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

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

LỜI CAM ĐOAN

Tôi xin cam đoan đây là công trình nghiên cứu do tôi thực hiện theo sự hướng dẫn khoa học của TS. Hồ Ngọc Duy và PGS.TS. Đoàn Văn Ban. Các số liệu và kết quả trình bày trong luận án này là trung thực, chưa được công bố bởi bất kỳ tác giả nào hay ở bất kỳ công trình nào khác.

Đại diện tập thể CBHD	**Nghiên cứu sinh**
TS. Hồ Ngọc Duy	**Nguyễn Kim Tuấn**

LỜI CẢM ƠN

Đầu tiên, tôi xin được bày tỏ lời cảm ơn kính trọng nhất đến quý Thầy hướng dẫn, thầy TS. Hồ Ngọc Duy và thầy PGS.TS. Đoàn Văn Ban. Nhờ sự chỉ bảo tận tình và đôn đốc liên tục của quý Thầy mà tôi mới có được một luận án như mong muốn ngày hôm nay. Tôi luôn biết ơn quý Thầy về điều này.

Tôi xin được gửi lời cảm ơn chân thành đến quý cấp lãnh đạo trường Đại học Duy Tân đã hỗ trợ mọi mặt để tôi hoàn thành khóa học. Quý lãnh đạo và quý đồng nghiệp ở trường Khoa học máy tính – Đại học Duy Tân – cũng đã hỗ trợ tôi rất nhiều trong quá trình học tập và thực hiện đề tài, tôi xin cảm ơn tất cả mọi người.

Cảm ơn những sinh viên và đồng nghiệp của tôi tại Phòng Thực nghiệm An ninh mạng – Đại học Duy Tân – đã hỗ trợ tôi rất nhiều trong quá trình hoàn thiện luận án này.

Trân trọng.

Nghiên cứu sinh

Nguyễn Kim Tuấn

MỤC LỤC

DANH MỤC CÁC TỪ VIẾT TẮT

Từ viết tắt	Nghĩa tiếng Anh	Nghĩa tiếng Việt
CDS	Collective Digital Scheme	Lược đồ chữ ký số tập thể
DLP	Discrete Logarithm Problem	Bài toán logarit rời rạc
DS	Digital Signature	Chữ ký số (đơn)
DSA	Digital Signature Algorithm	Thuật toán chữ ký số
DSS	Digital Signature Standard	Chuẩn chữ ký số
EC	Elliptic Curve	Đường cong Elliptic
ECC	Elliptic Curve Cryptography	Mật mã trên đường cong Elliptic
ECDLP	Elliptic Curve Discrete Logarithm Problem	Bài toán logarit rời rạc trên đường cong Elliptic
ECDSA	Elliptic Curve Digital Signature Algorithm	Thuật toán chữ ký số dựa trên đường cong Elliptic
FRMP	Problem of Finding Root Modulo	Bài toán tìm căn mo-du-lo
GDS	Group Digital Scheme	Lược đồ chữ ký số nhóm
GM	Group Manager	Người quản lý nhóm
GOST	GOvement STandard	Chuẩn chữ ký số chính phủ (Nga)
IFP	Integer Factorization Problem	Bài toán phân tích thừa số nguyên tố
PKI	Public key Instructure	Hạ tầng khóa công khai
RCS	Representative Collective Signature	Chữ ký tập thể đại diện
RSA	Rivest - Shamir - Adleman	Hệ mật mã bất đối xứng RSA

DANH MỤC CÁC HÌNH VẼ

DANH MỤC CÁC KÝ HIỆU

Ký hiệu	Ý nghĩa ký hiệu
"||"	Toán tử nối xâu
$\emptyset(n)$	Hàm phi Euler của n
$H(M)$	Giá trị băm của
Z_p^*	Nhóm nhân hữu hạn
$\{0,1\}^*$	Ký hiệu chuỗi bít có độ dài bất kỳ
$\{0,1\}^k$	Ký hiệu chuỗi bít có độ dài k

DANH MỤC CÁC BẢNG

MỞ ĐẦU

1. Tính cấp thiết và lý do chọn đề tài

Chúng ta đều biết, Internet mang lại rất nhiều lợi ích cho cộng đồng, nhưng đồng thời Internet cũng tiềm ẩn không ít rủi ro khi trao đổi thông tin dựa trên nó. Trên không gian mạng nói chung và Internet nói riêng, người dùng có thể nhận được thông tin từ một nguồn cung cấp chưa được chứng thực hoặc từ một đối tác truyền thông giả mạo. Ngoài ra, thông tin cũng có thể bị đánh cắp, bị nghe lén, hoặc bị làm thay đổi nội dung khi nó di chuyển trên không gian mạng. Nếu những điều này xảy ra thì nguy cơ mất an toàn, an ninh thông tin, của cá nhân người dùng và của toàn hệ thống, là rất lớn. Đây là vấn đề mà các người nghiên cứu an toàn thông tin và an ninh mạng rất quan tâm, họ muốn tạo ra một không gian mạng an toàn, tin cậy và hiệu quả hơn.

Để đảm bảo an toàn cho các giao dịch trên không gian mạng người ta thường sử dụng các hệ thống chứng thực, xác thực dựa trên chữ ký số. Chữ ký số (Digital signature) không những hỗ trợ *"xác thực"* (Authentication) nguồn gốc thông tin mà còn giúp kiểm tra tính *"toàn vẹn"* (Integrity) của thông tin khi nó được truyền đi từ nguồn đến đích. Ngoài ra, chữ ký số còn giúp chống lại sự *"chối bỏ trách nhiệm"* (Non-repudiation) của một đối tác truyền thông. Chữ ký số được xây dựng dựa trên nguyên lý hoạt động của các hệ mật mã bất đối xứng và tính khó giải của các bài toán khó nên tốc độ thực hiện và mức độ an toàn của nó là có thể được kiểm chứng và tin dùng.

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 số tập thể, lược đồ chữ ký số tập thể mù, v.v. Chữ ký số đơn, dù có nhiều ưu điểm, nhưng nó chỉ phù hợp cho việc xác thực các thực thể có tính đơn lẻ, độc lập, nó khó có thể đáp ứng yêu cầu xác thực của nhiều ứng dụng trao đổi thông tin có tính tập thể, cần mức độ tin cậy cao, thực tế hiện nay trên không gian mạng. 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 (Algorithm),

giao thức (Protocol), lược đồ (Scheme) liên quan đến chữ ký số nhóm và chữ ký số tập thể đã được nghiên cứu và công bố, đáp ứng tốt yêu cầu xác thực của hai bài toán thực tế kể trên. Tất cả các giao thức, các lược đồ này 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 số 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. Tập thể này gồm nhiều nhóm thành viên, mỗi nhóm thành viên gồm nhiều thành viên, được quản lý bởi một người trưởng nhóm. Ngoài ra, tập thể này có thể có thêm một số thành viên đơn lẻ, họ không thuộc nhóm thành viên nào cả, nhưng họ được xem như ngang cấp chức năng với những người trưởng nhóm. 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.. Vậy để chứng thực cho tập thể này thì bên chứng thực phải tiến hành kiểm tra tính hợp lệ của chữ ký của tất cả thành viên trong tập thể ký. Đối với thành viên nhóm, cần phải biết được họ thuộc nhóm nào, ai là nhóm trưởng của họ. Đối với trưởng nhóm, cần phải biết được họ là trưởng nhóm nào, nhóm này có thuộc tập thể đang xét hay không. Đối với thành viên đơn lẻ, phải biết được họ có là thành viên của tập thể ký hay không. Rõ ràng, công việc này là khá tốn thời gian và khá phức tạp với với bên chứng thực. Thời gian và độ phức tạp này sẽ tăng lên một cách đáng kể khi số lượng thành viên của tập thể ký tăng lên. Cũng theo cách này, vai trò của người trưởng nhóm có thể đã bị bỏ qua.

Khó khăn trong việc đáp ứng mô hình chứng thực vừa nêu là đã rõ, nhưng đây lại là vấn đề rất thực tế và cấp thiết - ngày càng nhiều ứng dụng giao dịch điện tử (e-Transactions), như thương mại (e-Commerce), ngân hàng (e-Bank), thanh toán điện tử (e-Pay), hành chính (e-Government) cần chứng thực cho nhiều nhóm thành viên khác nhau, với các cấp chức năng khác nhau, trong một tập thể, nên hiện có nhiều hướng nghiên cứu tập trung giải quyết vấn đề này. Một trong số đó là tìm cách tạo ra một chữ ký duy nhất, với sự tham gia của tất cả thành viên, có kích thước không phụ thuộc vào số lượng thành viên và nhóm thành viên, nhưng có thể đại diện cho một tập thể nhiều người ký. Khi đó, bên chứng thực chỉ cần

kiểm tra tính hợp lệ của duy nhất một chữ ký, nhưng nếu cần có thể kiểm tra được nhiều thông tin liên quan, nên sẽ đơn giản và hiệu quả hơn nhiều.

Như chúng ta đã biết, lược đồ chữ ký số nhóm và lược đồ chữ ký số tập thể đều có thể tạo ra một chữ ký duy nhất cho một tập thể nhiều người ký, nhưng nó khó có thể đáp ứng yêu cầu chứng thực mới đã nêu ở trên, vì chữ ký số nhóm chỉ có thể hỗ trợ tạo ra chữ ký chung cho các nhóm thành viên, trong khi đó, chữ ký số tập thể chỉ có thể hỗ trợ tạo ra chữ ký chung cho các trưởng nhóm và các thành viên đơn lẻ hoặc chung cho tất cả thành viên của tập thể. Vì vậy, theo nghiên cứu sinh, nếu kết hợp được nguyên lý hoạt động của lược đồ chữ ký số nhóm và lược đồ chữ ký số tập thể thì chúng ta có thể xây dựng được một dạng lược đồ chữ ký số đa người ký đáp ứng được yêu cầu chứng thực tập thể của bài toán đặt ra ở trên.

Cụ thể, đầu tiên, sử dụng lược đồ chữ ký số nhóm để tạo chữ ký số nhóm cho các nhóm thành viên trong tập thể, sau đó, sử dụng lược đồ chữ ký số tập thể để tạo ra chữ ký số 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 số 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 số tập thể, có thể đặt tên cho dạng chữ ký đa người ký mới này là "Chữ ký số tập thể đại diện".

Về bản chất thì chữ ký số tập thể đại diện vẫn là chữ ký số tập thể, nhưng thành viên của tập thể ký này là những người đại diện cho các nhóm người ký khác nhau và có thể gồm thêm một số người ký cá nhân mà họ có chức năng tương đương với những người trưởng nhóm trong tập thể ký này. Lược đồ chữ ký số tập thể mới này cũng phải đảm bảo các yêu cầu độ lớn của chữ ký số, về các thành phần của chữ ký số, về mức độ an toàn về hiệu năng tính toán như các lược đồ chữ ký số khác thì mới được thực tế công nhận và tin dùng.

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 số 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

Đối tượng nghiên cứu của luận án là:

- Hệ mật mã bất đối xứng và ứng dụng của nó trong lĩnh vực an toàn thông tin. Cơ sở toán học để xây dựng các hệ mật mã bất đối xứng. Các thuật toán và các giao thức chữ ký số được xây dựng dựa trên hệ mật mã bất đối xứng.
- Các chuẩn chữ ký số, các giao thức/lược đồ chữ ký số chuẩn, các chuẩn đánh giá mức độ an toàn của một chữ ký số và lược đồ chữ ký số.
- Các quy định của nhà nước về xác nhận, định danh, xác thực một cá nhân, một tổ chức thông qua chữ ký và/hoặc con dấu, được ký, được đóng dấu, trên văn bản, trên tài liệu mà họ phát hành.
- Các hệ thống xác thực dựa trên chữ ký số hoạt động trên PKI.

Phạm vi nghiên cứu của luận án là:

- Các thuật toán mã hóa bất đối xứng và ứng dụng của nó: RSA, ElGamal; Số học modulo; Số nguyên tố lớn; Lý thuyết nhóm trong đại số trừu tượng.
- Các bài toán khó được sử dụng trong xây dựng giao thức/lược đồ chữ ký số: Phân tích thành thừa số; Logarit rời rạc; Tìm căn modulo số nguyên tố.
- Các chuẩn chữ ký số: DSA, RSA, ElGamal và Schnorr; Các chuẩn đánh giá mức độ an toàn của một lược đồ chữ ký số; Và các kiểu tấn công vào các lược đồ chữ ký số: Tấn công private key; Tấn công Signature forgery; v.v..
- Thuật toán, lược đồ, yêu cầu bảo mật và hiệu năng liên quan đến 3 loại chữ ký số: Chữ ký số đơn, chữ ký số nhóm, chữ ký số tập thể, chữ ký số tập thể mù. Các công bố gần đây về 3 loại chữ ký số này.

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 số 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 số nguyên tố lớn trên trường Z_p.

- 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 (của các nhà nghiên cứu trong và ngoài nước).

- 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 xây dựng chữ ký số: i) Các hệ mật mã bất đối xứng, các thuật toán xử lý số nguyên tố lớn, v.v.; Và ii) Bài toán khó phân tích thừa số, bài toán khó Logarit rời rạc; v.v..

- Tiếp đến, nghiên cứu về việc sử dụng bài toán khó để xây dựng lược đồ chữ ký số: 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 số.
- Cuối cùng, áp dụng công cụ toán học và quy trình đã được xác định để xây dựng lược đồ chữ ký số cho lược đồ chữ ký số đã chọn.

5. Nội dung nghiên cứu

Nội dung nghiên cứu chính của luận án sẽ tập trung vào các phần sau:

Nghiên cứu tổng quan:

- Về cơ sở toán học: Mật mã bất đối xứng; Số nguyên tố lớn; Toán học modulo; Toán học trừu tượng; Đường cong Elliptic; Các bài toán khó; v.v..
- Các chuẩn chữ ký số; Các lược đồ chữ ký số chuẩn; Các dạng tấn công và chữ ký số và lược đồ chữ ký số; Các loại lược đồ chữ ký số v.v..
- Về tình hình nghiên cứu về chữ ký số trong và ngoài nước: Chữ ký số đơn; Chữ ký số nhóm; Chữ ký số tập thể; Chữ ký trên một bài toán khó v.v..
- Về tình hình và khả năng ứng dụng chữ ký số trong việc đảm bảo an toàn cho các ứng dụng giao dịch điện tử, tài liệu điện tử.

Nghiên cứu của nghiên cứu sinh:

- Nghiên cứu về ưu điểm, nhược điểm của các lược đồ chữ ký số đã công bố, đặc biệt là về chữ ký số nhóm và chữ ký số tập thể.
- 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 số 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 đã hệ thống lại được các vấn đề liên quan đến chữ ký số và lược đồ chữ ký số. Đặc biệt nó cho thấy khả năng ứng dụng của toán học modulo, của vấn đề số nguyên tố lớn, của các bài toán khó, v.v. trong việc xây dựng các giao thức chữ ký số có mức độ aan toàn cao.

- 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 số nhóm, các lược đồ chữ ký số 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 số 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

Bố cục của luận án là như sau: Ngoài phần Mở đầu và phần Kết luận, phần nội dung chính của luận án được trình bày theo 4 chương:

- **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 1. 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 số tập thể với chữ ký số 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.

Như vậy, NCS dành riêng chương 2 để xây dựng các lược đồ đề xuất dựa trên bài toán khó sẵn có: Bài toán logarit rời rạc.

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

Bài toán tìm căn modulo số nguyên tố lớn là bài toán khó mới, do giáo sư Nikolay A. Moldovyan đề xuất, có một số ưu điểm về bảo mật so với các bài toán khó sẵn có, nó cho phép sử dụng khóa bí mật với hai thành phần. Do đó, luận án dành riêng chương này để chứng tỏ các lược đồ chữ ký số tập thể đại diện do NCS đề xuất hoàn toàn có thể được xây dựng trên bài toán khó mới.

- **Chương 4 – Cải thiện kích thước và mức độ an toàn của chữ ký số tập thể đại diện:** Các chữ ký số 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 4 cũng cho thấy chữ ký số tập thể đại diện hoàn toàn có thể xây dựng dựa trên hai bài toán khó: Bài toán logarit rời rạc và Bài toán phân tích thừa số. Như vậy, chương này có thể xem như sự mở rộng của chương 2 và chương 3 và cũng là sự "kết lại" của luận án này.

CHƯƠNG 1:

TỔNG QUAN VỀ CHỮ KÝ SỐ VÀ 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 số mới thì mới đáp ứng được, đó là, chữ ký số tập thể đại diện. Tính thực tế và cấp thiết của loại chữ ký số 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 số nói chung và lược đồ chữ ký số tập thể đại diện nói riêng.

1.1. Chữ ký số và Lược đồ chữ ký số

1.1.1. Chữ ký số

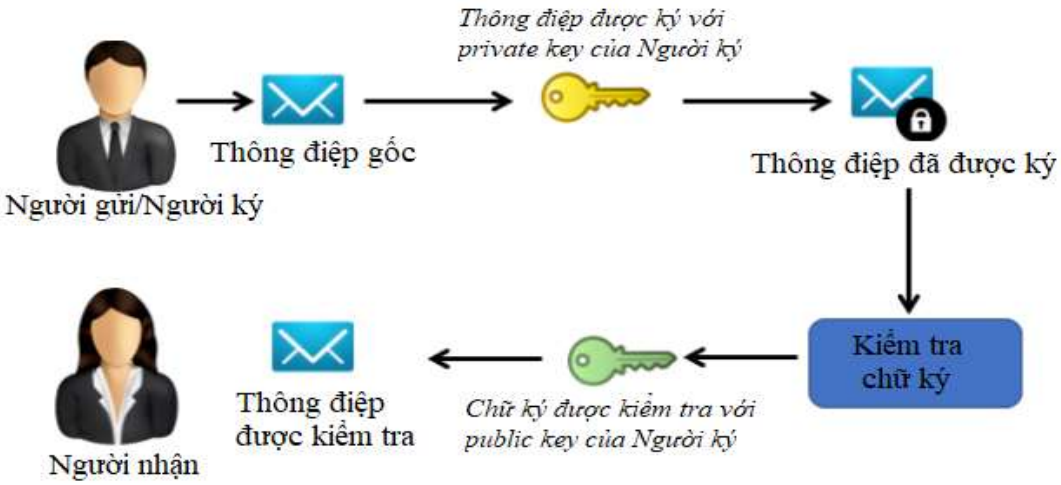
Chữ ký số (Digital signature: DS) là một mẫu thông tin ở dạng mã hóa, được gắn lên một tài liệu số. Nó được hình thành dựa trên nguyên lý hoạt động của hệ mật mã bất đối xứng [1-2], [10]. Để tạo ra một chữ số trên tài liệu số thì, trước tiên, người ký (signer) phải sở hữu một cặp khóa (key), khóa công khai (public key) và khóa riêng/khóa bí mật (secret key/private key). Sau đó, signer dùng private key của mình để tạo ra chữ ký số trên một tài liệu số. Và rồi, người kiểm tra (verifier) sẽ sử dụng public key của signer để kiểm tra tính hợp lệ của chữ ký số trên tài liệu số đã được ký bởi signer.

Chữ ký số được sử dụng cho ba mục đích:

- Xác thực (Authentication)**:** Chữ ký số giúp người nhận tin rằng, tài liệu mà họ nhận được là được tạo và được gửi đi từ một người gửi đã được chứng thực về mặt danh tính và nguồn gốc.
- Kiểm tra sự toàn vẹn (Integrity): Chữ ký số giúp đảm bảo rằng, tài liệu mà người nhận nhận được là không bị thay đổi so với bản gốc trong quá trình nó di chuyển trên đường truyền (từ bên gửi đến bên nhận).

- Chống lại sự chối bỏ trách nhiệm (Non-repudiation): Với chữ ký số, một ai đó khi đã ký lên một tài liệu thì không thể phủ nhận rằng họ không phải là tác giả của chữ ký đó.

Quá trình tạo chữ ký số trên thông điệp và kiểm tra tính hợp lệ của một chữ ký số đã tạo trên thông điệp được minh họa của hình 1.1 sau đây:



Hình 1.1. Sơ đồ tạo và kiểm tra chữ ký số trên một thông điệp số

Ý tưởng về lược đồ chữ ký số, hay lược đồ chữ ký số, lần đầu tiên được mô tả bởi Whitfield Diffie and Martin Hellman vào năm 1976. Đến năm 1977 thì lược đồ chữ ký số đầu tiên được xây dựng, đó là lược đồ chữ ký số dựa trên thuật toán mật mã bất đối xứng RSA.

Hiện tại đã có nhiều loại chữ ký số được nghiên cứu và ứng dụng, như chữ ký số đơn [33], [41], [51], đa chữ ký số [52], [62], [87], chữ ký số mù [15-17], [19], [26-28], [36], [79], chữ ký số nhóm [20-21], chữ ký số tập thể v.v..

1.1.2. Lược đồ chữ ký số

Lược đồ chữ ký số (Digital signature scheme: DSS) là một bộ gồm 3 thủ tục (procedure), mô tả về các bước thực hiện trong quá trình chứng thực một tài liệu số dựa trên chữ ký số.

Đó là các thủ tục, theo thứ tự: 1) Thủ tục sinh cặp khóa, gồm một private key và một public key, và các tham số đầu vào liên quan; 2) Thủ tục sinh chữ ký số trên tài liệu số M (gắn mẫu thông tin đã được mã hóa lên tài liệu số) và 3) Thủ tục kiểm tra tính hợp lệ của chữ ký số trên tài liệu số M (sau đây gọi là tài liệu M).

Một cách tương ứng, có 3 giao thức/thuật toán chính được sử dụng trong một lược đồ chữ ký số, với các chức năng cụ thể như sau:

- Thuật toán sinh khóa (Key generation algorithm): Thuật toán này giúp tạo ra một cặp khóa, gồm một private key cùng với public key tương ứng. Ngoài ra, nó còn tạo ra các tham số hệ thống.
- Thuật toán sinh chữ ký số (Signature generation algorithm): Thuật toán này giúp tạo ra một chữ ký số trên tài liệu cần ký. Đầu vào của thuật toán là private key của người ký, tài liệu mà họ cần ký và một số tham số cần thiết khác.
- Thuật toán kiểm tra chữ ký số (Signature verification algorithm): Thuật toán này giúp kiểm tra tính xác thực của chữ ký số được gắn trên một tài liệu, xem chữ ký số đó có đúng là được ký bởi người ký mong muốn hay không. Đầu vào của thuật toán là tài liệu đã được ký, public key của người ký và một số tham số cần thiết khác. Đầu ra là sự xác nhận về tính xác thực của chữ ký số trên tài liệu nhận được. Tính toàn vẹn của tài liệu M cũng được kiểm tra tại đây.

Ngoài ra, một lược đồ chữ ký số còn bao gồm:

- Tham số hệ thống và Tham số bảo mật: Tham số hệ thống (system parameter) được sử dụng cho cả bên tạo chữ ký số và bên kiểm tra chữ ký số. Tham số bí mật (secret parameters) thường được chọn bởi người muốn tạo ra chữ ký số, nó được giữ bí mật bởi chính người này.
- Không gian tài liệu cần ký: Đó là tập các tài liệu mà thuật toán sinh chữ ký số có thể thực hiện trên nó. Thông thường, tất cả các tài liệu cần ký đều được biểu diễn ở dạng xâu nhị phân, $\{0, 1\}^*$, có độ dài tùy ý (varying-length binary string) hoặc có độ dài xác định (fixed-length binary string).

Lược đồ chữ ký số có thể được xây dựa trên các bài toán khó như: Bài toán logarit rời rạc trên trường hữu hạn [3], [23], [42], bài toán logarit rời rạc trên đường cong Elliptic [11-12], [22], [25], [38], [47], [57], [96], bài toán phân tích thừa số, bài toán tìm căn modulo, v.v.. Cũng có thể xây dựng lược đồ chữ ký số dựa trên sự kết hợp của 2 trong số các bài toán khó vừa kể ra [5], [13-14], [18], [24], [30], [35], [45], [50], [66], [88], [93], [97-99].

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

Phần này của chương 1 trình bày về các chuẩn chữ ký số và các lược đồ chữ

ký số phổ biến, có thể gọi là lược đồ chữ ký số chuẩn, sẽ được sử dụng trong các chương sau của luận án.

1.2.1. Lược đồ chữ ký số RSA

Chữ ký số RSA (Ron Rivest, Adi Shamir và Leonard Adleman) [81] được hình thành dựa trên thuật toán mã hóa khóa công khai RSA, ở đây private key được sử dụng cho việc tạo ra chữ ký số trên tài liệu M và public key được sử dụng cho việc kiểm tra tính hợp lệ của chữ ký số trên tài liệu M. Độ an toàn của chữ ký số RSA dựa trên độ khó của bài toán phân tích số nguyên lớn thành thừa số.

Lược đồ chữ ký số RSA gồm 3 thủ tục dưới đây:

Trong lược đồ này, signer là người/là thực thể tạo ra chữ ký số trên tài liệu M; Verifier là người/là thực thể xác minh tính hợp lệ của chữ ký số mà họ nhận được cùng với tài liệu M:

- **Thủ tục sinh khóa:** Trước tiên, signer sử dụng thuật toán RSA để tạo ra cặp khóa bất đối xứng, public key và private key. Cụ thể như sau:

1. Chọn ngẫu nhiên 2 số nguyên tố lớn p và q, có cùng kích thước
2. Tính tích n:

$$n = pq \text{ và } \phi(n) = (p - 1)(q - 1) \quad (1.1)$$

3. Chọn ngẫu nhiên một số nguyên e, thỏa mãn $1 < e < \phi(n)$, sao cho

$$gcd(e, \phi(n)) = 1 \quad (1.2)$$

4. Sử dụng thuật toán Euclid để tính số nguyên d, thỏa mãn

$$1 < d < \phi(n), \text{ sao cho } ed = 1 \ (mod \ \phi(n)) \quad (1.3)$$

Kết quả: Public key của signer là (n, e) và private key của signer là (n, d).

- **Thủ tục sinh chữ ký số**: signer sử dụng private key được tạo ở trên để tạo chữ ký số của mình trên tài liệu M. Signer thực hiện như sau:

1. Tính $S = M^d \ mod \ n$ (1.4)

Kết quả: S chính là chữ ký số của signer trên tài liệu M.

- **Thủ tục kiểm tra chữ ký số:** Bất kỳ verifier nào cũng đều có thể kiểm tra tính hợp lệ chữ ký số của Signer gắn trên tài liệu M mà họ nhận được. Verifier thực hiện như sau:

1. Nhận public key xác thực của signer: (n, e)

2. Tính $M' = S^e \ mod \ n$ (1.5)

3. So sánh M' và M. Nếu $M' = M$ thì chữ ký số trên tài liệu M là hợp lệ.

- **Nhận xét về lược đồ chữ ký số RSA:**

- Tính đúng đắn của lược đồ dễ dàng được kiểm chứng. Vì nếu chữ ký số S đúng là được tạo bởi signer thì biểu thức $M' = M$ luôn xảy ra. Thật vậy:

$$\begin{aligned} M' = S^e \ (mod \ n) \quad &= (M^d)^e \ (mod \ n) \\ &= M^{de} \ (mod \ n) = MQ^{\phi(n)+1} \ (mod \ n) \\ &= M^{Q\phi(n)} \ M = (M^{\phi(n)})^Q M \\ &= 1^Q M \ (mod \ n) = M \end{aligned}$$

: Tức là: $M' = M$.

- Mức độ an toàn của lược đồ chữ ký số RSA dựa vào tính khó giải của bài toán phân tích một số nguyên dương thành các số nguyên tố, ở đây là phân tích n để tìm p và q. Độ khó của bài toán này càng tăng khi n càng lớn (n = 1024 bít, n = 2048 bít…). Tức là, khi p và q được chọn đủ lớn, thì việc phân tích $n = pq$ khó có thể thành công.

1.2.2. Lược đồ chữ ký số ElGamal

Chữ ký số ElGamal được hình thành cơ sở thuật toán khóa công khai ElGamal. Độ an toàn của chữ ký số này dựa trên độ khó của bài toán logarit rời rạc trên trường hữu hạn nguyên tố $GF(p)$.

Lược đồ chữ ký số ElGamal cho phép sinh chữ ký số trên tài liệu số dạng nhị phân có độ dài tùy ý. Lược đồ này yêu cầu sự hỗ trợ của hàm băm dạng: $\{0,1\}^* \rightarrow Z_p$, với p là một số nguyên tố lớn.

- **Thủ tục sinh khóa:** Mỗi signer tạo ra một cặp khóa public key và private key tương ứng. Cụ thể như sau:

1. Sinh ngẫu nhiên một số nguyên tố lớn p và một phân tử sinh α của nhóm nhân nguyên tố Z_p^*

2. Chọn ngẫu nhiên một số nguyên x: $1 \leq x \leq p-2$ (1.6)

3. Tính: $y = \alpha^x \ mod \ p$ (1.7)

Public key của signer là (p, α, y); Private key của signer là x.

- **Thủ tục sinh chữ ký số:** Signer tạo chữ ký số có độ dài tùy ý lên tài liệu M. Bất kỳ verifier nào đều cũng có thể kiểm tra tính hợp lệ của chữ ký này nếu họ

có được public key của signer. Signer thực hiện như sau:

1. Chọn ngẫu nhiên một số nguyên bí mật $k, 1 \leq k \leq p-2$, sao cho:

$$gcd(k, p-1) = 1 \quad (1.8)$$

2. Tính: $r = \alpha^k \ mod \ p$ (1.9)

3. Tính s theo biểu thức: $h(m) = xr + ks \ mod \ p - 1$, tức là,

$$s = k^{-1}(h(m) - xr) \ mod \ p - 1 \quad (1.10)$$

Chữ ký số của signer trên tài liệu M là cặp giá trị (r, s). Đây là dạng chữ ký số hai thành phần.

- **Thủ tục kiểm tra chữ ký số:** Để kiểm tra tính hợp lệ của chữ ký số, cặp (r, s), do signer tạo trên tài liệu M, verifier thực hiện như sau:

1. Nhận public key của A: (p, α, y)

2. Kiểm tra: $1 \leq r \leq p-1$: Nếu không thỏa thì từ chối chữ ký số của signer

3. Tính: $v_1 = y^r r^s \ mod \ p$ (1.11)

4. Tính $h(m)$ và $v_2 = \alpha^{h(m)} \ mod \ p$ (1.12)

5. So sánh v_1 và v_2. Nếu: $v_1 = v_2$: Chữ ký số của signer trên tài liệu M là hợp lệ. Ngược lại là không hợp lệ và sẽ bị từ chối.

▪ **Nhận xét về lược đồ chữ ký số ElGamal:**

- Tính đúng đắn của lược đồ dễ dàng được kiểm chứng.
- Vì mức độ an toàn của lược đồ chữ ký số ElGamal dựa vào tính khó giải của bài toán logarit rời rạc trên trường nguyên tố p. Tức là để tìm được private key x thì kẻ tấn công phải giải được bài toán khó logarit rời rạc $y = \alpha^x \ mod \ p$. Muốn giả mạo chữ ký số thì kẻ tấn công phải giải thêm 1 bài toán khó nữa: $r = \alpha^k \ mod \ p$, để tìm tham số bí mật k.

1.2.3. Chuẩn chữ ký số DSS

Tháng 08 năm 1991, Viện Quốc gia về chuẩn và công nghệ của Mỹ (NIST) đề xuất một thuật toán chữ ký số (gọi tắt là DSA). DSA sau đó trở thành chuẩn chữ ký số (gọi tắt là DSS) đầu tiên được công nhận bởi chính phủ Mỹ và nhiều chính phủ khác sau đó. Thuật toán DSA là một biến thể của lược đồ ElGamal.

Chữ ký số DSA sử dụng tập các tham số miền (domain) sau đây: Một private key x; Một secret key k, mỗi thông điệp có một k riêng, nên k gọi là (permessage

secret number k); Một public key y, có liên quan về mặt toán học với khóa x; Tài liệu số cần ký; và một Hàm băm an toàn. Private key x và secret key k được dùng trong quá trình sinh chữ ký số. Public key y dùng trong quá trình kiểm tra chữ ký số. Các tham số này được định nghĩa như sau: p: Là modulo nguyên tố, $2^{L-1} < p < 2^L$, với L là độ dài bít của p. L được chọn với những giá trị khác nhau; q: Là một ước nguyên tố của $(p-1)$, $2^{N-1} < q < 2^N$, với N là độ dài bít của q. N được chọn với những giá trị khác nhau; g: Là phần tử sinh của nhóm con có bậc q trong nhóm nhân của $GF(p)$, sao cho $1 < g < p$; x: Là private key của người ký, nó phải được giữ bí mật; x được chọn ngẫu nhiên hoặc là số nguyên được sinh theo cách giả ngẫu nhiên, $0 < x < q$, tức là $x \in [1, q-1]$; y: Là public key của người ký, $y = g^x \ mod \ p$; k: Là một số bí mật mà nó là duy nhất với mỗi tài liệu ký; k được chọn ngẫu nhiên hoặc là số nguyên được sinh theo cách giả ngẫu nhiên, $0 < k < q$, tức là $k \in [1, q-1]$.

- **Thủ tục sinh khóa:** Mỗi signer trước hết phải tạo ra một cặp khóa public key, private key và các tham số công khai. Signer thực hiện như sau:

1. Chọn số nguyên tố q sao cho $2^{159} \leq q \leq 2^{160}$
2. Chọn t sao cho $0 \leq t \leq 8$, và chọn một số nguyên tố p mà:

$$2^{511+64t} \leq p \leq 2^{512+64t}, \text{ với } q \mid (p-1) \quad (1.13)$$

3. Chọn phần tử sinh α của nhóm tuần hoàn có bậc q trong Z_p^*

   Chọn một phần tử g, $g \in Z_p^*$, và tính $\alpha = g^{(p-1)/q} \ mod \ p$ (1.14)

   Nếu $\alpha = 1$ thì chọn lại phần tử g
4. Chọn một số nguyên x, thỏa $1 < x < q$
5. Tính: $y = \alpha^x \ mod \ p$ (1.15)

Public key của signer là (p, q, α, y). Private key của signer là x.

- **Thủ tục sinh chữ ký số:** Signer thực hiện như sau:

1. Chọn một số nguyên bí mật k, $1 < k < q$ (1.16)
2. Tính: $R = (\alpha^k \ mod \ p) \ mod \ q$ (1.17)
3. Tính: $H = h(m)$; (m là tài liệu ký dạng nhị phân có độ dài tùy ý)
4. Tính: $S = \frac{H + xR}{k} \ mod \ q$ (1.18)

Chữ ký số của signer trên m là cặp giá trị (R, S).

- **Thủ tục kiểm tra chữ ký số:** Để kiểm tra tính hợp lệ của chữ ký số (R, S) của signer trên tài liệu m, verifier thực hiện như sau:

1. Nhận public key (p, q, α, y) xác thực của signer
2. Kiểm tra: Nếu $0 < R < q$ và $0 < S < q$ (1.19)
   không thỏa mãn thì chữ ký số bị từ chối
3. Tính: $H = h(m)$ (1.20)
4. Tính: $R' = (\alpha^{H/S} y^{R/S} \bmod p) \bmod q$ (1.21)
5. So sánh R'và R. Nếu $R' = R$ thì chữ ký số của signer trên m là hợp lệ. Ngược lại, chữ ký số không hợp lệ và bị từ chối.

- **Nhận xét về chuẩn chữ ký số DSS:**
  - Tính đúng đắn của lược đồ chữ ký đã được kiểm chứng.
  - Mức độ an toàn của chữ ký số DSS phụ thuộc vào tính khó giải của bài toán logarit rời rạc trên trường nguyên tố.

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

1.3.1. Chữ ký số nhóm

Chữ ký số nhóm (Group digital signature: GDS), được giới thiệu lần đầu bởi Chaum và Heyst [21] vào năm 1991, và gần đây được A. C. Enache mô tả trong [7], là loại chữ ký được hình thành trên danh nghĩa của một nhóm những người ký, gọi tắt là nhóm ký (signing group), nhưng thực tế thì nó được sinh ra chỉ bởi một thành viên ẩn danh của nhóm ký này. Điều này cũng có nghĩa, mặc dù chữ ký nhóm trên một tài liệu M là chỉ do một thành viên trong nhóm tạo ra nhưng việc xác minh tính hợp lệ của chữ ký sau này phải dựa vào các tham số công khai của nhóm ký, cụ thể ở đây là public key của nhóm ký.

Mỗi nhóm ký được điều hành bởi một người đứng đầu, gọi là người quản lý nhóm (Group manager: GM). Người này phải là một thành viên hoặc một đối tác tin cậy của nhóm ký. Nhiệm vụ chính của họ là tạo ra các tham số bí mật, các tham số hệ thống mà các thành viên nhóm sử dụng để tạo ra chữ ký nhóm của mỗi nhóm. Và chỉ có người này mới có thể tiết lộ được danh tính của thành viên đã tham gia vào việc sinh ra chữ ký nhóm lên tài liệu M.

1.3.2. Lược đồ chữ ký số nhóm

Lược đồ chữ ký số nhóm (Group digital signature scheme: GDS scheme)

[37], [83-86] mô tả hoạt động của một hệ thống xác thực dựa trên chữ ký số nhóm. Cũng như các lược đồ chữ ký số khác, nó gồm 3 thủ tục chính: Sinh khóa và các tham số hệ thống; Sinh chữ ký nhóm cho một nhóm những người ký; Kiểm tra tính hợp lệ của chữ ký nhóm dựa trên public key chung của cả nhóm.

Một lược đồ chữ ký nhóm được cho là đảm bảo an toàn thì nó phải thỏa mãn các tính chất sau:

- **Correctness** *(tính đúng đắn)*: Các chữ ký được sinh bởi thành viên nhóm, sử dụng thuật toán SIGN, phải được chấp nhận bởi VERIFY.
- **Unforgeability** *(tính không thể giả mạo)*: Chỉ những thành viên của nhóm mới có thể tạo ra các chữ ký nhóm hợp lệ.
- **Anonymity** *(tính ẩn danh)*: Với một chữ ký hợp lệ đã cho trên tài liệu M: Việc định danh chính xác ai là người đã tạo ra chữ này chỉ có thể được thực hiện bởi người quản lý nhóm.
- **Unlinkability** *(tính không thể liên kết)*: Với 2 chữ ký nhóm đã cho, rất khó để phân biệt hai chữ ký đó có được tạo ra bởi cùng một người ký hay không. Điều này đảm bảo rằng, nếu tính ẩn danh của một chữ ký hợp lệ bị phá vỡ bởi ai đó, thành viên ký được định danh, thì người này cũng khó có thể liên kết được, khó có thể biết được các chữ ký nhóm khác mà thành viên nhóm này tạo ra.
- **Exculpability** *(tính có thể biện giải):* Cả thành viên nhóm và người quản lý nhóm đều không thể tạo ra một chữ ký hợp lệ trên tài liệu M với tư cách của các thành viên khác trong nhóm. Điều này đảm bảo rằng, không một thành viên nhóm nào bị buộc là đã tạo ra chữ ký nhóm "hợp lệ" trên tài liệu M khi mà họ không thực hiện điều này.

Lược đồ chữ ký nhóm phải đáp ứng các điều kiện sau:

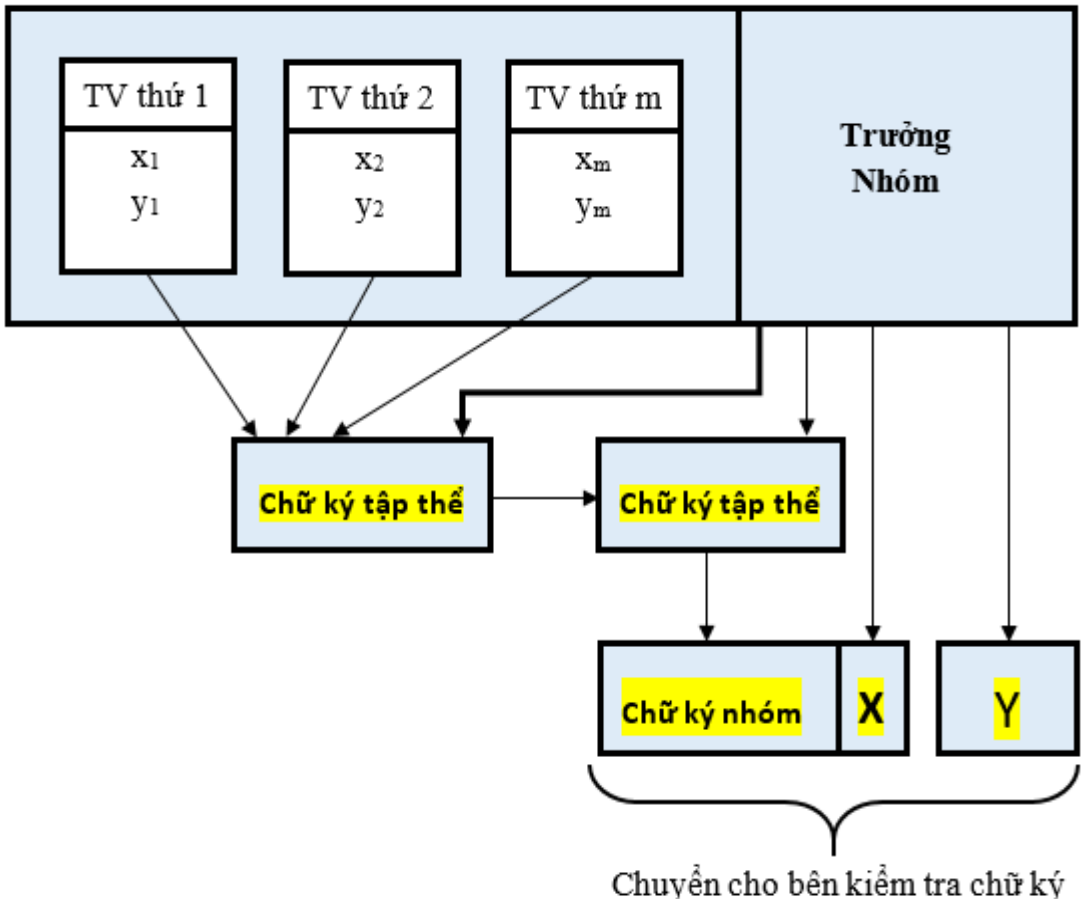
- Chỉ những thành viên của nhóm ký mới có thể ký lên các tài liệu số với danh nghĩa của nhóm những người ký đó.
- Người nhận có thể kiểm tra tính hợp lệ của chữ ký số được tạo ra bởi một nhóm ký nào đó, nhưng không thể biết được thành viên nào của nhóm ký đó đã tạo ra chữ ký mà họ nhận được.
- Khi cần người quản lý nhóm có thể "mở" (Open) chữ ký để biết được thành viên nào của nhóm ký đã tạo ra chữ ký của nhóm.

1.3.3. Minh họa hoạt động của một lược đồ chữ ký số nhóm

Phần sau đây mô tả hoạt động của một lược đồ chữ ký nhóm cụ thể, để minh họa vai trò của người quản lý nhóm, và sự tham gia của các thành viên trong nhóm ký, trong việc hình thành chữ ký nhóm cho một nhóm những người ký.

Giả sử có một nhóm gồm m thành viên (gọi là signer) và một người quản lý nhóm (ký hiệu là GM), gọi chung là nhóm ký, được chỉ định để tham gia vào việc sinh ra chữ ký nhóm của nhóm ký trên tài liệu M. Bất kỳ ai (gọi là verifier) cũng có thể kiểm tra tính hợp lệ, tính xác thực, của chữ ký nhóm này nếu họ có được public key của nhóm và các tham số liên quan khác. Thủ tục sinh chữ ký nhóm và Thủ tục kiểm tra chữ ký nhóm của lược đồ được mô tả như sau.

Quá trình hình thành chữ ký nhóm được mô tả trong hình 1.2 sau đây:



Hình 1.2. Sơ đồ quá trình hình thành chữ ký số nhóm

Hình 1.2 cho thấy, đầu tiên, nhóm thành viên từ 1 đến m phối hợp với nhau để tạo ra "Chữ ký tập thể". Sau đó, "Chữ ký tập thể" này được chuyển đến cho

"Trưởng nhóm", "Trưởng nhóm" sẽ thực hiện các công đoạn kiểm tra cần thiết trước khi sửa dụng private key X của chính "Trưởng nhóm" để tạo ra một "Chữ ký nhóm", nó đại diện cho cả nhóm ký. Cuối cùng, "Trưởng nhóm" sẽ chuyển "Chữ ký nhóm" và public key Y của nhóm ký (cũng là của "Trưởng nhóm") đến cho bên kiểm tra chữ ký.

Theo [75], private key của signer là x và public key tương ứng là y ($y_i = \alpha^{x_i} \bmod p, i = 1, 2, \dots, m$); Private key của GM là X và public key của GM là $Y = \alpha^X \bmod p$. Public key Y này được xem như public key tập thể của nhóm ký, nên được sử dụng để kiểm tra tính hợp lệ của chữ ký nhóm sau này; Cặp giá trị: Công khai (e), bí mật (d) được GM sinh ra theo thuật toán RSA, với p và q là hai số nguyên tố mạnh và $n = p.q$; F_{H} là hàm băm an toàn 256 bít; Tham số mặt nạ λ được sử dụng để ẩn public key của signer.

- **Thủ tục sinh chữ ký nhóm:**

1. GM thực hiện các công việc sau: Sử dụng hàm băm F_H để tính giá trị băm của M: $H = F_H(M)$; Tính tham số mặt nạ cho mỗi signer: $\lambda_i = (H + y_i)^d \bmod n$; Gửi các λ lại cho signer tương ứng.

Sau đó GM tính thành phần đầu tiên của chữ ký nhóm, giá trị U:

$$U = \prod_{i=1}^{m} {y_i}^{\lambda_i} \bmod p \tag{1.22}$$

Thành phần U được xem như mặt nạ của public key tập thể của nhóm ký.

2. Mỗi signer i thực hiện các công việc sau: Tính giá trị băm của tài liệu M: $H = F_H(M)$; Kiểm tra xem biểu thức ${\lambda_i}^e = y_i + H \bmod n$ có thỏa mãn hay không: Nếu thỏa mãn, thì λ_i là được cung cấp bởi chính GM; Sinh một số ngẫu nhiên $k_i < q$, và rồi tính giá trị $R_i = \alpha^{k_i} \bmod p$; Gửi R_i cho GM.

3. GM thực hiện tiếp các công việc sau: Sinh một số ngẫu nhiên $K < n$ và rồi tính giá trị $R' = \alpha^K \bmod p$; Tính R và rồi tính E:

$$R = R' \prod_{i=1}^{m} R_i \bmod p \tag{1.23}$$

$$= \alpha^{K + \sum_{i=1}^{m} k_i \bmod q} \bmod p$$

$$E = F_H(H \| R \| U), \| \text{ là ký hiệu kết xâu;} \tag{1.24}$$

GM gửi E cho tất cả signer trong nhóm ký.

E là thành phần thứ hai của chữ ký nhóm.

4. Mỗi signer i thực hiện như sau: Tính giá trị $S_i = k_i + \lambda_i x_i E \ mod \ q$ và rồi gửi kết quả này GM. S_i được xem như chữ ký của mỗi thành viên thứ i, họ chia sẻ cho GM để tạo ra chữ ký nhóm chung cho cả nhóm ký.

5. GM thực hiện tiếp các công việc sau:

- Tính thành phần chia sẻ chung của các thành viên trong nhóm ký S_c, theo công thức sau:

$$S_c = \sum_{i=1}^{m} S_i \ mod \ q \tag{1.25}$$

- Xác thực S_c bằng cách kiểm tra biểu thức sau có xảy ra hay không:

$$\frac{R}{R'} = U^{-E} \alpha^{S_c} \ mod \ p \tag{1.26}$$

- Nếu S_c hợp lệ thì GM sẽ tính S': $S' = K + XE \ mod \ q$. S' được xem là chữ ký mà GM góp vào để tạo ra chữ ký chung cho cả nhóm.

- Tính thành phần thứ ba của chữ ký số nhóm ký theo công thức sau:

$$S = S' + S_c \ mod \ q \tag{1.27}$$

Như vậy, bộ ba (U, E, S) là chữ ký nhóm của nhóm ký trên tài liệu M.

- **Thủ tục kiểm tra chữ ký nhóm**

Verifier thực hiện các công việc sau:

1. Tính giá trị băm của tài liệu M: $H = F_H(M)$ (1.28)

2. Sử dụng public key tập thể của nhóm ký (Y) và chữ ký nhóm (U, E, S) để tính R^* và rồi tính E^* theo các công thức sau:

$$R^* = (UY)^{-E} \alpha^S \ mod \ p \tag{1.29}$$

$$E^* = F_H(H \| R^* \| U) \tag{1.30}$$

3. So sánh E^* với E. Nếu $E^* = E$, thì chữ ký nhóm nhận được là hợp lệ. Ngược lại, chữ ký nhận được là không hợp lệ, và nó bị từ chối.

- **Nhận xét về lược đồ chữ ký số nhóm này:**

- Thủ tục sinh chữ ký cho thấy, mọi thành viên của nhóm ký đều tham gia trong quá trình hình thành các thành phần của chữ ký, nhưng chỉ có GM mới có quyền thực hiện bước cuối cùng. Như vậy, GM điều hành việc hình thành chữ ký nhóm và chịu trách nhiệm về tính hợp lệ của chữ ký này.

- Thủ tục kiểm tra chữ ký cho thấy, để xác thực tất cả thành viên của nhóm ký thì cần thực hiện trên chữ ký nhóm của nhóm ký này. Và chỉ có public key của

nhóm ký là được sử dụng trong bước kiểm tra tính hợp lệ của chữ ký nhóm.

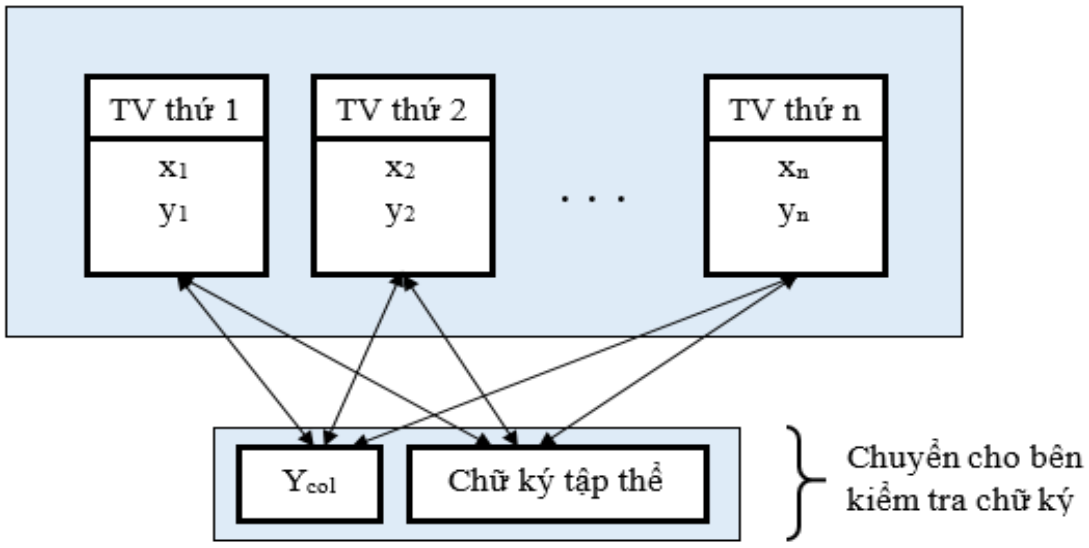
- Thành phần U trong chữ ký nhóm chứa thông tin của tất cả thành viên nhóm tham gia vào việc tạo ra chữ ký nhóm trên tài liệu M, nên khi cần, thì GM có thể "mở" (open) chữ ký để biết chính xác những thành viên này là ai. Ngoại trừ GM, không một thành viên nào thực hiện được việc mở này.

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

1.4.1. Chữ ký số tập thể

Chữ ký số tập thể (Collective Digital Signature) là loại chữ ký được hình thành với sự tham gia của tất cả thành viên trong một tập người ký đã được chỉ định trước, gọi là tập thể ký [1]. Điều này có nghĩa, chữ ký số tập thể trên một tài liệu M chỉ được công nhận là hợp lệ khi M được ký bởi tất cả người ký trong tập thể ký đó. Private key của mỗi người trong tập thể ký được sử dụng để tạo ra chữ ký số của tập thể ký này. Trong khi đó, public key của họ được sử dụng bởi thủ tục kiểm tra chữ ký để xác minh sự hợp lệ của chữ ký mà tập thể ký này tạo ra.

Quá trình hình thành chữ ký tập thể được mô tả ở hình 1.3 sau đây:



Hình 1.3. Sơ đồ quá trình hình thành chữ ký số tập thể

Hình 1.3 cho thấy, đầu tiên, n thành viên của tập thể ký phối hợp với nhau để tạo ra một "Chữ ký tập thể" duy nhất, chữ ký này đại diện cho tập thể ký. Y_{col} là public key của tập thể nó, nó được tạo ra từ public key của tất cả thành viên tham gia tạo ra "chữ ký tập thể". Sau đó, "Chữ ký tập thể" và Y_{col} sẽ được chuyển

đến cho bên kiểm tra chữ ký.

Ưu điểm của loại chữ ký này là: Có thể cài đặt nó dựa vào các giao thức chữ ký số cá nhân đang được triển khai trên các hạ tầng khóa công khai sẵn có. Và dễ dàng triển khai theo các chuẩn chữ ký số đã được công bố như: Chuẩn DSS của Mỹ, chuẩn GOST R 34.10-2012 của Nga [6], [31]. Chữ ký số tập thể dựa trên thuật toán mật mã công khai RSA lần đầu tiên được Punita Meelu and Sitender Malik đưa ra vào năm 2010 [81].

1.4.2. Lược đồ chữ ký số tập thể

Tương tự như các lược đồ chữ ký khác, lược đồ chữ ký số tập thể (Collective digital signature scheme: CDS scheme) cũng gồm 3 thủ tục chính: Sinh khóa và các tham số hệ thống; Sinh chữ ký tập thể cho tập thể ký; Kiểm tra tính hợp lệ của chữ ký tập thể dựa trên public key tập thể của tập thể ký.

- **Các yêu cầu cơ bản của chữ ký số tập thể:**

a) Kích thước của chữ ký số tập thể là cố định, không phụ thuộc số lượng thành viên tham gia vào việc tạo ra chữ ký, thường nó bằng độ lớn của chữ ký riêng lẻ của mỗi thành viên.

b) Khoá công khai tập thể của lược đồ chữ ký số tập thể được tạo ra bằng sự kết hợp khoá công khai của tất cả thành viên trong tập thể ký.

c) Chữ ký số tập thể được xác thực như cách thông thường nhưng ở đây sử dụng khóa công khai của tập thể ký.

d) Giả sử tập thể ký gồm m thành viên, thì m – 1 thành viên không thể ký thay cho người còn lại hoặc khó có thể giả mạo chữ ký của người còn lại.

Nghiên cứu sinh sử dụng lược đồ chữ ký tập thể cụ thể sau đây [72] để minh họa cho sự hoạt động của dạng lược đồ này. Lược đồ cũng cho thấy vai trò của các thành viên trong tập thể ký trong việc hình thành chữ ký tập thể cho tập thể ký.

Giả sử có một tập thể, một nhóm, gồm m thành viên cần ký lên tài liệu M, gọi chung là tập thể ký. Mỗi thành viên của tập thể ký này (gọi là signer) có private key là x_i và public key tương ứng là: $y_i = \alpha^{x_i} \bmod p$, với $i = 1, 2, \ldots, m$ và α là phần tử sinh có bậc q của nhóm Z_p^*. Public key tập thể của tập thể ký là Y, được tính theo công thức: $Y = y_1 y_2 \ldots y_m \bmod p$. Public key tập thể này được sử dụng để kiểm tra tính hợp lệ của chữ ký tập thể sau này. Bất kỳ ai (gọi là verifier) cũng

có thể kiểm tra tính hợp lệ, tính xác thực, của chữ ký tập thể này nếu họ có được public key tập thể và các tham số liên quan khác. Thủ tục sinh chữ ký tập thể và Thủ tục kiểm tra chữ ký tập thể của lược đồ được mô tả như sau:

- **Thủ tục sinh chữ ký tập thể:**

1. Mỗi signer trong tập thể ký thực hiện như sau: Tạo số ngẫu nhiên k_i, sao cho $1 < k_i < q$ (k_i đóng vai trò private key giả); Tính: $R_i = \alpha^{k_i} \, mod \, p$; Và rồi gửi R_i cho tất cả thành viên khác trong tập thể ký.

2. Một signer nào đó đại diện cho tập thể ký thực hiện các công việc sau: Tính tích các R_i: $R = R_1 R_2 \dots R_m \, mod \, p$, tích này đóng vai trò là thành phần ngẫu nhiên chung của tập thể ký; Tính E theo công thức: $E = F_H(M \,||\, R \,||\, Y)$: || là toán tử kết xâu. E là thành phần đầu tiên của chữ ký tập thể; Gửi E cho các thành viên trong nhóm ký.

3. Mỗi signer trong tập thể ký thực hiện như sau: Tính giá trị S_i theo công thức: $S_i = (k_i + x_i E) \, mod \, q$. S_i được xem như chữ ký cá nhân của signer thứ i, nó được người này chia sẻ với tập thể để tạo ra thành phần thứ hai của chữ ký tập thể; Gửi S_i cho tất cả thành viên khác trong tập thể ký.

4. Một signer nào đó đại diện tập thể ký tính thành phần thứ hai của chữ ký tập thể theo công thức: $S = S_1 + S_2 + \cdots + S_m \, mod \, q.$ (1.31)

Như vậy, cặp giá trị (E, S) là chữ ký tập thể của một tập thể ký gồm m thành viên trên tài liệu M.

- **Thủ tục kiểm tra chữ ký tập thể**

Verifier thực hiện các công việc sau:

1. Tính giá trị public key tập thể: $Y = y_1 y_2 \dots y_m \, mod \, p$ (1.32)

2. Tính giá trị $R^* = \alpha^S Y^{-E} \, mod \, p$ (1.33)

3. Tính E^*: $E^* = F_H(M \| R^* \| Y)$ (1.34)

4. So sánh giá trị E^*và E. Nếu E* = E, thì chữ ký tập thể nhận được là hợp lệ. Ngược lại, chữ ký nhận được là không hợp lệ, và nó bị từ chối.

- **Nhận xét về lược đồ chữ ký số tập thể:**

- Thủ tục sinh chữ ký cho thấy, mọi thành viên của tập thể ký đều có vai trò như nhau trong việc hình thành hai thành phần E và S của chữ ký tập thể, hoàn

toàn không có sự phân biệt về cấp chức năng ở đây. Người đại diện nhóm là một thành viên bất kỳ trong tập thể, họ không được "độc quyền" trong việc tạo ra chữ ký tập thể và họ cũng không có quyền xác thực thành viên của tập thể như người quản lý nhóm trong lược đồ chữ ký nhóm.

- Thủ tục kiểm tra chữ ký cho thấy, để xác thực tất cả thành viên của tập thể ký thì chỉ cần xác thực chữ ký tập thể của tập thể ký này. Nhưng khác với lược đồ chữ ký số nhóm, ở đây phải sử dụng public key tập thể, được tạo ra từ public key của tất thành viên trong tập thể ký.

- Dễ thấy rằng, kích thước chữ ký tập thể không phụ thuộc vào số lượng người ký lên bản tin M, nó đúng bằng $|q| + |E|$. Nếu chúng ta sử dụng hàm băm F_H có kích thước 160 bít thì kích thước chữ ký tập thể sẽ là 320 bít.

Chữ ký tập thể và chữ ký tập thể mù [29], [32], [39-40], [43], hiện được sử dụng khá phổ biến trong các ứng dụng bầu cử điện tử [9], [41], [44], [53], [55-56], [63] và tiền điện tử [64] trên không gian mạng.

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

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 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.

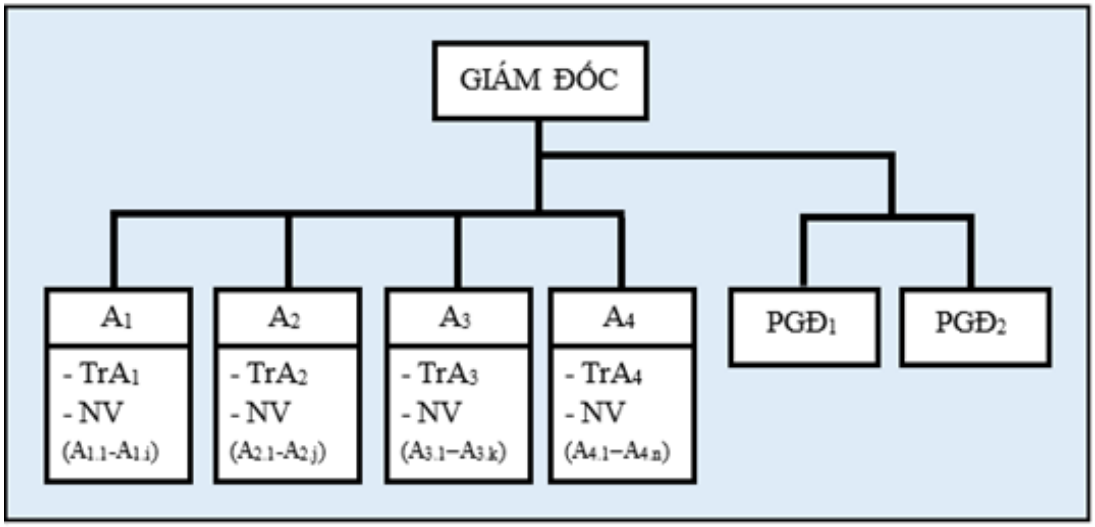
Xét cơ cấu tổ chức của một công ty trong thực tế, ví dụ Công ty A (xem hình 1.4): Ban lãnh đạo Công ty A gồm 1 giám đốc (GĐ) và 2 phó giám đốc (PGĐ1, PGĐ2); Có 4 đơn vị chức năng trong Công ty A: A1, A2, A3, A4. Mỗi đơn vị có một trưởng đơn vị: TrA1, TrA2, TrA3, TrA4, và một số nhân viên thuộc đơn vị. 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 định danh nguồn gốc của thành viên, họ 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 bên kiểm tra chữ ký nhưng khó khả thi trong thực tế, vì nó vi phạm tính đa cấp về mặt chức năng của tập thể ký.

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

- 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 số tập thể cho các nhóm ký (hay còn được gọi là Lược đồ chữ ký số 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 số 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.

Các dạng lược đồ này đều cung cấp khả năng sinh ra một chữ ký số đơn, trên tài liệu M, cho một tập thể người ký đa cấp. Chữ ký đơn này chứa thông tin

của tất cả thành viên tham gia vào việc hình thành chữ ký, nên khi cần hệ thống có thể biết được những ai đã cùng ký vào tài liệu M. Đây cũng là cơ sở để bên kiểm tra chữ ký tin rằng chữ ký đơn này đã được tạo ra bởi nhiều nhóm ký và nhiều cá nhân ký khác nhau. Một ưu điểm nữa của các lược đồ chữ ký tập thể mới này là khi cần nó có thể sử dụng để tạo ra các chữ ký số nhóm, các chữ ký số tập thể như những lược đồ chữ ký số nhóm, chữ ký số tập thể thông thường khác.

1.6. Một số nghiên cứu liên quan luận án

Đến nay đã có nhiều dạng lược đồ chữ ký số được nghiên cứu và công bố như*: Lược đồ chữ ký số đơn; Lược đồ chữ ký số mù; Lược đồ chữ ký số nhóm; Lược đồ chữ ký số tập thể; Lược đồ chữ ký số tập thể mù; v.v.*.

Tùy theo mô hình chứng thực của bài toán thực tế mà người dùng, thường là nhà phát triển ứng dụng trên không gian mạng, chọn một lược đồ chữ ký số phù hợp để triển khai. Sự lựa chọn này còn phụ thuộc vào cấp độ bảo mật và thời gian thực thi xác thực được yêu cầu của bài toán đặt ra. Ngoài ra, nó còn phụ thuộc vào hạ tầng PKI mà ứng dụng xác thực dự định triển khai trên đó.

1.6.1. Tình hình nghiên cứu trong nước

Trong nhiều năm gần đây, nhiều nhà khoa học trong nước đã nghiên cứu và công bố nhiều dạng chữ ký số, từ chữ ký đơn đến chữ ký số tập thể, từ áp dụng một bài toán khó đến áp dụng đồng thời hai bài toán khó, v.v., hầu hết chúng đều đáp ứng được các yêu cầu chứng thực của nhiều bài toán thực tế hiện này.

Trong phần này NCS chỉ điểm lại những công bố, những dạng lược đồ chữ ký số, mà nó liên quan đến hướng nghiên cứu của luận án.

- Trong [1], tác giả Lưu Hồng Dũng đã thành công trong việc sử dụng bài toán logarit rời rạc để xây dựng lược đồ đa chữ ký số, chữ ký tập thể, đáp ứng đầy đủ các yêu cầu cơ bản của chữ ký số thông thường. Lược đồ này cho phép một nhóm người cùng hợp tác để ký vào một văn bản, không một thành viên nào có thể phát sinh chữ ký cá nhân của mình, mà phải kết hợp với tất cả thành viên còn lại trong nhóm để tạo ra chữ ký chung trên văn bản cần ký. Vấn đề kiểm tra chữ ký cũng được thực hiện tương tự như trong chữ ký đơn nhưng bên kiểm tra sử dụng public key của cả nhóm ký chứ không phải của bất kỳ thành viên nào (2013).

Tác giả Lưu Hồng Dũng cũng cho thấy, khi người đại diện nhóm là "kẻ xấu" thì người này có thể giả mạo một thành viên của nhóm để tham gia vào việc

ký lên tài liệu M mà không cần phải tính private key của người đó, điều này có nghĩa, tính exculpability của lược đồ bị xâm phạm. Tuy nhiên, tác giả cũng đã chỉ ra rằng, hạn chế này có thể được khắc phục nếu lược đồ được triển khai trên hạ tầng PKI, với CA tin cậy.

- Trong [76], nhóm tác giả Nguyễn Hiếu Minh, Moldovyan Nikolay và cộng sự, đề xuất các lược đồ chữ ký số mù và chữ ký số tập thể mù dựa trên tính khó giải của bài toán tìm căn modulo của số nguyên tố lớn. Chữ ký của nhóm tác giả gồm 2 thành phần (E', S'), độ lớn của E' là 160 bít, của S' là 1024 bít, và được cho rằng khá phù hợp cho yêu cầu xác thực của các ứng dụng thực tế, như hệ thống thanh toán liên ngân hàng (2012).

- Năm 2020, trong luận án của mình [4], tác giả Nguyễn Tấn Đức đã nghiên cứu và trình bày khá nhiều vấn đề liên quan đến chữ ký số mù và chữ ký số tập thể mù. Tác giả đã sử dụng các chuẩn chữ ký số như GOST, Schnorr, EC-Schnorr, RSA và các bài toán khó như IFP, DLP, IFP-DLP để xây dựng các lược đồ chữ ký tập thể mù khác nhau. Mỗi lược đồ đều được tác giả chứng minh được tính đúng và tính an toàn của nó, đồng thời, tác giả cũng đã phân tích và so sánh hiệu năng của các lược đồ đề xuất với các lược đồ cùng loại đã công bố trong những năm gần đây. Theo NCS, đóng góp quan trọng nhất của đề tài luận án này là đã đưa ra được bài toán khó mới, sử dụng nhóm con hữu hạn không vòng hai chiều, và xây dựng thành công chữ ký số tập thể mù dựa trên bài toán khó mới này.

1.6.2. Tình hình nghiên cứu trên thế giới

Sau đây là một vài kết quả nghiên cứu về lược đồ chữ ký số của tác giả nước ngoài mà nó liên quan đến đề tài nghiên cứu trong luận án này của NCS.

- Một trong những giải pháp nhằm tăng cường mức độ an toàn của lược đồ chữ ký số được nhiều nhà nghiên cứu nước ngoài quan tâm là sử dụng đồng thời hai bài toán khó để xây dựng lược đồ. Nhưng thực tế thì điều này không phải luôn luôn đúng. Ví dụ, năm 2004, Tzeng [95] và cộng sự đã chỉ ra rằng, chữ ký số dựa vào hai bài toán khó, phân tích thành thừa số và logarit rời rạc, của Shao [100] và cộng sự là không an toàn. Tzeng đã đề xuất một thuật toán mới để thay thế thuật toán của Shao, nhưng vào năm 2005, Shao lại chứng tỏ rằng chữ ký của Tzeng cũng không an toàn [95]. Theo Shao, nếu ai đó có thể giải quyết được bài toán

logarit rời rạc thì họ có thể giả mạo chữ ký của Tzeng. Cũng theo Shao, chữ ký của Tzeng thực chất chỉ phụ thuộc vào một bài toán khó, phân tích thừa số hoặc logarit rời rạc.

- Trong [34], Ismail E.S và cộng sự đề xuất một lược đồ chữ ký dựa trên 2 vấn đề khó, phân tích thừa số và logarit rời rạc. Nhóm tác giả cho rằng các lược đồ chữ ký được xây dựng dựa trên hai bài toán khó sẽ an toàn hơn so với sử dụng một bài toán khó. Bài báo cũng cho thấy, lược đồ chữ ký đề xuất của nhóm tác giả có thể chống lại được 5 dạng tấn công vào lược đồ chữ ký số phổ biến. Cuối cùng, Ismail E.S và cộng sự nhận định: Các lược đồ chữ ký xây dựng trên nhiều bài toán khó, tuy có độ dài lớn hơn nhưng mức độ an toàn là khá cao hơn và chi phí thời gian khá thấp so với các lược đồ được xây dựng trên cùng bài/các bài toán khó.

- Chữ ký số tập thể và chữ ký số tập thể mù dựa trên bài toán logarit rời rạc, sử dụng lược đồ chữ ký số Schnorr, được Nikolay A. Moldovyan và Alexander A. Modovyan đề xuất trong [74]. Đây là một dạng mới của lược đồ đa chữ ký, tất cả người ký đều tham gia vào việc hình thành chữ ký. Nó cho phép tạo ra chữ ký 320 bít nhưng đạt cấp độ bảo mật 80 bít. Lược đồ này hỗ trợ ký đồng thời một gói các hợp đồng khác nhau bởi các tập người ký khác nhau (2011).

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

1.7.1. Bài toán phân tích thừa số

Cho số $n \in \mathbb{N}$, hãy tìm biểu diễn: $n = \prod_{i=1}^{k} {p_i}^{e_i}$; với: $e_i \geq 1$ ($i = 1, 2, \dots, k$) nguyên dương; $p_i \geq 1$ ($i = 1, 2, \dots, k$) nguyên tố.

Một trường hợp riêng của bài toán phân tích thừa số được ứng dụng để xây dựng hệ mật RSA mà ở đó n là tích của hai số nguyên tố p và q. Khi đó, bài toán phân tích thừa số được phát biểu như sau: Với mỗi số nguyên dương n, hãy tìm 2 số nguyên tố p hoặc q thỏa mãn biểu thức sau: $p \times q = n$.

Trong hệ mật RSA [81], bài toán phân tích số được sử dụng trong việc hình thành cặp public key/private key cho mỗi bên ký. Với việc giữ bí mật các tham số (p, q) thì việc tính được private key (d) từ public key (e) và *modulo* (n) là một bài toán khó nếu p, q được chọn đủ lớn và mạnh.

Hiện tại bài toán phân tích thành nhân tử vẫn được coi là bài toán khó do chưa có giải thuật thời gian đa thức hay đa thức xác suất cho nó và hệ mật RSA là

một minh chứng thực tế cho tính khó giải của bài toán này. Trong thực tế, các tham số, có thể chọn theo FIPS 186 – 4 của Hoa Kỳ cho hệ mật RSA.

1.7.2. Bài toán logarit rời rạc

Cho p là một số nguyên tố và g là phần tử sinh của nhóm Z_p^*. Khi đó bài toán logarit rời rạc (Discrete Logarithm Problem) trên trường Z_p được phát biểu như sau: Với mỗi số nguyên dương $\in Z_p^*$, hãy tìm x thỏa mãn phương trình sau:

$$g^x \ mod \ p = y \tag{1.35}$$

Giải thuật cho bài toán logarit rời rạc với các tham số $\{p, g\}$ công khai có thể được viết như một thuật toán tính hàm $DLP_{(p,g)}(.)$ với biến đầu vào là y còn giá trị hàm là nghiệm x của phương trình: $x = DLP_{(p,g)}(y)$ (1.36)

Bài toán DLP là khó theo nghĩa không thể thực hiện được trong thời gian thực, tuy nhiên không phải với mọi $y \in Z_p^*$ thì việc tính DLP đều khó, chẳng hạn những $y = g^x \ mod \ p$ với x không đủ lớn thì bằng cách duyệt dần $x = 1, 2, 3$ ... cho đến khi tìm được nghiệm của (1.35) ta sẽ tìm được private key x, do đó các giá trị của khóa mật x phải được lựa chọn sao cho việc tính $DLP_{(p,g)}$ đều khó.

Hiện tại, bài toán trên vẫn được coi là bài toán khó [3-5] do chưa có giải thuật thời gian đa thức cho nó và hệ mật ElGamal [67] là một chứng minh thực tế cho tính khó giải của bài toán này.

1.7.3. Bài toán tìm căn modulo số nguyên tố lớn

Bài toán tìm căn modulo số nguyên tố lớn là bài toán khó mới, được Nikolay A. Moldovyan đề xuất vào năm 2008 trong [70].

Vấn đề khó ở đây là tìm các căn modulo thứ k, với modulo là số nguyên tố lớn có cấu trúc $p = Nk^s + 1$, với N là một số chẵn ($|N| \geq 704 \ bít$), $s \geq 2$ và k là số nguyên tố lớn ($|k| \geq 160 \ bít$). Độ khó của bài toán mới này ước tính là O($\sqrt{k}$).

Theo bài toán khó này, nếu x là private của người ký thì public key tương ứng (y) của họ là: $y = x^k mod \ p$ ($|p| \geq 1024 \ bít$). Chữ ký của người ký được tạo ra trên tài liệu M là một cặp giá trị p bít (S, R). $S = tx^{f(R,M)} \ mod \ p$ và $R = t^k \ mod \ p$, trong đó $f(R, M)$ là một hàm băm nào đó. Khi đó biểu thức kiểm tra có dạng $S^k \ mod \ p = \ y^{f(R,M)} \ R \ mod \ p$. Độ lớn của chữ ký là: $|S| + \ |R| \ \approx 2 \ p$.

Nikolay A. Moldvyan đã chứng minh được, nếu chọn $|k| = 160 \ bít$, chọn $s = 2$ và chọn giá trị của N sao cho $|p| \ \geq 1024 \ bít$ thì cấp độ an toàn tối thiểu

của lược đồ chữ ký dựa trên bài toán khó này là $W = O(\sqrt{k}) \approx 2^{80}$. Tức là, để giả mạo được chữ ký này, kẻ giả mạo phải thực hiện 2^{80} phép lấy lũy thừa. Điều này là khó khả thi.

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 số 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 số tập thể cho nhiều nhóm ký (mục 2.1.3 và mục 2.2.3) và ii) Lược đồ chữ ký tập thể cho nhiều nhóm ký và nhiều người ký cá nhân (mục 2.1.4 và mục 2.2.4).

Vì tập thể đa cấp chức năng gồm nhiều nhóm thành viên và nhiều người ký cá nhân nên để xây dựng lược đồ chữ ký tập thể đại diện cho tập thể này thì trước hết phải xây dựng các lược đồ cơ sở, đó là:

i) Lược đồ chữ ký nhóm (mục 2.1.2 và mục 2.2.2): Để tạo ra chữ ký nhóm cho mỗi nhóm thành viên. Trong trường hợp này, người ký cá nhân cũng được xem như một nhóm nhưng là nhóm không có thành viên, chỉ có nhóm trưởng.

ii) Lược đồ chữ ký tập thể (mục 2.1.1 và mục 2.2.1): Được sử dụng làm lược đồ cở sở để tạo ra các lược đồ chữ ký tập thể đại diện.

Những vấn đề liên quan đến mức độ an toàn và hiệu năng tính toán của các lược đồ chữ ký tập thể đại diện được xây dựng dựa trên các bài toán logarit rời rạc cũng được trình bày khá rõ ở cuối chương này.

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

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

Phần này mô tả hoạt động một lược đồ chữ ký tập thể do nhóm tác giả Nikolay A. Moldovyan và Alexander A. Moldovyan đề xuất trong [74]. Lược đồ này được xây dựng dựa trên sự kết hợp giữa bài toán logarit rời rạc trên trường hữu hạn GF(p) và lược đồ chữ ký Schnorr. Chữ ký tập thể được sinh ra ở đây có tính tổng quát cao, gồm hai thành phần, có độ dài 320 bít.

Đây là một trong hai lược đồ cơ sở mà luận án sử dụng để xây dựng lược đồ chữ ký tập thể đại thể dựa trên bài toán logarit rời rạc trên trường nguyên tố.

Các tham số được sử dụng trong lược đồ CDS-2 bao gồm: Một số nguyên tố p đủ lớn, gọi là modulo nguyên tố p. Một số nguyên tố q, sao cho $q|p-1$ ($|q| = 160\ bít$). Kích thước được chọn của p và q cung cấp độ an toàn 80 bít; Phần tử g là phần tử sinh của nhóm con bậc q trong F_p^*.

Giả sử có một tập thể ký gồm m thành viên (người ký), muốn tạo một chữ ký tập thể trên tài liệu M. Private key của mỗi thành viên là x_i ($i = 1, 2, \dots, m$) và public key tương ứng của họ là y_i: $y_i = g^x \ mod\ p$. Public key của tập thể ký là Y, được kết hợp từ public key của tất cả thành viên tham gia vào việc tạo ra chữ ký của tập thể ký. Y này được sử dụng bởi bên kiểm tra chữ ký (hay người kiểm tra: verifier).

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

Gồm các bước sau:

1. Mỗi signer thứ i trong tập thể ký thực hiện:

- Sinh một giá trị ngẫu nhiên t_i và rồi tính R_i theo công thức:

$$R_i = g^{t_i} \ mod\ p \tag{2.1}$$

- Gửi R_i đến tất cả signer khác trong tập thể ký.

2. Một signer nào đó trong tập thể ký thực hiện:

- Tính giá trị tham số ngẫu nhiên R của chữ ký tập thể theo công thức:

$$R = \prod_{i=1}^{m} R_i \ mod\ p \tag{2.2}$$

- Sử dụng một hàm băm 160 bít (F_H) để tính E theo công thức:

$$E = F_H(M \| R) \tag{2.3}$$

("||" là toán tử nối xâu).

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

3. Mỗi signer thứ i trong tập thể ký thực hiện:

- Tính giá trị chia sẻ S_i của họ theo công thức:

$$S_i = t_i + x_i E \ mod\ q \tag{2.4}$$

- Gửi S_i đến tất cả signer khác trong tập thể ký.

4. Một signer nào đó trong tập thể ký thực hiện:

- Tính thành phần thứ hai S của chữ ký tập thể theo công thức:

$$S = \sum_{i=1}^{m} S_i \, mod \, q \tag{2.5}$$

Vậy cặp giá trị (E, S) là chữ ký tập thể của tập thể ký, gồm m thành viên, trên tài liệu M. Nó đại diện cho tập thể ký này.

Vì F_H là hàm băm 160 bít và $|q| = 160$ bít nên tổng kích thước của chữ ký này là 320 bít, nhỏ đáng kể so với các chữ ký tập thể được xây dựng dựa trên các bài toán khó khác, đặc biệt là bài toán tìm căn modulo số nguyên tố lớn [70].

- **Thủ tục kiểm tra chữ ký tập thể trên tài liệu M**

Thủ tục này được thực hiện tương tự thủ tục kiểm tra chữ ký trong lược đồ chữ ký Schnorr [49], ngoại trừ có thêm bước tính public key tập thể Y.

Để kiểm tra tính hợp lệ của chữ ký nhận được cùng với tài liệu M, bên kiểm tra (verifier), sử dụng chữ ký tập thể nhận được (E, S) và các tham số đầu vào công khai, thực hiện các bước sau:

1. Tính public key tập thể ký Y theo công thức:

$$Y = \prod_{i=1}^{m} Y_i \, mod \, p \tag{2.6}$$

2. Tính giá trị R^*theo công thức:

$$R^* = Y^{-E} g^S \, mod \, p \tag{2.7}$$

3. Tính E^* theo công thức:

$$E^* = F_H(M \| R) \tag{2.8}$$

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 (hoặc bị giả mạo hoặc tài liệu M không đảm bảo tính toàn vẹn), nó bị từ chối.

- **Chứng minh tính đúng của lược đồ CDS-2.1**

Tính đúng đắn, hay tính đúng, của một lược đồ chữ ký là sự phù hợp giữa phương pháp hình thành chữ ký với phương pháp kiểm tra tính hợp lệ của chữ ký và tính toàn vẹn của văn bản được ký.

Vậy để chứng minh tính đúng của lược đồ chữ ký tập thể này, ta phải chứng

minh được, chữ ký (E, S) được sinh ra từ thủ tục sinh chữ ký thỏa mãn công thức kiểm tra R^* trong thủ tục kiểm tra chữ ký. Nếu điều này xảy ra thì biểu thức $E^* = E$ luôn tồn tại. Tức là, tính đúng của lược đồ được đảm bảo.

Dễ thấy, chữ ký (E, S) luôn thỏa mãn công thức kiểm tra R^*. Thật vậy:

$$\begin{aligned} R^* &\equiv Y^{-E} g^S \equiv Y^{-E} g^{\sum_{i=1}^{m}(t_i + x_i E)} \\ &\equiv Y^{-E} g^{\sum_{i=1}^{m} t_i} g^{E \sum_{i=1}^{m} x_i} \\ &\equiv Y^{-E} g^{\sum_{i=1}^{m} t_i} Y^E \\ &\equiv \prod_{i=1}^{m} g^{t_i} \equiv \prod_{i=1}^{m} R_i \\ &\equiv R \bmod p \\ &\equiv R \end{aligned}$$

Suy ra: $E^* = F_H(M \| R^*) = F_H(M \| R) = E$

Vậy biểu thức $E^* = E$ luôn tồn tại: Chứng tỏ tính đúng của lược đồ chữ ký tập thể CDS-2.1 luôn được đảm bảo.

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

Trong phần này, trên cơ sở lược đồ chữ ký nhóm được Nikolay A. Moldovyan và cộng sự đề xuất trong [74], NCS xây dựng lược đồ chữ ký nhóm mới làm cơ sở cho lược đồ chữ ký tập thể đại diện của luận án.

Các tham số được sử dụng trong các giao thức của lược đồ bao gồm: i) Một số nguyên tố đủ lớn p $(|p| > 2048\ bít)$ và một số nguyên tố q $(|q| \geq 256\ bít)$, sao cho $q|p - 1$; ii) Một số α có bậc bằng q modulo p.

Giả sử có một nhóm ký gồm m thành viên (signer), muốn tạo một chữ ký nhóm trên tài liệu M. Mỗi signer thứ i (với $i = 1, 2, \ldots, m$) trong nhóm ký có private key là x_i $(|x| \geq 256$ bít*)* và public key tương ứng là $y_i = \alpha^{x_i} \bmod p$.

Private key của trưởng nhóm (GM: Group manager) là X và public key tương ứng của GM là: $Y = \alpha^X \bmod p$. Y cũng chính là public key của nhóm ký, nên Y được bên nhận chữ ký sử dụng để kiểm tra tính hợp lệ (xác thực) của chữ ký nhóm nhận được.

Lược đồ chữ ký nhóm này gồm các thủ tục dưới đây:

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

Gồm các bước sau:

1. GM thực hiện:

- Tính giá trị băm của tài liệu M (F_H là hàm băm MD5 hoặc SHA):

$$H = F_H(M) \tag{2.9}$$

- Tính các hệ số mặt nạ λ_i theo công thức sau ("||": Toán tử nối xâu):

$$\lambda_i = F_H\big(H||y_i||F_H(H||y_i||X)\big) \tag{2.10}$$

- Gửi λ_i đến mỗi signer tương ứng

- Tính thành phần đầu tiên U của chữ ký nhóm theo công thức:

$$U = \prod_{i=1}^{m} y_i^{\lambda_i} \, mod \, p \tag{2.11}$$

2. Mỗi signer thứ i trong nhóm ký thực hiện:

- Sinh số ngẫu nhiên k_i, thỏa $k_i < q$, rồi tính R_i theo công thức:

$$R_i = \alpha^{k_i} \, mod \, p \tag{2.12}$$

- Gửi R_i đến GM.

3. GM tiếp tục thực hiện:

- Sinh số ngẫu nhiên K, thỏa $K < q$, rồi tính giá trị thành phần ngẫu nhiên R của chữ ký theo các công thức:

$$R' = \alpha^{K} \, mod \, p \tag{2.13}$$

$$R = R' \prod_{i=1}^{m} R_i \, mod \, p \tag{2.14}$$

$$= \alpha^{K+\sum_{i=1}^{m} k_i} \, mod \, p \tag{2.15}$$

- Tính thành phần thứ hai E của chữ ký theo công thức:

$$E = F_H(M \| R \| U) \tag{2.16}$$

- Gửi E đến tất cả các signer trong nhóm ký (những người đã tham gia quá trình hình thành chữ ký từ ban đầu).

4. Mỗi signer thứ i trong nhóm ký tiếp tục thực hiện:

- Sinh số ngẫu nhiên k_i, thỏa $k_i < q$, rồi tính giá trị S_i theo công thức:

$$S_i = k_i - x_i \lambda_i E \, mod \, q \tag{2.17}$$

- Gửi S_i đến GM.

Cặp giá trị (R_i, S_i) được xem là chữ ký mà signer thứ i chia sẻ với nhóm ký, để tạo ra chữ ký nhóm của nhóm ký của họ (S_i thường được gọi là "thành phần chia sẻ" hay "chữ ký chia sẻ" của signer i).

5. GM thực hiện các công đoạn cuối cùng:

- Kiểm tra tính đúng của mỗi thành phần chia sẻ S_i theo công thức:

$$R_i = y_i^{\lambda_i E} \alpha^{S_i} \bmod p \tag{2.18}$$

- Nếu tất cả S_i đều thỏa mãn biểu thức trên thì thành phần chia sẻ S' của GM sẽ được tính theo công thức:

$$S' = K - XE \bmod q \tag{2.19}$$

- Tính thành phần thứ ba S của chữ ký nhóm theo công thức:

$$S = S' + \sum_{i=1}^{m} S_i \bmod q \tag{2.20}$$

Vậy bộ 3 giá trị (U, E, S) là chữ ký nhóm của nhóm ký, gồm m thành viên, trên tài liệu M. Nó đại diện cho nhóm ký này.

Giả sử F_H được sử dụng ở lược đồ này là hàm băm 128 bít, MD5. Khi đó độ lớn của chữ ký nhóm này là: $|U| + |E| + |S| = |p| + |F_H| + |q| \approx |p|$.

- **Thủ tục kiểm tra chữ ký nhóm trên tài liệu *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 giá trị băm của tài liệu M theo công thức:

$$H = F_H(M) \tag{2.21}$$

2. Tính giá trị R^* theo công thức:

$$R^* = (UY)^E \alpha^S \bmod p \tag{2.22}$$

3. Tính giá trị E^* theo công thức:

$$E^* = F_H(M \| R^* \| U) \tag{2.23}$$

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.

- **Chứng minh tính đúng của lược đồ GDS-2.1**

Tính đúng của lược đồ chữ ký nhóm này thể hiện qua: i) Sự tồn tại của công

thức kiểm tra chữ ký chia sẻ S_i của mỗi thành viên (2.17); và ii) Sự tồn tại của biểu thức kiểm tra $E^* = E$. Cụ thể như sau:

a) Tính đúng của công thức kiểm tra chữ ký chia sẻ của thành viên thứ i:

Nếu S_i là hợp lệ thì công thức (2.18) luôn tồn tại. Thật vậy:

$$\begin{aligned} R_i &= {y_i}^{\lambda_i E} \alpha^{S_i} \ mod\ p \\ &= (\alpha^{x_i})^{\lambda_i E}.\alpha^{k_i - x_i \lambda_i E} \ mod\ p \\ &= \alpha^{x_i \lambda_i E}.\alpha^{k_i}.\alpha^{-x_i \lambda_i E} \ mod\ p \\ &= \alpha^{k_i} \ mod\ p = R_i \end{aligned}$$

Điều này chứng tỏ tính đúng của công thức kiểm tra (2.18) được đảm bảo.

b) Tính đúng của thủ tục kiểm tra chữ ký:

Dễ thấy, chữ ký (U, E, S) được sinh ra ở thủ tục sinh chữ ký luôn thỏa mãn công thức kiểm tra $E^* = E$. Thật vậy, nếu thay thế các giá trị U, S từ các công thức (2.11) và (2.20) vào công thức (2.22) ta được:

$$\begin{aligned} R^* &= (UY)^E \ \alpha^S \ mod\ p \\ &= \left(\prod_{i=1}^{m} {y_i}^{\lambda_i} \alpha^X \right)^E \ \alpha^{S' + \sum_{i=1}^{m} S_i} \\ &= \alpha^{(\sum_{i=1}^{m} x_i \lambda_i + X)E} \alpha^{K - XE + \sum_{i=1}^{m}(k_i - x_i \lambda_i E)} \\ &= \alpha^{(\sum_{i=1}^{m} x_i \lambda_i E)} \alpha^{XE} \ \alpha^K \alpha^{-XE} \alpha^{\sum_{i=1}^{m} k_i} \alpha^{-(\sum_{i=1}^{m} x_i \lambda_i E)} \\ &= \alpha^K \alpha^{\sum_{i=1}^{m} k_i} \\ &= \alpha^{K + \sum_{i=1}^{m} k_i} \\ &= R \end{aligned}$$

Suy ra: $E^* = F_H(M \| R^* \| U) = F_H(M \| R \| U) = E$

Vậy biểu thức $E^* = E$ luôn tồn tại: Chứng tỏ tính đúng của thủ tục kiểm tra chữ ký, hay tính đúng của lược đồ GDS-2.1, luôn được đảm bảo.

2.1.3. Lược đồ chữ ký số 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 $Y_j = \alpha^{X_j} \ mod\ p$. 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 $i = 1, 2, \dots, m_j$) trong nhóm ký thứ j có private key là x_{ji} ($|x| \geq 256\ bít$) và public key tương ứng là $y_{ji} = \alpha^{x_{ji}}\ mod\ p$.

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 tài liệu 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 công thức (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

$$R_j = R_j' \prod_{i=1}^{m_j} R_{ji}\ mod\ p \tag{2.25}$$

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 của tập thể ký.

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

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

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

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

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 cá nhân 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 công đoạn cuối cùng:

- Kiểm tra tính hợp lệ của các thành phần chia sẻ 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:

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

Vậy bộ 3 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 tài liệu 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 được chia sẻ bởi tất cả các nhóm ký:

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

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

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

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

$$E^* = F_H(M \| R^* \| U) \tag{2.34}$$

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.

- **Chứng minh tính đúng của lược đồ RCS.01-2.1**

Tính đúng của lược đồ chữ ký tập thể đại diện này thể hiện qua: i) Sự tồn tại của công thức kiểm tra chữ ký chia sẻ S_j của mỗi nhóm ký (2.29); và ii) Sự tồn tại của biểu thức kiểm tra $E^* = E$. Cụ thể như sau:

a) Tính đúng của công thức kiểm tra chữ ký được chia sẻ của các nhóm ký:

Nếu S_j là hợp lệ thì công thức (2.30) luôn tồn tại. Thật vậy:

$$R_j = \left(U_j Y_j\right)^E \alpha^{S_j} = {U_j}^E \alpha^{X_j E} \alpha^{\left({S'}_j + \sum_{i=1}^{m_j} S_{ji}\right)}$$
$$= \prod_{i=1}^{m_j} \left({y_{ji}}^{\lambda_{ji} E}\right) \alpha^{X_j E} \alpha^{(K_j - X_j E) + \sum_{i=1}^{m_j} (k_{ji} - x_{ji}\lambda_{ji} E)}$$
$$= \alpha^{\sum_{i=1}^{m_j} x_{ji}\lambda_{ji} E} \alpha^{X_j E} \alpha^{(K_j - X_j E) + \sum_{i=1}^{m_j} (k_{ji} - x_{ji}\lambda_{ji} E)}$$
$$= \alpha^{\left(K_j + \sum_{i=1}^{m_j} k_{ji}\right)}$$
$$= R'_j \prod_{i=1}^{m_j} R_{ji} = R_j$$

Vậy công thức (2.30) luôn tồn tại. Có nghĩa, tính đúng của công thức kiểm tra (2.30) được đảm bảo.

b) Tính đúng của thủ tục kiểm tra chữ ký:

Dễ thấy, biểu thức kiểm tra chữ ký $E^* = E$ luôn tồn tại. Thật vậy:

$$R^* = (UY_{col})^E \alpha^S = U^E \alpha^{\sum_{j=1}^{g} X_j E} \alpha^{\sum_{j=1}^{g} (S_j + \sum_{i=1}^{m} S_{ji})}$$
$$= \prod_{j=1}^{g} \prod_{i=1}^{m} \left({y_{ji}}^{\lambda_{ji} E}\right) \alpha^{\sum_{j=1}^{g} X_j E} \alpha^{\sum_{j=1}^{g} [(K_j - X_j E) + \sum_{i=1}^{m} (k_{ji} - x_{ji} E)]}$$
$$= \alpha^{\sum_{j=1}^{g} \sum_{i=1}^{m} x_{ji}\lambda_{ji} E} \alpha^{\sum_{j=1}^{g} X_j E} \alpha^{\sum_{j=1}^{g} [(K_j - X_j E) + \sum_{i=1}^{m} (k_{ji} - x_{ji} E)]}$$
$$= \alpha^{\sum_{j=1}^{g} (K_j + \sum_{i=1}^{m} k_{ji})}$$
$$= \prod_{j=1}^{g} \left(\alpha^{K_j} \prod_{i=1}^{m} \alpha^{k_{ji}} \right)$$
$$= \prod_{j=1}^{g} R_j = R$$

Suy ra: $E^* = F_H(M \| R^* \| U) = F_H(M \| R \| U) = E$

Vậy biểu thức $E^* = E$ luôn tồn tại: Chứng tỏ tính đúng của thủ tục kiểm

tra chữ ký, hay tính đúng của lược đồ RCS.01-2.1, luôn được đảm bảo.

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

Lược đồ chữ ký tập thể cho nhiều nhóm ký và nhiều người ký cá nhân dưới đây được xây dựng từ hai lược đồ cơ sở đã được trình bày ở 2.1.1 và 2.1.2. Lược đồ này cũng được tham chiếu từ lược đồ RCS.01-2.1.

Chữ ký tập thể đại diện trong lược đồ RCS.01-2.1 được hình thành từ một tập thể ký gồm g nhóm ký. Chữ ký tập thể đại diện trong lược đồ RCS.02-2.1 này được hình thành từ một tập thể gồm g nhóm ký và m người ký cá nhân. Tất cả người ký của tập thể này, từ người ký thuộc nhóm ký đến những người ký đơn lẻ, đều tham gia vào việc hình thành chữ ký tập thể đại diện trên tài liệu M.

Lược đồ RCS.02-2.1 được xây dựng hoàn toàn tương tự lược đồ RCS.01-2.1, chỉ khác, mỗi người ký đơn lẻ được xem như là một nhóm ký mà ở đó chỉ có một người ký duy nhất. Do đó, giá trị U_j của người ký cá nhân j được cho bằng 1. Cho x_j là private key của người ký cá nhân thứ j và public key tương ứng của họ là y_j: $\mathrm{y_j} = \alpha^{\mathrm{x}}_{\mathrm{j}} \bmod \mathrm{p}$.

- Thủ tục sinh chữ ký tập thể cho các nhóm ký và các cá nhân ký trên tài liệu M được thực hiện tương tự như trong lược đồ RCS.01-2.1, nhưng:

Với các nhóm ký, các giá trị U_j, R_j, S_j sẽ được tính theo các công thức (2.24), (2.25) và (2.29). Với những người ký cá nhân thì: U_j được cho bằng 1 ($U_j = 1$).

Giá trị tham số ngẫu nhiên R_j được tính theo công thức: $R_j = \alpha^{k_j} \bmod p$ (thay vì sử dụng công thức (2.25)).

Giá trị S_j được tính theo công thức: $S_j = k_j - x_j E \bmod q$ (thay vì sử dụng công thức (2.29)).

- Thủ tục kiểm tra chữ ký cũng thực hiện tương tự như lược đồ RCS.01-2.1: Public key của mỗi người ký cá nhân sẽ được sử dụng để tính public key của chữ ký tập thể, Y_{col} (theo công thức (2.32)), như Y_j của các nhóm ký khác.

Dạng đầy đủ của lược đồ RCS.02-2.1 sẽ được mô tả ở các phần sau.

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

Nhiều kết quả nghiên cứu cho thấy, hệ mật mã trên đường cong Elliptic có

ưu điểm bảo mật vượt trội so với các hệ mật mã bất đối xứng khác. Hệ mật mã này đặc biệt hữu ích khi được sử dụng để xây dựng các lược đồ chữ ký số. Lược đồ chữ ký số được xây dựng dựa trên bài toán logarit rời rạc trên đường cong Elliptic cho cấp độ an toàn tương đương với khi sử dụng hệ mật mã khác nhưng có độ dài khóa nhỏ hơn rất nhiều.

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 số tập thể theo chuẩn ECDSA (Ký hiệu: CDS-2.2)

Tập tham số miền được sử dụng trong lược đồ này là: $D = (p, a, b, P, q, h)$ [8]. Giả sử có một tập thể ký gồm m người ký, muốn tạo chữ ký tập thể trên tài liệu M. m người ký này được chỉ định tham gia vào quá trình tạo ra chữ ký của tập thể ký trên tài liệu M.

Mỗi người ký (trong các thuật toán sau gọi là "signer") chọn một giá trị ngẫu nhiên $d \in [1, q-1]$ để làm private key. Public key tương ứng của mỗi signer là Q_i: $Q_i = d_i P; i = 1, 2, \dots, m$.

F_H là một hàm băm một chiều: Có thể là SHA-1 hoặc SHA- 2.

- **Thủ tục sinh chữ ký số tập thể trên tài liệu *M***

Gồm các bước sau:

1. Mỗi signer thứ i trong tập thể ký thực hiện:

- Chọn số ngẫu nhiên k_i, thỏa $k_i \in [1, q-1]$, và rồi tính R_i theo công thức:

$$R_i = k_i P \tag{2.35}$$

- Gửi R_i tới tất cả signer khác trong tập thể ký.

2. Một signer nào đó trong tập thể ký thực hiện:

- Tính giá trị ngẫu nhiên của tập thể R theo công thức:

$$R = R_1 + R_2 + \cdots + R_n = (x_R, y_R) \tag{2.36}$$

- Tính e theo công thức:

$$e = x_R H \ mod \ \delta \tag{2.37}$$

Trong đó, δ là một số nguyên tố có độ lớn $|\delta| = 160$ bít và H là giá trị băm

được tính từ tài liệu M: $H = F_H(M)$.

- Gửi giá trị e tới tất cả signer khác trong tập thể ký.

Thành phần đầu tiên của chữ ký tập thể là e.

3. Mỗi signer i trong tập thể ký tiếp tục thực hiện

- Tính thành phần chia sẻ s_i của họ theo công thức:

$$s_i = (k_i - ed_i)\ mod\ q \tag{2.38}$$

- Gửi s_i tới tất cả signer khác trong tập thể ký.

4. Một signer nào đó trong tập thể ký tính thành phần thứ hai s của chữ ký tập thể theo công thức:

$$s = s_1 + s_2 + \cdots + s_m\ mod\ q \tag{2.39}$$

Vậy cặp giá trị $(e,\ s)$ là chữ ký tập thể của tập thể ký, gồm m thành viên, trên tài liệu M. Nó đại diện cho tập thể ký này.

- **Thủ tục kiểm tra chữ ký trên tài liệu 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 của tập thể Q theo công thức:

$$Q = Q_1 + Q_2 + \cdots +\ Q_m \tag{2.40}$$

2. Tính giá trị ngẫu nhiên R' theo công thức:

$$R' = eQ + sP = (x_{R'}, y_{R'}) \tag{2.41}$$

3. Tính giá trị e' theo công thức:

$$e' =\ x_{R'}H\ mod\ \delta \tag{2.42}$$

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.

- **Chứng minh tính đúng của lược đồ CDS-2.2**

Tính đúng của lược đồ chữ ký tập thể này thể hiện thông qua sự tồn tại của biểu thức kiểm tra $e' = e$ trong thủ tục kiểm tra chữ ký tập thể.

Ta thấy:

Vì $Q = Q_1 + Q_2 + \cdots +\ Q_m$ và $s = s_1 + s_2 + \cdots + s_m$ nên:

$$R' = eQ + sP$$

$$= e\sum_{i=1}^{m} d_i P + \sum_{i=1}^{m}(k_i - ed_i)P$$
$$= \sum_{i=1}^{m} k_i P = R$$

Vì $R' = R$ nên $e' = e$ luôn tồn tại. Điều này chứng tỏ tính đúng của thủ tục kiểm tra chữ ký, hay tính đúng của lược đồ CSD-2.2, luôn được đảm bảo.

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

Cho một đường cong Elliptic thoả mãn các yêu cầu của chuẩn ECDSA và một điểm G có bậc nguyên tố lớn q thuộc đường cong.

Giả sử có một nhóm ký, gồm m người ký, muốn tạo ra chữ ký nhóm trên tài liệu M. Nhóm ký này được điều khiển bởi người quản lý nhóm (GM).

Mỗi người ký trong nhóm ký chọn ngẫu nhiên 1 số nguyên k để làm private key $k \in [1,\ p-1]$. k_i là private key của người ký thứ i, public key tương ứng của họ là P_i: $P_i = k_i G$ $(i = 1, 2, \dots, m)$. Người quản lý nhóm có private key và public key lần lượt là z và $L = zG$. L cũng chính là public key của nhóm ký, nó được sử dụng để kiểm tra tính hợp lệ của chữ ký nhóm sau này.

F_H là một hàm băm đã được chỉ định trước.

Lược đồ chữ ký nhóm dựa trên bài toán logarit rời rạc trên đường cong Elliptic sử dụng chuẩn ECDSA được mô tả như sau:

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

Gồm các bước sau:

1. GM thực hiện:

- Tính giá trị băm của tài liệu M:

$$H = F_H(M) \tag{2.43}$$

- Tính hệ số mặt nạ cho mỗi signer i trong nhóm theo công thức:

$$\lambda_i = F_H\left(H \| x_{P_i} \| F_H\left(H \| x_{P_i} \| z\right)\right) \tag{2.44}$$

- Gửi mỗi giá trị λ_i tới signer tương ứng trong nhóm ký
- Tính thành phần thứ nhất U của chữ ký nhóm theo công thức:

$$U = \sum_{i=1}^{m} \lambda_i P_i \tag{2.45}$$

2. Mỗi signer thứ i trong nhóm ký thực hiện:

- Sinh một số ngẫu nhiên ρ_i, thỏa $\rho_i < q$, và tính giá trị R_i theo công thức:

$$R_i = \rho_i G \tag{2.46}$$

- Gửi R_i lại cho GM.

3. GM tiếp tục thực hiện:

- Sinh một số ngẫu nhiên ρ', thỏa $\rho' < q$ và tính giá trị R' theo công thức:

$$R' = \rho' G \tag{2.47}$$

- Tính R và e theo các công thức:

$$R = R' + \sum_{i=1}^{m} R_i \tag{2.48}$$

$$e = F_H(M \| x_R \| x_U) \ mod \ \delta \tag{2.49}$$

Trong đó, δ là một số nguyên tố lớn ($|\delta|$ = 160 bít), x_R và x_U lần lượt là hoành độ của các điểm R và U trên đường cong Elliptic.

- Gửi giá trị e cho tất cả signer khác trong nhóm ký.

Giá trị e là thành phần thứ hai của chữ ký nhóm.

4. Mỗi signer thứ i trong nhóm ký tiếp tục thực hiện:

- Tạo thành phần chia sẻ của họ theo công thức:

$$s_i = \rho_i - e\lambda_i k_i \ mod \ q \tag{2.50}$$

- Gửi s_i cho GM.

5. GM thực hiện các công việc cuối cùng:

- Kiểm tra tính chính xác của mỗi thành phần chia sẻ s_i bằng công thức:

$$R_i = e\lambda_i P_i + s_i G \ mod \ q \tag{2.51}$$

- Nếu tất cả s_i đều hợp lệ thì giá trị của thành phần chia sẻ của GM sẽ được tính theo công thức:

$$s' = \rho' + ze \ mod \ q \tag{2.52}$$

- Tính thành phần thứ ba s của chữ ký nhóm theo công thức:

$$s = s' + \sum_{i=1}^{m} s_i \ mod \ q \tag{2.53}$$

Vậy bộ 3 giá trị (U, e, s) là chữ ký nhóm của nhóm ký, gồm m thành viên, trên tài liệu M. Nó đại diện cho nhóm ký này.

- **Thủ tục kiểm tra chữ ký nhóm trên tài liệu *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 giá trị băm của tài liệu M:

$$H = F_H(M) \tag{2.54}$$

2. Tính giá trị R^* theo công thức:

$$R^* = sG - e(U + L) \tag{2.55}$$

3. Tính giá trị e^* theo công thức:

$$e^* = F_H(M \| x_{R^*} \| x_U) \; mod \; \delta \tag{2.56}$$

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.

- **Chứng minh tính đúng của lược đồ GDS-2.2**

Tính đúng của lược đồ chữ ký nhóm này thể hiện qua: i) Sự tồn tại của công thức kiểm tra chữ ký chia sẻ s_i của mỗi signer R_i; và ii) Sự tồn tại của biểu thức kiểm tra chữ ký $e^* = e$. Cụ thể như sau:

a) Tính đúng của công thức kiểm tra chữ ký chia sẻ mỗi signer:

Dễ thấy biểu thức (2.51) luôn tồn tại. Thật vậy:

$$\begin{aligned} R_i &= e\lambda_i P_i + s_i G \\ &= e\lambda_i k_i G + (\rho_i - e\lambda_i k_i)G \\ &= \rho_i G = R_i \end{aligned}$$

b) Tính đúng của thủ tục kiểm tra chữ ký nhóm:

Dễ thấy, biểu thức kiểm tra chữ ký $e^* = e$ luôn tồn tại.

Thật vậy:

$$\begin{aligned} R^* &= sG - e(U + L) \\ &= \left(s' + \sum_{i=1}^{m} s_i\right)G - e\left(\sum_{i=1}^{m} \lambda_i P_i + zG\right) \\ &= \left(\rho' + ze + \sum_{i=1}^{m} (\rho_i - e\lambda_i k_i)\right)G - e\left(\sum_{i=1}^{m} \lambda_i k_i G + zG\right) \\ &= \left(\rho' + \sum_{i=1}^{m} \rho_i\right)G \end{aligned}$$

$$= R' + \sum_{i=1}^{m} R_i = R$$

Vì $R^* = R$ nên $e^* = e$. Thật vậy:

$$e^* = F_H(M \| x_{R^*} \| x_U) \; mod \; \delta$$
$$= F_H(M \| x_R \| x_U) \; mod \; \delta = e$$

Vậy biểu thức $e^* = e$ luôn tồn tại: Điều này chứng tỏ tính đúng của thủ tục kiểm tra chữ ký, hay tính đúng của lược đồ GDS-2.2, luôn được đảm bảo.

2.2.3. Lược đồ chữ ký số 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}: $P_{ji} = k_{ji} G$.

- **Thủ tục sinh chữ ký tập thể cho các nhóm ký trên tài liệu *M***

Gồm các bước sau:

1. GM, của nhóm ký thứ j, thực hiện:

- Tạo ra các tham số mặt nạ λ_{ji} cho những signer của nhóm j theo công thức (2.44) trong thủ tục sinh chữ ký của lược đồ GDS-2.2

- Tính U_j và R_j của nhóm ký thứ j theo công thức (2.57) và (2.58):

$$U_j = \sum_{i=1}^{m_j} \lambda_{ji} P_{ji} \tag{2.57}$$

$$R_j = R'_j + \sum_{i=1}^{m_j} R_{ji} \tag{2.58}$$

- Gửi các giá trị U_j và R_j đến các GM khác trong tập thể ký.

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

$$U = \sum_{j=1}^{g} U_j \quad (2.59)$$

$$R = \sum_{j=1}^{g} R_j \quad (2.60)$$

$$e = F_H(M \| x_R \| x_U) \; mod \; \delta \quad (2.61)$$

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

Thành phần thứ nhất và thứ hai của chữ ký tập thể này là U và e.

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

- Tính giá trị thành phần chia sẻ của nhóm ký đó theo công thức:

$$s_j = s'_j + \sum_{j=1}^{m_j} s_{ji} \; mod \; q \quad (2.62)$$

Trong đó, s_{ji} là thành phần chia sẻ của signer thứ i thuộc nhóm ký thứ j.

- Gửi giá trị s_j đến tất cả GM khác trong tập thể ký.

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

- Kiểm tra tính hợp lệ của các thành phần chia sẻ s_j bằng công thức:

$$R_j = s_j G - e(U_j + L_j) \; mod \; q \quad (2.63)$$

- 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:

$$s = \sum_{j=1}^{g} s_j \; mod \; q \quad (2.64)$$

Vậy bộ 3 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 tài liệu 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 như sau:

1. Tính public key tập thể L của tập thể ký theo công thức:

$$L = \sum_{j=1}^{g} L_j \quad (2.65)$$

2. Tính giá trị R^* theo công thức:

$$R^* = sG - (U + L)e \tag{2.66}$$

3. Tính giá trị e^* theo công thức:

$$e^* = F_H(M \| x_{R^*} \| x_U) \tag{2.67}$$

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.

- **Chứng minh tính đúng của lược đồ RCS.01-2.2**

Tính đúng của lược đồ chữ ký tập thể đại diện này thể hiện qua: i) Sự tồn tại của công thức kiểm tra chữ ký chia sẻ S_j của mỗi nhóm ký R_j (2.63); và ii) Sự tồn tại của biểu thức kiểm tra $e^* = e$. Cụ thể như sau:

a) Chứng minh tính đúng của công thức kiểm tra thành phần chia sẻ:

Dễ thấy biểu thức kiểm tra (2.63) luôn tồn tại. Thật vậy:

$$\begin{aligned}
R_j &= s_j G - e\left(U_j + L_j\right) \\
&= \left(s'_j + \sum_{i=1}^{m_j} s_{ji}\right) G - e\left(\sum_{i=1}^{m_j} \lambda_{ji} P_{ji} + z_j G\right) \\
&= \left(\rho'_j + z_j e + \sum_{i=1}^{m_j} \left(\rho_{ji} - e\lambda_{ji} k_{ji}\right)\right) G - e\left(\sum_{i=1}^{m_j} \lambda_{ji} k_{ji} G + z_j G\right) \\
&= \left(\rho'_j + \sum_{i=1}^{m_j} \rho_{ji}\right) G \\
&= R'_j + \sum_{i=1}^{m_j} R_{ji} = R_j
\end{aligned}$$

b) Chứng minh tính đúng của thủ tục kiểm tra chữ ký:

Dễ thấy, biểu thức kiểm tra chữ ký $e^* = e$ luôn tồn tại.

Thật vậy: Thế các giá trị s, U, L từ các công thức (2.64), (2.59) và (2.65) vào công thức kiểm tra R^* (2.66) ta nhận được:

$$\begin{aligned}
R^* &= sG - (U + L)e \\
&= \sum_{j=1}^{g} s_j G - \left(\sum_{j=1}^{g} U_j + \sum_{j=1}^{g} L_j\right) e
\end{aligned}$$

$$= \sum_{j=1}^{g} s_j G - \sum_{j=1}^{g} (U_j + L_j)e$$

$$= \sum_{j=1}^{g} (s_j G - (U_j + L_j)e)$$

$$= \sum_{j=1}^{g} R_j = R$$

Suy ra: $e^* = F_H(M \| x_{R^*} \| x_U) \ mod \ \delta$

$= F_H(M \| x_R \| x_U) \ mod \ \delta = e$

Vậy biểu thức $e^* = e$ luôn tồn tại: Điều này chứng tỏ tính đúng của thủ tục kiểm tra chữ ký, hay tính đúng của lược đồ RCS.01-2.2, luôn được đảm bảo.

2.2.4. Lược đồ chữ ký số 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 $= 1, 2, \ \dots,$ g) và mỗi người ký cá nhân được xem như một nhóm ký mà chỉ có một thành viên duy nhất.

Mỗi signer thứ i trong nhóm ký sở hữu một private key là k_{ji} và public key tương ứng là của họ là $P_{ji} = k_{ji}G$, với $i = 1, \dots, m$. 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 ($j = g + 1, g + 2, \dots, g + m$). 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.

- **Thủ tục sinh chữ ký tập thể cho nhiều nhóm ký và nhiều cá nhân ký trên tài liệu *M***

Gồm các bước sau:

1a. GM của mỗi nhóm ký j thực hiện:

- Tạo tham số mặt nạ λ_{ji} cho mỗi signer của nhóm j theo công thức (2.44) (λ_{ji} là hệ số mặt nạ của signer thứ i trong nhóm ký thứ j)

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

$$U_j = \sum_{i=1}^{m_j} \lambda_{ji} P_{ji} \tag{2.68}$$

U_j là thành phần chia sẻ của nhóm ký thứ j để tạo thành phần đầu tiên của chữ ký tập thể.

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

$$R_j = R'_j + \sum_{i=1}^{m_j} R_{ji} \tag{2.69}$$

R_j là thành phần chia sẻ của nhóm ký thứ j để tạo tham số ngẫu nhiên của chữ ký tập thể.

- Gửi giá trị U_j và R_j cho tất cả các quản lý khác và các cá nhân ký.

1b. Mỗi cá nhân ký thứ j thực hiện các công việc sau:

- Sinh một giá trị ngẫu nhiên ρ_j, thỏa $\rho_j < q$ và tính giá trị ngẫu nhiên R_j theo công thức:

$$R_j = \rho_j G \tag{2.70}$$

- Gửi giá trị R_j tới tất cả những GM và những cá nhân ký khác trong tập thể ký.

2. Một GM hoặc một cá nhân ký nào đó trong tập thể ký tính các giá trị U, R và e theo các công thức:

$$U = \sum_{j=1}^{g+m} U_j \tag{2.71}$$

$$R = \sum_{j=1}^{g+m} R_j \tag{2.72}$$

$$e = F_H(M \| x_R \| x_U) \bmod \delta \tag{2.73}$$

Trong đó, δ là một số nguyên tố lớn ($|\delta| = 160\ bít$); $U_j = \lambda_j P_j$ khi $j = g+1, g+2, \dots, g+m$).

U và e là thành phần thứ nhất và thứ hai của chữ ký nhóm.

3a. GM của mỗi nhóm thứ j thực hiện:

- Tính thành phần chia sẻ s_j của nhóm j theo công thức:

$$s_j = s_j' + \sum_{i=1}^{m_i} s_{ji} \; mod \; q \tag{2.74}$$

với s_{ji} là thành phần chia sẻ của cá nhân ký thứ i trong nhóm thứ j.

- Gửi s_j cho các GM và các cá nhân ký khác trong tập thể ký.

3b. Mỗi cá nhân ký thứ j $(j = g+1, g+2, \dots, g+m)$ thực hiện:

- Tính thành phần chia sẻ s_j của họ theo công thức:

$$s_j = \rho_j - e\lambda_j k_j \; mod \; q \tag{2.75}$$

- Gửi s_j cho những GM và cá nhân ký khác trong tập thể ký.

4. Một GM hoặc một cá nhân ký nào đó trong tập thể ký thực hiện:

- Kiểm tra tính hợp lệ của mỗi s_j theo công thức:

$$R_j = s_j G - e(U_j + L_j) \; mod \; q \tag{2.76}$$

với $j = 1, 2, \dots, g$ và

$$R_j = e\lambda_j P_j + s_j G \; mod \; q \tag{2.77}$$

với $j = g+1, g+2, \dots, g+m$

- Nếu tất cả s_j đều thoả mãn, thành phần thứ ba của chữ ký nhóm sẽ được tính theo công thức:

$$s = \sum_{j=1}^{g+m} s_j \; mod \; q \tag{2.78}$$

Vậy bộ 3 giá trị $(\mathrm{U}, \mathrm{e}, \mathrm{s})$ là chữ ký tập thể đại diện, của một tập thể gồm g nhóm ký và m cá nhân ký, trên tài liệu M (dạng chữ ký này còn được gọi là, chữ ký tập thể được chia sẻ bởi nhiều nhóm và nhiều cá nhân ký). Nó đại diện cho tập thể ký này.

- **Thủ tục kiểm tra chữ ký tập thể cho nhiều nhóm ký và nhiều cá nhân ký trên tài liệu *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 tậ 4p thể ký theo công thức:

$$L = \sum_{j=1}^{g} L_j \tag{2.79}$$

2. Tính giá trị tham số ngẫu nhiên R^* theo công thức:

$$R^* = sG - (U + L)e \quad (2.80)$$

3. Tính e^* theo công thức:

$$e^* = F_H(M \| x_{R^*} \| x_U) \quad (2.81)$$

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.

- **Chứng minh tính đúng của lược đồ chữ ký RCS.02-2.2**

Tính đúng của lược đồ chữ ký tập thể đại diện này thể hiện qua: i) Sự tồn tại của công thức kiểm tra chữ ký chia sẻ s_j của mỗi nhóm ký R_j (2.76); ii) Sự tồn tại của công thức kiểm tra chữ ký chia sẻ s_j của mỗi cá nhân ký R_j (2.77) và iii) Sự tồn tại của biểu thức kiểm tra $e^* = e$. Cụ thể như sau:

a) Tính đúng của công thức kiểm tra chữ ký chia sẻ của mỗi trưởng nhóm:

Dễ thấy biểu thức kiểm tra R_i luôn tồn tại. Thật vậy:

$$\begin{aligned} R_j &= s_j G - e(U_j + L_j) \\ &= \left(s'_j + \sum_{i=1}^{m_j} s_{ji}\right) G - e\left(\sum_{i=1}^{m_j} \lambda_{ji} P_{ji} + z_j G\right) \\ &= \left(\rho'_j + z_j e + \textstyle\sum_{i=1}^{m_j} (\rho_{ji} - e\lambda_{ji} k_{ji})\right) G - e\left(\textstyle\sum_{i=1}^{m_j} \lambda_{ji} k_{ji} G + z_j G\right) \\ &= \left(\rho'_j + \textstyle\sum_{i=1}^{m_j} \rho_{ji}\right) G \\ &= R'_j + \textstyle\sum_{i=1}^{m_j} R_{ji} = R_j \end{aligned}$$

b) Tính đúng của công thức kiểm tra chữ ký chia sẻ mỗi signer:

Dễ thấy biểu thức kiểm tra R_i luôn tồn tại. Thật vậy:

$$\begin{aligned} R_j &= s_j G - e\lambda_j P_j \\ &= (\rho_j - e\lambda_j k_j) G - e\lambda_j k_j G \\ &= \rho_j G = R_j \end{aligned}$$

c) Tính đúng của thủ tục kiểm tra chữ ký tập thể đại diện:

Dễ thấy, biểu thức kiểm tra chữ ký $e^* = e$ luôn tồn tại. Ta thấy:

$$\begin{aligned} R^* &= sG - (U + L)e \\ &= \sum_{j=1}^{g+m} s_j G - \left(\sum_{j=1}^{g+m} U_j + \sum_{j=1}^{g} L_j\right) e \end{aligned}$$

$$= \left(\sum_{j=1}^{g} s_j G - \sum_{j=1}^{g} (U_j + L_j) e \right) + \left(\sum_{j=g+1}^{g+m} s_j G - \sum_{j=g+1}^{g+m} U_j e \right)$$

$$= \sum_{j=1}^{g} (s_j G - (U_j + L_j) e) + \sum_{j=g+1}^{g+m} (s_j G - \lambda_j P_j e)$$

$$= \sum_{j=1}^{g} R_j + \sum_{j=g+1}^{g+m} R_j = R$$

Và tính: $e^* = F_H(M \| x_{R^*} \| x_U) \; mod \; \delta$

$= F_H(M \| x_R \| x_U) \; mod \; \delta = e$

Vậy biểu thức $e^* = e$ luôn tồn tại: Điều này chứng tỏ tính đúng của thủ tục kiểm tra chữ ký, hay tính đúng của lược đồ RCS.02-2.2, luôn được đảm bảo.

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

2.3.1. Khả năng chống tấn công từ bên trong của lược đồ chữ ký số tập thể

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 thứ m):**

Giả sử có $m - 1$ người ký, trong một tập thể ký gồm m thành viên, muốn tạo một chữ ký tập thể trên tài liệu M. Tức là, $m - 1$ người này muốn giả mạo chữ ký của người ký còn lại, tạm gọi là người ký thứ m, trong tập thể ký.

Trong trường hợp này, public key của tập thể ký có thể được viết như sau: $Y = Y^* Y_m \; mod \; p$, trong đó $Y^* = \prod_{i=1}^{m-1} Y_i \; mod \; p$ và Y_m là pubic key của người ký m.

Để việc giả mạo thành công thì $m - 1$ người ký phải tạo cho được một cặp số (E^*, S^*), tương ứng một chữ ký tập thể, thỏa mãn các công thức kiểm tra. Cụ thể là hai công thức tính R^* và E^*:

$$R^* = Y^{-E^*} g^{S^*} \; mod \; p \qquad (2.82)$$

$$E^* = F_H(M\|R^*) \quad (2.83)$$

Giả sử $m-1$ người ký có thể "tính" ra được một chữ ký tập thể hợp lệ (E^*, S^*) tương ứng với public key của tập thể ký: $Y = \prod_{i=1}^{m} Y_i \ mod\ p$. Chữ ký tập thể này thỏa mãn quan hệ sau:

$$\begin{aligned} R^* &\equiv Y^{-E^*} g^{S^*} \equiv (Y^* Y_m)^{-E^*} g^{S^*} \\ &\equiv {Y^*}^{-E^*} {Y_m}^{-E^*} g^{S^*} \equiv g^{-E^* \sum_{i=1}^{m-1} x_i} {Y_m}^{-E^*} g^{S^*} \\ &\equiv {Y_m}^{-E^*} g^{S^* - E^* \sum_{i=1}^{m-1} x_i} \ mod\ p \\ &\Rightarrow R^* \equiv {Y_m}^{-E^*} g^{S^{**}}, \end{aligned} \quad (2.84)$$

trong đó: $S^{**} = S^* - E^* \sum_{i=1}^{m-1} x_i$.

Như vậy, nhóm $m-1$ người ký giả mạo tập thể này đã tính ra được chữ ký (E^*, S^{**}) là một chữ ký hợp lệ, trên tài liệu M, của người ký thứ m (vì $E^* = F_H(M||R^*)$ và cặp số (E^*, S^{**}) thỏa mãn thủ tục kiểm tra của lược đồ chữ ký cơ sở (lược đồ chữ ký của Schnorr) dùng để xây dựng lược đồ chữ ký tập thể này).

Do đó, bất kỳ thành công nào trong việc phá vỡ giao thức chữ ký tập thể này cũng sẽ phá vỡ thuật toán chữ ký cơ sở [49]. Nhưng, như đã biết, lược đồ chữ ký Schnorr đã được chứng minh là an toàn nên lược đồ chữ ký tập thể này cũng được xem là an toàn trước những tấn công về giả mạo chữ ký.

- **Loại tấn công thứ hai (Tìm private key của người ký thứ m):**

Giả sử có $m-1$ người ký, chia sẻ một chữ ký tập thể (R, S) nào đó với người ký thứ m, đang tìm cách tính private key của người ký thứ m. Tạm gọi $m-1$ người ký này là "Nhóm tấn công".

Nhóm tấn công này biết các giá trị R_m và S_m được sinh ra bởi người ký thứ m. Các giá trị này thỏa mãn biểu thức $R_m = {Y_m}^{-E} g^{S_m} \ mod\ p$, trong đó các giá trị R_m và E nằm ngoài tầm kiểm soát của nhóm tấn công (vì giá trị R_m được tính theo công thức: $R_m = g^{t_m} \ mod\ p$, mà t_m là số ngẫu nhiên được tạo bởi người ký thứ m; và E là đầu ra của thuật toán hàm băm).

Giả sử hàm băm được sử dụng trong giao thức là đủ an toàn, nên nhóm tấn công không thể chọn được một giá trị R mà có thể tạo ra một giá trị E được chọn đặc biệt nào đó. Điều này có nghĩa là, giống như trong trường hợp lược đồ chữ ký của Schnorr [49], để tính ra được private key của người ký thứ m thì nhóm tấn công giải được bài toán logarit rời rạc, để: i) tìm $t_m = log\ R_m$, rồi tính $x_m = E^{-1}(S_m - t_m) \ mod\ q$; hoặc ii) để tính $x_m = log\ Y_m$. Nhưng, như đã biết, bài toán

logarit rời rạc là một bài toán khó.

Tóm lại, do tính khó giải của bài toán logarit rời rạc nên nhóm tấn công không có thể tính được private key của người ký thứ m. Tức là, lược đồ chữ ký tập thể này chống lại được kiểu tấn công "tìm private key của người ký thứ m".

2.3.2. Một số ưu điểm bảo mật của lược đồ chữ ký số nhóm GDS-2.1

Hoạt động của lược đồ cho thấy nó có những đặc trưng bảo mật như sau:

- Hoàn toàn không có giá trị bảo mật nào, private keys và secret keys, cần phải trao đổi hoặc cần phải chia sẻ giữa các thành viên của nhóm ký hoặc giữa thành viên nhóm ký với người quản lý của nhóm ký đó. Do đó, môi trường Internet là đủ để triển khai lược đồ này.
- Việc sử dụng public key Y của người quản lý nhóm như là public key của nhóm ký làm cho cả việc kiểm tra tính hợp lệ của chữ ký (của bên kiểm tra) và việc thay đổi tập thành viên tham gia hình thành chữ ký (của người quản lý nhóm) đều trở nên tiện lợi hơn rất nhiều.
- Quá trình hình thành các thành phần, đặc biệt là thành phần S, của chữ ký đều được thực hiện qua 2 bước: i) Đầu tiên, tất cả thành viên nhóm ký, được chỉ định, đều tham gia vào việc tạo ra tiền chữ ký nhóm (Group digital pre-signature) theo sự điều khiển của người trưởng nhóm và ii) Sau đó, người quản lý nhóm tiến hành tạo ra chữ ký nhóm (Group digital signature) của nhóm ký, sau khi đã xác nhận tính đúng của chữ ký của tất cả thành viên. Tất nhiên trong chữ ký nhóm cuối cùng có kèm theo thông tin và chữ ký của người trưởng nhóm. Điều này chứng tỏ, khó có thể giả mạo thành viên ký với lược đồ này. Đồng thời, tính chịu trách nhiệm và tính đại diện của người trưởng nhóm ở đây là rất cao.
- Thành phần U của chữ ký chứa thông tin của tất cả thành viên của nhóm ký đã tham gia vào việc hình thành chữ ký nhóm. Do đó, để định danh tập thành viên này người quản lý nhóm chỉ cần "mở" thành phần U để xem xét. Việc "mở" này chỉ có thể thực hiện bởi người quản lý nhóm bởi trong U có chứa các λ_i, mà trong λ_i có chứa private key X của người này. Điều này có nghĩa, thông tin của những thành viên đã tham gia trong quá trình hình thành chữ ký nhóm được bí mật bởi người quản lý nhóm.

Thực tế, nếu tất cả thành viên đã tham gia vào việc hình thành chữ ký thỏa thuận phối hợp với nhau thì họ cũng có thể "mở" chữ ký do họ tạo ra.

- Hệ số mặt nạ λ có các ưu điểm bảo mật sau đây: i) Chỉ những thành viên nhận được λ từ trưởng nhóm thì mới được quyền tham gia vào quá trình tạo ra chữ ký nhóm. Khó có ai có thể giả mạo được λ để được tham gia tạo chữ ký nhóm vì trong λ có chứa private key (X) của trưởng nhóm; ii) Public key của những thành viên tham gia tạo chữ ký đã bị "che" bởi λ nên danh tính của thành viên tham gia tạo chữ ký nhóm được giữ bí mật bởi trưởng nhóm; iii) Chỉ những thành viên nhận được E và nhận đúng λ thì mới có thể tạo được chữ ký cá nhân S_i hợp lệ, vượt qua được bước kiểm tra chữ ký thành viên của trưởng nhóm. Như vậy λ góp phần làm cho ý đồ giả mạo được chữ ký thành viên của kẻ tấn công trở nên khó khăn hơn; và iv) Nếu một thành viên nào đó nhận được λ, và có thể E, đến từ một trưởng nhóm giả mạo thì chữ ký cá nhân "hợp lệ" của họ S_i cũng không vượt qua được bước kiểm tra của trưởng nhóm "thật". Nếu trưởng nhóm giả mạo đánh lừa được tất cả thành viên nhóm để tạo ra chữ ký giả mạo (U, E, S) thì chữ ký này cũng sẽ không vượt qua công thức kiểm tra chữ ký của bên kiểm tra, vì ở đây sử dụng public key Y của trưởng nhóm "thật". Điều này giúp cho mỗi thành viên nhóm ký có thể xác thực người trưởng nhóm của họ.
- Các tham số ngẫu nhiên k_i và K được xem như private key thứ hai của thành viên nhóm ký và trưởng nhóm. Nó được chọn ngẫu nhiên cho mỗi lần tạo chữ ký, tức là nó chỉ được sử dụng một lần duy nhất. Điều này dẫn đến thành phần R cũng ngẫu nhiên và duy nhất trong mỗi chữ ký nhóm được tạo trên tài liệu M. Tính "sử dụng một lần" ở đây giúp nhóm ký có thể tạo ra các chữ ký khác nhau trên các tài liệu khác nhau, dù họ vẫn sử dụng cùng một cặp khóa public key và private key ban đầu. Như vậy kẻ tấn công khó có thể sử dụng phương pháp sưu tập chữ ký của nhóm ký trên các tài liệu khác nhau để từ đó tìm ra các thành phần bí mật trong tập chữ ký nhận được.

Phần này đã chỉ ra một số ưu điểm bảo mật của lược đồ chữ ký nhóm GDS-2.1, nhưng điều này cũng đúng với các lược đồ chữ ký nhóm GDS-2.2.

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

Các lược đồ chữ ký tập thể đại diện trong chương này được xây dựng dựa trên bài toán logarit rời rạc và các chuẩn chữ ký số theo bài toán logarit rời rạc nên nó thừa hưởng đầy đủ ưu điểm bảo mật và khả năng chống tấn công của bài toán khó đã nêu. Ngoài ra, lược đồ chữ ký tập thể đại diện được xây dựng từ hai lược

đồ cơ sở, chữ ký tập thể và chữ ký nhóm, nên nó cũng có những ưu điểm bảo mật và khả năng chống tấn công (mục 2.3.1 và 2.3.2) của các lược đồ này.

2.3.4. Đánh giá hiệu năng tính toán của lược đồ chữ ký số 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	$U = \sum_{j=1}^{g}(32m_j)\,T_m$ $e = [\sum_{j=1}^{g}(29m_j + 29) + 1]\,T_m$	$(59 + 0.12g)T_m$

	$s = \sum_{j=1}^{g}(61m_j + 1)\,T_m$ $Sum = [\sum_{j=1}^{g}(122m_j + 30) + 1]\,T_m$	
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 (RCS.01-2.1 và RCS.01-2.2) và lược đồ chữ ký tập thể cho nhiều nhóm ký và nhiều người ký cá nhân (RCS.02-2.1 và RCS.02-2.2).

Chương 2 cũng trình bày chi tiết về các lược đồ chữ ký tập thể (CDS-2.1 và CDS-2.2) và các lược đồ chữ ký nhóm (GDS-2.1 và GDS-2.2). 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: [CT2], [CT3], [CT7], [CT12].

CHƯƠNG 3:

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

Chương 2 đã cho thấy, có thể sử dụng vấn đề khó của các bài toán logarit rời rạc để xây dựng lược đồ chữ ký tập thể đại diện. 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 2 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). Như vậy trong chương 3 này, luận án sẽ trình bày những vấn đề sau: i) Xây dựng các lược đồ chữ ký tập thể đại diện dựa trên bài toán tìm căn modulo nguyên tố lớn theo hai cấu trúc modulo nguyên tố khác nhau; ii) Xây dựng các lược đồ cơ sở liên quan: Lược đồ chữ ký cá nhân, lược đồ chữ ký tập thể, lược đồ chữ ký nhóm và iii) Đánh giá mức an toàn và hiệu năng tính toán của các lược đồ đã được xây dựng.

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 trong [70]. Cụ thể, $p = Nk^2 + 1$, với k là một số nguyên tố lớn ($|k| \geq 160$ bít) và N là một số chẵn sao cho độ lớn của p thỏa mãn $|p| \geq 1024$ bít.

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, $|p| \geq 1024$ bít, độ lớn của E bằng độ lớn của δ, $|\delta| \geq 160$

bít, 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)

Phần này luận án sử dụng lược đồ chữ ký cá nhân được mô tả trong [70], và lược đồ chữ ký tập thể được đề xuất ở [71], để xây dựng lược đồ chữ ký tập thể cho một tập thể ký gồm s thành viên. Thành viên j trong tập thể ký này sở hữu khóa bí riêng x_j, $x_j < p$, và công khai y_j: $y_j = x_j^k \ mod\ p$, với j = 1, 2, …, s.

Giả sử tài liệu M cần được ký đồng thời bởi m thành viên (signer) của tập thể ký gồm s thành viên ($m < s$). Mỗi thành viên sở hữu một private key x_{α_j}và public key tương ứng y_{α_j}: $y_{\alpha_j} = x_{\alpha_j}^k \ mod\ p$.

- **Thủ tục sinh chữ ký số tập thể trên tài liệu M:**

Gồm các bước sau:

1. Mỗi signer thứ α_j thực hiện:

- Chọn một giá trị ngẫu nhiên t_{α_j}, thỏa $t_{\alpha_j} < p$, và tính giá trị công khai R_{α_j} theo công thức:

$$R_{\alpha_j} = t_{\alpha_j}^k \ mod\ p \tag{3.1}$$

- Gửi R_{α_j} đến tất cả signer khác trong tập thể ký.

2. Một signer nào đó trong tập thể ký, hoặc tất cả, thực hiện:

- Tính giá trị ngẫu nhiên chung của tập thể R theo công thức:

$$R = \prod_{j=1}^{m} R_{\alpha_j} \ mod\ p \tag{3.2}$$

- Tính thành phần đầu tiên E của chữ ký tập thể theo công thức:

$$E = f(R, M) = RH \ mod\ \delta \tag{3.3}$$

Với δ là một số nguyên tố lớn, có độ lớn: |δ| = 160 bít và f là một hàm nén đã được chỉ định trước; và H là giá trị băm từ tài liệu M ($H = F_{\mathrm{H}}(M)$).

3. Mỗi signer thứ α_j tiếp tục thực hiện:

- Tính giá trị thành phần chia sẻ cá nhân S_{α_j} theo công thức:

$$S_{\alpha_j} = x_{\alpha_j}^{f(R,M)} t_{\alpha_j} \ mod\ p \tag{3.4}$$

- Gửi S_{α_j} đến tất cả signer khác trong tập thể ký.

4. Một signer nào đó trong tập thể ký, hoặc tất cả, tính thành phần thứ hai

của chữ ký tập thể theo công thức:

$$S = \prod_{j=1}^{m} S_{\alpha_j} \, mod \, p \tag{3.5}$$

Vậy cặp giá trị (E, S) là chữ ký tập thể của tập thể ký gồm m người ký trên tài liệu M. Độ lớn của chữ ký là: $|E| + |S| = |p| + |\delta| \sim |p|$.

- **Thủ tục kiểm tra chữ ký số tập thể được thực hiện như sau.**

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 theo công thức:

$$y = \prod_{j=1}^{m} y_{\alpha_j} \, mod \, p \tag{3.6}$$

2. Tính giá trị R' theo công thức:

$$R' = S^k y^{-E} \, mod \, p \tag{3.7}$$

3. Tính giá trị E' theo công thức:

$$E' = f(R', M) = R'H \, mod \, \delta \tag{3.8}$$

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.

- **Chứng minh tính đúng của lược đồ CDS-3.1:**

Ở đây chỉ cần chứng minh sự tồn tại của biểu thức so sánh $E' = E$. Dễ thấy $R' = R$ luôn tồn tại. Thật vậy:

$$\begin{aligned} R' &= S^k y^{-E} \, mod \, p \\ &= \prod_{j=1}^{m} \left(x_{\alpha_j}^{E} t_{\alpha_j} \right)^k x_{\alpha_j}^{-kE} \, mod \, p \\ &= t_{\alpha_j}^{k} \, mod \, p \\ &= R \end{aligned}$$

Vì $R' =$ R nên $E' = E$ (vì: $E' = f(R', M) = R'H \, mod \, \delta$).

Vậy tính đúng của thủ tục kiểm tra, hay tính đúng của lược đồ CDS-3.1 được đảm bảo.

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

Lược đồ này cho phép tạo ra một chữ ký nhóm, trên tài liệu M, đại diện cho một nhóm ký gồm m thành viên, được gọi là nhóm ký. Quá trình tạo ra chữ ký nhóm cho nhóm ký này được điều hành người trưởng nhóm (GM).

Mỗi thành viên của nhóm ký sở hữu cặp private key, public key: x_i và y_i, $i = 1, 2, \dots, m$: $y_i = x_i^k \ mod \ p$. Tương tự, X và Y là private key và public key của người quản lý nhóm. Public key Y được tính theo bài toán logarit rời rạc: $Y = X^k \ mod \ p$. Giá trị Y này cũng chính là public key của nhóm ký, vì vậy Y được dùng trong thủ tục kiểm tra chữ ký, để xác thực cho chữ ký nhóm.

Giao thức ký nhóm được mô tả như sau:

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

Gồm các bước sau:

1. GM thực hiện:

- Tính giá trị băm của tài liệu M theo công thức sau (F_H là một hàm băm)

$$H = F_H(M) \tag{3.9}$$

- Tính toán hệ số mặt nạ cho tất cả signer trong nhóm ký:

$$\lambda_i = F_H(H \ \|y_i\| \ F_H(H \ \|y_i\| \ X)) \tag{3.10}$$

- Gửi λ_i cho signer tương ứng

- Tính thành phần đầu tiên U của chữ ký nhóm:

$$U = \prod_{i=1}^{m} y_i^{\lambda_i} \ mod \ p \tag{3.11}$$

2. Mỗi signer thứ i trong nhóm ký thực hiện:

- Sinh một giá trị ngẫu nhiên t_i, thỏa $t_i < p - 1$, và rồi tính giá trị R_i theo công thức:

$$R_i = t_i^k \ mod \ p \tag{3.12}$$

- Gửi R_i cho GM.

3. GM tiếp tục thực hiện:

- Sinh một giá trị ngẫu nhiên T, sao cho $T < p - 1$, và rồi tính giá trị ngẫu nhiên cá nhân R' theo công thức:

$$R' = T^k \ mod \ p \tag{3.13}$$

- Tính thành phần ngẫu nhiên R của chữ ký nhóm theo công thức:

$$R = R' \prod_{i=1}^{m} R_i \ mod\ p = \ (T. \prod_{i=1}^{m} t_i)^k \quad (3.14)$$

- Tính giá trị E theo công thức

$$E = F_H(M \| R \| U)\ mod\ \delta \quad (3.15)$$

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

E là thành phần thứ hai của chữ ký nhóm.

- Gửi E cho tất cả signer trong nhóm ký.

4. Mỗi signer thứ i trong nhóm ký tiếp tục thực hiện

- Tính thành phần chia sẻ cá nhân S_i theo công thức:

$$S_i = x_i^{E\lambda_i}.t_i\ mod\ p \quad (3.16)$$

- Gửi S_i cho GM.

5. GM thực hiện các công việc cuối cùng

- Xác thực tính đúng của mỗi thành phần chia sẻ S_i của tất cả signer trong nhóm ký theo công thức:

$$R_i = S_i^k y_i^{-E\lambda_i}\ mod\ p \quad (3.17)$$

- Nếu tất cả S_i đều thỏa mãn công thức kiểm tra thì tính thành phần chia sẻ cá nhân S' theo công thức:

$$S' = X^E.T\ mod\ p \quad (3.18)$$

- Tính thành phần thứ ba S của chữ ký nhóm theo công thức:

$$S = S'. \prod_{i=1}^{m} S_i\ mod\ p \quad (3.19)$$

Vậy bộ giá trị (U, E, S) là chữ ký nhóm của nhóm ký gồm m thành viên trên tài liệu M.

- **Thủ tục kiểm tra chữ ký nhóm trên tài liệu *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 giá trị băm của tài liệu M theo công thức:

$$H = F_H(M) \quad (3.20)$$

2. Tính public key tập thể Y theo công thức:

$$R^* = S^k(YU)^{-E}\ mod\ p \quad (3.21)$$

3. Tính giá trị E^* theo công thức:

$$E^* = F_H(\mathrm{M} \,\|R^*\|\, U) \tag{3.22}$$

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.

- **Chứng minh tính đúng của lược đồ GDS-3.1**

Tính đúng của lược đồ chữ ký nhóm này thể hiện qua: i) Sự tồn tại của công thức kiểm tra chữ ký chia sẻ s_i của mỗi signer R_i (3.17); và ii) Sự tồn tại của biểu thức kiểm tra chữ ký $E^* = E$. Cụ thể như sau:

a) Tính đúng của công thức kiểm tra thành phần chia sẻ

Dễ thấy biểu thức kiểm tra chữ ký R_i (3.17) luôn tồn tại. Thật vậy:

$$\begin{aligned} R_i &= S_i^k y_i^{-E\lambda_i} \; mod\; p \\ &= x_i^{E\lambda_i k} t_i^k x_i^{-k\lambda_i E} \; mod\; p \\ &= t^k \; mod\; p \\ &= R_i \end{aligned}$$

b) Tính đúng của thủ tục kiểm tra chữ ký

Dễ thấy biểu thức $E^* = E$ luôn tồn tại. Thật vậy:

$$\begin{aligned} R^* &= S^k\,(YU)^{-E} \; mod\; p \\ &= (X^E . T \prod_{i=1}^{m} x_i^{E\lambda_i} . t_i)^k (X^k . T \prod_{i=1}^{m} y_i^{\lambda_i})^{-E} \text{mod p} \\ &= X^{kE} . (T \prod_{i=1}^{m} x_i^{E\lambda_i} . t_i)^k X^{-kE} . (T \prod_{i=1}^{m} y_i^{k\lambda_i})^{-E} \text{mod p} \\ &= T^k . \prod_{i=1}^{m} t_i{}^k \; mod \\ &= R \end{aligned}$$

Vì $R^* = R$ nên $E^* = F_H(M\|R^*\|U) = F_H(M\|R\|U) = E$.

Vậy biểu thức $E^* = E$ luôn tồn tại: Điều này chứng tỏ tính đúng của thủ tục kiểm tra chữ ký luôn được đảm bảo.

Từ (a) và (b): Tính đúng của lược đồ GDS-3.1 được đảm bảo.

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 tài liệu 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 bít.

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 cho nhiều nhóm ký trên tài liệu 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.

- **Chứng minh tính đúng của lược đồ RCS.01-3.1:**

Tính đúng của lược đồ chữ ký tập thể đại diện này thể hiện qua: i) Sự tồn tại của công thức kiểm tra chữ ký chia sẻ S_{ji} được chia sẻ bởi các GM R_j; và ii) Sự tồn tại của biểu thức kiểm tra $E^* = E$ trong thủ tục kiểm tra chữ ký.

a) Chứng minh tính đúng của chữ ký thành viên:

Dễ thấy công thức kiểm tra chữ ký chia sẻ luôn tồn tại. Thật vậy:

$$R_j = S_j^k \left(Y_j U_j\right)^{-E} \bmod p$$
$$= (X_j^E . T_j \prod_{i=1}^{m_j} x_{ji}^{E\lambda_{ji}} . t_{ji})^{\,k} (X_j^k . T_j \prod_{i=1}^{m_j} y_{ji}^{\lambda_{ji}})^{-E}$$
$$= X_j^{kE} . (T_j \prod_{i=1}^{m_j} x_{ji}^{E\lambda_{ji}} . t_{ji})^k X_j^{-kE} . (T_j \prod_{i=1}^{m_j} y_{ji}^{k\lambda_{ji}})^{-E}$$
$$= T_j^k . \prod_{i=1}^{m_j} {t_{ji}}^k \bmod p = R_j$$

b) Chứng minh tính đúng của chữ ký cuối cùng:

Dễ thấy công thức $E^* = E$ luôn tồn tại. Thật vậy:

$$R^* = S^k (UY_{col})^{-E} \bmod p$$
$$= (\prod_{j=1}^{g} S_j)^k (\prod_{j=1}^{g} U_j \prod_{j=1}^{g} Y_j)^{-E} \bmod p$$
$$= \prod_{j=1}^{g} {S_j}^k (U_j Y_j)^{-E} \bmod p$$
$$= \prod_{j=1}^{g} R_j \bmod p = R$$

Vì $R^* = R$ nên $E^* = F_H(M \| R^* \| U) = F_H(M \| R \| U) = E$.

Vậy biểu thức $E^* = E$ luôn tồn tại: Điều này chứng tỏ tính đúng của thủ tục kiểm tra chữ ký luôn được đảm bảo.

Từ (a) và (b): Tính đúng của lược đồ RCS.01-3.1 được đảm bảo.

- **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)

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 public key và private key được chọn như lược đồ RCS.01-3.1.

- **Thủ tục sinh chữ ký tập thể cho nhiều nhóm ký và nhiều cá nhân ký trên tài liệu *M***

Gồm các bước sau:

1a. GM của mỗi nhóm ký j thực hiện:

- Tạo tham số mặt nạ λ_{ji} cho mỗi signer của nhóm j theo công thức (3.10) (λ_{ji} là hệ số mặt nạ của signer thứ i trong nhóm ký thứ j)
- Tính giá trị thành phần U_j của nhóm ký thứ j theo công thức:

$$U_j = \prod_{i=1}^{m_j} y_{ji}^{\lambda_{ji}} \ mod\ p \tag{3.34}$$

U_j là thành phần chia sẻ của nhóm ký thứ j để tạo thành phần đầu tiên của chữ ký tập thể.

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

$$R_j = R'_j \prod_{i=1}^{m_j} R_{ji} \ mod\ p \tag{3.35}$$

R_j là thành phần chia sẻ của nhóm ký thứ j để tạo tham số ngẫu nhiên của chữ ký tập thể.

- Gửi giá trị U_j và R_j cho tất cả các quản lý khác và các cá nhân ký.

1b. Mỗi cá nhân ký thứ j thực hiện các công việc sau:

- Chọn 1 số ngẫu nhiên t_j và tính giá trị ngẫu nhiên R_j theo công thức:

$$R_j = t_j^k \ mod\ p \tag{3.36}$$

- Gửi giá trị R_j tới tất cả signer những GM và những cá nhân ký khác trong tập thể ký.

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

$$U = \prod_{j=1}^{g+m} U_j \tag{3.37}$$

$$R = \prod_{j=1}^{g+m} R_j \tag{3.38}$$

$$E = F_H(M \parallel R \parallel U) \bmod \delta \tag{3.39}$$

Trong đó, δ là một số nguyên tố lớn ($|\delta| = 160\ bít$); $U_j = 1$ khi $j = g + 1, g + 2, \dots, g + m$).

U và E là thành phần thứ nhất và thứ hai của chữ ký nhóm.

3a. GM của mỗi nhóm thứ j thực hiện:

- Tính thành phần chia sẻ S_j của nhóm j theo công thức:

$$S_j = S'_j \prod_{i=1}^{m_j} S_{ji} \bmod p \tag{3.40}$$

với S_j là thành phần chia sẻ của cá nhân ký thứ i trong nhóm thứ j.

- Gửi S_j cho các GM và các cá nhân ký khác trong tập thể ký.

3b. Mỗi cá nhân ký thứ j ($j = g + 1, g + 2, \dots, g + m$) thực hiện:

- Tính thành phần chia sẻ S_j của họ theo công thức:

$$S_j = X_j^E t_j \bmod p \tag{3.41}$$

- Gửi S_j cho những GM và cá nhân ký khác trong tập thể ký.

4. Một GM hoặc một cá nhân ký nào đó trong tập thể ký thực hiện:

- Kiểm tra tính hợp lệ của mỗi S_j theo công thức:

$$R_j = S_j^k (Y_j U_j)^{-E} \bmod p \tag{3.42}$$

với $j = 1, 2, \dots, g$ và

$$R_j = S_j^k Y_j^{-E} \bmod p \tag{3.43}$$

với $j = g + 1, g + 2, \dots, g + m$

- Nếu tất cả đều thoả mãn, thành phần thứ ba của chữ ký nhóm sẽ được tính theo công thức:

$$S = \prod_{j=1}^{g+m} S_j \bmod p \tag{3.44}$$

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

- **Thủ tục kiểm tra chữ ký tập thể cho nhiều nhóm ký và nhiều cá nhân ký trên tài liệu *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 theo công thức:

$$Y_{col} = \prod_{j=1}^{g+m} Y_j \ mod\ p \tag{3.45}$$

2. Tính giá trị tham số ngẫu nhiên R^* theo công thức:

$$R^* = S^k (U Y_{col})^{-E} \ mod\ p \tag{3.46}$$

3. Tính e^* theo công thức:

$$e^* = F_H(M \| R^* \| U) \tag{3.47}$$

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.

- **Chứng minh tính đúng của lược đồ chữ ký RCS.02-3.1**

Tính đúng của lược đồ chữ ký tập thể đại diện này thể hiện qua: i) Sự tồn tại của công thức kiểm tra chữ ký chia sẻ S_j của mỗi nhóm ký R_j (3.42); ii) Sự tồn tại của công thức kiểm tra chữ ký chia sẻ S_j của mỗi cá nhân ký R_j (3.43) và iii) Sự tồn tại của biểu thức kiểm tra $E^* = E$. Cụ thể như sau:

a) Tính đúng của công thức kiểm tra chữ ký chia sẻ của mỗi trưởng nhóm:

Dễ thấy biểu thức kiểm tra chữ ký chia sẻ của mỗi nhóm ký luôn tồn tại.

Thật vậy:

$$R_j = S_j^k \left(Y_j U_j\right)^{-E} \ mod\ p$$
$$= \left(X_j^E . T_j \prod_{i=1}^{m_j} x_{ji}^{E\lambda_{ji}} . t_{ji} \right)^k \left(X_j^k . T_j \prod_{i=1}^{m_j} y_{ji}^{\lambda_{ji}} \right)^{-E}$$

$$= X_j^{kE}.\left(T_j\prod_{i=1}^{m_j}x_{ji}^{E\lambda_{ji}}.t_{ji}\right)^k X_j^{-kE}.\left(T_j\prod_{i=1}^{m_j}y_{ji}^{k\lambda_{ji}}\right)^{-E}$$

$$= T_j^k.\prod_{i=1}^{m_j}{t_{ji}}^k \bmod p$$

$$= R_j$$

b) Tính đúng của công thức kiểm tra chữ ký chia sẻ mỗi signer:

Dễ thấy biểu thức kiểm tra chữ ký chia sẻ của mỗi signer cá nhân luôn tồn tại. Thật vậy:

$$\begin{aligned} R_j &= S_j^k Y_j^{-E} \bmod p \\ &= X_j^{Ek} t_j^k X_j^{-kE} \bmod p \\ &= t_j^k \bmod p \\ &= R_j \end{aligned}$$

c) Tính đúng của thủ tục kiểm tra chữ ký tập thể đại diện:

Dễ thấy, biểu thức kiểm tra chữ ký $E^* = E$ luôn tồn tại. Thật vậy:

$$\begin{aligned} R^* &= S^k(UY_{col})^{-E} \bmod p \\ &= (\prod_{j=1}^{g+m} S_j)^k (\prod_{j=1}^{g+m} U_j \prod_{j=1}^{g+m} Y_j)^{-E} \bmod p \\ &= \prod_{j=1}^{g} {S_j}^k (U_j Y_j)^{-E} \prod_{j=g+1}^{g+m} {S_j}^k Y_j^{-E} \bmod p \\ &= \prod_{j=1}^{g+m} R_j \bmod p = R \end{aligned}$$

Và tính:

$$\begin{aligned} E^* &= F_H(M\|R^*\|U) \bmod \delta \\ &= F_H(M\|R\|U) \bmod \delta = E \end{aligned}$$

Vậy biểu thức $E^* = E$ luôn tồn tại. Điều này chứng tỏ tính đúng của thủ tục kiểm tra chữ ký, hay tính đúng của lược đồ RCS.02-3.1, luôn được đảm bảo.

3.2. Xây dựng lược đồ chữ ký số 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 số cá nhân (Ký hiệu: SDS-3.2)

Giao thức chữ ký số sau đây được xây dựng dựa trên độ khó của bài toán tìm căn lớn modulo số nguyên tố lớn p, với cấu trúc cụ thể của p là:

$$p = Nt_0t_1t_2 + 1$$

với N là số chẵn; t_0, t_1, t_2 là các số nguyên tố có độ lớn khoảng 80 bít [73].

Trong các lược đồ này, độ khó của việc tìm căn bậc w được định nghĩa bởi độ khó của việc thực hiện một lượng lớn nhưng lần kiểm tra được yêu cầu để tìm một giá trị mà có thể được biểu diễn như là mũ thứ w của một số nào đó.

Giả sử việc tính toán được thực hiện trong nhóm nhân của vòng hữu hạn $(Z_p, +, \bullet)$. Tính bảo mật của giao thức chữ ký số này, sử dụng modulo nguyên tố modulus $p = Nt_0t_1t_2 + 1$, được định nghĩa bởi thủ tục tìm các căn bậc q, với q là một số nguyên tố là ước của nhóm bậc Ω, chỉ có thể tính thực hiện cho Ω/q phần tử khác nhau của nhóm. Với giá trị p là đủ lớn thì khả năng mà một phần tử ngẫu nhiên a có thể được trình bày như x^q là không đáng kể.

Public key Y được hình thành bằng cách sử dụng hai private key K_1 và K_2 được chọn ngẫu nhiên, $K_1 < p$ và $K_2 < p$. Cụ thể, $Y = {K_1}^{w_1}{K_2}^{w_2}$, trong đó $w_1 = t_0t_1$, $w_2 = t_0t_2$. Đây là đặc trưng của lược đồ chữ ký này.

Thủ tục sinh chữ ký của giao thức này giúp tạo ra một chữ ký số gồm một bộ ba giá trị (e, S_1, S_2) trên tài liệu M:

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

Gồm các bước sau (được thực hiện bởi signer):

1. Chọn 2 số ngẫu nhiên T_1 và T_2
2. Tính tham số ngẫu nhiên R theo công thức:

$$R = {T_1}^{w_1}{T_2}^{w_2} \ mod \ p \tag{3.48}$$

3. Tính giá trị băm H của tài liệu M theo công thức:

$$H = F_H(M) \tag{3.49}$$

2. Tính giá trị e theo công thức:

$$e = F(R, M) = RH \ mod \ w_1 \tag{3.50}$$

e là thành phần đầu tiên của chữ ký.

3. Tính giá trị S_1 và S_2 theo công thức:

$$S_1 = T_1 {K_1}^{-e} \ mod \ p \tag{3.51a}$$

$$S_2 = T_2 {K_2}^{-e} \ mod \ p \tag{3.51b}$$

S_1 và S_2 là thành phần thứ 2 và thứ 3 của chữ ký.

Vậy bộ ba (e, S_1, S_2) là chữ ký cá nhân (của signer) trên tài liệu M.

- **Thủ tục kiểm tra chữ ký cá nhân trên tài liệu 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. Sử dụng chữ ký nhận được (e, S_1, S_2) tính giá trị R':

$$R' = Y^e {S_1}^{w_1} {S_2}^{w_2} \ (mod \ p) \tag{3.52}$$

2. Tính giá trị e':

$$e' = F(R', M) = R'H \ (mod \ w_1) \tag{3.53}$$

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

- **Chứng minh tính đúng của lược đồ SDS-3.2:**

Nếu chữ ký đã được hình thành là hợp lệ, tức là, việc sử dụng private key trong thủ tục tạo chữ ký là đúng thì biểu thức kiểm tra $e' = e$ trong thủ tục kiểm tra chữ ký luôn xảy ra. Vậy để chứng minh tính đúng của lược đồ này ta chỉ cần chứng minh sự tồn tại của biểu thức $e' = e$.

Dễ thấy, biểu thức kiểm tra $e' = e$ luôn tồn tại. Thật vậy:

$$\begin{aligned} R' &= Y^e {S_1}^{w_1} {S_2}^{w_2} \ mod \ p \\ &= ({K_1}^{w_1} {K_2}^{w_2})^e (T_1 {K_1}^{-e})^{w_1} (T_2 {K_2}^{-e})^{w_2} \ mod \ p \\ &= {T_1}^{w_1} {T_2}^{w_2} \ mod \ p = R \end{aligned}$$

Vì $R' = R$ nên $e' = R'H \ mod \ w_1 = RH \ mod \ w_1 = e$.

Vậy biểu thức $e' = e$ luôn tồn tại: Điều này chứng tỏ tính đúng của thủ tục kiểm tra chữ ký, hay tính đúng của lược đồ SDS-3.2, luôn được đảm bảo.

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

Sử dụng phương pháp chung xây dựng sơ đồ chữ ký tập thể được đề xuất trong nghiên cứu [71], trên cơ sở bài toán khai căn sơ đồ chữ ký tập thể được xây dựng như sau:

Giả sử có một nhóm gồm m thành viên cần ký lên tài liệu M. Các thành viên này có các public key lần lượt là: $Y_1, Y_2, \dots, Y_m$với $Y_i = K_{1_i}^{w_1} K_{2_i}^{w_2}$, $w_1 = t_0 t_1$ và $w_2 = t_0 t_2$ $(i = 1, 2, \dots, m)$. K_{1_i}, K_{2_i} là hai private key sao cho $K_{1_i} < p, K_{2_i} < p$. Public key tập thể dùng trong quá trình kiểm tra chữ ký tập thể được tính theo công thức $Y = \prod_{i=1}^{m} Y_i \ mod\ p$ và quá trình kiểm tra tính hợp lệ của chữ ký tập thể giống như trường hợp chữ ký cá nhân.

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

Gồm các bước sau:

1. Mỗi signer thứ i trong tập thể ký thực hiện:

- Tạo cặp số ngẫu nhiên T_{1_i} và T_{2_i} (đóng vai trò là private key giả)
- Tính giá trị R_i theo công thức:

$$R_i = T_{1_i}^{w_1} T_{2_i}^{w_2} \ mod\ p \tag{3.54}$$

- Gửi giá trị R_i cho các signer khác tập thể ký.

2. Một signer nào đó trong tập thể ký thực hiện:

- Tính giá trị R theo công thức:

$$R = \prod_{i=1}^{m} R_i \ mod\ p \tag{3.55}$$

R đóng vai trò là thành phần ngẫu nhiên chung của tập thể ký với sự đóng góp các thành phần ngẫu nhiên R_i của từng thành viên trong tập thể này.

- Tính giá trị e theo công thức:

$$e = F_H(M \| R \| Y) \tag{3.56}$$

- Gửi giá trị e cho các signer khác trong tập thể ký.

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

3. Mỗi signer thứ i trong tập thể ký thực hiện:

- Tính thành phần chữ ký chia sẻ của họ S_{1_i} và S_{2_i} theo công thức:

$$S_{1_i} = T_{1_i} K_{1_i}^{-e} \ mod\ p \tag{3.57a}$$

$$S_{2_i} = T_{2_i} K_{2_i}^{-e} \ mod\ p \tag{3.57b}$$

- Gửi giá trị S_{1_i}, S_{2_i} cho các signer khác trong tập thể ký.

4. Một signer nào đó trong tập thể ký thực hiện công việc cuối cùng: Tính thành phần thứ hai S_1 và thứ 3 S_2 của chữ ký tập thể theo các công thức:

$$S_1 = \prod_{i=1}^{m} S_{1_i} \, mod \, q \tag{3.58a}$$

$$S_2 = \prod_{i=1}^{m} S_{2_i} \, mod \, q \tag{3.58b}$$

Vậy bộ ba giá trị (e, S_1, S_2) là chữ ký tập thể của tập thể ký trên tài liệu M.

- **Thủ tục kiểm tra chữ ký tập thể trên tài liệu 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 giá trị public key tập thể Y theo công thức:

$$Y = \prod_{i=1}^{m} Y_i \; mod \, p \tag{3.59}$$

2. Tính giá trị R' theo công thức:

$$R' = Y^e {S_1}^{w_1} {S_2}^{w_2} \; mod \, p. \tag{3.60}$$

3. Tính giá trị e' theo công thức:

$$e' = F_H(M \| R' \| Y) \tag{3.61}$$

4. So sánh giá trị 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.

- **Chứng minh tính đúng của lược đồ CDS-3.2:**

Để chứng minh tính đúng của lược đồ này, ta chỉ cần chứng minh sự tồn tại của biểu thức kiểm tra $e' = e$ trong thủ tục kiểm tra chữ ký.

Dễ thấy, biểu thức kiểm tra $e' = e$ luôn tồn tại.

Ta có:

$$\begin{aligned} R' &= Y^e {S_1}^{w_1} {S_2}^{w_2} \; mod \, p \\ &= \prod_{i=1}^{m} \left({K_{1_i}}^{w_1} {K_{2_i}}^{w_2} \right)^e \prod_{i=1}^{m} \left(T_{1_i} {K_{1_i}}^{-e} \right)^{w_1} \prod_{i=1}^{m} \left(T_{2_i} {K_{2_i}}^{-e} \right)^{w_2} \; mod \, p \\ &= \prod_{i=1}^{m} T_{1_i}^{w_1} T_{2_i}^{w_2} \; mod \, p = \prod_{i=1}^{m} R_i \, mod \, p = R \end{aligned}$$

Vì $R' = R$ nên $e' = F_H\left(M \| R' \| Y\right) = F_H\left(M \| R \| Y\right) = e$

Vậy biểu thức $e' = e$ luôn tồn tại: Điều này chứng tỏ tính đúng của thủ tục kiểm tra chữ ký, hay tính đúng của lược đồ CDS-3.2, luôn được đảm bảo.

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

Sử dụng phương pháp chuẩn xây dựng sơ đồ chữ ký tập thể được đề xuất trong nghiên cứu [71], trên cơ sở bài toán khai căn sơ đồ chữ ký tập thể được xây dựng như sau:

Giả sử có một nhóm có m thành viên cần ký lên bản tin M. Với $w_1 = t_0 t_1$ và $w_2 = t_0 t_2$ Các thành viên này lần lượt có các public key: $Y_1, Y_2, \dots, Y_m$, $Y_i = K_{1_i}^{w_1} K_{2_i}^{w_2}$, $(i = 1, 2, \dots, m)$. K_{1_i}, K_{2_i} là hai private key của người ký tương ứng sao cho $K_{1_i}, K_{2_i} < p$. Người quản lý nhóm (GM) tạo cho mình một public key: $Y' = {K'}_1^{w_1} {K'}_2^{w_2}$, $(K_1', K_2' < p)$. (F_H là một hàm băm được chỉ định trước).

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

Gồm các bước sau:

1. GM thực hiện như sau:

- Tính giá trị băm của tài liệu M theo công thức:

$$H = F_H(M) \tag{3.62}$$

- Tính hệ số mặt nạ λ_i cho mỗi signer trong nhóm ký theo công thức:

$$\lambda_i = F_H(H \,\|Y_i\|\, F_H(H \,\|Y_i\|K_1'\|K_2')) \tag{3.63}$$

- Gửi λ_i cho mỗi signer i tương ứng
- Tính thành phần đầu tiên của chữ ký nhóm

$$U = \prod_{i=1}^{m} Y_i^{\lambda_i} \; mod \; p \tag{3.64}$$

2. Mỗi signer thứ i trong nhóm ký thực hiện:

- Tạo ngẫu nhiên cặp số T_{1_i} và T_{2_i} và rồi tính R_i theo công thức:

$$R_i = T_{1_i}^{w_1} T_{2_i}^{w_2} \; mod \; p \tag{3.65}$$

- Gửi giá trị R_i cho người quản lý nhóm.

3. GM tiếp tục thực hiện:

- Sinh ra một cặp giá trị ngẫu nhiên T_1' và T_2' và tính các giá trị R', R và e theo các công thức:

$$R' = {T_1'}^{w_1} {T_2'}^{w_2} \; mod \; p \tag{3.66}$$

$$R = R' \prod_{i=1}^{m} R_i \; mod \; p \tag{3.67}$$

$$e = F_H(M\|R\|U)\ mod\ \delta \quad (3.68)$$

Trong đó, với δ là một số nguyên tố có độ dài $|\delta| = 160$ bít.

e là thành phần thứ hai của chữ ký nhóm.

- Gửi giá trị e cho tất cả signer trong nhóm ký.

4. Mỗi signer i tiếp tục thực hiện như sau:

- Tính thành phần chữ ký chia sẻ của họ S_{1_i}, S_{2_i} theo công thức:

$$S_{1_i} = T_{1_i} K_{1_i}^{-\lambda_i e}\ mod\ p \quad (3.69a)$$

$$S_{2_i} = T_{2_i} K_{2_i}^{-\lambda_i e}\ mod\ p \quad (3.69b)$$

- Gửi giá trị S_{1_i}, S_{2_i} cho các signer khác trong nhóm ký.

5. GM thực hiện các công việc cuối cùng:

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

$$R_i = S_{1_i}^{w_1} S_{2_i}^{w_2} Y_i^{e\lambda_i}\ mod\ p \quad (3.70)$$

- Nếu tất cả các cặp số S_{1_i}, S_{2_i} đều thỏa mãn thì tính thành phần chữ ký chia sẻ cá nhân theo các công thức:

$$S_1' = T_1' K'^{-e}_1\ mod\ p \quad (3.71a)$$

$$S_2' = T_2' K'^{-e}_2\ mod\ p \quad (3.71b)$$

- Tính thành phần thứ ba S_1và thứ tư S_2 của chữ ký nhóm theo các công thức:

$$S_1 = S_1' \prod_{i=1}^{m} S_{1_i}\ mod\ q \quad (3.72a)$$

$$S_2 = S_2' \prod_{i=1}^{m} S_{2_i}\ mod\ q \quad (3.72b)$$

Vậy bộ giá trị (U, e, S_1, S_2) là chữ ký nhóm của nhóm ký trên tài liệu M.

- **Thủ tục kiểm tra chữ ký nhóm trên tài liệu *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 giá trị public key tập thể Y theo công thức:

$$Y = \prod_{i=1}^{m} Y_i\ mod\ p \quad (3.73)$$

2. Tính giá trị R^* theo công thức:

$$R^* = (UY')^e {S_1}^{w_1} {S_2}^{w_2} \ mod\ p. \quad (3.74)$$

3. Tính giá trị e^* theo công thức:

$$e^* = F_H(M \| R^* \| U) \quad (3.75)$$

4. So sánh giá trị 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.

- **Chứng minh tính đúng của lược đồ GDS-3.2**

Để chứng minh tính đúng của lược đồ này, ta chỉ cần chứng minh sự tồn tại của biểu thức kiểm tra $e^* = e$ trong thủ tục kiểm tra chữ ký.

Dễ thấy, biểu thức kiểm tra $e^* = e$ luôn tồn tại. Ta có:

$$\begin{aligned} R^* &= (UY')^e {S_1}^{w_1} {S_2}^{w_2} \ mod\ p \\ &= \left[\left({K'_1}^{w_1} {K'_2}^{w_2} \right)^e \prod_{i=1}^{m} \left({K_{1_i}}^{w_1} {K_{2_i}}^{w_2} \right)^{\lambda_i e} \right] \\ &\quad \left[(T'_1 {K'_1}^{-e})^{w_1} \prod_{i=1}^{m} \left(T_{1_i} {K_{1_i}}^{-\lambda_i e} \right)^{w_1} \right] \\ &\quad \left[(T'_2 {K'_2}^{-e})^{w_2} \prod_{i=1}^{m} \left(T_{2_i} {K_{2_i}}^{-\lambda_i e} \right)^{w_2} \ mod\ p \right] \\ &= {T'_1}^{w_1} {T'_2}^{w_2} \prod_{i=1}^{m} T_{1_i}^{w_1} T_{2_i}^{w_2} \ mod\ p \\ &= R' \prod_{i=1}^{m} R_i \ mod\ p = R \end{aligned}$$

Vì $R^* = R$ nên $e^* = F_H(M \| R^* \| U) = F_H(M \| R \| U) = e$.

Vậy biểu thức $e^* = e$ luôn tồn tại: Điều này chứng tỏ tính đúng của thủ tục kiểm tra chữ ký, hay tính đúng của lược đồ GDS-3.2, luôn được đảm bảo.

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

Phần này sử dụng 2 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 key được 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:

$$\lambda_i = F_H(H \| Y_i \| F_H(H \| Y_i \| K_1' \| K_2')) \tag{3.76}$$

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

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

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

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:

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

- 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:

$$U = \prod_{j=1}^{g} U_j \ mod\ p \tag{3.79}$$

$$R = \prod_{j=1}^{g} R_j \ mod\ p \tag{3.80}$$

và

$$e = F_H(M \| R \| U) \ mod\ \delta \tag{3.81}$$

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

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

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:

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

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

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:

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

- 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:

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

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

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 tài liệu *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:

$$Y_{col} = \prod_{j=1}^{g} Y'_j \ mod\ p \tag{3.85}$$

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

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

3. Tính giá trị e^* theo công thức:

$$e^* = F_H(M \ \|R^*\| \ U) \tag{3.87}$$

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.

- **Chứng minh tính đúng đắn của lược đồ RCS.01-3.2**

Tính đúng của lược đồ chữ ký tập thể đại diện này thể hiện qua: i) Sự tồn tại của công thức kiểm tra chữ ký chia sẻ S_{ji} được chia sẻ bởi các trưởng nhóm ký R_j; và ii) Sự tồn tại của biểu thức kiểm tra $e^* = e$ trong thủ tục kiểm tra chữ ký.

a) Chứng minh tính đúng của công thức kiểm tra chữ ký chia sẻ:

Dễ thấy công thức kiểm tra chữ ký chia sẻ S_{ji} được chia sẻ bởi các trưởng nhóm ký R_j luôn tồn tại. Thật vậy:

$$
\begin{aligned}
R_j &= \left(U_j Y_j'\right)^e {S_1}_j^{w_1} {S_2}_j^{w_2} \bmod p \\
&= \left[\left({K'}_{1_j}^{w_1} {K'}_{2_j}^{w_2}\right)^e \prod_{i=1}^{m_j} \left({K_1}_{ji}^{w_1} {K_2}_{ji}^{w_2}\right)^{\lambda_{ji} e}\right] \\
&\quad \left[\left(T_{1_j}' {K'}_{1_j}^{-e}\right)^{w_1} \prod_{i=1}^{m_j} \left(T_{1_{ji}} {K_1}_{ji}^{-\lambda_{ji} e}\right)^{w_1}\right] \\
&\quad \left[\left(T_{2_j}' {K'}_{2_j}^{-e}\right)^{w_2} \prod_{i=1}^{m_j} \left(T_{2_{ji}} {K_2}_{ji}^{-\lambda_{ji} e}\right)^{w_2} \bmod p\right] \\
&= {T_1'}_j^{w_1} {T_2'}_j^{w_2} \prod_{i=1}^{m_j} T_{1_{ji}}^{w_1} T_{2_{ji}}^{w_2} \bmod p \\
&= R_j' \prod_{i=1}^{m_j} R_{ji} \bmod p = R_j
\end{aligned}
$$

b) Chứng minh tính đúng của thủ tục kiểm tra chữ ký:

Dễ thấy, biểu thức kiểm tra chữ ký $e^* = e$ luôn tồn tại.

Ta có:

$$
\begin{aligned}
R^* &= (UY_{col})^e {S_1}^{w_1} {S_2}^{w_2} \bmod p \\
R^* &= \left(\prod_{j=1}^{g} U_j \prod_{j=1}^{g} Y_j'\right)^{-e} \left(\prod_{j=1}^{g} S_{1_j}\right)^{w_1} \left(\prod_{j=1}^{g} S_{2_j}\right)^{w_2} \bmod p \\
&= \prod_{j=1}^{g} \left(U_j Y_j'\right)^e {S_1}_j^{w_1} {S_2}_j^{w_2} \bmod p \\
&= \prod_{j=1}^{g} R_j \bmod p = R
\end{aligned}
$$

Vì $R^* = R$ nên $e^* = F_H(M \| R^* \| U) = F_H(M \| R \| U) = e$.

Vậy biểu thức $e^* = e$ luôn tồn tại: Điều này chứng tỏ tính đúng của thủ tục kiểm tra chữ ký luôn được đảm bảo.

Từ (a) và (b): Tính đúng của lược đồ RCS.01-3.2 được đảm bảo.

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)

Phần này sử dụng 2 lược đồ vừa mô tả ở trên làm cơ sở để xây dựng lược đồ chữ ký tập thể đại diện, dạng 2: Chữ ký tập thể cho nhiều nhóm ký và nhiều người ký cá nhân.

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 và m người ký cá nhân, được điều hành bởi người trưởng nhóm (GM).

Các tham số đầu vào, các public key, các private key được 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 tập thể cho nhiều nhóm ký và nhiều cá nhân ký trên tài liệu M**

Gồm các bước sau:

1a. GM của mỗi nhóm ký j thực hiện:

- Tạo tham số mặt nạ λ_{ji} cho mỗi signer của nhóm j theo công thức (3.10) (λ_{ji} là hệ số mặt nạ của signer thứ i trong nhóm ký thứ j)
- Tính giá trị thành phần U_j của nhóm ký thứ j theo công thức:

$$U_j = \prod_{i=1}^{m_j} Y_{ji}^{\lambda_{ji}} \ mod\ p \tag{3.88}$$

U_j là thành phần chia sẻ của nhóm ký thứ j để tạo thành phần đầu tiên của chữ ký tập thể.

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

$$R_j = R'_j \prod_{i=1}^{m_j} R_{ji} \ mod\ p \tag{3.89}$$

R_j là thành phần chia sẻ của nhóm ký thứ j để tạo tham số ngẫu nhiên của

chữ ký tập thể.

- Gửi giá trị U_j và R_j cho tất cả các quản lý khác và các cá nhân ký.

1b. Mỗi cá nhân ký thứ j thực hiện các công việc sau:

- Chọn 2 số ngẫu nhiên T_{1_j} và T_{2_j} và tính giá trị ngẫu nhiên R_j theo công thức:

$$R_j = {T_{1_j}}^{w_1} {T_{2_j}}^{w_2} \ mod \ p \tag{3.90}$$

- Gửi giá trị R_j tới tất cả những GM và những cá nhân ký khác trong tập thể ký.

2. Một GM hoặc một cá nhân ký nào đó trong tập thể ký tính các giá trị U, R và e theo các công thức:

$$U = \prod_{j=1}^{g+m} U_j \ mod \ p \tag{3.91}$$

$$R = \prod_{j=1}^{g+m} R_j \ mod \ p \tag{3.92}$$

$$e = F_H(M \| R \| U) \ mod \ \delta \tag{3.93}$$

Trong đó, δ là một số nguyên tố lớn ($|\delta| = \ 160 \ bít$); $U_j = 1$ khi $j = g + 1, g + 2, \dots, g + m$).

U và e là thành phần thứ nhất và thứ hai của chữ ký nhóm.

3a. GM của mỗi nhóm thứ j thực hiện:

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

$$S_{1_j} = S'_{1_j} \prod_{i=1}^{m_j} S_{1_{ji}} \ mod \ q \tag{3.94a}$$

$$S_{2_j} = S'_{2_j} \prod_{i=1}^{m_j} S_{2_{ji}} \ mod \ q \tag{3.94b}$$

với $S_{1_{ji}}, S_{2_{ji}}$ là thành phần chia sẻ của cá nhân ký thứ i trong nhóm thứ j.

- Gửi S_{1_j}, S_{2_j} cho các GM và các cá nhân ký khác trong tập thể ký.

3b. Mỗi cá nhân ký thứ j ($j = g + 1, g + 2, \dots, g + m$) thực hiện:

- Tính thành phần chia sẻ S_{1_j}, S_{2_j} của họ theo công thức:

$$S_{1_j} = T_{1_j} K_{1_j}^{-e} \ mod \ p \quad (3.95a)$$

$$S_{2_j} = T_{2_j} K_{2_j}^{-e} \ mod \ p \quad (3.95b)$$

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

4. Một GM hoặc một cá nhân ký nào đó trong tập thể ký thực hiện:

- Kiểm tra tính hợp lệ của mỗi S_{1_j}, S_{2_j} theo công thức:

$$R_j = (U_j Y_j')^e {S_{1_j}}^{w_1} {S_{2_j}}^{w_2} \ mod \ p \quad (3.96)$$

với $j = 1, 2, \dots, g$ và

$$R_j = S_{1_j}^{w_1} S_{2_j}^{w_2} Y_j^{-e} \ mod \ p \quad (3.97)$$

với $j = g+1, g+2, \dots, g+m$

- Nếu tất cả đều thoả mãn, thành phần thứ ba của chữ ký nhóm sẽ được tính theo công thức:

$$S_1 = \prod_{j=1}^{g+m} S_{1_j} \ mod \ q \quad (3.98a)$$

$$S_2 = \prod_{j=1}^{g+m} S_{2_j} \ mod \ q \quad (3.98b)$$

Vậy bộ giá trị (U, e, S_1, S_2) là chữ ký tập thể đại diện, của một tập thể gồm g nhóm ký và m cá nhân ký, trên tài liệu M (dạng chữ ký này còn được gọi là, chữ ký tập thể được chia sẻ bởi nhiều nhóm và nhiều cá nhân ký). Nó đại diện cho tập thể ký này.

- **Thủ tục kiểm tra chữ ký tập thể cho nhiều nhóm ký và nhiều cá nhân ký trên tài liệu *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 theo công thức:

$$Y_{col} = \prod_{j=1}^{g} Y_j' \prod_{j=g+1}^{g+m} Y_j \ mod \ p \quad (3.99)$$

2. Tính giá trị tham số ngẫu nhiên R^* theo công thức:

$$R^* = (UY_{col})^e {S_1}^{w_1} {S_2}^{w_2} \ mod \ p \quad (3.100)$$

3. Tính e^* theo công thức:

$$e^* = F_H(M \,\|R^*\|\, U) \tag{3.101}$$

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.

- **Chứng minh tính đúng của lược đồ chữ ký RCS.02-3.2**

Tính đúng của lược đồ chữ ký tập thể đại diện này thể hiện qua: i) Sự tồn tại của công thức kiểm tra chữ ký chia sẻ S_j của mỗi nhóm ký R_j^* (3.102); ii) Sự tồn tại của công thức kiểm tra chữ ký chia sẻ s_j của mỗi cá nhân ký R (3.103) và iii) Sự tồn tại của biểu thức kiểm tra $e^* = e$. Cụ thể như sau:

a) Tính đúng của công thức kiểm tra chữ ký chia sẻ của mỗi trưởng nhóm:

Dễ thấy công thức kiểm tra chữ ký chia sẻ S_{ji} được chia sẻ bởi các trưởng nhóm ký R_j luôn tồn tại. Thật vậy:

$$\begin{aligned}
R_j &= \left(U_j Y_j'\right)^e {S_{1_j}}^{w_1} {S_{2_j}}^{w_2} \; mod\; p \\
&= \left[\left({K'}_{1_j}^{w_1} {K'}_{2_j}^{w_2}\right)^e \prod_{i=1}^{m_j} \left({K_{1_{ji}}}^{w_1} {K_{2_{ji}}}^{w_2}\right)^{\lambda_{ji} e}\right] \\
&\quad \left[\left(T_{1_j}' {K'}_{1_j}^{-e}\right)^{w_1} \prod_{i=1}^{m_j} \left(T_{1_{ji}} {K_{1_{ji}}}^{-\lambda_{ji} e}\right)^{w_1}\right] \\
&\quad \left[\left(T_{2_j}' {K'}_{2_j}^{-e}\right)^{w_2} \prod_{i=1}^{m_j} \left(T_{2_{ji}} {K_{2_{ji}}}^{-\lambda_{ji} e}\right)^{w_2} \; mod\; p\right] \\
&= {T_{1_j}'}^{w_1} {T_{2_j}'}^{w_2} \prod_{i=1}^{m_j} T_{1_{ji}}^{w_1} T_{2_{ji}}^{w_2} \; mod\; p \\
&= R_j' \prod_{i=1}^{m_j} R_{ji} \; mod\; p = R_j
\end{aligned}$$

b) Tính đúng của công thức kiểm tra chữ ký chia sẻ mỗi signer:

Dễ thấy công thức kiểm tra chữ ký chia sẻ S_i được chia sẻ bởi các trưởng nhóm ký R luôn tồn tại. Thật vậy:

$$\begin{aligned}
R &= Y_j^e {S_{1_j}}^{w_1} {S_{2_j}}^{w_2} \; mod\; p \\
&= \left({K_{1_j}}^{w_1} {K_{2_j}}^{w_2}\right)^e \left(T_{1_j} {K_{1_j}}^{-e}\right)^{w_1} \left(T_{2_j} {K_{2_j}}^{-e}\right)^{w_2} \; mod\; p \\
&= {T_{1_j}}^{w_1} {T_{2_j}}^{w_2} \; mod\; p = R
\end{aligned}$$

c) Tính đúng của thủ tục kiểm tra chữ ký tập thể đại diện:

Dễ thấy, biểu thức kiểm tra chữ ký $e^* = e$ luôn tồn tại.

Ta thấy:

$$R^* = (UY_{col})^e {S_1}^{w_1} {S_2}^{w_2} \ mod\ p$$
$$= (\prod_{j=1}^{g+m} U_j \prod_{j=1}^{g} Y_j' \prod_{j=g+1}^{g+m} Y_j)^{-e} \left(\prod_{j=1}^{g+m} S_{1_j}\right)^{w_1} \left(\prod_{j=1}^{g+m} S_{2_j}\right)^{w_2} \ mod\ p$$
$$= \prod_{j=1}^{g} \left(U_j Y_j'\right)^e {S_{1_j}}^{w_1} {S_{2_j}}^{w_2} \prod_{j=g+1}^{g+m} Y_j^e {S_{1_j}}^{w_1} {S_{2_j}}^{w_2} \ mod\ p$$
$$= \prod_{j=1}^{g+m} R_j \ mod\ p = R$$

và tính:

$$e^* = F_H(M \ \|R^*\| \ U) \ mod\ \delta$$
$$= F_H(M \ \|R\| \ U) \ mod\ \delta$$
$$= e$$

Vậy biểu thức $e^* = e$ luôn tồn tại: Điều này chứng tỏ tính đúng của thủ tục kiểm tra chữ ký, hay tính đúng của lược đồ RCS.02-3.2, luôn được đảm bảo.

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

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

a) Loại tấn công thứ nhất: Giả sử kẻ tấn công có thể sinh được 2 số ngẫu nhiên T_1 và T_2, và rồi tính được $R = {T_1}^{w_1} {T_2}^{w_2} \ mod\ p$, $e = F(R, M)$ và thử tìm cặp số (S_1, S_2) thỏa mãn ${S_1}^{w_1} {S_2}^{w_2} = RY^{-e}$ (*), trong đó $S_1,\ S_2$ là các số chưa biết. Vế phải của biểu thức (*) là một giá trị ngẫu nhiên, bởi vì hàm $F(R, M)$ là một hàm dạng hàm băm và e được tính theo công thức $e = RH \ mod\ w_1$.

Nếu gán cố định S_2, thì biểu thức (*) trở thành một hàm 1 biến S_1. Trong biểu thức này, vế phải có xác suất rất nhỏ có một giá trị mà với nó thì phương trình có thể được giải. Một phép tính mũ $modulo\ p$ đã được sử dụng để kiểm tra tính có thể giải được của phương trình. Để đạt được trường hợp có thể giải được, yêu cầu phải xử lý những thủ tục đã được đề cập trung bình t_1 lần. Khi độ dài của t_1 là 80 bít hoặc hơn, độ phức tạp tính toán của việc giả mạo chữ ký là quá lớn để khả

thi trong thực tế. Tương tự, việc giả mạo chữ ký có thể xử lý thông qua việc giải quyết phương trình một ẩn S_2, và cần t_2 lần thực hiện thủ tục đã được đề cập. Nếu độ dài của t_2 là 80 bít hoặc hơn thì độ khó tính toán trong trường hợp này cũng khá cao và thực tế không thể thực hiện được.

b) Loại tấn công thứ hai: Loại tấn công này tinh vi hơn. Theo đó, đầu tiên kẻ tấn công sinh giá trị $R = Y^u \ mod\ p$, rồi tính $e = F(R, M)$, và thử tìm cặp số S_1 và S_2 bằng cách sử dụng biểu thức $S_1 = Y^{s_1 w_1} \ mod\ p$ và $S_2 = Y^{s_2 w_2} \ mod\ p$.

Để có được các giá trị S_1 và S_2 như mong muốn thì biểu thức $Y^u = Y^e Y^{s_1 w_1} Y^{s_2 w_2} \ mod\ p$ phải thỏa mãn, nếu quan hệ sau thỏa mãn: $u - e = s_1 w_1 + s_2 w_2 \ mod\ (p-1)$. Đây là một phương trình Diophantine [68] cho hai giá trị chưa biết s_1 và s_2.

Bởi vì $w_1 = t_0 t_1$ và $w_2 = t_0 t_2$, trong đó t_0, t_1, t_2 là số nguyên tố, và phương trình Diophantine có một lời giải trong số nguyên chỉ trong trường hợp khi vế phải của phương trình chia hết cho t_0, với t_0 bằng với ước chung lớn nhất của các hệ số của các số chưa biết s_1 và s_2. Giá trị e được xác định bởi công thức $e = F(R, M)$ và có 1 giá trị ngẫu nhiên. Xác suất để t_0 sẽ chia cho $u - e$ (để xác suất của phương tình Diophantine có kết quả) là khá nhỏ, $1/t_0$.

Khi độ lớn của t_0 là 80 bít, trong trường hợp này, để có thể giải được phương trình Diophantine thì cần trung bình 2^{80} phép thử giả mạo chữ ký. Tức là, độ khó của vấn đề xử lý này là 2^{80} lũy thừa $modulo\ p$.

c) Loại tấn công thứ ba: Kiểu tấn công này đạt hiệu quả cao khi tấn công vào các lược đồ chữ ký được xây dựng dựa trên bài toán logarit rời rạc trên trường hữu hạn $GF(p)$. Phương thức tấn công được mô tả như sau: Đầu tiên, kẻ tấn công tìm phần tử nguyên thủy G, là bậc của tất cả các phần tử khác 0 của trường $GF(p)$. Và rồi biểu diễn public key Y như sau:

$$\begin{aligned} Y &= G^z = {X_1}^{w_1} {X_2}^{w_2} \\ &= G^{x_1 w_1} G^{x_2 w_2} \\ &= G^{x_1 w_1 + x_2 w_2} \ mod\ p, \end{aligned}$$

với x_1 và x_2 là các giá trị của logarit rời rạc của private key tương ứng X_1 và X_2.

Phương trình trên cho thấy việc tìm logarit rời rạc z từ public key và cơ số G là tương đương việc giải phương trình sau:

$$z = x_1 w_1 + x_2 w_2$$

$$= x_1 t_0 t_1 + x_2 t_0 t_2 \; mod \; (p-1). \quad (3.102)$$

Phương trình này có thể giải dễ dàng thông qua biến x_1, x_2. Khả năng giải được bài toán phụ thuộc vào tính chia hết của z cho t_0. Cho $z = z' t_0$, ta có:

$$z' = x_1 t_1 + x_2 t_2 \; mod \; (p-1)/t_0. \quad (3.103)$$

Từ phương trình trên, với số nguyên N nào đó, ta nhận được phương trình chứa 2 biến x_1 và x_2 như sau:

$$z' + N\frac{p-1}{t_0} = x_1 t_1 + x_2 t_2 \quad (3.104)$$

suy ra:
$$z' = x_1 t_1 \; mod \; t_2 \; \Rightarrow \; x_1 = \frac{z'}{t_1} \; mod \; t_2 \quad (3.105)$$

Tương tự, ta có thể nhận được phương trình cho việc tính giá trị x_2:

$$x_2 = \frac{z'}{t_2} \; mod \; t_1 \quad (3.106)$$

Do đó, lược đồ chữ ký số được trình bày trong phần này yêu cầu sử dụng một số nguyên tố p, có độ lớn tối thiểu 1024 bít. Trong trường hợp trước, bài toán logarit rời rạc có thể được coi là bài toán khó, vì ta có thể ước lượng độ phức tạp để giải quyết bài toán là 2^{80} phép nhân $modulo\ p$ [73]. Do đó, lược đồ chữ ký số này đạt cấp bảo mật tối thiểu 2^{80} cho số nguyên tố p có độ lớn tối thiểu 1024 bít.

3.3.2. Tính bảo mật của lược đồ chữ ký số nhóm

Với lược đồ chữ ký nhóm, tồn tại hai dạng tấn công chủ yếu: Tấn công từ nội bộ và tấn công từ bên ngoài. Với dạng tấn công từ bên ngoài, kẻ tấn công chỉ biết được các tham số và public key, cùng với tài liệu M, còn với dạng tấn công từ nội bộ thì vì là thành viên của nhóm nên những kẻ tấn công sẽ biết được nhiều thông tin hơn. Phần này xem xét về hai dạng tấn công phổ biến vào lược đồ chữ ký nhóm, mà nó được thực hiện bởi người quản lý nhóm. Người này có được nhiều thông tin do các thành viên trong nhóm cung cấp nên khả năng tấn công thành công là khá cao.

- **Tấn công vào private key của thành viên nhóm**

Xét trường hợp nhóm ký gồm m thành viên và người quản lý nhóm (GM) muốn tấn công vào private key của người thứ m trong nhóm ký.

Vì GM biết được các giá trị (S_m, R_m, y_m) của thành viên thứ m nên GM có thể tính được private key x_m theo một trong hai phương trình sau:

$$x_m = \sqrt[k]{y_m}\ mod\ p \tag{3.107}$$

hoặc:

$$x_m = \sqrt[-Ek\lambda_m]{\frac{R_m}{S_m^k}}\ mod\ p \tag{3.108}$$

Đây lại là những bài toán khó mới (bài toán khó khai căn modulo số nguyên tố lớn), nên việc giải nó để tìm nghiệm x_m là không thể (tính đến hiện tại).

Như vậy, dù biết được nhiều thông tin của thành viên mình đang quản lý, nhưng GM vẫn khó có thể biết được private key những thành viên này.

- **Tấn công giả mạo chữ ký**

Xét trường hợp nhóm ký gồm m thành viên và người quản lý nhóm (GM) muốn giả mạo chữ ký của thành viên thứ m trong nhóm ký.

Vì biết được giá trị các (S_m, R_m, y_m) nên anh ta thực hiện các bước sau:

1. Chọn $X \in [1, n-1]$ và tính public key như sau:

$$Y = y_m^{\lambda_m} X^k\ mod\ p \tag{3.109}$$

Và rồi tính giá trị công khai chung cho cả nhóm ký:

$$U = \prod_{i=1}^{m} y_i^{\lambda_i}\ mod\ p \tag{3.110}$$

2. Chọn $T \in [1, q-1]$ và tính:

$$R' = R_m T^k\ mod\ p \tag{3.111}$$

3. Tính R và E, gửi E cho các thành viên khác trong nhóm:

$$R = R' \prod_{i=1}^{m} R_i\ mod\ p \tag{3.112}$$

$$E = F_H(M\ ||R||\ U) mod\ \delta \tag{3.113}$$

4. Tính:

$$S' = S_m X^E T\ \ mod\ p \tag{3.114}$$

Rồi tính:

$$S = S' \prod_{i=1}^{m} S_i\ mod\ p \tag{3.115}$$

Dễ thấy bộ ba (U, E, S) vẫn thỏa biểu thức kiểm tra:

$$R = S^k (YU)^{-E} \ mod \ p$$

Thật vậy:

$$\begin{aligned} R^* &= S^k \ (YU)^{-E} \ mod \ p \\ &= (S_m X^E T \prod_{i=1}^{m} x_i^{E\lambda_i} t_i)^k \ (X^k \prod_{i=1}^{m} y_i^{\lambda_i})^{-E} \\ &= \left(x_m^{Ek\lambda_m} t_m^k X^{kE} T^k \prod_{i=1}^{m} x_i^{Ek\lambda_i} t_i^k \right) \left(x_m^{-Ek\lambda_m} X^{-kE} \prod_{i=1}^{m} x_i^{-Ek\lambda_i} \right) \\ &= \ t_m^k T^k \prod_{i=1}^{m} t_i{}^k \ mod \ p = R \end{aligned}$$

Như vậy GM đã thành công trong việc giả mạo chữ ký của thành viên thứ m trong nhóm ký do người này quản lý.

Do đó, khi triển khai lược đồ chữ ký nhóm trên thực tế, để chống lại kiểu tấn công giả mạo này cần phải có một bộ phận, một cá nhân, đủ tin cậy đóng vai trò quản lý nhóm (thường gọi là bên thứ 3). Theo đó, khi xây dựng một nhóm ký, bên thứ 3 có trách nhiệm tiếp nhận public key của từng thành viên tham gia ký rồi tính và công bố public key chung của nhóm ký. Public key của các thành viên cũng phải được công bố công khai trong nhóm ký cho mọi thành viên của nhóm được biết. Các public key riêng của các thành viên và public key chung của cả nhóm là cố định, kẻ giả mạo sẽ khó thể tính toán lại như trong biểu thức $(*)$. Vì vậy lược đồ sẽ an toàn nếu được triển khai đúng đắn.

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

Các lược đồ chữ ký tập thể đại diện được xây dựng trên cơ sở của lược đồ chữ ký nhóm. Các lược đồ chữ ký nhóm lại được xây dựng trên cơ sở của bài toán khai căn modulo số nguyên tố lớn. Vì vậy lược đồ chữ ký tập thể đại diện thừa hưởng mức: i) Độ an toàn của bài toán khó mới, tìm căn modulo số nguyên tố lớn; ii) Ưu điểm bảo mật và khả năng chống tấn công từ lược đồ chữ ký nhóm.

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

Luận án đánh giá hiệu năng tính toán của các lược đồ chữ ký số 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	$U = \sum_{j=1}^{g}(243m_j + 1)\,T_m$ $e = [\sum_{j=1}^{g}(241m_j + 240) + 1]T_m$ $S = \sum_{j=1}^{g}(725m_j + 241)\,T_m$ $Sum = [\sum_{j=1}^{g}(1210m_j + 482) + 1]T_m$	$(481 + g)T_m$
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 cầu trúc $p = Nk2 + 1$ có chi phí thấp hơn nhiều sao với cấu trúc p còn lại (* Các ký hiệu sử dụng trong bảng trên đã được quy ước ở Chương 2).

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 hai dạng lược đồ: i) Chữ ký tập thể cho nhiều nhóm

ký (RCS.01-3.1 và RCS.01-3.2) và ii) Chữ ký tập thể cho nhiều nhóm ký và nhiều cá nhân ký (RCS.02-3.1 và RCS.02-3.2). Luận án cũng đã xây dựng các lược đồ chữ ký tập thể (CDS-3.1 và CDS-3.2) và các lược đồ chữ ký nhóm (GDS-3.1 và GDS-3.2) để làm lược đồ cơ sở cho các lược đồ chữ ký tập thể đại diện. Như vậy có 4 lược đồ chữ ký tập thể đại diện, hai lược đồ chữ ký tập thể và hai lược đồ chữ ký nhóm được xây dựng trong Chương 3. Tính đúng đắn, khả năng chống tấn công và chi phí tính toán của các lược đồ chữ ký tập thể đại diện được trình bày ở cuối chương.

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

CHƯƠNG 4:

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

Những nội dung đã được trình bày trong chương 2 và chương 3 đã chứng tỏ, lược đồ chữ ký tập thể đại diện mà nghiên cứu sinh nghiên cứu và xây dựng có tính khả thi cao, vì nó được xậy dựng dựa trên nhiều bài toán khó, nhiều chuẩn chữ ký số và nhiều lược đồ chữ ký chuẩn khác nhau. Tuy nhiên, 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 3 xuống còn 2 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. Cụ thể, chương này trình bày những nội dung sau: i) Vấn đề cần cải thiện của các lược đồ đã xây dựng và hướng giải quyết; ii) Xây dựng lược đồ chữ ký tập thể đại diện hai thành phần dựa trên bài toán logarit rời rạc; iii) Xây dựng lược đồ chữ ký tập thể đại diện dựa trên hai bài toán khó, logarit rời rạc và phân tích thừa số, với $p = 2n + 1$ và iv) Những vấn đề liên quan đến mức độ an toàn và hiệu năng tính toán của các lược đồ được xây dựng.

Như vậy, chương 4 được xem như sự mở rộng và hoàn thiện của chương 2 và chương 3, đồng thời nó cũng là sự "kết lại" của toàn bộ luận án.

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.. Trong Chương 4 này, NCS đề xuất: i) Dạng chữ ký số tập thể đại diện hai thành phần và ii) Dạng chữ ký số 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 chữ ký được đề xuất.

4.1.1. Chữ ký số tập thể đại diện 2 thành phần

Như đã biết, chữ ký nhóm là một dạng đa chữ ký, mà nó được hình thành

từ một nhóm người ký, được điều khiển bởi người trưởng nhóm (người quản lý nhóm ký). Chữ ký loại này thường gồm hai thành phần, hay cặp hai số nguyên đủ lớn E và S. Một lược đồ chữ ký nhóm phải đáp ứng các yêu cầu tối thiểu sau đây: i) Một tập (subset) bất kỳ người ký cá nhân, được chọn trong một nhóm thành viên, có thể tạo ra chữ ký, đại diện cho nhóm ký, trên tài liệu M; ii) Người quản lý nhóm ký có thể định danh tất cả những ai đã tham gia vào quá trình hình thành chữ ký nhóm của nhóm ký mà họ quản lý và chỉ có người quản lý nhóm mới có thể thực hiện được việc này; và iii) Những người bên ngoài nhóm ký không thể thiết lập một tập (subset) người ký cá nhân, để những người này tạo ra chữ ký nhóm đại diện cho nhóm ký.

Loại chữ ký nhóm tán thành (Approved Group Digital Signatures: AGDS) được sử dụng làm lược đồ cơ sở cho lược đồ chữ ký tập thể đại diện, còn thỏa mãn các điều kiện bổ sung sau đây: i) Không bất kỳ ai trong nhóm ký, kể cả người quản lý nhóm, biết được private key mà những người ký cá nhân sử dụng trong quá trình hình thành chữ ký nhóm; ii) Chữ ký nhóm được hình thành qua hai giai đoạn: Đầu tiên, mỗi người ký cá nhân tạo ra các tham số liên quan và chữ ký cá nhân chia sẻ của họ, và rồi chuyển tất cả đến cho người quản lý nhóm. Sau đó, người quản lý nhóm kiểm tra tính hợp lệ của mỗi chữ ký cá nhân chia sẻ nhận được, nếu tất cả là hợp lệ thì người quản lý tiến hành tạo ra chữ ký nhóm cuối cùng, từ các chữ ký chia sẻ và chữ ký của chính người quản lý. Đây là lý do mà chữ ký này có tên là chữ ký nhóm tán thành.

Do đó, để đáp ứng các điều kiện trên, chữ ký nhóm tán thành đã được thiết kế theo dạng gồm bộ 3 thành phần U, E và S. Thành phần U được sử dụng để lưu trữ thông tin của tất cả thành viên đã tham gia vào việc hình thành chữ ký nhóm, làm cơ sở cho việc định danh người ký sau này. Rõ ràng, việc lưu lại thông tin của những ai đã tham gia vào việc hình thành chữ ký nhóm là cần thiết, nhưng nó lại làm cho kích thước của chữ ký nhóm tăng lên đáng kể, đây được xem là hạn chế của các lược đồ chữ ký nhóm. Vì lược đồ chữ ký tập thể đại diện được xây dựng trên cơ sở của lược đồ AGDS, nên đây cũng chính là hạn chế của chữ ký tập thể đại điện ba thành phần (U, E, S). Để khắc phục hạn chế này, NCS tiến hành thay đổi lược đồ AGDS, và kéo theo thay đổi lược đồ chữ ký tập thể đại diện, để nó cho phép tạo ra chữ ký nhóm và chữ ký tập thể đại diện chỉ gồm bộ 2 thành phần (E, S).

Tất nhiên, vẫn chứa đầy đủ thông tin cần thiết để sau này có thể định danh được những ai đã tham gia vào việc tạo ra chữ ký nhóm của nhóm ký. Những thông tin này được chứa trong thành phần ngẫu nhiên (R), được sử dụng để hình thành thành phần E của chữ ký nhóm, chữ ký tập thể đại diện sau cùng.

Trong các lược đồ chữ ký nhóm 3 thành phần, tham số ngẫu nhiên (R) được hình thành từ một giá trị số được chọn một cách ngẫu nhiên (t). Trong giao thức chữ ký nhóm 2 thành phần, vì thông tin của tất cả người ký tham gia vào quá trình tạo ra chữ ký được nhúng vào tham số ngẫu nhiên (R), nên giá trị ngẫu nhiên (T) không được chọn một cách ngẫu nhiên mà nó được hình bởi một thuật toán sinh giá trị giả ngẫu nhiên nào đó. Tham số ngẫu nhiên trong trường hợp này không những thỏa mãn các yêu cầu về tính duy nhất, tính bí mật và tính không thể đoán trước mà còn đảm bảo chức năng bảo vệ private key của những người tham gia vào việc hình chữ ký nhóm của nhóm ký. Thuật toán sinh số ngẫu nhiên giả được sử dụng trong các lược đồ chữ ký nhóm dưới đây đáp ứng đầy đủ điều này.

Thủ tục sinh AGDS trong trường hợp này, tạo ra chữ ký nhóm 2 thành phần, được thực hiện qua các bước sau đây:

1. Tập những người ký cá nhân cùng nhau tạo ra một chữ ký tập thể trên tài liệu M cần ký. Sau đó, gửi chữ ký tập thể vừa tạo được $(E_{\text{col}}, S_{\text{col}})$ đến cho người quản lý nhóm.

2. Người quản lý nhóm sử dụng chữ ký tập thể nhận được $(E_{\text{col}}, S_{\text{col}})$, tài liệu M và private key z của mình để tính giá trị giả ngẫu nhiên T, theo thuật toán đã được xác định trước.

3. Sử dụng giá trị giả ngẫu nhiên vừa tính được, người quản lý nhóm tính thành phần ngẫu nhiên của chữ ký nhóm (R), và rồi tính hai thành phần của chữ ký của trưởng nhóm (E, S) trên tài liệu M. Đây cũng chính là chữ ký nhóm của cả nhóm ký trên tài liệu M.

Như vậy, kích thước của chữ ký nhóm và chữ ký tập thể đại diện đã được giảm bằng cách không sử dụng thành phần U để chứa thông tin người ký, mà những thông tin này được nhúng vào tham số ngẫu nhiên R.

Tức là chữ ký nhóm và chữ ký tập thể đại diện được rút gọn còn 2 thành phần (E, S), nhưng vẫn chứa đầy đủ những thông tin cần thiết để phục vụ cho việc định danh người ký sau này.

4.1.2. Chữ ký số tập thể được xây dựng dựa trên 2 bài toán khó

Hầu hết các chữ ký số đều được xây dựng dựa trên tính khó giải của một bài toán khó, như: i) Bài toán phân tích một số nguyên lớn thành các thừa số nguyên tố [58-59], [55]; ii) Bài toán logarit rời rạc trên trường hữu hạn nguyên tố [54], [55]; iii) Bài toán logarit rời rạc trên đường cong Elliptic [90], [92], [96] và iv) Bài toán tìm căn modulo số nguyên tố lớn [65], [54]. Điều này không phân biệt đó là chữ ký số đơn [1-3] hay chữ ký số mù [46], chữ ký số nhóm [77], [82-86] hay chữ ký số tập thể [42], [55], chữ ký mù [89] hay chữ ký tập thể mù [80] v.v.. Hai dạng chữ ký tập thể đại diện được đề xuất trong luận án này cũng không phải là ngoại lệ. NCS đã xây dựng thành công các lược đồ này trên các bài toán khó đã kể ở trên (xem Chương 2, 3).

Khả năng chống tấn công và mức độ an toàn của các thuật toán chữ ký số được xây dựng dựa trên một bài toán khó đã được kiểm chứng và được tin dùng, nhưng tất cả đều phụ thuộc vào độ khó giải của bài toán mà nó sử dụng. Hiện tại chưa có thuật giải thời gian đa thức nào được đưa ra, trừ các thuật toán lượng tử, có thể giải được các bài toán khó như phân tích thừa số, bài toán logarit rời rạc và bài toán tìm căn modulo số nguyên tố v.v. nên các lược đồ chữ ký số được xây dựng trên cơ sở một trong những bài toán khó này đảm bảo mức độ an toàn cần thiết. Điều này có nghĩa, trong tương lai, nếu có một thuật giải thời gian đa thức cho một bài toán khó nào đó thì xem như mức độ an toàn của lược đồ chữ ký số được xây dựng dựa trên bài toán khó này sẽ bị phá vỡ hoàn toàn.

Liên quan đến vấn đề này, để nâng cao mức độ an toàn cho các lược đồ chữ ký số, người ta tìm cách xây dựng lược đồ dựa trên đồng thời hai bài toán khó như: Phân tích thừa số và Logarit rời rạc [59-60], [78], [94-95]; Logarit rời rạc và Khai căn; Logarit rời rạc trên trường hữu hạn nguyên tố và Logarit rời rạc trên đường cong Elliptic… Khi đó, để phá vỡ được các lược đồ này thì, về mặt lý thuyết, kẻ tấn công phải giải quyết được cả hai bài toán khó liên quan.

Thực tế cũng đã chỉ ra rằng, có một số lược đồ chữ ký được xây dựng trên cả hai bài toán khó, nhưng kẻ tấn công chỉ cần giải quyết được một bài toán khó, hoặc thậm chí không cần giải quyết bài toán khó nào, thì đã có thể phá vỡ được lược đồ. Ví dụ: Vào năm 1994, He và Kiesler [48] đề xuất các giao thức chữ ký số dựa trên hai bài toán khó, phân tích thừa số (i) và logarit rời rạc (ii). Nhưng một

năm sau đó, Harn [61] cho thấy các giao thức của He và Kiesler có thể bị phá vỡ nếu kẻ tấn công có khả năng giải quyết chỉ một vấn đề (i). Trong khi đó Lee và Hwang [69] lại cho rằng, chỉ cần kẻ tấn công có thể giải quyết được vấn đề (ii) thì họ có thể phá vỡ các chữ ký của He-Kiesler. Shimin Wei [91] lại cho rằng, bất kỳ kẻ tấn công nào cũng có thể giả mạo chữ ký của He-Kiesler mà không cần giải quyết bất kỳ bài toán khó nào; Vào năm 2005, Shao cho thấy [100], thuật toán chữ ký của Tzeng [95] là không an toàn, nếu kẻ tấn công giải quyết được vấn đề logarit rời rạc thì có thể dễ dàng giả mạo chữ ký của Tzeng trên bất kỳ tài liệu số nào, bằng cách sử dụng thuật toán được Pollard và Schorr đề xuất trong [49]. Shao cũng cho rằng, thuật toán chữ ký của Tzeng thực chất chỉ phụ thuộc vào một bài toán khó, phân tích thừa số hoặc logarit rời rạc v.v..

Tuy vậy, hầu hết các lược đồ chữ ký số được xây dựng trên hai bài toán khó đều thể hiện mức độ an toàn cao của nó. Trong [34], Ismail E.S. và cộng sự cho thấy, giao thức chữ ký dựa trên đồng thời hai bài toán khó, phân tích thừa số và logarit rời rạc, mà họ xây dựng có thể chống lại năm dạng tấn công phổ biến vào lược đồ chữ ký số và có chi phí thời gian cho việc sinh và kiểm tra chữ ký là ngang bằng với các chữ ký dựa trên một bài toán khó.

Đây là cơ sở để NCS chọn hướng tiếp cận, xây dựng chữ ký dựa trên đồng thời hai bài toán khó, logarit rời rạc và phân tích thừa số, để cải thiện mức độ an toàn của lược đồ chữ ký tập thể đại diện đề xuất trong luận án này.

4.2. Xây dựng lược đồ chữ số 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 số nhóm (Ký hiệu: GDS-4.2)

Phần này mô tả lược đồ chữ ký nhóm 2 thành phần [CT4], từ cơ sở các lược đồ chữ ký nhóm 3 thành phần đã được mô tả trong Chương 2 và Chương 3. Nhóm ký trong trường hợp này gồm m người ký và một người đóng vai trò người quản lý nhóm (GM). Các tham số đầu vào được chọn như trong lược đồ CDS-4.2. M là tài liệu cần được tạo ra chữ ký nhóm trên đó.

Mỗi người ký thứ j tạo ra một số bí mật ngẫu nhiên x_j để làm private key. Public key y_j được tính theo công thức: $y_j = \alpha^{x_j} \bmod p$; $j = 1, 2, 3, \dots, m$; GM cũng chọn số bí mật ngẫu nhiên z, $z < q$, làm private key. Public key của GM là:

$Y = \alpha^z \, mod \, p$. Y này cũng là public key của nhóm ký.

Các thủ tục chính của lược đồ chữ ký nhóm hai thành phần trên tài liệu M được mô tả như dưới đây.

- **Thủ tục sinh chữ ký nhóm 2 thành phần trên tài liệu *M***

Chữ ký nhóm trong trường hợp này được hình thành qua hai gia đoạn: i) Tạo chữ ký tập thể trên tài liệu M, được thực hiện bởi một tập thể m người ký cá nhân; ii) Trên cơ sở chữ ký tập thể vừa được tạo ra GM tạo chữ ký nhóm 2 thành phần, đại diện cho cả nhóm ký.

1. Những signer cá nhân tạo một chữ ký tập thể trên bản tin M:

1.1. Mỗi signer thứ i sinh một số ngẫu nhiên t_i, $t_i < r$, và rồi tính R_i:

$$R_i = \alpha^{t_i} \, mod \, p \tag{4.1}$$

Sau đó gửi R_i cho những người ký khác trong nhóm (i = 1, 2, …, m).

1.2. Một signer nào đó trong nhóm ký, hoặc tất cả, tính R_{col}:

$$R_{col} = (R_1 R_2 \ldots R_m) \, mod \, p = \alpha^{t_1 + t_1 + .. + t_m} \, mod \, p \tag{4.2}$$

Và tính E_{col}:

$$E_{\text{col}} \; = \; F_H(M \parallel R_{\text{col}}) \; mod \; 2^{80} \tag{4.3}$$

Trong đó F_H là một hàm băm cho trước. Giá trị E_{col} là thành phần đầu tiên trong chữ ký tập thể.

1.3. Mỗi signer thứ i tính giá trị chia sẻ cá nhân S_i:

$$S_i = E_{\text{col}}(t_i + x_i E_{\text{col}}) \, mod \, r \tag{4.4}$$

Và rồi gửi S_i đến những signer khác trong nhóm ký.

1.4. Một signer nào đó trong nhóm ký, hoặc tất cả, tính S_{col}:

$$S_{\text{col}} = (S_1 + S_2 + \ldots + S_m) \, mod \, r \tag{4.5}$$

Vậy bộ giá trị (E_{col}, S_{col}) là chữ ký tập thể của nhóm ký gồm m thành viên. Độ dài của chữ ký là: $|E_{\text{col}}| + |S_{\text{col}}| \approx 240$ bít.

Chữ ký tập thể này được chuyển đến cho GM.

2. GM kiểm tra/xác thực của chữ ký tập thể nhận được (E_{col}, S_{col}) bằng việc kiểm

tra biểu thức sau:

$$R_{\text{col}} = y_{\text{col}}^{-E_{\text{col}}} \alpha^{E_{\text{col}}^{-1} S_{\text{col}}} \, mod \, p \tag{4.6}$$

Trong đó

$$y_{\text{col}} = (y_1 y_2 \ldots y_m) \, mod \, p \tag{4.7}$$

Nếu chữ ký tập thể là hợp lệ, GM cần tính giá trị giả ngẫu nhiên T:

$$T \; = \; (E_{\text{col}} \parallel S_{\text{col}})^{z^*} H_z \, mod \, \text{q} \tag{4.8}$$

Trong đó: $H_z = F_H(M, \, z) \, mod \, q$ và

$$z^* = \min\{z_i \colon \, z_i = z + i; \, \gcd(z_i, \, q - 1) = 1; \, i = 0, 1, 2, \ldots\} \tag{4.9}$$

3. GM tính các giá trị R, E và S:

$$R = \alpha^T \, mod \, p, \tag{4.10}$$

$$E \; = \; F_H(M \parallel R) \, mod \, 2^{128} \tag{4.11}$$

và

$$S = E(T + zE) \, mod \, q \tag{4.12}$$

Vậy bộ giá trị (E, S) là chữ ký nhóm của nhóm ký gồm m người ký, và một người trưởng nhóm, trên tài liệu M. Độ dài là | E | + | S | = 384 bít.

- **Thủ tục kiểm tra chữ ký nhóm 2 thành phần trên tài liệu 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:

2. Tính giá trị tham số ngẫu nhiên R^* theo công thức:

$$R^* = Y^{-E} \, \alpha^{E^{-1} S} \, mod \, p \tag{4.13}$$

3. Tính E theo công thức:

$$E^* = F_H(M \| R^*) \, mod \, 2^{128} \tag{4.14}$$

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.

- **Chứng minh tính đúng của lược đồ chữ ký GDS-4.2**

Tính đúng của lược đồ chữ ký số nhóm này thể hiện qua: i) Sự tồn tại của công thức kiểm tra chữ ký tập thể R_{col} (4.6) và ii) Sự tồn tại của biểu thức kiểm

tra $E^* = E$. Cụ thể như sau:

a) Tính đúng của công thức kiểm tra chữ ký tập thể:

Dễ thấy công thức kiểm tra chữ ký tập thể luôn đúng. Thật vậy:

$$\begin{aligned} R_{col} &= y_{col}^{-E_{col}} \alpha^{E_{col}^{-1} S_{col}} \, mod \, p \\ &= \alpha^{\sum_{i=1}^{m} -x_i E} \alpha^{E^{-1} E (\sum_{i=1}^{m} t_i + x_i E)} \, mod \, p \\ &= \alpha^{\sum_{i=1}^{m} t_i} \, mod \, p \\ &= \prod_{i=1}^{m} R_i \bmod p = R_{col} \end{aligned}$$

b) Tính đúng của thủ tục kiểm tra chữ ký nhóm:

Dễ thấy, biểu thức kiểm tra chữ ký $E^* = E$ luôn tồn tại. Thật vậy:

$$\begin{aligned} R^* &= Y^{-E} \, \alpha^{E^{-1} S} \, mod \, p \\ &= \alpha^{-zE} \, \alpha^{E^{-1} E (T + zE)} \, mod \, p \\ &= \alpha^{T} \, mod \, p = R \end{aligned}$$

Và tính:

$$\begin{aligned} E^* &= F_H(M \| R^*) \, mod \, 2^{128} \\ &= F_H(M \| R) \; mod \, 2^{128} = E \end{aligned}$$

Vậy biểu thức $E^* = E$ luôn tồn tại: Điều này chứng tỏ tính đúng của thủ tục kiểm tra chữ ký, hay tính đúng của lược đồ GDS-4.2, luôn được đảm bảo.

- **Thủ tục định danh người ký, được thực hiện bởi người quản lý nhóm, gồm các bước sau:**

- Sử dụng chữ ký nhóm (E, S) để tính lại T theo công thức:

$$T = SE^{-1} - zE \, mod \, q \tag{4.15}$$

- Tính $H_z = F_H(M, z) \, mod \, q$, và rồi tính lại giá trị chữ ký tập thể $E_{col} || S_{col}$ theo công thức:

$$E_{\text{col}} \| S_{\text{col}} = (T {H_z}^{-1})^{z^{-1} \, mod \, (q-1)}. \tag{4.16}$$

- Chọn một nhóm ký (subset) gồm m thành viên bất kỳ từ tập thể ký (đây là nhóm signer được chọn ra từ tập thể ký, họ được giao nhiệm vụ tạo ra chữ ký tập thể trên tài liệu M): Sử dụng public key của nhóm ký này để tạo ra public key tập thể. Sử dụng public key tập thể vừa được tính để tính lại $E_{col} || S_{col}$: Nếu giá trị

này bằng $E_{col}||S_{col}$ của (4.16) thì chính những người trong nhóm ký này đã tham gia vào việc tạo chữ ký tập thể của tập thể ký; Nếu ngược lại, người quản lý nhóm sẽ chọn nhóm ký khác và thực hiện như trên cho đến khi tìm được nhóm ký mà public key của họ dẫn đến việc tạo được cặp giá trị $E_{col}||S_{col}$ thỏa (4.16). Tức là, lặp lại cho đến khi định danh được những người ký đã tham gia tạo ra chữ ký của tập thể thì dừng lại (Ở đây chấp nhận: Xác suất trùng hợp ngẫu nhiên là không đáng kể).

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 tài liệu 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 tài liệu 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:

$$Y_{col} = \prod_{j=1}^{g} Y_j \; mod \, p \tag{4.22}$$

2. Tính giá trị R^* theo công thức:

$$R^* = Y_{col}^{-E} \alpha^{E^{-1}S} \, mod \, p \tag{4.23}$$

3. Tính giá trị E^* theo công thức:

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

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.

- **Chứng minh tính đúng của lược đồ RCS.01-4.2:**

Tính đúng của lược đồ chữ ký tập thể đại diện này thể hiện qua: i) Sự tồn tại của công thức kiểm tra chữ ký chia sẻ S_j được chia sẻ bởi các trưởng nhóm ký R_j; và ii) Sự tồn tại của biểu thức kiểm tra $E^* = E$ trong thủ tục kiểm tra chữ ký.

a) Chứng minh tính đúng của chữ ký thành viên:

Dễ thấy công thức kiểm tra chữ ký chia sẻ S_j được chia sẻ bởi các trưởng nhóm ký R_j luôn tồn tại. Thật vậy:

$$\begin{aligned} R_j^* &= Y_j^{-E} \; \alpha^{E^{-1}S_j} \, mod \, p \\ &= \alpha^{-z_j E} \; \alpha^{E^{-1}E(T_j + z_j E)} \, mod \, p \\ &= \alpha^{T_j} \, mod \, p = R_j \end{aligned}$$

b) Chứng minh tính đúng của chữ ký cuối cùng:

Dễ thấy, biểu thức kiểm tra chữ ký $E^* = E$ luôn tồn tại. Thật vậy:

$$R^* = Y_{col}^{-E}\,\alpha^{E^{-1}S}\ mod\ p$$
$$= \prod_{j=1}^{g}\left(Y_j^{-E}\right)\alpha^{E^{-1}\sum_{j=1}^{g}S_j}\ mod\ p$$
$$= \prod_{j=1}^{g}(\alpha^{-z_jE})\,\alpha^{E^{-1}\sum_{j=1}^{g}E(T_j+z_jE)}\ mod\ p$$
$$= \prod_{j=1}^{g}(\alpha^{-z_jE})\prod_{j=1}^{g}(\alpha^{T_j+z_jE})\ mod\ p$$
$$= \prod_{j=1}^{g}\alpha^{T_j}\ \ mod\ p = \prod_{j=1}^{g}R_j\ mod\ p = R$$

Vì $R^* = R$ nên

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

Vậy biểu thức $E^* = E$ luôn tồn tại: Điều này chứng tỏ tính đúng của thủ tục kiểm tra chữ ký luôn được đảm bảo.

Từ (a) và (b): Tính đúng của lược đồ RCS.01-4.2 được đảm bảo.

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.

- **Thủ tục sinh chữ ký tập thể cho g nhóm ký và m người ký cá nhân trên tài liệu M**

Gồm các bước sau:

1a. GM của mỗi nhóm ký j thực hiện:

- Sinh chữ ký nhóm theo như lược đồ cho nhóm ký GDS-4.2 ở trên và rồi

gửi R_j đến tất cả GM của các nhóm ký trong tập thể ký.

- R_j là thành phần chia sẻ của nhóm ký thứ j để tạo tham số ngẫu nhiên của chữ ký tập thể.

1b. Mỗi cá nhân ký thứ j thực hiện các công việc sau:

- Chọn 1 số ngẫu nhiên t_j và tính giá trị ngẫu nhiên R_j theo công thức:

$$R_j = \alpha^{t_j} \, mod \, p \tag{4.25}$$

- Gửi giá trị R_j tới tất cả những GM và những cá nhân ký khác trong tập thể ký.

2. Một GM hoặc một cá nhân ký nào đó trong tập thể ký tính các giá trị R và E theo các công thức:

$$R = \prod_{j=1}^{g+m} R_j \tag{4.26}$$

$$E = F_H(M \| R) \, mod \, 2^{128} \tag{4.27}$$

Trong đó $j = 1, 2, 3, \dots, g + m$. E là thành phần đầu tiên của chữ ký nhóm.

3a. GM của mỗi nhóm thứ j thực hiện:

- Tính thành phần chia sẻ S_j của nhóm j theo công thức:

$$S_j = E\left(T_j + z_j E\right) mod \, q \tag{4.28}$$

- Gửi S_j cho các GM và các cá nhân ký khác trong tập thể ký.

3b. Mỗi cá nhân ký thứ j ($j = g + 1, g + 2, \dots, g + m$) thực hiện:

- Tính thành phần chia sẻ S_j của họ theo công thức:

$$S_j = E\left(t_j + x_j E\right) mod \, q \tag{4.29}$$

- Gửi S_j cho những GM và cá nhân ký khác trong tập thể ký.

4. Một GM hoặc một cá nhân ký nào đó trong tập thể ký thực hiện:

- Kiểm tra tính hợp lệ của mỗi S_j theo công thức:

$$R_j = Y_j^{-E} \, \alpha^{E^{-1} S_j} \, mod \, p \tag{4.30}$$

với $j = 1, 2, \dots, g$ và

$$R_j = y_j^{-E} \, \alpha^{E^{-1} S_j} \, mod \, p \tag{4.31}$$

với $j = g + 1, g + 2, \dots, g + m$

- Nếu tất cả đều thoả mãn, thành phần thứ ba của chữ ký nhóm sẽ được

tính theo công thức:

$$S = \sum_{j=1}^{g+m} S_j \ mod\ p \tag{4.32}$$

Vậy cặp giá trị (E, S) là chữ ký tập thể đại diện, của một tập thể gồm g nhóm ký và m cá nhân ký, trên tài liệu. Nó đại diện cho tập thể ký này.

- **Thủ tục kiểm tra chữ ký tập thể cho nhiều nhóm ký và nhiều cá nhân ký trên tài liệu *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 theo công thức:

$$Y_{col} = \prod_{j=1}^{g} Y_j \prod_{j=g+1}^{g+m} y_j \ mod\ p \tag{4.33}$$

2. Tính giá trị tham số ngẫu nhiên R^* theo công thức:

$$R^* = Y_{col}^{-E} \alpha^{E^{-1}S} \ mod\ p \tag{4.34}$$

3. Tính E^* theo công thức:

$$E^* = F_H(M \| R) \ mod\ 2^{128} \tag{4.35}$$

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.

- **Chứng minh tính đúng của lược đồ chữ ký RCS.02-4.2**

Tính đúng của lược đồ chữ ký tập thể đại diện này thể hiện qua: i) Sự tồn tại của công thức kiểm tra chữ ký chia sẻ S_j của mỗi nhóm ký (4.30); ii) Sự tồn tại của công thức kiểm tra chữ ký chia sẻ S_j của mỗi cá nhân ký (4.31) và iii) Sự tồn tại của biểu thức kiểm tra $E^* = E$. Cụ thể như sau:

a) Tính đúng của công thức kiểm tra chữ ký chia sẻ của mỗi trưởng nhóm:

Dễ thấy công thức kiểm tra chữ ký chia sẻ của mỗi trưởng nhóm luôn tồn tại. Thật vậy:

$$\begin{aligned} R_j^* &= Y_j^{-E}\ \alpha^{E^{-1}S_j} \ mod\ p \\ &= \alpha^{-z_j E}\ \alpha^{E^{-1}E(T_j + z_j E)} \ mod\ p \\ &= \alpha^{T_j} \ mod\ p = R_j \end{aligned}$$

b) Tính đúng của công thức kiểm tra chữ ký chia sẻ mỗi signer:

Dễ thấy công thức kiểm tra chữ ký chia sẻ của mỗi trưởng nhóm luôn tồn tại. Thật vậy:

$$\begin{aligned} R_j^* &= y_j^{-E}\alpha^{E^{-1}S_j} \bmod p \\ &= \alpha^{-x_jE}\ \alpha^{E^{-1}E(T_j+x_jE)} \bmod p \\ &= \alpha^{t_j} \bmod p = R_j \end{aligned}$$

c) Tính đúng của thủ tục kiểm tra chữ ký tập thể đại diện:

Dễ thấy, biểu thức kiểm tra chữ ký $E^* = E$ luôn tồn tại. Thật vậy:

$$\begin{aligned} R^* &= Y_{col}^{-E}\alpha^{E^{-1}S} \bmod p \\ &= \prod_{j=1}^{g} Y_j^{-E} \prod_{j=g+1}^{g+m} y_j^{-E}\ \alpha^{E^{-1}\sum_{j=1}^{g+m} S_j} \bmod p \\ &= \prod_{j=1}^{g}\left(Y_j^{-E}\alpha^{E^{-1}S_j}\right) \prod_{j=g+1}^{g+m}\left(y_j^{-E}\alpha^{E^{-1}S_j}\right) \bmod p \\ &= \prod_{j=1}^{g} R_j \prod_{j=g+1}^{g+m} R_j \bmod p \\ &= \prod_{j=1}^{g+m} R_j \bmod p = R \end{aligned}$$

Và tính: $E^* = F_H(M\|R^*) \bmod \delta$

$$= F_H(M\|R) \bmod \delta = E$$

Vậy biểu thức $E^* = E$ luôn tồn tại: Điều này chứng tỏ tính đúng của thủ tục kiểm tra chữ ký, hay tính đúng của lược đồ RCS.02-4.2, luôn được đảm bảo.

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 bít (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 số cá nhân (Ký hiệu: SDS-4.3)

Chọn tham số α có bậc n modulo p. Giá trị S trong phương trình xác minh

của Schnorr được thay bằng S^2.

Cho private key của signer là x $(1 < x < n - 1)$, public key tương ứng của người này là y: $y = \alpha^x \ mod \ p$.

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

Bao gồm các bước sau (Được thực hiện bởi người ký):

1. Chọn giá trị ngẫu nhiên k, thỏa $k < n$, và rồi tính:

$$R = \alpha^k \ mod \ p \tag{4.36}$$

2. Tính thành phần đầu tiên của chữ ký: $E = f(R, M)$, với f là một hàm nén cho trước. Có thể chọn hàm f như sau:

$$E = F_H(RH) \ mod \ \delta \tag{4.37}$$

Với δ là một số nguyên tố lớn |δ| =160 bít; F_H là một hàm băm một chiều như SHA-1 hoặc SHA-2; và H là giá trị băm được tính từ tài liệu M.

3. Tính giá trị S theo công thức:

$$S = (k + xE)^{1/2} \ mod \ n \tag{4.38}$$

Sao cho thỏa công thức:

$$R = \alpha^{S^2} y^{-E} \bmod p \tag{4.39}$$

Vậy cặp giá trị (S, E) là chữ ký đơn của người ký trên tài liệu M.

- **Thủ tục kiểm tra chữ ký cá nhân trên tài liệu *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 R^*:

$$R^* = \alpha^{S^2} y^{-E} \bmod p \tag{4.40}$$

2. Tính E^*:

$$E^* \ = F_H(R^* H) \ mod \ \delta \tag{4.41}$$

3. So sánh E^* và 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.

- **Chứng minh tính đúng của lược đồ SDS-4.3:**

Nếu chữ ký đã được hình thành là hợp lệ, tức là, việc sử dụng private key trong thủ tục tạo chữ ký là đúng thì biểu thức kiểm tra $E' = E$ trong thủ tục kiểm tra chữ ký luôn xảy ra. Vậy để chứng minh tính đúng của lược đồ này ta chỉ cần

chứng minh sự tồn tại của biểu thức $E' = E$.

Dễ thấy, biểu thức kiểm tra $E' = E$ luôn tồn tại. Thật vậy:

$$\begin{aligned} R^* &= \alpha^{S^2} y^{-E} \bmod p \\ &= \alpha^{(k+xE)} \alpha^{-xE} \bmod p \\ &= \alpha^k \bmod p = R \end{aligned} \tag{4.42}$$

Vì $R^* = R$ nên $E^* = R^* H \bmod \delta = RH \bmod \delta = E$.

Vậy biểu thức $E^* = E$ luôn tồn tại: Điều này chứng tỏ tính đúng của thủ tục kiểm tra chữ ký, hay tính đúng của lược đồ SDS-4.3, luôn được đảm bảo.

Nhận xét: Việc giải bài toán logarit rời rạc trên trường $GF(p)$ là không đủ để phá vỡ lược đồ này. Để phá vỡ được lược đồ, kẻ tấn công cần phải giải thêm được bài toán phân tích thừa số, phân tích n thành các thừa số nguyên tố q và q'.

Thật vậy, lời giải của bài toán logarit rời rạc dẫn đến việc tính được private key x và có thể tính được giá trị:

$$(k + xE) \bmod n = S^* \tag{4.43}$$

Tuy nhiên, để tính thành phần chữ ký S cần phải tính được căn bậc 2 modulo n từ giá trị S^*. Điều này yêu cầu phải giải quyết được bài toán phân tích được n thành thừa số q và q'.

Như vậy, đây chính là lược đồ chữ ký dựa trên hai bài toán khó: Phân tích thành nhân tử và Logarit rời rạc.

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

Phần này sử dụng lược đồ chữ ký cá nhân ở trên để xây dựng lược đồ chữ ký tập thể trên tài liệu M.

Giả sử có m người ký ($1 \leq i \leq m$) cùng một thông điệp M. Mỗi người ký chọn ngẫu nhiên một số nguyên x_i từ khoảng $[1, n-1]$ và tính một public key tương ứng: $y = \alpha^{x_i} \bmod p$ (x_i là private key của người dùng thứ i, α là một số ngẫu nhiên có bậc nguyên tố q mô-đun p).

Sau đây là các thủ tục chính của lược đồ chữ ký tập thể, gồm m người ký, ký lên tài liệu M.

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

Gồm các bước chính sau đây:

1. Mỗi signer chọn một số ngẫu nhiên k_i, $k_i \in [1, n-1]$, và tính:

$$R_i = \alpha^{k_i} \, mod \, p \tag{4.44}$$

Và gửi R_i cho tất cả những signer còn lại trong tập thể ký

2. Một signer nào đó, hoặc tất cả, trong tập thể ký tính giá trị ngẫu nhiên chung của tập thể R:

$$R = R_1 R_2 \dots R_m \ mod \, p \tag{4.45}$$

và tính thành phần đầu tiên của chữ ký tập thể:

$$E = f(R, M) \tag{4.46}$$

Với f là một hàm nén cho trước. Có thể như sau: $E = RH \, mod \, \delta$, với δ là một số nguyên tố lớn: $|\delta| = 160$ bít và H là giá trị băm được tính toán từ tài liệu M (E sẽ được quảng bá cho tất cả người tham gia ký).

3. Mỗi signer tính chữ ký chia sẻ S_i theo công thức sau:

$$S_i = (k_i + x_i E)^{1/2} \, mod \, n \tag{4.47}$$

Và rồi chuyển S_i cho tất cả signer khác trong tập người ký được chọn.

4. Một signer nào đó, hoặc tất cả, trong tập thể ký tính thành phần thứ hai của chữ ký tập thể S:

$$S = (S_1^2 + S_2^2 + \cdots + S_m^2)^{1/2} \bmod n \tag{4.48}$$

Vậy cặp giá trị (E, S) là chữ ký của tập thể gồm m người ký trên tài liệu M.

- **Thủ tục kiểm tra chữ ký tập thể trên tài liệu *M***

Gồm các bước sau (được thực hiện bởi người kiểm tra chữ ký):

1. Tính public key tập thể y:

$$y = y_1 y_2 \dots y_m \, mod \, p \tag{4.49}$$

2. Tính giá trị R^*:

$$R^* = \alpha^{S^2} y^{-E} \, mod \, p \tag{4.50}$$

3. Tính giá trị E':

$$E' = R^* H \, mod \, \delta \tag{4.51}$$

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.

- **Chứng minh tính đúng của lược đồ CDS-4.3:**

Nếu chữ ký tập thể được hình thành là hợp lệ, tức là, việc sử dụng private

key trong thủ tục tạo chữ ký là đúng thì biểu thức kiểm tra $E' = E$ trong thủ tục kiểm tra chữ ký luôn xảy ra. Vậy để chứng minh tính đúng của lược đồ này ta chỉ cần chứng minh sự tồn tại của biểu thức $\mathrm{E}' = E$.

Dễ thấy, biểu thức kiểm tra $E' = E$ luôn tồn tại. Thật vậy:

$$R^* = \alpha^{S_1^2+S_2^2+\cdots+S_m^2} \prod_{i=1}^{m} y_i^{-E} \bmod p$$

$$= \prod_{i=1}^{m} \alpha^{S_i^2} \prod_{i=1}^{m} \alpha^{x_i(-E)} \bmod p$$

$$= \prod_{i=1}^{m} \alpha^{k_i+x_iE} \prod_{i=1}^{m} \alpha^{x_i(-E)} \bmod p$$

$$= \prod_{i=1}^{m} \alpha^{k_i} \bmod p = \prod_{i=1}^{m} R_i \bmod p = R$$

Vì $R' = R$ nên $E^* = E$ ($E' = R^*H \ mod \ \delta = RH \ mod \ \delta = E$).

Vậy biểu thức $E^* = E$ luôn tồn tại: Điều này chứng tỏ tính đúng của thủ tục kiểm tra chữ ký, hay tính đúng của lược đồ CDS-4.4, luôn được đảm bảo.

Dễ dàng thấy rằng, trong giao thức sinh chữ ký của lược đồ chữ ký tập thể này, người ký không sinh ra chữ ký cá nhân, mà chỉ sinh ra thành phần chia sẻ (S_i) của họ, để góp với $n-1$ người ký được chọn khác hình thành chữ ký chung của tập thể ký (S) trên tài liệu M đã cho. Cơ chế này còn giúp, ngăn chặn ai đó, sử dụng tập thành phần chia sẻ của tập người ký này để tạo ra chữ ký tập thể mà nó liên quan đến tập người khác. Đây là những ưu điểm bảo mật của giao thức này, vì nó vừa đảm được tính bí mật của private key của mỗi thành viên tập thể ký, vừa đảm bảo tính toàn vẹn bên trong của chữ ký tập thể (S).

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

Phần này xây dựng lược đồ chữ ký nhóm, của một nhóm ký gồm m thành viên/người ký, trên tài liệu M.

Mỗi người ký i ($1 \le i \le m$) chọn ngẫu nhiên một số nguyên x_i, thuộc khoảng $[1, n-1]$, làm private key và tính một public key tương ứng theo công thức: $y = \alpha^{x_i} \ mod \ p$ (x_i là private key của người ký thứ i, α là một số ngẫu nhiên có bậc nguyên tố q modulo p).

Public key Y của người quản lý nhóm (GM) được tính như sau:

$Y = \alpha^X \ mod\ p$. Trong đó X là private key của người quản lý nhóm. Giá trị Y cũng là public key của nhóm, và được dùng để xác minh chữ ký.

Sau đây là các thủ tục chính của lược đồ chữ ký nhóm, gồm m thành viên (hay "người ký"), ký lên tài liệu M.

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

Gồm các bước sau:

1. GM thực hiện các việc sau:

- Tính giá trị băm từ tài liệu M: $H = F_H(M)$, trong đó F_H là một hàm băm được chỉ định trước

- Tính giá trị mặt nạ λ_i cho từng signer trong tập thể ký:

$$\lambda_i = F_H(H \ \|y_i\| \ F_H(H \ \|y_i\| \ X)) \tag{4.52}$$

- Gửi λ_i đến những signer tương ứng trong nhóm ký

- Tính thành phần thứ nhất của chữ ký nhóm:

$$U = \prod_{i=1}^{m} y_i^{\lambda_i} \ mod\ p \tag{4.53}$$

2. Mỗi signer thực hiện như sau:

- Chọn một số ngẫu nhiên k_i, $k_i \in [1, n-1]$, và tính:

$$R_i = \alpha^{k_i} \ mod\ p \tag{4.54}$$

- Gửi R_i cho GM

3. GM sinh một số ngẫu nhiên K, $K < q$, và rồi tính các giá trị ngẫu nhiên cá nhân R':

$$R' = \alpha^K \ mod\ p, \tag{4.55}$$

- Rồi tính giá trị ngẫu nhiên cho nhóm ký

$$R = R' \prod_{i=1}^{m} R_i \ mod\ p = \alpha^{K + \sum_{i=1}^{m} k_i} \tag{4.56}$$

- Và tính thành phần thứ hai của chữ ký E:

$$E = F_H(M \| R \| U) \ mod\ \delta \tag{4.57}$$

Với δ là một số nguyên tố lớn: $|\delta| = 160\ bít$.

Giá trị E là thành phần thứ hai của chữ ký (E sẽ được quảng bá cho tất cả

thành viên nhóm tham gia vào việc hình thành chữ ký).

4. Mỗi signer tính chữ ký chia sẻ S_i và gửi nó cho GM:

$$S_i = (k_i + x_i\lambda_i E)^{1/2}\ mod\ n \tag{4.58}$$

5. GM thực hiện các công việc cuối cùng:

- Xác minh tính đúng của mỗi S_i bằng biểu thức:

$$R_i = \alpha^{{S_i}^2} y^{-\lambda_i E}\ mod\ p \tag{4.59}$$

- Nếu tất cả chữ ký chia sẻ S_i đều đúng. GM tính giá trị chia sẻ cá nhân:

$$S' = (K + XE)^{1/2}\ mod\ p \tag{4.60}$$

- Và rồi tính thành phần thứ ba của chữ ký nhóm:

$$S = ({S'}^2 + \sum_{i=1}^{m} {S_i}^2)^{1/2} \bmod n \tag{4.61}$$

Vậy bộ ba giá trị (U, E, S) là chữ ký nhóm của nhóm ký gồm m thành viên trên tài liệu M.

- **Thủ tục kiểm tra chữ ký nhóm trên tài liệu M:**

Gồm các bước sau (được thực hiện bởi người kiểm tra)

1. Tính giá trị băm của bản tin M:

$$H = F_H(M) \tag{4.62}$$

2. Tính lại giá trị ngẫu nhiên của nhóm ký:

$$R^* = \alpha^{S^2}(UY)^{-E}\ mod\ p \tag{4.63}$$

3. Tính giá trị E:

$$E = F_H(M \| R \| U)\ mod\ \delta \tag{4.64}$$

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.

- **Chứng minh tính đúng của lược đồ GDS-4.3:**

Tính đúng của lược đồ chữ ký nhóm này thể hiện qua: i) Sự tồn tại của công thức kiểm tra chữ ký tập thể R_i (4.59); ii) Sự tồn tại của biểu thức kiểm tra $E^* = E$. Cụ thể như sau:

a) Chứng minh tính đúng của chữ ký chia sẻ cá nhân

Dễ thấy, biểu thức kiểm tra chữ ký chia sẻ luôn tồn tại. Thật vậy:

$$R_i^* = \alpha^{S_i^2} y_i^{-\lambda_i E} \bmod p$$
$$= \alpha^{(k_i + x_i \lambda_i E)} \alpha^{-x_i \lambda_i E} \bmod p$$
$$= \alpha^{k_i} \, mod \, p = R_i$$

b) Chứng minh tính đúng của lược đồ

Dễ thấy, biểu thức kiểm tra $E^* = E$ luôn tồn tại. Thật vậy:

Thay giá giá trị trong các biểu thức:

$$S = S'^2 + \sum_{i=1}^{m} S_i{}^2 \; mod \, p$$

$$Y = \alpha^X \, mod \, p$$

$$U = \prod_{i=1}^{m} y_i^{\lambda_i} \, mod \, p$$

vào vế phải của phương trình xác minh ta có:

$$R^* = \alpha^{S^2} (UY)^{-E} \, mod \, p$$
$$= \alpha^{S'^2 + \sum_{i=1}^{m} S_i{}^2} \left(\alpha^X \prod_{i=1}^{m} y_i{}^{\lambda_i} \right)^E \bmod p$$
$$= \alpha^{(K + XE) + \sum_{i=1}^{m} (k_i + x_i \lambda_i E)} \left(\alpha^{XE} \prod_{i=1}^{m} \alpha^{x_i \lambda_i E} \right) \bmod p$$
$$= \alpha^{K + \sum_{i=1}^{m} k_i} \, mod \, p = R$$

Vì $R^* = R$ nên $E^* = E$ ($E^* = R^* H \, mod \, \delta = RH \, mod \, \delta = E$).

Vậy biểu thức $E^* = E$ luôn tồn tại: Điều này chứng tỏ tính đúng của thủ tục kiểm tra chữ ký, hay tính đúng của lược đồ GDS-4.4, luôn được đảm bảo.

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

Phần này dựa vào lược đồ chữ ký tập thể và chữ ký nhóm ở trên để xây dựng lược đồ chữ ký nhóm cho các nhóm ký.

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 $Y_j = \alpha^{X_j} \, mod \, p$. 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 $i = 1, 2, \dots, m_j$) 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 đầu vào được chọn như ở lược đồ chữ ký nhóm.

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

Gồm các bước sau:

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

- Sinh tham số mặt nạ λ_{ji} cho những signer trong nhóm ký j theo công thức (4.52) trong lược đồ GDS-4.3.
- Tính giá trị thành phần đầu tiên của chữ ký:

$$U_j = \prod_{i=1}^{m_j} y_{ji}^{\lambda_{ji}} \ mod\ p \tag{4.65}$$

U như là giá trị chia sẻ thứ j trong thành phần đầu tiên của chữ ký tập thể nhóm.

- Tính tham số ngẫu nhiên:

$$R_j = R'_j \prod_{i=1}^{m_j} R_{ji} \ mod\ p \tag{4.66}$$

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

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

$$U = \prod_{j=1}^{g} U_j \ mod\ p \tag{4.67}$$

$$R = \prod_{j=1}^{g} R_j \ mod\ p \tag{4.68}$$

và

$$E = F_H(M \| R \| U) \ mod\ \delta \tag{4.69}$$

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

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

3) GM thứ j tính giá trị chia sẻ của nhóm j theo công thức sau:

$$S_j = (S'^2_j + \sum_{i=1}^{m_j} S_{ji}^2)^{1/2} \bmod n \tag{4.70}$$

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

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

4) Một GM nào đó, hoặc tất cả GM, trong tập thể ký xác thực tính đúng của S_j bằng các kiểm tra biểu thức R_j:

$$R_j = \alpha^{{S_j}^2} (U_j Y_j)^{-\lambda_j E} \; mod \; p \tag{4.71}$$

- Nếu tất cả S_j thoả mãn phương trình trên, thì phần tử thứ ba S của chữ ký tập thể được tính như sau:

$$S = \left(\sum_{j=1}^{g} {S_j}^2 \right)^{1/2} \mod n \tag{4.72}$$

Bộ ba giá trị (U, E, S) được sinh bởi thủ tục trên là chữ ký tập thể, đại diện cho một chữ ký tập thể ký gồm g nhóm ký, trên tài liệu M.

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

Gồm các bước sau (được thực hiện bởi bên kiểm tra chữ ký):

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

$$Y_{col} = \prod_{j=1}^{g} Y_j \; mod \; p \tag{4.73}$$

2. Tính giá trị R^*:

$$R^* = \alpha^{S^2} (U Y_{col})^{-E} \; mod \; p \tag{4.74}$$

3. Tính giá trị E^*:

$$E^* = F_H(M \| R^* \| U) \tag{4.75}$$

4. So sánh E^* và 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.

- **Chứng minh tính đúng của lược đồ RCS.01-4.3**

Tính đúng của lược đồ chữ ký tập thể đại diện này thể hiện qua: i) Sự tồn tại của công thức kiểm tra chữ ký chia sẻ S_j của mỗi nhóm ký R_j; và ii) Sự tồn tại của biểu thức kiểm tra $E^* = E$. Cụ thể như sau:

a) Chứng minh tính đúng của công thức kiểm tra chữ ký được chia sẻ của các nhóm ký:

Nếu S_j là hợp lệ thì công thức (4.71) luôn tồn tại. Thật vậy:

$$R_j^* = \alpha^{S_j^2}\left(U_j Y_j\right)^{-E} \; mod\; p$$
$$= \alpha^{S_j'^2 + \sum_{i=1}^{m_j} {S_{ji}}^2}\left(\alpha^{X_j}\prod_{i=1}^{m_j} {y_{ji}}^{\lambda_{ji}}\right)^{-E} \bmod p$$
$$= \alpha^{(K_j + X_j E) + \sum_{i=1}^{m_j}(k_{ji} + x_{ji}\lambda_{ji}E)}\left(\alpha^{-X_j E_j}\prod_{i=1}^{m_j}\alpha^{-x_{ji}\lambda_{ji}E}\right) \bmod p$$
$$= \alpha^{K_j + \sum_{i=1}^{m_j} k_{ji}} \; mod\; p = R$$

Vậy công thức (4.71) luôn tồn tại. Có nghĩa, tính đúng của công thức kiểm tra (4.71) được đảm bảo.

b) Chứng minh tính đúng của lược đồ

Dễ thấy, biểu thức kiểm tra chữ ký $E^* = E$ luôn tồn tại. Thật vậy:

Thay các giá trị S, U, Y_{col} sau đây:

$$S = (\sum_{j=1}^{g} {S_j}^2)^{1/2} \bmod n$$
$$U = \prod_{j=1}^{g} U_j \; mod\; p$$
$$Y_{col} = \prod_{j=1}^{g} Y_j \; mod\; p$$

vào vế phải của biểu thức tính R^* (4.74) ta được:

$$R^* = \alpha^{S^2}(UY_{col})^{-E} \; mod\; p$$
$$= \alpha^{\sum_{j=1}^{g} {S_j}^2}(\prod_{j=1}^{g} U_j\, Y_j)^{-E} \; mod\; p$$
$$= \prod_{j=1}^{g} \alpha^{S_j^2}(U_j Y_j)^{-E} \; mod\; p$$
$$= \prod_{j=1}^{g} R_j \; mod\; p = R$$

Vì $R^* = R$ nên $E^* = E$ ($E^* = F_H(M\|R^*\|U) = F_H(M\|R\|U) = E$).

Vậy biểu thức $E^* = E$ luôn tồn tại: Chứng tỏ tính đúng của thủ tục kiểm tra chữ ký, hay tính đúng của lược đồ RCS.01-4.3, luôn được đảm bảo.

4.3.5. Lược đồ chữ ký số 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 ký, 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. $Y_j = \alpha^{X_j} \, mod \, p$; $(j = g+1, g+2, \dots, g+m)$.

Lược đồ chữ ký tập thể cho g nhóm ký và m người ký cá nhân bao gồm các thủ tục chính dưới đây.

- **Thủ tục sinh chữ ký tập thể cho g nhóm ký và m người ký cá nhân trên tài liệu M**

Gồm các bước sau:

1a. GM, của nhóm ký thứ j, thực hiện:

- Tạo ra các tham số mặt nạ λ_{ji} cho những signer của nhóm j theo công thức (4.49) trong thủ tục sinh chữ ký của lược đồ GDS-4.3.

- Tính U_j và R_j của nhóm ký thứ j theo công thức (4.97) và (4.98):

$$U_j = \prod_{i=1}^{m_j} y_{ji}^{\lambda_{ji}} \, mod \, p \tag{4.76}$$

U là giá trị chia sẻ thứ j trong thành phần đầu tiên của chữ ký tập thể.

$$R_j = R'_j \prod_{i=1}^{m_j} R_{ji} \, mod \, p \tag{4.77}$$

- Gửi giá trị U_j và R_j cho các GM khác và các cá nhân ký trong tập thể ký.

1b. Mỗi cá nhân ký thứ j thực hiện các công việc sau:

- Sinh một giá trị ngẫu nhiên K_j, $K_j < p$, và rồi tính:

$$R_j = \alpha^{K_j} \, mod \, p \tag{4.78}$$

- Gửi R_j đến tất cả signer (các quản lý nhóm và cá nhân tham gia ký).

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

$$U = \prod_{j=1}^{g} U_j \ mod\ p \tag{4.79}$$

$$R = \prod_{j=1}^{g+m} R_j \ mod\ p \tag{4.80}$$

và

$$E = F_H(M \| R \| U) \ mod\ \delta \tag{4.81}$$

Trong đó, δ là một số nguyên tố lớn: $|\delta| = 160$ bít. $U = 0$ for $j = g + 1, g + 2, \dots, g + m$.

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

3a. GM của nhóm thứ j tính toán giá trị chia sẻ của nhóm j:

$$S_j = (S_j'^2 + \sum_{i=1}^{m_j} S_{ji}{}^2)^{1/2} \bmod n \tag{4.82}$$

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

- Gửi nó cho những người quản lý khác.

3b. Mỗi signer cá nhân thứ j tính giá trị chia sẻ cá nhân:

$$S_j = (K_j + X_j E)^{1/2} \ mod\ n \tag{4.83}$$

- Gửi S_j cho những GM và cá nhân ký khác trong tập thể ký.

4. Một GM hoặc một cá nhân ký nào đó trong tập thể ký thực hiện:

- Kiểm tra tính hợp lệ của S_j bằng các kiểm tra theo các công thức:

$$R_j = \alpha^{S_j^2} (Y_j U_j)^{-E} \ mod\ p \tag{4.84}$$

$$R_j = \alpha^{S_j^2} Y_j^{-E} \bmod p \tag{4.85}$$

- Nếu tất cả S_j thoả mãn phương trình trên, phần tử thứ ba S của chữ ký tập thể được tính như sau:

$$S = (\sum_{j=1}^{g+m} S_j{}^2)^{1/2} \bmod n \tag{4.86}$$

Bộ ba (U, E, S) được sinh bởi thủ tục trên là chữ ký đại diện cho chữ ký tập thể gồm g nhóm ký và m người ký cá nhân trên tài liệu M.

- **Thủ tục kiểm tra chữ ký tập thể cho g nhóm ký và m người ký cá nhân trên tài liệu 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 được chia sẻ bởi tất cả các nhóm và cá nhân tham gia vào quá trình ký:

$$Y_{col} = \prod_{j=1}^{g+m} Y_j \ mod\ p \tag{4.87}$$

2. Tính lại giá trị R^*:

$$R^* = \alpha^{S^2}(UY_{col})^{-E}\ mod\ p \tag{4.88}$$

3. Tính E^*:

$$E^* = F_H(M\|R^*\|U) \tag{4.89}$$

4. So sánh E^* và 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.

- **Chứng minh tính đúng của lược đồ RCS.02-4.3:**

Tính đúng của lược đồ chữ ký tập thể đại diện này thể hiện qua: i) Sự tồn tại của công thức kiểm tra chữ ký chia sẻ S_j của mỗi nhóm ký R_j (4.84); ii) Sự tồn tại của công thức kiểm tra chữ ký chia sẻ S_j của mỗi cá nhân ký R_j (4.85) và iii) Sự tồn tại của biểu thức kiểm tra $E^* = E$. Cụ thể như sau:

a) Chứng minh tính đúng của công thức kiểm tra chữ ký nhóm

Dễ thấy công thức kiểm tra chữ ký nhóm luôn tồn tại. Thật vậy:

$$\begin{aligned} R_j^* &= \alpha^{S_j^2}\left(U_jY_j\right)^{-E}\ mod\ p \\ &= \alpha^{{S_j'}^2+\sum_{i=1}^{m_j}{s_{ji}}^2}\left(\alpha^{X_j}\prod_{i=1}^{m_j}{y_{ji}}^{\lambda_{ji}}\right)^{-E} \bmod p \\ &= \alpha^{(K_j+X_jE)+\sum_{i=1}^{m_j}(k_{ji}+x_{ji}\lambda_{ji}E)}\left(\alpha^{-X_jE_j}\prod_{i=1}^{m_j}\alpha^{-x_{ji}\lambda_{ji}E}\right) \bmod p \\ &= \alpha^{K_j+\sum_{i=1}^{m_j}k_{ji}}\ mod\ p = R \end{aligned}$$

b) Chứng minh tính đúng của công thức kiểm tra chữ ký của cá nhân

Dễ thấy công thức kiểm tra chữ ký cá nhân luôn tồn tại. Thật vậy:

$$\begin{aligned} R_j^* &= \alpha^{S_j^2}Y_j^{-E} \bmod p \\ &= \alpha^{(K_j+X_jE)}\alpha^{-\mathrm{x_j}E} \bmod p \end{aligned}$$

$$= \alpha^{K_j} \, mod \, p = R_j$$

c) Chứng minh tính đúng của lược đồ

Dễ thấy, biểu thức kiểm tra chữ ký $E^* = E$ luôn tồn tại. Thật vậy:

Thay các giá trị S, U, Y_{col}:

$$S = (\sum_{j=1}^{g+m} {S_j}^2)^{1/2} \bmod n$$

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

$$Y_{col} = \prod_{j=1}^{g+m} Y_j \; mod \, p$$

Vào vế phải của phương trình xác minh ta được:

$$\begin{aligned} R^* &= \alpha^{S^2}(UY_{col})^{-E} \, mod \, p \\ &= \alpha^{\Sigma_{j=1}^{g+m} {S_j}^2}(\prod_{j=1}^{g} U_j \prod_{j=1}^{g+m} Y_j)^{-E} \, mod \, p \\ &= \alpha^{\Sigma_{j=1}^{g} {S_j}^2 + \Sigma_{j=g+1}^{g+m} {S_j}^2}(\prod_{j=1}^{g} U_j \prod_{j=1}^{g} Y_j \prod_{j=g+1}^{g+m} Y_j)^{-E} \, mod \, p \\ &= \prod_{j=1}^{g} \alpha^{{S_j}^2}\left(U_j Y_j\right)^{-E} \prod_{j=g+1}^{g+m} \alpha^{{S_j}^2} {Y_j}^{-E} \; mod \, p \\ &= \prod_{j=1}^{g} R_j \prod_{j=g+1}^{g+m} R_j \, mod \, p = R \end{aligned}$$

Vì $R^* = R$ nên $E^* = E$ ($E^* = F_H(M \| R^* \| U) = F_H(M \| R \| U) = E$).

Vậy biểu thức $E^* = E$ luôn tồn tại: Điều này chứng tỏ tính đúng của thủ tục kiểm tra chữ ký, hay tính đúng của lược đồ RCS.02-4.3, luôn được đảm bảo.

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

4.4.1. Độ bảo mật của lược đồ chữ ký số 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 4.1.2).

4.4.2. Độ bảo mật của lược đồ chữ ký số 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.

- **Tấn công vào private key của thành viên nhóm ký:**

Xét trường hợp nhóm ký gồm m thành viên và người quản lý nhóm (GM) muốn tấn công vào private key của người thứ m trong nhóm ký.

Vì GM biết được các giá trị (S_m, R_m, y_m) của thành viên thứ m nên GM có thể tính được private key x_m theo một trong hai phương trình sau:

$$x_m = \log_\alpha y_m \ mod\ p \tag{4.90}$$

Hoặc tính:

$$z_m = \log_\alpha R_m \ mod\ p \tag{4.91}$$

Rồi sau đó tính:

$$x_m = \frac{S_m^2 - z_m}{E} \ mod\ n \tag{4.92}$$

Đây lại là những bài toán khó logarit rời rạc, nên việc giải nó để tìm nghiệm x_m là không thể (tính đến hiện tại).

Như vậy, dù biết được nhiều thông tin của thành viên mình đang quản lý, nhưng GM vẫn khó có thể biết được private key những thành viên này.

- **Tấn công giả mạo chữ ký của thành viên nhóm ký:**

Xét trường hợp nhóm ký gồm m thành viên và người quản lý nhóm (GM) muốn giả mạo chữ ký của thành viên thứ m trong nhóm ký.

Vì biết được giá trị các (S_m, R_m, y_m) nên anh ta thực hiện các bước sau:

1. Chọn $X \in [1, n-1]$ và tính public key của mình:

$$Y = y_m^{\lambda_m} \alpha^X \ mod\ p \tag{4.93}$$

2. Và tính giá trị công khai chung cho cả nhóm.

$$U = \prod_{i=1}^{m} y_i^{\lambda_i} \ mod\ p \tag{4.94}$$

3. Chọn $K \in [1, q-1]$ và tính:

$$R' = R_m \alpha^K \ mod\ p \tag{4.95}$$

4. Tính R và E, gửi E cho các thành viên khác trong nhóm.

$$R = R' \sum_{i=1}^{m} R_i \ mod\ p \tag{4.96}$$

$$E = F_H(M \| R \| U) mod\ \delta \tag{4.97}$$

Tính:

$$S' = (S_m^2 + K + XE)^{1/2} \ mod\ n \tag{4.98}$$

5. Rồi tính:

$$S = \left(S'^2 + \sum_{i=1}^{m} S_i^2 \right)^{1/2} \ mod\ n \tag{4.99}$$

Dễ thấy bộ ba (U, E, S) vẫn thỏa biểu thức kiểm tra:

$$R = \alpha^{S^2} (UY)^E \ mod\ p$$

Chứng minh như sau.

$$\begin{aligned}
R^* &= \alpha^{S^2} (UY)^E \ mod\ p \\
&= \alpha^{S'^2 + \sum_{i=1}^{m} S_i^2} \left(y_m^{\lambda_m} \alpha^X \prod_{i=1}^{m} y_i^{\lambda_i} \right)^{-E} \ mod\ p \\
&= \alpha^{S_m^2 + (K+XE) + \sum_{i=1}^{m} S_i^2} y_m^{-E\lambda_m} \alpha^{-EX} \prod_{i=1}^{m} y_i^{-E\lambda_i} \ mod\ p \\
&= \alpha^{(k_m + x_m \lambda_m E) + (K+XE) + \sum_{i=1}^{m} (k_i + x_i \lambda_i E)} \alpha^{-x_m \lambda_m E} \alpha^{-XE} \alpha^{\sum_{i=1}^{m} -x_i \lambda_i E} \ mod\ p \\
&= \alpha^{k_m + K + \sum_{i=1}^{m} k_i} \\
&= R' \sum_{i=1}^{m} R_i \ mod\ p \\
&= R \text{ (đpcm)}
\end{aligned}$$

Như vậy GM đã thành công trong việc giả mạo chữ ký của thành viên thứ

m trong nhóm ký do người này quản lý.

Do đó, khi triển khai lược đồ chữ ký nhóm trên thực tế, để chống lại kiểu tấn công giả mạo này cần phải có một bộ phận, một cá nhân, đủ tin cậy đóng vai trò quản lý nhóm (thường gọi là bên thứ ba).

Theo đó, khi xây dựng một nhóm ký, bên thứ ba có trách nhiệm tiếp nhận public key của từng thành viên tham gia ký rồi tính và công bố public key chung của nhóm ký. Public key của các thành viên cũng phải được công bố công khai trong nhóm ký cho mọi thành viên của nhóm được biết. Các public key riêng của các thành viên và public key chung của cả nhóm là cố định, kẻ giả mạo sẽ không thể tính toán lại như trong biểu thức (*), (mục 3.3.1.a). Vì vậy lược đồ sẽ an toàn nếu được triển khai đúng đắn.

4.4.3. Độ bảo mật của lược đồ chữ ký số 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 số 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 dựa 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	$U = \sum_{j=1}^{g}(243m_j + 1)\,T_m$ $e = [\sum_{j=1}^{g}(241m_j + 240) + 241m + 1]T_m$ $S = [\sum_{j=1}^{g}(1254m_j + 1781) + 1250m + 290]T_m$ $Sum = [\sum_{j=1}^{g}(1738m_j + 2022) + 1491m + 292]T_m$	$(723 + g + m)T_m$

** Các ký hiệu sử dụng trong bảng này đã được quy ước ở mục 2.3.4 - 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 3 thành phần. Bảng này cũng cho thấy, với lược đồ chữ ký tập thể đại diện trên 2 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. Lược đồ chữ ký mới hai thành phần cho thấy nó kế thừa đầy đủ ưu điểm và yêu cầu của chữ ký cùng loại ba thành phần. 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. Khả năng chống tấn công của lược đồ dựa trên đồng thời hai bài toán khó cũng được chỉ ra ở chương này.

Những công bố của NCS được sử dụng trong chương này: [CT1], [CT4], [CT6], [CT8], [CT10], [CT11].

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 hệ thống lại được các vấn đề liên quan đến chữ ký số và lược đồ chữ ký số. Và hệ thống lại được các loại chữ ký số được xây dựng dựa trên một bài toán khó và dựa trên đồng thời hai bài toán khó.
- 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: $p = Nt_0t_1t_2 + 1$ (2 lược đồ) và $p = Nk^2 + 1$ (hai lược đồ).
- Đề xuất được 4 lược đồ chữ ký số tập thể đại diện 2 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 số 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 chuẩn chữ ký Schnorr.
- Tất cả các lược đồ chữ ký số đề xuất và xây dựng đều được: i) Chứng minh được tính đúng đắn; ii) Phân tích bảo mật; và iii) Đánh giá hiệu năng.

2. Đóng góp khoa học của luận án

Những đóng góp khoa học của luận án bao gồm:

a. Phát hiện và lược đồ hóa được hai yêu cầu chứng thực dựa vào chữ ký số 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 số tập thể mới - "**chữ ký số tập thể đại diện" -** có tính thực tế và cấp thiết cao. Có hai dạng lược đồ chữ ký số 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. Các lược đồ này được hình thành dựa trên sự kết hợp những ưu điểm của lược đồ chữ ký số nhóm và lược đồ chữ ký số tập thể nên ưu điểm và khả năng ứng dụng của nó là khá cao.

b. Kết quả nghiên cứu cho thấy, hoàn toàn có thể: i) Sử dụng một bài toán khó hoặc sử dụng đồng thời hai bài toán khó, như IFP, DLP, ECDLP, PFRM (Một vấn đề khó mới), v.v. và ii) Dựa vào các chuẩn chữ ký số và các lược đồ chữ ký số chuẩn phổ biến, như: Schnorr, DSA, ECDSA, GOST R34.10-2001, v.v. để xây dựng các lược đồ chữ số tập thể đại diện được đề xuất trong luận án này.

Điều này cũng chứng tỏ hiệu quả sử dụng, tính an toàn và tính khả thi của các lược đồ chữ ký số đề xuất ở đây là có thể ghi nhận và tin dùng.

c. Nguyên lý hoạt động của các lược đồ chữ ký số đề xuất chứng tỏ những lược đồ này hoàn toàn có thể triển khai trên các hạ tầng PKI hiện có. Người sử dụng vẫn sử dụng cặp khóa private key và public key để tham gia vào hệ thống xác thực dựa trên chữ ký số tập thể nhưng vẫn đảm bảo tính bí mật và tính riêng tư của cặp khóa bất đối xứng mà họ sở hữu.

Như vậy, kết quả nghiên cứu của luận án đã đóng góp cho cộng đồng hai dạng lược đồ chữ ký số tập thể mới có tính thực tế, cập thiết và ứng dụng cao. Luận án cũng đã công bố các lược đồ chữ ký số cụ thể của hai dạng lược đồ đề xuất. Cơ sở toán học, tính đúng đắn, tính an toàn và hiệu năng tính toán của các lược đồ này cũng đã được chỉ ra.

Nghiên cứu sinh tin rằng, những kết quả được công bố trong luận án này hoàn toàn có thể áp dụng vào thực tế, đáp ứng được các yêu cầu chứng thực cho cả một tập thể gồm nhiều cấp độ chức năng của nhiều ứng dụng trao đổi thông tin trên không gian mạng hiện nay.

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:

- Luận án mới chỉ dừng lại ở việc Phân tích bảo mật và Đánh giá hiệu năng của chính các lược đồ đề xuất. 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.

- Hầu hết các lược đồ chữ ký số trong luận án này đều xây dựng dựa trên các bài toán khó, các thuật toán chữ ký số, các giao thức chữ ký số có sẵn. 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.

- Xây dựng các ứng dụng xác thực dựa trên lược đồ chữ ký số tập thể đại diện, hỗ trợ cho các yêu cầu chứng thức, có tính tập thể, của nhiều bài toán khác nhau trong thực tế. Các ứng dụng này phải có tính an toàn và tốc độ thực thi cao khi hoạt động trên môi trường mạng Internet.

- 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, như: Xác thực dựa trên chữ ký số cá nhân; Xác thực dựa trên chữ ký số nhóm; Xác thực dựa trên chữ ký số tập thể; Xác thực dựa trên chữ ký số tập thể mù/tập thể đại diện v.v..

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 Signatures 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 Signatures 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, no.6, pp.478-485, 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).

XÁC NHẬN CỦA HƯỚNG DẪN ĐẠI DIỆN	**NGHIÊN CỨU SINH**
TS. Hồ Ngọc Duy	**Nguyễn Kim Tuấn**

TÀI LIỆU THAM KHẢO

Tiếng Việt:

[1] Lưu Hồng Dũng (2013), "Nghiên cứu, phát triển các lược đồ chữ ký số tập thể", *Luận án tiến sỹ kỹ thuật,* Học viện Kỹ thuật Quân sự.

[2] Lưu Hồng Dũng, Nguyễn Đức Thụy, Nguyễn Lương Bình và Tống Minh Đức (2016), "Phát *triển* thuật toán mã hóa khóa công khai dựa trên bài Toán logarit rời rạc", *Kỷ yếu Hội nghị Quốc gian lần thứ IX về "Nghiên cứu cơ bản về ứng dụng Công nghệ thông tin (FAIR'9)"*, Cần Thơ.

[3] Nguyễn Đức Thụy, Hồ Nhật Quang và Lưu Hồng Dũng (2015), "Phát triển lược đồ chữ ký số trên bài toán logarit rời rạc", *Tạp chí Nghiên cứu Khoa học và Công nghệ quân sự,* 37.

[4] Nguyễn Tấn Đức (2020), "Nghiên cứu phát triển một số lược đồ chữ ký số mù, chữ ký số tập thể mù dựa trên các chuẩn chữ ký số", *Luận án tiến sỹ kỹ thuật,* Học viện Công nghệ Bưu chính Viễn Thông.

Tiếng Anh:

[5] A. B. Nimbalkar (2018), "The Digital Signature Schemes Based on Two Hard Problems: Factorization and Discrete Logarithm", *Advances in Intelligent Systems and Computing*, *Cyber Security*, 729, pp. 493-498.

[6] A. Beresneva, A. Epishkina, O. Isupova, K. Kogos and M. Shimkiv (2016), "Special digital signature schemes based on GOST R 34.10-2012", *In 2016 IEEE NW Russia Young Researchers in Electrical and Electronic Engineering Conference (EIConRusNW)*, IEEE, pp. 135-140.

[7] A. C. Enache (2012), "About Group Digital Signatures". *Journal of Mobile, Embedded and Distributed Systems*, 4 (3), pp. 193-202.

[8] A. Corbellini (2015), "Elliptic Curve Cryptography: ECDH and ECDSA", *https://andrea.corbellini.name/2015/05/30/elliptic-curve-cryptography-ecdh-and-ecdsa/, (Accessed date: 01-04-2021).*

[9] A. Darwish and Maged M El-Gendy (2017), "A New Cryptographic Voting Verifiable Scheme for E-Voting System Based on Bit Commitment and Blind Signature*", Int J Swarm Intel Evol Computer 2017*, 6 (2), DOI: 10.4172/2090-4908.1000158.

[10] A. J. Menezes and S. A. Vanstone (1996), "Handbook of Applied Cryptography", *CRC Press.*

[11] A. Komarova, A. Menshchikov and T. Klyaus (2017), "Analysis and comparison of electronic digital signature state standards GOST R34.10-1994, GOST R34.10-2001 and GOST R34.10-2012", In *Proc. The 10th International Conference,* Jaipur, India.

[12] A. Kunal (2019), "Elliptic Curve Cryptography based Certification

Authority", *IEEE India Info*, 14 (1), pp. 87-95.

[13] A. N. Berezin, N. A. Moldovyan and V.A. Shcherbacov (2013), "Cryptoschemes based on difficulty of simultanous solving two different difficult problems", *Computer Science Journal of Moldova*, 21 (no.2(62)), pp. 280-290.

[14] B. Sushila Vishnoi and Vishal Shrivastava (2012), "A new digital signature algorithm based on factorization and discrete logarit problem", *International Journal of Computer Trends and Technology*, 3 (4), pp. 653-657.

[15] C. Popescu (1999), "Blind signature and BMS using elliptic curves. Studia Univ Babes-Bolyai", *Informatica*, pp. 43-49.

[16] C. C. Lee, M. S. Hwang and Y. C. Lai (2003), "An untraceable blind signature scheme", *IEICE Transaction on Fundamentals*, E86-A (7), pp. 1902-1906.

[17] C. I. Fan, W. Z. Sun and V. S. M. Huang (2010), "Provably secure randomized blind signature scheme based on bilinear pairing", *Journal Computers & Mathematics with Applications*, 60 (2), pp. 285-293.

[18] C. T. Wang, C. H. Lin and C. C. Chang (2003), "Signature Scheme Based on Two Hard Problems Simultaneously", *Proceedings of the 17th International Conference on Advanced Information Networking and Application*, pp. 557-560.

[19] Cheng-Chi Lee, Min-Shiang Hwang and WeiPang Yang (2005), "A New Blind Signature Based on the Discrete Logarithm Problem for Untraceability", *Applied Mathematics and Computation*, 164 (3), pp. 837-841.

[20] Chin-Ming Hsu (2003), "A group digital signature technique for authentication", *IEEE 37th Annual 2003 International Carnahan Conference on Security Technology*, Proceedings.

[21] D. Chaum and E. Heyst (1991), "Group signatures". In *Advances in Cryptology - EUROCRYPT' 91*, Springer-Verlag, pp. 257-265.

[22] D. Johnson and A. J. Menezes (1999), "*The elliptic curve digital signature algorithm (ECDSA)*"

[23] D. Poulakis (2009), "A variant of digital signature algorithm". *Designs, Codes and Cryptography*, 51 (1), pp. 99-104.

[24] D. W. Hopkins, T. W. Collins and S. W. Wierenga (2006), "Group signature generation system using multiple primes", *Hewlett Packard Development Company LP*, Houston, TX, US.

[25] Dang Minh Tuan (2012), "New elliptic curve digital multi-signature schemes for multi-section messages", *International Conference on Computing and Communications Technologies Research - Innovation and Vision for the*

future, Ho Chi Minh city - Viet Nam, pp. 25-28.

[26] Debasish Jena, Sanjay Kumar Jena and Banshidhar Majhi (2007), "A Novel Blind Signature Scheme Based on Nyberg-Rueppel Signature Scheme and Applying in Off-Line Digital Cash", *In Proceedings of the 10th International Conference on Information Technology (ICIT'07)*, pp. 19-22.

[27] Debasish Jena, Sanjay Kumar Jena and Banshidhar Majhi (2007), "A Novel Untraceable Blind Signature Based on Elliptic Curve Discrete Logarithm Problem", *IJCSNS International Journal of Computer Science and Network Security*, 7 (6), pp. 269-275.

[28] Debasish Jena, Sanjay Kumar Jena and Banshidhar Majhi, S. K. Panigrahy (2008), "A novel ECDLP-based blind signature scheme with an illustration", *Web engineering and applications*, pp. 59-68.

[29] Debiao, Chen and Zhang (2011), "An efficient identity-based blind signature scheme without bilinear pairings", *Computers & Electrical Engineering*, 37 (4), pp. 444-450.

[30] Dimitrios Poulakis and Robert Rolland (2015), "A digital signature scheme based on two hard problems", In *Computation, Cryptography, and Network Security*, Springer, pp. 441-450.

[31] Dolmatov V. and Degtyarev A. (2013), "GOST R 34.11-2012: Digital Signature Algorithm", *RFC 7091*, URL: https://datatracker.ietf.org/doc/html/rfc7091, Access on 01/04/2021.

[32] Dominique Schroder and Dominique Unruh (2012), "Security of Blind Signatures Revisited", *International Workshop on Public Key Cryptography*, Springer Link, pp. 662-679.

[33] D. Poulakis (2016), "New lattice attacks on DSA schemes", *Journal of Mathematical Cryptology*, 10(2), pp.135-144.

[34] E. Ismail, N. Tahat, and R. R. Ahmad (2008), "A new digital signature scheme based on factoring and discrete logarits", *Journal of Mathematics and Statistics*, 4 (4), pp. 222-225.

[35] E. S. Dernova (2009), "Information authentication protocols based on two hard problems", *Ph.D. Dissertation. St. Petersburg State Electrotechnical University*, St. Petersburg, Russia.

[36] F. G. Jeng, T. L. Chen and T. S. Chen (2010), "An ECC-Based Blind Signature Scheme", *Journal of networks*, 5 (8), pp. 921-928.

[37] F. Shah and H. Patel (2016), "A Survey of Digital and Group Signature", *International Journal of Computer Science and Mobile Computing*, 5 (6), pp. 274-278.

[38] Federal Office for Information Security (2018), "Technical Guideline - Elliptic Curve Cryptography", *Technical Guideline TR-03111*, pp. 24-25.

[39] G. K. Verma and B. B. Singh (2016), "New ID based fair blind signatures". *International Journal Of Current Engineering And Scientific Research (IJCESR)*, 3 (1), pp. 41-47.

[40] G. K. Verma and B. B. Singh (2018), "Efficient identity-based blind message recovery signature scheme from pairings". *The Institution of Engineering and Technology 2018*, 12 (2), pp. 150-156.

[41] G. Z. Qadah, R. Taha (2007), "Electronic voting systems - Requirements, design and implementation", *Computer Standards & Interfaces 2007*, 29, pp. 376-386.

[42] H. N. Duy, D. V. Binh, N. H. Minh and N. A. Moldovyan (2014), "240-bit collective signature protocol in a non-cyclic finite group", *International conference on Advanced Technologies for Communications (ATC) 2014*, Hanoi, pp. 467-470.

[43] H. Zhu, Y. Tan, L. Zhu, Q. Zhang and Y. Li (2018), "An efficient identity-based proxy blind signature for semioffline services", *Wireless Communications and Mobile Computing 2018*.

[44] Huian Li, A. R. Kankanala and X. Zou (2014), "A taxonomy and comparison of remote voting schemes", In *23rd International Conference on Computer Communication and Networks (ICCCN'14)*, pp. 666-673.

[45] Hung Min Sun (2002), "Cryptanalysis of a Digital Signature Scheme Based on Factoring and Discrete Logarithms", In *Proceedings of the National Computer Symposium*, pp. F043-F045.

[46] J. L. Zhang, J. Z. Zhang and S. C. Xie, (2018), "Improvement of a quantum proxy blind signature scheme". *Int. J. Theor. Phys*, 57 (6), pp. 1612-1621.

[47] J. Lee, H. Kim, Y. Lee, S. M. Hong and H. Yoon (2017), "Parallelized scalar multiplication on elliptic curves defined over optimal extension field", *International Journal of Network Security*, 4 (1), pp. 99-106.

[48] J. He and T. Kiesler (1994), "*Enhancing the security of El Gamal's signature scheme"*, In Computers and Digital Techniques, IEE Proceedings, vol.141, pp.249-252. IET.

[49] J. M. Pollard and C. P. Schnorr (1987), "An efficient solution of the congruence x2+ ky2 = m (mod n)", *IEEE Transactions on Information Theory*, 33 (5), pp. 702-709.

[50] J. Li and G. Xiao (1998), "Remarks on new signature scheme based on two hard problems", *Electronics Letters*, 34 (25), pp. 2401.

[51] J. Pieprzyk, T. Hardjono and J. Seberry (2003), "Fundamentals of computer security", *Springer-Verlag*, Berlin.

[52] Jun Zhang (2010), "Cryptographic analysis of the two structured multi-signature schemes", *Journal of Computational Information Systems*, 6 (9),

pp. 3127-3135.

[53] K. Ganaraj (2017), "Advanced E-Voting Application Using Android Platform", *International Journal of Computer- Aided Technologies (IJCAx)*, 4 (1/2).

[54] K. Ganeshkumar and D. Arivazhagan (2014) "Generating A Digital Signature Based On New Cryptographic Scheme For User Authentication And Security", *Indian Journal of Science and Technology*, 7 (S6).

[55] K. M. Rokibul Alam and S. Tamura (2012), "Electronic voting - Scopes and limitations", in *Proceedings of International Conference on Informatics*, Electronics & Vision (ICIEV12), pp. 525-529.

[56] K. M. Rokibul Alam, Adnan Maruf, Md. Rezaur Rahman Rakib, G. G. Md. Nawaz Ali, Peter Han Joo Chong and Yasuhiko Morimoto (2018), "An Untraceable Voting Scheme Based on Pairs of Signatures", *International Journal of Network Security*, 20 (4), pp. 774-787.

[57] L. C. Washington (2008), "Elliptic curves number theory and crytography", Second Edition, *CRC Press*, 2008.

[58] Laura Savu (2012), "Combining public key encryption with Schnorr digital signature", *Journal of Software Engineering and Applications*, 5 (2), pp. 102-108.

[59] Lee (1999), "Security of Shao's Signature Schemes Based on Factoring and Discrete Logarithms", *IEEE Proceeding*, 146 (2), pp. 119-121.

[60] Lin, C. Gun, and C. Chen (2009), "Comments on Wei's Digital Signature Scheme Based on Two Hard Problems", IJCSNS International Journal of *Computer Science and Network Security*, 9 (2), pp. 1-3.

[61] L. Harn (1995), "*Enhancing the security of El Gamal's signature scheme"*. IEE Proceedings-Computers and Digital Techniques, pp.142:156.

[62] M. Burmester, Y. Desmedt, H. Doi, M. Mambo, E. Okamoto, M. Tada and Y. Yoshifuji (2000), "A structured ELGamal-type multisignature scheme", *Proceedings of Third International Workshop on Practice and Theory in Public Key Cryptosystems (PKC 2000)*, Springer-Verlag, pp. 466-483.

[63] M. Kumar, C. P. Katti and P. C. Saxena (2017), "An Identity-based Blind Signature Approach for E-voting System". *Int. J. Modern Education and Computer Science*, 9 (10), pp. 47-54.

[64] Malik Sikandar Hayat Khiyal, Aihab Khan, Saba Bashir, Farhan Hassan Khan, and Shaista Aman (2011), "Dynamic blind group digital signature scheme in e-banking", *International Journal of Computer and Electrical Engineering*, 3 (4), pp. 514-519.

[65] Minh Hieu, Hai Nam, N. A. Moldovyan and Giang Tien (2017), "New blind signature protocols based on a new hard problem", *The International Arab*

Journal of Information Technology, 14 (3), pp. 307-313.

[66] Mustafa Al-Fayoumi, Sattar J Aboud and Mohammad Al-Fayoumi (2010), "A New Digital Signature Scheme Based on Interger Factoring and Discrete Logarit Problem", *IJCA*, 17 (2).

[67] Muthanna Abdulwahed Khudhair (2017), "A New Multiple Blind Signatures Using El-Gamal Scheme". *International Journal of Engineering and Information Systems (IJEAIS)*, ISSN: 2000-000X, 1 (7), pp. 149-154.

[68] Yu. Matiyasevich (2001), Hilbert's Tenth Problem: Diophantine Equations from Algorithmic Point of View, *Hilbert's Problems Today*, 5th–7th, Italy.

[69] N. Y. Lee and T. Hwang. Modi_ed Har (2002), "Signature scheme based on factorizing and discrete logarits", *In Computers and Digital Techniques, IEE Proceedings*, vol.143, pp.196-198.

[70] N. A. Moldovyan (2008), "Digital Signature Scheme Based on a New Hard Problem", *Computer Science Journal of Moldova*, 16 (2), pp.163-182.

[71] N. A. Moldovyan (2010), "Blind Collective Signature Protocol Based on Discrete Logarithm Problem", *International Journal of Network Security*, 11(2), pp.56-73.

[72] N. A. Moldovyan (2011), "Blind Collective Signature Protocol", *Computer Science Journal of Moldova*, 19 (1), pp. 80-91.

[73] Nikolai A. Moldovyan and Victor A. Shcherbacov (2012), "New signature scheme based on difficulty of finding roots", *Quasigroups and Related Systems*, 20, pp. 261-266.

[74] N. A. Moldovyan and A. A. Moldovyan (2014), "Group signature protocol based on masking public keys", *Quasigroups and Related Systems*, 22, pp. 133-140.

[75] N. A. Moldovyan, N. H. Minh, D. T. Hung and T. X. Kien (2016), "Group Signature Protocol Based on Collective Signature Protocol and Masking Public Keys Mechanism", *International Journal of Emerging Technology and Advanced Engineering*, 6 (6), pp. 1-5.

[76] N. H. Minh, D. V. Binh, N. T. Giang and N. A. Moldovyan (2012), "Blind signature protocol based on difficulty of simultaneous solving two difficult problems", *Journal of Applied Mathematical Sciences*, 6 (139), pp. 6903-6910.

[77] N. Q. Phong, Jiang Zhang and Zhenfeng Zhang (2015), "Simpler efficient group signature from lattices", *Proc. of 18th IACR International Conference on Practice and Theory in Public-Key Cryptography*, pp. 401-426.

[78] N. Tahat, E. Ismail and A. K. Alomari (2018), "Partially blind signature scheme based on chaotic maps and factoring problems". *Italian Journal ofPure and Applied Mathematics*, 39, pp. 165-177.

[79] N. Tahat, E. Ismail and R. Ahmad (2009), "A New Blind Signature Scheme Based on Factoring and Discrete Logarithms", *International Journal of Cryptology Research*, 1 (1), pp. 1-9.

[80] P. Sarde and A. Banerjee (2017), "A Secure ID-Based Blind and Proxy Blind Signature Scheme from Bilinear Pairings". *Journal of Applied Security Research*, 12 (2), pp. 276-286.

[81] Punita Meelu and Sitender Malik (2010), "RSA and its correctness through modular arithmetic", *International Conference On Methods And Models In Science And Technology*, ICM 2st-10, AIP Conference Proceedings 1324, pp. 463-466.

[82] Q. Alamélou, O. Blazy, S. Cauchie and Ph. Gaborit (2017), "A code-based group signature scheme", *Designs, Codes and Cryptography*, 82, pp. 469-493.

[83] Qi Su and Wen-Min Li (2016), "Improved Group Signature Scheme Based on Quantum Teleportation", *International Journal of Theoretical Physics*, 53 (4), pp. 1208-1216.

[84] R. S. Rajasree (2014), "Generation of dynamic group digital signature", *International Journal of Computer Applications*, 98 (9), pp. 3-5.

[85] R. Seetha and R. Saravanan (2016), "Digital Signature Schemes for group communication: A Survey", *International Journal of Applied Engineering Reseach*, 11, pp. 4416-4422.

[86] Run Xie, Chunxiang Xu, Chanlian He and Xiaojun Zhang (2016), "A new group signature scheme for dynamic membership", *International Journal of Electronic Security and Digital Forensics*, 8 (4), pp. 332-351.

[87] R. Ghasemi, A. Safi, M. H. Dehkordi (2017), "Efficient multisecret sharing scheme using new proposed computational security model". *International Journal of Communication Systems*, 13(1), pp. e999.

[88] S. F. Tzeng, C. Y. Yang, and M. S. Hwang (2004), "A new digital signature scheme based on factoring and discrete logarits". *International Journal of Computer Mathematics*, 81 (1), pp. 9-14.

[89] S. James, T. Gowri, G. V. R. Babu and P. V. Reddy (2017), "Identity-Based Blind Signature Scheme with Message Recovery", *International Journal of Electrical and Computer Engineering (IJECE)*, 7 (5), pp. 2674-2682.

[90] S. Selvakumaraswamy and U. Govindaswamy (2016), "Efficient Transmission of PKI Certificates using ECC and its Variants", *The International Arab Journal of Information Technology*, 13 (1), pp. 38-43.

[91] S. Wei (2004), "A New Digital Signature Scheme Based on Factoring and Discrete Logarits", *Progress on Cryptography*, pp. 107-111.

[92] Sharon Levy (2015), "Performance and Security of ECDSA",

http://www.semanticscholar.org.

[93] Shimin Wei (2007), “Digital signature scheme based on two hard problems”, *International Journal of Computer Science and Network Security*, 7 (12), pp. 207-209.

[94] Shin-Yan Chiou and Yi-Xuan He (2013), "Remarks on new Digital Signature Algorithm based on Factorization and Discrete Logarithm problem", *International Journal of Computer Trends and Technology (IJCTT)*, 4 (9), pp. 3322-3324.

[95] S.F. Tzeng, C.Y. Yang, and M.S. Hwang (2004), “A new digital signature scheme based on factoring and discrete logarit*s”. International Journal of Computer Mathematics*, 81(1), pp.9-14.

[96] V. Dolmatov (2010), "GOST R 34.10-2001: Digital Signature Algorithm", *RFC 5832*.

[97] H. He (2001), “Digital signature scheme based on factoring and discrete logarits”, *Electronics Letters*, 37 (4), pp. 220-222.

[98] Z. Shao (2005), “Security of a new digital signature scheme based on factoring and discrete logarithms”. *International Journal of Computer Mathematics*, 82 (10), pp. 1215-1219.

[99] Z. Y. Shen and X. Y. Yu (2004), “Digital signature schemes based on discrete logarits and factoring”, *Information Technology*, 28, pp. 21-22.

[100] Zheng, Z. Shao, S. Huang and T. Yu (2008), “Security of two signature schemes based on two hard problems”, *Proc. of the 11th IEEE International Conference on Communication Technology*, pp. 745-748.