BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC DUY TÂN

NGUYỄN KIM TUẤN

NGHIÊN CỨU VÀ XÂY DỰNG LƯỢC ĐỒ CHỮ KÝ SỐ TẬP THỂ ĐẠI DIỆN

CHUYÊN NGÀNH: KHOA HỌC MÁY TÍNH
MÃ SỐ: 948 0101

TÓM TẮT LUẬN ÁN TIẾN SĨ KHOA HỌC MÁY TÍNH

NGƯỜI HƯỚNG DẪN KHOA HỌC:
1. TS. Hồ Ngọc Duy
2. PGS.TS. Đoàn Văn Ban

ĐÀ NẴNG – NĂM 2023

MỞ ĐẦU

1. Lý do chọn đề tài

Hiện đã có nhiều dạng lược đồ chữ ký số đã được nghiên cứu và công bố, như lược đồ chữ ký số đơn, lược đồ đa chữ ký số, lược đồ chữ ký số mù, lược đồ chữ ký số nhóm, lược đồ chữ ký tập thể, lược đồ chữ ký tập thể mù, v.v. Các hệ thống xác thực dựa trên chữ ký số nhóm, chữ ký số tập thể, v.v. hỗ trợ tốt cho các ứng dụng mà ở đó cần sự i) chứng thực đồng thời cả danh tính của người tạo ra thông tin và danh tính của tổ chức mà người này là một thành viên của nó và/hoặc ii) chứng thực đồng thời danh tính của tất cả thực thể trong một tổ chức tạo ra thông tin.

Đến nay đã có nhiều thuật toán, giao thức, lược đồ (Scheme) liên quan đến chữ ký số nhóm và chữ ký số tập thể đã được nghiên cứu và công bố, tất cả đều có điểm chung là chỉ tạo ra một chữ ký số duy nhất, nhưng nó đại diện được cho cả một nhóm hoặc một tập thể những người tham gia tạo ra chữ ký đó.

Gần đây, trong thực tế xuất hiện một dạng yêu cầu chứng thực dựa trên chữ ký (viết tay) mới, đó là, chứng thực cho cả một tập thể người ký. Mỗi thành viên trong tập thể này được định danh bằng một chữ ký riêng của họ. Sự định danh này bao gồm cả việc nhận biết một thành viên nào đó: i) Là thuộc nhóm thành viên nào; ii) Là thành viên đơn lẻ của tập thể; iii) Là trưởng nhóm của một nhóm thành viên nào; v.v.. cách đáng kể khi số lượng thành viên của tập thể tăng lên.

Theo nghiên cứu sinh, nếu kết hợp được nguyên lý hoạt động của lược đồ chữ ký nhóm và lược đồ chữ ký tập thể thì chúng ta có thể xây dựng được một dạng lược đồ đa người ký đáp ứng được yêu cầu chứng thực tập thể của bài toán xác thực nhiều thành viên.

Cụ thể, đầu tiên, sử dụng lược đồ chữ ký nhóm để tạo chữ ký

nhóm cho các nhóm thành viên trong tập thể, sau đó, sử dụng lược đồ chữ ký tập thể để tạo ra chữ ký tập thể từ những chữ ký của các nhóm thành viên và chữ ký của các cá nhân đơn lẻ. Lược đồ mới này hỗ trợ tạo ra một chữ ký đơn, nhưng có sự tham gia của tất cả thành viên trong tập thể ký nên nó đại diện cho tập thể ký này. Có thể xem đây là một dạng mở rộng của lược đồ chữ ký tập thể, có thể đặt tên cho dạng chữ ký đa người ký mới này là "Chữ ký tập thể đại diện".

Với mong muốn tìm hiểu khả năng ứng dụng vào thực tế của các lược đồ chữ ký số nhóm và lược đồ chữ ký số tập thể đã công bố, từ cơ sở đó đề xuất các lược đồ chữ ký tập thể đại điện đáp ứng yêu cầu xác thực cho nhiều bài toán thực tế hiện nay, nghiên cứu sinh chọn đề tài **"Nghiên cứu và Xây dựng lược đồ chữ ký số tập thể đại diện"** (Researching and Building the representative collective digital signature schemes) để nghiên cứu và trình bày trong luận án của mình.

2. Đối tượng và Phạm vi nghiên cứu

3. Mục tiêu và Nhiệm vụ nghiên cứu

Mục tiêu nghiên cứu của luận án là:

- Đề xuất được các lược đồ chữ ký số tập thể đại diện dựa trên một bài toán khó và dựa trên hai bài toán khó. Chứng minh được tính đúng đắn của lược đồ; Phân tích được mức độ an toàn (tính kháng "tấn công") và Đánh giá được hiệu năng của các lược đồ đề xuất.
- Đề xuất được các dạng lược đồ chữ ký tập thể đại diện chỉ gồm 2 thành phần nhưng vẫn đáp ứng được các yêu cầu cần thiết của một chữ ký số tập thể.

Nhiệm vụ nghiên cứu của luận án là:

- Tìm hiểu về các bài toán khó được sử dụng để xây dựng các dạng lược đồ chữ ký số: Bài toán phân tích thừa số; Bài toán logarit

rời rạc trên trường hữu hạn nguyên tố Z_p; Bài toán logarit rời rạc trên đường cong Elliptic; Bài toán tìm căn modulo.

- Tìm hiểu về các chuẩn chữ ký số quốc tế (DSS của Mỹ, GOST R34.10 của Nga, v.v.) và chuẩn đánh giá về mức độ an toàn của một số lược đồ chữ ký số. Phân tích hoạt động và cấp độ an toàn của một số lược đồ chữ ký số vừa được công bố trong những năm gần đây.
- Tìm hiểu về các lược đồ chữ ký số đơn (RSA, ElGamal, Rabin), chữ ký số nhóm, chữ ký số tập thể được xây dựng trên các bài toán khó: Phân tích thừa số, Logrit rời rạc, Tìm căn modulo. Đây là cơ sở để luận án đề xuất lược đồ chữ ký số tập thể đại diện được xây dựng dựa trên một bài toán khó.
- Tìm hiểu về các lược đồ chữ ký số nhóm, chữ ký số tập thể được xây dựng trên đồng thời hai bài toán khó.
- Từ hiểu biết này, luận án đề xuất lược đồ chữ ký số tập thể cho các nhóm ký được xây dựng dựa trên đồng thời hai bài toán khó: Bài toán Phân tích thừa số - Bài toán Logarit rời rạc.
- Tìm hiểu khả năng ứng dụng của chữ ký tập thể đại diện trong thực tế.

4. Phương pháp nghiên cứu

Luận án sử dụng kết hợp hai phương pháp nghiên cứu: Phương pháp nghiên cứu Toán học và Phương pháp nghiên cứu Mô hình hóa.

i) Theo phương pháp nghiên cứu Toán học:

- Đầu tiên, nghiên cứu về những kiến thức toán học được sử dụng để phát triển: i) Các hệ mật mã bất đối xứng, các thuật toán xử lý số nguyên tố lớn, v.v.; Và ii) Các bài toán khó: Bài toán phân tích thừa số; Bài toán logarit rời rạc; v.v..
- Tiếp đến, nghiên cứu về việc sử dụng bài toán khó để xây dựng: Chuẩn chữ ký số và Thuật toán và lược đồ chữ ký số.
- Cuối cùng, tìm ra công cụ toán học và quy trình để xây dựng

một lược đồ chữ ký số tập thể mới mà nó đảm bảo tính đúng, tính an toàn và hiệu năng cao. Tất cả điều này phải được chứng minh về mặt toán học.

ii) Theo phương pháp nghiên cứu Mô hình hóa:

- Đầu tiên, tìm hiểu yêu cầu chứng thực của một số bài toán thực tế, đặc biệt là các yêu cầu chứng thực cho một tập thể nhiều thành viên.
- Tiếp đến, tìm cách mô hình hóa bài toán yêu cầu chứng thực tập thể theo hướng có thể xây dựng được lược đồ chữ ký.
- Cuối cùng, áp dụng công cụ toán học và quy trình đã được xác định để xây dựng lược đồ chữ ký số.

5. Nội dung nghiên cứu

Nghiên cứu tổng quan:

Nghiên cứu của nghiên cứu sinh:

- Nghiên cứu về ưu điểm, nhược điểm của các lược đồ chữ ký số đã công bố. Nghiên cứu về khả năng ứng dụng của các lược đồ chữ ký số nhóm và lược đồ chữ ký số tập thể. Từ đó tìm cách xây dựng lược đồ chữ ký số cho bài toán chứng thực tập thể ký được nêu ra ở trên (Mục 1).
- Nghiên cứu xây dựng các lược đồ chữ ký tập thể đại diện dựa trên một bài toán khó hoặc trên đồng thời hai bài toán khó: Phân tích thành nhân tử; Logarit rời rạc trên trường hữu hạn nguyên tố $GP(p)$ và trên đường cong Elliptic; Tìm căn modulo số nguyên tố lớn; v.v..
- Chứng minh bằng toán học độ an toàn, độ phức tạp và hiệu năng tính toán của lược đồ chữ ký số tập thể được đề xuất.
- Nghiên cứu khả năng ứng dụng của các lược đồ chữ ký số tập thể đại diện được đề xuất vào các ứng dụng giao dịch điện tử, trao đổi tài liệu điện tử mà nó cần mức độ bảo mật, tính toàn vẹn và khả năng xác thực cao.

6. Ý nghĩa Khoa học và Thực tiễn của đề tài

Ý nghĩa khoa học của đề tài :

- Đề tài cho thấy, dựa vào các bài toán khó như: Logarit rời rạc trên trường nguyên tố hữu hạn và trên đường cong Elliptic; Tìm căn modulo số nguyên tố lớn; Phân tích số nguyên thành các nhân tử nguyên tố; v.v. chúng ta có thể xây dựng được các lược đồ chữ ký nhóm, các lược đồ chữ ký tập thể đại diện theo các chuẩn chữ ký số khác nhau, như: DSS, GOST, v.v., đảm bảo độ an toàn cao.
- Đề tài cũng chỉ ra rằng, mức độ an toàn của một lược đồ chữ ký số tập thể không những phụ thuộc vào tính khó giải của bài toán khó được áp dụng mà còn phụ thuộc vào hoạt động của các giao thức sử dụng trong lược đồ.

Ý nghĩa thực tiễn của đề tài:

- Các lược đồ chữ ký số tập thể đại diện mà đề tài đề xuất hoàn toàn có thể đáp ứng được yêu cầu chứng thực, mang tính tập thể đa cấp, ngày càng cao của nhiều ứng dụng giao dịch, trao đổi thông tin hoạt động trên không gian mạng.
- Các lược đồ chữ ký mà đề tài đề xuất có thể triển khai hoạt động dựa trên hạ tầng PKI đang tồn tại trong các hệ thống chứng thực, chữ ký số hiện nay.

7. Bố cục của luận án

- **Chương 1 - Tổng quan về chữ ký số và chữ ký số tập thể:** Những kiến thức cơ sở liên quan đến chữ ký số và lược đồ chữ ký số được tìm hiểu và chọn trình bày ở chương này. Cụ thể: Các chuẩn lược đồ chữ ký số; Cơ sở toán học và các bài toán khó thường được sử dụng để xây dựng chữ ký số; Sự tương đương và sự khác biệt giữa chữ ký số nhóm và chữ ký tập thể với chữ ký tập thể đại diện.
- **Chương 2 - Xây dựng lược đồ chữ ký số tập thể đại diện dựa trên các bài toán logarit rời rạc:** Chương này trình bày các lược đồ chữ ký số tập thể đại diện, do NCS đề xuất, được xây dựng

dựa trên: i) Bài toán logarit rời rạc trên trường hữu hạn nguyên tố; ii) Bài toán logarit rời rạc trên đường cong Elliptic.

- **Chương 3 - Xây dựng lược đồ chữ ký số tập thể đại diện dựa trên bài toán tìm căn modulo số nguyên tố:** Nội dung chính của chương 3 là các lược đồ chữ ký tập thể đại diện dựa trên bài toán tìm căn modulo số nguyên tố lớn, với modulo p là số nguyên tố lớn có cấu trúc: i) $p = Nt_0t_1t_2 + 1$ (private key hai thành phần); và $p = Nk^2 + 1$ (private key một thành phần).

- **Chương 4 – Cải thiện Kích thước và Mức độ an toàn của chữ ký tập thể đại diện:** Các chữ ký tập thể đại diện được xây dựng trong các chương 2 và 3 tồn tại hai vấn đề cần xem xét: Kích thước của chữ ký lớn và Mức độ an toàn chỉ dựa vào một bài toán khó. Hạn chế và hướng giải quyết cho vấn đề này được chỉ ra ở phần đầu của chương 4.

CHƯƠNG 1:

TỔNG QUAN VỀ CHỮ KÝ SỐ VÀ LƯỢC ĐỒ CHỮ KÝ SỐ TẬP THỂ

Chương này trình bày các vấn đề cơ sở nhất liên quan đến chữ ký số và lược đồ chữ ký số. Chữ ký số tập thể và chữ ký số nhóm sẽ được mô tả chi tiết ở đây. Nội dung chính của chương 1 là phần trình bày về một yêu cầu chứng thực thực tế, mà nó đòi hỏi phải có một loại đa chữ ký mới thì mới đáp ứng được, đó là, chữ ký tập thể đại diện. Tính thực tế và cấp thiết của loại chữ ký tập thể mới này được trình bày khá rõ ở mục 1.5. Những nghiên cứu liên quan đến đề tài luận án và hướng nghiên cứu của nghiên cứu sinh cũng được đề cập trong chương 1. Vấn đề được trình bày ở cuối chương là cơ sở toán học được sử dụng để xây dựng các lược đồ chữ ký nói chung và lược đồ chữ tập thể đại diện nói riêng.

1.1. Chữ ký số và Lược đồ chữ ký số

1.2. Chuẩn chữ ký số và Lược đồ chữ ký số chuẩn

1.3. Chữ ký số nhóm và Lược đồ chữ ký số nhóm

1.4. Chữ ký số tập thể và Lược đồ chữ ký số tập thể

1.5. Chữ ký số tập thể đại diện và Hướng nghiên cứu

1.5.1. Chữ ký số tập thể đại diện

Trong phần Lý do chọn đề tài, luận án đã chỉ ra một yêu cầu chứng thực khá thực tế hiện nay, đó là chứng thực dựa trên chữ ký (viết tay) cho một tập thể người ký, trong đó gồm nhiều nhóm thành viên, mỗi nhóm thành viên có một trưởng nhóm, và một số thành viên đơn lẻ.

Xét cơ cấu tổ chức của một công ty trong thực tế, ví dụ Công ty A (xem hình 1.4): Ban lãnh đạo Công ty A gồm 1 giám đốc (GĐ) và 2 phó giám đốc (PGĐ1, PGĐ2); Có 4 đơn vị chức năng trong Công ty A: A1, A2, A3, A4. Mỗi đơn vị có một trưởng đơn vị: TrA1,

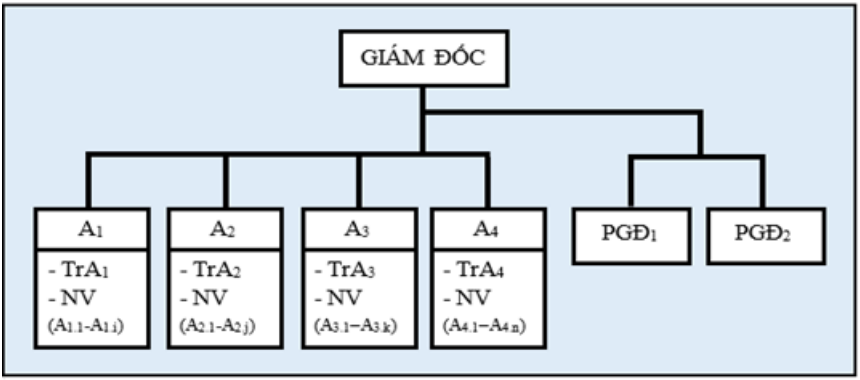
TrA2, TrA3, TrA4, và một số nhân viên thuộc đơn vị. Nhân viên A1-1 và A1-5 thuộc đơn vị A1, nhân viên A2-5 thuộc đơn vị A2… Khi yêu cầu chứng thực cho tất cả nhân sự trong công ty này được đặt ra thì nó có thể xem như một tập thể ký đa cấp: GĐ, PGĐ – Trưởng đơn vị và Nhân viên trong đơn vị. Tập thể ký này gồm 4 nhóm thành viên: A1, A2, A3, A4. Các trưởng nhóm tương ứng là: TrA1, TrA2, TrA3, TrA4. Thành viên đơn lẻ là PGĐ1 và PGĐ2 (ở đây chưa xét đến vai trò của GĐ). Vấn đề đặt ra ở đây là: i) Làm thế nào để chứng thực cho tất cả thành viên của Công ty A chỉ với một chữ ký duy nhất hay ii) Làm thế nào để định danh chính xác một nhân viên nào đó của Công ty A là thuộc một đơn vị nào hay là thành viên đơn lẻ, họ có phải trưởng đơn vị hay không, một thành viên nào đó, một đơn vị nào đó có phải thuộc công ty hay không.

Nếu yêu cầu chứng thực này được thực hiện theo cách truyền thống, tức là, mọi thành viên của tập thể ký này, từ thành viên nhóm ký đến trưởng nhóm ký và cả những người ký đơn lẻ, đều ký lên tài liệu cần ký, thì công việc của bên kiểm tra chữ ký sẽ rất phức tạp và tốn nhiều thời gian, vì phải kiểm tra tính hợp lệ của từng chữ ký của các đối tượng người ký khác nhau, thành viên nhóm, trưởng nhóm thành viên, thành viên đơn lẻ.

Có thể khắc phục hạn chế vừa nêu bằng cách chỉ tạo ra một chữ ký duy nhất, đại diện cho cả một tập thể người ký, mọi công việc chứng thực cho tập thể này chỉ thực hiện trên một chữ ký chung đó. Sau đây là một vài cách tiếp cận được xem xét để tạo ra một chữ ký chung đại diện cho một tập thể ký:

i) Mỗi thành viên của một nhóm ký, tạo ra một chữ ký, rồi "nối" lại thành một chữ ký của nhóm ký. Sau đó "nối" các chữ ký của các nhóm ký và các chữ ký của các thành viên đơn lẻ thành một chữ ký chung cho tập thể ký. Khi đó công việc của bên kiểm tra chữ ký sẽ đơn giản hơn vì chỉ thực hiện trên một chữ ký duy nhất. Nhưng điều này khó khả thi trong thực tế, vì làm cách nào để "nối" và điều

gì sẽ xảy ra khi số lượng thành viên của tập thể ký là lớn.



Hình 1.4. Sơ đồ tổ chức của Công ty A

ii) Chỉ sử dụng chữ ký của trưởng nhóm như là chữ ký đại diện của nhóm ký của họ. Bước tiếp theo thực hiện như cách trên. Cách này có vẻ khả thi trong thực tế hơn về thường số lượng nhóm ký và người ký đơn lẻ trong một tập thể ký không nhiều. Nhưng "dấu vết" của các thành viên trong các nhóm ký hoàn toàn không xuất hiện trong chữ ký cuối cùng của tập thể. Như vậy, khả năng "chống chối bỏ" của hệ chứng thực dựa trên chữ ký này khó có thể đảm bảo.

iii) Tất cả thành viên của tập thể đều đóng góp những thông tin liên quan cần thiết để từ đó tạo ra một chữ ký duy nhất chung cho tập thể ký. Chữ ký này sẽ là đại diện cho tập thể trong việc xác thực sau này. Vì chữ ký chung của tập thể có chứa thông tin của tất cả thành viên tham gia vào việc tạo ra chữ ký nên vấn đề "chống chối bỏ", vấn đề xác định nguồn gốc của thành viên, thuộc nhóm thành viên nào, của hệ chứng thực này có thể được đảm bảo. Cách tiếp cận này có thể giải quyết được vấn đề thời gian và độ phức tạp của bên kiểm tra chữ ký nhưng hoàn toàn không khả thi trong thực tế.

Như vậy, những hướng tiếp cận ở trên đều khó có thể triển khai trong thực tế, trên hệ chữ ký viết tay. Điều này đã mở ra một hướng nghiên cứu mới là, xây dựng một lược đồ chữ ký số mà đáp ứng

được yêu cầu của bài toán chứng thực cho một tập thể ký đa cấp chức năng như đã nêu. Đây cũng chính là nhiệm vụ nghiên cứu của NCS trong đề tài luận án này.

Qua nghiên cứu bước đầu, NCS thấy rằng, mặc dù cả lược đồ chữ ký nhóm và lược đồ chữ ký tập thể đều hỗ trợ tạo ra một chữ ký chung, đại diện cho một tập nhiều người ký, chứa đầy đủ thông tin cần thiết để có thể truy vết, định danh nguồn gốc thành viên và chống lại "sự chối bỏ trách nhiệm" sau này. Nhưng cả hai dạng lược đồ này khó có thể đáp ứng được mô hình chứng thực cho các thành viên của một tập thể người ký đa cấp được nêu ra trong luận án này. Theo NCS, nếu kết hợp được những ưu điểm của lược đồ chữ ký nhóm và lược đồ chữ ký tập thể thì có thể xây dựng được một dạng lược đồ chữ ký tập thể mở rộng có thể đáp ứng được yêu cầu của bài toán chứng thực tập thể đa cấp chức năng đã được đặt ra (như đã phân tích ở phần Lý do chọn đề tài). Luận án tạm đặt tên cho dạng lược đồ chữ ký tập thể mới này là "Lược đồ chữ ký số tập thể đại diện" (Representative collective signature scheme).

Theo cách tiếp cận này, bài toán chứng thực tập thể cho Công ty A ở trên có thể thực hiện thông qua một chữ ký số duy nhất (đơn), nhưng chữ ký này được hình thành như sau: i) Đầu tiên, mỗi trưởng đơn vị chịu trách nhiệm tạo ra chữ ký nhóm cho đơn vị của họ. Việc kiểm tra tư cách thành viên và lưu trữ thông tin định danh của những thành viên nhóm đã tham gia vào việc tạo ra chữ ký này do trưởng nhóm thực hiện. Theo cách này, mỗi thành viên đơn lẻ cũng được xem là một trưởng nhóm, nhưng nhóm của họ không có thành viên; ii) Sau đó, từ chữ ký của các nhóm và của các thành viên đơn lẻ, một trưởng nhóm hoặc một thành viên đơn lẻ bất kỳ hoặc là Giám đốc công ty thực hiện nhiệm vụ tạo chữ ký tập thể, đại diện cho tập thể ký. Việc kiểm tra tư cách thành viên của những người tham gia tạo ra chữ ký tập thể cũng được thực hiện ở đây. Những thông tin liên quan cần thiết cũng được lưu trữ trong chữ ký của tập thể ký;

Như vậy, việc chứng thực cho tập thể Công ty A chỉ cần thực hiện trên chữ ký tập thể của công ty. Chữ ký này có đủ thông tin cần thiết để phục vụ cho việc truy vết, định danh thành viên nhóm/thành viên tập thể và chống lại "sự chối bỏ trách nhiệm" khi cần.

1.5.1. Hướng nghiên cứu của nghiên cứu sinh

Từ những phân tích trên, NCS tập trung nghiên cứu các nội dung chính sau:

- Xây dựng khung lược đồ chữ ký tập thể đại diện, sao cho vừa đáp ứng bài toán chứng thực tập thể đặt ra vừa thỏa mãn các yêu cầu quy chuẩn của một lược đồ đa chữ ký.
- Sử dụng các chuẩn chữ ký số và/hoặc các dạng lược đồ chữ ký số chuẩn để xây dựng các lược đồ chữ ký tập thể đại diện.
- Xây dựng lược đồ chữ ký tập thể đại diện dựa trên một bài toán khó hoặc dựa trên hai bài toán khó. Đồng thời tìm cách thay đổi cấu trúc của một số tham số đầu vào để tăng độ khó của một số lược đồ.

Trong luận án này, NCS đề xuất và xây dựng hai dạng lược đồ chữ ký số tập thể đại diện: i) Lược đồ chữ ký tập thể cho các nhóm ký (hay còn được gọi là Lược đồ chữ ký tập thể được chia sẻ bởi nhiều nhóm ký): Cung cấp khả năng chứng thực cho một tập thể ký mà trong đó gồm nhiều nhóm ký khác nhau và ii) Lược đồ chữ ký tập thể cho các nhóm ký và các cá nhân ký (hay còn được gọi là Lược đồ chữ ký số tập thể được chia sẻ bởi nhiều nhóm ký và nhiều cá nhân ký): Cung cấp khả năng chứng thực cho một tập thể ký mà trong đó gồm nhiều nhóm ký và nhiều người ký cá nhân khác nhau.

1.6. Một số nghiên cứu liên quan luận án

1.7. Một số bài toán khó dùng trong xây dựng lược đồ

Kết luận Chương 1:

Chương này của luận án đã trình bày những nội dung chính sau đây: i) Các định nghĩa, khái niệm, thuật ngữ, v.v. liên quan đến chữ

ký số và lược đồ chữ ký số, đặc biệt, là chữ ký số nhóm và chữ ký số tập thể; ii) Mô tả một số lược đồ chữ ký số chuẩn và một số lược đồ chữ ký số thuộc các chuẩn của Mỹ và của Nga; iii) Trình bày mục tiêu và hướng nghiên cứu của đề tài: Yêu cầu xác thực tập thể và Chữ ký tập thể đại diện (phần chính của chương 1); iv) Phần cuối của Chương 1 trình bày những vấn đề toán học cơ sở và các bài toán khó liên quan mà NCS sử dụng để xây dựng các lược đồ được đề xuất trong các chương sau của luận án.

CHƯƠNG 2:

XÂY DỰNG LƯỢC ĐỒ CHỮ KÝ SỐ TẬP THỂ ĐẠI DIỆN DỰA TRÊN CÁC BÀI TOÁN LOGARIT RỜI RẠC

Trong chương này, nghiên cứu sinh sẽ thực hiện đồng thời hai việc chính. Thứ nhất, đề xuất hai dạng lược đồ chữ ký tập thể mới mà nó cho phép tạo ra một chữ ký tập thể đại diện duy nhất, đại diện cho một tập thể đa cấp chức năng, đã được trình bày ở chương 1. Thứ hai, sử dụng các bài toán logarit rời rạc để xây dựng: i) Lược đồ chữ ký tập thể cho nhiều nhóm ký và ii) Lược đồ chữ ký tập thể cho nhiều nhóm ký và nhiều người ký cá nhân.

2.1. Xây dựng lược đồ chữ ký tập thể đại diện dựa trên bài toán logarit rời rạc trên trường hữu hạn nguyên tố

2.1.1. Lược đồ chữ ký tập thể (Ký hiệu: CDS-2.1)

2.1.2. Lược đồ chữ ký số nhóm (Ký hiệu: GDS-2.1)

2.1.3. Lược đồ chữ ký tập thể cho nhiều nhóm ký (Ký hiệu: RCS.01-2.1)

Lược đồ chữ ký tập thể cho nhiều nhóm ký dưới đây được xây dựng từ hai lược đồ cơ sở đã được trình bày ở 2.1.1 (CDS-2.1) và 2.1.2 (GDS-2.1). Giả sử có một tập thể ký gồm g nhóm ký, muốn tạo chữ ký tập thể đại diện lên tài liệu M. Cho X_j là private key của GM của nhóm ký thứ j ($j = 1, 2, \ldots, g$) và public key tương ứng là $Y_j = \alpha^{X_j} \bmod p$. Y_j cũng chính là public key của nhóm ký thứ j của tập thể ký này.

Giả sử nhóm ký thứ j gồm m thành viên ký (ký hiệu là m_j), đây là những người được chỉ định tham gia vào việc hình thành chữ ký nhóm của nhóm ký thứ j. Mỗi thành viên thứ i (với $i = 1, 2, \ldots, m_j$) trong nhóm ký thứ j có private key là x_{ji} ($|x| \geq 256\ bít$) và public key tương ứng là $y_{ji} = \alpha^{x_{ji}} \bmod p$.

Các tham số được sử dụng trong các giao thức của lược đồ bao

gồm: i) Một số nguyên tố đủ lớn p ($|p| > 2048\ bít$), một số nguyên tố q ($|q| \geq 256\ bít$), sao cho $q|p-1$; ii) Một số α có bậc bằng q modulo p.

- **Thủ tục sinh chữ ký tập thể cho nhiều nhóm ký trên M**

Gồm các bước sau:

1. Mỗi GM, của nhóm ký thứ j, thực hiện:

- Tạo ra các tham số mặt nạ λ_{ji} cho những người ký của nhóm j theo (2.10) trong thủ tục sinh chữ ký của lược đồ GDS-2.1.
- Tính U_j và R_j của nhóm ký thứ j theo công thức (2.24) và (2.25):

$$U_j = \prod_{i=1}^{m_j} y_{ji}^{\lambda_{ji}} \, mod\, p \tag{2.24}$$

và $R_j = R_j' \prod_{i=1}^{m_j} R_{ji} \, mod\, p$ (2.25)

Đây là hai giá trị mà nhóm ký thứ j chia sẻ với các nhóm ký khác để tạo chữ ký tập thể của tập thể ký gồm g nhóm ký.

- Gửi U_j và R_j đến tất cả GM của các nhóm ký khác.

2. Một GM nào đó trong tập thể ký thực hiện việc tính các giá trị U, R và E theo các công thức:

$$U = \prod_{j=1}^{g} U_j \, mod\, p \tag{2.26}$$

$$R = \prod_{j=1}^{g} R_j \, mod\, p = \alpha^{\sum_{j=1}^{g} K_j} \, mod\, p \tag{2.27}$$

$$\mathrm{E} = \mathrm{F_H}(\mathrm{M}\|\mathrm{R}\|\mathrm{U}) \tag{2.28}$$

U và E là hai thành phần đầu tiên của chữ ký tập thể cho g nhóm ký.

3. Mỗi GM, của nhóm ký thứ j, tiếp tục thực hiện:

- Tính thành phần chia sẻ của nhóm ký thứ j:

$$S_j = S_j' + \sum_{i=1}^{m_j} S_{ji} \, mod\, q \tag{2.29}$$

S_{ji} là thành phần chia sẻ của người ký thứ i trong nhóm thứ j.

- Gửi S_j cho tất cả GM của các nhóm ký khác trong tập thể ký.

4. Một GM nào đó trong tập thể ký thực hiện việc cuối cùng:

- Kiểm tra tính hợp lệ của các thành phần S_j bằng công thức:

$$R_j = \left(U_j Y_j\right)^E \alpha^{S_j} \, mod\, p \tag{2.30}$$

- Nếu tất cả S_j đều thỏa mãn công thức này thì tính thành phần thứ ba S của chữ ký tập thể theo công thức:

$$S = \sum_{j=1}^{g} S_j \, mod \, q \quad (2.31)$$

Vậy bộ ba giá trị (U, E, S) là chữ ký tập thể đại diện, của một tập thể gồm g nhóm ký, trên tài liệu M (dạng chữ ký này còn được gọi là, chữ ký tập thể được chia sẻ bởi g nhóm ký). Nó đại diện cho tập thể ký này.

- **Thủ tục kiểm tra chữ ký tập thể cho nhiều nhóm ký trên M**

Để kiểm tra tính hợp lệ của chữ ký nhận được cùng với tài liệu M, bên kiểm tra (người kiểm tra/verifier) thực hiện các bước sau:

1. Tính public key tập thể được chia sẻ bởi tất cả các nhóm ký:

$$Y_{col} = \prod_{j=1}^{g} Y_j \, mod \, p = \alpha^{\sum_{j=1}^{g} X_j} \, mod \, p \quad (2.32)$$

2. Tính giá trị R^*theo công thức sau:

$$R^* = (UY_{col})^E \alpha^S \, mod \, p \quad (2.33)$$

3. Tính giá trị E^*theo công thức sau:

$$E^* = F_H(M \| R^* \| U) \quad (2.34)$$

4. So sánh E^* với E.

Nếu $E^* = E$: Chữ ký nhận được là hợp lệ; Ngược lại, chữ ký nhận được là không hợp lệ, nó bị từ chối.

2.1.4. Lược đồ chữ ký tập thể cho nhiều nhóm ký và nhiều người ký cá nhân (Ký hiệu: RCS.02-2.1)

2.2. Xây dựng lược đồ chữ ký tập thể đại diện dựa trên bài toán logarit rời rạc trên đường cong Elliptic sử dụng chuẩn ECDSA

Thuật toán chữ ký dựa trên bài toán logarit rời rạc trên đường cong Elliptic đã được chuẩn hóa trong các chuẩn ECDSA và GOST R34.10-2001. NCS sử dụng các chuẩn này để xây dựng các lược đồ chữ ký tập thể đại diện nhằm "hưởng lợi" từ các ưu điểm bảo mật của hệ mật mã trên đường cong Elliptic.

2.2.1. Lược đồ chữ ký tập thể theo ECDSA (K. hiệu: CDS-2.2)

2.2.2. Lược đồ chữ ký nhóm theo ECDSA (K. hiệu: GDS-2.2)

2.2.3. Lược đồ chữ ký tập thể cho nhiều nhóm ký theo chuẩn ECDSA (Ký hiệu: RCS.01-2.2)

Giả sử có một tập thể ký gồm g nhóm ký, muốn tạo chữ ký tập thể đại diện lên tài liệu M. Cho z_j là private key của GM của nhóm ký thứ j (j $= 1, 2, \ldots,$ g) và public key tương ứng là $L_j = z_j G$. L_j cũng chính là public key của nhóm ký thứ j của tập thể ký này.

Giả sử nhóm ký thứ j gồm m thành viên ký (ký hiệu là m_j), đây là những người được chỉ định tham gia vào việc hình thành chữ ký nhóm của nhóm ký thứ j. Mỗi thành viên thứ i (với i $= 1, 2, \ldots, m_j$), trong nhóm ký thứ j, có private key là k_{ji} public key tương ứng của họ là P_{ji}: $P_{ji} = k_{ji} G$.

2.2.4. Lược đồ chữ ký tập thể cho nhiều nhóm ký và nhiều người ký cá nhân theo chuẩn ECDSA (Ký hiệu: RCS.02-2.2)

Giả sử có một tập thể ký gồm g nhóm ký và m người ký cá nhân, muốn tạo chữ ký tập thể đại diện lên tài liệu M. Giả sử nhóm ký thứ j gồm m thành viên ký (ký hiệu là m_j), đây là những người được chỉ định tham gia vào việc hình thành chữ ký nhóm của nhóm ký thứ j (j $= 1, 2, \ldots,$ g) và mỗi người ký cá nhân được xem như một nhóm ký mà chỉ có một thành viên duy nhất.

Mỗi người ký (signer) thứ i trong nhóm ký sở hữu một private key là k_{ji} và public key tương ứng của họ là $P_{ji} = k_{ji} G$, với $i = 1, \ldots, m$. GM của nhóm ký thứ j có private key và public key lần lượt là z_j và L_j ($L_j = z_j G$). L_j cũng chính là public key của nhóm ký thứ j.

Public key và private key của mỗi người ký cá nhân là $L_j = k_j G$ và k_j ($j = g + 1, g + 2, \ldots, g + m$). Trong lược đồ này, "chữ ký nhóm" tương ứng với mỗi người ký cá nhân là (O, e, s), trong đó O là điểm vô cực của đường cong Elliptic.

2.3. Đánh giá khả năng bảo mật và hiệu năng tính toán của lược

đồ chữ ký tập thể đại diện đã được xây dựng

2.3.1. Khả năng chống tấn công từ bên trong

Đối với chữ ký tập thể, những người tham gia vào việc hình thành chữ ký lại là những người có nhiều khả năng tấn công vào chính lược đồ chữ ký mà họ tạo ra hơn là những người từ bên ngoài.

Vì thế, sau đây chỉ trình bày về hai dạng tấn công dựa vào lược đồ chữ ký tập thể phổ biến mà nó xuất phát từ chính những thành viên của tập thể ký.

- Loại tấn công thứ nhất (Giả mạo chữ ký của người ký m)
- Loại tấn công thứ hai (Tìm private key của người ký m)

2.3.2. Ưu điểm bảo mật của lược đồ chữ ký nhóm GDS-2.1

2.3.3. Khả năng bảo mật của các lược đồ chữ ký tập thể đại diện

2.3.4. Đánh giá hiệu năng tính toán của lược đồ chữ ký tập thể đại diện

Luận án đánh giá hiệu năng tính toán của các lược đồ chữ ký tập thể đại diện thông qua việc tính chi phí thời gian mà lược đồ cần cho quá trình sinh chữ ký (Thủ tục sinh chữ ký) và cần cho quá trình kiểm tra tính hợp lệ của chữ ký (Thủ tục kiểm tra chữ ký).

Sau đây là một số quy ước được sử dụng trong các công thức tính chi phí thời gian thực hiện các phép tính trong hai thủ tục nói trên: T_h: Chi phí tính toán của phép toán băm trên Z_p; T_s: Chi phí tính toán của phép nhân tích vô hướng trên Z_p; T_{inv}: Chi phí tính toán của phép nghịch đảo trên Z_p; T_e: Chi phí tính toán của phép mũ trên Z_p; T_m: Chi phí tính toán của phép nhân trên Z_p; T_+: Chi phí tính toán của cộng các điểm trên Z_p. Quy đổi: $T_h \approx T_m, T_s \approx 29T_m, T_{inv} \approx 240T_m, T_e \approx 240T_m,\ T_+ \approx 0.12T_m$ (theo [15]).

Kết quả tính toán được cho ở các bảng sau:

Bảng 2.1: Chi phí thời gian của các lược đồ RCS dựa trên bài toán DLP

Lược đồ	Chi phí thời gian	
	Sinh chữ ký	Kiểm tra chữ ký

RCS.01-2.1	$U = \sum_{j=1}^{g}(243m_j + 1)\,T_m$ $E = [\sum_{j=1}^{g}(241m_j + 240) + 1]T_m$ $S = \sum_{j=1}^{g}(484m_j + 1)\,T_m$ $Sum = [\sum_{j=1}^{g}(968m_j + 242) + 1]T_m$	$(483 + g)T_m$
RCS.02-2.1	$U = \sum_{j=1}^{g}(243m_j + 1)\,T_m$ $E = [\sum_{j=1}^{g}(241m_j + 240) + 240m + 1]T_m$ $S = [\sum_{j=1}^{g}(484m_j + 1) + 482m]T_m$ $Sum = [\sum_{j=1}^{g}(968m_j + 242) + 722m + 1]T_m$	$(483 + g + m)T_m$
RCS.01-2.2	$U = \sum_{j=1}^{g}(32m_j)\,T_m$ $e = [\sum_{j=1}^{g}(29m_j + 29) + 1]\,T_m$ $s = \sum_{j=1}^{g}(61m_j + 1)\,T_m$ $Sum = [\sum_{j=1}^{g}(122m_j + 30) + 1]\,T_m$	$(59 + 0.12g)T_m$
RCS.02-2.2	$U = \sum_{j=1}^{g}(32m_j)\,T_m$ $e = \sum_{j=1}^{g}[(29m_j + 29) + 29m + 1]\,T_m$ $s = [\sum_{j=1}^{g}(61m_j + 1) + 61m]T_m$ $Sum = [\sum_{j=1}^{g}(122m_j + 30) + 90m + 1]\,T_m$	$(59 + 0.12g + 0.12m)T_m$

Dữ liệu trong bảng này cho thấy, chi phí thời gian cho việc sinh chữ ký và kiểm tra chữ ký của lược đồ chữ ký tập thể đại diện dựa trên bài toán logarit rời rạc trên GF(p) là cao hơn khá nhiều so với chữ ký và bài toán cùng loại trên đường cong Elliptic. Điều này thêm một lần nữa khẳng định ưu thế của hệ mật mã đường cong Elliptic so với các hệ mật mã khác thường được sử dụng để xây dựng chữ ký số và lược đồ chữ ký số.

Kết luận Chương 2:

Chương này trình bày các lược đồ chữ ký tập thể đại diện được xây dựng dựa trên bài toán logarit rời rạc trên trường nguyên tố hữu hạn và bài toán logarit rời rạc trên đường cong Elliptic sử dụng chuẩn ECDSA. Với mỗi bài toán, có hai dạng của lược đồ chữ ký tập thể đại diện được xây dựng, đó là: Lược đồ chữ ký tập thể cho nhiều nhóm ký và lược đồ chữ ký tập thể cho nhiều nhóm ký và nhiều người ký cá nhân.

Chương 2 cũng trình bày chi tiết về các lược đồ chữ ký tập và các lược đồ chữ ký nhóm. Đây là các lược đồ cơ sở mà NCS sử dụng để xây dựng các lược đồ chữ ký tập thể đại diện. Khả năng chống tấn công, ưu điểm bảo mật và hiệu năng tính toán của các lược đồ chữ ký được xây dựng cũng được trình bày ở chương này.

Những công bố của NCS được sử dụng trong chương này: [CT3], [CT5], [CT9], [CT14].

CHƯƠNG 3:

XÂY DỰNG LƯỢC ĐỒ CHỮ KÝ TẬP THỂ ĐẠI DIỆN DỰA TRÊN BÀI TOÁN TÌM CĂN MODULO SỐ NGUYÊN TỐ LỚN

Trong chương này, để củng cố tính khả thi của lược đồ chữ ký tập thể đại diện, nghiên cứu sinh sử dụng vấn đề khó của bài toán tìm căn modulo số nguyên tố lớn, đây là một dạng bài toán khó mới do Nikolay A. Moldovyan đề xuất, để xây dựng các lược đồ chữ ký tập thể đề xuất. Vấn đề khó của bài toán này phụ thuộc nhiều vào cấu trúc của modulo nguyên tố p nên chương 3 sẽ nghiên cứu và trình bày các lược đồ liên quan đến hai cấu trúc của p: $p = Nk^2 + 1$ (i) và $p = Nt_0t_1t_2 + 1$ (ii). Private key hai thành phần, một dạng khóa mới có nhiều ưu điểm bảo mật, được sử dụng khi lược đồ được xây dựng với modulo nguyên tố p có cấu trúc (ii).

3.1. Xây dựng lược đồ chữ ký số tập thể đại diện dựa trên bài toán tìm căn modulo số nguyên tố lớn có cấu trúc $p = Nk^2 + 1$

Phần này trình bày về 2 dạng của lược đồ chữ ký tập thể đại diện, và các lược đồ cơ sở liên quan, được xây dựng dựa trên độ khó của bài toán tìm căn modulo số nguyên tố lớn, với số nguyên tố có cấu trúc đặc biệt, được đề xuất bởi Nikolay A. Moldovyan và Victor A. Shcherbacov trong [70]. Cụ thể, $p = Nk^2 + 1$, với k là một số nguyên tố lớn ($|k| \geq 160$ bit) và N là một số chẵn sao cho độ lớn của p thỏa mãn $|p| \geq 1024$ bit.

Để tạo ra chữ ký cá nhân dựa trên bài toán khó này, người ký phải chọn ngẫu nhiên một số x để làm private key. Public key y được tính theo công thức sau: $y = x^k \ mod \ p$. Chữ ký số trên tài liệu M, là tài liệu cần được ký lên đó bởi người ký, được tạo ra trong trường hợp này là cặp giá trị số (E, S). Độ lớn của S bằng với độ lớn của p, $|p| \geq 1024$ bit, độ lớn của E bằng độ lớn của δ, $|\delta| \geq 160$ bit, với δ là một số nguyên tố được chỉ định trước.

3.1.1. Lược đồ chữ ký số tập thể (Ký hiệu: CDS-3.1)

3.1.2. Lược đồ chữ ký nhóm (Ký hiệu: GDS-3.1)

3.1.3. Lược đồ chữ ký số tập thể cho nhiều nhóm ký (Ký hiệu RCS.01-3.1)

Lược đồ chữ ký tập thể và chữ ký nhóm được mô tả ở trên là cơ sở để luận án xây dựng lược đồ chữ ký tập thể cho một tập thể ký. Tập thể ký này gồm g nhóm ký, mỗi nhóm ký gồm m thành viên. Nhóm thứ j có m_j cá nhân ký.

Private key và public key của mỗi nhóm ký là: X_j và Y_j ($j = 1, 2, \dots, g$): $Y_j = X_j^k \ mod\ p$. Giao thức của chữ ký tập thể cho các nhóm ký được mô tả như sau.

- **Thủ tục sinh chữ ký tập thể cho nhiều nhóm ký trên M:**

Gồm các bước sau:

1. Mỗi GM của nhóm ký thứ j thực hiện:

- Tính tham số mặt nạ λ_{ji} cho những signer trong nhóm ký j theo công thức (3.10); λ_{ji} là của signer thứ i trong nhóm ký thứ j.
- Tính thành phần chia sẻ của nhóm ký U_j theo công thức:

$$U_j = \prod_{i=1}^{m_j} y_{ji}^{\lambda_{ji}} \ mod\ p \tag{3.23}$$

- Tính tham số ngẫu nhiên của nhóm ký R_j theo công thức:

$$R_j = {R'}_j \prod_{i=1}^{m_j} R_{ji} \ mod\ p \tag{3.24}$$

- Gửi giá trị U_j và R_j cho tất cả GM khác trong tập thể ký.

2. Một GM nào đó trong tập thể ký, hoặc tất cả, tính các giá trị U, R và E theo các công thức sau:

$$U = \prod_{j=1}^{g} U_j \ mod\ p \tag{3.25}$$

$$R = \prod_{j=1}^{g} R_j \ mod\ p \tag{3.26}$$

và

$$E = F_H(M \| R \| U) \ mod\ \delta \tag{3.27}$$

Trong đó, δ là một số nguyên tố lớn, có độ lớn: |δ| = 160 bit.

U và E là thành phần đầu tiên và thành phần thứ hai của chữ ký

tập thể.

3. GM của mỗi nhóm ký thứ j tiếp tục thực hiện:

- Tính thành phần chia sẻ S_j của nhóm ký:

$$S_j = S'_j \prod_{i=1}^{m_j} S_{ji} \ mod\ p \tag{3.28}$$

Trong đó, S_{ji} là chữ ký chia sẻ của cá nhân ký thứ i trong nhóm thứ j.

- Gửi S_{ji} cho tất cả GM khác trong tập thể ký.

4. Một GM nào đó trong tập thể ký, hoặc tất cả, thực hiện các công việc cuối cùng:

- Xác thực tính đúng của thành phần chia sẻ S_j của mỗi nhóm ký bằng công thức:

$$R_j = S_j^k (Y_j U_j)^{-E} \ mod\ p \tag{3.29}$$

- Nếu tất cả S_j đều thoả mãn công thức kiểm tra thì phần tử thứ ba S của chữ ký tập thể được tính theo công thức:

$$S = \prod_{j=1}^{g} S_j \ mod\ p \tag{3.30}$$

Vậy bộ ba giá trị (U, E, S) là chữ ký tập thể của một tập thể gồm g nhóm ký trên tài liệu M.

- **Thủ tục kiểm tra chữ ký tập thể của nhiều nhóm trên M:**

Để kiểm tra tính hợp lệ của chữ ký nhận được cùng với tài liệu M, bên kiểm tra (verifier) thực hiện các bước sau:

1. Tính public key tập thể Y_{col} theo công thức:

$$Y_{col} = \prod_{j=1}^{g} Y_j \ mod\ p = (\prod_{j=1}^{g} X_j)^k \ mod\ p \tag{3.31}$$

2. Tính giá trị R^* theo công thức:

$$R^* = S^k (U Y_{col})^{-E} \ mod\ p \tag{3.32}$$

3. Tính giá trị E^* theo công thức:

$$E^* = F_H(M \| R^* \| U) \tag{3.33}$$

4. So sánh E^* với E. Nếu $E^* = E$: Chữ ký nhận được là hợp lệ; Ngược lại chữ ký nhận được là không hợp lệ, nó bị từ chối.

- **Nhận xét:** Thành phần đầu tiên U của chữ ký tập thể chứa thông tin của tất cả thành viên nhóm cho mỗi nhóm ký trên văn bản

M. Lưu ý rằng thủ tục định danh cá nhân ký yêu cầu sự tham gia của các trưởng nhóm có chung chữ ký tập thể. Đồng thời, độ phức tạp tính toán của thủ tục này là tương đối cao và tăng nhanh chóng cùng với sự gia tăng số lượng của các nhóm ký có chung chữ ký tập thể.

3.1.4. Lược đồ chữ ký số tập thể cho nhiều nhóm ký và nhiều người ký cá nhân (Ký hiệu: RCS.02-3.1)

3.2. Xây dựng lược đồ chữ ký tập thể đại diện dựa trên bài toán tìm căn modulo số nguyên tố có cấu trúc $p = Nt_0t_1t_2 + 1$

Phần này trình bày về giao thức chữ ký số được xây dựng dựa trên độ khó của bài toán tìm căn modulo số nguyên tố lớn, với số nguyên tố có cấu trúc đặc biệt, được đề xuất bởi Nikolay A. Moldovyan và Victor A. Shcherbacov trong [73].

3.2.1. Lược đồ chữ ký cá nhân (Ký hiệu: SDS-3.2)

3.2.2. Lược đồ chữ ký tập thể (Ký hiệu: CDS-3.2)

3.2.3. Lược đồ chữ ký nhóm (Ký hiệu: GDS-3.2)

3.2.4. Lược đồ chữ ký số tập thể cho nhiều nhóm ký (Ký hiệu: RCS.01-3.2)

Phần này sử dụng hai lược đồ vừa mô tả ở trên làm cơ sở để xây dựng lược đồ chữ ký tập thể đại diện, dạng 1: Chữ ký tập thể cho nhiều nhóm ký. Lược đồ này cho phép tạo ra một chữ ký tập thể, trên tài liệu M, đại diện cho một tập thể ký có g nhóm ký, mỗi nhóm ký gồm m thành viên, được điều hành bởi người trưởng nhóm (GM).

Các tham số đầu vào, các public key, các private keyđược chọn, được tính như các lược đồ cơ sở ở trên.

Sau đây là các thủ tục của lược đồ:

- **Thủ tục sinh chữ ký trên tài liệu M**

1. Mỗi GM của nhóm ký thứ j thực hiện:

- Tính hệ số mặt nạ λ_{ji} cho những signer trong nhóm ký j theo công thức: $\lambda_i = F_H(H \| Y_i \| F_H(H \| Y_i \| K_1' \| K_2'))$ (3.76)

(λ_{ji} là hệ số mặt nạ của người ký thứ i trong nhóm ký thứ j)

- Tính giá trị thành phần U_j của nhóm ký thứ j theo công thức:

$$U_j = \prod_{i=1}^{m_j} Y_{ji}^{\lambda_{ji}} \ mod\ p \quad (3.77)$$

U_j được xem như là giá trị chia sẻ của nhóm ký thứ j trong thành phần đầu tiên của chữ ký tập thể cho các nhóm ký

- Tính thành phần ngẫu nhiên R_j theo công thức:

$$R_j = R'_j \prod_{i=1}^{m_j} R_{ji} \ mod\ p \quad (3.78)$$

- Gửi giá trị U_j và R_j cho tất cả GM khác trong tập thể ký.

2. Một GM nào đó trong tập thể ký, hoặc tất cả, tính giá trị các thành phần U, R và e của chữ ký tập thể theo các công thức sau:

$$U = \prod_{j=1}^{g} U_j \ mod\ p \quad (3.79)\ ;\ R = \prod_{j=1}^{g} R_j \ mod\ p \quad (3.80)$$

và $$e = F_H(M \| R \| U) \ mod\ \delta \quad (3.81)$$

Trong đó δ là một số nguyên tố lớn $|\delta| = 160$ bit.

U và e là thành phần đầu tiên và thành phần thứ hai của chữ ký.

3. Mỗi GM của nhóm thứ j tiếp tục thực hiện:

- Tính chữ ký chia sẻ S_{1_j}, S_{2_j} của nhóm ký thứ j theo công thức:

$$S_{1_j} = S'_{1_j} \prod_{i=1}^{m_j} S_{1_{ji}} \ mod\ p \quad (3.82a)$$

$$S_{2_j} = S'_{2_j} \prod_{i=1}^{m_j} S_{2_{ji}} \ mod\ p \quad (3.82b)$$

Với S_{ji} là chữ ký chia sẻ của cá nhân ký thứ i trong nhóm thứ j.

- Gửi S_{1_j}, S_{2_j} cho những GM khác trong tập thể ký.

4. Một GM nào đó trong tập thể ký, hoặc tất cả, thực hiện:

- Kiểm tra tính đúng của chữ ký chia sẻ S_{1_i}, S_{2_i} của tất cả nhóm ký trong tập thể ký bằng công thức:

$$R_j = \left(U_j Y'_j\right)^e S_{1_j}{}^{w_1} S_{2_j}{}^{w_2} \ mod\ p \quad (3.83)$$

- Nếu tất cả S_{1_i}, S_{2_i} đều thoả mãn. Tính thành phần thứ ba và thứ tư S_{1_i}, S_{2_i} của chữ ký tập thể theo các công thức:

$$S_1 = \prod_{j=1}^{g} S_{1_j} \ mod\ p \quad (3.84a)$$

$$S_2 = \prod_{j=1}^{g} S_{2_j} \ mod\ p \quad (3.84b)$$

Vậy bộ 4 (U, e, S_1, S_2) là chữ ký tập thể của nhiều nhóm ký trên

tài liệu M.

- **Thủ tục kiểm tra chữ ký tập thể cho nhiều nhóm ký trên M**

Để kiểm tra tính hợp lệ của chữ ký nhận được cùng với tài liệu M, bên kiểm tra (verifier) thực hiện các bước sau:

1. Tính public key tập thể của tập thể ký Y_{col} theo công thức:

$$Y_{col} = \prod_{j=1}^{g} Y_j' \ mod\ p \quad (3.85)$$

2. Tính giá trị thành phần ngẫu nhiên R^* theo công thức:

$$R^* = (UY_{col})^e {S_1}^{w_1} {S_2}^{w_2} \ mod\ p \quad (3.86)$$

3. Tính giá trị e^* theo công thức:

$$e^* = F_H(M \| R^* \| U) \quad (3.87)$$

4. So sánh e^* với e. Nếu $e^* = e$: Chữ ký nhận được là hợp lệ; Ngược lại, chữ ký nhận được là không hợp lệ, nó bị từ chối.

3.2.5. Lược đồ chữ ký số tập thể cho nhiều nhóm ký và nhiều người ký cá nhân (Ký hiệu: RCS.02-3.2)

3.3. Đánh giá khả năng bảo mật và hiệu năng tính toán của các lược đồ chữ ký tập thể đại diện đã được xây dựng

3.3.1. Các loại tấn công có thể vào lược đồ SDS-3.2:

3.3.2. Tính bảo mật của lược đồ chữ ký nhóm

3.3.3. Tính bảo mật của lược đồ chữ ký tập thể đại diện

3.3.4. Đánh giá hiệu năng tính toán của lược đồ chữ ký mới

Luận án đánh giá hiệu năng tính toán của các lược đồ chữ ký tập thể đại diện thông qua việc tính chi phí thời gian mà lược đồ cần cho quá trình sinh chữ ký (Thủ tục sinh chữ ký) và cần cho quá trình kiểm tra tính hợp lệ của chữ ký (Thủ tục kiểm tra chữ ký).

Bảng 3.1: Chi phí thời gian của các lược đồ RCS dựa trên bài toán FRM

Lược đồ	Chi phí thời gian	
	Sinh chữ ký	Kiểm tra chữ ký
RCS.01-3.1	$U = \sum_{j=1}^{g}(243m_j + 1)\,T_m$ $e = [\sum_{j=1}^{g}(241m_j + 240) + 1]T_m$	$(481 + g)T_m$

	$S = \sum_{j=1}^{g}(725m_j + 241)\,T_m$ $Sum = [\sum_{j=1}^{g}(1210m_j + 482) + 1]T_m$	
RCS.02-3.1	$U = \sum_{j=1}^{g}(243m_j + 1)\,T_m$ $e = [\sum_{j=1}^{g}(241m_j + 240) + 241m + 1]T_m$ $S = [\sum_{j=1}^{g}(725m_j + 241) + 723m]T_m$ $Sum = [\sum_{j=1}^{g}(1210m_j + 482) + 965m + 1]T_m$	$(481 + g + m)T_m$
RCS.01-3.2	$U = \sum_{j=1}^{g}(243m_j + 1)\,T_m$ $e = [\sum_{j=1}^{g}(481m_j + 481) + 1]T_m$ $S_1 + S_2 = \sum_{j=1}^{g}(1209m_j + 484)\,T_m$ $Sum = [\sum_{j=1}^{g}(1934m_j + 966) + 1]T_m$	$(724 + g)T_m$
RCS.02-3.2	$U = \sum_{j=1}^{g}(243m_j + 1)\,T_m$ $e = [\sum_{j=1}^{g}(481m_j + 481) + 481m + 1]T_m$ $S_1 + S_2 = [\sum_{j=1}^{g}(1209m_j + 484) + 1206m]T_m$ $Sum = [\sum_{j=1}^{g}(1934m_j + 966) + 1687m + 1]T_m$	$(724 + g + m)T_m$

Dữ liệu trong bảng này cho thấy, lược đồ chữ ký tập thể đại diện được xây dựng từ modulo có cấu trúc $p = Nk2 + 1$ có chi phí thấp hơn nhiều sao với cấu trúc p còn lại.

Kết luận Chương 3:

Trong chương này, luận án trình bày các lược đồ chữ ký tập thể được xây dựng dựa trên bài toán khai căn modulo số nguyên tố lớn,

với hai dạng cấu trúc khác nhau của modulo nguyên tố p: i) $p = Nt_0t_1t_2 + 1$ (với private key gồm hai thành phần); và ii) $p = Nk^2 + 1$ (với private key chỉ một thành phần). Với mỗi cấu trúc p, luận án xây dựng cả 2 dạng lược đồ: i) Chữ ký tập thể cho nhiều nhóm ký và ii) Chữ ký tập thể cho nhiều nhóm ký và nhiều cá nhân ký. Luận án cũng đã xây dựng các lược đồ chữ ký tập thể và các lược đồ chữ ký nhóm để làm lược đồ cơ sở cho các lược đồ chữ ký tập thể đại diện.

Những công bố của NCS được sử dụng trong chương này: [CT4], [CT7], [CT11].

CHƯƠNG 4:
CẢI THIỆN KÍCH THƯỚC VÀ MỨC ĐỘ AN TOÀN CỦA CHỮ KÝ TẬP THỂ ĐẠI DIỆN

Những lược đồ mà nghiên cứu sinh đã xây dựng vẫn còn tồn tại hai vấn đề cần xem xét để cải thiện: i) Giảm số thành phần của chữ ký từ ba xuống còn hai thành phần để giảm kích thước chữ ký và ii) Tăng mức độ an toàn của chữ ký bằng cách sử dụng đồng thời hai bài toán khó, thay vì sử dụng một bài toán khó, để xây dựng lược đồ. Hai vấn đề này sẽ được xem xét và đề xuất hướng giải quyết trong chương 4. Như vậy, chương 4 được xem như sự mở rộng và hoàn thiện của chương 2 và chương 3.

4.1. Vấn đề đặt ra và Hướng tiếp cận

Đã có nhiều hướng tiếp cận được đưa ra để có thể nâng cao chất lượng và khả năng triển khai vào thực tế của các chữ ký số và lược đồ chữ ký số, như tăng chiều dài khóa, giảm kích thước chữ ký, xây dựng bài toán khó mới – dựa vào các cấu trúc đại số trừu tượng đã có, xây dựng chữ ký dựa vào nhiều bài toán khó, sử dụng modulo nguyên tố có cấu trúc đặc biệt v.v.. Chương 4 này, NCS đề xuất: i) Dạng chữ ký tập thể đại diện hai thành phần và ii) Dạng chữ ký tập thể đại diện dựa trên đồng thời hai bài toán khó để cải thiện kích thước và nâng cao mức độ an toàn cho các lược đồ này.

4.2. Xây dựng lược đồ chữ ký tập thể đại diện hai thành phần dựa trên bài toán logarit rời rạc trên trường hữu hạn

4.2.1. Lược đồ chữ ký nhóm (Ký hiệu: GDS-4.2)

4.2.2. Lược đồ chữ ký số tập thể cho nhiều nhóm ký (Ký hiệu: RCS.01-4.2)

Lược đồ này tạo ra chữ ký tập thể cho g nhóm ký, với public key của mỗi người quản lý nhóm (GM), và cũng chính là public key của mỗi nhóm ký: $Y_j = X_j^k \ mod \ p$; với($j = 1, 2, \dots , \ g$), và X_j là private key của GM thứ j. Giả sử nhóm thứ j có m_j cá nhân ký. M là tài liệu

cần được ký trên đó. Giao thức của chữ ký tập thể cho các nhóm ký được mô tả như sau.

- **Thủ tục sinh chữ ký tập thể cho g nhóm ký trên M:**

Gồm các bước sau:

1. Mỗi nhóm thứ *j* sinh chữ ký nhóm theo như lược đồ cho nhóm ký GDS-4.2 ở trên và rồi gửi R_j cho tất cả các nhóm còn lại trong tập thể ký.

2. Một GM nào đó trong tập thể ký, hoặc tất cả, tính các giá trị R và E theo các công thức sau:

$$R = \prod_{j=1}^{g} R_j \ mod\ p \tag{4.17}$$

$$E = \ F_H(M \| R) \ mod\ 2^{128} \tag{4.18}$$

E là thành phần đầu tiên của chữ ký tập thể.

3. GM của mỗi nhóm ký thứ *j* tiếp tục thực hiện:

- Tính thành phần chia sẻ S_j của nhóm ký:

$$S_j = E\left(T_j + z_j E\right) mod\ q \tag{4.19}$$

- Gửi S_j cho tất cả GM khác trong tập thể ký.

4. Một GM nào đó trong tập thể ký, hoặc tất cả, thực hiện các công việc cuối cùng:

- Xác thực tính đúng của thành phần chia sẻ S_j của mỗi nhóm ký bằng công thức:

$$R^* = Y_j^{-E} \alpha^{E^{-1} S_j} \ mod\ p \tag{4.20}$$

- Nếu tất cả S_j đều thoả mãn công thức kiểm tra thì phần tử thứ ba S của chữ ký tập thể được tính theo công thức:

$$S = \sum_{j=1}^{g} S_j \ mod\ p \tag{4.21}$$

Vậy cặp giá trị (E, S) là chữ ký tập thể, hai thành phần, của một tập thể gồm g nhóm ký trên tài liệu M.

- **Thủ tục kiểm tra chữ ký tập thể cho g nhóm ký trên M:**

Để kiểm tra tính hợp lệ của chữ ký nhận được cùng với tài liệu M, bên kiểm tra (verifier) thực hiện các bước sau:

1. Tính public key tập thể Y_{col} theo công thức:

$$Y_{col} = \prod_{j=1}^{g} Y_j \ mod\ p \quad (4.22)$$

2. Tính giá trị R^* theo công thức:

$$R^* = Y_{col}^{-E} \alpha^{E^{-1}S} \ mod\ p \quad (4.23)$$

3. Tính giá trị E^* theo công thức:

$$E^* = F_H(M \| R^*) \ mod\ 2^{128} \quad (4.24)$$

4. So sánh E^* với E. Nếu $E^* = E$: Chữ ký nhận được là hợp lệ; Ngược lại chữ ký nhận được là không hợp lệ, nó bị từ chối.

4.2.3. Lược đồ chữ ký số tập thể cho nhiều nhóm ký và nhiều người ký cá nhân (Ký hiệu: RCS.02-4.2)

Giả sử có một tập thể ký gồm g nhóm ký và m người ký cá nhân, muốn tạo chữ ký tập thể đại diện lên tài liệu M. Giả sử nhóm ký thứ j gồm m thành viên ký (ký hiệu là m_j), đây là những người được chỉ định tham gia vào việc hình thành chữ ký nhóm của nhóm ký thứ j (j $= 1, 2, \ \ldots,$ g) và mỗi người ký cá nhân được xem như một nhóm ký mà chỉ có một thành viên duy nhất.

Các tham số đầu vào, private key, public key v.v. được chọn và tính như lược đồ RCS.01-4.2.

4.3. Xây dựng lược đồ chữ ký số tập thể đại diện dựa trên hai bài toán khó

Hai bài toán khó được chọn ở đây là: Bài toán logarit rời rạc trên trường hữu hạn nguyên tố $GF(p)$ và Bài toán phân tích thành thừa số. Sự kết hợp này được hình thành trên cơ sở: i) Modulo nguyên tố p được chọn với cấu trúc đặc biệt: $p = 2n + 1$, với $n = q'q;\ q'$ và q là số nguyên tố có độ lớn tối thiểu 512 bit (q' và q được chọn sao cho 3 không phải là ước của $q' - 1$ và $q - 1$) các số nguyên tố q' và q là các phần tử được giữ bí mật; và ii) Lược đồ chữ ký cá nhân được xây dựng theo lược đồ chữ ký của Schnorr.

4.3.1. Lược đồ chữ ký cá nhân (Ký hiệu: SDS-4.3)

4.3.2. Lược đồ chữ ký tập thể (Ký hiệu: CDS-4.3)

4.3.3. Lược đồ chữ ký nhóm (Ký hiệu: GDS-4.3)

4.3.4. Lược đồ chữ lý tập thể cho nhiều nhóm ký (Ký hiệu: RCS.01-4.3)

4.3.5. Lược đồ chữ ký tập thể cho nhiều nhóm ký và nhiều người ký cá nhân (Ký hiệu: RCS.02-4.3)

Trong cơ sở của giao thức chữ ký nhóm được mô tả ở trên và lược đồ chữ ký tập thể cho các nhóm ký, phần này xây dựng lược đồ chữ ký tập thể, của một tập thể gồm nhiều nhóm ký và nhiều người ký cá nhân, trên tài liệu M.

Tập thể ký trong trường hợp này gồm g nhóm ký và m người ký cá nhân. Các giá trị tham số đầu vào và các giá trị khóa của trưởng nhóm (GM) của thành viên nhóm được chọn/tính như trên. Private key và public key của người ký cá nhân lần lượt là: X_j và Y_j. $Y_j = \alpha^{X_j} \, mod \, p$; $(j = g + 1, g + 2, \dots, g + m)$.

4.4. Đánh giá mức độ bảo mật và hiệu năng tính toán của lược đồ chữ ký tập thể đại diện được xây dựng

4.4.1. Độ bảo mật của lược đồ chữ ký cơ sở

Mức độ bảo mật của lược đồ mới này phụ thuộc vào độ khó của việc giải đồng thời hai bài toán khó: Bài toán logarit rời rạc trên $GF(p)$ và Bài toán phân tích thành thừa số nguyên tố của một số nguyên lớn. Tức là, để phá vỡ được lược đồ này kẻ tấn công trước hết phải giải được bài toán logarit rời rạc, sau đó phải giải được bài toán phân tích thừa số (xem ở mục 4.3.1).

4.4.2. Độ bảo mật của lược đồ chữ ký nhóm

Với lược đồ chữ ký nhóm, tồn tại hai dạng tấn công chủ yếu: Tấn công nội bộ (từ chính những thành viên của nhóm ký) và Tấn công từ bên ngoài (từ những người không phải là thành viên nhóm ký). Một cách hình thức, lược đồ chữ ký nhóm dễ bị tấn công từ bên trong hơn so với tấn công từ bên ngoài. Vì, kẻ tấn công bên ngoài chỉ biết được các tham số hệ thống, các public key và tài liệu M, trong khi đó, kẻ tấn công từ nội bộ, vì là thành viên của nhóm

ký nên có nhiều hơn thông tin liên quan đến mục tiêu tấn công.

Phần sau đây xem xét hai dạng tấn công phổ biến vào lược đồ chữ ký nhóm, nó xuất phát từ người trưởng nhóm, nên khả năng thành công là rất cao.

4.4.3. Độ bảo mật của lược đồ chữ ký tập thể đại diện

Lược đồ chữ ký sô tập thể đại diện được xây dựng trên cơ sở của lược đồ chữ ký số tập thể và lược đồ chữ ký số nhóm nên nó thừa hưởng tất cả ưu điểm bảo mật từ hai lược đồ cơ sở này

4.4.4. Đánh giá hiệu năng tính toán của các lược đồ chữ ký tập thể đại diện

Luận án đánh giá hiệu năng tính toán của các lược đồ chữ ký tập thể đại diện thông qua việc tính chi phí thời gian mà lược đồ cần cho quá trình sinh chữ ký (Thủ tục sinh chữ ký) và cần cho quá trình kiểm tra tính hợp lệ của chữ ký (Thủ tục kiểm tra chữ ký).

Bảng 4.1: Chi phí thời gian của các lược đồ RCS hai thành phần

Lược đồ	Chí phí thời gian	
	Sinh chữ ký	Kiểm tra chữ ký
RCS.01-4.2	$E = [\sum_{j=1}^{g}(244m_j + 1204) + 1]T_m$ $S = (724g)T_m$ $Sum = [\sum_{j=1}^{g}(244m_j + 1928) + 1]T_m$	$(723 + g)T_m$
RCS.02-4.2	$E = [\sum_{j=1}^{g}(244m_j + 1204) + 241m + 1]T_m$ $S = (724g + 724m)T_m$ $Sum = [\sum_{j=1}^{g}(244m_j + 1928) + 965m + 1]T_m$	$(723 + g + m)T_m$

Bảng 4.2: Chi phí thời gian của các lược đồ RCS trên hai bài toán khó

Lược đồ	Chí phí thời gian	
	Sinh chữ ký	Kiểm tra chữ ký
RCS.01-4.4	$U = \sum_{j=1}^{g}(243m_j + 1)\,T_m$ $e = [\sum_{j=1}^{g}(241m_j + 240) + 1]T_m$ $S = [\sum_{j=1}^{g}(1254m_j + 1781) + 290]T_m$ $Sum = [\sum_{j=1}^{g}(1738m_j + 2022) + 291]T_m$	$(723 + g)T_m$
RCS.02-4.4	$U = \sum_{j=1}^{g}(243m_j + 1)\,T_m$ $e = [\sum_{j=1}^{g}(241m_j + 240) + 241m + 1]T_m$ $S = [\sum_{j=1}^{g}(1254m_j + 1781) + 1250m + 290]T_m$ $Sum = [\sum_{j=1}^{g}(1738m_j + 2022) + 1491m + 292]T_m$	$(723 + g + m)T_m$

** Ký hiệu sử dụng trong bảng này đã được quy ước ở Chương 2.*

Dữ liệu từ bảng này cho thấy, giảm khá nhiều chi phí thời gian cho cả sinh chữ ký và kiểm tra chữ ký, so với các chữ ký cùng loại ba thành phần. Bảng này cũng cho thấy, với lược đồ chữ ký tập thể đại diện trên hai bài toán khó, chúng ta phải chấp nhận chi phí thời gian cho việc sinh chữ ký và kiểm tra chữ ký là khá cao để đổi lấy mức độ an toàn cao từ cả hai bài toán khó, logarit rời rạc và phân tích thành nhân tử.

Kết luận Chương 4:

Chương này đã đề xuất và xây dựng được hai lược đồ chữ ký tập thể đại diện hai thành phần (E, S) và hai lược đồ chữ ký tập thể đại diện dựa trên hai bài toán khó, logarit rời rạc và khai căn, với modulo p có cấu trúc đặc biệt $p = 2n + 1$. Tất cả lược đồ đều được chứng minh tính đúng và đánh giá hiệu năng. Việc loại bỏ

thành phần U khỏi chữ ký, kéo theo giảm được kích thước của chữ ký và làm cho chi phí thời gian cho cả quá trình sinh chữ ký và quá trình kiểm tra chữ ký giảm một cách đáng kể.

Những công bố của NCS được sử dụng trong chương này: [CT1], [CT6], [CT8], [CT10], [CT12].

KẾT LUẬN

Qua quá trình thực hiện đề tài "*Nghiên cứu và Xây dựng lược đồ chữ ký số tập thể đại diện*", luận án có được những kết quả và những đóng góp sau đây:

1. Kết quả đạt được của luận án

- Đã đề xuất được hai dạng lược đồ chữ ký số tập thể đại diện, có tính thực tế cao: i) Chữ ký số tập thể cho các nhóm ký và ii) Chữ ký số tập thể cho các nhóm ký và các cá nhân ký.
- Đã xây dựng được bốn lược đồ chữ ký số tập thể đại diện dựa trên các bài toán logarit rời rạc: Trên trường nguyên tố hữu hạn (hai lược đồ); Trên đường cong Elliptic sử dụng chuẩn ECDSA (hai lược đồ).
- Xây dựng được bốn lược đồ chữ ký số tập thể đại diện dựa trên bài toán khó mới, tìm căn modulo số nguyên tố lớn, với các modulo nguyên tố có cấu trúc đặc biệt khác nhau: $p = Nt_0t_1t_2 + 1$ (hai lược đồ) và $p = Nk^2 + 1$ (hai lược đồ).
- Đề xuất được bốn lược đồ chữ ký số tập thể đại diện hai thành phần dựa trên các bài toán logarit rời rạc: Trên trường nguyên tố hữu hạn (hai lược đồ); Trên đường trên đường cong Elliptic sử dụng chuẩn GOST R34.10-2012 (hai lược đồ).
- Đề xuất được hai lược đồ chữ ký tập thể đại diện dựa trên đồng thời hai bài toán khó: Bài toán phân tích thành nhân tử và Bài toán logarit rời rạc trên trường hữu hạn nguyên tố, sử dụng Schnorr.

2. Đóng góp khoa học của luận án

Những đóng góp khoa học của luận án bao gồm:

Phát hiện và lược đồ hóa được hai yêu cầu chứng thực dựa vào chữ ký khá phổ biến trong thực tế hiện nay. Đó là: i) Chứng thực được thực hiện cho nhiều nhóm thành viên khác nhau, mỗi nhóm gồm nhiều thành viên, trong đó một người đóng vai trò trưởng nhóm

và ii) Chứng thực được thực hiện cho nhiều nhóm thành viên và nhiều thành viên đơn lẻ khác nhau.

Từ đó đề xuất được một loại chữ ký tập thể mới - "chữ ký tập thể đại diện" - có tính thực tế và cấp thiết cao. Có hai dạng lược đồ chữ ký tập thể đại diện: i) Lược đồ chữ ký số tập thể cho các nhóm ký và ii) Lược đồ chữ ký số tập thể cho các nhóm ký và các cá nhân ký.

3. Hướng phát triển tiếp theo của đề tài

Trong tương lai, NCS sẽ tiếp tục nghiên cứu và phát triển luận án theo các hướng cụ thể sau đây:

- Trong thời gian tới, NCS tiếp tục nghiên cứu để so sánh cấp độ bảo mật và hiệu năng tính toán của các lược đồ được đề xuất trong luận án với các lược đồ tương tự đã/sẽ được công bố.
- Trong tương lai, NCS cố gắng xây dựng lược đồ chữ ký số tập thể đại trên cơ sở bài toán khó hay giao thức chữ ký số do chính NCS phát triển.
- Triển khai các ứng dụng xác thực, chứng thực dựa trên chữ ký tập thể đại diện trên hạ tầng PKI hiện có. Điều này không những giúp giảm chi phí xây dựng hạ tầng mà còn giúp một cá nhân chỉ sở hữu một cặp khóa Private key và Public key nhưng có thể sử dụng đồng thời cho các yêu cầu chứng thực khác nhau, tính bí mật và tính riêng tư trong trường hợp này vẫn đảm bảo. Qua quá trình nghiên cứu về chữ ký số tập thể đại diện, với những kết quả đạt được cho đến thời điểm hiện tại, NCS có đầy đủ cở sở để tin rằng những hướng nghiên cứu tiếp theo cũng sẽ mang đến những kết quả khả quan.

CÁC CÔNG TRÌNH ĐÃ CÔNG BỐ

[CT1] **Nguyen Kim Tuan**, Ho Ngoc Duy, "*Xây dựng sơ đồ chữ ký tập thể mù trên cơ sở hệ mật Schnorr",* Journal of Science & Technology of Duy Tan University, 2015.

[CT2] **N. K. Tuan**, V. L. Van, N. A. Moldovyan and H. N. Duy, A. A. Moldovyan, "*Collective signature protocols for signing groups",* Information Systems Design and Intelligent Applications. Advances in Intelligent Systems and Computing (Scopus), INDIA, pp.78-87, 2017.

[CT3] **N. K. Tuan**, N. A Moldovyan, H. N Duy, T. T. V. Lam, V. L. Van*, "New protocols of collective digital signature based on Elliptic curve",* Hội thảo quốc gia: Một số vấn đề chọn lọc của Công nghệ thông tin và truyền thông - Chủ đề: An ninh không gian mạng, Quy Nhơn, pp.57-67, 2018.

[CT4] **Tuan Nguyen Kim**, Duy Ho Ngoc, Nikolay A. Moldovyan, *"Constructing the 2-element AGDS protocol based on the discrete logarithm problem",* International Journal of Network Security & Its Applications, vol.13, no.4, pp.13-22, 2021.

[CT5] **Tuan Nguyen Kim**, Duy Ho Ngoc, Nikolay A. Moldovyan, *"Collective signature protocols for signing groups based on problem of finding roots modulo large prime number",* International Journal of Network Security & Its Applications, vol.13, no.4, pp.59-69, 2021.

[CT6] **Tuan Nguyen Kim**, Nguyen Tran Truong Thien, Duy Ho Ngoc, Nikolay A. Moldovyan. *"Constructing New Collective Signature Schemes Based on Two Hard Problems Factoring and Discrete Logarithm"*, International Journal of Computer Networks & Communications, vol.14, no.2, pp.115-133, 2022 (Scopus).

[CT7] **Tuan Nguyen Kim**, Duy Ho Ngoc, Nikolay A. Moldovyan, "*New Collective Signature Protocols Based on The Elliptic Curve Discrete Logarithm Problem*", Computers, Materials & Continua, vol.73, no.1, pp.595-610, 2021 (SCI/Q2).

[CT8] **Tuan Nguyen Kim**, Duy Ho Ngoc, Nikolay A.

Moldovyan, "*New Representative Collective Signature Schemes Based on The Discrete Logarithm Problem*", Computers, Materials & Continua, vol.73, no.1, pp.783-799, 2021 (SCI/Q2).
[CT9] **Tuan Nguyen Kim**, Duy Ho Ngoc, Nikolay A. Moldovyan, "*Constructing Collective Signature Schemes Using Problem of Finding Roots Modulo",* Computers, Materials & Continua, vol.72, no.1, pp.1105-1122, 02/2022 (SCI/Q2).
[CT10] **Tuan Nguyen Kim**, Duy Ho Ngoc, Nikolay A. Moldovyan, *"Constructing New Representative Collective Signature Using The GOST R34.10-2012 Digital Signature Standard"***,** Journal of Communication, vol.17, n0.6, pp.478-485, 06/2022 (SCI/Q3).
[CT11] Tuan Nguyen Kim, Duy Ho Ngoc, Nin Ho Le Viet, Nikolay A. Moldovyan, *"The New Collective Signature Schemes Based on Two Hard Problems Using Schnorr's Signature Standard"*, Journal of Advances in Information Technology, vol.14, no.1,pp.77-84, 2022 (SCI/Q3).
[CT12] **Tuan Nguyen Kim**, Duy Ho Ngoc, Nikolay A. Moldovyan, *"Constructing Representative Collective Signature Protocols Using The GOST R34.10-1994 Standard",* Computers, Materials & Continua, vol.74, no.6, pp.1475-1491, 2022 (SCI/Q2).