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

TÓM TẮT LUẬN ÁN TIẾN SĨ KỸ THUẬT

HÀ NỘI – NĂM 2020

Công trình hoàn thành tại:

Học viện Công nghệ Bưu chính Viễn thông

Người hướng dẫn khoa học:

1. PGS.TS. Nguyễn Hiếu Minh

2. TS. Ngô Đức Thiện

Phản biện 1: PGS.TS. Đặng Văn Chuyết
Phản biện 2: PGS.TS. Tạ Minh Thanh
Phản biện 3: TS. Lê Quang Minh

Luận án được bảo vệ trước Hội đồng cấp Học viện tại:

Học viện Công nghệ Bưu chính Viễn thông

Số 122 Hoàng Quốc Việt, Hà Nội.

Vào lúc:

Có thể tìm hiểu luận án tại:

1) Thư viện Quốc Gia

2) Thư viện Học viện Công nghệ Bưu chính Viễn thông

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 hình tiên tri ngẫu nhiên ROM [9] 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, chuẩn GOST R34.10-94, GOST R34.10-2012.
- Đề xuất các lược đồ chữ ký số tập thể mù dựa trên các chuẩn 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 các 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.

NỘI DUNG

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

1.1. TỔNG QUAN VỀ CHỮ KÝ SỐ

Trình bày một số kiến thức cơ bản về chữ ký số, lược đồ chữ ký số, phương thức tạo và xác thực chữ ký số, chức năng chữ ký số, phân loại tấn công và các dạng phá vỡ lược đồ chữ ký số.

1.1.1. Khái niệm chữ ký số

Chữ ký số là một loại chữ ký điện tử, được tạo bằng sự chuyển đổi thông điệp dữ liệu sử dụng hệ mật không đối xứng, theo đó người có được thông điệp dữ liệu ban đầu và khóa công khai của người ký

1.1.2. Lược đồ chữ ký số

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.

1.1.3. Tạo và xác thực chữ ký số

1.1.4. Chức năng của chữ ký số

Chức năng của chữ ký số gồm: Xác thực được nguồn gốc thông điệp; Tính toàn vẹn của thông điệp; Chống từ chối thông điệp.

1.1.5. Phân loại tấn công chữ ký số

1.1.6. Các dạng phá vỡ lược đồ chữ ký số

1.2. CHỮ KÝ SỐ TẬP THỂ

Lược đồ chữ ký số tập thể cho phép một tập thể người ký tham gia ký văn bản và người xác thực có thể xác thực được rằng văn bản đã được từng thành viên trong tập thể ký.

Các thành phần của lược đồ chữ ký số tập thể gồm: Giao thức sinh khóa; Thuật toán ký tập thể; Thuật toán kiểm tra chữ ký

1.3. CHỮ KÝ SỐ MÙ

Theo Chaum trình bày trong [13] thì lược đồ chữ ký số mù là loại lược đồ mà người yêu cầu nhận một chữ ký $Sig(M)$ cho thông điệp M của mình từ người ký, người này chỉ 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.

Các thuộc tính của chữ ký số mù:

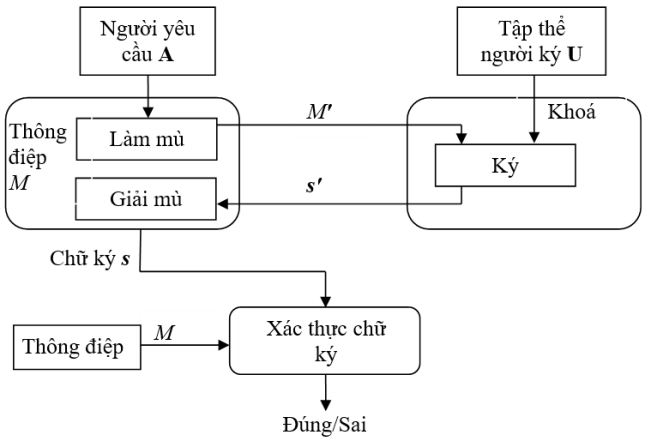
+ Tính mù: Nội dung thông điệp bị làm mù đối với người ký.

+ 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.

+ 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.

1.4. CHỮ KÝ SỐ TẬP THỂ MÙ

Tiến trình của một chữ ký số tập thể mù được mô tả như sau: 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', A đưa M' cho U ký. 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 1.1. Tiến trình của chữ ký số tập thể mù

1.5. MÔ HÌNH ĐÁNH GIÁ TÍNH AN TOÀN CHO CHỮ KÝ SỐ (ROM)

Năm 1993 Phillip Rogaway và Mathir Bellare đề xuất ra mô hình tiên tri ngẫu nhiên (*Random Oracle Model-ROM*) [9]. Mô hình ROM là công cụ mạnh 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

Trình bày 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 hình thức tấn công các bài toán đó.

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

1.6.2. Bài toán logarit rời rạc (DLP)

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

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

Trình bày các lược đồ chữ ký số phổ biến và các chuẩn chữ ký số đang được ứng dụng trong thực tế là RSA, Schnorr, EC-Schnorr, GOST R34.10-94 và GOST R34.10-2012.

1.7.1. Lược đồ chữ ký số RSA

1.7.2. Lược đồ chữ ký số Schnorr

1.7.3. Lược đồ chữ ký số EC-Schnorr

1.7.4. Chuẩn chữ ký số GOST R34.10-94

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

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.

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.

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 [72] được sử dụng so sánh với lược đồ đề xuất trong chương 2.

1.8.1.3. Lược đồ chữ ký số trong [73]

Năm 2011, A.Moldovyan đề xuất lược đồ ký số tập thể mù dựa trên chuẩn GOST R34.10-94 [73]. Lược đồ [73] được sử dụng so sánh với lược đồ đề xuất trong chương 2.

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]. Lược đồ [70] được sử dụng so sánh với lược đồ đề xuất trong chương 3.

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

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

Năm 1983, David Chaum đề xuất lược đồ chữ ký số mù đầu tiên dựa trên chữ ký số RSA, sau đó có 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, 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. 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 như sau:

(i) Lược đồ xây dựng mới chỉ dựa trên các bài toán khó đơn như IFP, DLP và ECDLP: 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. Để tăng cường an toàn cho các lược đồ chữ ký số, cần phải phát triển các lược đồ thực sự dựa trên nhiều bài toán khó, sẽ làm cho việc tấn công trở nên khó khăn hơn khi phải giải đồng thời nhiều bài toán khó.

(ii) Lược đồ đề xuất dựa trên hai bài toán khó nhưng chưa chứng minh trong mô hình chuẩn hoặc 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,...

2) Lược đồ không dựa trên chuẩn: Một số lược đồ công bố nhưng 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 có thể dựa trên một bài toán khó 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.

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, mô hình ROM. Ba bài toán khó là IFP, DLP và ECDLP. Trình bày các lược đồ chữ ký số phổ biến và các chuẩn chữ ký số đang được ứng dụng trong thực tế như RSA, Schnorr, EC-Schnorr, GOST R34.10-94 và GOST R34.10-2012. Đồng thời cũng đã trình bày khái quát một số các công trình nghiên cứu liên quan gần đây trong nước là các đề tài luận án tiến sĩ đã được công bố, chỉ ra các hướng nghiên cứu và định hướng hướng nghiên cứu của NCS.

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

Chương 2 xây dựng 02 lược đồ dựa trên bài toán DLP là lược đồ dựa trên chuẩn chữ ký số GOST R34.10-94 và lược đồ Schnorr, và 02 lược đồ dựa trên bài toán ECDLP là 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. 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.

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

2) Trích xuất: Mỗi người ký trong **B** chọn một số 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:

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

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

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

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

4) Tạo chữ ký: Mỗi người ký trong **B** nhận cặp $(\bar{r}, \bar{h})$ từ **A**, mỗi người ký tính s_i và gửi cho TTP để tính $\bar{s}$ và gửi lại cho người yêu cầu, với: $s_i = k_i \bar{h} + d_i \bar{r} \bmod q$; $\bar{s} = \sum_{i=1}^{n} s_i \bmod q$

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

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:

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

Người yêu cầu **A** (M)	Dữ liệu	Tập thể người ký **B** (p, q, $\rho, \bar{c}$)
		Công khai (p, q, $\rho, \bar{c}$)
Chọn: $\alpha, \beta \in \{1,2,...,q-1\}$	←	
$\bar{h} = \alpha h \bmod p$		
$c = \bar{c}^{\beta} g^{\alpha} \bmod p$		
$r = c \bmod q$		
$\bar{r} = (r\beta^{-1}\alpha) \bmod q$	$\bar{h}, \bar{r}$ →	$s_i = k_i \bar{h} + d_i \bar{r} \bmod q$
		$\bar{s} = \sum_{i=1}^{n} s_i \bmod q$
$s = (\beta\alpha^{-1}\bar{s} + \alpha h) \bmod q$	$\bar{s}$ ←	
Chữ ký số là cặp: (r,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 được xác định bởi hai đặc trưng là tính mù và không 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 $(\bar{h}, \bar{r}, \bar{s})$ là dữ liệu được lưu trong các lược đồ chữ ký số được phát hành từ **B**. Sẽ tồn tại hai tham số ngẫu nhiên α, β liên kết $(\bar{h}, \bar{r}, \bar{s})$ tới (M, r, s).

Từ mô tả trên, 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 các số 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 số ngẫu nhiên (*k′,d′*) và tính $c^*=(\rho')^{k'}g^{d'} \bmod p$. (2.3)

d′ được xem như là khoá riêng của người ký, *k′* là số 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′,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 $(M,\bar{r}',\bar{s}')$. 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 $s_1^*=(h,\bar{r}',\bar{s}_1')$ trên *M* bởi khoá bí mật *d′*. B lại thực hiện lần nữa bằng cách giữ nguyên $(h,\bar{r}')$ và lại yêu cầu **A** ký tiếp và thu được $s_2^*=(h,\bar{r}',\bar{s}_2')$. **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.

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

2.1.2.1. Xây dựng lược đồ

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

2) Trích xuất: Mỗi người ký trong **B** chọn một số 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: $c_i = g^{k_i} \bmod p, i = 1,2,...,n;$ $\overline{c} = \prod_{i=1}^{n} c_i \bmod p = g^{\sum_{i=1}^{n} k_i \bmod q} \bmod p$

3) Làm mù: Người yêu cầu **A** chọn hai số ngẫu nhiên $\alpha, \beta \in \{1,2,...,q\text{-}1\}$ và tính $h = H(M \| c)$ và tính: $c = \overline{c} g^{\alpha} \rho^{\beta} \bmod p; r = h \bmod q; \overline{r} = (r - \beta) \bmod q$. 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 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.

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

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

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

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*. Kết quả 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]. Độ phức tạp thời gian của lược đồ chữ ký số tập thể mù dựa trên Schnorr thấp hơn trong [72].

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

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

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

Mỗi người ký trong **B** chọn ngẫu nhiên số $k_i \in Z_q$ và tính C_i sau đó gửi đến TTP để tính $\overline{C}$ như sau: $C_i = k_i \times G$ *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 số $\alpha, \beta \in \{1,2,...,q-1\}$ 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: $C' = (se^{-1} \bmod q) \times G - (re^{-1} \bmod q) \times P$ và $r' = x_{C'} \bmod q$

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

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

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.

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

Mỗi người ký chọn ngẫu nhiên số $k_i \in Z_q$ và tính C_i sau đó gửi đến TTP để tính $\overline{C}$ như: $C_i = k_i \times G$ *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 số $\alpha, \beta \in \{1,2,...,q\text{-}1\}$ 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.

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

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

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

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*. Kết quả ở 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. 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.

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

2.3.1. Thực nghiệm

Kết quả thực nghiệm ở 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 ms và lược đồ chữ ký số tập thể mù dựa trên chuẩn GOST R34.10-2012 (bài toán ECDLP) là 43.9465 ms, tức là thời gian tính toán của LĐ 2.03 khoảng 1.5 lần thời gian của LĐ 2.01. 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 ms và lược đồ chữ ký số tập thể mù dựa trên lược đồ EC-Schnorr (LĐ 2.04) là 5.4920 ms, tức là thời gian tính toán của lược đồ LĐ 2.04 khoảng 1.5 lần thời gian của LĐ 2.02.

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

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 ứng dụng trong thực tế.

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).

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

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

3.2. Lược đồ chữ ký số mù, chữ ký số tập thể mù dựa trên việc 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 $d = e^{-1} \bmod \phi(n)$.

a) Tạo khoá

1) Chọn số 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 ngẫu nhiên số bí mật $x \in Z_p^*$ 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 số 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.

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

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 số 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 ngẫu nhiên số bí mật $x_i \in Z_p^*$ 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 (x_i, d)

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 $R' = \overline{R} g^{\varepsilon} y^{\tau} \bmod p$, $E' = H(M \| R')$, $E = E' - \tau$ 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 $D' = \mu^e (\overline{D} + \varepsilon) \bmod n$ và D' cho **B**

Vòng 5 (tập thể người ký **B**):

Tính $D'' = D'^d = \mu^{ed} (\overline{D} + \varepsilon)^d = \mu (\overline{D} + \varepsilon)^d \bmod n$ 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 $E'^* = H(M \| R'^*)$, 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*.

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*.

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.

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.

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. 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.

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

3.3.1. Tổng quan về lược đồ đề xuất

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 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 cyclic 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 như vậy.

3.3.2. Thiết lập các nhóm con 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 $|q| \approx \lambda\ bit, |p| \approx 2\lambda\ bit$ [12]. 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 ($\rho = 80$ 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 số γ có bậc r modulo p
2) Tạo số δ có bậc r modulo q
3) Chọn số ngẫu nhiên $0 < h < r$ và $0 < k < r$ và tìm số α thỏa mãn hệ phương trình đồng dư sau đây:

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

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

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

Các tham số 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 số α và β là *r* theo các công thức dưới đây:

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

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

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 cyclic không vòng hai chiều và được tạo bởi hai thành phần 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 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 số α (số 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 số ngẫu nhiên bậc *r* mod *n*.

Xác suất để hai số 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 số 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 số 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 $\alpha'(\beta') = z^r \bmod n \neq 1$, thì số α' (số β') lấy số $\alpha'^r \bmod n$ (số $\beta'^r \bmod n$). Ngược lại thì lặp lại bước 1-3

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

Nếu số được tạo bởi α' và β' có bậc r^2 thuộc các nhóm con cyclic khác nhau G_{p^2} thì số α và β sẽ cũng thuộc các nhóm con cyclic khác nhau. Xác suất $\Pr(\alpha', \beta' \in G_{p^2})$ 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:

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

Vì vậy, thuật toán thứ hai tạo ra hai số 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 số 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 ra số 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 số 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 $y = \alpha^x \beta^w \bmod n$.

b) Tạo chữ ký

1) Chọn số 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

3.3.5. Xây dựng lược đồ ký số tập thể mù mới

Lược đồ ký số mù đề xuất 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 số 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 số 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 số 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

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 (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 tham số 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.

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 tham số (E, S, U) là chữ ký số hợp lệ tương ứng với thông điệp *M*.

Định lý 3.7 (chữ ký số mù): Bộ 3 số (E, S, U) là chữ ký số mù hợp lệ tương ứng với thông điệp *M*.

Định lý 3.8 (chữ ký số tập thể mù): Bộ 3 số (E,S,U) là chữ ký số tập thể mù hợp lệ tương ứng với thông điệp *M*.

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.

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.

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

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, 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 [69] và [93] là lược đồ chữ ký số tập thể mù dựa trên hai bài toán khó là IFP và DLP. 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. 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.

3.4. KẾT LUẬN CHƯƠNG 3

Chương 3 xây dựng lược đồ chữ ký số mù, chữ ký số tập thể mù dựa trên các lược đồ phổ biến như Schnorr và RSA để đảm bảo được tính an toàn và hiệu quả. 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].

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

Chương 4 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.

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.

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. 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.

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

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

4.3.3. Chữ ký số trên token được làm mù

4.3.4. Chữ ký trên phiếu bầu được làm mù

4.3.5. Xác thực thông tin dựa trên thông tin ẩn danh

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

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.

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

Trong tầng này, V_j và **BĐH** tương tác nhau như sau:

1) **BĐH** xác thực về tính hợp lệ của cử tri V_j bằng thông tin xác thực dựa trên thông tin ẩn danh [91].

2) Sau khi xác thực, **BĐH** chuyển $T_j(A, ID_j, Z_j)$ vào bảng ***danhsachcutri***.

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***.

4.4.2.2. Tầng đăng ký

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 tham số 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***. **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 $\delta_j(\alpha_j, \beta_j, T_j)$, gửi cho **BĐH** tính chữ ký số chung là $\{s_1(T_j), s_2(T_j)\}$ và gửi V_j.

5) V_j kiểm tra tính hợp lệ của chữ ký trên T_j được làm mù.

4.4.2.3. Tầng bỏ phiếu

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 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***

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 $t_j(\alpha'_j, \beta'_j, v_j) = \bar{s}'_j$ và đăng chúng lên bảng ***bangphieubau***

4.4.2.4. Tầng kiểm phiếu

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.

4.5. ĐÁNH GIÁ VÀ PHÂN TÍCH

Theo kết quả thực nghiệm, 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 ms. 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

Lược đồ bầu cử điện tử đề xuất đáp ứng độ an toàn theo các tính chất được đề cập trong [29] như: Tính riêng tư của cử tri; Không lộ thông tin bầu cử; Tính chính xác; Tính mạnh mẽ; Công bằng; Khả năng kiểm chứng; Dân chủ; Chống cưỡng chế.

4.7. KẾT LUẬN CHƯƠNG 4

Chương 4 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.

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, 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 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.

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 một 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.

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.