

**TRƯỜNG ĐẠI HỌC AN GIANG
KHOA CÔNG NGHỆ THÔNG TIN**

THỰC TẬP CUỐI KHÓA NGÀNH CÔNG NGHỆ THÔNG TIN

**NGHIÊN CỨU VÀ CẢI TIẾN GIẢI THUẬT
CP-ABE DỰA TRÊN RELIC**

**VÕ PHÁT THÀNH
AN GIANG, 4-2025**

TRƯỜNG ĐẠI HỌC AN GIANG
KHOA CÔNG NGHỆ THÔNG TIN

THỰC TẬP CUỐI KHÓA NGÀNH CÔNG NGHỆ THÔNG TIN

NGHIÊN CỨU VÀ CẢI TIẾN GIẢI THUẬT
CP-ABE DỰA TRÊN RELIC

VÕ PHÁT THÀNH
DTH216157

GIẢNG VIÊN HƯỚNG DẪN: TS. LÊ HOÀNG ANH
AN GIANG, 4-2025

NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN

M-07

Đồng ý cho sinh viên Võ Phát Thành – DTH216157 báo cáo thực tập cuối khóa./.

Giảng viên hướng dẫn

(Ký và ghi rõ họ tên)

Lê Hoàng Anh

Nội dung nhận xét:

- **Đồng ý** hay **không đồng ý** cho sinh viên báo cáo TTCK; Nếu không đồng ý cần ghi rõ lý do.
- Kết quả đạt được so với yêu cầu;
- Ý kiến khác (nếu có)

LỊCH LÀM VIỆC

Họ và sinh viên: Võ Phát Thành

Cơ quan thực tập: Trường đại học An Giang

Họ và tên giảng viên hướng dẫn: TS.Lê Hoàng Anh

Thời gian thực tập: từ ngày 24 tháng 2 năm 2025 đến ngày 20 tháng 4 năm 2025

Tuần	Nội dung công việc được giao	Tự nhận xét về mức độ hoàn thành	Nhận xét của giảng viên hướng dẫn	Chữ ký của giảng viên hướng dẫn
01 Từ ngày 12/2 đến ngày 19/2	Lập kế hoạch, xác định các yêu cầu cơ bản của đề tài.	Hoàn thành		
02 Từ ngày 20/2 đến ngày 27/2	Tìm hiểu về giải thuật mã hóa CP-ABE	Hoàn thành		
03 Từ ngày 28/2 đến ngày 6/3	Tìm hiểu RELIC	Hoàn thành		
04 Từ ngày	Tiến hành cài đặt CP-ABE	Hoàn thành		

7/3 đến ngày 14/3				
05 Từ ngày 15/3 đến ngày 22/3	Cải tiến CP- ABE dựa trên RELIC	Hoàn thành 50%		
06 Từ ngày 23/3 đến ngày 30/3	Cải tiến CP- ABE dựa trên RELIC	Hoàn thành nhưng chưa đầy đủ		
07 Từ ngày 31/3 đến ngày 7/4	Sửa những lỗi chưa giải quyết được	Hoàn thành		
08 Từ ngày 8/4 đến ngày 15/4	Viết báo cáo hoàn thành các phần còn lại	Hoàn thành		

LỜI CẢM ƠN

Là một sinh viên đang theo đuổi đam mê trong lĩnh vực Công nghệ Thông tin tại Trường Đại học An Giang, Khoa Công nghệ Thông tin, em xin được gửi lời cảm ơn chân thành và sâu sắc nhất đến Ban giám hiệu Nhà trường cùng quý Thầy Cô trong Khoa, những người đã tận tình giảng dạy, hỗ trợ và tạo điều kiện thuận lợi cho em trong suốt 4 năm học tập và rèn luyện vừa qua. Những kiến thức và kỹ năng mà em có được hôm nay là nhờ vào sự tận tâm, tận tụy của Thầy Cô, những người luôn dành tâm huyết cho sự phát triển của sinh viên.

Đặc biệt, em xin gửi lời cảm ơn chân thành đến thầy Lê Hoàng Anh, người đã trực tiếp hướng dẫn em trong suốt quá trình thực hiện đề tài thực tập cuối khóa này. Thầy không chỉ cung cấp những kiến thức quý báu, định hướng rõ ràng trong nghiên cứu, mà còn luôn kiên nhẫn và động viên em mỗi khi gặp khó khăn. Nhờ sự giúp đỡ nhiệt tình và sự hướng dẫn tận tâm của thầy, em đã vượt qua những thử thách và hoàn thành tốt báo cáo thực tập của mình.

Bên cạnh đó, em cũng muốn bày tỏ lòng biết ơn sâu sắc đến gia đình và bạn bè, những người luôn bên cạnh, động viên, khích lệ và là chỗ dựa tinh thần vững chắc để em có thể yên tâm học tập, nghiên cứu và hoàn thành tốt nhiệm vụ của mình.

Mặc dù đã rất nỗ lực để hoàn thiện báo cáo với tất cả sự tận tâm huyết và khả năng hiện có, nhưng do những giới hạn nhất định về thời gian, kinh nghiệm cũng như kiến thức thực tiễn, bài báo cáo chắc chắn không tránh khỏi những thiếu sót. Em rất mong nhận được những góp ý chân thành từ quý Thầy Cô để em có thể tiếp tục hoàn thiện bản thân và đạt kết quả tốt hơn trong tương lai.

Em xin chân thành cảm ơn.

An Giang, ngày ... tháng ... năm 2025

Sinh viên thực hiện

Võ Phát Thành

MỤC LỤC

CHƯƠNG 1 GIỚI THIỆU CƠ QUAN THỰC TẬP VÀ ĐẶC VẤN ĐỀ	1
1.1 Giới thiệu cơ quan thực tập.....	1
1.1.1 Trường đại học An Giang.....	1
1.1.2 Khoa công nghệ thông tin	1
1.2 Đặt vấn đề	2
1.3 Mục tiêu nghiên cứu:	4
CHƯƠNG 2 TỔNG QUAN VÀ CƠ SỞ LÝ THUYẾT	6
2.1 Đặt vấn đề	6
2.2 Lịch sử giải quyết vấn đề	6
2.3 Phạm vi của đề tài	7
2.4 Phương pháp nghiên cứu và hướng giải quyết vấn đề	7
2.5 Cơ sở lý thuyết	8
2.5.1 Hệ thống CP-ABE.....	8
2.5.2 RELIC (Efficient Library for Cryptography).....	17
2.5.3 PBC (Pairing-Based Cryptography)	18
2.5.4 So sánh các hàm sử dụng trong PBC và RELIC	19
CHƯƠNG 3 PHÂN TÍCH THIẾT KẾ HỆ THỐNG	21
3.1 Tổng quan cài đặt.....	21
3.1.1 Khởi tạo (Setup)	21
3.1.2 Tạo khóa (Key Generation).....	22
3.1.3 Mã hóa (Encryption)	23
3.1.4 Giải mã (Decryption).....	23
3.2 Kết quả thực nghiệm	24
3.3 Ưu điểm, nhược điểm và hướng phát triển	29
3.3.1 Ưu điểm	29
3.3.2 Nhược điểm	30
3.3.3 Định hướng phát triển	30
TÀI LIỆU THAM KHẢO	32

DANH MỤC HÌNH ẢNH

Hình 1: Thực hiện setup.....	25
Hình 2: Thực hiện keygen	26
Hình 3: Các thuộc tính được thêm thành công	26
Hình 4: Thực hiện enc	27
Hình 5: Fill các policy và tính AES key	27
Hình 6: Thực hiện dec và check các thuộc tính.....	28
Hình 7: Lỗi AES-GCM authentication failed	28

DANH MỤC BẢNG

Bảng 1: So sánh hàm PBC và RELIC	20
--	----

TÓM TẮT

Thuật toán mã hóa dựa trên chính sách thuộc tính (CP-ABE - Ciphertext-Policy Attribute-Based Encryption) là một giải pháp mã hóa tiên tiến, giúp bảo mật dữ liệu và kiểm soát quyền truy cập hiệu quả trong môi trường điện toán phân tán hiện nay. Trước đây, CP-ABE chủ yếu được triển khai dựa trên thư viện PBC (Pairing-Based Cryptography), tuy nhiên, thư viện này tồn tại một số hạn chế về khả năng mở rộng và hiệu suất xử lý trên các nền tảng mới.

Xuất phát từ vấn đề trên, đề tài này tập trung nghiên cứu việc cải tiến và triển khai thuật toán CP-ABE dựa trên thư viện RELIC – một thư viện mã hóa hiện đại hơn, hỗ trợ tốt hơn cho các phép toán ghép cặp bilinear và tối ưu hóa hiệu năng trên nhiều nền tảng khác nhau. Nội dung chính của đề tài bao gồm nghiên cứu chuyên sâu về thuật toán CP-ABE, phân tích chi tiết những hạn chế khi sử dụng PBC, và từ đó đề xuất các phương pháp xây dựng, tối ưu mã nguồn CP-ABE dựa trên thư viện RELIC để cải thiện hiệu quả thực thi và tính tương thích trong phép pairing.

Kết quả thực nghiệm cho thấy, việc chuyển đổi sang RELIC không chỉ khắc phục được các hạn chế tồn tại trong PBC, mà còn cải thiện đáng kể hiệu suất và khả năng tương thích giữa các nhóm toán học $\mathbb{G}_1, \mathbb{G}_2$. Từ những cải tiến này, đề tài góp phần làm rõ tính khả thi và hiệu quả của việc sử dụng RELIC như là một giải pháp thay thế tiềm năng cho PBC trong việc triển khai mã hóa CP-ABE trong thực tế.

ABSTRACT

Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is an advanced encryption method that effectively ensures data security and access control in modern distributed computing environments. Traditionally, CP-ABE has been implemented using the Pairing-Based Cryptography (PBC) library, which has certain limitations in terms of scalability and performance on contemporary computing platforms.

Motivated by these limitations, this thesis focuses on improving and implementing the CP-ABE algorithm based on the RELIC cryptographic library—a more modern and versatile library with enhanced support for bilinear pairing operations and optimized performance across various platforms. The main contributions of this work include an in-depth study of the CP-ABE algorithm, detailed analysis of the limitations inherent in the PBC library and proposing optimized methods for implementing CP-ABE using RELIC to enhance computational efficiency and pairing compatibility.

Experimental results demonstrate that migrating from PBC to RELIC not only resolves previously encountered issues but also significantly enhances performance and compatibility across mathematical groups \mathbb{G}_1 and \mathbb{G}_2 . These improvements validate the feasibility and effectiveness of RELIC as a promising alternative to PBC in practical implementations of CP-ABE encryption schemes.

CHƯƠNG 1

GIỚI THIỆU CƠ QUAN THỰC TẬP VÀ ĐẶC VẤN ĐỀ

1.1 Giới thiệu cơ quan thực tập

1.1.1 Trường đại học An Giang

Trường Đại học An Giang (AGU) là một cơ sở giáo dục đại học công lập trực thuộc Đại học Quốc gia Thành phố Hồ Chí Minh. Tiền thân của trường là Trường Cao đẳng Sư phạm An Giang, sau đó được nâng cấp thành trường đại học vào năm 1999. Đến năm 2019, Trường Đại học An Giang chính thức trở thành một thành viên của hệ thống Đại học Quốc gia TP.HCM – một trong những hệ thống đại học lớn và uy tín hàng đầu cả nước.

Với sứ mệnh cung cấp nguồn nhân lực chất lượng cao, thực hiện nghiên cứu khoa học gắn liền với nhu cầu phát triển kinh tế - xã hội của khu vực Đồng bằng sông Cửu Long, trường hiện đào tạo trên 40 ngành bậc đại học thuộc nhiều lĩnh vực như: Nông nghiệp, Công nghệ, Kinh tế, Sư phạm, Văn hóa – Xã hội, và Khoa học cơ bản.

Trường có đội ngũ giảng viên giàu kinh nghiệm, cơ sở vật chất ngày càng hiện đại, cùng mạng lưới hợp tác quốc tế rộng khắp. Đặc biệt, trong những năm gần đây, Trường Đại học An Giang đã tích cực ứng dụng công nghệ thông tin vào hoạt động giảng dạy, nghiên cứu và quản lý, góp phần nâng cao chất lượng đào tạo và hội nhập quốc tế.

Với môi trường học tập thân thiện, năng động và hiện đại, Trường Đại học An Giang không chỉ là nơi đào tạo nguồn nhân lực có chuyên môn mà còn là trung tâm nghiên cứu, chuyển giao tri thức phục vụ phát triển bền vững cho khu vực.

1.1.2 Khoa công nghệ thông tin

Khoa Công nghệ Thông tin (CNTT) trực thuộc Trường Đại học An Giang – Đại học Quốc gia TP.HCM, là đơn vị đào tạo và nghiên cứu khoa học trong lĩnh vực công nghệ thông tin và truyền thông. Khoa có trụ sở đặt tại cơ sở chính của trường, với hệ thống phòng học, phòng máy tính và phòng thực hành hiện đại, đáp ứng tốt nhu cầu giảng dạy và học tập của sinh viên.

Khoa được thành lập với sứ mệnh đào tạo nguồn nhân lực có trình độ chuyên môn cao, kỹ năng thực hành vững vàng và phẩm chất đạo đức tốt, có khả năng thích ứng nhanh với sự phát triển của khoa học – công

nghệ và yêu cầu của thị trường lao động. Các chương trình đào tạo của khoa chú trọng tính ứng dụng thực tế, đồng thời cập nhật xu hướng công nghệ mới như trí tuệ nhân tạo, dữ liệu lớn, lập trình di động, và an toàn thông tin.

Hiện nay, Khoa Công nghệ Thông tin đào tạo ngành Công nghệ Thông tin ở các trình độ đại học và liên thông. Bên cạnh hoạt động đào tạo, khoa còn tích cực tham gia nghiên cứu khoa học, chuyển giao công nghệ và hợp tác quốc tế. Đội ngũ giảng viên của khoa bao gồm những thạc sĩ, tiến sĩ được đào tạo trong và ngoài nước, tâm huyết với nghề, luôn nỗ lực đổi mới phương pháp giảng dạy để nâng cao chất lượng đào tạo.

Trong quá trình học tập và thực tập, sinh viên ngành Công nghệ Thông tin được tạo điều kiện tham gia các hoạt động nghiên cứu, câu lạc bộ học thuật, các dự án phần mềm cũng như các chương trình thực tế tại doanh nghiệp. Đây là môi trường thuận lợi để sinh viên phát triển năng lực chuyên môn và kỹ năng mềm, sẵn sàng đáp ứng yêu cầu công việc sau khi tốt nghiệp.

1.2 Đặt vấn đề

Trong thời đại công nghệ số phát triển mạnh mẽ như hiện nay, thông tin và dữ liệu đang trở thành những tài sản có giá trị cao đối với cá nhân, tổ chức và doanh nghiệp, nhu cầu chia sẻ, xử lý và lưu trữ dữ liệu giữ vai trò trọng yếu trong các hệ thống hiện đại, đặc biệt là trong môi trường điện toán đám mây, hệ thống IoT, và các mô hình quản lý phân tán. Tuy nhiên, sự gia tăng khối lượng và tính chất nhạy cảm của dữ liệu đã đặt ra những thách thức lớn về bảo mật và quyền riêng tư, do đó yêu cầu về bảo mật thông tin ngày càng cấp thiết. Các phương pháp mã hóa truyền thống tuy vẫn còn giá trị nhất định, nhưng dần bộc lộ nhiều hạn chế trong việc quản lý quyền truy cập phức tạp, đặc biệt là khi phải đáp ứng các yêu cầu linh hoạt theo thuộc tính người dùng và vừa mã hóa vừa chia sẻ với nhiều người.

Trong nhiều tình huống thực tế như quản lý hồ sơ y tế, chia sẻ dữ liệu giáo dục, trao đổi thông tin trong các tổ chức hành chính hay vận hành thiết bị thông minh, yêu cầu về kiểm soát truy cập không thể được đáp ứng hiệu quả chỉ với các hệ thống mã hóa truyền thống, vốn chủ yếu dựa trên danh tính người dùng. Thay vào đó, cần có một cơ chế cho phép mô tả và thực thi chính sách truy cập chi tiết hơn, dựa trên tập hợp các thuộc tính đặc trưng cho người dùng hoặc đối tượng truy cập.

Trong bối cảnh đó, mã hóa dựa trên chính sách thuộc tính CP-ABE (Ciphertext-Policy Attribute-Based Encryption), được Bethencourt, Sahai

và Waters đề xuất vào năm 2007, đã mở ra một hướng tiếp cận hoàn toàn mới trong lĩnh vực kiểm soát truy cập dữ liệu và được xem là một giải pháp mã hóa hiện đại, mang tính linh hoạt cao trong kiểm soát truy cập. CP-ABE cho phép dữ liệu được mã hóa theo các chính sách thuộc tính, từ đó chỉ những người dùng có thuộc tính phù hợp mới có thể giải mã thông tin. Đây là một bước tiến quan trọng nhằm nâng cao khả năng bảo mật và kiểm soát truy cập trong các hệ thống chia sẻ thông tin phức tạp.

Mặc dù CP-ABE mang lại nhiều lợi ích về mặt chức năng, việc triển khai thuật toán này trong thực tế lại gặp không ít khó khăn, đặc biệt liên quan đến yêu cầu tính toán cao của các phép toán ghép cặp bilinear trên các nhóm elliptic curve. Các phiên bản triển khai đầu tiên của CP-ABE thường dựa trên thư viện Pairing-Based Cryptography (PBC), tuy nhiên, PBC đã bộc lộ nhiều hạn chế về hiệu suất, mức độ bảo mật (chỉ đạt 80-bit), và khả năng tương thích với các hệ thống hiện đại. Đây là một rào cản lớn đối với việc ứng dụng rộng rãi CP-ABE trong thực tiễn.

Đáng chú ý là các nghiên cứu trước đây thường chỉ tập trung vào thuật toán CP-ABE mà ít đi sâu vào đánh giá nền tảng thực thi nhằm thay thế PBC. Trong bối cảnh đó, thư viện RELIC (Efficient Library for Cryptography) đã được phát triển như một giải pháp thay thế tiềm năng. RELIC không chỉ hỗ trợ đa dạng các nhóm toán học như \mathbb{G}_1 , \mathbb{G}_2 và \mathbb{G}_T , mà còn cho phép người dùng cấu hình bảo mật ở mức cao hơn, với hỗ trợ các đường cong hiện đại như BN và BLS. Đặc biệt, RELIC hỗ trợ pairing bất đối xứng (asymmetric pairing), một tính năng mở ra cơ hội tối ưu hóa thuật toán CP-ABE theo những cách mà các thư viện trước đó không thực hiện được.

Chính vì vậy, việc nghiên cứu và triển khai thuật toán CP-ABE trên nền thư viện RELIC thay vì PBC là một định hướng mang tính thực tiễn và cấp thiết. Đề tài không chỉ nhằm mục tiêu khắc phục các nhược điểm của các thư viện cũ như PBC, việc ứng dụng RELIC còn hứa hẹn nâng cao hiệu suất xử lý, mở rộng khả năng tích hợp và đảm bảo an toàn ở mức bảo mật cao hơn cho CP-ABE trong các môi trường thực tế.

Với nền tảng lý luận từ CP-ABE và thực trạng hạn chế của PBC, kết hợp cùng tiềm năng kỹ thuật của RELIC, đề tài được định hướng triển khai theo các nội dung chính sau:

- Khảo sát, phân tích thuật toán CP-ABE truyền thống; đánh giá các điểm mạnh, yếu của PBC trong quá trình triển khai;

- Nghiên cứu RELIC và tái thiết lại thuật toán CP-ABE trên nền RELIC;
- Thực nghiệm đánh giá, so sánh hiệu năng giữa hai nền tảng và đưa ra hướng ứng dụng thực tiễn.

Toàn bộ nội dung này sẽ được trình bày rõ ràng, mạch lạc và có dẫn chứng định lượng trong các chương tiếp theo.

Về mặt lý luận, đề tài bổ sung thêm một hướng tiếp cận mới cho việc triển khai CP-ABE, đồng thời cung cấp cái nhìn sâu sắc hơn về vai trò của nền tảng thư viện mật mã trong hiệu năng tổng thể của hệ thống. Về mặt thực tiễn, nếu triển khai thành công, đề tài sẽ mang lại một giải pháp triển khai CP-ABE hiệu quả hơn, giúp nâng cao độ tin cậy và khả năng ứng dụng trong các hệ thống thực tế, từ doanh nghiệp đến các hệ thống công nghệ thông tin chính phủ.

1.3 Mục tiêu nghiên cứu:

Xuất phát từ các vấn đề đã được phân tích ở phần trên, mục tiêu chính của đề tài là nghiên cứu sâu về giải thuật CP-ABE và cải tiến việc triển khai thuật toán này trên nền tảng thư viện RELIC. Cụ thể, nghiên cứu không chỉ dừng lại ở việc tái hiện thuật toán gốc mà còn bao gồm quá trình điều chỉnh, tối ưu hóa các thành phần trong thuật toán để phù hợp với đặc điểm cấu trúc và các hàm thư viện mà RELIC cung cấp.

Trước hết, đề tài hướng đến việc phân tích chi tiết các thành phần của CP-ABE, bao gồm các giai đoạn khởi tạo hệ thống (Setup), sinh khóa (KeyGen), mã hóa (Encrypt) và giải mã (Decrypt). Tiếp đó, nghiên cứu sẽ tập trung tìm hiểu cách thức mà RELIC tổ chức các nhóm toán học G_1 , G_2 , GT và xử lý các phép toán như pairing, hash-to-curve, nhân, lũy thừa,... nhằm xác định khả năng kết hợp hiệu quả giữa CP-ABE và RELIC.

Tiếp theo, đề tài tiến hành triển khai thuật toán CP-ABE trên thư viện RELIC bằng cách tái hiện đầy đủ các bước xử lý, thay thế toàn bộ các phép toán ghép cặp và nhóm toán học từ PBC sang RELIC. Trong quá trình này, các phép tối ưu sẽ được áp dụng để khai thác tối đa hiệu suất của RELIC, đồng thời đảm bảo tính tương thích với logic thuật toán CP-ABE gốc.

Sau khi hoàn tất triển khai, hệ thống CP-ABE cải tiến này sẽ được kiểm thử và đánh giá hiệu năng dựa trên các tiêu chí cụ thể. Các chỉ số được theo dõi bao gồm thời gian mã hóa, thời gian giải mã, và khả năng mở rộng hệ thống khi tăng số lượng thuộc tính hoặc người dùng.

Cuối cùng, đề tài hướng đến việc đưa ra đánh giá tổng quan về tính khả thi khi sử dụng RELIC như một nền tảng thay thế PBC trong việc xây dựng các hệ thống mã hóa hiện đại, đồng thời đề xuất các khuyến nghị thực tiễn cho các nhà phát triển khi lựa chọn thư viện mật mã cho các hệ thống bảo mật dữ liệu dựa trên thuộc tính.

CHƯƠNG 2

TỔNG QUAN VÀ CƠ SỞ LÝ THUYẾT

2.1 Đặt vấn đề

Trong xu hướng phát triển hỗn hợp của các hệ thống phân tán và điện toán đám mây, bảo mật truy cập dữ liệu trở thành bài toán then chốt. Những yêu cầu thực tế ngày càng gia tăng trong việc chia sẻ dữ liệu nhạy cảm như hồ sơ bệnh án trong ngành y tế, kết quả học tập trong lĩnh vực giáo dục, hay dữ liệu cảm biến trong các hệ thống IoT đã khiến việc kiểm soát truy cập trở nên phức tạp hơn. Trong khi các phương pháp mã hóa truyền thống thường gắn với việc mã hóa dữ liệu cho một đối tượng cụ thể, chúng lại bộc lộ nhiều hạn chế trong những bối cảnh linh hoạt và không định danh trước. Câu hỏi đặt ra là: liệu có thể thiết lập các chính sách truy cập mã hóa dựa trên thuộc tính người dùng mà không cần mô tả đối tượng nhận cụ thể hay không?

Thuật toán Ciphertext-Policy Attribute-Based Encryption (CP-ABE) ra đời và giải quyết thành công vấn đề trên bằng cách cho phép người mã hóa dữ liệu được quyền định ai là người được truy cập, thông qua việc định nghĩa các chính sách truy cập biểu diễn dưới dạng cây truy cập được xây dựng từ các thuộc tính. CP-ABE đã mở ra một hướng tiếp cận mới cho truy cập dữ liệu bảo mật, thay thế cho mô hình truy cập truyền thống dựa trên danh tính [1].

Tuy nhiên, việc triển khai CP-ABE trong thực tế đòi hỏi nền tảng toán học mạnh và hiệu quả để thực hiện các phép toán ghép cặp bilinear. Trong bối cảnh đó, thư viện RELIC nổi bật như một nền tảng hiện đại, hỗ trợ đầy đủ các nhóm toán học cần thiết (G_1 , G_2 , GT), đồng thời cung cấp hiệu năng cao và tính linh hoạt khi tích hợp vào các hệ thống thực tế. Không giống như các thư viện truyền thống như PBC, RELIC cho phép tối ưu sâu các phép toán nền tảng, phù hợp với nhu cầu cải tiến hiệu suất của các thuật toán mã hóa như CP-ABE. Do vậy, việc lựa chọn RELIC làm nền tảng để cải tiến và triển khai lại CP-ABE không chỉ xuất phát từ nhu cầu kỹ thuật, mà còn phản ánh một định hướng nghiên cứu thực tiễn, phù hợp với xu thế hiện nay trong lĩnh vực bảo mật dữ liệu.

2.2 Lịch sử giải quyết vấn đề

Khái niệm Attribute-Based Encryption (ABE) được đề xuất lần đầu trong công trình của Sahai và Waters vào năm 2005, với mô hình ban đầu là Fuzzy IBE [2]. Sau đó, Goyal et al. vào năm 2006 đã mở rộng ý tưởng này và phát

triển mô hình Key-Policy ABE (KP-ABE), cho phép thiết kế các chính sách truy cập dưới dạng cây ngưỡng [3]. Tuy nhiên, trong KP-ABE, quyền kiểm soát truy cập lại thuộc về bên cấp khóa, thay vì người mã hóa, dẫn đến tính linh hoạt bị hạn chế.

Để khắc phục điều đó, năm 2007, Bethencourt, Sahai và Waters đã giới thiệu mô hình Ciphertext-Policy ABE (CP-ABE), trong đó người mã hóa giữ vai trò chủ động trong việc xác định chính sách truy cập. Công trình của họ đã thiết lập nền tảng vững chắc cho các hệ thống kiểm soát truy cập mã hóa hiện đại, cho phép biểu diễn chính sách linh hoạt và chống lại tấn công liên kết khóa [1].

Tuy nhiên, trong thực tế triển khai, các hệ thống CP-ABE thường được xây dựng dựa trên thư viện PBC (Pairing-Based Cryptography), vốn có những giới hạn về hiệu suất xử lý, khả năng mở rộng, cũng như tính tương thích với các kiến trúc phần cứng hiện đại [4]. Các công trình như cpabe-toolkit đã cung cấp những bản cài đặt mẫu nhưng vẫn còn phụ thuộc sâu vào thư viện PBC [1].

Trong khi đó, thư viện RELIC, ra đời sau và được thiết kế tối ưu hơn cho các phép toán pairing cũng như hỗ trợ linh hoạt nhiều loại nhóm (G_1 , G_2 , GT), đã được ứng dụng trong nhiều hệ mật mã hiện đại nhưng chưa có nhiều nghiên cứu áp dụng nó cho CP-ABE. Do đó, việc tìm hiểu và triển khai CP-ABE trên nền RELIC thay thế cho PBC là một hướng nghiên cứu mới, có tiềm năng ứng dụng cao và góp phần hoàn thiện tính thực tiễn của CP-ABE.

2.3 Phạm vi của đề tài

Đề tài tập trung nghiên cứu và cải tiến giải thuật mã hóa dựa trên chính sách thuộc tính (CP-ABE) với mục tiêu triển khai hiệu quả trên nền tảng thư viện mật mã RELIC.

2.4 Phương pháp nghiên cứu và hướng giải quyết vấn đề

Về lý thuyết: tiến hành tổng hợp, phân tích các nghiên cứu liên quan, đặc biệt là CP-ABE do Bethencourt et al. (2007) đề xuất [1]. Từ đó làm rõ nguyên lý hoạt động, các bước thực hiện, đặc điểm của cấu trúc cây truy cập và yêu cầu toán học đối với các phép ghép cặp bilinear. Bên cạnh đó đề tài cũng nghiên cứu chi tiết các đặc trưng của thư viện RELIC, bao gồm các hỗ trợ nhóm G_1 , G_2 , GT và khả năng tùy biến đường cong elliptic từ đó xác định các cải tiến phù hợp cho CP-ABE.

Về thực nghiệm: triển khai một phiên bản cải tiến của CP-ABE trên nền thư viện RELIC. Mã nguồn được xây dựng để phản ánh đầy đủ chức năng của

thuật toán gốc, đồng thời khai thác triệt để khả năng tối ưu hiệu suất của RELIC. Hệ thống được kiểm thử với nhiều bộ thuộc tính và chính sách truy cập khác nhau nhằm đánh giá khả năng đáp ứng trong thực tế.

2.5 Cơ sở lý thuyết

2.5.1 Hệ thống CP-ABE

Mô hình Ciphertext-Policy Attribute-Based Encryption (CP-ABE), được giới thiệu bởi Bethencourt, Sahai và Waters vào năm 2007 [1], là một hệ thống mã hóa hiện đại cho phép người nắm giữ dữ liệu kiểm soát quyền truy cập dựa trên các thuộc tính của người dùng. Trong CP-ABE, khóa bí mật của mỗi người dùng được liên kết với một tập hợp các thuộc tính. Bản mã (ciphertext) được gắn với một chính sách truy cập, thường biểu diễn dưới dạng cây truy cập, xác định tập hợp thuộc tính nào thì có quyền giải mã. Việc giải mã chỉ thành công khi và chỉ khi tập thuộc tính của người dùng thỏa mãn chính sách truy cập đã gắn với bản mã.

Trong mục này, em sẽ trình bày chi tiết các thành phần cốt lõi tạo nên hệ thống CP-ABE. Nội dung sẽ được chia thành bốn phần chính: khái niệm thuộc tính và chính sách truy cập – là hai yếu tố trung tâm xác định quyền giải mã; bốn thuật toán cơ bản của hệ thống bao gồm khởi tạo, sinh khóa, mã hóa và giải mã; nền tảng toán học của hệ thống, bao gồm phép ghép cặp bilinear và các nhóm elliptic; và cuối cùng hướng triển khai hệ thống trong thực tế. Cách trình bày theo từng tiểu mục sẽ giúp người đọc dễ dàng nắm bắt toàn diện nguyên lý và cấu trúc vận hành của CP-ABE.

2.5.1.1 Thuộc tính và chính sách truy cập

Trong hệ thống CP-ABE, hai thành phần then chốt đóng vai trò nền tảng là "thuộc tính" và "chính sách truy cập". Đây là hai yếu tố tạo nên sự linh hoạt và hiệu quả trong kiểm soát quyền truy cập dữ liệu, cho phép người nắm giữ dữ liệu thiết lập các điều kiện truy cập chi tiết và có thể mở rộng theo nhu cầu thực tế.

Thuộc tính (Attribute) là các đặc điểm hoặc tính chất mô tả người dùng hoặc dữ liệu. Chúng có thể là các chuỗi ký tự tự do, không có ràng buộc định dạng cụ thể. Trong thực tế, các thuộc tính thường phản ánh thông tin hành chính hoặc chuyên môn như "bộ môn CNTT", "giới tính Nam", hoặc "An Giang". Một người dùng có thể có nhiều thuộc tính, và mỗi thuộc tính này sẽ được hệ thống ánh xạ thành các phần tử trong nhóm toán học để phục vụ cho quá trình sinh khóa bí mật. Thuộc tính đóng vai trò quyết định trong việc cấp phát khóa bí

mật cho người dùng, mỗi người dùng trong hệ thống sẽ được cấp một khóa bí mật tương ứng với tập hợp thuộc tính mà họ sở hữu, chính các thuộc tính này sẽ được hệ thống sử dụng để đối chiếu với chính sách truy cập trong bản mã nhằm quyết định ai có thể giải mã dữ liệu.

Chính sách truy cập (Access Policy/Access Structure) là điều kiện logic được định nghĩa bởi người mã hóa để quy định những tập thuộc tính nào thì được phép giải mã dữ liệu. Chính sách truy cập được nhúng vào bản mã tại thời điểm mã hóa và có thể biểu diễn dưới nhiều hình thức. Phổ biến nhất là cấu trúc cây truy cập (Access tree) với các cổng ngưỡng (Threshold Gates) và thường được biểu diễn dưới dạng cây truy cập với các cổng ngưỡng. Các cổng AND (n -of- n threshold gates) và OR (1-of- n threshold gates) có thể được xây dựng từ cổng ngưỡng, trong đó các lá là thuộc tính và các nút trong là các cổng logic như AND, OR hoặc các cổng ngưỡng (threshold gate)[5]. Ví dụ, chính sách "CNTT và Nam và (An Giang hoặc Cần Thơ)" có thể được biểu diễn bằng một cây gồm nút gốc là AND, có ba nhánh con tương ứng với các điều kiện logic.

Ngoài cây truy cập, chính sách còn có thể được biểu diễn bằng biểu thức boolean (biểu thức logic) kết hợp các thuộc tính bằng các phép AND, OR, NOT, chẳng hạn như "(CNTT AND Nam) AND (An Giang OR Cần Thơ)", giúp diễn đạt các điều kiện phức tạp một cách linh hoạt. Một hướng biểu diễn chính sách khác là thông qua ma trận chia sẻ bí mật tuyến tính (LSSS), trong đó chính sách được mã hóa dưới dạng ma trận M kết hợp với một hàm ánh xạ π gán mỗi hàng trong ma trận cho một thuộc tính cụ thể. Phương pháp này được sử dụng rộng rãi trong các hệ thống ABE hiện đại vì khả năng biểu diễn chính sách phức tạp và tích hợp với các thuật toán toán học hiệu quả.

Mối quan hệ giữa thuộc tính và chính sách truy cập là mối quan hệ giữa dữ liệu đầu vào (thuộc tính của người dùng) và điều kiện xác thực (chính sách trong bản mã). Việc giải mã chỉ thành công nếu và chỉ nếu tập hợp thuộc tính của người dùng thỏa mãn hoàn toàn chính sách truy cập đã định. Đây chính là cơ chế kiểm soát truy cập chủ động, an toàn và linh hoạt mà CP-ABE cung cấp.

2.5.1.2 Nền tảng toán học

Nền tảng toán học của hệ thống CP-ABE dựa trên các cấu trúc then chốt bao gồm đường cong elliptic, nhóm cyclic hữu hạn, phép ghép cặp bilinear và các giả định mật mã học. Đây là những yếu tố có mối

liên hệ chặt chẽ, đóng vai trò trung tâm trong việc xây dựng và thực thi các phép toán mật mã một cách an toàn và hiệu quả.

Đường cong elliptic (Elliptic Curves):

Đường cong elliptic là một loại đường cong đại số được định nghĩa trên một trường hữu hạn, \mathbb{F}_{p^m} với p là số nguyên tố và m là số nguyên dương. Dạng rút gọn thường dùng trong mật mã học là dạng Weierstrass ngắn:

$$E: y^2 = x^3 + ax + b \quad (1)$$

Trong đó, $a, b \in \mathbb{F}_{p^m}$, thỏa điều kiện $4a^3 + 27b^2 \neq 0$ (2), để đảm bảo đường cong không kỳ dị (non-singular), tức không có điểm uốn hoặc giao nhau. Tập hợp các điểm (x, y) thỏa phương trình trên, cùng với điểm ở vô cực, tạo thành một nhóm Abel giao hoán dưới phép cộng điểm. Các phép toán như cộng hai điểm, nhân đôi điểm hoặc nhân vô hướng (một điểm với một số nguyên) là các thao tác nền tảng cho việc thực hiện mã hóa và sinh khóa.

Gọi $P = (x_1, y_1)$ và $Q = (x_2, y_2)$ là hai điểm khác nhau thuộc tập điểm trên E , một số phép toán quan trọng trên đường cong elliptic bao gồm:

Phép cộng điểm trên đường cong elliptic ECA (Elliptic Curve Addition) cho phép kết hợp hai điểm P và Q trên đường cong elliptic để tạo ra một điểm thứ ba ký hiệu là R . Phép toán này là nền tảng cho các phép toán phức tạp hơn trên đường cong elliptic và có công thức như sau [6]: nếu $P \neq Q$ và $x_1 \neq x_2$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \quad (3)$$

$$\begin{cases} x_R = \lambda^2 - x_1 - x_2 \\ y_R = \lambda(x_1 - x_R) - y_1 \end{cases} \quad (4)$$

Phép nhân đôi điểm ECD (Elliptic Curve Doubling) là trường hợp đặc biệt của phép cộng điểm khi $P = Q$. Về cơ bản nhân đôi điểm P tương đương với việc cộng điểm đó với chính nó $(P + P) = 2P$ và có công thức tính như sau[6]:

$$\lambda = \frac{3x^2 + a}{2y} \quad (5)$$

$$\begin{cases} x_R = \lambda^2 - 2x \\ y_R = \lambda(x - x_R) - y \end{cases} \quad (6)$$

Phép nhân vô hướng trên đường cong elliptic SCM (Elliptic curve Scalar Multiplication) là việc lặp đi lặp lại phép cộng một điểm P trên đường cong elliptic với chính nó một số nguyên lần s [6]:

$$R = sP = \underbrace{P + P + \dots + P}_{s-1 \text{ lần cộng}} \quad (7)$$

SCM đóng vai trò then chốt trong nhiều thuật toán mật mã dựa trên đường cong elliptic, bao gồm cả ABE, đặc biệt trong quá trình sinh khóa bí mật và khóa công khai.

Đường cong elliptic là nền tảng để xây dựng các nhóm toán học mạnh trong mật mã học nhờ vào tính chất khó giải quyết của bài toán logarithm rời rạc trên đó (Elliptic Curve Discrete Logarithm Problem - ECDLP). Cụ thể trong nhóm cộng các điểm trên đường cong elliptic, việc tính toán $R = sP$ với $P \in E(\mathbb{F}_p)$ rất đơn giản nhờ vào thuật toán như double-and-add. Tuy nhiên việc tìm lại s từ P và R là cực kì khó. Theo các tài liệu như [7] và [8], an toàn của các hệ mật mã dựa trên ghép cặp như CP-ABE phụ thuộc trực tiếp vào độ khó của việc giải hai bài toán này. Ngoài ra, độ khó cũng tỷ lệ thuận với độ dài bit của bậc nhóm r ; ví dụ, ELiPS-based CP-ABE sử dụng nhóm có bậc 308 bit trong khi PBC-based chỉ dùng 160 bit, cho thấy mức độ an toàn của hệ ELiPS cao hơn. Tính chất này được tận dụng trong việc xây dựng khóa và kiểm tra chính sách trong CP-ABE.

Nhóm cyclic hữu hạn (Finite Cyclic Groups):

Từ các điểm trên đường cong elliptic, ta xây dựng các nhóm con có bậc nguyên tố lớn, gọi là nhóm cyclic hữu hạn. Nhóm cyclic (Cyclic Groups) là các nhóm mà mọi phần tử trong nhóm đều có thể được tạo ra bằng cách lấy lũy thừa của một phần tử duy nhất được gọi là phần tử sinh. Cụ thể, nếu g là phần tử sinh và r là bậc của nhóm, thì mọi phần tử u trong nhóm đều có dạng:

$$u = g^x, \text{ với } x \in \mathbb{Z}_r.$$

Theo định lý Hasse, số điểm trên đường cong elliptic trên trường là [6]:

$$\#E(\mathbb{F}_p) = p + 1 - t, \quad (8)$$

$$\text{với } |t| \leq 2\sqrt{p}$$

Với một số nguyên tố r là ước của $\#E(\mathbb{F}_p)$, ta xét bậc nhúng k , là số nguyên nhỏ nhất sao cho $r|(p^k - 1)$ [6].

Khi $k > 1$, ta cần mở rộng trường sang \mathbb{F}_{p^k} để các điểm trong $E[r]$ được định nghĩa đầy đủ. Điều này đặc biệt quan trọng để đảm bảo phép pairing tồn tại và tính toán được trong hệ thống CP-ABE.

Trong các hệ mã hóa dựa trên thuộc tính (ABE), đặc biệt là CP-ABE, thường sử dụng các nhóm cyclic có bậc nguyên tố lớn (prime order) và thường ký hiệu là r hoặc p để đảm bảo độ khó trong việc giải bài toán logarit rời rạc [1]. Các nhóm $\mathbb{G}_1, \mathbb{G}_2$ trong CP-ABE thường là nhóm con có bậc r của tập điểm trên đường cong elliptic. Chúng được định nghĩa như sau[6]:

$$\begin{cases} \mathbb{G}_1 = E[r] \cap \text{Ker}(\pi_p - [1]), \\ \mathbb{G}_2 = E[r] \cap \text{Ker}(\pi_p - [p]), \end{cases} \quad (9)$$

Trong đó, π_p là ánh xạ Frobenius, được định như sau: $\pi_p(x, y) = (x^p, y^p)$. Hạt nhân của ánh xạ ϕ , ký hiệu là $\text{Ker}(\phi)$, là tập các điểm được ánh xạ tới điểm đơn vị. Do đó:

$$\text{Ker}(\pi_p - [1]) = \{P \in E[r] \mid \pi_p(P) = P\} \quad (10)$$

$$\text{Ker}(\pi_p - [p]) = \{P \in E[r] \mid \pi_p(P) = [p]P\} \quad (11)$$

Trong thực tế, các nhóm cyclic \mathbb{G}_1 và \mathbb{G}_2 thường được xây dựng dựa trên các điểm trên đường cong elliptic với tọa độ thuộc các trường hữu hạn (finite fields) \mathbb{F}_p với p là số nguyên tố, hoặc các trường mở rộng như \mathbb{F}_{p^2} hoặc $\mathbb{F}_{p^{12}}$

Việc chọn $\mathbb{G}_1, \mathbb{G}_2$ như vậy giúp đảm bảo các nhóm tương thích để thực hiện phép pairing chính xác và bảo mật.

Phép ghép cặp song tuyến tính (Bilinear Pairing):

Phép ghép cặp (pairing) trong hệ thống CP-ABE là công cụ toán học cốt lõi để xây dựng cơ chế mã hóa và giải mã. Ánh xạ này cho phép kiểm tra sự phù hợp giữa tập thuộc tính của người dùng và chính sách truy cập nhúng trong bản mã mà không làm rò rỉ thông tin bí mật.

Cụ thể, theo nguồn [9] phép ghép cặp được định nghĩa như sau: cho \mathbb{G}_1 và \mathbb{G}_2 là hai nhóm cyclic có bậc nguyên tố p , với g_1 là phần tử sinh của \mathbb{G}_1 và g_2 là phần tử sinh của \mathbb{G}_2 . Phép ghép cặp e là một ánh xạ:

$$e: \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T \quad (12)$$

Trong đó nhóm \mathbb{G}_T là nhóm đích được định nghĩa trên một trường mở rộng như \mathbb{F}_{p^k} với k là bậc nhúng (embedding degree), chứa kết quả của phép ghép cặp (pairing) giữa các phần tử thuộc \mathbb{G}_1 và \mathbb{G}_2 . Việc định nghĩa \mathbb{G}_T trên một trường mở rộng cho phép sử dụng các kỹ thuật pairing hiệu quả, đồng thời đảm bảo tính không suy biến và tính toán được của phép ghép cặp[5], [6].

Trong đó nhóm \mathbb{G}_T cũng là một nhóm cyclic đích được định nghĩa trên một trường mở rộng như \mathbb{F}_{p^k} với k là bậc nhúng (embedding degree), chứa kết quả của phép ghép cặp (pairing) giữa các phần tử thuộc \mathbb{G}_1 và \mathbb{G}_2 , việc định nghĩa \mathbb{G}_T trên một trường mở rộng cho phép sử dụng các kỹ thuật pairing hiệu quả. Để phục vụ cho các ứng dụng trong mật mã, ánh xạ này phải thỏa mãn ba điều kiện quan trọng: tính song tuyến tính, tính không suy biến và khả năng tính toán hiệu quả.

Tính song tuyến tính (Bilinearity) định nghĩa rằng với mọi $u \in \mathbb{G}_1$, $v \in \mathbb{G}_2$ và $a, b \in \mathbb{Z}_p$, ta có:

$$e(u^a, v^b) = e(u, v)^{ab} \quad (13)$$

Tính chất này cho phép biến đổi các phép toán mũ trong nhóm vào thành phép nhân trong nhóm kết quả. Ngoài ra, tính chất này cũng bao hàm rằng:

$$e(u_1 + u_2, v) = e(u_1, v) \cdot e(u_2, v) \quad (14)$$

Tính không suy biến (Non-degeneracy): Nếu g_1 là phần tử sinh của \mathbb{G}_1 và g_2 là phần tử sinh của \mathbb{G}_2 , thì $e(g_1, g_2) \neq 1$ (phần tử đơn vị của nhóm \mathbb{G}_T). Tính chất này giúp hệ mã tránh các trường hợp ánh xạ vô hiệu.

Nguồn [1] cũng lưu ý rằng khi \mathbb{G}_1 và \mathbb{G}_2 trùng nhau ($\mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$) và phép ghép cặp e thỏa mãn tính song tuyến tính và không suy biến, thì phép ghép cặp này là đối xứng (symmetric) vì $e(g^a, g^b) = e(g, g)^{ab} = e(g^b, g^a)$.

Tính hiệu quả (Computability): Phép ánh xạ phải được tính toán hiệu quả trên thực tế, tức có thuật toán thực hiện trong thời gian đa thức.

Dựa trên mối quan hệ giữa G_1 và G_2 , người ta phân chia phép ghép cặp thành ba loại:

Loại I – Phép ghép cặp đối xứng (Type I – Symmetric Pairing): Đây là loại cơ bản nhất, khi $\mathbb{G}_1 = \mathbb{G}_2$. Phép ánh xạ có dạng $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$. Thư viện PBC sử dụng loại này trong đó \mathbb{G} là nhóm cộng trên đường cong elliptic, còn \mathbb{G}_T là nhóm nhân hữu hạn. Tuy nhiên, loại này chỉ đạt mức bảo mật khoảng 80-bit và có thể bị tấn công bởi các phương pháp hiện đại.

Loại II – Phép ghép cặp bất đối xứng có đẳng cấu một chiều (Type II – Asymmetric Pairing with One-Way Isomorphism): Loại này xuất hiện khi $\mathbb{G}_1 \neq \mathbb{G}_2$, nhưng tồn tại phép đẳng cấu $\phi: \mathbb{G}_2 \rightarrow \mathbb{G}_1$ có thể tính toán hiệu quả, trong khi không có chiều ngược lại. Mặc dù cải thiện bảo mật so với loại I, loại II ít được ứng dụng rộng rãi do chi phí tính toán đẳng cấu.

Loại III – Phép ghép cặp bất đối xứng hoàn toàn (Type III – Fully Asymmetric Pairing): Đây là loại mạnh và phổ biến nhất trong các hệ mật mã hiện đại, trong đó $\mathbb{G}_1 \neq \mathbb{G}_2$ và không tồn tại đẳng cấu hiệu quả giữa hai nhóm. Thư viện ELP và RELIC đều hỗ trợ phép ghép cặp loại này. Loại III không chỉ có hiệu năng tốt mà còn hỗ trợ nhiều giả định mật mã học khác nhau (như External DDH), điều mà các loại I và II không cung cấp được.

Dựa trên sự phân loại các phép ghép cặp (Type I, II và III), có thể thấy rằng mỗi loại có đặc điểm riêng về cấu trúc toán học, tính bảo mật và khả năng triển khai. Tuy nhiên, trong các hệ thống mã hóa hiện đại như CP-ABE, phép ghép cặp loại III (bất đối xứng hoàn toàn) đã và đang trở thành lựa chọn phổ biến nhất. Việc lựa chọn này không chỉ xuất phát từ đặc tính toán học nội tại mà còn dựa vào các phân tích hiệu quả và an toàn trong thực tiễn triển khai.

Thứ nhất, loại III giúp tăng cường mức độ bảo mật vì không tồn tại phép ánh xạ hiệu quả giữa hai nhóm đầu vào \mathbb{G}_1 và \mathbb{G}_2 . Điều này ngăn chặn các kiểu tấn công dựa trên việc chuyển đổi phần tử giữa hai nhóm, vốn là lỗ hổng trong các hệ sử dụng loại I và II.

Thứ hai, Type III cho phép áp dụng nhiều giả định tính toán an toàn hơn như giả định External Diffie-Hellman hoặc giả định DBDH trong từng nhóm riêng biệt. Điều này giúp hệ thống dễ dàng chứng minh tính an toàn trong các mô hình tấn công thực tế hơn.

Thứ ba, việc tách biệt hai nhóm đầu vào tạo điều kiện cho các tối ưu tính toán, như sử dụng nhóm \mathbb{G}_1 trên trường nhỏ và tận dụng sextic

twist để giảm chi phí trên \mathbb{G}_2 . Nhờ đó, hiệu năng tổng thể của hệ thống được cải thiện rõ rệt.

Cuối cùng, Type III được các thư viện mật mã hiện đại như ELiPS, MCL và RELIC hỗ trợ mạnh mẽ, và cũng là loại pairing được khuyến nghị trong nhiều tiêu chuẩn quốc tế. Sự hỗ trợ rộng rãi này giúp đảm bảo khả năng triển khai thực tế và tính mở rộng của hệ mã.

Ngoài ra, để ánh xạ một thuộc tính từ chuỗi ký tự thành điểm trên đường cong elliptic, hệ thống sử dụng một hàm băm lên đường cong elliptic (hash-to-curve)[6], ký hiệu là:

$$\mathcal{H}: \{0,1\}^* \rightarrow \mathbb{G}_1 \quad (15)$$

Hàm \mathcal{H} phải có tính ngẫu nhiên, không xác định trước và phân phối đều các thuộc tính về không gian nhóm, đảm bảo tính an toàn và không thể dự đoán được. Hàm này rất quan trọng để ánh xạ các thuộc tính như “Giới tính: Nam” hay “Bộ môn: CNTT” thành phần tử mật mã tương ứng.

Trong các hệ mã CP-ABE, hàm \mathcal{H} được sử dụng trong nhiều giai đoạn quan trọng như:

Tạo khóa (KeyGen): Ánh xạ mỗi thuộc tính a_i của người dùng sang phần tử $H(a_i)$ trong \mathbb{G}_1 , từ đó sinh ra các thành phần của khóa bí mật.

Mã hóa (Encrypt): Ánh xạ thuộc tính xuất hiện trong chính sách truy cập sang phần tử trên đường cong để tạo các phần tử trong bản mã.

Khởi tạo (Setup): Xác định trước hàm băm hoặc seed để mô phỏng trong random oracle.

Để đảm bảo tính an toàn, hàm băm \mathcal{H} phải thỏa mãn các tính chất mật mã học cơ bản:

Tính kháng tiền ảnh (Pre-image resistance): Không thể tính ngược từ đầu ra để tìm đầu vào tương ứng.

Tính kháng tiền ảnh thứ hai (2nd pre-image resistance): Không thể tìm hai đầu vào khác nhau có cùng giá trị băm.

Tính kháng va chạm (Collision resistance): Không thể tìm được hai thuộc tính khác nhau nhưng lại ánh xạ tới cùng một điểm trong .

Trong mô hình chứng minh an toàn, hàm \mathcal{H} thường được xem như một oracle ngẫu nhiên (random oracle), tức là một hộp đen trả về đầu

ra ngẫu nhiên nhưng nhất quán với cùng đầu vào. Tóm lại, hàm băm \mathcal{H} không chỉ là công cụ ánh xạ kỹ thuật mà còn là cầu nối giữa không gian thuộc tính rời rạc và không gian toán học liên tục trên đường cong elliptic, đóng vai trò thiết yếu trong việc bảo toàn an toàn và hiệu quả cho các hệ mã CP-ABE.

Trong các hệ pairing Type III bất đối xứng hiện đại, nhóm \mathbb{G}_2 thường được định nghĩa trên trường rất lớn như $\mathbb{F}_{p^{12}}$, điều này gây tốn kém về mặt tính toán. Kỹ thuật sextic twist cho phép ánh xạ các điểm từ đường cong twist E' trên trường nhỏ hơn \mathbb{F}_{p^2} sang đường cong gốc E trên $\mathbb{F}_{p^{12}}$, từ đó giúp thực hiện các phép toán trong \mathbb{G}_2 với chi phí thấp hơn.

CP-ABE sử dụng cấu trúc chia sẻ bí mật tuyến tính (Linear Secret Sharing Scheme – LSSS) để biểu diễn chính sách truy cập. Chính sách được mã hóa dưới dạng một ma trận M và một hàm ánh xạ π gán mỗi hàng của M cho một thuộc tính. Ma trận LSSS cho phép chia sẻ một khóa bí mật thành nhiều phần tuyến tính. Trong quá trình giải mã, chỉ khi người dùng có đủ tập thuộc tính tương ứng với các hàng của M , họ mới có thể kết hợp các phần đó để khôi phục lại khóa phiên, nghĩa là giải mã thành công[1].

An toàn của hệ thống CP-ABE được xây dựng dựa trên các giả định về độ khó tính toán, trong đó phổ biến nhất là Decisional Bilinear Diffie-Hellman (DBDH)[1]. Giả định này phát biểu rằng: không thể phân biệt được giữa $e(g, g)^{a,b,c}$ và $e(g, g)^z$ nếu không biết các số mũ a, b, c . Điều này đảm bảo rằng không có kẻ tấn công nào có thể giải mã được dữ liệu nếu không có khóa hợp lệ.

2.5.1.3 Các thuật toán cơ bản trong hệ CP-ABE

Dựa trên các thành phần toán học đã được trình bày ở các mục trước – bao gồm đường cong elliptic, nhóm cyclic hữu hạn, phép ghép cặp song tuyến tính và mô hình chia sẻ bí mật tuyến tính (LSSS) – hệ mã hóa CP-ABE (Ciphertext-Policy Attribute-Based Encryption) được xây dựng từ bốn thuật toán cơ bản: Khởi tạo, Tạo khóa, Mã hóa và Giải mã. Các thuật toán này phối hợp nhằm hiện thực hóa kiểm soát truy cập chi tiết dựa trên thuộc tính, đảm bảo chỉ người dùng có tập thuộc tính phù hợp mới có thể giải mã dữ liệu.

Khởi tạo (Setup): Thuật toán thiết lập các tham số hệ thống, bao gồm nhóm cyclic trên đường cong elliptic, ánh xạ pairing và hàm băm

thuộc tính. Kết quả là một khóa công khai (public key) phân phối công khai và khóa bí mật chủ (master secret key) giữ bởi bên quản lý.

Tạo khóa (Key Generation): Dựa trên master secret key và tập thuộc tính của người dùng, thuật toán sinh ra khóa bí mật cá nhân. Mỗi thuộc tính được ánh xạ lên đường cong elliptic bằng hàm băm và kết hợp với các tham số hệ thống để tạo nên khóa con.

Mã hóa (Encryption): Người gửi mã hóa dữ liệu dựa trên một chính sách truy cập, thường được biểu diễn bằng LSSS. Khóa phiên được sinh ngẫu nhiên, mã hóa dữ liệu bằng thuật toán đối xứng, sau đó được bảo vệ bằng CP-ABE thông qua các phép toán trên nhóm elliptic.

Giải mã (Decryption): Người nhận sử dụng khóa bí mật và thực hiện các phép pairing với bản mã. Nếu thuộc tính của họ thỏa mãn chính sách, họ có thể khôi phục khóa phiên và giải mã dữ liệu.

2.5.2 RELIC (Efficient Library for Cryptography)

RELIC Toolkit (RELIC Cryptographic Library) là một thư viện mã nguồn mở mạnh mẽ, được thiết kế nhằm cung cấp nền tảng toán học hiệu năng cao cho các ứng dụng mật mã học hiện đại, đặc biệt là các hệ thống sử dụng đường cong elliptic và phép ghép cặp. Không giống như một số thư viện cũ hơn như PBC (Pairing-Based Cryptography), RELIC được phát triển với định hướng tối ưu hóa linh hoạt cho cả hiệu suất và tính bảo mật, đồng thời hỗ trợ triển khai trên nhiều nền tảng phần cứng khác nhau, từ hệ thống nhúng cho đến máy chủ hiệu năng cao.

Một trong những đặc điểm nổi bật khiến RELIC trở thành lựa chọn phù hợp cho việc triển khai hệ mã CP-ABE chính là khả năng hỗ trợ tốt cho phép ghép cặp loại III (Type III asymmetric pairings). Như đã phân tích ở các phần trước, phép ghép cặp loại III mang lại nhiều ưu điểm đáng kể về bảo mật, khi nó loại bỏ được những giả định yếu về tính tự đối xứng như trong phép ghép cặp loại I. Ngoài ra, pairing loại III còn giúp mở rộng tính tương thích với các giả định mật mã học mạnh hơn, chẳng hạn như giả định External Diffie-Hellman, từ đó tăng cường khả năng chống lại các tấn công hiện đại.

Thư viện RELIC còn cho phép người dùng linh hoạt trong việc cấu hình các thành phần hệ thống. Cụ thể, RELIC hỗ trợ nhiều lớp số học trong trường hữu hạn như \mathbb{F}_p , \mathbb{F}_{p^2} và $\mathbb{F}_{p^{12}}$, đồng thời cho phép bật hoặc tắt các

mô-đun như pairing, EP1, EP2, và các thuật toán số học dựa trên thư viện GMP. Khả năng này rất hữu ích khi cần xây dựng các nhóm $\mathbb{G}_1, \mathbb{G}_2$ và \mathbb{G}_T một cách cụ thể, phục vụ cho các mô hình CP-ABE sử dụng ánh xạ từ đường cong elliptic sang nhóm đích.

Ngoài ra, RELIC còn hỗ trợ nhiều loại đường cong mật mã học như BN (Barreto–Naehrig) và BLS, cũng như các thuật toán ánh xạ pairing tối ưu như Optimal Ate pairing, vốn được xem là lựa chọn phổ biến trong các hệ thống mã hóa hiện đại nhờ khả năng cân bằng giữa tốc độ và độ bảo mật. Khả năng tối ưu hóa cấp thấp (low-level optimization) của RELIC cho nhiều kiến trúc phần cứng như Intel, ARM hay RISC-V càng khẳng định giá trị thực tiễn của thư viện này trong các hệ thống yêu cầu hiệu năng cao.

Một yếu tố quan trọng khác là sự tích cực phát triển và cập nhật của cộng đồng mã nguồn mở dành cho RELIC, giúp đảm bảo rằng thư viện luôn theo kịp các tiêu chuẩn bảo mật mới nhất. Trong khi đó, một số thư viện như PBC đã không còn được duy trì thường xuyên, khiến chúng trở nên kém phù hợp cho các nghiên cứu và ứng dụng yêu cầu độ tin cậy cao.

Từ những phân tích trên, có thể thấy rằng việc lựa chọn RELIC làm nền tảng cho việc triển khai hệ mã hóa CP-ABE trong nghiên cứu này là hoàn toàn hợp lý. RELIC không chỉ cung cấp các công cụ toán học cần thiết một cách đầy đủ và hiệu quả, mà còn đảm bảo khả năng thích ứng cao với yêu cầu bảo mật và triển khai thực tế.

2.5.3 PBC (Pairing-Based Cryptography)

Thư viện PBC (Pairing-Based Cryptography Library) là một thư viện mã nguồn mở được phát triển bởi Ben Lynn[4], nhằm hỗ trợ triển khai các hệ thống mật mã dựa trên ghép cặp song tuyến tính, đặc biệt là các hệ như IBE (Identity-Based Encryption), ABE (Attribute-Based Encryption) và các biến thể mã hóa hiện đại khác. Trong nhiều năm, PBC đã đóng vai trò quan trọng trong việc minh họa và hiện thực hóa các thuật toán mật mã thuộc lớp pairing-based cryptography, đặc biệt trong môi trường học thuật và nghiên cứu.

Tương tự như RELIC, PBC cũng cung cấp các nhóm toán học chính bao gồm \mathbb{G}, \mathbb{G}_T và ánh xạ $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$. Tuy nhiên, điểm khác biệt cốt lõi giữa PBC và các thư viện hiện đại là PBC chỉ hỗ trợ ghép cặp đối xứng (Type I pairing), trong đó hai nhóm đầu vào là giống nhau ($\mathbb{G}_1 = \mathbb{G}_2 = \mathbb{G}$). Loại pairing này tuy thuận tiện khi lập trình và triển khai, nhưng lại tiềm ẩn những rủi ro về bảo mật khi phải đối mặt với các mô

hình tấn công hiện đại, do chỉ đạt mức an toàn tương đương khoảng 80-bit[5].

PBC sử dụng các đường cong elliptic dạng siêu phân biệt (supersingular) với nhóm cộng điểm được định nghĩa trên trường hữu hạn \mathbb{F}_p , điển hình là đường cong:

$$E: y^2 = x^3 + x$$

Việc khởi tạo các tham số trong PBC được thực hiện thông qua tệp cấu hình .param, giúp đơn giản hóa quá trình thử nghiệm và kiểm tra thuật toán. Các hàm cấp cao như pairing_init_set_buf(), element_init_G1(), element_pow_zn() hay element_pairing() cho phép người dùng thao tác trực tiếp với các phần tử trong nhóm, tính toán mũ, hash thuộc tính lên đường cong và thực hiện ghép cặp[4].

Mặc dù PBC từng là lựa chọn hàng đầu trong triển khai các hệ mã dựa trên thuộc tính, thư viện này hiện đã bộc lộ một số hạn chế lớn. Cụ thể:

- Bảo mật: chỉ hỗ trợ mức bảo mật thấp (khoảng 80-bit), không còn đáp ứng các tiêu chuẩn khuyến nghị hiện nay (tối thiểu 128-bit theo NIST).
- Không hỗ trợ pairing bất đối xứng (Type III) – loại pairing đang được các hệ mã hóa hiện đại như CP-ABE với RELIC, MCL, hay ELiPS ưa chuộng do hiệu suất và bảo mật tốt hơn
- Khả năng mở rộng: thiếu hỗ trợ cho các đường cong mới như BLS12-381, BN-P256,... và không tối ưu cho các kiến trúc phần cứng hiện đại.
- Tình trạng phát triển: dự án đã ngừng cập nhật từ năm 2013, dẫn đến việc không còn tương thích tốt với các hệ điều hành hoặc nền tảng biên dịch mới[10].

Từ những phân tích trên, có thể thấy rằng, mặc dù PBC vẫn còn hữu ích trong các nghiên cứu mô phỏng hoặc giảng dạy, nhưng không còn phù hợp để triển khai các hệ thống mật mã thực tiễn với yêu cầu cao về bảo mật và hiệu suất. Điều này lý giải vì sao các thư viện hiện đại như RELIC, MCL hoặc ELiPS đang dần thay thế vai trò của PBC trong lĩnh vực triển khai các hệ mã hóa dựa trên thuộc tính như CP-ABE.

2.5.4 So sánh các hàm sử dụng trong PBC và RELIC

Bảng dưới đây trình bày sự khác biệt giữa các hàm chủ yếu được sử dụng trong thư viện Pairing-Based Cryptography (PBC) với các hàm tương ứng trong RELIC. Mỗi chức năng đều được phân loại rõ ràng, cho thấy

cách RELIC tổ chức cấu trúc các hàm theo nhóm toán học ($\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$), đồng thời hỗ trợ các phép toán tương đương với mức bảo mật cao hơn.

Chức năng	PBC	RELIC	Ghi chú
Khởi tạo hệ pairing	pairing_init_set_buf()	pc_param_set_any + pc_map()	PBC dùng file .param RELIC cho phép chọn tham số đường cong lập trình
Khởi tạo phần tử nhóm	element_init_G1(), element_init_GT()	ep_new(), ep2_new(), fp12_new()	RELIC phân biệt rõ G1, G2, GT theo loại nhóm
Sinh phần tử ngẫu nhiên	element_random()	bn_rand_mod()	PBC dùng chung cho mọi nhóm, RELIC dùng riêng cho số mũ bn_t
Luỹ thừa (exponentiation)	element_pow_zn()	ep_exp(), ep2_exp(), fp12_exp()	RELIC chia rõ theo nhóm (G1, G2, GT)
Phép nhân	element_mul()	ep_mul(), ep2_mul()	Cùng chức năng, thực hiện trên phần tử cùng nhóm
Phép nghịch đảo	element_invert()	ep_inv(), ep2_inv()	Dùng trong tính toán chia khóa hoặc tái tạo Lagrange
Tính pairing	element_pairing(out, a, b)	pc_map(out, in1, in2)	RELIC hỗ trợ pairing bất đối xứng (Type III), bảo mật cao hơn
Hash lên đường cong (Hash-to-curve)	element_from_hash()	md_map_sh256() + ep_map()	RELIC tách riêng băm và ánh xạ để kiểm soát tốt hơn
So sánh phần tử	element_cmp()	ep_cmp(), ep2_cmp()	So sánh chính xác trong bước xác thực/thử nghiệm
Khởi tạo số mũ từ chuỗi/byte	element_set_str(), element_from_bytes()	bn_read_str(), bn_read_bin()	Cùng vai trò đọc tham số hoặc thành phần đã serialize

Bảng 1: So sánh hàm PBC và RELIC

CHƯƠNG 3

PHÂN TÍCH THIẾT KẾ HỆ THỐNG

3.1 Tổng quan cài đặt

Việc triển khai hệ mã CP-ABE với thư viện RELIC thay thế cho các thư viện truyền thống như PBC hay ELiPS không chỉ mang lại mức độ bảo mật cao hơn (128-bit) mà còn cho phép kiểm soát tốt hơn về hiệu năng và khả năng tối ưu hóa các phép toán mật mã.

Hệ thống CP-ABE bao gồm bốn thuật toán chính: Khởi tạo (Setup), Tạo khóa bí mật (Key Generation), Mã hóa (Encryption) và Giải mã (Decryption). Trong phần này, các thuật toán trên sẽ được triển khai dựa trên thư viện mật mã RELIC, với cấu trúc và tham số cụ thể nhằm đảm bảo hiệu quả và bảo mật. Dưới đây là phân tích chi tiết từng thuật toán cùng với các công thức toán học và mã nguồn tương ứng.

3.1.1 Khởi tạo (Setup)

Thuật toán Setup được thực hiện một lần duy nhất bởi cơ quan cấp khóa (authority) nhằm sinh ra bộ khóa công khai (public key - PK) và khóa bí mật chủ (master secret key - MSK). Cụ thể, thuật toán khởi tạo được tiến hành như sau:

Trước tiên, sinh lần lượt các phần tử sinh $g_1 \in \mathbb{G}_1$ và $g_2 \in \mathbb{G}_2$ tương ứng là phần tử sinh của hai nhóm con trên đường cong elliptic được định nghĩa lần lượt trên trường \mathbb{F}_p và \mathbb{F}_{p^2} . Các nhóm này được thiết lập để tương thích với cấu trúc pairing bất đối xứng (Type III), trong đó nhóm mục tiêu \mathbb{G}_T là nhóm con của trường nhân $\mathbb{F}_{p^{12}}$. Việc sử dụng các phần tử sinh chuẩn đảm bảo các phép toán sau đó như nhân vô hướng, ánh xạ pairing hay kiểm tra thuộc tính đều diễn ra chính xác theo đặc tả của hệ mã.

Tiếp theo, hai số ngẫu nhiên $\alpha, \beta \in \mathbb{Z}_r$ được sinh ngẫu nhiên và dùng để xây dựng các tham số khóa. Từ đó thực hiện tính toán các giá trị của PK và MSK với:

$$MSK = (\beta, g_\alpha)$$

$$PK = (g_1, g_2, h, e(g_1, g_\alpha))$$

Trong đó:

$$h = g_1^\beta \in \mathbb{G}_1 \text{ được dùng để mã hóa thông tin.}$$

$g_\alpha = g_2^\alpha \in \mathbb{G}_2$ là thành phần chứa bí mật chủ α trong dạng sẵn sàng sử dụng với pairing, và được dùng để sinh khóa bí mật cho người dùng sao cho khi pairing với phần tử mã hóa, ta có thể khôi phục được khóa phiên hoặc thông điệp.

$e(g_1, g_\alpha)$ là phần tử pairing được nâng mũ bởi α , sử dụng để mã hóa khóa phiên.

Việc sinh các tham số trên dựa trên đường cong elliptic pairing-friendly được hỗ trợ bởi RELIC và nhằm đáp ứng cấu trúc pairing bất đối xứng (Type III).

3.1.2 Tạo khóa (Key Generation)

Sau khi hệ thống đã được khởi tạo với bộ khóa công khai và khóa bí mật chủ, bước tiếp theo là thuật toán tạo khóa (KeyGen) nhằm sinh khóa bí mật cá nhân cho người dùng, dựa trên tập thuộc tính mà họ sở hữu.

Mục tiêu chính của thuật toán là sinh ra khóa bí mật SK cho người dùng có tập thuộc tính $S = \{attr_1, attr_2, \dots, attr_n\}$. Khóa bí mật này cho phép người dùng có thể giải mã các bản mã mà chính sách truy cập thỏa mãn tập thuộc tính của họ.

Thuật toán nhận đầu vào gồm MSK và tập thuộc tính S của người dùng. Trước hết, hệ thống sinh một phần tử ngẫu nhiên $r = \mathbb{Z}_r$. Sau đó, thuật toán tiến hành tính toán thành phần chính của khóa bí mật:

$$D = \frac{g_\alpha \cdot g_2^r}{\beta} = g_2^{(\alpha+r)/\beta} \in \mathbb{G}_2$$

Với mỗi thuộc tính $i \in S$, hệ thống sinh một số ngẫu nhiên $r_i \in \mathbb{Z}_r$, sau đó tính toán các thành phần tương ứng như sau:

$$d_i = g_2^{r_i} \in \mathbb{G}_2$$

$$d'_i = H(x)^{r_i} \in \mathbb{G}_1$$

Kết quả, khóa bí mật của người dùng có dạng:

$$SK = (D, \{(d_i, d'_i)\}_{i \in S})$$

Cấu trúc khóa này đảm bảo rằng chỉ khi người dùng có đầy đủ thuộc tính thỏa mãn chính sách truy cập được nhúng trong bản mã, họ mới có thể tái tạo thành công khóa phiên và giải mã dữ liệu. Các thuộc tính trong tập S được ánh xạ ngẫu nhiên và riêng biệt lên đường cong elliptic, giúp tăng cường bảo mật trước các tấn công phân tích.

3.1.3 Mã hóa (Encryption)

Thuật toán mã hóa trong CP-ABE cho phép người gửi dữ liệu mã hóa thông điệp M sao cho chỉ những người dùng sở hữu tập thuộc tính phù hợp với chính sách truy cập mới có thể giải mã được.

Chính sách truy cập A có thể được biểu diễn dưới dạng cây truy cập (access tree), bao gồm các cổng logic như AND, OR hoặc ngưỡng (threshold). Mỗi nút lá trong cây tương ứng với một thuộc tính cụ thể. Việc biểu diễn chính sách này cho phép linh hoạt định nghĩa các điều kiện truy cập phức tạp.

Trước tiên, thuật toán chọn một phần tử ngẫu nhiên $s \in \mathbb{Z}_r$, được xem là bí mật chính dùng để mã hóa. Từ s , thuật toán xây dựng một vector bí mật dùng để chia sẻ đến các nút trong cây truy cập bằng sơ đồ chia sẻ bí mật tuyến tính (Linear Secret Sharing Scheme - LSSS).

Tiếp theo, thuật toán tính các thành phần mã hóa như sau:

$$C = M \cdot e(g_1, g_2)^{\alpha s} \in \mathbb{G}_T$$

$$C' = g^s \in \mathbb{G}_1$$

Với mỗi $x \in A$, gắn với thuộc tính i , ta tính:

$$C_i = g^{\lambda_i} \in \mathbb{G}_1$$

$$C'_i = H(i)^{\lambda_i} \in \mathbb{G}_1$$

Trong đó λ_i là thành phần chia sẻ của bí mật s tại nút i .

Cấu trúc bản mã sau cùng là:

$$CT = (C, C', \{(C_x, C'_x)\}_{x \in A})$$

Toàn bộ các thành phần trên cùng với cấu trúc chính sách tạo thành bản mã (ciphertext). Cơ chế này đảm bảo rằng người dùng chỉ có thể giải mã nếu tập thuộc tính của họ đủ để tái tạo lại bí mật. Đây là cơ chế cốt lõi trong việc kiểm soát truy cập dữ liệu trong hệ thống CP-ABE.

3.1.4 Giải mã (Decryption)

Thuật toán giải mã là bước cuối cùng trong hệ thống CP-ABE, cho phép người dùng khôi phục lại thông điệp ban đầu từ bản mã với điều kiện tập thuộc tính họ sở hữu phải thỏa mãn chính sách truy cập nhúng trong bản mã. Quá trình này sử dụng mô hình chia sẻ bí mật tuyến tính (Linear Secret Sharing Scheme - LSSS) kết hợp với phép ghép cặp (pairing) để tính lại khóa phiên đã được sử dụng trong bước mã hóa.

Thuật toán thực hiện kiểm tra xem tập thuộc tính trong khóa bí mật cá nhân có thỏa mãn chính sách truy cập trong bản mã hay không. Nếu có, nó sẽ kết hợp các thành phần của bản mã và khóa bí mật bằng cách sử dụng phép ghép cặp (pairing) để khôi phục lại khóa phiên đã dùng để mã hóa thông điệp ban đầu.

Quá trình giải mã bắt đầu bằng việc xác định xem tập thuộc tính của người dùng có đủ để tái tạo lại bí mật chia sẻ thông qua LSSS không. Nếu thỏa mãn, tồn tại một tập con $S' \subseteq S$ đủ để tái tạo lại bí mật chia sẻ thông qua hệ số Lagrange $\{\omega_x\}$ để tính toán lại:

$$\begin{aligned} K &= \frac{e(C', D)}{\prod_{x \in S'} e(C_i, d') \cdot e(C'_i, d_i)} \\ &= e(g_1^s, g_2^{\frac{\alpha+r}{\beta}}) \cdot \left(\prod_{i \in S'} e(g^{\lambda_i}, H(i)^{r_i}) \cdot e(H(i)^{\lambda_i}, g_2^{r_i}) \right)^{-1} \end{aligned}$$

Nhờ tính chất song tuyến tính của phép pairing, các thành phần chứa r_i sẽ triệt tiêu nhau, và biểu thức rút gọn về:

$$K = e(g_1, g_2)^{\alpha s}$$

Từ khóa phiên $K = e(g_1, g_2)^{\alpha s}$, ta trích xuất thông điệp gốc M từ thành phần C của bản mã bằng:

$$M = \frac{C}{K}$$

Quá trình giải mã dựa trên sự kết hợp giữa thuộc tính người dùng, chính sách truy cập, và cấu trúc chia sẻ tuyến tính. Phép pairing là công cụ trung gian để kiểm tra sự thỏa mãn chính sách và khôi phục khóa phiên. Hệ số Lagrange đảm bảo quá trình tổng hợp các chia sẻ λ_i tái dựng lại chính xác giá trị sss ban đầu mà không cần tiết lộ nó.

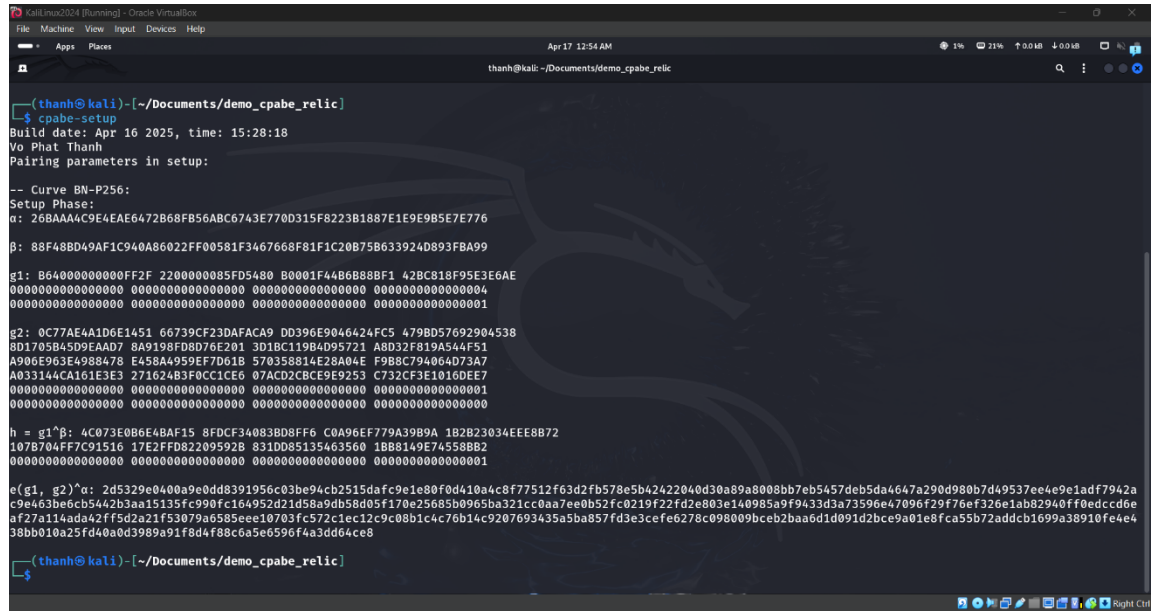
Tóm lại, quá trình giải mã trong CP-ABE đảm bảo rằng chỉ những người dùng có tập thuộc tính phù hợp với chính sách truy cập mới có thể giải mã thành công dữ liệu. Phép ghép cặp kết hợp với LSSS đóng vai trò cốt lõi trong cơ chế này, cung cấp một mô hình kiểm soát truy cập linh hoạt và bảo mật cao.

3.2 Kết quả thực nghiệm

Quá trình thực nghiệm triển khai CP-ABE đã được thực hiện trên môi trường hệ điều hành Kali Linux, với công cụ dòng lệnh được xây dựng dựa trên thư viện RELIC. Các thuật toán setup, keygen, encrypt và decrypt được

biên dịch thành chương trình độc lập và được kiểm thử thông qua các tập tin dữ liệu thật (ví dụ: security_report.pdf) cùng các bộ thuộc tính tương ứng.

Ở bước khởi tạo hệ thống (setup), hệ thống đã sinh thành công các tham số chính bao gồm các phần tử $g_1 \in \mathbb{G}_1, g_2 \in \mathbb{G}_2, h = g_1^\beta, g_2^\alpha$ và cặp pairing $e(g_1, g_2)^\alpha$. Đường cong sử dụng trong hệ thống là Barreto-Naehrig BN-P256, với các phần tử sinh và giá trị tuần tự hóa được in ra và xác minh đúng cấu trúc.



```
(thanh@kali)~[/Documents/demo_cpabe_relic]
$ cpabe-setup
Build date: Apr 16 2025, time: 15:28:18
Vo Phat Thanh
Pairing parameters in setup:

-- Curve BN-P256:
Setup Phase:
g: 268AAA4C9E4EAE6472B68FB56ABC6743E770D315F8223B1887E1E9E9B5E7E776
B: 8BF48BD49AF1C940A86022FF00581F3467668F81F1C20B75B633924D893FBA99

g1: B64000000000FF2F 2200000085FD5480 B0001F44B6888BF1 42BC818F95E3E6AE
0000000000000000 0000000000000000 0000000000000000 0000000000000000
0000000000000000 0000000000000000 0000000000000000 0000000000000000

g2: 0C77AE4A1D6E1451 66739CF23DAFACA9 DD396E9046424FC5 479BD57692904538
8D1705B45D9EAD07 8A9198FD8D76E201 3D18C119B4D95721 A8D32F819A544F51
A906E963E4988478 E458A4959EF7D61B 570358814E28A04E F9B8C794064D73A7
A033144CA161E3E3 27162483F0CC1CE6 07ACD2CBC9E9253 C732CF3E1016DEE7
0000000000000000 0000000000000000 0000000000000000 0000000000000000
0000000000000000 0000000000000000 0000000000000000 0000000000000000

h = g1^B: 4C073E0B6E4BAF15 8FDCF34083B08FF6 C0A96EF779A39B9A 1B2B23034EE8B72
107B704FF7C91516 17E2FFD82209592B 831DD85135463560 1B88149E74558B82
0000000000000000 0000000000000000 0000000000000000 0000000000000000

e(g1, g2)^alpha: 2d5329e0400a9e0dd8391956c03be94cb2515dafc9e1e80f0d410a4c8f77512f63d2fb578e5b42422040d30a89a8008bb7eb5457deb5da4647a290d980b7d49537ee4e9e1adf7942a
c9e463be6cb5442b3aa15135fc990fc164952d21d58a9db58d05f170e25685b0965ba321cc0aa7ee0b52fc0219f22fd2e803e140985a9f9433d3a73596e47096f29f76ef326e1ab82940ff0edccdc6e
af27a114ada42ff5d2a21f53079a6585ee10703fc572c1ec12c9c08b1c4c76b14c9207693435a5ba857fd3e3cfe6278c098009bceb2baa6d1d091d2bce9a01e8fca55b72addcb1699a38910fe4e4
38bb01a25fd40ad3989a91f8d4f88c6a5e6596f4a3dd64ce8

(thanh@kali)~[/Documents/demo_cpabe_relic]
```

Hình 1: Thực hiện setup

Tiếp theo, thuật toán tạo khóa (keygen) được thực hiện với tập thuộc tính đầu vào gồm 5 thuộc tính, bao gồm cả các thuộc tính có định dạng có cấu trúc như `executive_level=7`. Hệ thống đã sinh đúng định dạng các thành phần của khóa bí mật người dùng, bao gồm phần tử chính $D = g_2^{(\alpha+r)/\beta}$, cùng với mỗi thành phần $d_i = g_2^{r_i}, d'_i = H(attr_i)^{r_i}$ được ánh xạ và hiển thị đầy đủ.

```

(thanh@kali) ~/Documents/demo_cpabe_relic
$ cpabe-keygen -o kevin_priv_key pub_key master_key business_staff strategy_team 'executive_level=7#32' 'office=2362#32' 'hire_date=1742309083#32'
Vo Phat Thanh
Public key size: 439
g size: 33
gp size: 65
Master key size: 105
Keygen: Attribute: business_staff
dp: B2CC3C366A6DEB12 3668A7F55E78DC18 C50EE399EA57BE73 21B71DD488300FD6
6B3E506ACC6CFED2 C6B72FC5F533233 8552D93E44CF9906 00FF03581F3DD7C3
00000000000000 0000000000000000 0000000000000000 0000000000000001

d: 11CE8B1B7C678FC9 48FBF339793A2C39 EE009CB61B037B1A 12F4F33474A9C6C2
A71E690781BC36FC 0604E0AAD2D838EF B3993A8831FC93DD D0969091427AF6EB
5214B024FCEFB51 5AC29A8B54E87C5D C6E314FF5688998D 2FFA464392F7F1E9
24385F9D11DA0674 64387AE340F075CA B461313CA6757607 74DFC33992C08829
00000000000000 0000000000000000 0000000000000000 0000000000000001
00000000000000 0000000000000000 0000000000000000 0000000000000000

Keygen: Attribute: strategy_team
dp: 668F8E973FA71C72 ABC76D4854867F4E 3E26FAE5C0A7CFA8 141E8D6956E3B09A
3CF8F664316881B6 CB74731144DB87D8 28606A032432BFC8 D981466D29588A77
00000000000000 0000000000000000 0000000000000000 0000000000000001

d: 3DBE67897A9867EB 2CC83D99502304E1 B5ACC51532240ACC 33F20BF34760561F
7109F70C4731096A EA28B0768C75802D FB62AAFC4E0AA19 58C8188656CD3D1A
AE70517F1BEC0E6F 0AE812BA3D19D6D9 0A1B2DD2E7AE43AD 3C026E6504AD269B
9A4A024230AAD27A 35A9B00095909EB0 70D816A27183FCFA CA9533DA32D61145
00000000000000 0000000000000000 0000000000000000 0000000000000001
00000000000000 0000000000000000 0000000000000000 0000000000000000

Keygen: Attribute: executive_level=7#32
dp: 6508CF996A5A299 CF08BA1F00E98FE C80CB23B425DA9B3 FADFESDAF6D985FA
27037651F60415F5 2558E5A6852C38D2 27F7CE99A118194D 9FB420AA46AA67B3
00000000000000 0000000000000000 0000000000000000 0000000000000001

```

Hình 2: Thực hiện keygen

```

Keygen: Attribute: office=2362#32
dp: AB3A404D3B13BA6B 5D31639B18059CA3 B0ECBBE140E727C5 BC952A86BE762201
60729B2BE5EB1C40 DBC4A2BC958A1CAE 26BAF0992C601316 7CD2FAE7475454F3
00000000000000 0000000000000000 0000000000000000 0000000000000001

d: A70E72D8031CCB9F BA15AA082922226A 4A14881790ABEDCA 2C7C7E198044F525
894F33DD13E2816D 6AC9E7D732710D73 5DF0DCE4F7DAC002 21602F914678921F
5610F680C4D67ED F541E08B11F020D0 FA28367BF800724 D3026DC0C9FAF99F
71002E552EC1705F 208D31E2B8A46BE2 09EC905CE6843E4E 0882F9BD0740BBCE
00000000000000 0000000000000000 0000000000000000 0000000000000001
00000000000000 0000000000000000 0000000000000000 0000000000000000

Keygen: Attribute: hire_date=1742309083#32
dp: 63963D880E6577C2 A96AC478E47FC89D 974346B46FC2BE69 EBA3979BFF493D38
0328D62018DC2A75 5FDBE920AA8F6130 D12C235900B9DE9B 98E163C0F2A7856F
00000000000000 0000000000000000 0000000000000000 0000000000000001

d: 9531BCF6756FD562 4FA6233BEEA90B47 45571627D7EFF2F1 FDB60DC75E1A741C
2438B052E39C4835 7D879ED9427C9621 1E08210848DF1766 82C6644E325E3A92
260A5EC11703E5AF 09FF3490CCC7233D 3329BC98067FD28D 143BC55C83DCE963
3C71D49F1160148D 86F5C520819836FC BF65C59BE9D40C86 5BDE5117BEEFBEC5
00000000000000 0000000000000000 0000000000000000 0000000000000001
00000000000000 0000000000000000 0000000000000000 0000000000000000

Debug: Number of attributes added = 5
Generated Private Key attributes:
Attribute 0: business_staff
Attribute 1: strategy_team
Attribute 2: executive_level=7#32
Attribute 3: office=2362#32
Attribute 4: hire_date=1742309083#32

```

Hình 3: Các thuộc tính được thêm thành công

Bước mã hóa (encrypt) sử dụng chính sách truy cập dạng ngưỡng "5of5" bao phủ toàn bộ các thuộc tính. Hệ thống đã tính toán thành công giá trị AES key ngẫu nhiên để mã hóa nội dung tệp, và giá trị này được bảo vệ bởi CP-ABE thông qua các thành phần bản mã $C, C', \{C_i, C'_i\}$. Kết quả log cho thấy các thuộc tính được ánh xạ đúng và các thành phần bản mã đã được tạo và tuần tự hóa theo đúng cấu trúc định sẵn.

```

(thanh@kali)~[/Documents/demo_cpabe_relic]
$ cpabe-enc pub_key security_report.pdf \
"business_staff strategy_team executive_level=7#32 office=2362#32 hire_date=1742309083#32 5of5"
Vo Phat Thanh
Pairing parameters in encryption:

-- Curve BN-P256:
g size: 33
gp size: 65
Public key loaded successfully (size: 439 bytes).
Public key element g in encryption:
B6400000000FF2F 2200000085FD5480 B0001F44B6888BF1 42BC818F95E3E6AE
00000000000000 0000000000000000 0000000000000000 0000000000000004
00000000000000 0000000000000000 0000000000000000 0000000000000001

Public key element gp in encryption:
0C77AE4A1D6E1451 66739CF23DAFACA9 DD396E9046424FC5 479BD57692904538
8D1705845D9EAA07 8A9198FD8D76E201 3D18C11984D95721 A8D32F819A544F51
A906E963E4988478 E458A4959EF7D61B 570358814E28A04E F988C794064D73A7
A033144CA161E3E3 27162483F0CC1CE6 07ACD2CBC9E9253 C732CF3E1010DEE7
00000000000000 0000000000000000 0000000000000000 0000000000000001
00000000000000 0000000000000000 0000000000000000 0000000000000000

Enc: Public key elements before pairing:
g: B6400000000FF2F 2200000085FD5480 B0001F44B6888BF1 42BC818F95E3E6AE
00000000000000 0000000000000000 0000000000000000 0000000000000004
00000000000000 0000000000000000 0000000000000000 0000000000000001

gp: 0C77AE4A1D6E1451 66739CF23DAFACA9 DD396E9046424FC5 479BD57692904538
8D1705845D9EAA07 8A9198FD8D76E201 3D18C11984D95721 A8D32F819A544F51
A906E963E4988478 E458A4959EF7D61B 570358814E28A04E F988C794064D73A7
A033144CA161E3E3 27162483F0CC1CE6 07ACD2CBC9E9253 C732CF3E1010DEE7
00000000000000 0000000000000000 0000000000000000 0000000000000001
00000000000000 0000000000000000 0000000000000000 0000000000000000
AES key (size: 128): 0C77AE4A1D6E1451 66739CF23DAFACA9 DD396E9046424FC5 479BD57692904538

```

Hình 4: Thực hiện enc

```

(thanh@kali)~[/Documents/demo_cpabe_relic]
$ cpabe-dec security_report.pdf \
"business_staff strategy_team executive_level=7#32 office=2362#32 hire_date=1742309083#32 5of5"
Vo Phat Thanh
Pairing parameters in decryption:

-- Curve BN-P256:
g size: 33
gp size: 65
Public key loaded successfully (size: 439 bytes).
Public key element g in encryption:
B6400000000FF2F 2200000085FD5480 B0001F44B6888BF1 42BC818F95E3E6AE
00000000000000 0000000000000000 0000000000000000 0000000000000004
00000000000000 0000000000000000 0000000000000000 0000000000000001

Public key element gp in encryption:
0C77AE4A1D6E1451 66739CF23DAFACA9 DD396E9046424FC5 479BD57692904538
8D1705845D9EAA07 8A9198FD8D76E201 3D18C11984D95721 A8D32F819A544F51
A906E963E4988478 E458A4959EF7D61B 570358814E28A04E F988C794064D73A7
A033144CA161E3E3 27162483F0CC1CE6 07ACD2CBC9E9253 C732CF3E1010DEE7
00000000000000 0000000000000000 0000000000000000 0000000000000001
00000000000000 0000000000000000 0000000000000000 0000000000000000

Enc: Public key elements before pairing:
g: B6400000000FF2F 2200000085FD5480 B0001F44B6888BF1 42BC818F95E3E6AE
00000000000000 0000000000000000 0000000000000000 0000000000000004
00000000000000 0000000000000000 0000000000000000 0000000000000001

gp: 0C77AE4A1D6E1451 66739CF23DAFACA9 DD396E9046424FC5 479BD57692904538
8D1705845D9EAA07 8A9198FD8D76E201 3D18C11984D95721 A8D32F819A544F51
A906E963E4988478 E458A4959EF7D61B 570358814E28A04E F988C794064D73A7
A033144CA161E3E3 27162483F0CC1CE6 07ACD2CBC9E9253 C732CF3E1010DEE7
00000000000000 0000000000000000 0000000000000000 0000000000000001
00000000000000 0000000000000000 0000000000000000 0000000000000000

AES key (size: 128): 0C77AE4A1D6E1451 66739CF23DAFACA9 DD396E9046424FC5 479BD57692904538
Decrypted data (size: 1024): 4db07222398b149a6fale85235b959ee985f31/e
Value of q->coeff[0]: 8e640e2f2f3682e07409d31642f0206005baf6f9a2d0c5b9dbd687ef1f72115
DEBUG fill_policy: Mapped attribute 'strategy_team' in G1: 03248dc25e9ac5d3548dc2f3645a2e3a3d0fb0393113383ed9c6dfe72a75854965
DEBUG fill_policy: Mapped attribute 'strategy_team' in G2: 026377d45aefc243d11a3d3c728c51b93846d3c3dca674bf42565738a17f3226b56e383d623ec
dc7bc66bd6d42edebb53a18de03be021811cfca331f639fed48db
DEBUG fill_policy: p->c for 'strategy_team': 02756be3cd011467c49ca42c36157776e0eb30d3836973b774b2ff8fd18a4e713c
DEBUG fill_policy: p->cp for 'strategy_team': 023774bb60afc7ed295acddc61a5d1e72567373c9d63e02ad29f689e078aff2fa5994c9f0f14199f8313ccfded
4d59c4417c6b4aded82df61125c9ad00f053ba49
Value of q->coeff[0]: 4f05680ff39e7c62a15041448c478ecb821fa3380cb7aa9c8c680ccd7c045fef
DEBUG fill_policy: Mapped attribute 'executive_level=7#32' in G1: 036e0546557376da48fb10e3fe0269d199902f902027a88a8cce407c0612799b4c
DEBUG fill_policy: Mapped attribute 'executive_level=7#32' in G2: 02860c192ef8723a0735cb5dbd191ac7367481a9daf5581ad64b1477fba9b1ad9104b
c96b887c0b14b170e0d528463ab86c1b808dd9b6d5c1d3244049f1262d7
DEBUG fill_policy: p->c for 'executive_level=7#32': 02228432c6390e13a1ae356fa78018958a7916a3fdf21197abdb42c819c6bab68
DEBUG fill_policy: p->cp for 'executive_level=7#32': 020e39d6e44db69adaee45fb983854a78f59a5fc5fd2bcfd13305ef24e7b15b0aea646f5bfe425ff1
5ed8834a1755c6e1aeadc54298aea4e6296b85e5e4580c
Value of q->coeff[0]: 44b969cdf552b061e1b0e9855873d4edbe35a815ca37925fa37cd445d5be1e13
DEBUG fill_policy: Mapped attribute 'office=2362#32' in G1: 029f54663e75f78709652ee174a07cbb5f603b3b1f4eaa5ef49fa6b78f0314cad1
DEBUG fill_policy: Mapped attribute 'office=2362#32' in G2: 03102c3951fa22e7de2016fafdd1436108c5d1c05c91fbe201f59d1354933b10d54cd13cdc2
173598d9ec2272610cd487129034b8ec543be6b64a436fa7b6cf17
DEBUG fill_policy: p->c for 'office=2362#32': 035372881b9679033ac66ab35a5d811822eeb8179d2701aa59e799e8994c83bd39
DEBUG fill_policy: p->cp for 'office=2362#32': 03ac6d15c3f961891badc52e565f5cd90ef664bf696d09f3ba55289104a72c19752b5e6662c096662c3ec590
fd3a85b275a6b03cd10fd3519e798149d96ec5167
Value of q->coeff[0]: 7e59c5354226a9792479c95a1ad90daf8b6ff7173e1a78d35287c83ca97ab3
DEBUG fill_policy: Mapped attribute 'hire_date=1742309083#32' in G1: 023ade13809fc816cd06506cffa3d3e363ec74291e4cef0a9b06d7b42972d7f810
DEBUG fill_policy: Mapped attribute 'hire_date=1742309083#32' in G2: 029b8307eabfca34b1472b0bb512ce8ac1d7666a92d8644afc5806dc035194c0610
2bc770e6f9dacbd57164d72a963c23a3bc7deb5cf145cdc718c43f2cf52ff64
DEBUG fill_policy: p->c for 'hire_date=1742309083#32': 039be0d955508d94a2688a84cb9c2cbb2eaf2f0ee0d3097cc44c74969938d2db42
DEBUG fill_policy: p->cp for 'hire_date=1742309083#32': 02a3e592fdeb598ce80581a80686305f66a04209503fdd0476f6977fd9024d527638a0cc9749906e
99f94e7944e1daf1fd06c0904942a51565b09b9397781460d0

```

Hình 5: Fill các policy và tính AES key

Ở bước giải mã (decrypt), quá trình khôi phục khóa AES từ bản mã diễn ra đúng như lý thuyết: thuật toán thực hiện kiểm tra thỏa mãn chính sách, tính toán các hệ số Lagrange, thực hiện các phép pairing và khai triển công thức khôi phục khóa như:

$$K = \frac{e(C', D)}{\prod_{i \in S'} e(C_i, d') \cdot e(C'_i, d_i)}$$


```
Kali Linux 2024 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Apr 17 1:00 AM
thanh@kali: ~/Documents/demo_cpabe_relic

(thanh@kali)~/Documents/demo_cpabe_relic
$ cpabe-dec pub_key kevin_priv_key security_report.pdf.cpabe
Vo Phat Thanh
g size: 33
gp size: 65

ERROR in ep_read_bin() at /home/thanh/Documents/relic/src/ep/relic_ep_util.c:286: invalid value passed as input.
Before IV: offset=0, need=12, file_len=9727
Before tag: offset=12, need=16, file_len=9727
Before sym_len: offset=28, need=4, file_len=9727
Before abe_len: offset=32, need=4, file_len=9727
DEBUG (dec): cph_buf->len = 1179, expected = 1179
AES key (dec read from file): ec045e481f0d62e49b8752d6fc24d20
[check_sat] leaf: policy_attr='business_staff', key_attr='business_staff'
[check_sat] match => satisfiable=1, attri=0
[check_sat] leaf: policy_attr='strategy_team', key_attr='business_staff'
[check_sat] leaf: policy_attr='strategy_team', key_attr='strategy_team'
[check_sat] match => satisfiable=1, attri=1
[check_sat] leaf: policy_attr='executive_level=7#32', key_attr='business_staff'
[check_sat] leaf: policy_attr='executive_level=7#32', key_attr='strategy_team'
[check_sat] leaf: policy_attr='executive_level=7#32', key_attr='executive_level=7#32'
[check_sat] match => satisfiable=1, attri=2
[check_sat] leaf: policy_attr='office=2362#32', key_attr='business_staff'
[check_sat] leaf: policy_attr='office=2362#32', key_attr='strategy_team'
[check_sat] leaf: policy_attr='office=2362#32', key_attr='executive_level=7#32'
[check_sat] leaf: policy_attr='office=2362#32', key_attr='office=2362#32'
[check_sat] match => satisfiable=1, attri=3
[check_sat] leaf: policy_attr='hire_date=1742309083#32', key_attr='business_staff'
```

Hình 6: Thực hiện dec và check các thuộc tính

```
Kali Linux 2024 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Apr 17 1:02 AM
thanh@kali: ~/Documents/demo_cpabe_relic

ce28488e1b61e0f47fa7c4d343300f57d5fc25afb7579c6213fba6f2e9fa452d9d1e3923cc3b0bbc2471f9bfc7eea2313e3adf768b4e470a837784876bdafdf05f3a7d6
8e38bfe22eb9373fb353ad88cca9fa05256dc368465f75c8f32fc939f4de665d7cbf4a6828276e30b1fbac72545b9b9cc0b58b414b7f11560e94f75c31c8c16feac0341
1a4ee18e9549aa9f88139350745c03a4b2f861fad206d33d72d58a8a3aad5e736792a4f21a42ca2ad1d6a7495230c89c9ff108122711f939c813992ad4ad71047921
3cfe0198617f0d42ec8f938b
p->c: 039be0d95508d94a2688a84cb9c2cbb2eaf2f0ee0d3097cc44c74969938d2db42
c->d: 029531bcf6756fd5624fa6233beea9db4745571627d7eff2f1fd860dc75e1a741c243bb052e39c40357d879ed9427c96211e0b210848df176682c664e325e3492
c->dp: 0263963d880e6577c2a96ac478e47f89d974346b46fc2be69eba3979bfff493d38
p->cp: 02a3e592fdeb598ce80581a80686305f66a04209503fdd0476f6977fd9024d527638a0cc9749906e99f94e7944e1daf1fd06c0904942a51565b09b9397781460d
0
[dec_node_naive] leaf => p->attr='hire_date=1742309083#32', attri=4
[dec_node_naive] Lambda coefficient for index 5: 1
[dec_node_naive] Intermediate temp after exponentiation: 8745daa8b422b7ec325f79db686ff802c3f89958f1ad25fb68b143cc115cd4724cd11dae2f1ddfc
c983e9cfcaeeec38c7b23bc264db6dc1cad73fa8f8c704ba8306c3bc68bd33117b858c5e5c5ba7597069b14c1937ed13b400f21875376b61cab1372bca0cc3f2e5b1bd
6ca6491e97f3c56755a7b473081d75ea071aefdf03cb7923ddb357150866c61b276eb70205f9bca320ad733e20dc9e54737d8135909b778d6c1306e578187c5326eb2e42
4721bc060971d6035c07b01f5706600c5b7846a635ebc7dc334d5bffc93404a1304dd29ea437b13e05791d6e348d4b2b5d14784dd014157c2c19cd76284604b7ad6a50
de8713397fddc411228df7f3f1
Value of F: aeec28c5a4e8512f66bda4df947cf8729691dc52371120055c9f59e5dd4962374a3acc9fe977cd82ff79bfe72af4ac13dbc11996cac0c32c46e3c6750e6f
ca448ada86a984f779b8cbd7f8ef1048a679e1ee19ab43e4d8ed752600a0658ec358c2b597eac658ff96a09d1f6702f6797c7cea97b57f45e4d75e432d114b04fb76d2e
784aab4b7d58f643f5762259f0da1b2ee01906f9c56270182d69164a1c7be5a4102b9a5d88ab3d2ee640a74a0b39418fde323a5ed61394874d4e28897b39247068f92d
c1b9a5eeaf9aaf651db058494cb6bbba55db505e53ac443fa8ec2026e0dd8e649d072e650eba8cad311da8fcf75daa495793e27e3be5a6082ec1
Value of m (dec): 0e2c25272b4145da0a20d6972da200990292ca9b7f74187c901a8f7602c00b321e90252979a0323b3d7b9b6143ebb5e19e0cfc23909e8ba42c5876
c2913d694ba1011c2c4e85a480ef19ad981e63c4fc87f23028a02e4083a34e29ae7d61e47b2a96b42d7efb481be11220df787841ca504efe8fcbbcb02f6dde2f481b4d75d
943565b24e2f89af199f968ae7744b39d6cc54ae107ba4fb67c40048a6b83718da29b9900913a45e51b2e523cbaee513aeec38972324a95a1c6c30b6c9d988bd229a7412
1a043e71a854e79d801df50dc77eaf5a65fb37c4e6ec6ba21ab9413cfff170c5e5c1742aff921e750281bd00fe3910f79fc1b108ebfb9c66b2412ab2dc2
AES key (dec computed): 8eb8e4d02c0b9e4bef4b53c9e1c4219b
IV: bf008f6068157cecca7129eb
Tag: d468681a040f686e28f278df3fd9ee4b
AES-GCM authentication failed! Possible incorrect key.
```

Hình 7: Lỗi AES-GCM authentication failed

Kết quả cho thấy giá trị $F = \frac{e(C,D)}{\prod_i e(C_i', D_i)}$ được tính ra trùng khớp với giá trị $e(g_1, g_2)^{as}$, tuy nhiên khi giải mã AES-GCM, hệ thống thông báo lỗi “AES-GCM authentication failed”, cho thấy có thể xảy ra một trong các lỗi sau: Sai sót khi serialize hoặc unserialize các thành phần bản mã; Lỗi ánh xạ không đồng nhất giữa mã hóa và giải mã; Sự không tương thích trong cấu trúc hoặc chỉ số chính sách.

Mặc dù quá trình mã hóa và giải mã ABE thành công về mặt toán học, lỗi thực thi AES cho thấy có thể có vấn đề trong bước khôi phục chính xác khóa phiên (session key) hoặc truyền sai IV, tag trong dữ liệu mã hóa.

Tóm lại, hệ thống đã cho thấy tính hoàn chỉnh về mặt thuật toán, với tất cả các bước của CP-ABE được triển khai và hoạt động ổn định. Tuy nhiên, lỗi thực thi trong giai đoạn giải mã AES đã mở ra một hướng cần kiểm tra và hiệu chỉnh kỹ hơn về việc lưu trữ và đọc tuần tự bản mã, đồng thời cho thấy tầm quan trọng của việc tích hợp chính xác giữa mã hóa thuộc tính và mã hóa đối xứng.

3.3 Ưu điểm, nhược điểm và hướng phát triển

Sau quá trình triển khai CP-ABE bằng thư viện mật mã RELIC, hệ thống đã thể hiện được nhiều điểm mạnh cả về mặt lý thuyết lẫn thực nghiệm. Tuy nhiên, bên cạnh đó vẫn tồn tại một số điểm cần cải tiến để đáp ứng các yêu cầu khắt khe hơn trong thực tế ứng dụng. Phần này trình bày tổng quan những ưu điểm, nhược điểm và một số định hướng phát triển cho hệ thống trong tương lai.

3.3.1 Ưu điểm

Một trong những ưu điểm đáng kể nhất là khả năng kiểm soát truy cập chi tiết và linh hoạt. CP-ABE cho phép người mã hóa đính kèm một chính sách truy cập bất kỳ vào bản mã, trong khi người dùng chỉ có thể giải mã nếu thuộc tính của họ đáp ứng chính sách đó. Cơ chế này vượt trội hơn hẳn so với các phương pháp mã hóa khóa công khai truyền thống, vốn thường yêu cầu quản lý khóa trực tiếp giữa các bên.

Bên cạnh đó, việc sử dụng thư viện RELIC giúp tăng hiệu suất thực thi hệ thống một cách rõ rệt. RELIC cung cấp hỗ trợ mạnh mẽ cho các phép toán đường cong elliptic và pairing loại III — loại pairing có khả năng đảm bảo bảo mật cao hơn và giảm sự phụ thuộc vào các phép đẳng cấu. Các kỹ thuật như sextic twist, phép toán trên trường $\mathbb{F}_{p^{12}}$, và khả năng tối ưu hóa lũy thừa cuối cùng (final exponentiation) đã giúp giảm thiểu thời gian thực hiện các phép pairing, vốn là bước tiêu tốn nhiều chi phí nhất trong CP-ABE. Trong các thử nghiệm thực tế được trích từ tài liệu A Minimization Number of Final Exponentiations, việc tối giản số lần lũy thừa cuối cùng trong quá trình pairing có thể giảm thời gian tổng thể tới 30-40%, tùy thuộc vào cấu hình phần cứng và kỹ thuật cụ thể được áp dụng.

Về mặt tổ chức, hệ thống được xây dựng theo hướng mô-đun, với bốn thành phần rõ ràng: setup, keygen, encrypt và decrypt. Mỗi thành phần đảm nhiệm một vai trò cụ thể, vừa đảm bảo khả năng tái sử dụng mã nguồn, vừa thuận tiện cho việc mở rộng và kiểm thử. Ngoài ra, việc sử dụng hàm băm ánh xạ lên đường cong elliptic giúp ánh xạ thuộc tính từ chuỗi ký tự thành phần tử trên nhóm \mathbb{G}_1 , qua đó mở rộng khả năng biểu đạt chính sách và hỗ trợ các loại thuộc tính đa dạng.

3.3.2 Nhược điểm

Tuy nhiên, hệ thống vẫn còn tồn tại một số nhược điểm đáng lưu ý. Trước hết, chi phí tính toán vẫn còn cao, đặc biệt là ở các bước pairing và nhân vô hướng (scalar multiplication) trên đường cong elliptic. Khi số lượng thuộc tính trong chính sách tăng lên, thời gian mã hóa và giải mã tăng tuyến tính theo. Điều này gây trở ngại nếu triển khai trên các thiết bị tài nguyên giới hạn như cảm biến IoT hay thiết bị nhúng. Theo các thống kê định lượng từ tài liệu tham khảo, quá trình pairing có thể chiếm tới 70% tổng thời gian giải mã, trong khi đó scalar multiplication chiếm khoảng 20%.

Ngoài ra, hiện tại hệ thống chưa hỗ trợ chính sách truy cập động, như các biểu thức logic phức tạp nhiều lớp, truy vấn theo thời gian, hoặc theo ngữ cảnh. Mức độ bảo mật mới chỉ dừng lại ở mô hình CPA (Chosen Plaintext Attack), chưa có cơ chế chống tấn công CCA (Chosen Ciphertext Attack). Việc cập nhật chính sách truy cập hoặc thu hồi khóa bí mật của người dùng vẫn chưa được thực hiện một cách linh hoạt.

3.3.3 Định hướng phát triển

Từ những đánh giá nêu trên, có thể đề xuất một số định hướng phát triển cho hệ thống trong tương lai. Thứ nhất là tối ưu hóa hiệu năng, bằng cách áp dụng kỹ thuật tính toán trước (precomputation), lũy thừa song song (multi-exponentiation), hoặc pairing hàng loạt (batch pairing). Những kỹ thuật này đã chứng minh hiệu quả trong việc giảm chi phí mã hóa/giải mã ở các hệ thống lớn. Thứ hai là mở rộng khả năng biểu đạt chính sách truy cập, chẳng hạn như tích hợp cây truy cập động, các điều kiện ngữ nghĩa, hoặc các chính sách ràng buộc theo thời gian. Thứ ba là nâng cao mức độ bảo mật, thông qua việc tích hợp mô hình xác thực mạnh hơn hoặc triển khai theo mô hình phân tán với nhiều authority (multi-authority CP-ABE). Cuối cùng, hệ thống cũng có thể được tích hợp với các nền tảng lưu trữ phân tán hiện đại như blockchain, IPFS hoặc cloud

storage để đáp ứng nhu cầu bảo mật trong môi trường chia sẻ dữ liệu rộng lớn.

Tóm lại, việc triển khai CP-ABE bằng thư viện RELIC không chỉ giúp khai thác các lợi thế về hiệu năng và tính linh hoạt mà còn mở ra nhiều cơ hội nghiên cứu và ứng dụng trong các lĩnh vực yêu cầu kiểm soát truy cập chi tiết và bảo mật cao. Với các định hướng phát triển rõ ràng và phù hợp, hệ thống hoàn toàn có tiềm năng trở thành một giải pháp mã hóa mạnh mẽ và thực tiễn trong tương lai.

TÀI LIỆU THAM KHẢO

- [1] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-Policy Attribute-Based Encryption,” in *2007 IEEE Symposium on Security and Privacy (SP '07)*, Berkeley, CA: IEEE, May 2007, pp. 321–334. doi: 10.1109/SP.2007.11.
- [2] A. Sahai and B. Waters, “Fuzzy Identity-Based Encryption,” in *Advances in Cryptology – EUROCRYPT 2005*, vol. 3494, R. Cramer, Ed., in Lecture Notes in Computer Science, vol. 3494. , Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 457–473. doi: 10.1007/11426639_27.
- [3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data,” 2006, 2006/309. Accessed: Apr. 17, 2025. [Online]. Available: <https://eprint.iacr.org/2006/309>
- [4] B. Lynn, “ON THE IMPLEMENTATION OF PAIRING-BASED CRYPTOSYSTEMS”.
- [5] L. H. Anh, Y. Kawada, S. Huda, Md. A. Ali, Y. Koderu, and Y. Nogami, “ELiPS-based Ciphertext-Policy Attribute-Based Encryption,” *Int. J. Netw. Comput.*, vol. 14, no. 2, pp. 186–205, 2024, doi: 10.15803/ijnc.14.2_186.
- [6] L. H. Anh, Y. Kawada, S. Huda, Md. A. Ali, Y. Koderu, and Y. Nogami, “A Minimization Number of Final Exponentiations and Inversions for Reducing the Decryption Process Time in ELiPS-Based CP-ABE,” *J. Adv. Inf. Technol.*, vol. 15, no. 6, pp. 748–755, 2024, doi: 10.12720/jait.15.6.748-755.
- [7] L. Cheung and C. Newport, “Provably secure ciphertext policy ABE,” in *Proceedings of the 14th ACM conference on Computer and communications security*, Alexandria Virginia USA: ACM, Oct. 2007, pp. 456–465. doi: 10.1145/1315245.1315302.
- [8] L. H. Anh, Y. Kawada, S. Huda, Md. A. Ali, Y. Koderu, and Y. Nogami, “An implementation of ELiPS-based Ciphertext-Policy Attribute-Based Encryption,” in *2023 Eleventh International Symposium on Computing and Networking Workshops (CANDARW)*, Matsue, Japan: IEEE, Nov. 2023, pp. 220–226. doi: 10.1109/CANDARW60564.2023.00044.
- [9] Lê Phi Thường, Lê Đình Hải, Trịnh Việt Cường, and Lê Xuân Lâm, “HỆ MÃ HÓA DỰA TRÊN THUỘC TÍNH MỚI HỖ TRỢ TÍNH CHẤT PHI TẬP TRUNG HÓA”.

- [10] Z. Cao and L. Liu, “On the Disadvantages of Pairing-based Cryptography,” 2015, 2015/084. Accessed: Apr. 18, 2025. [Online]. Available: <https://eprint.iacr.org/2015/084>