gồm có các thành phần: các cử tri là người đi bỏ phiếu; Ban tổ chức bầu cử thì có ủy ban bầu cử sẽ quản lý chung toàn bộ quá trình bầu cử; Ban điều hành (**BĐH**) quản lý việc thực hiện bỏ phiếu và có thể đóng vai trò là bên trung gian (hay còn gọi là **TTP**) trong quá trình gửi yêu cầu và ký trong một số phần của lược đồ bầu cử; Ban kiểm phiếu (**BKP**) sẽ thực hiện chức năng ký phiếu bầu, nhận phiếu, kiểm phiếu và công bố kết quả bầu cử.

Theo phương thức bỏ phiếu truyền thống, cử tri mang chứng minh nhân dân hoặc thẻ căn cước công dân và lá phiếu chưa có nội dung gì đến bàn đóng dấu, ở đó người ta kiểm tra giấy tờ để xác minh quyền bỏ phiếu, sau đó đóng dấu xác thực lên lá phiếu. Cử tri vào phòng bỏ phiếu, như vậy lá phiếu hoàn toàn không có thông tin định danh. Quá trình bỏ phiếu kiểu này được coi là "*nặc danh*".

Trong một hệ thống bầu cử điện tử, các cử tri sẽ gửi yêu cầu xác thực, yêu cầu chữ ký, bỏ phiếu và kiểm tra qua mạng internet mà không đến trực tiếp điểm bỏ phiếu như hình thức bỏ phiếu truyền thống. Theo phương thức bỏ phiếu điện tử, mỗi lá phiếu phải có thông tin định danh. Nó có thể là một con số *x* nào đó và phải khác nhau. Trên mỗi lá phiếu phải có chữ ký trên số định danh *x*, thì lá phiếu mới có giá trị để bầu cử. Cử tri biến đổi *x* thành *y* trước khi đưa cho **BKP** kí xác nhận. **BKP** ký vào *y*, mà không biết đó là số định danh *x* đã bị che dấu. **BKP** trao chữ ký trên *y* là *z* cho cử tri. Cử tri "xóa mù" trên *z* sẽ được chữ ký của **BKP** trên số định danh *x*, như vậy cử tri có quyền bầu cử.

4.3. CÁC LƯỢC ĐỒ CHỮ KÝ SỐ SỬ DỤNG TRONG LƯỢC ĐỒ BẦU CỬ ĐIỆN TỬ ĐỀ XUẤT

Phần này trình bày sơ lược về các lược đồ chữ ký số được sử dụng trong lược đồ bầu cử điện tử đề xuất [CT6]. Đó là lược đồ chữ ký số tập thể mù dựa trên lược đồ Schnorr và lược đồ chữ ký số tập thể mù dựa trên lược đồ EC-Schnorr do NCS nghiên cứu và đề xuất trong luận án ở chương 2. Việc sử dụng các lược đồ dựa trên lược đồ Schnorr để xây dựng mô hình do nó dễ hiểu và dễ thực hiện khi sử dụng hệ mật khóa công khai và được nhiều nghiên cứu trong những năm gần đây. Lược đồ đề xuất trong phần này dựa trên mô hình được trình bày trong [52], tuy nhiên khác biệt ở đây là [52] sử dụng lược đồ chữ ký số mù đơn của Chaum [12] cho việc ký lên token đã được làm mù và lược đồ chữ ký số mù của Hwang [58] để xây dựng phiếu bầu. Trong khi lược đồ chữ ký số được sử dụng trong phần này là lược đồ chữ ký số tập thể mù do NCS đề xuất, cụ thể là lược đồ chữ ký số tập thể mù dựa trên lược đồ EC- Schnorr [CT2], sử dụng để xây dựng phiếu bầu được ký mù và lược đồ chữ ký số tập thể mù dựa trên lược đồ Schnorr [CT3] sử dụng cho việc ký mù trên token xác minh thông tin cử tri.

Lược đồ bầu cử điện tử đề xuất trong [52] sử dụng các lược đồ chữ ký số mù đơn trong hệ thống có nhiều người ký (là các thành viên của ban điều hành, ở đây xem như có *m* người). Trong giai đoạn đăng ký, cử tri làm mù token T_j thành hai phần khác nhau, các thành viên ban kiểm phiếu ký vào cả hai phần đó, sau đó cử tri

mới giải mù để được chữ ký trên T_j. Giả sử 3 thành viên ban kiểm phiếu thì cử tri V_j phải làm mù token của mình thành 6 phần khác nhau. Các thành viên BKP_i ký lên 6 phần đó, sau đó cử tri giải mù cả 6 phần chữ ký đó. Ở giai đoạn bỏ phiếu, là phiếu v_j của cử tri V_j cũng được làm mù thành hai phần khác nhau, do đó mà với 3 BKP_i thì cử tri phải làm mù phiếu bầu thành 6 phần khác nhau bằng cách sử dụng hai bộ khóa công khai của 3 BKP_i, đó phiếu bầu v_j cũng được ký thành 6 phần khác nhau do 3 BKP_i ký. Trong giai đoạn kiểm phiếu, cử tri phải giải mù phiếu bầu đã được ký của mình thành 6 phần khác nhau. Do đó mà thời gian tính toán để làm mù token, phiếu bầu, ký vào token; ký vào token và phiếu bầu đã được làm mù và giải mù token, phiếu bầu mù đã được ký là tỷ lệ thuận với số lượng thành viên ban kiểm phiếu BKP_i tham gia vào lược đồ bầu cử. Đồng thời hệ thống yêu cầu dung lượng lưu trữ phải lớn.

Trong khi đó, lược đồ bầu cử điện tử đề xuất sử dụng các lược đồ chữ ký số tập thể mù nên cử tri không quan tâm đến số lượng thành viên ban điều hành, ban kiểm phiếu mà chỉ gửi một token hoặc một phiếu bầu được làm mù cho tập thể thành viên đó và họ tự ký và tạo chữ ký tập thể và gửi lại cử tri nên sẽ giảm thời gian tính toán và dung lượng lưu trữ của hệ thống.

Đồng thời với việc sử dụng lược đồ dựa trên bài toán ECDLP nên độ dài khóa cũng sẽ ngắn hơn bài toán RSA và DLP nên có thể sử dụng được trong các mạng có năng lực xử lý thấp như tốc độ đường truyền, khả năng lưu trữ và năng lực tính toán của hệ thống như ứng dụng trong các thiết bị Iot, thẻ thông minh,…

4.3.1. Lược đồ chữ ký số tập thể mù dựa trên Schnorr

Lược đồ chữ ký số tập thể mù trong [CT3] có 5 pha được mô tả như sau:

Pha tạo khóa: Người ký (*ở đây là Ban kiểm phiếu* - **BKP**), chọn tham số hệ thống là (p, q, g); hai số nguyên tố p, q với $q|(p-1)$; phần tử sinh g có bậc q (tức là $g^q \bmod p \equiv 1 \bmod p$); và khoá bí mật là d với $1 < d < q$.

Mỗi thành viên của **BKP** là BKP_i tính khoá công khai ρ_i của mình và gửi cho bên thứ ba tin cậy (*ở đây là ban điều hành bầu cử* - **BĐH**) để tính khoá công khai của tập thể **BKP** là ρ như sau:

$$\rho_i = g^{d_i} \bmod p, i = 1,2,...,m \ \rho = \prod_{i=1}^{n} \rho_i \bmod p$$

Mỗi thành viên của ban kiểm phiếu BKP_i chọn một giá trị ngẫu nhiên $k_i \in Z_q^*$, tính c_i và gửi tới **BĐH** để tính $\overline{c}$, $\overline{c}$ được gửi tới các cử tri, với:

$$c_i = g^{k_i} \bmod p, i = 1,2,...,m \ \overline{c} = \prod_{i=1}^{m} c_i \bmod p = g^{\sum_{i=1}^{m} k_i \bmod q} \bmod p$$

Khoá công khai là $(\rho, g, \overline{c})$ và khoá bí mật là (d). **BKP** giữ bí mật (p,q,d) và công khai $(\rho, g, \overline{c})$.

Pha làm mù: Cử tri V_j có một thông điệp (*ở đây là token* T_j), và cử tri này muốn **BKP** ký lên token T_j đã được làm mù của mình. Cử tri V_j làm mù T_j của mình bằng cách chọn hai giá trị ngẫu nhiên $\alpha, \beta \in \{1,2,...,q-1\}$ và tính:

$$\begin{cases} c = \overline{c} g^{\alpha} \rho^{\beta} \bmod p; h = H(T_j \| c) \\ r = h \bmod q; \overline{r} = (r - \beta) \bmod q \end{cases}$$

Cử tri gửi $\overline{r}$ cho **BKP**. $\overline{r}$ là token của V_j đã được làm mù.

Pha ký số : Khi nhận $\overline{r}$ từ V_j, mỗi thành viên BKP_i sử dụng các giá trị riêng của mình là (k_i, d_i) để tính s_i: $s_i = k_i - d_i \overline{r} \bmod q$, và gửi tới **BĐH** để tính chữ ký số tập thể $\overline{s}$: $\overline{s} = \sum_{i=1}^{m} s_i \bmod q$ và gửi $\overline{s}$ tới cử tri V_j.

Pha giải mù: Sau khi nhận $\overline{s}$ từ **BĐH**, cử tri V_j giải mù bằng cách tính s theo công thức: $s = (\overline{s} + \alpha) \bmod q$. Cặp số (r, s) là chữ ký trên token của cử tri V_j.

Pha kiểm tra: Cặp (r,s) là chữ ký trên token T_j. Bất kỳ ai cũng có thể kiểm tra tính hợp lệ của chữ ký số bằng cách tính c' và r' và so sánh r' với *r*, nếu $r' = r$ thì chữ ký được chấp nhận, ngược lại thì chữ ký không được chấp nhận, với:

$$c' = g^s \rho^r \bmod p;\quad r' = H(T_j \| c') \bmod q$$

4.3.2. Lược đồ chữ ký số tập thể mù dựa trên EC-Schnorr

Lược đồ chữ ký số tập thể mù đề xuất trong [CT2] sử dụng đường cong elliptic có dạng: $y^2 = x^3 + ax + b \bmod p$; p là số nguyên tố lớn tạo trường *GF*(*p*) của đường cong elliptic; q là số nguyên tố chỉ số lượng nhóm điểm của đường cong elliptic; *P* là điểm của đường cong có bậc *q; G* là điểm khác gốc *O* của đường cong elliptic và có toạ độ là (x_G, y_G); *H*(*M*) là giá trị của hàm băm; d' là khoá riêng của người ký và $1 < d' < q$. Lược đồ này gồm 5 pha và được mô tả như sau:

Pha tạo khóa: Trong pha này, ban kiểm phiếu thực hiện như sau: Mỗi thành viên BKP_i (*trong mô hình này xem như có* ***m*** *thành viên của ban kiểm phiếu*) tính giá trị khóa công khai P_i: $P_i = d'_i \times G$ của mình và gửi đến **BĐH** để tính giá trị khóa công khai tập thể của **BKP** là *P*: $P = P_1 + P_2 + ... + P_m = \sum_{i=1}^{m} d'_i \times G$ với *i=1,2…m*

Mỗi BKP_i chọn ngẫu nhiên giá trị k_i với $k_i \in Z_q$ và tính C_i: $C_i = k_i \times G$, sau đó gửi đến **BĐH** để tính $\bar{C}$ chung: $\bar{C} = \sum_{i=1}^{m} C_i = \sum_{i=1}^{m} k_i \times G$. Khóa công khai của **BKP** là $(P, G, \bar{C})$ và khóa bí mật là (d').

Pha làm mù: Cử tri V_j có thông điệp (*ở đây là phiếu bầu* v_j) và muốn có chữ ký của **BKP**. Cử tri V_j chọn ngẫu nhiên 2 giá trị $\alpha, \beta \in \{1,2,...,q-1\}$, tính $C = \bar{C} + \alpha \times G + \beta \times P$; $r = H(v_j, x_C) \bmod q; \bar{r} = (r - \beta) \bmod q$ và gửi $\bar{r}$ cho **BKP**.

Pha ký số: Sau khi nhận $\bar{r}$ từ cử tri V_j, **BKP** thực hiện ký như sau: Mỗi thành viên BKP_i sử dụng các giá trị bí mật (d_i, k_i) của mình để tính s_i:

$s_i = k_i - d_i\overline{r} \bmod q$, và gửi đến **BĐH** để tính $\overline{s}$: $\overline{s} = \sum_{i=1}^{m} s_i \bmod q$, và gửi cho cử tri V_j.

Pha giải mù: Sau khi nhận $\overline{s}$ từ **BĐH**, cử tri V_j tính $s = (\overline{s} + \alpha) \bmod q$, cặp (*r*,*s*) là chữ ký số trên phiếu bầu v_j. Sau đó V_j chuyển (v_j, r, s) cho **BKP.**

Pha kiểm tra: Kết quả cặp (r, s) là chữ ký trên phiếu bầu v_j. Bây giờ bất kỳ ai cũng có thể kiểm tra tính hợp lệ của chữ ký bằng cách: tính $C' = s \times G + r \times P$ và $r' = H(v_j, x_{C'})$. Nếu $r' = r$ thì chữ ký là đúng.

4.3.3. Chữ ký số trên token được làm mù

+ Cử tri có thể bầu cử mà không tiết lộ danh tính của mình khi chứng minh tính hợp lệ (*đủ điều kiện bỏ phiếu*) của mình bằng cách sử dụng token. Để chứng minh tính hợp lệ bằng cách ẩn danh, cử tri V_j làm mù token T_j của mình bằng cách chọn hai giá trị ngẫu nhiên $\alpha_j, \beta_j \in \{1,2,...,q-1\}$ và sử dụng các tham số công khai của tập thể ban kiểm phiếu **BKP** là $(\rho, g, \overline{c})$ để tính:

$$\begin{cases} c_j = \overline{c} g^{\alpha_j} \rho^{\beta_j} \bmod p; h_j = H(T_j \| c_j) \\ r_j = h_j \bmod q; \overline{r}_j = (r_j - \beta_j) \bmod q \end{cases}$$

Việc xác nhận định danh của cử tri V_j bởi thông tin xác thực dựa trên thông tin ẩn danh là $T_j(A, ID_j, Z_j)$ của V_j.

+ Các thành viên của ban kiểm phiếu BKP_i $(i = 1,2,...,m)$ ký trên token đã được làm mù là $\delta_j(\alpha_j, \beta_j, T_j) = \overline{r}_j$ bằng cách sử dụng các giá trị riêng của mình là (k_i, d_i) và tính s_i: $s_i = k_i - d_i\overline{r}_j \bmod q;$ và gửi tới **BĐH** để tính chữ ký số tập thể $\overline{s}_j$: $\overline{s}_j = \sum_{i=1}^{m} s_i \bmod q$.

Cử tri V_j giải mù thành token đã được ban kiểm phiếu ký bằng cách tính: $s_j = (\overline{s}_j + \alpha_j) \bmod q$. Cặp giá trị (r_j, s_j) là chữ ký số trên token của cử tri V_j.

Gọi $s_1(T_j) = r_j$ là thành phần thứ nhất và $s_2(T_j) = s_j$ là thành phần thứ hai của chữ ký số của **BKP** trên token T_j. Do các thành viên BKP_i đã ký mà không biết T_j nên không ai ngoài V_j biết được (s_j, r_j) là từ V_j.

4.3.4. Chữ ký trên phiếu bầu được làm mù

+ Trong pha gửi phiếu bầu, cử tri V_j sử dụng các hệ số làm mù của mình là (α'_j, β'_j) và khóa công khai của các thành viên ban kiểm phiếu là $(P, G, \overline{C})$ để làm mù phiếu bầu v_j của mình bằng cách tính:

$$C_j = \overline{C} + \alpha'_j \times G + \beta'_j \times P;\ r'_j = H(v_j, x_{C_j}) \bmod q;\ \overline{r}'_j = (r'_j - \beta'_j) \bmod q.$$

+ Các thành viên BKP_i ký lên $\gamma_j(\alpha'_j, \beta'_j, v_j) = \overline{r}'_j$ bằng cách sử dụng giá trị bí mật của mình là (d'_i, k'_i) để tính chữ ký của mình là $s'_i = k'_i - d'_i \overline{r}'_j \bmod q$, sau đó gửi **BĐH** để tính chữ ký chung của **BKP** là: $\overline{s}'_j = \sum_{i=1}^{m} s'_i \bmod q$.

+ V_j giải mù phiếu bầu của mình bằng cách tính $s'_j = (\overline{s}'_j + \alpha'_j) \bmod q$, cặp (s'_j, r'_j) là chữ ký số trên phiếu bầu v_j của cử tri V_j.

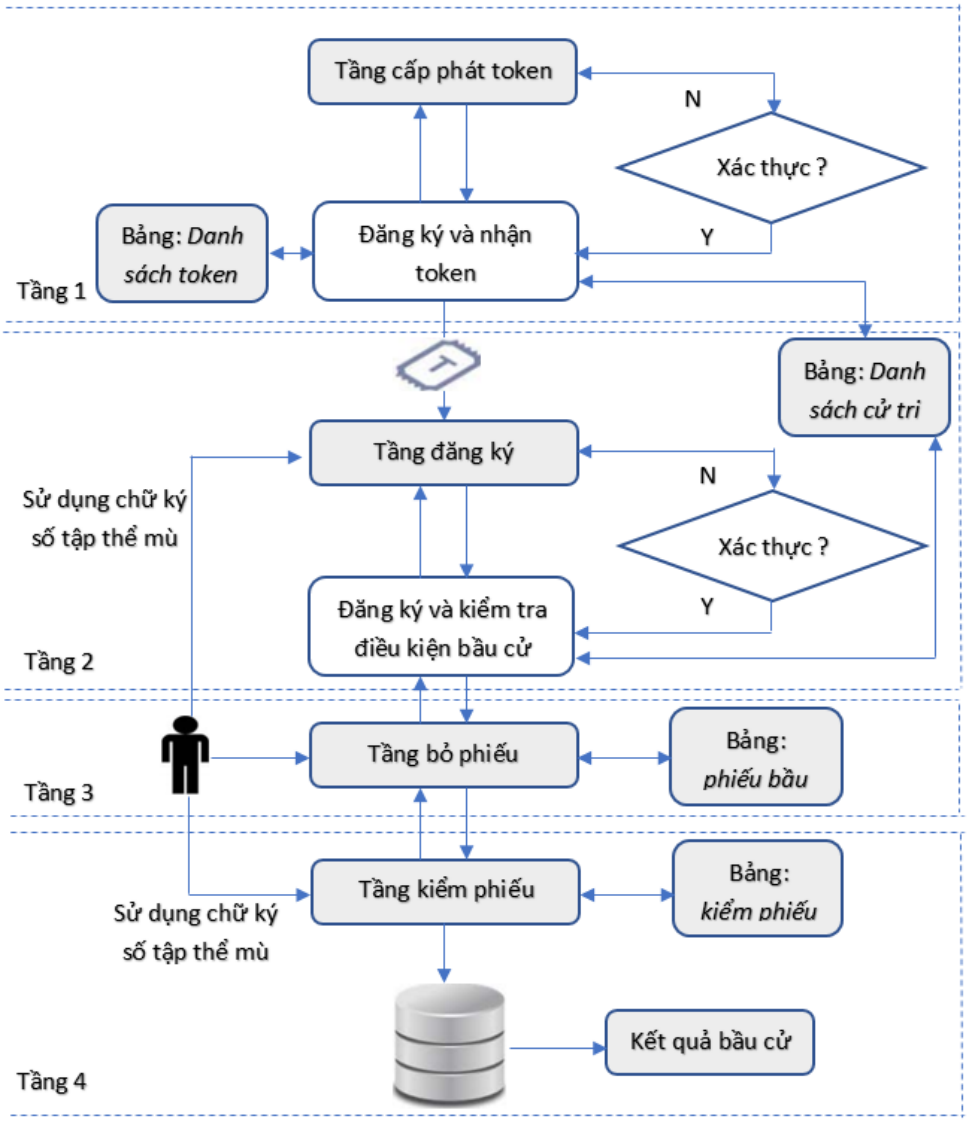
4.3.5. Xác thực thông tin dựa trên thông tin ẩn danh

Chứng chỉ dựa trên thông tin ẩn danh $T_j(A, ID_j, Z_j)$ được đề xuất trong [91] do cơ quan phát hành chứng chỉ (**CQPHCC**) cung cấp cho phép cử tri V_j chứng minh mình đủ điều kiện bỏ phiếu với bất kỳ cơ quan nào. Ví dụ: đầu tiên V_j cung cấp số định danh của mình cho **CQPHCC**, sau đó **CQPHCC** cung cấp thông tin xác thực $T_j(A, ID_j, Z_j)$ nếu cử tri V_j đủ điều kiện bỏ phiếu. Sau này, bất kỳ cơ quan có thẩm quyền nào đều có thể buộc V_j tính toán $U_j^{Z_j} \bmod n$ từ một số nguyên U_j sử dụng Z_j trong $T_j(A, ID_j, Z_j)$ mà không cần biết Z_j của V_j. Sau đó, bất kỳ cơ quan

có thẩm quyền nào đều có thể sử dụng con dấu $U_j^{Z_j}$ để xác thực V_j chính là cử tri tương ứng với $T_j(A, ID_j, Z_j)$. Tóm lại, cùng với việc sử dụng con dấu $U_j^{Z_j}$ được sử dụng thay thế thông tin $T_j(A, ID_j, Z_j)$, sẽ làm thỏa mãn tính ẩn danh, không liên kết, có thể xác minh, không thể chối bỏ và có thể hủy bỏ [37], [91].

4.4. LƯỢC ĐỒ BẦU CỬ ĐIỆN TỬ SỬ DỤNG LƯỢC ĐỒ CHỮ KÝ SỐ TẬP THỂ MÙ ĐỀ XUẤT DỰA TRÊN SCHNORR VÀ EC-SCHNORR

4.4.1. Cấu hình của lược đồ đề xuất



Hình 4.1. Kiến trúc tổng quan của lược đồ bầu cử điện tử đề xuất

Lược đồ bầu cử điện tử đề xuất gồm các thông số chính như sau:

+ Gọi *N* là số cử tri được quyền đi bầu, cử tri thứ *j* được ký hiệu là V_j

+ Ban điều hành bỏ phiếu: Gồm một hoặc nhiều người, ký hiệu là **BĐH**.

+ Ban kiểm phiếu: gồm *m* người ký hiệu là $BKP_i(i=1,...,m)$, $m \geq 2$, ký hiệu là **BKP**.

+ Cơ quan phát hành chứng chỉ xác thực thông tin: Ký hiệu là **CQPHCC**;

+ Bốn bảng dữ liệu chính của hệ thống được thiết kế là: ***danhsachcutri*** (danh dách cử tri), ***danhsachtoken*** (danh sách token chứa thông tin xác thực cử tri), ***bangphieubau*** (bảng chứa thông tin phiếu bầu) và ***bangkiemphieu*** (bảng chứa thông tin phiếu bầu được giải mù). Lược đồ này xem như các dữ liệu chứa thông tin công dân đã có và được cơ quan có thẩm quyền quản lý và được truy vấn trong phần cấp quyền bầu cử.

Hình 4.1 mô tả kiến trúc tổng quan của lược đồ bầu cử điện tử đề xuất. Trong đó, hoạt động của các bên tham gia chính trong lược đồ được mô tả như sau:

a) Cử tri (V_j): Mỗi cử tri V_j có mã định danh ID_j và mật khẩu để chứng minh tính hợp lệ của mình tới cơ quan phát hành chứng chỉ **CQPHCC** để nhận được thông tin ẩn danh $T_j(A, ID_j, Z_j)$ từ **CQPHCC**.

+ V_j sử dụng giá trị $U_j^{Z_j}$ để chứng minh việc mình nhận được token T_j chưa được sử dụng bỏ phiếu và sử dụng hệ số làm mù bí mật của mình là α_j, β_j để làm mù token T_j thành $\delta_j(\alpha_j, \beta_j, T_j)$.

+ Cử tri V_j cũng sử dụng các tham số (α'_j, β'_j) để làm mù và giải mù phiếu bầu v_j của mình thành $\gamma_j(\alpha'_j, \beta'_j, v_j)$.

b) Ban điều hành bỏ phiếu (BĐH): BĐH kiểm tra tính hợp lệ ẩn danh của cử tri V_j sử dụng $T_j(A, ID_j, Z_j)$, chuyển $U_j^{Z_j}$ của cử tri vào bảng ***danhsachtoken***, chuyển phiếu bầu đã được làm mù vào ***bangphieubau*** và chuyển dữ liệu về cử tri, token và phiếu bầu làm mù vào các bảng ***danhsachcutri*** và ***bangkiemphieu***. **BĐH** cũng ký trên các T_j trước khi chuyển chúng vào bảng ***danhsachtoken***.

c) Ban kiểm phiếu (BKP):

Có $m \geq 2$ người trong ban kiểm phiếu. Mỗi thành viên BKP_i có trách nhiệm ký trên token được làm mù của cử tri và gửi cho **BĐH** tính chữ ký chung là $t_j(\alpha_j, \beta_j, T_j)$ và phiếu bầu đã được làm mù là $t_j(\alpha'_j, \beta'_j, v_j)$ bằng cách:

+ Mỗi BKP_i sử dụng khóa riêng (k_i, d_i) để ký trên token mù $\delta_j(\alpha_j, \beta_j, T_j)$ và gửi cho **BĐH** để tính chữ ký chung là $t_j(\alpha_j, \beta_j, T_j)$.

+ Mỗi BKP_i sử dụng cặp khóa riêng (d'_i, k'_i) để ký trên phiếu bầu được làm mù là $\gamma_j(\alpha'_j, \beta'_j, v_j)$ và gửi **BĐH** tính chữ ký chung là $t_j(\alpha'_j, \beta'_j, v_j)$.

d) Cơ quan phát hành chứng chỉ xác thực: CQPHCC có nhiệm vụ tạo và phát hành chứng chỉ xác thực dựa trên thông tin ẩn danh $T_j(A, ID_j, Z_j)$ cho V_j (*với A là thông tin của cơ quan phát hành chứng chỉ A*).

e) Bảng danh sách cử tri (*danhsachcutri*): Gồm 3 phần là "*ID*", "*thongtinxacthuc*" và "*token-mu*"

+ Trường "*ID"*: ID_j là thông tin mã định danh của cử tri hợp lệ V_j;

+ Trường "*thongtinxacthuc*": chứa thông tin về chứng chỉ xác thực dựa trên thông tin ẩn danh $T_j(A, ID_j, Z_j)$ của cử tri hợp lệ V_j;

+ Trường "*token-mu"*: chứa giá trị token đã được làm mù là $\delta_j(\alpha_j, \beta_j, T_j)$.

Bất kỳ ai cũng có thể thấy được bảng danh sách cử tri (bảng 4.1).

Bảng 4.1. Bảng danh sách cử tri (danhsachcutri)

ID	***thongtinxacthuc***	***token-mu***
ID_1	$T_1(A, ID_1, Z_1)$	$\delta_1(\alpha_1, \beta_1, T_1)$
…	…	…
ID_j	$T_j(A, ID_j, Z_j)$	$\delta_j(\alpha_j, \beta_j, T_j)$
…	…	…
ID_N	$T_N(A, ID_N, Z_N)$	$\delta_N(\alpha_N, \beta_N, T_N)$

f) Bảng chứa thông tin token (*danhsachtoken*): bao gồm thông tin token, con dấu $U_j^{Z_j}$ như là quyền ẩn danh của cử tri V_j đã có T_j.

+ Trường *"token"*: Chứa thông tin là một số duy nhất mà **BĐH** đã chuẩn bị trước để cấp cho cử tri.

+ Trường "*token-ttad*": Chứa thông tin ẩn danh của V_j. Khi cử tri V_j chọn token T_j, **BĐH** chuyển thông tin $U_j^{Z_j}$ vào phần "*token-ttad* " trong bảng ***danhsachtoken*** (bảng 4.2).

*Bảng 4.2. Bảng danh sách token (*danhsachtoken*)*

token	***token-ttad***
T_1	$U_1^{Z_1}$
…	…
T_j	$U_j^{Z_j}$
…	…
T_N	$U_N^{Z_N}$

g) Bảng thông tin về phiếu bầu (*bangphieubau*): bảng này chứa thông tin phiếu bầu đã được làm mù và phần xác nhận phiếu bầu đó.

+ Trường "*phieubau-mu*": Chứa thông tin của phiếu bầu đã được ký mù của cử tri thứ *j* tương ứng với T_j. Do đó mà ở phần bỏ phiếu, chữ ký của **BKP** trên phiếu bầu làm mù là $t_j(\alpha'_j, \beta'_j, v_j)$.

+ Trường "*xacthuc*": Chứa phần thứ nhất của chữ ký trên T_j là $s_1(T_j)$ như là phần xác thực của phiếu bầu trong bảng ***bangphieubau*** (bảng 4.3).

*Bảng 4.3. Bảng danh sách phiếu bầu đã làm mù (*bangphieubau*)*

phieubau-mu	*xacthuc*
$t_1(\alpha'_1, \beta'_1, v_1)$	$s_1(T_1) = r_1$
…	…
$t_j(\alpha'_j, \beta'_j, v_j)$	$s_1(T_j) = r_j$
…	…
$t_N(\alpha'_N, \beta'_N, v_N)$	$s_1(T_N) = r_N$

h) Bảng kiểm phiếu (*bangkiemphieu*): bảng này chứa phần phiếu bầu đã giải mù và phần xác thực.

+ Trường "*phieubau-giaimu*": Chứa thông tin phiếu bầu đã được giải mù bởi chính cử tri đó là: $s_j(\alpha'_j, \beta'_j, v_j)$.

+ Trường "*xacthuc*": chứa phần thứ hai của chữ ký tương ứng với T_j là $s_2(T_j)$, xem như cử tri xác nhận tính chính xác của chữ ký của **BKP** trên phiếu bầu đã được làm mù của mình. Ai cũng có thể theo dõi các cử tri đã bỏ phiếu và xác nhận phiếu bầu của họ trong bảng 4.4.

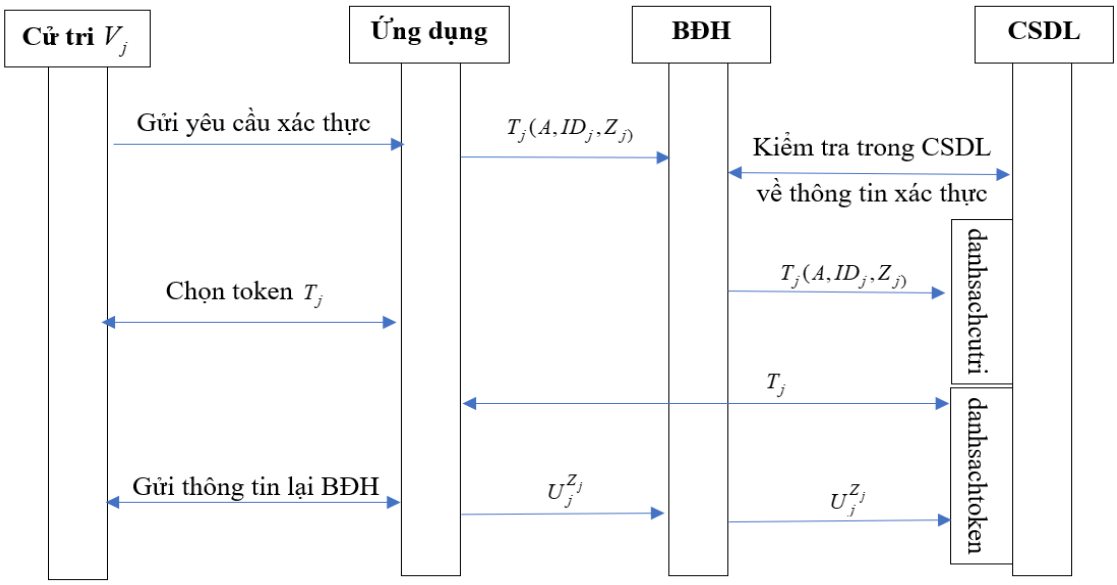
*Bảng 4.4. Bảng danh sách phiếu bầu đã được giải mù (*bangkiemphieu*)*

phieubau-giaimu	*xacthuc*
$s_1(\alpha'_1, \beta'_1, v_1)$	$s_2(T_1) = s_1$
…	…
$s_j(\alpha'_j, \beta'_j, v_j)$	$s_2(T_j) = s_j$
…	…
$s_N(\alpha'_N, \beta'_N, v_N)$	$s_2(T_N) = s_N$

4.4.2. Các tầng hoạt động của lược đồ đề xuất

Luồng dữ liệu và mối quan hệ của các thành phần trong lược đồ đề xuất bao gồm 4 tầng được trình bày như sau:

4.4.2.1. Tầng cấp phát token



Hình 4.2. Sơ đồ luồng dữ liệu của tầng cấp phát token

Trong tầng này, mỗi cử tri V_j nhận được token T_j là duy nhất trong hệ thống, trong khi vẫn duy trì tính ẩn danh của mình. Để đảm bảo tính ẩn danh cho cử tri, ít nhất N mã token được tạo trước và được đặt vào bảng ***danhsachtoken*** để cử tri chọn mã token cho mình. Trong đó N là số cử tri đủ điều kiện bỏ phiếu. Mỗi T_j trong bảng ***danhsachtoken*** đều có chữ ký của **BĐH** (chữ ký này khác với chữ ký của **BKP** là $\{s_1(T_j), s_2(T_j)\}$ và đảm bảo rằng T_j đã được chọn từ bảng ***danhsachtoken***). Trong tầng này, V_j và **BĐH** tương tác nhau như sau:

1) **BĐH** xác thực ẩn danh về tính hợp lệ của cử tri V_j bằng thông tin xác thực dựa trên thông tin ẩn danh [90].

2) Sau khi xác thực, **BĐH** chuyển $T_j(A, ID_j, Z_j)$ vào bảng ***danhsachcutri*** như trong bảng 4.1.

3) Cử tri V_j đã được xác thực, chọn token T_j chưa sử dụng trong bảng ***danhsachtoken*** (*token T_j đã có chữ ký của* **BĐH** *và chữ ký này không thể hiện trong lược đồ đề xuất*); chuyển $U_j^{Z_j}$ của mình cho **BĐH**.

4) Vì T_j đã được V_j chọn nên **BĐH** chuyển tham số $U_j^{Z_j}$ của V_j tương ứng vào bảng ***danhsachtoken*** như trong bảng 4.2.

Các vấn đề bảo mật của tầng này như sau:

+ Mỗi cử tri V_j có thể nhận được nhiều token: **BĐH** đặt tham số $U_j^{Z_j}$ của V_j tương ứng với T_j của cử tri đó trên bảng ***danhsachtoken*** để đổi lấy thông tin xác thực. Do đó V_j không thể yêu cầu nhiều token.

+ Mỗi cử tri có thể không nhận được token: Vì ít nhất có *N* token được tạo nên mọi cử tri đều có thể nhận được token. Nếu bất kỳ V_j nào không thể nhận được token, cử tri đó có thể yêu cầu nhiều lần.

+ Cử tri có thể sử dụng token do mình tự tạo: Trên T_j có chữ ký của **BĐH** và **BĐH** chỉ chấp nhận token có chữ ký của **BĐH**. Do đó V_j không thể sử dụng T_j của riêng mình tự tạo.

4.4.2.2. Tầng đăng ký

Trong tầng này (hình 4.3), ban kiểm phiếu ký trên T_j được làm mù của cử tri là $\delta_j(\alpha_j, \beta_j, T_j)$. Đầu tiên, cử tri V_j làm mù T_j của mình và sau đó các BKP_i ký mù trên chúng như được mô tả trong phần 4.3.3. Các BKP_i ký vào T_j mà không biết nội dung của nó. T_j đã được làm mù và được ký để chứng minh V_j đủ điều kiện của bỏ phiếu và ẩn danh trong các giai đoạn sau. Vì bảng ***danhsachcutri*** là công khai nên bất kỳ ai cũng có thể kiểm tra một V_j đã đăng ký nhưng không biết nội dung T_j vì T_j trên bảng ***danhsachcutri*** ở dạng mù. Trong tầng này, V_j và **BĐH** tương tác như sau:

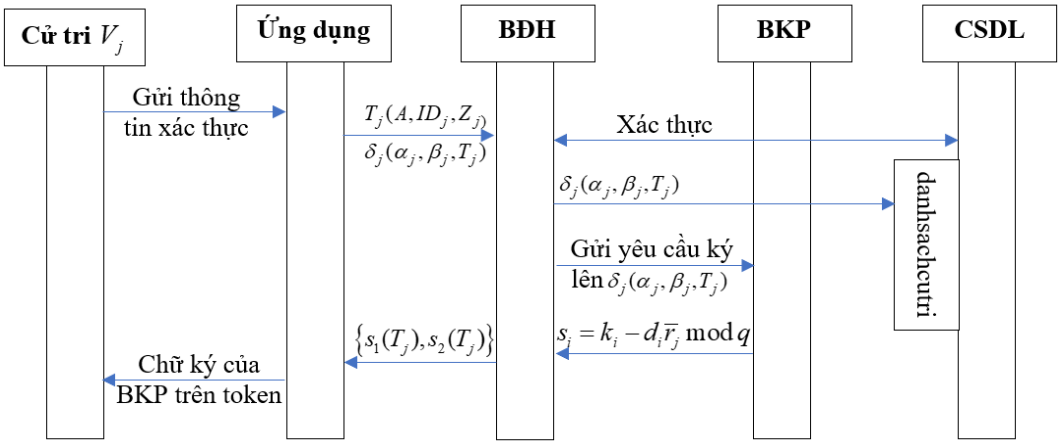
1) V_j làm mù token T_j của mình bằng cách sử dụng các giá trị bí mật của mình, tính $\delta_j(\alpha_j, \beta_j, T_j)$.

2) V_j chuyển thông tin xác thực $T_j(A, ID_j, Z_j)$ và token được làm mù là $\delta_j(\alpha_j, \beta_j, T_j)$ tới **BĐH**.

3) Sau khi xác thực, **BĐH** chuyển $\delta_j(\alpha_j, \beta_j, T_j)$ vào bảng ***danhsachcutri*** như trong bảng 4.1. **BĐH** cũng gửi $\delta_j(\alpha_j, \beta_j, T_j)$ tới các BKP_i để yêu cầu ký lên token.

4) Các BKP_i ký vào $\delta_j(\alpha_j, \beta_j, T_j)$ và gửi cho **BĐH** tính chữ ký số chung là $\{s_1(T_j), s_2(T_j)\}$ và gửi đến V_j.

5) V_j kiểm tra tính hợp lệ của chữ ký trên T_j được làm mù.



Hình 4.3. Sơ đồ luồng dữ liệu của tầng đăng ký

Các vấn đề bảo mật của tầng này như sau:

BĐH có thể đặt chữ ký không hợp lệ trên T_j được làm mù: V_j có thể chứng minh sự không trung thực của **BĐH** bằng cách chỉ ra $\delta_j(\alpha_j, \beta_j, T_j)$ và token đã được ký là không chính xác.

4.4.2.3. Tầng bỏ phiếu

Trong tầng bỏ phiếu (hình 4.4), cử tri V_j sử dụng thành phần thứ nhất của chữ ký trên token đã được làm mù của mình là $\{s_1(T_j)\} = (r_j)$ để xác thực. **BĐH** kiểm tra tính hợp lệ của V_j bằng cách xác minh chữ ký **BKP** trên T_j là $\{s_1(T_j)\}$. Sau đó, V_j làm mù phiếu bầu v_j của mình thành $\gamma_j(\alpha'_j, \beta'_j, v_j)$ như được mô tả trong phần 4.3.4. Sau đó V_j gửi $\gamma_j(\alpha'_j, \beta'_j, v_j)$ đến **BĐH** để đưa vào bảng ***bangphieubau***. Sau khi tìm thấy phiếu bầu đã được làm mù của mình trên bảng ***bangphieubau***, V_j xác nhận phiếu bầu đó bằng cách gửi $\{s_1(T_j)\}$ tới **BĐH** để được đăng trên phần xác thực (*xacthuc*) của bảng ***bangphieubau***. Do đó, bất kỳ ai cũng có thể kiểm tra một cử tri đã gửi phiếu bầu được làm mù mà không biết danh tính của cử tri và phiếu bầu thực tế. Cuối cùng, **BKP** ký vào phiếu bầu được làm mù của cử tri V_j và đưa vào bảng ***bangphieubau*** như được mô tả trong phần 4.3.4 là $t_j(\alpha'_j, \beta'_j, v_j)$. Thủ tục tạo phiếu bầu thể hiện trong hình 4.5. Trong tầng này, V_j và **BĐH** tương tác như sau:

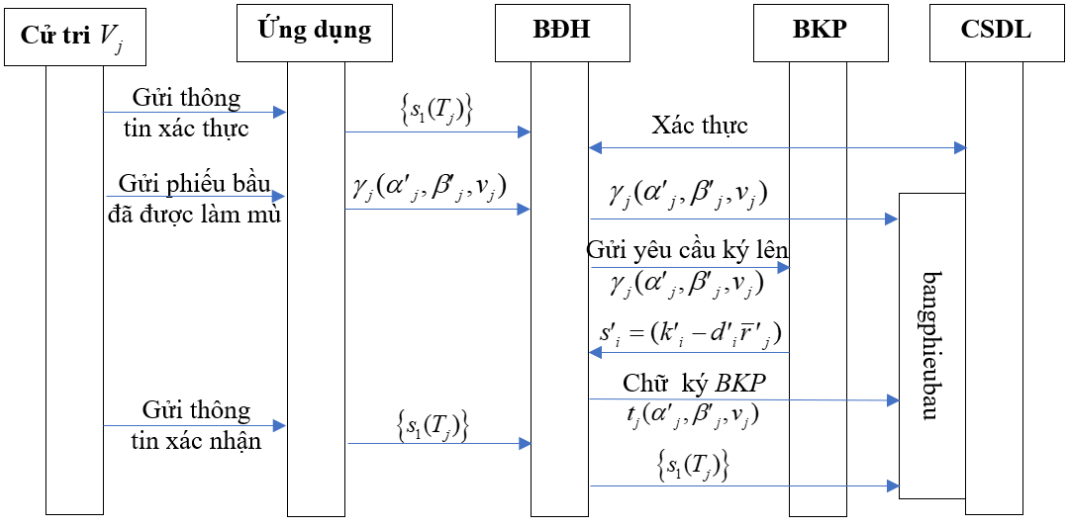
1) V_j gửi $\{s_1(T_j)\}$ cho **BĐH**. Bằng cách kiểm tra tính hợp lệ của chữ ký trên T_j để đảm bảo T_j không được sử dụng nhiều lần.

2) V_j làm mù phiếu bầu của mình bằng cách tính $\gamma_j(\alpha'_j, \beta'_j, v_j)$ như được trình bày trong phần 4.3.4.

3) V_j gửi $\gamma_j(\alpha'_j, \beta'_j, v_j)$ như là lá phiếu được làm mù cho **BĐH** để đăng nó trên bảng ***bangphieubau*** (*tuy nhiên, nó không được hiển thị trên bảng* ***bangphieubau***).

4) Bằng cách kiểm tra phiếu bầu được làm mù của mình trên trên bảng ***bangphieubau***, V_j xác nhận bằng cách gửi thành phần thứ nhất của chữ ký trên token đã được làm mù của mình là $\{s_1(T_j)\}$ để đăng trên phần xác thực (*xacthuc*) trên bảng ***bangphieubau***.

5) **BKP** ký vào phiếu bầu được làm mù $\gamma_j(\alpha'_j, \beta'_j, v_j)$ như được trình bày trong phần 4.3.4 và **BĐH** tính chữ ký tập thể của **BKP** là $t_j(\alpha'_j, \beta'_j, v_j) = \overline{s}'_j$ và đăng chúng lên bảng ***bangphieubau*** như trong bảng 4.3.



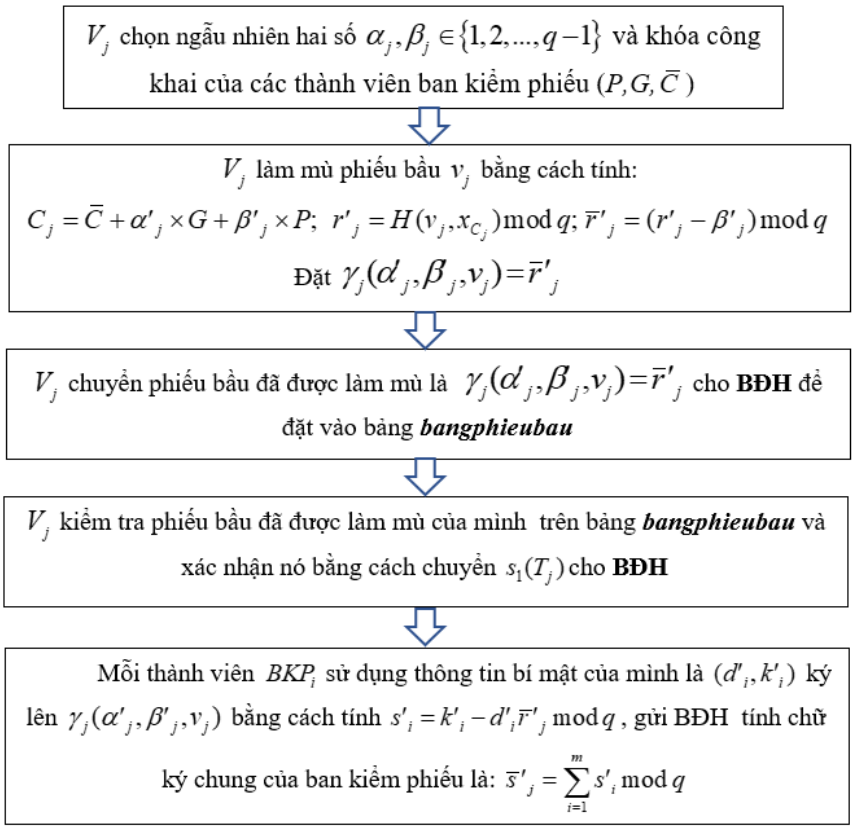
Hình 4.4. Sơ đồ luồng dữ liệu của tầng bỏ phiếu

Đối với tầng này, các vấn đề bảo mật như sau:

+ Cử tri có thể gửi phiếu bầu không hợp lệ: V_j tự gửi và xác thực phiếu bầu làm mù của mình trên bảng ***bangphieubau***. Sau này, V_j không thể tuyên bố rằng phiếu bầu của mình bị hủy ngay cả khi phiếu bầu là vô nghĩa khi giải mù.

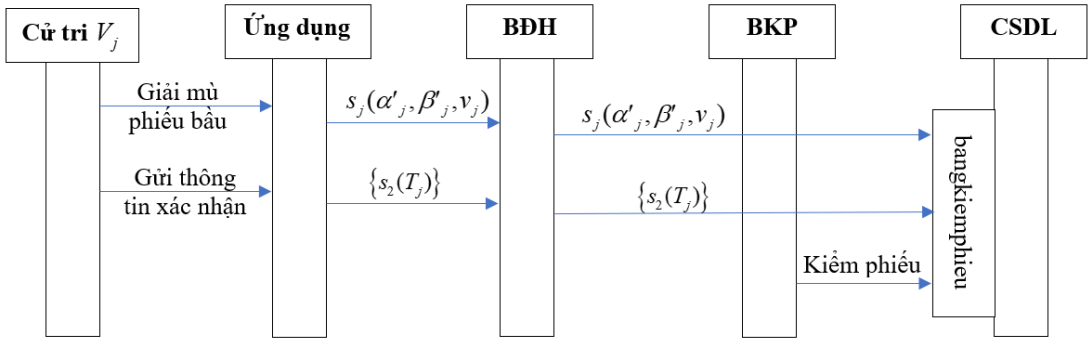
+ **BĐH** không chuyển phiếu hoặc chuyển phiếu không chính xác vào bảng ***bangphieubau***: Vì bảng ***danhsachcutri*** mở cho mọi người xem nên V_j có thể yêu cầu **BĐH** bỏ phiếu của mình vào bảng ***bangphieubau*** bằng cách gửi phiếu trước đây đã được chấp thuận. Nếu **BĐH** cập nhật không chính xác trên bảng ***bangphieubau*** thì V_j có thể từ chối việc bỏ phiếu đó.

+ Phiếu bầu trong bảng ***bangphieubau*** có thể được sửa đổi bởi kẻ tấn công: Vì bảng ***bangphieubau*** mở công khai cho mọi người nên không ai có thể sửa đổi nội dung của nó một cách bất hợp pháp.



Hình 4.5. Thủ tục tạo phiếu bầu ở tầng bỏ phiếu

4.4.2.4. Tầng kiểm phiếu



Hình 4.6. Sơ đồ luồng dữ liệu của tầng kiểm phiếu

Tất cả các phiếu bầu trên bảng ***bangphieubau*** đều ở dạng mù. Khi quá trình bỏ phiếu kết thúc, mỗi cử tri cần giải mù phiếu bầu của mình bằng cách tính $s_j(\alpha'_j, \beta'_j, v_j)$ như được mô tả trong phần 4.3.4. V_j kiểm tra tính chính xác chữ ký của **BKP** trên phiếu bầu được làm mù của mình, V_j gửi $s_j(\alpha'_j, \beta'_j, v_j)$ cho **BĐH** để

đưa nó lên bảng ***bangkiemphieu***. Sau đó, V_j xác nhận chúng bằng cách gửi thành phần thứ hai của chữ ký trên T_j là $s_2(T_j) = s_j$ lên phần xác thực (*xacthuc*) của bảng ***bangkiemphieu***. Ở đây, dữ liệu của cử tri V_j trên bảng ***bangphieubau*** và bảng ***bangkiemphieu*** có thể giống nhau hoặc không. Nếu giống nhau thì phiếu bầu được ký và được làm mù và giải mù là giống nhau trên bảng ***bangphieubau*** và bảng ***bangkiemphieu*** và được xác nhận bởi cùng một T_j. Nếu không giống nhau sẽ không có sự xác nhận nào được đưa vào bảng ***bangkiemphieu***, không ai bao gồm **BKP** có thể biết được mối liên kết giữa chúng vì sử dụng lược đồ chữ ký số tập thể mù. Do đó mà liên kết của phiếu bầu đã ký bị mù trên bảng ***bangphieubau***, phiếu bầu được ký và được giải mù trên bảng ***bangkiemphieu*** và danh tính của V_j đăng ký trên bảng ***danhsachcutri*** cũng bị xóa đi.

Các bước thực hiện của giai đoạn này như sau:

1) V_j giải mù phiếu bầu đã được ký của mình thành $s_j(\alpha'_j, \beta'_j, v_j)$ và kiểm tra tính chính xác chữ ký của **BKP** trên phiếu bầu.

2) V_j gửi $s_j(\alpha'_j, \beta'_j, v_j)$ cho **BĐH** để đăng chúng trên bảng ***bangkiemphieu***.

3) Bằng cách gửi thành phần thứ hai của chữ ký trên T_j là $s_2(T_j) = s_j$ cho **BĐH** đưa lên phần xác thực (*xacthuc*) của bảng ***bangkiemphieu***, V_j đã xác nhận việc bỏ phiếu của mình.

Các vấn đề bảo mật của tầng này như sau:

BKP có thể thêm hoặc xóa phiếu bầu: Nếu làm như thế thì số lượng phiếu bầu trên bảng ***bangphieubau*** và bảng ***bangkiemphieu*** sẽ khác nhau mà bất kỳ ai cũng có thể phát hiện được.

4.5. ĐÁNH GIÁ VÀ PHÂN TÍCH

Sharon Levy trong [90] đã chỉ ra rằng, với cùng mức độ an toàn thì độ dài khóa của lược độ dựa trên bài toán IFP và DLP yêu cầu là 1024 bit, trong khi bài toán ECDLP chỉ yêu cầu khoảng 192 bit.

Trong phần này, thời gian tính toán cho các pha đăng ký, bỏ phiếu và kiểm phiếu là 3 trình quản lý độc lập được phát triển, tức là không có ứng dụng web dựa trên máy khách nào được phát triển trong môi trường thực tế nơi có nhiều thực thể được phân phối ở các nơi khác nhau. Do đó tất cả thời gian tính toán không bao gồm thời gian giao tiếp. Ngoài ra, phần này được giả định rằng các yếu tố gây mù, số nguyên bí mật, số nguyên tố… của các thực thể liên quan được chuẩn bị trước. Đồng thời, hoạt động của các thực thể không liên quan đến mật mã không được xem xét.

Phần thực nghiệm sử dụng máy tính ảo hóa trên nền VMWare đặt tại trung tâm dữ liệu tỉnh Tây Ninh, với cấu hình máu chủ là: Processor Intel Xeon Silver 4216 2.1G, 16C/32T, 9.6GT/s, 22M Cache, Turbo, HT (100W) DDR4-2400; Memory 16GB; Microsoft Windows 10 (10.0) Professional 64-bit. Các tham số đầu vào sử dụng khóa 1024 bit cho các lược đồ dựa trên bài toán DLP và 192 bit cho các lược đồ dựa trên bài toán ECDLP, sử dụng hàm băm là SHA-256, số thành viên ký trong lược đồ ký tập thể là n=3. Kết quả được tính trung bình 1000 lần chạy và được chỉ ở bảng 4.5 bên dưới:

Bảng 4.5. Chi phí thời gian yêu cầu cho các tầng của lược đồ bầu cử

	Các tầng của lược đồ (mili giây)		
Pha	**Đăng ký**	**Bỏ phiếu**	**Kiểm phiếu**
Làm mù	1.8551	3.2692	-
Tạo chữ ký	0.1232	0.2132	-
Giải mù	0.0004	-	0.0005
Kiểm tra	-	-	2.2190
Tổng	**1.9787**	**3,4824**	**2.2195**

Theo bảng 4.5, tổng thời gian cho phần đăng ký, bỏ phiếu và kiểm phiếu của lược đồ đề xuất khoảng: 1.9787+3.4924+2.2195=7.6806 mili giây.

Ví dụ: Nếu có 1,000 phiếu bầu thì có thể được tính trong khoảng 7.68 giây; Nếu có khoảng một triệu cử tri tham gia bỏ phiếu (*tương đương công dân của tỉnh Tây Ninh năm 2019*) thì mất (7.68 *1,000,000 = 7,680,000 mili giây) hay bằng (7,680,000/1000)/60/60 = 2.13 giờ.

Như vậy lược đồ đề xuất có độ phức tạp về thời gian là tương đối thấp, đủ khả thi để thực hiện trong thực tế, nhất là với việc triển khai trên các hệ thống CNTT tốc độ cao thì lược đồ bầu cử đề xuất hoàn toàn có thể triển khai cho một tỉnh như tỉnh Tây Ninh.

4.6. ĐÁNH GIÁ ĐỘ AN TOÀN CỦA LƯỢC ĐỒ BẦU CỬ ĐỀ XUẤT

Phần này phân tích độ an toàn của lược đồ bầu cử điện tử đề xuất theo các tính chất được đề cập trong [31].

+ Tính riêng tư của cử tri: Việc sử dụng các lược đồ chữ ký số mù cho việc ký token và phiếu bầu của cử tri nên các bên khác, kể cả các thành viên của ban kiểm phiếu đều không thể biết được nội dung bầu cử của cử tri.

+ Không lộ thông tin bầu cử: Do phiếu bầu được xây dựng gồm nhiều thành phần tham gia như cử tri, ban điều hành và ban kiểm phiếu nên mặc dù cử tri biết phiếu bầu đã ký của mình trên bảng *bangphieubau*, nhưng cử tri không thể chứng minh điều đó với người cưỡng chế.

+ Tính chính xác: Chỉ những phiếu bầu đã được ký và được giải mù và được xác nhận của cử tri có trên bảng *bangkiemphieu* thì mới được đưa vào kiểm phiếu. Ngoài ra, nếu ban điều hành không chuyển phiếu hoặc chuyển phiếu không chính xác vào bảng ***bangphieubau*** thì cử tri có thể từ chối việc bỏ phiếu đó.

+ Tính mạnh mẽ: Do phiếu bầu được giải mù được xác nhận của cử tri trên bảng *bangphieubau* nên cử tri không thể cho rằng phiếu bầu của mình bị phá hoại. Ngoài ra thì ban điều hành và ban kiểm phiếu cũng không thể phá vỡ được lược đồ bầu cử, trừ khi tất cả các thành viên đều liên kết với nhau để phá vỡ lược đồ.

+ Công bằng: Do mọi phiếu bầu trên bảng *bangphieubau* đều bị làm mù và được ký bởi các thành viên của ban kiểm phiếu nên không ai có thể biết kết quả bỏ phiếu trước khi kiểm phiếu. Chỉ cử tri mới có thể giải mù phiếu bầu của mình.

+ Khả năng kiểm chứng: Mọi cử tri đều phải xác nhận phiếu bầu được ký và được làm mù của mình trên bảng *bangphieubau* và phiếu bầu đã được giải mù của mình trên bảng *bangkiemphieu*. Do đó, lược đồ bầu cử đảm bảo rằng tất cả những phiếu bầu có sự xác nhận của cử tri tương ứng mới được đưa vào kiểm phiếu.

+ Dân chủ: Cử tri được xác thực bằng các thông tin ẩn danh. Đồng thời để gửi và xác nhận phiếu bầu của mình, thông tin định danh của cử tri được đảm bảo bởi token đã được giải mù là duy nhất. Hơn nữa, token của mỗi cử tri được ký bởi nhiều cơ quan nên không ai có thể giả mạo chữ ký trên token và do đó nên tất cả cử tri đủ điều kiện đều được tham gia bỏ phiếu.

+ Chống cưỡng chế: Lược đồ bầu cử được cho là ngăn chặn việc cưỡng ép vì người bỏ phiếu phải đảm bảo nhiều lần xác thực và phải xác nhận phiếu bầu được ký và được làm mù của mình trên bảng *bangphieubau* và phiếu bầu đã được giải mù của mình trên bảng *bangkiemphieu*. Người có thẩm quyền như ban điều hành hoặc ban kiểm phiếu cũng không thể ép buộc cử tri.

4.7. KẾT LUẬN CHƯƠNG 4

Chương 4 đã trình bày lược đồ bầu cử điện tử sử dụng các lược đồ chữ ký số tập thể mù dựa trên lược đồ Schnorr và lược đồ chữ ký số tập thể mù dựa trên lược đồ EC-Schnorr đề xuất trong luận án, cụ thể là lược đồ chữ ký số tập thể mù dựa trên lược đồ EC- Schnorr được sử dụng để xây dựng phiếu bầu và lược đồ chữ ký số tập thể mù dựa trên lược đồ Schnorr được sử dụng cho việc ký mù trên token xác minh thông tin cử tri [CT6].

Trên cơ sở so sánh các lược đồ chữ ký số tập thể mù đề xuất ở chương 2, đã chọn hai lược đồ có độ phức tạp thời gian tính toán thấp nhất để thiết kế lược đồ bầu cử điện tử. Đồng thời cũng tiến hành chạy thực nghiệm và đánh giá, qua đó cho

thấy lược đồ bầu cử điện tử đề xuất có thể sử dụng được trong thực tế như ứng dụng cho bầu cử trực tuyến cho hội đồng nhân dân các cấp và Đại biểu quốc hội của một tỉnh có quy mô cử tri khoảng một triệu người như tỉnh Tây Ninh. Góp phần thúc đẩy việc xây dựng Chính quyền điện tử và Chính quyền số trong thời gian tới.

Việc lựa chọn lược đồ chữ ký số tập thể mù dựa trên EC-Schnorr sử dụng cho lược đồ bầu cử đề xuất do tính vượt trội của hệ mật ECC so với các lược đồ dựa trên IFP hoặc DLP, do với cùng yêu cầu về độ an toàn thì kích thước khóa của hệ mật ECC nhỏ hơn nhiều lần so với IFP và DLP. Một lợi thế lớn của việc có kích thước khóa nhỏ hơn này là việc tính toán có thể được thực hiện nhanh hơn. Ngoài ra, điều này giúp giảm không gian lưu trữ, tiêu thụ năng lượng, sức mạnh xử lý và băng thông. Đây là một trong những ưu điểm của hệ mật ECC mà các nhà nghiên cứu đang quan tâm nghiên cứu để xây dựng các lược đồ chữ ký số có thể ứng dụng được trong hạ tầng mạng còn nhiều hạn chế như ở Việt Nam hiện nay, nhất là khi Việt Nam đang đẩy nhanh việc nghiên cứu và ứng dụng các thiết bị dạng IoT vào sản xuất và ứng dụng, phát triển kinh tế xã hội.

KẾT LUẬN

Qua thời gian nghiên cứu và tìm hiểu về đề tài "***Nghiên cứu phát triển một số lược đồ chữ ký số mù, chữ ký số tập thể mù dựa trên các chuẩn chữ ký số***", luận án đã đạt được một số kết quả chính và đóng góp như sau:

Trong các hệ thống thông tin tự động sử dụng các lược đồ chữ ký số khoá công khai để ký số các tài liệu điện tử. Độ an toàn của lược đồ chữ ký số thường dựa trên hai yếu tố, thứ nhất là thuật toán nổi tiếng để việc giả mạo chữ ký số là không khả thi về mặt tính toán, và thứ hai là xác suất xuất hiện các thuật toán mới để phá vỡ lược đồ chữ ký số đó là không đáng kể. Do đó mà việc cải tiến và phát triển các lược đồ chữ ký số nhằm đảm bảo khó bị phá vỡ, chữ ký số được rút ngắn, đồng thời khả thi có thể triển khai trong thực tế, là yêu cầu luôn được đặt ra cho các nhà nghiên cứu và các quốc gia.

I. Các kết quả đạt được và đóng góp của luận án

1) Đóng góp lớn nhất và quan trọng nhất của luận án này là xây dựng bài toán khó mới dựa trên nhóm con hữu hạn không vòng hai chiều. Trên cơ sở đó xây dựng lược đồ chữ ký số mới dựa trên độ khó của bài toán DLP modulo hợp số nguyên $n = p*q$, trong đó sử dụng số nguyên tố có cấu trúc là $p = 2n+1$. Lược đồ đề xuất có tính an toàn cao do giảm xác suất phá vỡ tiềm năng của lược đồ vì yêu cầu giải pháp tiềm năng đó phải giải được hai vấn đề khó về tính toán là (1) phân tích hợp số n chứa hai số nguyên tố chưa được biết p, q, và (2) Tìm logarit rời rạc modulo các số nguyên tố p, q. Khi chọn các tham số có độ an toàn 80-bit thì chữ ký số trong lược đồ ký số mù đề xuất có kích thước 240 bits (và không phụ thuộc vào số người ký).

Cụ thể: Xây dựng bài toán khó mới, trên cơ sở đó xây dựng lược đồ chữ ký số cơ sở mới có kích thước số ngắn hơn một số lược đồ đã công bố cùng hướng nghiên cứu nhưng vẫn đảm bảo yêu cầu an toàn tương đương các lược đồ đó. Dựa trên lược đồ cơ sở mới, đề xuất lược đồ chữ ký số mù, tập thể mù mới.

Do độ dài chữ ký số ngắn nên có thể ứng dụng được trong các hệ thống có hạ tầng công nghệ thông tin và truyền thông thấp như khả năng lưu trữ, xử lý, năng lượng,… Kết quả nghiên cứu đã được công bố tại công trình [CT1].

2) Xây dựng các lược đồ chữ ký số tập thể mù mới dựa trên các chuẩn chữ ký số và các lược đồ chữ ký số phổ biến nhằm kế thừa tính an toàn và hiệu quả của chúng.

Cụ thể: Luận án đề xuất 02 lược đồ chữ ký số tập thể mù dựa trên các chuẩn chữ ký số GOST R34.10-94 và lược đồ chữ ký số phổ biến Schnorr. Và 02 lược đồ chữ ký số tập thể mù dựa trên các chuẩn chữ ký số GOST R34.10-2012 và lược đồ chữ ký số phổ biến EC-Schnorr. Cải tiến là dựa trên chuẩn và lược đồ phổ biến đề xuất phương pháp để xây dựng các lược đồ chữ ký số tập thể mù hiệu quả từ chữ ký số đơn. Qua đó có thể sử dụng được trong các ứng dụng yêu cầu nhiều người ký (dạng chữ ký tập thể) và cần tính ẩn danh (tính mù). Kết quả nghiên cứu được công bố tại [CT2],[CT3].

Các lược đồ chữ ký số tập thể mù dựa trên lược đồ Schnorr có độ phức tạp thời gian ở phía người yêu cầu và người kiểm tra thấp hơn ở phía người ký, đặc biệt là khi số lượng người trong tập thể ký lớn, nên các lược đồ này có nhiều hiệu quả khi sử dụng trong các ứng dụng mà yêu cầu khả năng lưu trữ, khả năng xử lý và băng thông đường truyền thấp ở phía người yêu cầu như bầu cử điện tử trên hệ thống di động, thanh toán trực tuyến và các ứng dụng sử dụng thiết bị IoT,…

3) Xây dựng các lược đồ chữ ký số mù, chữ ký số tập thể mù dựa trên hai bài toán khó. Đồng thời dựa trên các chuẩn hoặc các lược đồ phổ biến để đảm bảo được tính an toàn và hiệu quả của nó.

Cụ thể: Luận án đề xuất lược đồ chữ ký số cơ sở và lược đồ chữ ký số mù, chữ ký số tập thể mù dựa trên hai bài toán khó IFP và DLP. Các lược đồ này được xây dựng dựa trên việc kết hợp các lược đồ chữ ký số RSA và Schnorr. Cải tiến là kết hợp hai lược đồ, mỗi lược đồ dựa trên một bài toán đơn để xây dựng lược đồ kết hợp được hai bài toán khó nhằm nâng cao hơn tính an toàn cho lược đồ ký số. Đồng

thời đề xuất các lược đồ chữ ký số mù, chữ ký số tập thể mù mới dựa trên lược đồ cơ sở mới đề xuất. Kết quả nghiên cứu đã được công bố tại công trình [CT5].

Do lược đồ dựa trên hai bài toán khó nên để phá vỡ lược đồ sẽ mất rất nhiều thời gian để phải phá vỡ hai bài toán khó. Vì vậy mà lược đồ đề xuất này có thể sử dụng trong các ứng dụng yêu cầu thời gian lưu trữ kết quả đủ lâu. Kết quả này được công bố trong công trình [CT1], [CT5].

4) Ứng dụng các lược đồ chữ ký số tập thể mù đề xuất vào lược đồ bầu cử điện tử: Sử dụng các lược đồ chữ ký số tập thể mù dựa trên lược đồ Schnorr và lược đồ chữ ký số tập thể mù dựa trên lược đồ EC-Schnorr đã đề xuất trong chương 2. Lược đồ bầu cử sử dụng chữ ký số tập thể mù đảm bảo các thuộc tính cơ bản của một lược đồ bầu cử điện tử [CT6].

Cụ thể: Sử dụng lược đồ chữ ký số tập thể mù dựa trên lược đồ EC- Schnorr để xây dựng phiếu bầu và lược đồ chữ ký số tập thể mù dựa trên lược đồ Schnorr để ký mù trên token xác minh thông tin cử tri. Đồng thời cũng tiến hành chạy thực nghiệm và đánh giá, qua đó cho thấy lược đồ bầu cử điện tử ứng dụng chữ ký số tập thể mù có thể sử dụng được trong thực tế như ứng dụng cho bầu cử trực tuyến cho hội đồng nhân dân các cấp của một tỉnh có quy mô cử tri khoảng một triệu người như tỉnh Tây Ninh.

Trong hầu hết các ứng dụng dựa trên các chữ ký số mù, người ký (tập thể người ký) thường phải xử lý nhiều phép tính hơn người yêu cầu, trong khi khả năng tính toán của người yêu cầu có thể bị hạn chế trong một số tình huống xác định như sử dụng thiết bị di động,... nên để bảo đảm chất lượng của các dịch vụ phổ biến dựa trên chữ ký số mù thì điều quan trọng là giảm tính toán cho phía người yêu cầu so với người ký (tập thể người ký). Các lược đồ chữ ký số mù đề xuất trong luận án này đáp ứng xu thế đó. Các chứng minh về tính hiệu quả và an toàn của các lược đồ chữ ký số đề xuất thể hiện rằng, nếu việc lựa chọn các tham số cẩn thận trong thực tế sẽ giúp cho việc sử dụng các lược đồ đề xuất trong các ứng dụng thực tế.

II. Hướng nghiên cứu tiếp theo

- Tiếp tục nghiên cứu đề xuất các dạng lược đồ chữ ký số mù, chữ ký số tập thể mù dựa trên các chuẩn chữ ký số mới hoặc dựa trên hai bài toán khó đối với các ứng dụng đòi hỏi yêu cầu về tính an toàn cao trong hệ thống có hạ tầng hạn chế về nguồn lực như các thiết bị công nghiệp 4.0 như IoT,...

- Nghiên cứu cải tiến giao thức ký số mới trong luận án nhằm nâng cao tính an toàn của lược đồ ký số đồng thời với việc giảm thêm kích thước chữ ký để có thể thực hiện tốt hơn trong thực tế cho các thiết bị di động và IoT.

- Nghiên cứu thêm về lược đồ bầu cử điện tử đề xuất, lựa chọn các tham số hệ thống và môi trường tính toán phù hợp để có thể triển khai ứng dụng trong thực tế.

CÁC CÔNG TRÌNH KHOA HỌC ĐÃ CÔNG BỐ

[CT1] Hai Nam Nguyen, Duc Tan Nguyen, Minh Hieu Nguyen, Nikolay Adreevich Moldovyan (2018), "New Blind Signature Protocols Based on Finite Subgroups with Two-Dimensional Cyclicity", *Iranian Journal of Science and Technology, Transactions of Electrical Engineering (Springer), SCIE Index*, https://link.springer.com/article/10.1007/s40998-018-0129-6.

[CT2] Duc Nguyen Tan, Hai Nguyen Nam, Minh Nguyen Hieu, Hiep Nguyen Van, Lam Tran Thi (2018), "New Blind Muti-signature Schemes Based on ECDLP", *IJECE, Vol.8, No.2, April 2018, pp.1074~1083, ISSN: 2088-8708, DOI:10.11591/ijece.v8i2*, pp1074-1083 (Scopus index).

[CT3] Duc Nguyen Tan, Hai Nguyen Nam, Minh Nguyen Hieu, Hiep Nguyen Van, Lam Tran Thi (2017), "New Blind Multisignature Schemes based on Signature Standards", *The International Conference on Advanced Computing and Applications (ACOMP 2017)*, ĐHBK TP.HCM DOI: 10.1109/ACOMP.2017.4, page(2):23-27, IEEE Catalog Number: CFP17E01-POD, ISBN:978-1-5386-0608-7

[CT4] Nguyễn Tấn Đức, Nguyễn Nam Hải, Nguyễn Hiếu Minh (2017), "Lược đồ chữ ký số mù, tập thể mù dựa trên hai bài toán khó", *Hội thảo Quốc gia 2017 về điện tử, truyền thông và công nghệ thông tin -REV-ECIT 2017*. Trang 95-100.

[CT5] Duc Nguyen Tan, Hai Nguyen Nam, Minh Nguyen Hieu (2019) "Blind Multi-Signature Scheme Based On Factoring And Discrete Logarithm Problem", *TELKOMNIKA, Vol.17, No.5, October 2019*, pp.2327~2334. D O I : 10.12928/TELKOMNIKA.v17i5.10525 (Scopus index).

[CT6] Nguyễn Tấn Đức, Nguyễn Hiếu Minh, Ngô Đức Thiện (2020) "Lược Đồ Bầu Cử Điện Tử Không Truy Vết Dựa Trên Lược Đồ Chữ Kỹ Số Tập Thể Mù", Tạp chí KH&CN Thông tin và Truyền thông, Số 03&04 (2019), Trang 17-25.

TÀI LIỆU THAM KHẢO

Tiếng Việt:

[1] Lưu Hồng Dũng (2013), "Nghiên cứu, phát triển các lược đồ chữ ký số tập thể", *Luận án tiến sỹ kỹ thuật,* Học viện Kỹ thuật Quân sự.

[2] Lưu Hồng Dũng, Nguyễn Tiền Giang, Hồ Ngọc Duy, Nguyễn Thị Thu Thủy (2013), "Phát triển một dạng lược đồ chữ ký số mới", *Kỷ yếu Hội thảo Quốc gia làn thứ XVI: một số vấn đề chọn lọc của CNTT-TT*, Đà Nẵng, ngày 13-14/11/2013.

[3] Lưu Hồng Dũng, Hoàng Thị Mai, Nguyễn Hữu Mộng (2015), "Nghiên cứu về một dạng lược đồ chữ ký số mới được xây dựng trên bài toán phân tích một số". *Kỷ yếu Hội nghị Quốc gia lần thứ VIII về Nghiên cứu cơ bản và ứng dụng Công nghệ thông tin (FAIR),* Hà Nội, ngày 9-10/7/2015.

[4] Lưu Hồng Dũng, Nguyễn Đức Thụy, Lê Đình Sơn, Nguyễn Thị Thu Thủy (2016), "Một phương pháp xây dựng lược đồ chữ ký số dựa trên bài toán logarit rời rạc", *Kỷ yếu Hội nghị Khoa học Quốc gia lần thứ IX về Nghiên cứu cơ bản và ứng dụng Công nghệ thông tin (FAIR'9),* Cần Thơ, ngày 4-5/8/2016.

[5] Nguyễn Tiền Giang, Nguyễn Vĩnh Thái, Lưu Hồng Dũng (2014), "Lược đồ chữ ký số mù xây dựng trên bài toán khai căn", *Tạp chí Khoa học và Kỹ thuật (Học viện Kỹ thuật Quân sự),* chuyên san CNTT và TT số 5, 10/2014.

[6] Đào Tuấn Hùng (2017), "Nghiên cứu, phát triển một số lược đồ chữ ký số hướng tới nhóm", *Luận án tiến sỹ toán học,* Viện khoa học và công nghệ quân sự.

[7] Đặng Minh Tuấn (2017), "Nghiên cứu xây dựng một số dạng lược đồ mới cho chữ ký số tập thể", *Luận án tiến sỹ toán học,* Viện khoa học và công nghệ quân sự.

Tiếng Anh:

[8] Ari Juels, Michael Luby, Rafail Ostrovsky (1997), "Security of blind digital signature", *Advances in Cryptology — CRYPTO '97*, pp.150-164.

[9] Bellare, M., Rogaway, P. (1993), "Random oracles are practical: a paradigm for designing efficient protocols", *Proceedings of the 1st ACM conference on Computer and communications security*, pp. 62–73.

[10] Benaloh and D. Tuinstra (1994), "Receipt-free secret-ballot elections," Proceedings of 26th Symposium on Theory of Computing, pp. 544–553.

[11] Camenisch, Jean-Marc Piveteau, and Markus A. Stadler (1994), "Blind Signatures Based on the Discrete Logarithm Problem", *In Advances in Cryptology-EUROCRYPT '94, Vol 950 of Lecture Notes in Computer Science,* pp 428– 432.

[12] Chaum (1981), "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of ACM*, vol. 24, pp. 84–90.

[13] Chaum (1983), "Blind signatures for untraceable payments", *Advances in Cryptology-CRYPTO'82,* pp.199-203.

[14] Chaum (1998), "Elections with unconditionally- secret ballots and disruption equivalent to breaking RSA", Advances in Cryptology – Eurocrypt'88, LNCS 330, Springer-Verlag, pp. 177–182.

[15] Cheng-Chi Lee, Min-Shiang Hwang, and WeiPang Yang (2005), "A New Blind Signature Based on the Discrete Logarithm Problem for Untraceability",
Applied Mathematics and Computation, 164(3): 837–841.

[16] Darrel Hankerson, Alfred Meneze, Scott Vanstone (2004), "Guide to Elliptic Curve Cryptography", *Springer, NewYork, USA*.

[17] Darwish, Maged M El-Gendy (2017), "A New Cryptographic Voting Verifiable Scheme for E-Voting System Based on Bit Commitment and Blind Signature", Int J Swarm Intel Evol Comput 2017, 6:2 DOI: 10.4172/2090-4908.1000158.

[18] Debasish Jena, Sanjay Kumar Jena, and Banshidhar Majhi (2007), "A Novel Blind Signature Scheme Based on Nyberg-Rueppel Signature Scheme and Applying in Off-Line Digital Cash", *In Proceedings of the 10th International Conference on Information Technology (ICIT'07),* pp.19–22.

[19] Debasish Jena, Sanjay Kumar Jena, and Banshidhar Majhi (2007), “A Novel Untraceable Blind Signature Based on Elliptic Curve Discrete Logarithm Problem”, *IJCSNS International Journal of Computer Science and Network Security*, 7(6): 269-275.

[20] Debasish, J. K. Sanjay, M. Banshidhari, and P. K. Saroj (2008), “A novel ECDLP-based blind signature scheme with an illustration", Web engineering and applications, (2008), pp. 59-68.

[21] Debiao, Chen, Zhang (2011), “An efficient identity-based blind signature scheme without bilinear pairings”, *Journal Computers and Mathematics with Applications*, pp.444-450.

[22] Dernova, E. S. (2009), "Information authentication protocols based on two hard problems", *Ph.D. Dissertation. St. Petersburg State Electrotechnical University. St. Petersburg, Russia*.

[23] Diffie and Hellman (1976), “New Directions in cryptography”, *IEEE Transactions on Information Theory*, Vol.22, pp.644-654.

[24] Dolmatov (2013), “Digital Signature Algorithm draft-dolmatov-gost34-10-2012-00 ”, *Cryptocom, Ltd*.

[25] Dominique Schroder and Dominique Unruh (2012), “Security of Blind Signatures Revisited”, *Springer Link.*

[26] Fan, C.-I., Sun, W.-Z., Huang, V.S.-M. (2010), “Provably secure randomized blind signature scheme based on bilinear pairing”, *Journal Computers & Mathematics with Applications*, pp. 285- 293.

[27] Fan, D. J. Guan, Chih-I Wang, and Dai-Rui Lin (2009),”Cryptanalysis of Lee-Hwang-Yang Blind Signature Scheme”, *Computer Standards & Interfaces*, 31(2):319–320.

[28] Federal Office for Information Security (2012), “Technical Guideline - Elliptic Curve Cryptography”, *Technical Guideline TR-03111,* pp.24-25.

[29] Fuchsbauer and D. Vergnaud (2010), “Fair Blind Signatures without Random Oracles”, *Lecture Notes in Computer Science*, Vol 6055, pp.16-33.

[30] Fuchsbauer, C. Hanser, D. Slamanig (2015), “Practical round-optimal blind signatures in the standard model”. Proceedings of the 35th Annual Cryptology Conference, CRYPTO 2015.

[31] Fujioka A, Okamoto T, Ohta K (1992), “A practical secret voting scheme for large scale elections”, *Adv Cryptol-AUCRYPT’92. Springer-Verlag,* pp. 244-251.

[32] Ganaraj K (2017), “ADVANCED E-VOTING APPLICATION USING ANDROID PLATFORM “, International Journal of Computer- Aided Technologies (IJCAx) Vol.4, No.1/2.

[33] Ghassan Z. Qadah, Rani Taha (2007), “Electronic voting systems: Requirements, design, and implementation”, Computer Standards & Interfaces 29 (2007) 376 – 386.

[34] Goldwasser, S. Micali, and R. L. Rivest (1995), “A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks”, *SIAM Journal of Computing*, 17 (2), pp. 281–308.

[35] GOST R 34.10-94 (1994), “Russian Federation Standard Information Technology. Cryptographic data Security Produce and check procedures of Electronic Digital Signature based on Asymmetric Cryptographic Algorithm”, *Government Committee of the Russia for Standards, Russian*.

[36] Guo, W., Zhang, J.Z., Li, Y.P., et al.(2016), “Multi-proxy strong blind quantum signature scheme”. Int. J. Theor. Phys. 55(8), 3524–3536.

[37] Haddad. N. Islam S. Tamura and A. K. Md. Rokibul (2015), “An incoercible e- voting scheme based on revised simplified verifiable re-encryption mix-nets”, *Information Security and Computer Fraud,* vol. 3, no. 2, pp. 32–38.

[38] Harn (1994), "Public-key cryptosystem design based on factoring and discrete logarithms", *IEE Proc. Of Computers and Digital Techniques*, vol.141, no.3, pp.193-195.

[39] Harn (1995), “Cryptanalysis of the Blind Signatures Based on the Discrete Logarithm Problem”, *Electronic Letters*, 31(14):1136.

[40] Hirt and K. Sako (2000), “Efficient Receipt-Free Voting Based on Homomorphic Encryption,” Proceedings of EUROCRYPT, LNCS, Vol. 1807, pp. 539-556. Springer.

[41] Horster, M. Michels, and H. Petersen (1995), "Comment: Cryptanalysis of the Blind Signatures Based on the Discrete Logarithm Problem”, *Electronic Letters,* 31(21):1827.

[42] Horster, M. Michels, and H. Petersen (1995), “Blind multisignature schemes and their relevance for electronic voting”, *Proc. of 11th Annual Computer Security Applications Conference, New Orleans, IEEE Press*.

[43] Huian, A. R. Kankanala, and X. Zou (2014), “A taxonomy and comparison of remote voting schemes,” in 23rd International Conference on Computer Communication and Networks (ICCCN’14), pp. 1–8.

[44] Hung Min Sun (2002), “Cryptanalysis of a Digital Signature Scheme Based on Factoring and Discrete Logarithms”, *NCS*.

[45] Ismail, Tahat, and Ahmad (2008), “ A New Digital Signature Scheme Based on Factoring and Discrete Logarithms”, *Journal of Mathematics and Statistics*, 4(4):222-225.

[46] James, S.; Gowri, T.; Babu, G.R.; Reddy, P.V. (2017), “Identity-Based Blind Signature Scheme with Message Recovery”. Int. J. Electr. Comput. Eng. 7, 2674–2682.

[47] Jeng, T. L. Chen, and T. S. Chen (2010), “An ECC-Based Blind Signature Scheme”, *Journal of networks*, vol. 5, no. 8.

[48] Johnson, Don and Menezes, Alfred (1999), ”The Elliptic Curve Digital Signature Algorithm (ECDSA)”, Web. http://cacr.uwaterloo.ca/ techreports/1999/corr99-34.pdf.

[49] Joseph K. Liu, Joonsang Baek, Jianying Zhou, Yanjiang Yang ang Jun Wen Wong (2010), “Efficient Online/Offline Identity-Based Signature for Wireless Sensor Network”, *Institute for Infocomm Research Singapore*.

[50] Juels and M. Jakobsson (2002), “Coercion-resistant electronic elections,” Cryptology ePrint Archive, Report 2002/165, <http://eprint.iacr.org/>.

[51] Kazi Md and S. Tamura (2012), “Electronic voting: Scopes and limitations”, in Proceedings of International Conference on Informatics, Electronics & Vision (ICIEV12), pp. 525–529.

[52] Kazi Md. Rokibul Alam, Adnan Maruf, Md. Rezaur Rahman Rakib, G. G. Md. Nawaz Ali, Peter Han Joo Chong and Yasuhiko Morimoto (2018), “An Untraceable Voting Scheme Based on Pairs of Signatures”, *International Journal of Network Security*, Vol.20, No.4, PP.774-787.

[53] Koblitz (1987), “Elliptic curve cryptosystems”, *Mathematics of Computation*, Vol.48, pp.203-209.

[54] Kumar, C. P. Katti, and P. C. Saxena (2017), “A New Blind Signature Scheme Using Identity-Based Technique,” Int. J. Control Theory Appl., vol. 10, no. 15, pp. 36–42.

[55] Kumar, M.; Katti, C.P.; Saxena, P.C. (2017),”An Identity-Based Blind Signature Approach for E-Voting System”. Int. J. Modern Educ. Comput. Sci, 10, 47–54.

[56] Laura Savu (2012), “Combining public key encryption with Schnorr digital signature”, *Journal of Software Engineering and Applications*.

[57] Lee (1999), “Security of Shao’s Signature Schemes Based on Factoring and Discrete Logarithms”, *IEEE Proceeding*, 146(2):119-121.

[58] Lee M. S. Hwang and Y. C. Lai (2003), “An untraceable blind signature scheme”, *IEICE Transaction on Fundamentals*, vol. E86-A, no. 7, pp. 1902–1906.

[59] Lee N. Y., T. Hwang (1996), "Modified Harn signature scheme based on factoring and discrete logarithms", *IEEE Proceeding of Computers Digital Techniques, IEEE Xplore, USA*, pp:196-198.

[60] Lee, and K. Kim (2002), “Receipt-free electronic voting scheme with a tamperresistant randomizer”, ICISC 2002, LNCS 2587, Springer-Verlag, pp. 389–406.

[61] Lee, C. Boyd, E. Dawson, K. Kim, J. Yang and S. Yoo (2004), "Providing receipt-freeness in Mixnet-based voting protocols", in Proceedings of the information Security and Cryptology (ICISC '03), pp. 245–258.

[62] Li and G. Xiao (1998), "Remarks on new signature scheme based on two hard problems", *Electronics Letters*, Vol 34 , Issue: 25.

[63] Lin, C. Gun, and C. Chen (2009), "Comments on Wei's Digital Signature Scheme Based on Two Hard Problems", *IJCSNS International Journal of Computer Science and Network Security*, 9(2):1-3

[64] Mahender Kumar, C.P. Katti, P. C. Saxena (2017), "An Identity-based Blind Signature Approach for E-voting System", I.J. Modern Education and Computer Science, 10, 47-54.

[65] Manivannan1, K.Ramesh2 (2015), "E-VOTING SYSTEM USING ANDROID SMARTPHONE", International Research Journal of Engineering and Technology (IRJET), e-ISSN: 2395-0056, Volume: 02 Issue: 06.

[66] Markus Michels, David Naccache, and Holger Petersen (1996), "GOST 34.10 – A Brief Overview of Russia's DSA", Computers & Security 15(8):725-732.

[67] Menezes A. J. Vanstone S.A (1996), "Handbook of Applied Cryptography", *CRC Press*.

[68] Miller (1986), "Uses of elliptic curves in cryptography", *Advances in Cryptology CRYPTO'85*, Vol.218, pp.417-426.

[69] Minh NH, Binh DV, Giang NT, Moldovyan NA (2012), "Blind Signature Protocol Based on Difficulty of Simultaneous Solving Two Difficult Problems", *Applied Mathematical Sciences*, vol. 6, no. 139, pp. 6903-6910.

[70] Minh NH, Moldovyan NA, Giang NT (2017), "New Blind Signature Protocols Based on a New Hard Problem", *The International Arab Journal of Information Technology*, vol.14, no.3, pp. 307-313.

[71] Moldovyan, NA (2008), "Digital Signature Scheme Based on a new hard problem", *Computer Science Journal of Moldova*, vol.16, no 2, pp.163-182.

[72] Moldovyan, NA, Moldovyan, AA (2010), "Blind Collective Signature Protocol Based on Discrete Logarithm Problem", *International Journal of Network Security*. Vol.11, No.2, pp.106-113.

[73] Moldovyan, NA. (2011), "Blind Signature Protocols from Digital Signature Standards", *International Journal of Network Security*. pp 22-30.

[74] Muthanna Abdulwahed Khudhair (2017), "A New Multiple Blind Signatures Using El-Gamal Scheme". International Journal of Engineering and Information Systems (IJEAIS) ISSN: 2000-000X Vol. 1 Issue 7, September – 2017, Pages: 149-154.

[75] Nakamura and K. Itakura (1983), "A public-key cryptosystem suitable for digital multisignatures", *NEC Research and Development*, 71, pp. 1–8.

[76] Neff (2001), "A verifiable secret shuffle and its application to E-voting", ACM CCS 2001, ACM Press, pp. 116–125.

[77] Nidhi Gupt, Praveen Kumar, Satish Chhokar (2011), "A Secure Blind Signature Application in E Voting", Proceedings of the 5 th National Conference; INDIACom-2011

[78] Pollard (1978), "Monte Carlo methods for index computation mod *p*", *Mathematics of Computation*, Vol.32, pp.918-924.

[79] Popescu, C. (1999), "Blind Signature and BMS Using Elliptic Curves", *Studia univ. "babes¸–bolyai", Informatica*, pp 43-49.

[80] Rabin (1979), "Digitalized signatures and public-key functions as intractable as factorization", *MIT Laboratory for Computer Science, USA*.

[81] Rahul Patil, Pritam Bhor, George Ebenez, Ashish Rasal (2014), "E-Voting System on Android Platform", International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 3 Issue 2.

[82] Ribarski and L. Antovski (2014), "Comparison of ID-based blind signatures from pairings for e-voting protocols," in Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2014 37th International Convention on, 2014, pp. 1394–1399.

[83] Rivest R, Shamir A, Adleman A (1978), “A method for Obtaining Digital Signatures and Public-Key Cryptosystems”, *Communication of the ACM*, Vol. 21. N 2. pp. 120–126.

[84] Sarde, P.; Banerjee, A. (2017), “A Secure ID-Based Blind and Proxy Blind Signature Scheme from Bilinear Pairings”. J. Appl. Secur. Res. 2017, 12, 2.

[85] Schnorr (1991), “Efficient signature generation by smart cards”, *Journal of Cryptology*, Vol.4, pp.161-174.

[86] Schweisgut (2006), “Coercion-resistant electronic elections with observer,” 2nd International Workshop on Electronic Voting, Bregenz.

[87] Shanks (1971), “Class number, a theory of factorization, and genera”, *In Proc. Symp, Pure Math*, Vol 20, pp. 415-440

[88] Shao (1998), “Signature Schemes Based on Factoring and Discrete Logarithms”, *Computers and Digital Techniques, IEE Proceeding*, 145(1):33-36.

[89] Shao (2005), “Security of a new digital signature scheme based on factoring and discrete logarithms”, *International Journal of Computer Mathematics*, 82(10), 1215-1219.

[90] Sharon Levy (2015), “Performance and Security of ECDSA”, http://www.semanticscholar.org.

[91] Shinsuke Tamura and Shuji Taniguchi (2014), “Enhanced anonymous tag based credentials”, *Information Security and Computer Fraud*, vol. 2, no. 1, pp. 10-20.

[92] Shin-Yan Chiou, Yi-Xuan He (2013), "Remarks on new Digital Signature Algorithm based on Factorization and Discrete Logarithm problem", *International Journal of Computer Trends and Technology (IJCTT)*, V4(9): 3322-3324.

[93] Tahat NMF, Ismail ES, Ahmad RR (2009), “A New Blind Signature Scheme Based On Factoring and Discrete Logarithms”, *International Journal of Cryptology Research*, vol.1 (1), pp.1-9.

[94] Tahat, N., Ismail, E. S., & Alomari, A. K. (2018). Partially blind signature scheme based on chaotic maps and factoring problems. Italian Journal of Pure and Applied Mathematics, (39), 165-177.

[95] Tzeng, C.Y. Yang, and M.S. Hwang (2004), "A new digital signature scheme based on factoring and discrete logarithms", *International Journal of Computer Mathematics*, 81(1):9-14.

[96] Verma and B. B. Singh (2017), "Efficient message recovery proxy blind signature scheme from pairings," Transactions on Emerging Telecommunications Technologies, vol. 28, no. 11.

[97] Verma, G.K.; Singh, B.B. (2016), "New ID based fair blind signatures". Int. J. Current Eng. Sci. Res. 2016, 3, 41–47.

[98] Verma, G.K.; Singh, B.B. (2018), "Efficient identity-based blind message recovery signature scheme from pairings". Inst. Eng. Technol. J. 2018, 12, 150–156

[99] Vishnoi, V. Shrivastava (2012) "A new Digital Signature Algorithm based on Factorization and Discrete Logarithm problem", *International Journal of Computer Trends and Technology (IJCTT).*

[100] Wang, C. H. Lin, and C. C. Chang (2003), "Signature Scheme Based on Two Hard Problems Simultaneously", *Proceedings of the 17th International Conference on Advanced Information Networking and Application*, pp. 557-561.

[101] Wei (2007), "Digital Signature Scheme Based on Two Hard Problems", *International Journal of Computer Science and Network Security*, 7(12):207-209

[102] Wei. (2004), "A New Digital Signature Scheme Based on Factoring and Discrete Logarithms", *Progress on Cryptography*, pp 107-111.

[103] Wei-Hua He (2001), "Digital Signature Scheme Based on Factoring and Discrete Logarithms", *Electronics Letters*, 37(4):220-222

[104] Wen-Shenq, L. Chin-Laung and L. Horng-Twu (2002), “A verifiable multi-authority secret election allowing abstention from voting,” The Computer Journal, Vol. 45(6), pp. 672– 82.

[105] Williams (1980), “A modification of the RSA public-key encryption procedure”, *IEEE Transactions on Information Theory*, Vol.26, pp.726-729.

[106] Wu Ting and Jin-Rong Wang (2005), “Comment: A New Blind Signature Based on the Discrete Logarithm Problem for Untraceability”, *Applied Mathematics and Computation*, 170(2): 999-1005.

[107] Xiaoming Hu, J. Wang, Y. Yang (2011), “Secure ID-Based Blind Signature Scheme without Random Oracle”, *NCIS '11 Proceedings of the 2011 International Conference on Network Computing and Information Security*, Vol 01.

[108] Zhang, J.L., Zhang, J.Z., Xie, S.C. (2018), “Improvement of a quantum proxy blind signature scheme”. Int. J. Theor. Phys. 57(6), 1612–1621.

[109] Zheng, Z. Shao, S. Huang and T. Yu (2008), “Security of two signature schemes based on two hard problems”, *Proc. of the 11th IEEE International Conference on Communication Technology*, pp.745-748.

[110] Zhu, Y.-A. Tan, L. Zhu, Q. Zhang, and Y. Li (2018), “An efficient identity-based proxy blind signature for semioffline services,” Wireless Communications and Mobile Computing, vol. 2018.