BỘ GIÁO DỤC VÀ ĐÀO TẠO BỘ QUỐC PHÒNG
VIỆN KHOA HỌC VÀ CÔNG NGHỆ QUÂN SỰ

Đặng Minh Thảo

NGHIÊN CỨU XÂY DỰNG MỘT SỐ DẠNG LƯỢC ĐỒ MỚI CHO CHỮ KÝ SỐ TẬP THỂ

LUẬN ÁN TIẾN SĨ TOÁN HỌC

Hà Nội – 2027

BỘ GIÁO DỤC VÀ ĐÀO TẠO BỘ QUỐC PHÒNG
VIỆN KHOA HỌC VÀ CÔNG NGHỆ QUÂN SỰ

Đặng Minh Thảo

NGHIÊN CỨU XÂY DỰNG MỘT SỐ DẠNG LƯỢC ĐỒ MỚI CHO CHỮ KÝ SỐ TẬP THỂ

Chuyên ngành: Cơ sở toán học cho tin học
Mã số: 62 46 01 10

LUẬN ÁN TIẾN SĨ TOÁN HỌC

NGƯỜI HƯỚNG DẪN KHOA HỌC:

1. PGS. TS Nguyễn Văn A
2. PGS. TS Đặng Đình B

Hà Nội – 2027

LỜI CAM ĐOAN

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

Hà Nội, ngày 10 tháng 06 năm 2027

Đặng Minh Thảo

(Xem hướng dẫn sử dụng LaTeX tại Chương 2 trang 12).

LỜI CẢM ƠN

Trong quá trình nghiên cứu và hoàn thành Luận án, Nghiên cứu sinh đã nhận được sự định hướng, giúp đỡ, các ý kiến đóng góp quý báu và những lời động viên của các nhà khoa học, các thầy cô giáo, đồng nghiệp và gia đình.

Trước hết, Nghiên cứu sinh xin bày tỏ lời cảm ơn tới các thày PGS.TS Nguyễn Văn A, PGS.TS Đặng Đình B đã tận tình hướng dẫn và giúp đỡ trong quá trình nghiên cứu.

Cho phép Nghiên cứu sinh chân thành cảm ơn các thày cô giáo, các nhà khoa học của Viện Khoa học và Công nghệ quân sự, Viện Công nghệ thông tin, Viện Toán học,... đã có các góp ý quý báu cho Nghiên cứu sinh trong quá trình thực hiện Luận án này.

Nghiên cứu sinh chân thành cảm ơn Ban Giám đốc, Phòng Đào tạo, Viện Khoa học và Công nghệ quân sự đã tạo điều kiện thuận lợi để Nghiên cứu sinh hoàn thành nhiệm vụ nghiên cứu.

Cuối cùng Nghiên cứu sinh bày tỏ lời cảm ơn tới các đồng nghiệp, gia đình, bạn bè đã luôn động viên, chia sẻ, ủng hộ và giúp đỡ Nghiên cứu sinh vượt qua khó khăn để đạt được những kết quả nghiên cứu trong Luận án này.

NCS Đặng Minh Thảo

MỤC LỤC

DANH MỤC CÁC KÝ HIỆU, CÁC CHỮ VIẾT TẮT

$\{0,1\}^*$	Ký hiệu chuỗi bit có độ dài bất kỳ
$\{0,1\}^\infty$	Ký hiệu chuỗi bit có độ dài vô tận
ϵ	Hàm nhỏ không đáng kể
σ	Chữ ký số
$\perp$	Thuật toán không cho ra kết quả
$\mathfrak{V}$	Vector phân công ký tập thể
ACMA	Tấn công văn bản được lựa chọn thích ứng (Adaptive Chosen Message Attacks)
CDH	Bài toán Deffie-Hellman (Computational Diffie-Hellman)
det	Định thức
d	Khóa bí mật trong hệ mật ECC
DSA	Thuật toán chữ ký số (Digital Signature Algorithm)
e	Giá trị băm của hàm băm $e = H(m)$
EC	Đường cong Elliptic (Elliptic Curve)
ECC	Hệ mật dựa trên đường cong Elliptic (Elliptic Curve Cryptography)
ECDH	Thuật toán Elliptic Curve Diffie–Hellman
ECDLP	Bài toán logarithm rời rạc (Elliptic Curve Logarithm Problem)
ECDSA	Thuật toán chữ ký số dựa trên đường cong elliptic (Elliptic Curve Digital Signature Algorithm)
FPGA	Mạch tích hợp cỡ lớn có khả năng lập trình (Field-Programmable Gate Array)
$\mathbb{F}$	Trường hữu hạn
gcd	Ước số chung lớn nhất (Greatest Common Divisor)
H	Hàm băm (Hash fuction)

DANH MỤC CÁC HÌNH VẼ

DANH MỤC CÁC BẢNG BIỂU

MỞ ĐẦU

Tính cấp thiết của đề tài nghiên cứu:

Trong những năm gần đây, các điều kiện về cơ sở hạ tầng và cơ sở pháp lý cho chính phủ điện tử và thương mại điện tử ở Việt Nam đã chín muồi. Cụ thể là theo sách trắng Công nghệ thông tin năm 2014, đến nay Việt Nam đã có gần 33.2 triệu người sử dụng Internet, băng thông Internet quốc tế đã đạt 640 Gbps. Luật giao dịch điện tử đã có hiệu lực từ năm 2005, theo đó, các giao dịch điện tử hoàn toàn có tính pháp lý như những giao dịch thực hiện bằng các văn bản giấy cùng với chữ ký và con dấu truyền thống. Có thể nói, chính phủ điện tử và thương mại điện tử chỉ có thể phát triển được khi và chỉ khi hệ thống chữ ký số, chứng thư số được áp dụng đồng bộ. Bởi vì chính chữ ký số mới có thể bảo đảm tính pháp lý của các giao dịch điện tử.

Về hành lang pháp lý, liên quan đến chữ ký số, chứng thư số, Việt Nam đã có 04 văn bản luật, 10 nghị định, 12 thông tư và 7 quyết định. Sau khi Trung tâm Chứng thực chữ ký số Quốc gia (Root CA) được thành lập vào năm 2008, đến năm 2016 đã có 09 công ty (VDC, Viettel, FPT, Nacencomm, BKAV...) cung cấp chứng thực chữ ký số cho các tổ chức và cá nhân, và có thể cung cấp một số dịch vụ chữ ký số như kê khai thuế qua mạng, hải quan điện tử, ký email, hóa đơn, hợp đồng, đấu thầu điện tử. Tuy nhiên, hiện nay các doanh nghiệp mới chỉ cung cấp các dịch vụ cho chữ ký đơn, khi mỗi người ký số chỉ ký vào một văn bản duy nhất. Mặc dù các điều kiện cơ bản về hạ tầng kỹ thuật và hạ tầng pháp lý đã hội tụ, song chính phủ điện tử và thương mại điện tử ở Việt Nam vẫn chưa phát triển được như mong đợi, một phần là bởi vì các ứng dụng về chứng thư số và chữ ký số vẫn còn chưa được triển khai rộng rãi, các nghiên cứu lý thuyết và thực tiễn áp dụng chữ ký số vẫn còn ở mức rất khiêm tốn.

Chữ ký số tập thể có nhiều ứng dụng trong thực tiễn, ví dụ dùng để kiểm

tra đồng loạt nhóm chữ ký số theo lô, xác thực đa yếu tố, hoặc dùng cho các kênh quảng bá: IP Multi-cast, Peer-to-Peer file sharing, grid computing, mobile adhoc networks...

Từ cơ sở trên chúng ta thấy nghiên cứu chữ ký số nói chung và chữ ký số tập thể nói riêng là rất cần thiết, có ý nghĩa to lớn về mặt học thuật cũng như thực tiễn.

Mục tiêu nghiên cứu:

Mục tiêu của Luận án là nghiên cứu tổng quan về chữ ký số, chữ ký số tập thể; từ đó phát triển mới một số dạng lược đồ cho chữ ký số tập thể, có thể ứng dụng triển khai trong thực tiễn (chữ ký số tập thể đa thành phần, kết hợp giữa chữ ký số tập thể đa thành phần với chữ ký số mù và với chữ ký số ủy nhiệm...). Chứng minh bằng toán học các lược đồ chữ ký số sẽ xây dựng có tính đúng đắn và độ an toàn đáp ứng được các yêu cầu triển khai thực tiễn.

Nội dung nghiên cứu:

- Nghiên cứu đề xuất mô hình chữ ký số tập thể đa thành phần.
- Đề xuất lược đồ ký tập thể dựa trên hệ mật đường cong elliptic, cặp song tuyến tính, hệ mật dựa trên bài toán logarithm rời rạc.
- Nghiên cứu, đề xuất mô hình kết hợp giữa chữ ký số tập thể đa thành phần với chữ ký số ủy nhiệm.
- Nghiên cứu, đề xuất mô hình kết hợp giữa chữ ký số tập thể đa thành phần với chữ ký số mù.

Đối tượng và phạm vi nghiên cứu:

Đối tượng nghiên cứu là lược đồ chữ ký số tập thể, kết hợp với chữ ký số ủy nhiệm, chữ ký số mù trong một số hệ mật mã thông dụng: ElGamal (logarithm rời rạc), elliptic, hệ mật định danh (ID-Based), song tuyến tính.

Phương pháp nghiên cứu:

Tham khảo các công trình, bài báo và sách, tài liệu chuyên ngành về lĩnh vực chữ ký số tập thể từ đó đề xuất mô hình mới giải quyết vấn đề còn tồn tại. Sử dụng các lý thuyết về các hệ mật phổ biến để xây dựng các giao thức và lược đồ chữ ký số cho các hệ mật này chứng minh cho mô hình mới phát triển. Sử dụng lý thuyết về độ phức tạp thuật toán để đánh giá độ an toàn và hiệu năng của lược đồ chữ ký số tập thể. Cài đặt thử nghiệm bằng phần mềm và triển khai trên Chip FPGA (Field-Programmable Gate Array), áp dụng vào thực tiễn triển khai đề tài cấp Nhà nước.

Ý nghĩa khoa học và thực tiễn của luận án:

Về mặt lý thuyết, Luận án đã đưa mô hình chữ ký tập thể mới là mô hình tổng quát của nhiều lớp chữ ký số tồn tại trước đây, trên cơ sở mô hình mới này sẽ mở ra hàng loạt hướng nghiên cứu mới kết hợp giữa chữ ký số tập thể đa thành phần với các mô hình chữ ký số khác như chữ ký số mù, chữ ký số ủy nhiệm, chữ ký số ngưỡng, chữ ký số vòng, chữ ký số cấu trúc, đồng thời cũng mở ra nghiên cứu triển khai mô hình này cho các hệ mật khác nhau như hệ mật đường cong elliptic, hệ mật định danh, hệ mật dựa trên nhóm Braid, hệ mật dựa trên nhóm dàn (lattice).

Về mặt thực tiễn, mô hình chữ ký số tập thể đa thành phần do có độ dài chữ ký số không phụ thuộc vào số người ký và số văn bản được phân tách thành các thành phần, vì thế khi số lượng người ký tăng lên thì không gian lưu trữ chữ ký số không bị tăng tuyến tính với số lượng người ký và như vậy sẽ tiết kiệm được rất nhiều không gian lưu trữ và băng thông chuyển tải chữ ký số trên đường truyền. Bên cạnh đó do mô hình chữ ký số tập thể đa thành phần cho phép ký một lần cho tất cả các thành viên và với tất cả các thành phần của văn bản trong một lần nên sẽ tiết kiệm được thời gian tính toán và tài nguyên tính toán để hình thành chữ ký số và xác thực chữ ký số do thời gian và tài nguyên tính toán không bị tăng tuyến tính theo số lượng người ký và số thành phần của văn bản. Chữ ký số tập thể đa thành phần cũng đáp ứng tốt thực tiễn hơn các lược đồ tộn tại, do cho phép số người ký và số phần của văn bản khác nhau.

Bố cục của luận án:

Ngoài phần mở đầu và phần kết luận, kiến nghị, Luận án được chia thành 3 chương với bố cục như sau:

Chương 1: Tổng quan về chữ ký số và chữ ký tập thể.

Chương 1 trình bày tình hình nghiên cứu tổng quan về chữ ký số, chữ ký số tập thể, chữ ký số tập thể ủy nhiệm, chữ ký số tập thể mù. Chương này cũng trình bày một số khái niệm và định nghĩa cơ bản về chữ ký số, các loại hình tấn công và phá vỡ lược đồ chữ ký số. Tiếp theo, chương 1 đưa ra định nghĩa chữ ký số tập thể và phân loại chữ ký số tập thể.

Chương 2: Chữ ký số tập thể đa thành phần.

Chương này trình bày về kết quả nghiên cứu mới của Luận án đó là mô hình ký số tập thể mới: chữ ký số tập thể đa thành phần. Mô hình mới này cho phép đáp ứng tốt hơn, linh hoạt hơn so với các mô hình ký tập thể hiện có. Mô hình này cũng là mô hình khái quát hóa một số các mô hình trước đây.

Trong chương 2, Luận án cũng định nghĩa chặt chẽ (formal) chữ ký số tập thể đa thành phần, các khả năng tấn công vào mô hình mới.

Sau khi đề xuất định nghĩa tổng quát về chữ ký số tập thể đa thành phần, chương 2 trình bày đề xuất cụ thể 03 lược đồ theo mô hình chữ ký tập thể mới đó là:

- Đề xuất chữ ký số tập thể đa thành phần dựa trên đường cong elliptic.
- Đề xuất chữ ký số tập thể đa thành phần dựa trên bài toán logarithm rời rạc.
- Đề xuất chữ ký số tập thể đa thành phần dựa trên cặp song tuyến tính.

Chương 3: Kết hợp chữ ký số tập thể đa thành phần với các mô hình ký khác.

Chương 3 trình bày kết quả nghiên cứu mới về việc kết hợp chữ ký số tập thể đa thành phần với chữ ký số ủy nhiệm, bao gồm định nghĩa chặt chẽ về mô hình

chữ ký số mới này và đề xuất một lược đồ cụ thể chữ ký số tập thể ủy nhiệm dựa trên hệ mật định danh.

Tiếp theo, chương này trình bày kết quả nghiên cứu mới về việc kết hợp chữ ký số tập thể đa thành phần với chữ ký số mù (có nhiều ứng dụng trong tiền ảo và bầu cử điện tử), bao gồm định nghĩa chặt chẽ về mô hình chữ ký số mới này đồng thời đề xuất một lược đồ cụ thể chữ ký mù dựa trên đường cong elliptic.

CHƯƠNG 1. HIỆN TRẠNG VỀ VIẾT LUẬN ÁN TIẾN SĨ

Chương này trình bày tổng quan về vấn đề một số quy định hiện hành về soạn thảo luận án tiến sĩ đồng thời cũng chỉ ra một số hạn chế của việc soạn thảo hiện hành.

1.1. Quy định về soạn thảo luận án

- Luận án sử dụng chữ VnTime (Roman) cỡ 13 hoặc 14 của hệ soạn thảo Winword hoặc tương đương;
- Mật độ chữ bình thường, không được nén hoặc kéo giãn khoảng cách giữa các chữ, giãn dòng đặt ở chế độ 1,5 lines;
- Lề trên 3,5cm; lề dưới 3cm; lề trái 3,5cm; lề phải 2cm.
- Số trang được đánh ở giữa, phía trên đầu mỗi trang giấy;
- Nếu có bảng biểu, hình vẽ trình bày theo chiều ngang khổ giấy thì đầu bảng là lề trái của trang, nhưng nên hạn chế trình bày theo cách này;
- Luận án được in trên một mặt giấy trắng khổ A4 (210 x 297), dày không quá 150 trang.

1.2. Quy định về trình bày tài liệu tham khảo

Một trong những công việc khá mất nhiều thời gian công sức của người viết luận án tiến sĩ, luận văn thạc sĩ là sắp xếp và trích dẫn tài liệu tham khảo, đặc biệt khi số lượng tài liệu tham khảo lên đến hàng chục hàng trăm. Nếu tiến

hành công việc này bằng phương pháp thủ công sẽ rất dễ gây nhầm lẫn và tốn nhiều thời gian.

Dưới đây là quy định về cách sắp xếp và trích dẫn tài liệu tham khảo trong luận án, luận văn của rất nhiều trường đại học ở Việt Nam:

1. Tài liệu tham khảo được xếp riêng theo từng ngôn ngữ (Việt, Anh, Đức, Nga, Trung, Nhật...). Các tài liệu bằng tiếng nước ngoài phải giữ nguyên văn, không phiên âm, không dịch, kể cả tài liệu bằng tiếng Trung Quốc, Nhật... (đối với những tài liệu bằng ngôn ngữ còn ít người biết có thể thêm phần dịch tiếng Việt đi kèm theo mỗi tài liệu).

2. Tên tài liệu tham khảo xếp theo thứ tự ABC họ tên tác giả luận án theo thông lệ của từng nước:

   - Tác giả là người nước ngoài: xếp theo thứ tự ABC theo họ.
   - Tác giả là người Việt Nam: xếp theo thứ tự ABC theo tên nhưng vẫn giữ nguyên thứ tự thông thường của tên người Việt Nam, không đảo tên lên trước họ.
   - Tài liệu không có tên tác giả thì xếp theo thứ tự ABC từ đầu của tên cơ quan ban hành báo cáo hay ấn phẩm.

3. Tài liệu tham khảo là sách, luận án, báo cáo phải ghi đầy đủ các thông tin sau:

   - Tên tác giả hoặc cơ quan ban hành (không có dấu ngăn cách).
   - (Năm xuất bản), (đặt trong ngoặc đơn, dấu phẩy sau ngoặc đơn).
   - *Tên sách, luận án hoặc báo cáo, (in nghiêng, dấu phẩy cuối tên).*
   - Nhà xuất bản, (dấu chấm kết thúc tài liệu tham khảo).
   - Nơi xuất bản (dấu chấm kết thúc tài liệu tham khảo).

4. Tài liệu tham khảo là bài báo trong tạp chí, bài trong một cuốn sách... ghi đầy đủ các thông tin sau:

- Tên tác giả (không có dấu ngoặc kép).
- (Năm công bố), (đặt trong ngoặc đơn, dấu phẩy sau ngoặc đơn).
- "Tên bài báo", (đặt trong ngoặc kép, không in nghiêng, dấu phẩy cuối tên).
- *Tên tạp chí hoặc tên sách, (in nghiêng, dấu phẩy cuối tên).*
- Tập (không có dấu ngăn cách).
- (Số) đặt trong ngoặc đơn, dấu phẩy sau ngoặc đơn).
- Các số trang, (gạch ngang giữa hai chữ số, dấu chấm kết thúc).

Có thể thấy các quy định này không tương thích với các định dạng tài liệu tham khảo có sẵn trong MS Word và kể cả trong các gói hỗ trợ tài liệu tham khảo cho LaTeX.

1.3. Soạn thảo luận án luận án bằng MS Word

MS Word là phần mềm soạn thảo văn phòng và không được thiết kế để soạn thảo các công thức phức tạp cho các luận án. Dù MS Word có công cụ là Equation Editor tuy nhiên việc soạn thảo công thức bằng chuột không phải thuận tiện và chức năng cũng rất hạn chế so với phần mềm công cụ của hãng thứ 3 là MathType, xem [8]. MathType có hạn chế lớn là các công thức đều được biến đổi thành các ảnh bitmap, do đó khi số lượng công thức nhiều thì file soạn thảo sẽ nặng, và việc đồng bộ giữa ảnh và chữ (text) trong MS Word không được tối ưu, khi thay đổi size của text thì các công thức sẽ bị xô lệch.

Một số hạn chế khác của việc soạn thảo luận án bằng MS Word:

- Hạn chế lớn nhất là không hỗ trợ định dạng tài liệu thảo khảo đúng theo yêu cầu của Bộ Giáo dục và Đào tạo. Cụ thể là không hỗ trợ việc tách riêng tài liệu tiếng Việt với các tài liệu bằng ngôn ngữ khác; không hiển thị năm công bố ngay sau tên tác giả. Vì thế đa phần phải tiến hành lập danh sách

tài liệu tham khảo và tham chiếu bằng tay và đó là công việc rất tốn thời gian công sức và dễ bị nhầm lẫn, không có khả năng tự động đồng bộ.

- Mục lục các chương mục không có khả năng tùy biến hiển thị riêng trong luận án và hiển thị khác trong phần mục lục. Nếu dùng chức năng tự động tạo mục lục thì nhiều khi không hiển thị đúng theo yêu cầu và do đó buộc phải thực hiện bằng tay.

- Không có khả năng tự động căn chỉnh các thành phần trong luận án do đó phần hiển thị không được tự động tối ưu như LaTeX.

1.4. Soạn thảo luận án luận án bằng LaTeX

Hệ thống chế bản TeX lần đầu tiên được công bố bởi Donald Knuth vào năm 1978 và thường được sử dụng để chế bản các sách và tài liệu khoa học chất lượng cao, khi chứa nhiều công thức toán học và vật lý. LaTeX là ngôn ngữ được đóng gói dạng macro của TeX và được thực hiện bởi Leslie Lamport vào năm 1986. *Một số ưu điểm của LaTeX:*

- LaTeX có thể coi là một ngôn ngữ phục vụ chế bản, nhưng bản thân nó cũng là một ngôn ngữ lập trình, cho phép định nghĩa kế thừa và định nghĩa những lệnh mới. Các lệnh LaTeX không chỉ dễ dàng tạo ra các công thức toán học chuyên nghiệp mà còn có thể vẽ các công thức hóa học, các mạch điện và các hình dạng vetor có độ phức tạp rất cao (xem phụ lục).

- LaTeX tự động dàn trang và trình bày một cách tự động và tối ưu nên bản in luôn hợp lý và chuyên nghiệp.

- Những cấu trúc phức tạp như chú thích, tham chiếu, biểu bảng, mục lục, ... cũng được tạo một cách dễ dàng.

- LaTeX có tính tương thích rất cao, có thể được sử dụng trên nhiều hệ điều hành khác nhau, và các phần mềm để soạn thảo LaTeX thường là mã nguồn

mở và miễn phí.

- LaTeX có thể mở rộng bằng các gói phần mềm trình bày tại https://www.ctan.org/ với 5378 gói (packages - ngày 25/8/2017). Các gói này có thể được cài đặt bằng tay hoặc hoàn toàn tự động khi được sử dụng lần đầu tiên.

Từ những ưu điểm nói trên có thể thấy LaTeX rất phù hợp để soạn thảo luận văn, luận án, chuyên đề và sách chuyên khảo của các ngành kỹ thuật và công nghệ.

Một số hạn chế của LaTeX:

- Tương đối khỏ sử dụng đối với người dùng mới tiếp cận.

- Thường là không trực quan WYSIWYG (gõ đến đâu hiển thị đến đấy) như soạn thảo bằng MS Word, phải dùng các câu lệnh tiếng Anh khó nhớ, ngay đến việc căn chỉnh, kích thước, canh lề hay giãn dòng đều phải dùng các lệnh không phải dễ dàng đối với người mới.

- Các gói mặc định không hỗ trợ kiểu định dạng tài liệu tham khảo theo quy định của Bộ Giáo dục và Đào tạo.

  Có 2 phần mềm phổ biến để biên dịch dữ liệu về tài liệu tham khảo đó là BibTex và biber, và 2 gói macro hay được sử dụng là natbib và bilatex. Trong đó BibTex và natbib là phần mềm và gói macro đã cũ và tồn tại hàng chục năm qua, nhược điểm lớn nhất của 2 thành phần này là không hỗ trợ Unicode do đó không thể sử dụng tên tác giả hay tên tài liệu bằng tiếng Việt Unicode (trừ trường hợp sử dụng liệt kê tài liệu tham khảo bằng tay).

  Nhược điểm của natbib còn được thấy ở chỗ, gói này không hỗ trợ phân nhiều tách thành nhiều phần tài liệu tham khảo theo ngôn ngữ Việt-Anh, hay theo các tiêu chí khác hoặc buộc phải thực hiện nhiều công đoạn và lập trình khác. Ngôn ngữ để viết cho gói này là postfix tương đối khó lập trình và phải yêu cầu file .bst.

Trong khi đó bilatex chỉ sử dụng ngôn ngữ macro của LaTeX nên sẽ dễ dàng hơn cho lập trình viên. Biblatex có thể được biên dịch bởi biber hoặc BibTex 8-Bit (có hỗ trợ Unicode UTF-8). Ngoài ra bilatex cũng có rất nhiều lựa chọn (options) và có khả năng tùy biến rất linh hoạt và mềm dẻo. Tài liệu hướng dẫn sử dụng gói này cũng lên đến gần 280 trang.

Vấn đề sẽ giải quyết trong Luận án:

Mục tiêu của Luận án là xây dựng các gói phần mềm và định dạng chuyên dùng (**vietkey.luanan.1.2.cls**) cho việc soạn thảo luận văn, luận án theo đúng quy định của Bộ. Đơn giản hóa công tác soạn thảo, giảm thiểu các câu lệnh phức tạp rắc rối trong khâu căn chỉnh định dạng để người viết chỉ cần tập trung vào nội dung chuyên môn mà không cần phải học các câu lệnh LaTeX quá phức tạp và khó nhớ.

Ngoài ra tác giả cũng soạn một luận án mẫu, cấu trúc các thành phần đúng như quy định để nghiên cứu sinh dễ dàng tùy biến, chỉnh sửa thành luận án của mình.

1.5. Kết luận chương 1

Chương này nghiên cứu sinh (NCS) trình bày tổng quan về vấn đề nghiên cứu: soạn thảo luận văn, luận án tiến sĩ. NCS đã trình bày các công cụ phổ biến, ưu nhược điểm của các công cụ này, những tồn tại hạn chế cần giải quyết trong khuôn khổ luận án.

CHƯƠNG 2. HƯỚNG DẪN VIẾT LUẬN ÁN BẰNG LaTeX

Chương này là phần trọng tâm của Luận án, bao gồm: phần cài đặt môi trường và gói phần mềm vietkey.luanan.1.2.cls, tiếp theo là phần hướng dẫn sử dụng gói phần mềm này, cuối cùng là một số lưu ý khi sử dụng LaTeX trong việc soạn thảo luận án.

2.1. Cài đặt môi trường soạn thảo LaTeX

2.1.1. Cài đặt LaTeX

- Cài đặt lõi cho môi trường LaTeX : vào trang chủ https://miktex.org/ và download phần mềm MiKTeX tương ứng cho hệ điều hành đang sử dụng. Không nên cài gói này từ các link hay đĩa CD không chính chủ.
- Nên cài đặt phần mềm soạn thảo LaTeX là TeXStudio từ trang chủ http://www.texstudi (mặc dù trong bộ MiKTeX cũng đã có kèm phần mềm soạn thảo là TeXworks nhưng phần mềm này khá thô sơ và ít tính năng nâng cao).

2.1.2. Cài đặt vietkey.luanan.1.2.cls

- Vào trang web theo đường dẫn **http://j.mp/trinhbayluanan** và download file **MauLA.zip**.
- Copy và giải nén file**MauLA.zip** vào thư mục làm việc, là thư mục chứa file .tex gốc của luận án, luận văn.

2.1.3. Các file tối thiểu của gói vietkey.luanan

- **vietkey.luanan.1.2.cls**
- **luanan.bbx**
- **clean.bat**

2.2. Hướng dẫn soạn thảo luận án bằng LaTeX

Cách đơn giản nhất là sử dụng class của tác giả đã xây dựng là *vietkey.luanan* phiên bản hiện thời là 1.2 (25/8/2017).

File gốc hay master là **LuanAn.tex** xem Hình 2.1. Các chương mục sẽ được cấu trúc thành các file khác nhau. Dùng lệnh **\include{tenFile.tex}** để gắn các chương mục này vào file gốc. Các file này có thể nằm ở thư mục khác nhưng để tiện soạn thảo các chương mục này nên nằm trong cùng một thư mục.

Các lệnh do tác giả xây dựng có tiết đầu tố là **\VK***.

2.2.1. Tài liệu tham khảo

Ví dụ tham chiếu tài liệu tham khảo [2], hay [1], hoặc [11], và một số khác nữa: [7], [11]. [5], [10], [4]. [9], [6], [3].

Nhập liệu về tài liệu tham khảo trong file .bib như thường lệ xem file mẫu *bibdmt.bib* đi kèm , tuy nhiên để có thể phân loại tài liệu tiếng Việt và tiếng Anh, chúng ta thêm hai trường là **langid = {slovene}** và **keywords = "Vietnam"** để phân biệt với các văn bản tiếng Anh, có thể làm tương tự với tiếng Nga, tiếng Trung. *Đáng tiếc là gói BibLaTex chưa hỗ trợ ngôn ngữ tiếng Việt do đó tác giả phải chọn ngôn ngữ slovene* để tùy biến.

Ngoài ra ở trong file .bib có thể gõ tiếng Việt Unicode. Dưới đây là một mục (bài báo) trong file .bib có số liệu bằng tiếng Việt.

LuanAn.tex | chuong_hien_trang.tex | chuong_huong_dan_viet_luan_an.tex | phulucc...

```
1  %% Mẫu luận án tiến sĩ (thạc sĩ) theo style vietkey.luanan.1.2.cls - Version 1.2
2  %% (c) Dang Minh Tuan, Vietkey Group.
3  %% Tel: +84-98-868-6636, Email: tuanvietkey@gmail.com.
4  %%
5  %% History:
6  %% - version 1.2 (2017/08/11)
7  %% - Created on 2016/08/16.
8
9  \documentclass[fontsize=13pt,oneside,a4paper,openany]{vietkey.luanan.1.2}
10
11 \usepackage[backend=bibtex,bibstyle=luanan,sorting=nyvt,block=none,defernumbers=
   true,babel=other]{biblatex} %tham số firstinits=true để viết tắt, defernumbers
   để số thứ tự liền mạch.
12
13 \addbibresource{bibdmt.bib} %%% dữ liệu về tài liệu tham khảo.
14 \begin{document}
15
16 \include{trangbia}      %%% có thể thay đổi
17
18 \VKnumRoman             %%% đánh số bằng chữ cái i, ii...
19
20 \include{loicamdoan}    %%% có thể thay đổi
21 \include{loicamon}      %%% có thể thay đổi
22
23 \VKmucLuc               %%% mục lục
24
25 \include{kyhieu}        %%% có thể thay đổi
26
27 \VKdanhMucHinhVe        %%% danh mục hình vẽ
28 \VKdanhMucBangBieu      %%% danh mục bảng biểu
29 %\VKdanhMucDinhLy
30 %\VKdanhMucDinhNghia
31 \VKbatDaudanhSo         %%% bắt đầu đánh số từ 1,2,3...
32
33 \include{loinoidau}     %%% có thể thay đổi
34 \include{chuong_hien_trang} %%% có thể thay đổi (Chương 1)
35 \include{chuong_huong_dan_viet_luan_an} %%% có thể thay đổi (Chương 2)
36 \include{chuong_mau}    %%% có thể thay đổi (Chương 3)
37 \include{ketluan}       %%% có thể thay đổi
38 \include{chdanhmuccongbo}   %%% có thể thay đổi
39
40 \VKngatTrang            %%% ngắt trang để chuyển sang tài liệu tham khảo
41 \VKtaiLieuThamKhao      %%% tài liệu tham khảo
42 \VKdanhSoPhuLuc         %%% bắt đầu đánh số cho phụ lục
43
44 \include{phuluccaidat}  %%% có thể thay đổi
45
46 \end{document}
47
```

Hình 2.1: *File gốc LuanAn.tex*

Bài báo:

```
@article{Bai22,
author    ="Nguyễn Hiếu Minh and Đỗ Thị Bắc",
title     ="{Một số lược đồ chữ ký số mù mới
            dựa trên bài toán DLP và ECDLP}",
journal   ="Tạp Chí Khoa học và Công nghệ năm 2015",
volume    ="11",
number    ="5",
pages     ="3--11",
year      ="2015",
langid    = {slovene},
keywords  = "Vietnam"
```

Sách:

```
@book{V10945,
author ="Lưu Hồng Dũng",
title  ="Nghiên cứu, phát triển các lược đồ chữ ký số tập thể",
publisher ="Luận án tiến sĩ kỹ thuật, Học viện KTQS",
year ="2013",
keywords ="Vietnam"
```

2.3. Các gói đã được nhúng trong *vietkey.luanan*

- \usepackage[vietnam]{babel}
- \usepackage[utf8]{vietnam}
- \usepackage{enumerate}
- \usepackage{amsmath,amsxtra,amssymb,latexsym, amscd,amsthm}
- \usepackage{indentfirst}

- \usepackage{mathptmx}
- \usepackage{fancyhdr}
- \usepackage{picinpar}
- \usepackage{floatflt}
- \usepackage{epic}
- \usepackage{curves}
- \usepackage{makeidx}
- \usepackage{longtable}
- \usepackage{multicol}
- \usepackage{listings}
- \usepackage[fontsize=13pt]{scrextend}
- \usepackage[tight,vietnam]{minitoc}
- \usepackage{fancybox}
- \usepackage{pdflscape}
- \usepackage{tcolorbox}
- \usepackage{enumitem}
- \usepackage{tikz}
- \usepackage[utf8]{inputenc, vietnam}
- \usepackage{color, graphicx}
- \usepackage[chapter]{algorithm}
- \usepackage{algorithmic}

- \usepackage{eso-pic,calc}
- \usepackage{hyperref}
- \usepackage{bookmark}
- \usepackage{titlesec}
- \usepackage{thmtools}
- \usepackage{booktabs}
- \usepackage{geometry}

2.4. Một số kinh nghiệm và lưu ý khi sử dụng

- Trong một số trường hợp khi cập nhật tài liệu tham khảo, việc đồng bộ giữa tham chiếu tài liệu tham khảo và dữ liệu tài liệu tham khảo có thể có sự khác biệt, khi đó cần phải xóa các file trung gian để phần mềm soạn thảo biên dịch lại từ đầu. Tác giả đã tạo ra một file chạy **clean.bat** tự động xóa hết các file này. Kích hoạt bằng cách nháy đúp con chuột vào file này trong File Explore.
- Tên các chương có thể được hiển thị khác nhau trong phần nội dung và phần mục lục. Trong phần nội dung do phải dùng font lớn để làm tiêu đề chương nên với tên dài cần phải ngắt dòng, tuy nhiên ở phần mục lục dùng font chữ nhỏ hơn nếu để tự động thì ở phần mục lục cũng ngắt dòng tương ứng như vậy sẽ không hợp lý. Để có thể hiển thị và ngắt dòng khác nhau có thể dùng dấu [] và {} sau lệnh \chapter tương ứng với hiển thị trong mục lục và tiêu đề trong nội dung luận án.

2.5. Kết luận chương 2

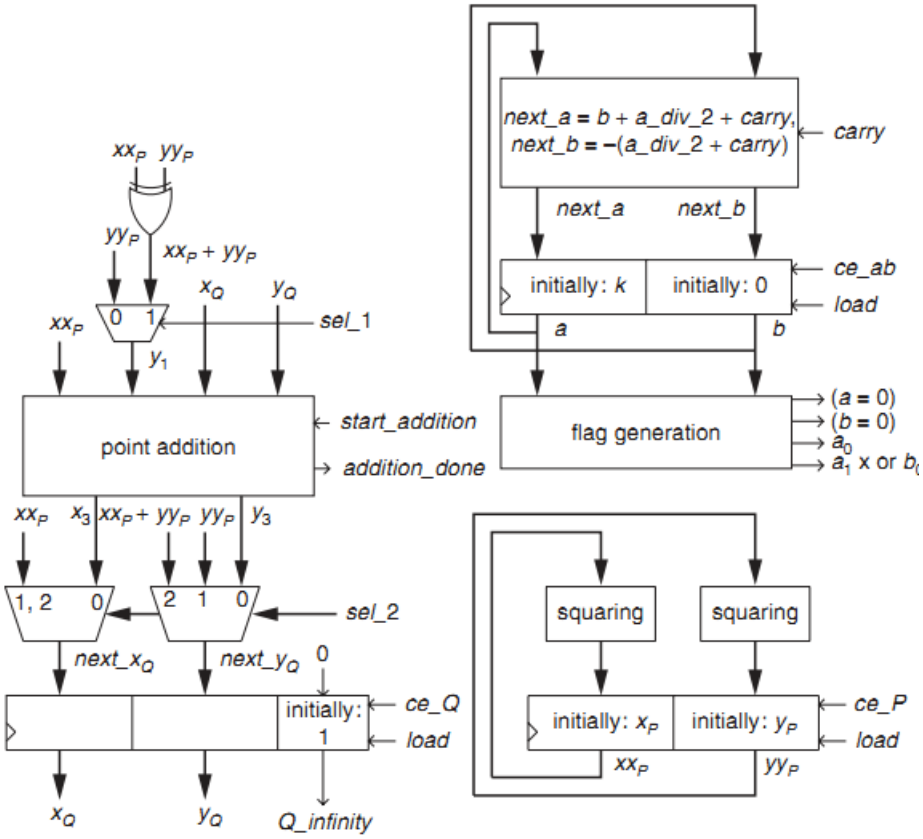
LaTeX nói chung và gói bilatex đang là xu thế được sử dụng để biên soạn luận án, luận văn và quản lý, sắp xếp tài liệu tham khảo một cách mềm dẻo và linh hoạt. Với class mới được phát triển "**vietkey.luanan**" có thể đáp ứng được hầu hết các yêu cầu trình bày luận án và cách sắp xếp và trích dẫn tài liệu tham khảo do các trường đại học ở Việt Nam quy định.

Mọi góp ý và đóng góp cho tài liệu cũng như gói class "**vietkey.luanan**" xin gửi về **tuanvietkey@gmail.com** hoặc thông qua **facebook.com/tuanvietkey**.

CHƯƠNG 3. KẾT HỢP CHỮ KÝ SỐ TẬP THỂ ĐA THÀNH PHẦN VỚI CÁC MÔ HÌNH KHÁC

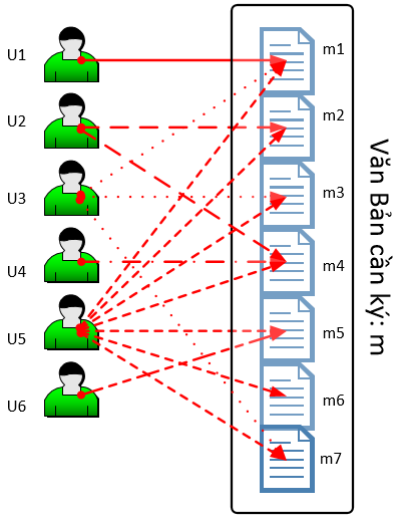
Chương này đề xuất mô hình kết hợp giữa chữ ký số tập thể đa thành phần với chữ ký số ủy nhiệm và với chữ ký số mù. Ở mỗi loại hình kết hợp sẽ có lần lượt định nghĩa tổng quát, khả năng tấn công và đề xuất một lược đồ cụ thể để chứng minh tính đúng đắn của mô hình kết hợp.

3.1. Đề xuất mô hình chữ ký số tập thể đa thành phần



Hình 3.1: *Phép nhân vô hướng trên đường cong elliptic*

Luận án đưa ra mô hình ký tập thể mới và gọi là *Chữ ký số tập thể đa thành phần*. Ở đó mỗi thành viên có thể được giao cho nhiệm vụ ký một hay nhiều phần khác nhau của văn bản (các phần này không nhất thiết phải liên tục liền kề), mặt khác trong mô hình này, một thành phần của văn bản cũng có thể được một hay nhiều thành viên phụ trách và họ sẽ phải ký đồng thời vào thành phần này.



Hình 3.2: *Mô hình ký tập thể phân biệt trách nhiệm đa thành phần*

Hình 3.2 minh họa cho khái niệm chữ ký số tập thể đa thành phần. Ở đây có sáu người ký và văn bản được chia thành bảy phần khác nhau. Như vậy số thành viên ký trong tập thể và số thành phần văn bản được chia ra có tính độc lập tương đối với nhau. Số thành phần của văn bản có thể lớn hơn hay nhỏ hơn số thành viên của tập thể.

Trong Hình 3.2, có thể thấy vai trò và trách nhiệm ký của tập thể người ký như sau:

- Các người ký $U1, U4, U6$ ký vào một phần của thông điệp m, tương ứng là các phần m_1, m_4, m_5.
- Người ký $U2$ ký và có trách nhiệm với 02 phần m_2 và m_4 của văn bản m.

- Người ký $U3$ có trách nhiệm ký với 03 phần m_1, m_3, m_7 của văn bản m.
- Người ký $U5$ có trách nhiệm ký tất cả các thành phần của văn bản m.

Mặt khác cũng trên Hình 3.2, các thành phần của văn bản m được ký bởi những người ký sau:

- Thành phần m_6 chỉ do một người chịu trách nhiệm ký là $U5$.
- Các thành phần có 02 người chịu trách nhiệm ký là m_2, m_3, m_5, m_7.
- Riêng phần m_4 có 03 người chịu trách nhiệm ký là $U2, U4, U5$.

Thuật toán 3.1 Sinh chữ ký số ECDSA

INPUT: Tham số D = (q, FR, S, a, b, P, n, h), khóa bí mật d, thông điệp m.
OUTPUT: Chữ ký số (r, s).

1: Chọn ngẫu nhiên $k \in [1, n-1]$,
2: $R \leftarrow kP = (x_1, y_1)$ và chuyển đổi $\bar{x_1} \leftarrow x_1$.
3: $r \leftarrow \bar{x_1} \pmod n$.
4: **if** $r = 0$ or $R = \infty$ **then**
5: Nhảy đến bước 1:
6: **end if**
7: $e \leftarrow H(m)$.
8: $s \leftarrow k^{-1}(e + dr) \pmod n$.
9: **if** $s = 0$ **then**
10: Nhảy đến bước 1:
11: **end if**
12: Trả về (r, s)

Đối với các tổ chức, cơ quan quản lý, văn bản m có thể là công văn được phát ra, có nhiều thành phần liên quan đến chức năng của các phòng ban khác nhau trong tổ chức, có những thành phần sẽ liên quan chồng chéo giữa nhiều phòng ban và các phòng ban này phải chung nhau chịu trách nhiệm xem xét và ký duyệt.

Coi NSIG là tổng số các thành viên trong tập thể giam giá ký văn bản m, và NSEC là tổng số các thành phần cấu thành lên văn bản m. Tùy theo mối quan

Bảng 3.1: *Chữ ký số theo quan hệ giữa* NSIG *và* NSEC

TT	Quan hệ	Mô hình chữ ký
1	NSIG $= 1$ và NSEC $= 1$	Mô hình chữ ký số đơn thông thường.
2	NSIG > 1 và NSEC $= 1$	Mô hình chữ ký số tập thể không phân biệt trách nhiệm người ký.
3	NSIG > 1 và NSIG $=$ NSEC	Mô hình chữ ký số tập thể phân biệt trách nhiệm người ký.
4	Với mọi NSIG và NSEC	Mô hình chữ ký số tập thể đa thành phần (có phân biệt trách nhiệm người ký).

hệ và giá trị của NSIG và NSEC chúng ta có thể tổng hợp các mô hình ký văn bản trong Bảng 3.1. Quan sát bảng này chúng ta sẽ thấy: khi NSEC $=$ NSIG $= 1$ chúng ta sẽ có chữ ký số đơn. Trường hợp thứ 2 khi NSIG > 1 và NSEC $= 1$ chúng ta có mô hình chữ ký số tập thể không phân biệt trách nhiệm người ký. Trường hợp thứ 3 khi NSIG > 1 và NSIG $=$ NSEC chúng ta có mô hình chữ ký số tập thể có phân biệt trách nhiệm người ký. Và cuối cùng là trường hợp thứ 4 khi NSIG và NSEC có giá trị bất kỳ. Qua Bảng 3.1 chúng ta cũng dễ dàng nhận thấy mô hình ký tập thể đa thành phần mới được đề xuất là trường hợp tổng quát của tất cả các mô hình trước đó (ký đơn, ký tập thể không phân biệt trách nhiệm, ký tập thể có phân biệt trách nhiệm).

3.2. Mô hình kết hợp chữ ký số tập thể đa thành phần và chữ ký số ủy nhiệm

Chữ ký số ủy nhiệm là mô hình, lược đồ ký số mà ở đó một cá nhân có thể ủy quyền cho một cá nhân khác ký thay cho mình khi đi vắng. Và việc ký thay này có thể được gắn với một thuộc tính nào đó để hạn chế về điều kiện hiệu lực của việc ủy nhiệm, ví dụ như hạn chế về mặt thời gian, hạn chế về mặt nội

dung, lĩnh vực ký.

3.2.1. Định nghĩa chữ số tập thể ủy nhiệm đa thành phần tổng quát

Luận án đưa ra mô hình ký tập thể mới và gọi là *Chữ ký số tập thể ủy nhiệm đa thành phần*. Ở đó mỗi thành viên có thể được giao cho nghiệm vụ ký một hay nhiều phần khác nhau của văn bản (các phần này không nhất thiết phải liên tục liền kề), mặt khác trong mô hình này, một thành phần của văn bản cũng có thể được một hay nhiều thành viên phụ trách và họ sẽ phải ký đồng thời vào thành phần này.

Giả sử có NSIG người ký U_i; $1 \leqslant i \leqslant \mathsf{NSIG}$ cần ký văn bản $m \in \{0,1\}^*$. Chia m thành NSEC phần, sao cho có thể biểu diễn m dưới dạng:

$$m = (m_1 \parallel m_2 \parallel m_3 \parallel \cdots \parallel m_{\mathsf{NSEC}}).$$

sử dụng ký hiệu và định nghĩa mảng phân công ký $\mathfrak{V}$.

Từng thành viên U_i sẽ chịu trách nhiệm ký một số phần của văn bản m, tính giá trị hàm băm $h_i(m_j)$; $1 \leqslant j \leqslant \mathsf{NSEC}$ và gửi cho người ủy nhiệm, người này sẽ tính giá trị băm tổng hợp H_e.

Định nghĩa 3.2.1 (Chữ ký số tập thể ủy nhiệm đa thành phần - MSM-S-PROXY)**.** *Giả sử văn bản m được chia thành* NSEC*, có tập thể* NOSIG *người ủy nhiệm cần ủy nhiệm quyền ký cho tập thể* NPSIG *người ký, chữ ký tập thể ủy nhiệm đa thành phần là tập bộ 13 thành phần (*$\mathbf{Setup}$*,* $\mathbf{KeyGen}_{OSIG}$*,* $\mathbf{KeyGenPub}_{OSIG}$*,* $\mathbf{Sign}_{OSIG}$*,* $\mathbf{SignPub}_{OSIG}$*,* $\mathbf{Verify}_{OSIG}$*,* $\mathbf{VerifyPub}_{OSIG}$*,* $\mathbf{KeyGen}_{PSIG}$*,* $\mathbf{KeyGenPub}_{PSIG}$*,* $\mathbf{Sign}_{PSIG}$*,* $\mathbf{SignPub}_{PSIG}$*,* $\mathbf{Verify}_{PSIG}$*,* $\mathbf{VerifyPub}_{PSIG}$ *) có thuật toán thực hiện trong thời gia đa thức với các giao thức sau:*

(1) Khởi tạo tham số params *với k là tham số độ an toàn, R là tham số ngẫu nhiên.*

$$\mathsf{params} \xleftarrow{R} \mathbf{Setup}(1^k) \tag{3.1}$$

(2) Sinh khóa công khai và bí mật cho các thành viên $OSIG_i$, $1 \leqslant i \leqslant \mathsf{NOSIG}$.

$$(\mathsf{PK.OSIG_i}, \mathsf{SK.OSIG_i}) \leftarrow \textbf{KeyGen}_{\boldsymbol{OSIG}}(\mathsf{params}, 1^k, i) \tag{3.2}$$

Sau khi có khóa công khai của từng thành viên, sinh khóa công khai của cả tập thể bằng thuật toán:

$$(\mathsf{PK.OSIG_{pub}}) \leftarrow \{\textbf{KeyGenPub}_{\boldsymbol{OSIG}}(\mathsf{PK.OSIG_i})\}_{i=1}^{\mathsf{NOSIG}} \tag{3.3}$$

(3) Hình thành chữ ký của tập thể người ủy nhiệm: Từng thành viên $OSIG_i$ tham gia ký văn bản theo thuật toán dưới đây:

$$\sigma.OSIG_i \leftarrow \textbf{Sign}_{\boldsymbol{OSIG}}{}^{R}(\mathtt{SK.OSIG_i}, m) \tag{3.4}$$

Người tổng hợp cần phải kiểm tra chữ ký của từng thành viên bằng thuật toán sau:

$$\{0,1\} \leftarrow \{\textbf{Verify}_{\boldsymbol{OSIG}}(\mathsf{PK.OSIG_i}, m, \sigma_i)\}_{i=1}^{\mathsf{NOSIG}} \tag{3.5}$$

Nếu tất cả đều hợp lệ (Accept) thì tiến hành tính chữ ký của cả tập thể, nếu không thì yêu cầu thực hiện lại bước này.

$$\sigma.OSIG_{pub} \leftarrow \{\textbf{SignPub}_{\boldsymbol{OSIG}}{}^{R}(\sigma_i)\}_{i=1}^{\mathsf{NOSIG}} \tag{3.6}$$

(4) Xác thực văn bản của tập thể người ủy nhiệm:

$$\{0,1\} \leftarrow \textbf{VerifyPub}_{\boldsymbol{OSIG}}(\mathsf{PK.OSIG_{pub}}, m', \sigma.OSIG_{pub}) \tag{3.7}$$

(5) Sinh khóa công khai và bí mật cho các thành viên được ủy nhiệm $PSIG_j$, $1 \leqslant j \leqslant \mathsf{NPSIC}$, w là giá trị bảo đảm.

$$(\mathsf{PK.PSIG_j}, \mathsf{SK.PSIG_j}) \leftarrow \textbf{KeyGen}_{\boldsymbol{PSIG}}(\mathsf{params}, w, 1^k, j, \mathfrak{V}_j) \tag{3.8}$$

Sau khi có khóa công khai của từng thành viên, sinh khóa công khai của cả

tập thể bằng thuật toán:

$$(\mathsf{PK.PSIG_{pub}}) \leftarrow \{\mathbf{KeyGenPub}_{\boldsymbol{PSIG}}(\mathsf{PK.PSIG_j}, \mathfrak{V}_j)\}_{j=1}^{\mathsf{NPSIC}} \tag{3.9}$$

(6) Hình thành chữ ký của tập thể người ủy nhiệm: Từng thành viên $PSIG_j$ tham gia ký văn bản theo thuật toán dưới đây:

$$\sigma.PSIG_j \leftarrow \mathbf{Sign}_{\boldsymbol{PSIG}}{}^{R}(\mathtt{SK.PSIG_j}, w, m, \mathfrak{V}_j) \tag{3.10}$$

Người tổng hợp cần phải kiểm tra chữ ký của từng thành viên bằng thuật toán sau:

$$\{0,1\} \leftarrow \{\mathbf{Verify}_{\boldsymbol{PSIG}}(\mathsf{PK.PSIG_j}, w, m, \sigma_j, \mathfrak{V}_j)\}_{j=1}^{\mathsf{NPSIC}} \tag{3.11}$$

Nếu tất cả đều hợp lệ (Accept) thì tiến hành tính chữ ký của cả tập thể, nếu không thì yêu cầu thực hiện lại bước này.

$$\sigma.PSIG_{pub} \leftarrow \{\mathbf{SignPub}_{\boldsymbol{PSIG}}{}^{R}(\sigma_j, \mathfrak{V})\}_{j=1}^{\mathsf{NPSIC}} \tag{3.12}$$

(7) Xác thực văn bản của tập thể người được ủy nhiệm:

$$\{0,1\} \leftarrow \mathbf{VerifyPub}_{\boldsymbol{PSIG}}(\mathsf{PK.PSIG_{pub}}, m', \sigma.PSIG_{pub}) \tag{3.13}$$

3.2.2. Tấn công ACMA - Adaptive Chosen Message Attacks với mô hình MSMS-PROXY

Đây là loại hình tấn công mạnh nhất, kẻ tấn công có thể được lựa chọn văn bản để ký phụ thuộc vào khóa công khai cũng như những chữ ký số có từ trước đó. Có thể biểu diễn việc này thông qua khả năng truy cập đến hàm Oracle, ký hiệu là $\mathsf{Sign}(\cdot)_{sk}$.

$$\epsilon_{\mathcal{A}}(k) \stackrel{\text{def}}{=} \Pr\left[\begin{array}{l} \{m_{i_m}\}_{i_m=1}^{\ell} \leftarrow M_k; \\ (\mathsf{PK.OSIG_i}, \mathsf{SK.OSIG_i}) \leftarrow \textbf{KeyGen}_{\boldsymbol{OSIG}}(\mathsf{params}, 1^k, i); \\ (\mathsf{PK.OSIG_{pub}}) \leftarrow \{\textbf{KeyGenPub}_{\boldsymbol{OSIG}}(\mathsf{PK.OSIG_i})\}_{i=1}^{\mathsf{NOSIG}}; \\ \sigma.OSIG_i \leftarrow \textbf{Sign}_{\boldsymbol{OSIG}}{}^{R}(\mathtt{SK.OSIG_i}, m); \\ (\mathsf{PK.PSIG_j}, \mathsf{SK.PSIG_j}) \leftarrow \textbf{KeyGen}_{\boldsymbol{PSIG}}(\mathsf{params}, w, 1^k, j, \mathfrak{V}_j); \\ (\mathsf{PK.PSIG_{pub}}) \leftarrow \{\textbf{KeyGenPub}_{\boldsymbol{PSIG}}(\mathsf{PK.PSIG_j}, \mathfrak{V}_j)\}_{j=1}^{\mathsf{NPSIC}}; \\ \sigma.PSIG_j \leftarrow \textbf{Sign}_{\boldsymbol{PSIG}}{}^{R}(\mathtt{SK.PSIG_j}, w, m, \mathfrak{V}_j); \\ \sigma.PSIG_{pub_{i_m}} \leftarrow \{\textbf{SignPub}_{\boldsymbol{PSIG}}{}^{R}(\sigma_j, \mathfrak{V})\}_{j=1}^{\mathsf{NPSIC}}; \\ (m, \sigma.PSIG_{pub_{i_m}}) \leftarrow \mathcal{A}^{\mathsf{Sign}(\cdot)_{sk}}\left(\mathsf{PK_{pub}}\right) \end{array} : \begin{array}{l} 1 \leftarrow \textbf{VerifyPub}(\mathsf{PK_{pub}}, m, \sigma_{pub}, \mathfrak{V}) \\ \wedge \quad m \notin \{m_1, \ldots, m_\ell\} \end{array}\right] \tag{3.14}$$

$$\epsilon_{\mathcal{A}}(k) \leq \mathsf{negl}(k)$$

Định nghĩa 3.2.2. *Lược đồ MSMS-PROXY được cho là không thể giả mạo với tấn công ACMA khi với mọi thuật toán thời gian đa thức của người tấn công $\mathcal{A}$, xác suất thành công của thực nghiệm dưới đây là một hàm nhỏ không đáng kể:*

(1) Chuỗi $\ell = \ell(k)$ văn bản $m_1, \ldots, m_\ell$ được chọn một cách ngẫu nhiên trong không gian M_k.

(2) Thực hiện các thuật toán trong lược đồ để tạo ra chữ ký $\sigma_{pub_{i_m}}$.

(3) Thuật toán $\mathcal{A}$ với đầu vào là $\mathsf{PK_{pub}}$ và có thể truy cập đến $\mathsf{Sign}(\cdot)_{sk}$ với một số văn bản bất kỳ và sẽ cho ra chữ ký số (m, σ_{pub}). Không gian các văn bản truy vấn này gọi là M.

(4) Thực nghiệm tấn công thành công nếu $1 \leftarrow \textbf{VerifyPub}(\mathsf{PK_{pub}}, m, \sigma_{pub}, \mathfrak{V})$ *và* $m \neq M$.

3.2.3. Đề xuất chữ ký số tập thể đa thành phần ủy nhiệm dựa trên hệ mật định danh

3.2.3.1. Cài đặt

Coi G_1 là nhóm cộng cyclic có bậc là số nguyên tố q và phần tử sinh là P. G_2 là nhóm nhân cyclic có cùng bậc q. e là một ánh xạ song tuyến tính:

$$\hat{e} : G_1 \times G_1 \rightarrow G_2$$

H_1, H_2, H_3 là các hàm băm được sử dụng cho mục đích bảo mật và được định nghĩa như sau:

$$H_1 : \{0,1\}^* \rightarrow G_1 \tag{3.15}$$

$$H_2 : \{0,1\}^* \rightarrow \mathbb{Z}_q^* \tag{3.16}$$

$$H_3 : \{0,1\}^* \times \{0,1\}^* \rightarrow \mathbb{Z}_q^* \tag{3.17}$$

(1) Với tham số bảo mật k chọn ngẫu nhiên $s \in \mathbb{Z}_q^*$.

(2) Tính khóa công khai của hệ thống:

$$P_{pub} = sP \in G_1$$

(3) Công bố tham số của hệ thống là:

$$Params = (k, G_1, G_2, q, \hat{e}, H_1, H_2, H_3, P, P_{pub})$$

3.2.3.2. Tách khóa

Người ký ủy nhiệm có định danh là ID, có NPSIC người có thể ký ủy nhiệm ID_{B_i} với $1 \leq i \leq \mathsf{NPSIC}$.

(1) Bất kỳ ai cũng có thể tính khóa công khai của người cần ủy nhiệm:

$$Q_{ID} = H_1(ID) \in G_1$$

và những người được ủy nhiệm:

$$Q_{ID_{B_i}} = H_1(ID_{B_i}) \in G_1$$

(2) Người quản trị hệ thống sẽ tính khóa bí mật cho người ủy nhiệm và được ủy nhiệm:

$$S_{ID} = sQ_{ID}$$
$$S_{ID_{B_i}} = sQ_{ID_{B_i}} \quad 1 \leq i \leq \mathsf{NPSIC}$$

Người quản trị sẽ thông qua kênh bí mật gửi các khóa bí mật này cho các thành viên.

3.2.3.3. Hình thành chữ ký của người ủy nhiệm

(1) Với văn bản $m \in \{0,1\}^*$, người ký chọn ngẫu nhiên $x \in \mathbb{Z}_q^*$.

(2) Tính các giá trị:

$$V_s = xP$$
$$H = H_2(m)$$
$$W_s = HS_{ID} + xP_{pub}$$

(3) chữ ký của người ủy nhiệm là $\sigma = (W_s, V_s)$.

3.2.3.4. Xác thực chữ ký người ủy nhiệm

(1) Với văn bản m' và chữ ký $\sigma = (W_s, V_s)$ nhận được, người xác thực tính:

$$H' = H_2(m')$$

$$Q_{ID} = H_1(ID)$$

(2) Chấp nhận chữ ký khi điều kiện sau thỏa mãn:

$$\hat{e}(W_s, P) = \hat{e}(H'Q_{ID} + V_s, P_{pub}) \tag{3.18}$$

3.2.3.5. Sinh khóa cho người được ủy nhiệm

Trong giai đoạn này người ủy nhiệm sẽ trao đổi với người được ủy nhiệm với các quyền được ủy nhiệm. Để làm việc này người ủy nhiệm sẽ tạo ra một văn bản bảo đảm w, văn bản này sẽ kèm theo một số thông tin về văn bản, về những hạn chế của văn bản sẽ ủy nhiệm, thời gian hoặc định danh của những người sẽ ủy nhiệm.

(1) *Ủy nhiệm*: Người cần ủy nhiệm chọn ngẫu nhiên $t \in \mathbb{Z}_q^*$ và tính:

$$V = tP,$$
$$h = H_2(w),$$
$$W = hS_{ID} + tP_{pub} \in G_1$$

Chuyển giá trị (W, V, w) với các thành viên qua kênh truyền bí mật.

(2) *Kiểm tra ủy nhiệm*: mỗi thành viên ID_{B_i} sẽ tính $h = H_2(w)$ và kiểm tra điều kiện sau (nếu không thỏa mãn thì phải yêu cầu gửi lại hoặc hủy giao thức):

$$\hat{e}(W, P) = \hat{e}(hQ_{ID} + V, P_{pub})$$

(3) *Sinh khóa ủy nhiệm*: mỗi thành viên ID_{B_i} sẽ tính $h = H_2(w)$ tính khóa bí mật ủy nhiệm:

$$S_{pk_i} = W + hS_{ID_{B_i}}$$

3.2.3.6. Hình thành chữ ký ủy nhiệm

Trong pha này sẽ có một người phụ trách có nhiệm vụ tập hợp hết tất cả các chữ ký thành phần.

(1) Mỗi thành viên ID_{B_i} $(1 \leqslant i \leqslant \mathsf{NPSIC})$ chọn ngẫu nhiên số nguyên $x_i \in Z_q^*$ như là khóa bí mật và tính khóa công khai tương ứng theo công thức:

$$U_{p_i} = x_i P \tag{3.19}$$

Giả thiết có NPSIC người ID_{B_i}; $1 \leqslant i \leqslant \mathsf{NPSIC}$ cần ký văn bản $m \in \{0,1\}^*$. Chia văn bản m thành NSEC phần, sao cho có thể viết m theo dạng

$$m = (m_1||m_2||m_3||\ldots||m_{\mathsf{NSEC}})$$

sử dụng ký hiệu và định nghĩa mảng phân công ký $\mathfrak{V}$ như ở Định nghĩa **??** (trang **??**).

Từng thành viên ID_{B_i} sẽ chịu trách nhiệm ký một số phần của văn bản m, tính giá trị hàm băm $h_i(m_j)$; $1 \leqslant j \leqslant \mathsf{NSEC}$ và gửi cho người ủy nhiệm, người này sẽ tính giá trị băm cho m_j như sau:

$$e_j = \sum_{i=1}^{\mathsf{NSIG}} (\mathfrak{V}_i[j] \times h_i(m_j))\,; \quad 1 \leqslant j \leqslant \mathsf{NSEC} \tag{3.20}$$

$$h_3 = H_3(e_1||e_2 \cdots ||e_{\mathsf{NSEC}}, w) \tag{3.21}$$

Bằng cách tính như trên chúng ta thu được chữ ký số tập thể có phân biệt trách nhiệm, gửi giá trị U_{p_i} đến $(\mathsf{NPSIC} - 1)$ các thành viên còn lại.

(2) Các thành viên tính và gửi σ_{p_i} :

$$U_p = \sum_{i=1}^{\mathsf{NPSIG}} U_{p_i}$$

$$\sigma_{p_i} = h_3 S_{pk_i} + x_i P_{pub}$$

(3) Người phụ trách sau khi có các chữ ký thành phần sẽ tạo khóa công khai

ủy nhiệm:

$$Q_{pk_i} = h\left(Q_{ID} + Q_{ID_{B_i}}\right) + V \tag{3.22}$$

Và sau đó kiểm tra điều kiện:

$$\hat{e}(P, \sigma_{p_i}) = \hat{e}(P_{pub}, h' Q_{pk_i} + U_{p_i}) \tag{3.23}$$

$$\sigma_p = \sum_{i=1}^{\mathsf{NPSIG}} \sigma_{p_i} \tag{3.24}$$

sau đó chữ ký số ủy nhiệm sẽ là $(\sigma_p, V, w, U_p, \mathfrak{V})$.

3.2.3.7. Xác thực chữ ký ủy nhiệm

Người xác thực chữ ký ủy nhiệm sau khi nhận văn bản m' và chữ ký $(\sigma_p, V, w, U_p, \mathfrak{V})$ sẽ tiến hành các bước sau:

(1) Kiểm tra m' và bảo đảm w và các điều kiện liên quan.

(2) Kiểm tra sự ủy quyền của NPSIG người ký. Nếu không hợp lệ thì dựng lại và từ chối chữ ký.

(3) Tính các giá trị:

$$\begin{aligned} h &= H_2(w) \\ h'_3 &= H_3(m', w) \\ Q_{pk} &= h\left[\mathsf{NPSIG} \cdot Q_{ID} + \sum_{i=1}^{\mathsf{NPSIG}} Q_{ID_{B_i}}\right] + \mathsf{NPSIG} \cdot V \end{aligned}$$

(4) Kiểm tra điều kiện sau nếu đúng thì chấp nhận chữ ký, ngược lại là từ chối chữ ký:

$$\hat{e}(P, \sigma_p) = \hat{e}(P_{pub}, h'_3 Q_{pk} + U_p) \tag{3.25}$$

Định lý 3.2.3 [Lược đồ ký tập thể ủy nhiệm đa thành phần] *Nếu $m' = m$ thì $\hat{e}(P, \sigma_p) = \hat{e}(P_{pub}, h'_3 Q_{pk} + U_p)$.*

Chứng minh.

$$\hat{e}(P, \sigma_p) = \hat{e}(P_{pub}, h_3' Q_{pk} + U_p)$$

$$\hat{e}(P, \sum_{i=1}^{\mathsf{NPSIG}} \sigma_{p_i}) = \hat{e}(P_{pub}, h_3' Q_{pk} + U_p)$$

$$\hat{e}(P, \sum_{i=1}^{\mathsf{NPSIG}} \left[h_3 S_{pk_i} + x_i P_{pub}\right]) = \hat{e}(P_{pub}, h_3' Q_{pk} + U_p)$$

$$\hat{e}(P, \sum_{i=1}^{\mathsf{NPSIG}} \left[h_3 \left(W + h S_{ID_{B_i}}\right) + x_i P_{pub}\right]) = \hat{e}(P_{pub}, h_3' Q_{pk} + U_p)$$

$$\hat{e}(P, \sum_{i=1}^{\mathsf{NPSIG}} \left[h_3 \left(h S_{ID} + t P_{pub} + h S_{ID_{B_i}}\right) + x_i P_{pub}\right]) = \hat{e}(P_{pub}, h_3' Q_{pk} + U_p)$$

$$\hat{e}(P, \sum_{i=1}^{\mathsf{NPSIG}} \left[h_3 \left(h s Q_{ID} + t s P + h s Q_{ID_{B_i}}\right) + x_i s P\right]) = \hat{e}(P_{pub}, h_3' Q_{pk} + U_p)$$

$$\hat{e}(P_{pub}, \sum_{i=1}^{\mathsf{NPSIG}} \left[h_3 \left(h Q_{ID} + t P + h Q_{ID_{B_i}}\right) + x_i P\right]) = \hat{e}(P_{pub}, h_3' Q_{pk} + U_p)$$

$$\hat{e}(P_{pub}, \sum_{i=1}^{\mathsf{NPSIG}} \left[h_3 \left(h Q_{ID} + V + h Q_{ID_{B_i}}\right)\right] + U_p) = \hat{e}(P_{pub}, h_3' Q_{pk} + U_p)$$

$$\hat{e}(P_{pub}, h_3 \left[\sum_{i=1}^{\mathsf{NPSIG}} \left(h Q_{ID_{B_i}}\right) + \mathsf{NPSIG} \cdot h Q_{ID} + \mathsf{NPSIG} \cdot V\right] + U_p) = \hat{e}(P_{pub}, h_3' Q_{pk} + U_p)$$

$$\hat{e}(P_{pub}, h_3 \left[h \left[\mathsf{NPSIG} \cdot Q_{ID} + \sum_{i=1}^{\mathsf{NPSIG}} Q_{ID_{B_i}}\right] + \mathsf{NPSIG} \cdot V\right] + U_p) = \hat{e}(P_{pub}, h_3' Q_{pk} + U_p)$$

$$\hat{e}(P_{pub}, h_3 Q_{pk} + U_p) = \hat{e}(P_{pub}, h_3' Q_{pk} + U_p)$$

Biểu thức cuối cùng đúng khi $h_3' = h_3$. □

Phần phân tích hiệu năng và an toàn của lược đồ đề xuất theo mô hình an toàn đã định nghĩa rất dài và vì chương này chỉ mang tính minh họa cho việc kết hợp mô hình chữ ký số tập thể đa thành phần với mô hình chữ ký khác nên không được trình bày cụ thể ở đây.

3.3. Mô hình kết hợp chữ ký số tập thể đa thành phần và chữ ký số mù

3.3.1. Định nghĩa chữ ký số tập thể mù đa thành phần tổng quát

Luận án đưa ra mô hình ký tập thể mới và gọi là *Chữ ký số tập thể mù đa thành phần*. Ở đó mỗi thành viên có thể được giao cho nghiệm vụ ký một hay nhiều phần khác nhau của văn bản (các phần này không nhất thiết phải liên tục liền kề), mặt khác trong mô hình này, một thành phần của văn bản cũng có thể được một hay nhiều thành viên phụ trách và họ sẽ phải ký đồng thời vào thành phần này.

Giả sử có NSIG người ký U_i; $1 \leqslant i \leqslant \mathsf{NSIG}$ cần ký văn bản $m \in \{0,1\}^*$. Chia m thành NSEC phần, sao cho có thể biểu diễn m dưới dạng:

$$m = (m_1 \parallel m_2 \parallel m_3 \parallel \cdots \parallel m_{\mathsf{NSEC}})$$

Sử dụng ký hiệu và định nghĩa mảng phân công ký $\mathfrak{V}$.

Từng thành viên U_i sẽ chịu trách nhiệm ký một số phần của văn bản m, tính giá trị hàm băm $h_i(m_j)$; $1 \leqslant j \leqslant \mathsf{NSEC}$ và gửi cho người ủy nhiệm, người này sẽ tính giá trị băm tổng hợp H_e như Định nghĩa.

Định nghĩa 3.3.1 (Chữ ký số tập thể mù đa thành phần)**.** *Lược đồ chữ ký số tập thể đa thành phần là tập bộ 09 thành phần (***Setup***,* **KeyGen***,* **KeyGenPub***,* **Blind***,* **Sign***,* **SignPub***,* **UnBlid***,* **Verify***,* **VerifyPub***) có thuật toán thực hiện trong thời gia đa thức và có giao thức giữa các thành phần như sau:*

(1) Bộ khởi tạo **Setup***: đầu ra là bộ tham số* params

$$\mathsf{params} \xleftarrow{R} \textbf{Setup}(1^k) \tag{3.26}$$

(2) Sinh khóa công khai và bí mật cho các thành viên U_i, $1 \leqslant i \leqslant \mathsf{NSIG}$.

$$(\mathsf{PK_i}, \mathsf{SK_i}) \leftarrow \textbf{KeyGen}(\mathsf{params}, 1^k, i) \tag{3.27}$$

Sau khi có khóa công khai của từng thành viên, sinh khóa công khai của cả tập thể bằng thuật toán:

$$(\mathsf{PK_{pub}}) \leftarrow \{\textbf{KeyGenPub}(\mathsf{PK_i}, \mathfrak{V}_i)\}_{i=1}^{\mathsf{NSIG}} \tag{3.28}$$

(3) Người cần ký $\boldsymbol{\mathcal{U}}$ mã hóa văn bản m để tạo ra bản mã $\overline{m}$ bằng thuật toán **Blind***:*

$$\overline{m} \leftarrow \{\textbf{Blind}(m, \mathsf{PK_i})\}_{i=1}^{\mathsf{NSIG}} \tag{3.29}$$

(4) Ký văn bản: Từng thành viên U_i tham gia ký văn bản theo thuật toán dưới đây:

$$\overline{\sigma}_i \leftarrow \textbf{Sign}^R(\mathtt{SK_i}, \overline{m}, \mathfrak{V}_i) \tag{3.30}$$

Người tổng hợp cần phải kiểm tra chữ ký của từng thành viên bằng thuật toán sau:

$$\{0,1\} \leftarrow \{\textbf{Verify}(\mathsf{PK_i}, m, \sigma_i, \mathfrak{V}_i)\}_{i=1}^{\mathsf{NSIG}} \tag{3.31}$$

Nếu tất cả đều hợp lệ (Accept) thì tiến hành tính chữ ký của cả tập thể, nếu không thì yêu cầu thực hiện lại bước này.

$$\overline{\sigma}_{pub} \leftarrow \{\textbf{SignPub}^R(\overline{\sigma}_i)\}_{i=1}^{\mathsf{NSIG}} \tag{3.32}$$

(5) Người cần ký $\boldsymbol{\mathcal{U}}$ xóa mù cho chữ ký tập thể:

$$\sigma_{pub} \leftarrow \{\textbf{UnBlind}^R(\overline{\sigma}_{pub}, \mathsf{PK_i})\}_{i=1}^{\mathsf{NSIG}} \tag{3.33}$$

(6) Xác thực văn bản:

$$\{0,1\} \leftarrow \textbf{VerifyPub}(\mathsf{PK_{pub}}, m', \sigma_{pub}, , \mathfrak{V}) \tag{3.34}$$

3.3.2. Tấn công ACMA - Adaptive Chosen Message Attacks với mô hình MSMS-BL

Đây là loại hình tấn công mạnh nhất, kẻ tấn công có thể được lựa chọn văn bản để ký phụ thuộc vào khóa công khai cũng như những chữ ký số có từ trước đó. Có thể biểu diễn việc này thông qua khả năng truy cập đến hàm Oracle, ký hiệu là $\mathsf{Sign}(\cdot)_{sk}$.

$$\epsilon_{\mathcal{A}}(k) \stackrel{\text{def}}{=} \Pr\left[\begin{array}{l} \{m_{i_m}\}_{i_m=1}^{\ell} \leftarrow M_k; \\ \left\{(\mathsf{PK_i}, \mathsf{SK_i}) \leftarrow \textbf{Gen}(\mathsf{params}, 1^k)\right\}_{i=1}^{\mathsf{NSIG}}; \\ \mathsf{PK_{pub}} \leftarrow \{\textbf{GenPub}(\mathsf{PK_i}, \mathfrak{V}_i)\}_{i=1}^{\mathsf{NSIG}}; \\ \overline{m} \leftarrow \{\textbf{Blind}(m, \mathsf{PK_i})\}_{i=1}^{\mathsf{NSIG}}; \\ \overline{\sigma}_i \leftarrow \textbf{Sign}^R(\mathtt{SK_i}, \overline{m}, \mathfrak{V}_i); \\ \overline{\sigma}_{pub} \leftarrow \{\textbf{SignPub}^R(\overline{\sigma}_i)\}_{i=1}^{\mathsf{NSIG}}; \\ \sigma_{pub_{i_m}} \leftarrow \{\textbf{UnBlind}^R(\overline{\sigma}_{pub}, \mathsf{PK_i})\}_{i=1}^{\mathsf{NSIG}}; \\ (m, \sigma_{pub}) \leftarrow \mathcal{A}^{\mathsf{Sign}(\cdot)_{sk}}\left(\mathsf{PK_{pub}}\right) \end{array} : \begin{array}{l} 1 \leftarrow \textbf{VerifyPub}(\mathsf{PK_{pub}}, m, \sigma_{pub}, \mathfrak{V}) \\ \wedge \quad m \notin \{m_1, \ldots, m_\ell\} \end{array}\right]$$

$$\epsilon_{\mathcal{A}}(k) \leq \mathsf{negl}(k)$$

Định nghĩa 3.3.2. *Lược đồ MSMS được cho là không thể giả mạo với tấn công ACMA khi với mọi thuật toán thời gian đa thức của người tấn công $\mathcal{A}$, xác suất thành công của thực nghiệm dưới đây là một hàm nhỏ không đáng kể:*

(1) Chuỗi $\ell = \ell(k)$ văn bản $m_1, \ldots, m_\ell$ được chọn một cách ngẫu nhiên trong

không gian M_k.

(2) Thực hiện các thuật toán trong lược đồ để tạo ra chữ ký $\sigma_{pub_{i_m}}$.

(3) Thuật toán $\mathcal{A}$ với đầu vào là $\mathsf{PK_{pub}}$ và có thể truy cập đến $\mathsf{Sign}(\cdot)_{sk}$ với một số văn bản bất kỳ và sẽ cho ra chữ ký số (m, σ_{pub}). Không gian các văn bản truy vấn này gọi là M.

(4) Thực nghiệm tấn công thành công nếu $1 \leftarrow \mathbf{VerifyPub}(\mathsf{PK_{pub}}, m, \sigma_{pub}, \mathfrak{V})$ và $m \neq M$.

3.3.3. Đề xuất chữ ký số tập thể mù đa thành phần dựa trên đường cong elliptic

Giả sử có NSIG người ký U_i; $1 \leqslant i \leqslant \mathsf{NSIG}$ cần ký văn bản $m \in \{0,1\}^*$. Chia m thành NSEC phần, sao cho có thể biểu diễn m dưới dạng:

$$m = (m_1 \parallel m_2 \parallel m_3 \parallel \cdots \parallel m_{\mathsf{NSEC}}).$$

Sử dụng ký hiệu và định nghĩa mảng phân công ký $\mathfrak{V}$ như ở Định nghĩa 2.1.

Có NSIG người ký là U_i, với $1 \leq i \leq \mathsf{NSIG}$. Quá trình sinh khóa được thực hiện như sau:

3.3.3.1. Sinh khóa

(1) Mỗi người ký U_i $(1 \leqslant i \leqslant \mathsf{NSIG})$ chọn ngẫu nhiên số nguyên d_i như là khóa bí mật trong khoảng $[1, q-1]$ và tính khóa công khai tương ứng như điểm:

$$Q_i = d_i P$$

(2) Khóa công khai của cả tập thể sẽ là:

$$Q = \sum_{i=1}^{\mathsf{NSIG}} Q_i$$

3.3.3.2. Giao thức lược đồ ký mù tập thể

(1) Mỗi thành viên U_i sinh cặp khóa một lần $(\overline{k}_i, \overline{R}_i)$ bằng cách chọn ngẫu nhiên $k_i \in [1, q-1]$ và tính:

$$\overline{R}_i = (\mathfrak{V}_i \otimes k_i)P = (x_{\overline{k}_i}, y_{\overline{k}_i})$$

Tính $\overline{r}_i = c(x_{\overline{k}_i})$ và gửi $\overline{r}_i$ tới người cần ký.

(2) Người cần ký sẽ chọn hệ số mù $a, b \in [1, q-1]$ và tính điểm R trên đường cong elliptic E, tính:

$$\overline{R} = \sum_{i=1}^{\mathsf{NSIG}} \overline{R_i} = (x_{\overline{R}}, y_{\overline{R}})$$

gọi $c()$ là hàm chuyển đổi từ điểm sang giá trị tọa độ theo trục x từ đó tính $\overline{r} = c(x_{\overline{R}})$ và tính:

$$R = a\overline{R} + bQ = (x_R, y_R)$$

Tiếp theo tính giá trị $r = c(x_R)$ và:

$$\overline{m} = (H(m) + r + b)a^{-1} - \overline{r} \tag{3.35}$$

Và gửi các giá trị $\overline{m}, \overline{r}$ tới các thành viên U_i.

(3) Các thành viên U_i với $1 \leq i \leq \mathsf{NSIG}$ ký văn bản mù bằng cách tính:

$$\overline{s}_i = d_i(\overline{m} + \overline{r}) + (\mathfrak{V}_i \otimes k_i) \pmod{q} \tag{3.36}$$

Gửi giá trị này tới người cần ký.

(4) Người cần ký tính:

$$R_{e_i} = (x_{e_i}, y_{e_i}) = \overline{s}_i P - (\overline{m} + \overline{r})Q_i \tag{3.37}$$

Và kiểm tra $r_i = c(x_{e_i}) \pmod q$ và tính:

$$\overline{s} = \sum_{i=1}^{\mathsf{NSIG}} \overline{s}_i \tag{3.38}$$

$$s = \overline{s}a \pmod q \tag{3.39}$$

Chữ ký mù tập thể của văn bản m sẽ là $(r, s, \mathfrak{V})$.

3.3.3.3. Xác thực chữ ký mù tập thể

Người xác thực nhận được văn bản m' và chữ ký (r, s). Tính giá trị:

$$(x_e, y_e) = sP - (H(m) + r)Q \tag{3.40}$$

Kiểm tra điều kiện $r = c(x_e) \pmod q$ nếu thỏa mãn thì chữ ký hợp lệ.

$$sP - (H(m) + r)Q = R$$

Định lý 3.3.3 [Lược đồ ký tập thể mù đa thành phần] *Nếu $m' = m$ thì $sP - (H(m) + r)Q = R$.*

Chứng minh.

$$\begin{aligned}
R = a\overline{R} + bQ &= a\sum_{i=1}^{\mathsf{NSIG}} \overline{R}_i + bQ \\
&= a\sum_{i=1}^{\mathsf{NSIG}} \overline{R}_i + \left((\overline{m} + \overline{r})a - H(m) - r\right) Q \\
&= a\left(\sum_{i=1}^{\mathsf{NSIG}} \left((\mathfrak{V}_i \otimes k_i) + d_i(\overline{m} + \overline{r})\right)\right) P - \left(H(m) + r\right) Q \\
&= a\sum_{i=1}^{\mathsf{NSIG}} \overline{s}_i P - \left(H(m) + r\right) Q \\
&= a\overline{s}P - \left(H(m) + r\right) Q \\
&= sP - \left(H(m) + r\right) Q
\end{aligned}$$

□

3.3.3.4. Phân tích độ an toàn của lược đồ chữ ký mới và thảo luận

Phương pháp tấn công có thể là xây dựng thuật toán để giả mạo chữ ký (r, s). Giá trị r có thể dễ dàng tính được thông qua các khóa công khai của các thành viên, tuy nhiên để có được thành phần s, người tấn công bắt buộc phải tìm được cả $\overline{s}$ và a theo (3.39). Và đây là bài toán phân tích ra thừa số, là một bài toán khó. Hoặc xây người tấn công có thể xây dựng thuật toán mới để tính $\overline{s}$. Theo các công thức (3.38) và (3.36) để tính được $\overline{s}$ thì cần phải tìm được các giá trị $\overline{m}$, d_i, k_i và để tính được các giá trị này người tấn công buộc phải giải bài toán (3.36) phân tích ra thừa số.

3.4. Kết luận chương 3

Chương 3, Luận án cũng trình bày về đề xuất mô hình ký kết hợp giữa chữ ký tập thể đa thành phần với chữ ký mù. Cũng tương tự như ở mô hình kết hợp với chữ ký số ủy nhiệm NCS cũng mô tả dạng tấn công ACMA đối với mô hình kết hợp với chữ ký số mù. Để chứng minh cho tính đúng đắn của mô hình kết hợp giữa chữ ký số tập thể đa thành phần và chữ ký số mù, NCS đã đề xuất một lược đồ cụ thể ký tập thể đa thành phần với chữ ký mù. Các kết quả nghiên cứu trong chương này đã được công bố trong các công trình [CT6], [CT7], [CT8].

KẾT LUẬN

Với các nội dung nghiên cứu đã trình bày, Luận án đã đạt được các kết quả chính và đóng góp mới như sau:

Luận án đã đề xuất một khái niệm mới của chữ ký số tập thể là chữ ký số tập thể đa thành phần, ở đó mỗi thành viên có thể ký vào nhiều phần khác nhau của văn bản và một phần của văn bản có thể được ký bởi nhiều người. Sau khi đạt vấn đề, Luận án đã trình bày các định nghĩa chặt chẽ để làm nền tảng cho việc phát triển chữ ký số đa thành phần. Tiếp theo Luận án triển khai mô hình và khái niệm mới này cho 03 hệ mật tiêu biểu, sau đó Luận án trình bày sự kết hợp của mô hình, và khái niệm mới với mô hình chữ ký số khác là chữ ký số ủy nhiệm và chữ ký số mù.

Những đóng góp mới của đề tài luận án:

(1) Đề xuất mô hình ký tập thể hoàn toàn mới: Chữ ký số tập thể đa thành phần tổng quát. Mô hình này cho phép ứng dụng mềm dẻo và linh hoạt, đồng thời tổng quát hóa một số mô hình ký tập thể trước đây (mục 2.2 trang 13). Triển khải mô hình ký tập thể đa thành phần cho các hệ mật khác nhau:

- Xây dựng mới lược đồ ký tập thể đa thành phần dựa trên hệ mật đường cong elliptic.
- Xây dựng mới lược đồ ký tập thể đa thành phần dựa trên trên bài toàn logarithm rời rạc.
- Xây dựng mới lược đồ ký tập thể đa thành phần dựa trên trên cặp song tuyến tính .

(2) Đề xuất mới về mô hình ký kết hợp giữa chữ ký tập thể đa thành phần với

chữ ký ủy nhiệm: xây dựng định nghĩa tổng quát (mục 3.2.1 trang 23). Xây dựng mới lược đồ ký tập thể ủy nhiệm đa thành phần dựa trên hệ mật định danh (mục 3.2.3, trang 27).

(3) Đề xuất mới về mô hình ký kết hợp giữa chữ ký tập thể đa thành phần với chữ ký mù: xây dựng định nghĩa tổng quát (mục 3.3.1 trang 33). Xây dựng mới lược đồ ký tập thể mù đa thành phần dựa trên đường cong elliptic (mục 3.3.3, trang 36).

Kiến nghị về hướng nghiên cứu tiếp theo:

Về học thuật: Tiếp tục triển khai mô hình ký tập thể đa thành phần cho các hệ mật khác và kết hợp với các loại hình ký khác: ký tập thể đa thành phần có cấu trúc.... Nghiên cứu cài đặt các lược đồ chữ ký số tập thể cho hệ mật khác như Lattice, hệ mật sử dụng nhóm bện (Braid Group), tiếp tục nghiên cứu các dạng chữ ký số tập thể khác như Aggregate Multisignature, Proxy Multisignature, Undeniable Multisignature, Ring Multisignature...

Về thực tiễn: Xây dựng một số sản phẩm phần mềm hoàn chỉnh phục vụ cho việc tác quản lý, khởi tạo, cấp phát, xác thực chữ ký số tập thể đa thành phần. Xây dựng một số sản phẩm phần mềm ứng dụng chữ ký số trong công tác bầu cử điện tử (e-voting) thông qua mô hình chữ ký số mù.

CÁC CÔNG TRÌNH KHOA HỌC ĐÃ CÔNG BỐ

[CT1] Đặng Minh Tuấn, "Đánh giá lược đồ thuật toán chữ ký số tập thể Popescu và đễ xuất sửa đổi", *Tạp chí Nghiên cứu KH&CN Quân sự*, số 13 (06–2011), tr. 63–69, 2011.

[CT2] Đặng Minh Tuấn, "Lược đồ chữ ký số tập thể đa thành phần dựa trên bài toán Lô-ga-rít rời rạc", *Tạp chí Nghiên cứu KH&CN Quân sự*, Đặc san 11-2011, tr. 7–14, 2011.

[CT3] Dang Minh Tuan, "New Elliptic Curve Digital Multi-Signature Schemes for Multi-Section Messages", *2012 IEEE RIVF,Ho Chi Minh City, VietNam*, pp. 25–28, 2012.

[CT4] Đặng Minh Tuấn, "Lược đồ chữ ký số tập thể đa thành phần dựa trên cặp song tuyến tính", *Tạp chí Nghiên cứu KH&CN Quân sự*, Đặc san 5-2012, tr. 10–15, 2012.

[CT5] Đặng Minh Tuấn, "Chế tạo thiết bị VPN IPSec bằng phần cứng đầu tiên ở Việt Nam", *Tạp chí Công nghệ thông tin & Truyền thông*, pp. 41–45, 2014.

[CT6] Đặng Minh Tuấn, "Đề xuất mô hình chữ ký số tập thể đa thành phần tổng quát và kết hợp với một số mô hình khác", *Tạp chí Nghiên cứu KH&CN Quân sự*, số 45 (10–2016), tr. 91–98, 2016.

[CT7] Đặng Minh Tuấn, Nguyễn Ánh Việt, "Đề xuất chữ ký số tập thể ủy nhiệm đa thành phần dựa trên hệ mật định danh", *Kỷ yếu Hội thảo toàn quốc về Điện tử, Truyền thông và Công nghệ thông tin*, Hà Nội, 23/12/2016, tr. 3.12–3.17, 2016.

TÀI LIỆU THAM KHẢO

Tiếng Việt:

[1] Nguyễn Tiền Giang, Nguyễn Vĩnh Thái và Lưu Hồng Dũng (2014), "Lược đồ chữ ký số mù xây dựng trên bài toán khai căn", *Chuyên san Công nghệ thông tin và Truyền thông*, (5), tr. 102–114.

[2] Nguyễn Thị Huyền và cộng sự (2015), "Một số lược đồ chữ ký số mù mới dựa trên hai bài toán DLP và ECDLP", *Tạp Chí Khoa học và Công nghệ năm 2015*, 11 (5), tr. 3–11.

[3] Đặng Minh Tuấn (2014), "Chế tạo thiết bị VPN IPSec bằng phần cứng đầu tiên ở Việt Nam", *Tạp chí CNTT & TT*, (2), tr. 41–45.

Tiếng Anh:

[4] Laurent Berger et al. (2013), *Elliptic curves, Hilbert modular forms and Galois deformations*, Birkhauser.

[5] Craig Gentry and Zulfikar Ramzan (2006), "Identity-Based Aggregate Signatures", *Proceeding of Public Key Cryptography, LNCS 3958*, pp. 257–273.

[6] Darrel Hankerson, Julio Lopez Hernandez, and Alfred Menezes (2000), "Software Implementation of Elliptic Curve Cryptography over Binary Fields", *CHES2000*, 1965, pp. 243–267.

[7] Jonathan Katz (2010), *Digital signatures*, Springer.

[8] *MathType vs. Equation Editor*, URL: `http://www.dessci.com/en/products/mathtype/mt{\_}vs{\_}ee.htm`.

[9] Joseph H. Silverman and John T. Tate (2015), *Rational Points on Elliptic Curves - Second Edition*, Springer.

[10] Ying Sun et al. (2009), "Analysis and Improvement of a Proxy Blind Multi-signature Scheme without a Secure Channel", *Fifth International Conference on Information Assurance and Security*, pp. 661–664.

[11] Qin Wang and Zhenfu Cao (2007), "Identity based proxy multi-signature", *The Journal of Systems and Software*, 80, pp. 1023–1029.

PHỤ LỤC A. MỘT SỐ CÔNG THỨC TOÁN HỌC THƯỜNG GẶP

$$\tilde{f}(\omega) = \frac{1}{2\pi} \int_{-\infty}^{\infty} f(x) e^{-i\omega x}\, dx\,,$$

$$\dot{\vec{\omega}} = \vec{r} \times \vec{I}$$

$$\exp(i\theta) = \cos\theta + i\sin\theta\,, \quad \sinh(\log x) = \frac{1}{2}\left(x - \frac{1}{x}\right).$$

Một số hàm có dạng phức tạp:

$$\lim_{q\to\infty} \|f(x)\|_q = \max_x |f(x)|,$$

$$\begin{aligned} e^x &= \sum_{n=0}^{\infty} \frac{x^n}{n!} \quad \text{với } n! = \prod_{i=1}^{n} i\,, \\ \overline{U_\alpha} &= \bigcap_\alpha U_\alpha\,. \end{aligned}$$

Biểu thức có dạng rút gọn: $1/(1-x) = \sum_{n=0}^{\infty} x^n$ trong một dòng mà vẫn bảo đảm độ giãn dòng không thay đổi.

$$\begin{matrix} -2 & 1 & 0 & 0 & \cdots & 0 \\ 1 & -2 & 1 & 0 & \cdots & 0 \\ 0 & 1 & -2 & 1 & \cdots & 0 \\ 0 & 0 & 1 & -2 & \ddots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \ddots & 1 \\ 0 & 0 & 0 & \cdots & 1 & -2 \end{matrix}$$

P2

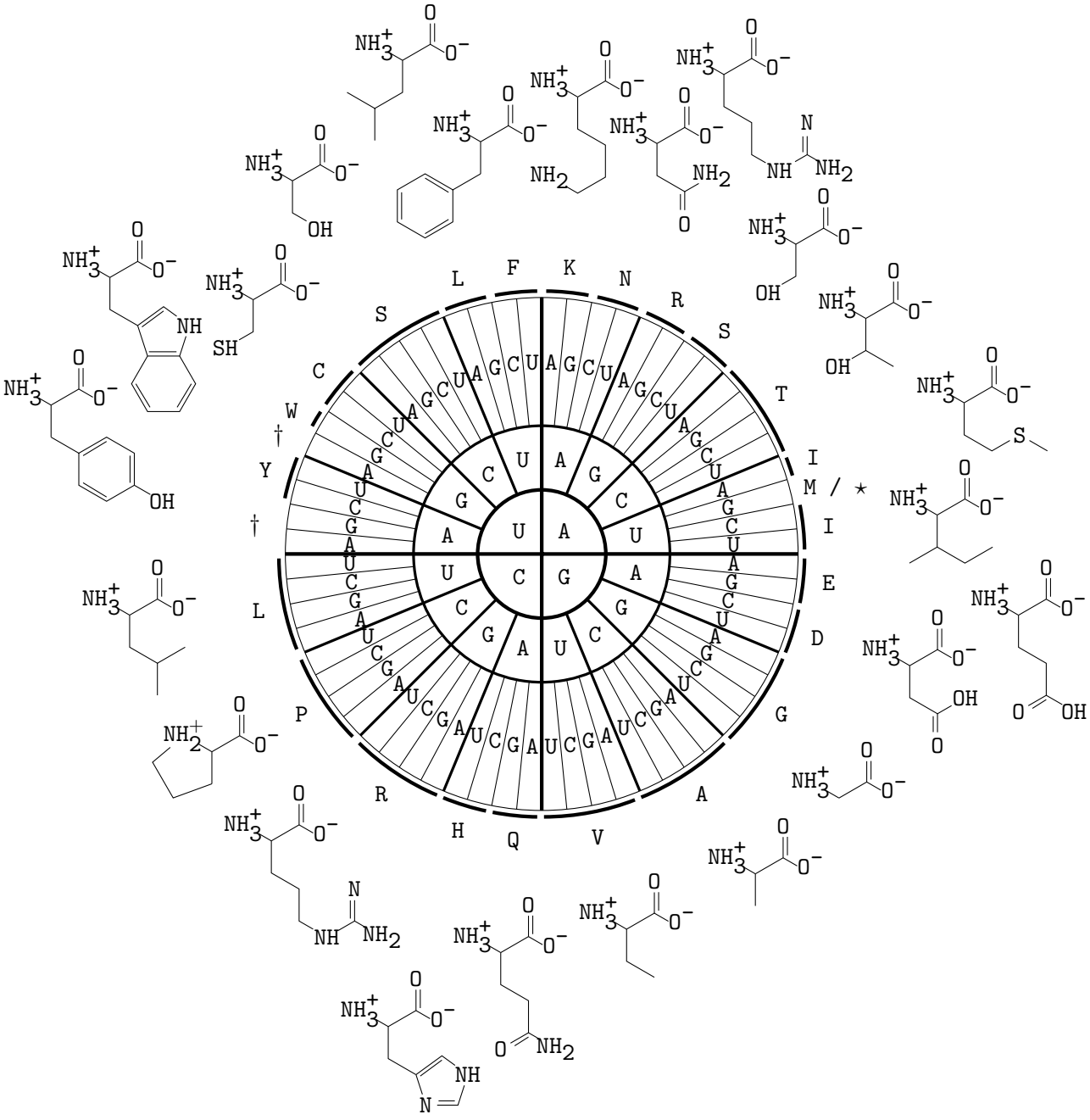
$$f(n) = \begin{cases} n/2 & \text{nếu } n \text{ chẵn} \\ -(n+1)/2 & \text{nếu } n \text{ lẻ} \end{cases}$$

$$A_{m,n} = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix}$$

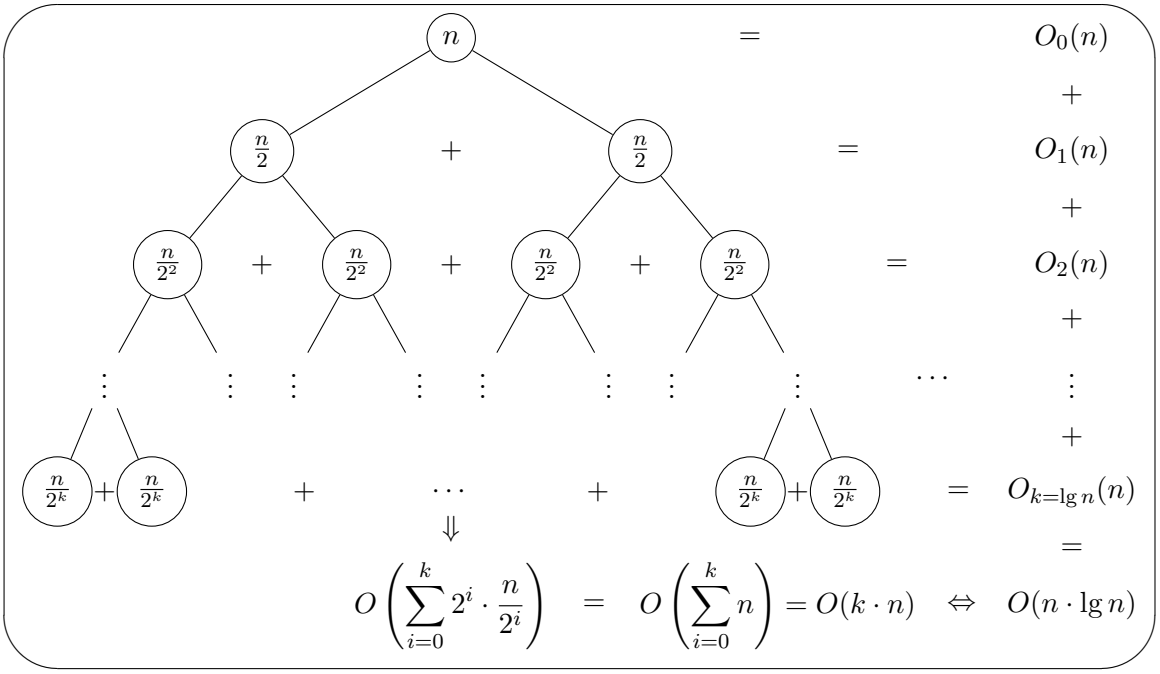
$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4}}}} \tag{A.1}$$

PHỤ LỤC B. MỘT SỐ VÍ DỤ VỀ LỆNH VẼ LATEX CỦA GÓI TIKZ

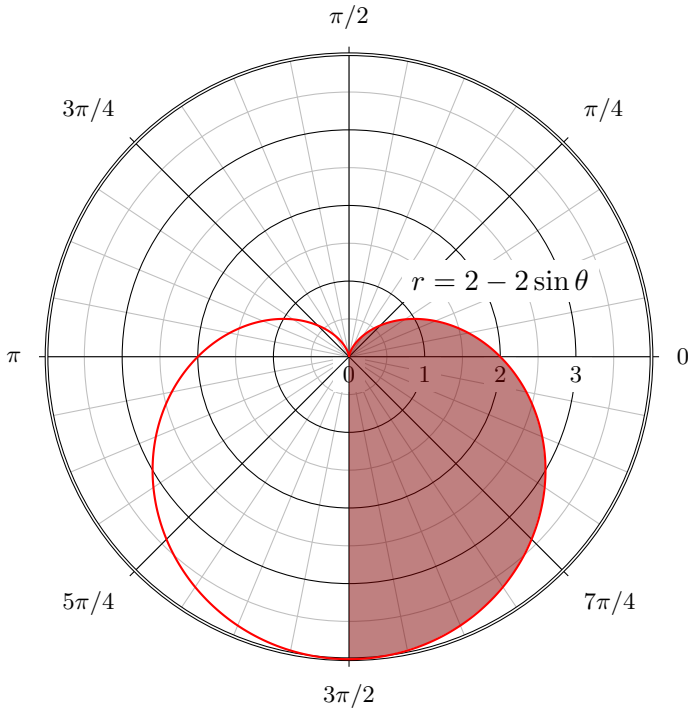
B.1. Ví dụ 1 - câu lệnh biểu diễn công thức hóa học



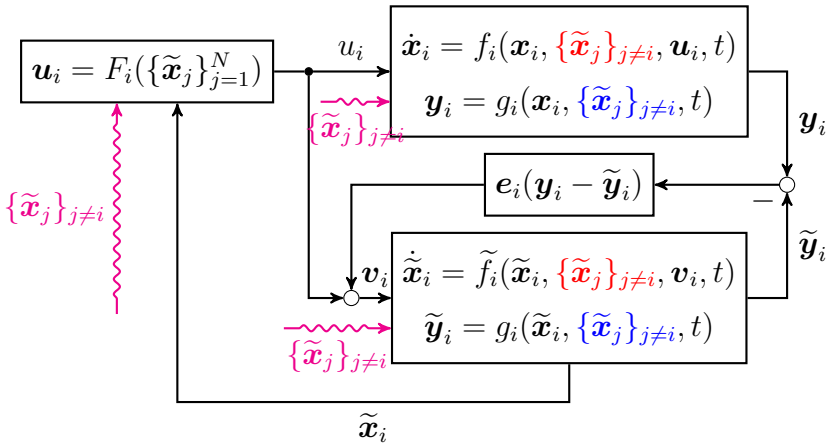
B.2. Ví dụ 2 - câu lệnh vẽ cây tìm kiếm đệ quy



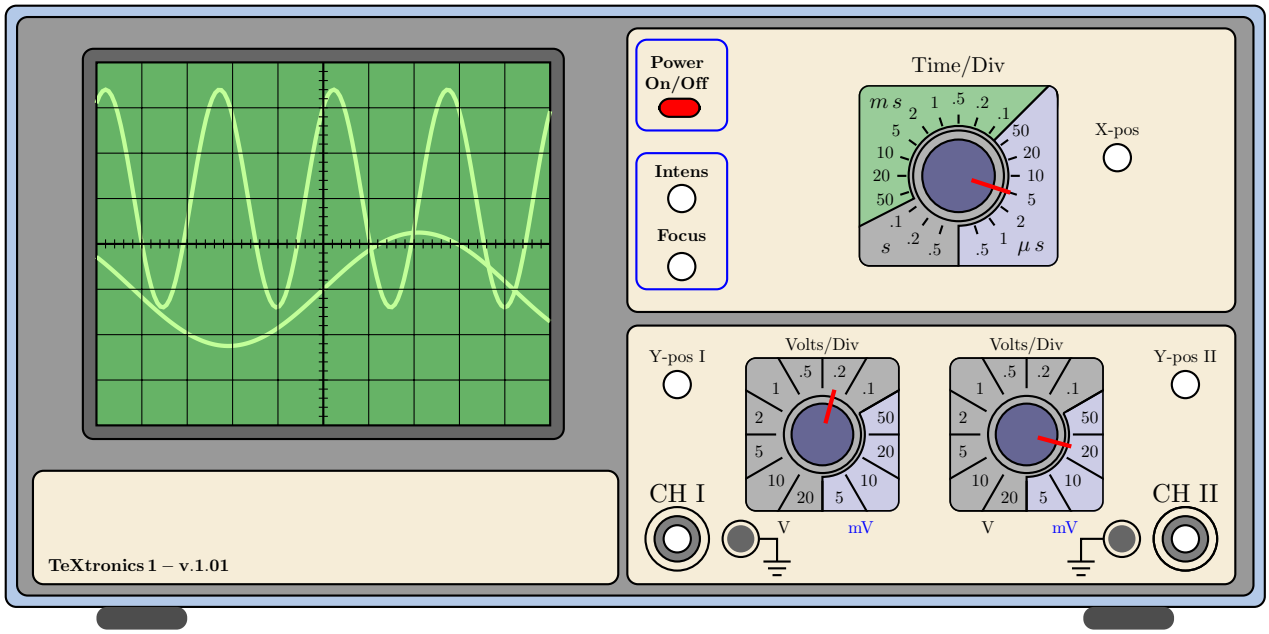
B.3. Ví dụ 3 - vẽ lưới và tọa độ cực



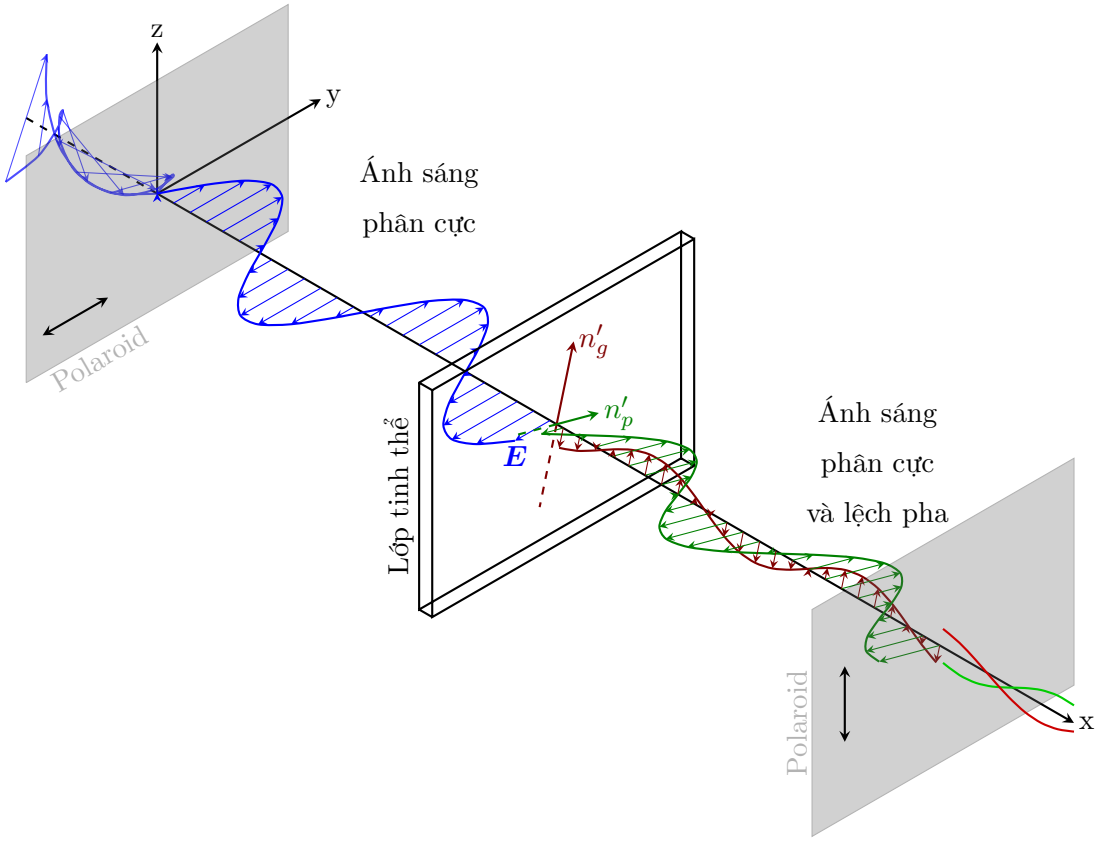
B.4. Ví dụ 4 - câu lệnh vẽ sơ đồ nguyên lý



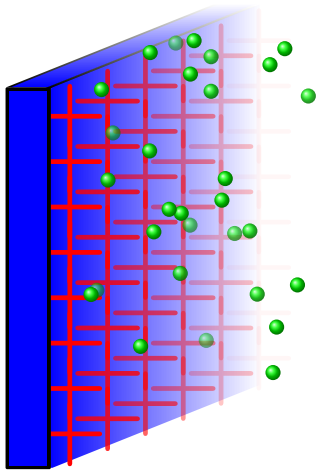
B.5. ví dụ 5 - câu lệnh vẽ máy Oscilloscope



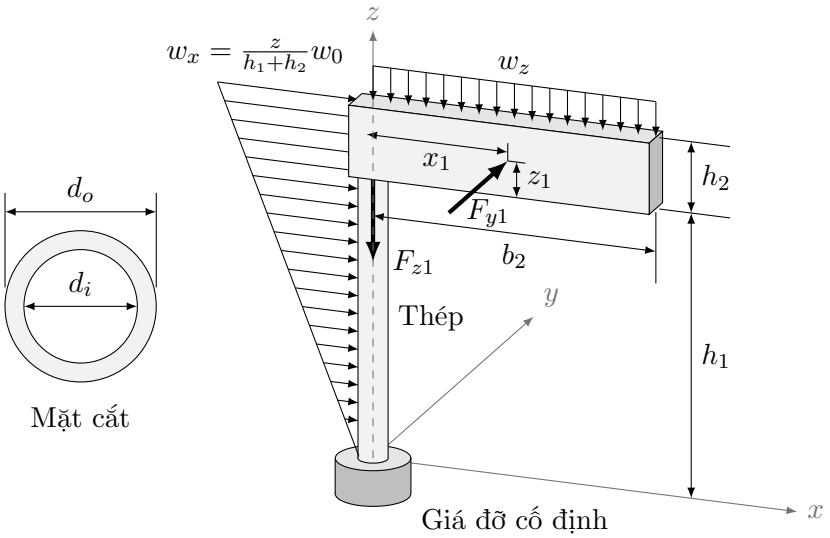
B.6. ví dụ 6 - câu lệnh thể hiện tính chất của ánh sáng



B.7. ví dụ 7 - câu lệnh vẽ Màng ion



B.8. ví dụ 8 - câu lệnh vẽ tải trọng



B.9. Ví dụ 9 - vẽ biểu đồ thời gian