**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**


**TRỊNH VĂN ANH**

# MỘT SỐ HỆ MÃ HÓA VỚI QUYỀN GIẢI MÃ LINH ĐỘNG

**Chuyên ngành : Hệ thống thông tin**

**Mã sô : 9.48.01.04**

**TÓM TẮT LUẬN ÁN**

**TIẾN SĨ HỆ THỐNG THÔNG TIN**

**Hà Nội – Năm 2021**

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**TRỊNH VĂN ANH**

# MỘT SỐ HỆ MÃ HÓA VỚI QUYỀN GIẢI MÃ LINH ĐỘNG

**Chuyên ngành: Hệ thống thông tin**

**Mã số: 9.48.01.04**

**TÓM TẮT LUẬN ÁN TIẾN SĨ KỸ THUẬT**

**NGƯỜI HƯỚNG DẪN KHOA HỌC:**

**1. GS.TS. Nguyễn Bình**

**2. TS. Hồ Văn Hương**

**HÀ NỘI – NĂM 2021**

# MỞ ĐẦU

Mật mã đã được phát triển và dùng từ hàng ngàn năm nay, với mục tiêu ban đầu là cho phép người gửi gửi thông tin một cách an toàn tới người nhận thông qua một kênh không an toàn. Để thực hiện điều đó, người gửi và người nhận thống nhất trước với nhau một khóa bí mật chung ban đầu. Thông tin trước khi gửi sẽ được biến đổi (gọi là mã hóa) dựa trên khóa bí mật chung này sang một dạng khác không có ý nghĩa, gọi là bản mã. Tiếp theo bản mã sẽ được gửi tới người nhận thông qua kênh không an toàn. Người nhận cuối cùng dựa trên khóa chung này để chuyển bản mã thành dạng thông tin ban đầu (gọi là giải mã) có ý nghĩa. Các kẻ tấn công có thể dựa trên kênh truyền không an toàn để lấy được bản mã, nhưng do không biết khóa bí mật chung của người gửi và người nhận nên không thể nào giải mã được. Một hệ thống với các bước gửi nhận thông tin như vậy được gọi là một hệ mã hóa.

**Lý do chọn đề tài:**

Trong thực tiễn, an toàn thông tin đang là vấn đề cấp bách của xã hội, việc xác định cách bảo mật, cách xây dựng hệ thống an toàn thông tin tránh hiện tượng mất cắp, rò rỉ thông tin đang được các nhà khoa học nghiên cứu và đây cũng là vấn đề đang được nước ta và các quốc gia trên thế giới đặc biệt quan tâm. Việc để những thông tin mật, thông tin quan trọng bị xâm hại trái phép là mối nguy hiểm cho toàn bộ người dùng, cơ quan, tổ chức.

Để giải quyết vấn đề an toàn thông tin cho các hệ thống, kỹ thuật được dùng cơ bản hiện nay là các hệ mã hóa. Tuy nhiên trong các hệ thống thực tế ngày nay, yêu cầu về các dạng mã hóa phải linh động và đa dạng hơn. Ví dụ, với hệ thống truyền hình trả tiền hay radio cho quân đội, trung tâm phát sóng sẽ mã hóa sóng trước khi phát và rất nhiều người dùng với các đầu thu của mình có thể giải mã sóng để xem (hoặc nghe). Như vậy trong trường hợp này mã hóa không còn ở dạng 1-1 (tức là thông tin chỉ hiểu được hay giải mã được bởi một người nhận duy nhất) mà là 1-n với n > 1 là số người dùng có khả năng giải mã. Dĩ nhiên cách đơn giản để chuyển từ mã hóa 1-1 sang 1-n là cho phép n người dùng cùng biết một khóa bí mật, tuy nhiên vấn đề nảy sinh là hệ thống không thể loại bỏ một đầu thu không cho phép giải mã nữa (ví dụ đầu thu này hết hạn không nạp tiền thuê bao) mà không ảnh hưởng đến các đầu thu khác, vì các đầu thu cùng chia sẻ chung một khóa bí mật. Để giải quyết vấn đề này kỹ thuật mã hóa quảng bá (Broadcast encryption) đã được giới thiệu bởi Fiat and Naor [28], trong đó hệ thống cho phép mỗi đầu thu sở hữu một khóa bí mật khác nhau, ở mỗi lần mã hóa trung tâm phát sóng có thể dễ dàng loại bỏ những đầu thu cụ thể khỏi tập các đầu thu có thể giải mã được. Cụ thể ở mỗi lần mã hóa bản mã $m$ trung tâm phát sóng có thể chọn tùy ý một tập người dùng S có khả năng giải mã.

Phan và các tác giả [47] đã giới thiệu mã hóa quảng bá đa kênh (multi-channel broadcast encryption) là mở rộng khái niệm của mã hóa quảng bá từ việc gửi một thông tin $m$ đến một nhóm người dùng $S$, đến việc cho phép cùng lúc gửi nhiều thông tin $m_1, m_2, \ldots, m_k$ đến các tập người dùng khác nhau tương ứng $S_1, S_2, \ldots, S_k$, và người dùng trong tập nào thì chỉ có thể giải mã được bản mã mã hóa cho tập đó.

Một loại hệ mã hóa khác là mã hóa dựa trên thuộc tính (Attribute-based encryption), được giới thiệu bởi Sahai và Waters [53], là mở rộng của mã hóa quảng bá, trong đó cho phép điều kiện giải mã linh động hơn so với mã hóa quảng bá.

Ngày nay với sự phát triển của mạng vạn vật (Internet of Things), các thiết bị tham gia hệ thống có thể có năng lực rất yếu, dẫn đến các hệ mã hóa quảng bá, mã hóa quảng bá đa kênh và mã hóa dựa trên thuộc tính ngoài yêu cầu đảm bảo về an toàn phải thực sự đảm bảo về mặt hiệu quả, đặc biệt là ở ba tính chất là độ dài bản mã, độ dài khóa bí mật và tốc độ giải mã.

Để giải quyết một số tồn tại trong mã hóa quảng bá, mã hóa quảng bá đa kênh và mã hóa dựa trên thuộc tính. Nghiên cứu sinh chọn đề tài nghiên cứu "*Một số hệ mã hóa với quyền giải mã linh động*".

**Mục tiêu nghiên cứu:**

Đề tài tập trung nghiên cứu các hệ mã hóa quảng bá, các hệ mã hóa quảng bá đa kênh và các hệ mã hóa dựa trên thuộc tính, nhằm đạt được các mục tiêu chính sau đây:

1. Nắm bắt được tổng quan tình hình nghiên cứu hiện nay của một số loại mã hóa như: Mã hóa quảng bá, mã hóa quảng bá đa kênh và mã hóa dựa trên thuộc tính.

2. Xây dựng được lược đồ mã hóa quảng bá đa kênh mới, khắc phục được một số điểm yếu của hệ BE hiện có như: Tốc độ giải mã chậm, chỉ hệ thống mới có khả năng mã hóa.

3. Xây dựng được lược đồ mã hóa ABE mới có các tính chất như: Độ dài bản mã ngắn, độ dài khóa bí mật và tốc độ giải mã không quá dài, quá chậm, so với các hệ khác, hỗ trợ chức năng tìm kiếm trên dữ liệu đã được mã hóa.

**Đối tượng, phạm vi nghiên cứu và nội dung nghiên cứu:**

Đối tượng và phạm vi nghiên cứu trong luận án là các hệ mã hóa quảng bá, các hệ mã hóa quảng bá đa kênh và các hệ mã hóa dựa trên thuộc tính. Trong phạm vi đề tài này, Nghiên cứu sinh sẽ thực hiện các nội dung nghiên cứu sau đây:

1. Tìm hiểu một số kỹ thuật, đưa ra lược đồ mã hóa cải tiến để xây dựng hoàn thiện hơn cho hệ mã hóa quảng bá, hệ mã hóa quảng bá đa kênh.

2. Nghiên cứu lược đồ mã hóa quảng bá đa kênh mới, dựa trên các kỹ thuật xây dựng một số hệ mã hóa quảng bá khác như hệ mã hóa quảng bá Delerablee [25] và các cải tiến được viết tại các tài liệu [55, 56].

3. Tìm hiểu một số kỹ thuật về mã hóa dựa trên thuộc tính, đưa ra lược đồ mã hóa mới để góp phần xây dựng các hệ mã hóa dựa trên thuộc tính hiện nay được hiệu quả hơn.

4. Nghiên cứu lược đồ mã hóa dựa trên thuộc tính và một số kỹ thuật xây dựng hệ mã hóa quảng bá, mã hóa quảng bá đa kênh, đặc biệt tập trung vào việc xây dựng lược đồ mã hóa dựa trên thuộc tính, có tính chất là độ dài bản mã là hằng số và tìm kiếm trên dữ liệu đã được mã hóa.

5. Nghiên cứu mức an toàn của một số hệ mã hóa dựa trên thuộc tính hiện nay.

**Đóng góp của luận án**

1. Đóng góp thứ nhất: Đề xuất một lược đồ mã hóa quảng bá đa kênh dựa trên hệ Delerablee [25] có độ hiệu quả và an toàn tương tự như hệ [47, 15] nhưng ở dạng mã hóa công khai, không còn ở dạng bí mật. Được công bố tại công trình số 4.

2. Đóng góp thứ hai: Đề xuất lược đồ CP-ABE mới, có khóa bí mật ngắn hơn các hệ CP-ABE khác. Các hệ khác có cùng tính chất, độ dài bản mã là hằng số. Điểm yếu của đề xuất so với các hệ mã này là, có mức độ an toàn yếu hơn các hệ khác cso cùng tính chất. Nội dung đề xuất được công bố tại công trình số 4.

3. Đóng góp thứ 3: Đề xuất mới, dựa trên hệ ABE hiện có [42], xây dựng một lược đồ ABE mới hỗ trợ tìm kiếm trên dữ liệu đã được mã hóa; được công bố tại công trình số 2.

**Bố cục luận án:**

Luận án bao gồm 3 chương

Chương 1: **TỔNG QUAN VỀ MÃ HÓA**

Chương này Nghiên cứu sinh trình bày giới thiệu chung về một số hệ mã hóa cơ bản quan trọng đang được sử dụng hiện nay. Bao gồm ba loại hệ mã tiên tiến hiện nay là hệ mã hóa quảng bá, hệ mã hóa quảng bá đa kênh và hệ mã hóa dựa trên thuộc tính. Ba loại hệ mã hóa này hỗ trợ quyền giải mã linh động và đang được ứng dụng trong rất nhiều loại ứng dụng hiện nay như các ứng dụng truyền hình trả tiền, chia sẽ files, social network (facebooks, twitter,...), lưu trữ an toàn dữ liệu trên đám mây cho mọi loại ứng dụng như e-Health, chính phủ điện tử, ...

Chương 2: **MÃ HÓA QUẢNG BÁ ĐA KÊNH**

Chương này sẽ trình bày cụ thể chi tiết về mã hóa quảng bá đa kênh (multi-channel broadcast encryption) bao gồm định nghĩa chung về một hệ mã hóa quảng bá đa kênh, mô hình an toàn của một hệ mã hóa quảng bá đa kênh, một số hệ mã hóa quảng bá đa kênh quan trọng và các hạn chế đối với các hệ mã hóa quảng bá đa kênh hiện có. Phần cuối chương nghiên cứu sinh sẽ trình bày hệ mã hóa quảng bá đa kênh nghiên cứu sinh đề xuất nhằm khắc phục một số hạn chế này.

Chương 3: **MÃ HÓA DỰA TRÊN THUỘC TÍNH**

Chương này sẽ trình bày cụ thể chi tiết về hệ mã hóa dựa trên thuộc tính bao gồm định nghĩa chung về một hệ mã hóa dựa trên thuộc tính, mô hình an toàn của một hệ mã hóa dựa trên thuộc tính, một số hệ mã hóa dựa trên thuộc tính quan trọng hiện nay. Phần cuối chương sẽ trình bày 02 hệ mã hóa dựa trên thuộc tính mới do nghiên cứu sinh đề xuất.

# Chương 1
# TỔNG QUAN VỀ MÃ HÓA

Phần đầu chương, nghiên cứu sinh giới thiệu chung về ba loại mã hóa cụ thể hiện nay: Thứ nhất là mã hóa quảng bá, thứ hai là mã hóa quảng bá đa kênh và thứ ba là mã hóa dựa trên thuộc tính. Trong phần nội dung, tác giả trình bày chi tiết một số mã hóa quảng bá hiện nay mà luận án nghiên cứu, sau đó trình bày sơ lược kết quả nghiên cứu mới và các vấn đề tồn đọng cần khắc phục đối với ba loại mã này.

## 1.1 Mã hóa quảng bá và tổng quan tình hình nghiên cứu

Mã hóa quảng bá (BE) được giới thiệu bởi Fiat and Naor với mục tiêu tạo ra một hệ mã hóa mà ở mỗi lần mã hóa người mã hóa có thể chọn một tập người dùng tùy ý có thể giải mã được. Trong khi đó cả độ dài bản mã, độ dài khóa bí mật và tốc độ giải mã đều ở mức chấp nhận được.

**Hệ NNL** [44] và các cải tiến [26, 49]: là hệ mã hóa quảng bá khóa bí mật (tức là chỉ có ai biết khóa bí mật của người dùng mới có thể thực hiện được việc lập mã) dựa trên cấu trúc cây nhị phân, trong đó người dùng là các lá ở trên cây. Hệ NNL dùng hệ mã hóa khóa bí mật (ví dụ AES ) để mã hóa và giải mã nên tốc độ mã hóa và giải mã rất nhanh. Độ dài của bản mã và khóa bí mật là $r \cdot logN$ và $logN$ với hệ NNL-1; 2r-1 và $log^2N$ với hệ NNL-2, trong đó N là số tối đa người dùng trong hệ thống và $r$ là số người dùng không có khả năng giải mã đối với bản mã đó.

Một số cải tiến đối với hệ NNL như Dodis và Fazio [26] sử dụng kỹ thuật mã hóa dựa trên định danh, chuyển cả NNL-1 và NNL-2 sang hệ mã hóa quảng bá khóa công khai (tức là ai cũng có thể thực hiện việc mã hóa, sau này nghiên cứu sinh gọi tắt là hệ mã hóa quảng bá), nhưng với chi phí phải trả là hệ trở nên kém hiệu quả hơn do dùng IBE thay vì dùng hệ mã hóa khóa đối xứng để mã hóa và giải mã. Phan và Trinh [49] mở rộng hơn khi chuyển đổi NNL-1 sang dạng mã hóa quảng bá dựa trên định danh và độ dài khóa bí mật lúc này chỉ là hằng số, không phụ thuộc vào $r$ và $N$. Với việc dựa trên định danh, lúc này khóa công khai của mỗi người dùng trong hệ thống không còn là một con số ngẫu nhiên nữa, mà nó gắn liền với một định danh cụ thể của người dùng đó, ví dụ như số chứng minh thư hay địa chỉ email (hệ thống không còn cần dùng cơ sở hạ tầng khóa công khai để cấp chứng thư số cho khóa công khai của người dùng).

**Truy vết**: Các người dùng hợp lệ có thể dùng khóa bí mật của mình để tạo ra các thiết bị giải mã không hợp pháp, sau đó có thể bán thiết bị giải mã ở chợ đen với mục đích kinh tế. Để giải quyết vấn đề này cấp thẩm quyền phải có khả năng truy ngược lại được người dùng nào đã làm điều này. Một hệ mà hỗ trợ khả năng như vậy gọi là hệ hỗ trợ truy tìm dấu vết. Các hệ BE hỗ trợ truy vết hiệu quả nhất hiện nay là [44, 12, 1].

**Hệ BGW** [9] và các cải tiến [46, 10, 29]: dựa trên kỹ thuật phép ghép cặp đôi (Pairings) các tác giả đã đề xuất một hệ mã hóa quảng bá có độ dài bản mã và độ dài khóa bí mật là 2 và 1 phần tử, tốc độ giải mã có thời gian chấp nhận được. Tuy nhiên độ dài khóa công khai là khá lớn, phụ thuộc vào tổng số người dùng trong hệ thống. Các tác giả cũng đề xuất phương

pháp cân bằng (trade -off) giữa độ dài của bản mã và khóa công khai, khi cả hai cùng phụ thuộc vào căn bậc hai của tổng số người dùng trong hệ thống. Ngoài ra an toàn của hệ BGW khá yếu và dựa trên một giả thuyết mạnh. Gần đây các tác giả trong bài báo [29] dựa trên hệ BGW đã đề xuất một cải tiến trong đó họ đề xuất một hệ tương tự BGW nhưng có mức an toàn cao hơn (adaptive security) và dựa trên một giả thuyết yếu hơn, điểm yếu của hệ này là có độ dài khóa công khai dài hơn so với hệ BGW. Lưu ý các hệ kể trên đều không hỗ trợ truy vết.

**Hệ Delerablee** [25] và các cải tiến [55, 56]: dựa trên Parings, tác giả đề xuất một hệ mã hóa quảng bá có độ dài bản mã, độ dài khóa bí mật, độ dài khóa công khai và tốc độ giải mã tương tự như hệ BGW, tuy nhiên điểm mạnh là hệ Delerablee là hệ mã hóa quảng bá dựa trên định danh. Điểm yếu của hệ này là hệ đạt mức an toàn yếu (selective security) dưới một bài toán khó ở mức trung bình GDDHE, và ngoài ra hệ còn phải dựa vào giả thuyết là tồn tại hàm băm lý tưởng (random oracle). Hệ cũng không hỗ trợ truy vết.

**Vấn đề phân phối khóa**: trong các hệ mã hóa quảng bá, nhà quản trị hệ thống (authority) sẽ chịu trách nhiệm phân phối khóa bí mật cho các người dùng. Điều này dẫn đến hai vấn đề hoặc là hệ thống có thể bị tấn công dẫn đến hệ thống không hoạt động và các người dùng bị lộ khóa bí mật, hoặc tự bản thân quản trị hệ thống không trung thực. Để giải quyết vấn đề này có hai phương pháp đã được các nhà nghiên cứu đề xuất: một là chia nhỏ các hệ thống thành các hệ thống con [51, 42] (gọi là multi-authority), và người dùng phải nhận được tất cả các khóa bí mật thành phần từ các hệ thống con này để tạo ra khóa bí mật cho riêng mình; hai là chỉ cần một số lượng nhất định (lớn hơn một ngưỡng được quy định) các authority con phối hợp với nhau là có thể cấp khóa bí mật được cho người dùng [48] (decentralized authority).

**Vấn đề ẩn danh người nhận**: một hướng mở rộng khác của mã hóa quảng bá là vấn đề ẩn danh người nhận (anonymous broadcast encryption – mã hóa quảng bá ẩn danh) [13]. Tức là kẻ tấn công thu được bản mã nhưng từ bản mã không thể biết được ai là người có khả năng giải mã. Điều này có thể đảm bảo an toàn cho người nhận, đặc biệt trong các môi trường mang tính chất nhạy cảm về an ninh

### 1.2 Mã hóa quảng bá đa kênh và tổng quan tình hình nghiên cứu

Dựa trên hệ mã hóa quảng bá BGW, các tác giả ở [47] đã mở rộng khái niệm của mã hóa quảng bá từ việc gửi một thông tin m đến một nhóm người dùng S, đến việc cho phép cùng lúc gửi nhiều thông tin m1, m2, . . . , mk đến các tập người dùng khác nhau tương ứng S1, S2, . . . , Sk . Một hệ mã hóa như vậy được gọi là hệ mã hóa quảng bá đa kênh (Multi-channel BE - MCBE). Ứng dụng của MCBE trong thực tế ví dụ như truyền hình trả tiền khi mã mỗi thông tin mi như là một kênh, và mỗi tập Si là một nhóm người trả tiền đăng ký xem kênh đó, tức là trung tâm cùng lúc có thể phát sóng rất nhiều kênh. Các tác giả [47] đã đề xuất một hệ mã có độ dài bản mã chỉ 2 phần tử tương tự như hệ BGW (lưu ý rằng nếu dùng hệ BGW để gửi k thông tin khác nhau đến k tập người dùng khác nhau, độ dài bản mã sẽ là 2k), tuy nhiên điểm yếu của hệ mã này là tốc độ giải mã không hiệu quả và là hệ mã hóa quảng bá khóa bí mật. Hệ cũng không hỗ trợ traitor tracing. Các tác giả [60] đã cải tiến

hệ này bằng cách rút ngắn hơn độ dài của khóa công khai. Các tác giả [15] làm tăng hơn nữa an toàn và hiệu năng của hệ khi đưa ra xây dựng dựa trên Parings loại ba (Type 3 Parings). Rất gần đây các tác giả trong bài báo [3], đã giới thiệu hệ mã hóa quảng bá đa kênh mới có tính chất là mã hóa khóa công khai, tức là người lập mã không cần phải biết bất kỳ tham số bí mật gì khi thực hiện mã hóa.

### 1.3 Mã hóa dựa trên thuộc tính và tổng quan tình hình nghiên cứu

Mã hóa dựa trên thuộc tính (ABE) là hệ mã hóa mà cho phép quá trình mã hóa và giải mã có thể dựa trên thuộc tính. Mã hóa dựa trên thuộc tính được phân ra làm hai loại: thứ nhất là mã hóa dựa trên thuộc tính có chính sách ở bản mã (CP-ABE); loại thứ hai là mã hóa dựa trên thuộc tính có chính sách ở khóa (KP-ABE). Đối với CP-ABE, thông tin *m* sẽ được mã hóa dưới một chính sách  nào đó, ví dụ như:

(NV and PKT and e-H) or (NV and PCS and e-H)

Người dùng sở hữu tập thuộc tính nào sẽ nhận khóa bí mật tương ứng với tập thuộc tính đó, và miễn là tập thuộc tính thỏa mãn chính sách ở bản mã là người dùng có thể giải mã được. Ngược lại đối với KP-ABE, thông tin *m* sẽ được mã hóa dưới một tập thuộc tính, ví dụ như:

(NV, PKT, e-H)

Người dùng sẽ sở hữu một chính sách nào đó và nhận khóa bí mật tương ứng với chính sách đó. Và miễn là chính sách đó được thỏa mãn bởi tập thuộc tính ở bản mã là người dùng có thể giải mã được.

Với hệ mã hóa dựa trên thuộc tính ta có thể điểm qua một số hệ tiêu biểu với các ưu điểm khác nhau như sau. Hệ CP-ABE hoặc có độ dài bản mã là hằng số (constant size ciphertext) [21, 22, 8, 4, 15, 18], hoặc có độ dài khóa bí mật là hằng số [17, 16]. Trong đó các hệ [21, 22] chỉ hỗ trợ chính sách là And-gates hoặc Threshold, các hệ [8, 4, 15, 18] có thể hỗ trợ chính sách là chính sách linh động. Hệ ABE có tốc độ giải mã nhanh [6, 4, 5, 42], hệ ABE hỗ trợ truy viết kẻ phản bội[39], Decentralized (phi tập trung hóa) ABE hay Multi-authority (nhiều trung tâm cấp khóa) ABE [41, 19, 61, 51, 43]. Đối với vấn đề an toàn cho hệ mã, với sự kết hợp của kỹ thuật Pairing Encoding [7] và Dual system encryption (mã hóa cặp) [58], các hệ ABE đạt được bảo mật thích ứng và được xây dựng [6, 5, 4, 7]. Hệ ABE hỗ trợ general circuit được xây dựng từ multilinear maps [33] hay từ giả thuyết LWE [32].

Một hướng nghiên cứu mở rộng của ABE hiện nay đang rất được quan tâm là vấn đề tìm kiếm trên dữ liệu đã được mã hóa [11, 57, 14, 24, 37, 23, 59, 34, 45].

### 1.4 Kết luận chương 1

Trong chương này Nghiên cứu sinh trình bày tổng quát về ba loại hệ mã tiên tiến hiện nay là hệ mã hóa quảng bá, mã hóa quảng bá đa kênh và hệ mã hóa dựa trên thuộc tính. Ba loại hệ mã hóa này hỗ trợ quyền giải mã linh động và đang được ứng dụng trong rất nhiều loại ứng dụng hiện nay như các ứng dụng truyền hình trả tiền, chia sẽ files, social network (facebooks, twitter,...), lưu trữ an toàn dữ liệu trên đám mây cho mọi loại ứng dụng

như e-Health, chính phủ điện tử, ... Trong chương này nghiên cứu sinh cũng trình bày tình hình nghiên cứu hiện nay của ba loại hệ mã hóa này, cũng như các vấn đề mở đang được nghiên cứu và một số cách cách tiếp cận khả thi để giải quyết các vấn đề mở này.

# Chương 2: MÃ HÓA QUẢNG BÁ ĐA KÊNH

Trong chương này, nghiên cứu sinh trình bày về hệ mã hóa quảng bá đa kênh bao gồm: Định nghĩa chung về mã hóa quảng bá đa kênh, mô hình an toàn của một hệ mã hóa quảng bá đa kênh, một số hệ mã hóa quảng bá đa kênh quan trọng và các hạn chế đối với một số hệ mã hóa quảng bá đa kênh hiện nay. Phần cuối là nội dung cụ thể về lược đồ mã hóa quảng bá đa kênh do NCS đề xuất nhằm khắc phục một số hạn chế của mã hóa này.

## 2.1 Định nghĩa hệ mã hóa quảng bá đa kênh

Mã hóa quảng bá đa kênh được giới thiệu bởi Pointcheval và các tác giả [47] với mục tiêu mở rộng khái niệm của mã hóa quảng bá từ việc gửi một thông tin $m$ đến một nhóm người dùng $S$, đến việc cho phép cùng lúc gửi nhiều thông tin $m_1, m_2, \ldots, m_k$ đến các tập người dùng khác nhau tương ứng $S_1, S_2, \ldots, S_k$. Trong khi đó cả độ dài bản mã, độ dài khóa bí mật và tốc độ giải mã đều ở mức chấp nhận được.

Hệ [47] có nhược điểm là hệ mã hóa khóa bí mật, tức là người lập mã phải biết khóa bí mật của hệ thống. Ngoài ra tốc độ mã hóa và giải mã của hệ còn chậm.

## 2.2 Hệ mã hóa quảng bá đa kênh đề xuất

Trong khuôn khổ luận án này nghiên cứu sinh đề xuất một hệ mã hóa quảng bá đa kênh có các ưu điểm so với các hệ mã hóa quảng bá đa kênh khác như sau:

Là hệ mã hóa quảng bá đa kênh khóa công khai, tức là người lập mã không cần phải biết bất kỳ tham số bí mật gì khi thực hiện mã hóa.

Hệ mã có tốc độ giải mã nhanh. Cụ thể người giải mã chỉ cần tính 2 phép tính parings khi giải mã. Nghiên cứu sinh cũng cài đặt hệ mã và đưa ra các đánh giá cụ thể về thời gian chạy của hệ mã;

Hệ mã có độ dài bản mã Hdr chỉ gồm hai phần tử, độ dài khóa bí mật của người dùng có số lượng phần tử chính bằng số lượng kênh mà người dùng đăng ký để xem.

### 2.2.1 Ý tưởng xây dựng

Trong hệ [25], khóa bí mật của người dùng có dạng

$$g^{\frac{1}{\alpha+ID_u}}$$

Bản mã tương ứng với tập người dùng S có dạng

$$h^{k.\prod_{i\in S}(\alpha+ID_i)}$$

và miễn là $u \in S$ thì người dùng $u$ có thể tính được khóa phiên $e(g, h)^k$, $k$ là số ngẫu nhiên được chọn mỗi lần lập mã.

Trong ngữ cảnh của hệ mã hóa quảng bá đa kênh, chúng ta có $m$ tập người dùng (tương ứng với $m$ kênh) $S_1, \ldots, S_m$, và mỗi tập có một khóa phiên tương ứng. Ý tưởng là với mỗi tập người dùng $S_i$ , $i = 1, \ldots, m$, đặt khóa phiên của tập này là $e(g,h)^{k.\beta_i}$, trong đó $\beta_1, \ldots, \beta_m$ là các số ngẫu nhiên được chọn ở thuật toán khởi tạo. Với ý tưởng như vậy, khóa bí mật của người dùng lúc này sẽ có dạng:

$$g^{\frac{\beta_i}{\alpha+ID_{ui}}}$$

Vì mỗi người dùng *u* có thể đăng ký tối đa m kênh, nên mỗi người dùng *u* sẽ có tối đa *m* khóa bí mật $g^{\frac{\beta_i}{\alpha+ID_{ui}}}$ , $i = 1, \ldots, m$.

### 2.2.2 Hệ mã đề xuất và so sánh

Hệ mã được xây dựng như sau

**Khởi tạo** ($1^{\lambda}$ ) : Đầu vào của giải thuật là tham số an toàn $\lambda$, đầu ra của giải thuật là khóa bí mật của hệ thống msk, khóa công khai của hệ thống param bao gồm cả *m* là số tối đa các kênh, *n* là số tối đa người dùng đăng ký vào một kênh.

Đặt N = $m \cdot n$, giải thuật tạo ra hệ thống bilinear map $D = (p, \mathbb{G}, \widetilde{\mathbb{G}}, \mathbb{G}_T, e)$, chọn ngẫu nhiên $h \xleftarrow{\$} \widetilde{\mathbb{G}}$, $g \xleftarrow{\$} \mathbb{G}$ và $\alpha, \beta_1, \ldots, \beta_m \xleftarrow{\$} \mathbb{Z}_p^*$. Giả sử $\mathcal{H}$ là hàm băm sao cho $\mathcal{H}: \{0,1\}^* \to \mathbb{Z}_p^*$.

Giải thuật cho đầu ra:

$$\text{param} = \left(D, \left\{h^{\alpha^i}\right\}_{i=0,\ldots,N}, \left\{h^{\beta_i \alpha^j}\right\}_{\substack{i=1,\ldots,m \\ j=0,\ldots,N}}, g^{\alpha}, \left\{e(g,h)^{\beta_i}\right\}_{i=1,\ldots,m}, \mathcal{H}\right)$$

và khóa bí mật của hệ thống:

$$\text{msk} = (g, \alpha, \beta_1, \ldots, \beta_m)$$

**Tạo khóa**($ID_{i,j}$ , msk, param) : Giả sử rằng định danh của người dùng *i* trong kênh *j* là chuỗi bit bất kỳ $ID_{i,j} \in \{0, 1\}^*$. Người dùng *i* đăng ký vào kênh *j* sẽ nhận được khóa bí mật tương ứng sau:

$$sk_{ID_{i,j}} = g^{\frac{\beta_j}{\alpha+\mathcal{H}(ID_{i,j})}}$$

Ký hiệu (*i, j*) là chỉ số khóa bí mật. Trong hệ thống, mỗi người dùng có thể đăng ký vào nhiều kênh và nhận khóa bí mật tương ứng với từng kênh. Ví dụ người dùng *i* đăng ký vào kênh 1, . . . , *t*, người dùng *i* sẽ nhận các khóa bí mật $\left\{sk_{ID_{i,j}}\right\}_{j=1,\ldots,t}$.

**Mã hóa** (param, $S_1, \ldots, S_t$) : Đầu vào của giải thuật là *t* tập chỉ số khóa bí mật của người dùng trong *t* kênh $S_1, \ldots, S_t$ , $t \leq m$. Trong đó $S_1, \ldots, S_t$ là các tập không giao nhau. Ký hiệu $S = \cup_{i=1}^{t} S_i$ là tập đầy đủ tất cả các chỉ số khóa bí mật của người dùng cho một lần mã hóa. Giải thuật chọn ngẫu nhiên $k \in \mathbb{Z}_p^*$, tính khóa phiên bí mật cho *t* kênh như sau:

$$K_i = e(g,h)^{k\beta_i}, i = 1, \ldots, t$$

Sau đó tính bản mã Hdr = ($C_1$, $C_2$) như sau:

$$C_1 = g^{-\alpha.k} \quad , \quad C_2 = h^{k.\prod_{(i,j)\in S}\left(\alpha+\mathcal{H}(ID_{i,j})\right)}$$

Cuối cùng giải thuật cho đầu ra $K = \{K_i\}_{i=1,\ldots,t}$ và $\text{Hdr} = (C_1, C_2)$ bao gồm cả thông tin của tập *S*.

**Giải mã**($sk_{ID_{i,j}}$,Hdr, param) : Giải thuật đầu tiên kiểm tra xem chỉ số *(i, j)* ∈ *S* có đúng hay không, nếu sai thì cho đầu ra là ⊥. Nếu đúng là thuộc tập *S*, giải thuật tính giá trị $K' = h^{\gamma}$ trong đó:

$$\gamma = \frac{\rho_j}{\alpha}\Big| \prod_{(i',j')\in S} \Big(\alpha + \mathcal{H}\big(ID_{i',j'}\big)\Big) - \prod_{(i',j')\in S} \mathcal{H}\big(ID_{i',j'}\big) \Big| \quad (2.24)$$

Lưu ý rằng giải thuật có thể tính $K'$ từ các thông tin có trong khóa công khai param. Đặt

$$B = \prod_{\substack{(i',j')\in S \\ (i',j')\neq(i,j)}} \mathcal{H}\big(ID_{i',j'}\big)$$

Giải thuật cuối cùng cho đầu ra

$$K_j = \left(e(C_1, K').e\left(sk_{ID_{i,j}}, C_2\right)\right)^{\frac{1}{B}}$$

**Tính đúng đắn**:

$$K_j = \left(e(C_1, K').e\left(sk_{ID_{i,j}}, C_2\right)\right)^{\beta} \quad (2.25)$$

$$= \left( e(g^{-\alpha.k}, h^{\gamma}) . e\left( g^{\alpha+\mathcal{H}(ID_{i,j})}. h^{k.\prod_{(i,j)\in S}(\alpha+\mathcal{H}(ID_{i,j}))} \right) \right) \quad (2.26)$$

$$= \left( e(g,h) \quad {}_{(i',j')\neq(i,j)} \right) \quad (2.27)$$

$$= e(g,h)^{k\beta_j} \quad (2.28)$$

So sánh với các hệ mã khác

Để đánh giá độ hiệu quả của hệ mã hóa đa kênh đề xuất, nghiên cứu sinh lập bảng 2.1 so sánh với các hệ mã hóa quảng bá đa kênh hiện có, trong đó:

**Header** là độ dài của bản mã Hdr; **S-key** là độ dài khóa bí mật; **P-key** là độ dài khóa công khai;

**Dec time** là thời gian giải mã; Security bao gồm mô hình an toàn và có hoặc không dùng ROM (máy tư vấn ngẫu nhiên - random oracle);

Setting là kiểu mã hóa bí mật (Secret-ke) hay công khai (Public-key).

| | Header | S-key | P-key | Dec time | Security | Setting |
|---|---|---|---|---|---|---|
| [15]-1 | 2\|$\mathbb{G}$\| | m\|$\widetilde{\mathbb{G}}$\| | 3mn\|$\mathbb{G}$\|+ 2mn\|$\widetilde{\mathbb{G}}$\| | *(m + 1)P* | Selective | Secret-key |
| [15]-2 | 3\|$\mathbb{G}$\|+1\|$\mathbb{G}$\| | m\|$\widetilde{\mathbb{G}}$\| | 2mn\|$\mathbb{G}$\| + 2mn\|$\widetilde{\mathbb{G}}$\| | *(m + 2)P* | Selective-CCA+ROM | Secret-key |
| [60] | 2\|$\mathbb{G}$\| | m\|$\widetilde{\mathbb{G}}$\| | 2mn\|$\mathbb{G}$\|+ 2mn\|$\widetilde{\mathbb{G}}$\| | *(m + 1)P* | Selective | Secret-key |
| [3] | 2\|$\mathbb{G}$\| | m\|$\mathbb{G}$\| | (mn + m) \|$\mathbb{G}$\| | 2*P* | Selective | Public-key |
| Hệ MCBE đề xuất | 1\|$\mathbb{G}$\|+1\|$\widetilde{\mathbb{G}}$\| | m\|$\mathbb{G}$\| | $m^2$n\|$\widetilde{\mathbb{G}}$\| | 2*P* | Selective +ROM | Public-key |

*Bảng 2.1 So sánh các hệ mã hóa đa kênh hiện có và hệ mã hóa đa kênh đề xuất.*

*n là số tối đa người dùng trong một kênh, m là số tối đa kênh, P là một phép tính Parings. |𝔾| là kích thước của một phần tử trong nhóm 𝔾, |$\widetilde{\mathbb{G}}$| là kích thước của một phần tử trong nhóm $\widetilde{\mathbb{G}}$.*

Hệ của nghiên cứu sinh là hệ mã hóa khóa công khai trong khi 3 hệ [15]-1 và [15]-2 và [60] đều là mã hóa bí mật, độ dài của bản mã hệ nghiên cứu sinh đề xuất có độ dài ngắn nhất. Thời gian giải mã của hệ nghiên cứu sinh đề xuất chỉ là 2 phép toán Perings (2P) còn các hệ khác lớn hơn hoặc bằng.

Cài đặt hệ MCBE đề xuất ở trên bằng ngôn ngữ C và dùng thư viện PBC [40]. Mã nguồn của chương trình cài đặt có ở địa chỉ *https://github.com/tranvinhduc/MCBE*

Nghiên cứu sinh cài đặt trên máy tính xách tay với bộ vi xử lý Intel Core i7-4600U @ 2.1 GHz. Đo kết quả trung bình 1000 lần. Trên máy tính này thư viện PBC tính một Parings khoảng 0.9ms, một phép mũ trên đường cong elliptic của nhóm 𝔾 khoảng xấp xỉ 1.3ms.

Với hệ MCBE, thời gian thực hiện mã hóa chủ yếu là đi tính khóa phiên *Ki* và thành phần $C_2$, tương ứng với việc cần tính *m* và *N* phép mũ trong nhóm 𝔾. Thời gian giải mã cần tính *N* phép mũ trong 𝔾 và hai phép Parings

Kết quả thực nghiệm được trình bày trên bảng 2.2. Như nhận định, cả hai giải thuật mã hóa và giải mã chạy khá nhanh, và tốc độ tăng tuyến tính với *N*.

| *m* | N | Encrypt | Decrypt |
|---|---|---|---|
| 10 | 20 | 29ms | 25ms |
| 10 | 40 | 55ms | 50ms |
| 10 | 80 | 106ms | 102ms |
| 20 | 40 | 56ms | 50ms |
| 20 | 80 | 108ms | 102ms |
| 20 | 160 | 211ms | 207ms |
| 25 | 50 | 70ms | 64ms |
| 25 | 100 | 136ms | 129ms |
| 25 | 200 | 266ms | 260ms |

*Bảng 2.2: Thực nghiệm cài đặt hệ MCBE đề xuất*

*m* là số kênh, mỗi kênh có *n* người dùng, và $N = n \times m$ là tổng số của tất cả các đăng ký trong tất cả các kênh.

## 2.3 Kết luận chương 2

Các nghiên cứu của chương 2 được Nghiên cứu sinh công bố trong công trình số 4 trong các bài báo tạp chí công bố trong luận án.

Trong chương này nghiên cứu sinh đã trình bày về hệ mã hóa quảng bá đa kênh. Điểm yếu chung của một số hệ mã hóa quảng bá đa kênh là vấn đề người lập mã cần biết các tham số bí mật (ở dạng mã hóa khóa bí mật). Rất gần đây các tác giả trong [3] đã giới thiệu một hệ mã hóa quảng bá đa kênh mà người lập mã không cần biết các tham số bí mật. Chương này trình bày hệ mã hóa quảng bá đa kênh do nghiên cứu sinh đề xuất có cùng tính chất và độ hiệu quả tương đương như hệ [3], tuy nhiên dùng phương pháp hoàn toàn khác là dựa trên kỹ thuật của hệ Delerablee. nghiên cứu sinh cũng trình bày chứng minh chi tiết rằng hệ đề xuất  là đạt an toàn .

# Chương 3: HỆ MÃ HÓA DỰA TRÊN THUỘC TÍNH

Chương 3 trình bày giới thiệu chung về hệ mã hóa dựa trên thuộc tính bao gồm: Định nghĩa chung về mã hóa dựa trên thuộc tính, mô hình an toàn của mã hóa dựa trên thuộc tính, một số hệ mã hóa dựa trên thuộc tính quan trọng hiện nay. Nội dung chương, tác giả sẽ trình bày 02 hệ mã hóa dựa trên thuộc tính mới được đề xuất, đó cũng chính là đóng góp mới trong luận án.

## 3.1 Định nghĩa hệ mã hóa dựa trên thuộc tính

Mã hóa dựa trên thuộc tính được giới thiệu bởi Sahai và Waters [53], là mở rộng của mã hóa quảng bá, trong đó cho phép điều kiện giải mã linh động hơn so với mã hóa quảng bá. Vấn đề khó khăn với mã hóa quảng bá là người lập mã phải biết cụ thể tập người dùng có thể giải mã được tại thời điểm lập mã, tuy nhiên trong thực tế người lập mã không phải lúc nào cũng biết được điều này. Ví dụ, công ty FPT lưu trữ dữ liệu của họ trên đám mây, họ muốn lưu trữ một văn bản mà cho phép các nhân viên của phòng kỹ thuật và phòng hỗ trợ khách hàng, đồng thời tham gia trong dự án e-Health có thể giải mã được.

Với kỹ thuật mã hóa quảng bá, công ty FPT phải biết ngay tại thời điểm mã hóa văn bản là những nhân viên cụ thể nào của hai phòng trên tham gia vào dự án e-Health. Tuy nhiên trong thực tế, do tính chất công việc dự án e-Health có thể thêm nhân viên từ các phòng trên. Để giải quyết vấn đề này, công ty FPT phải thực hiện lại quá trình mã hóa văn bản và upload lên trên Cloud, điều này hiển nhiên là không hợp lý.

Mã hóa dựa trên thuộc tính được phát triển để giải quyết những vấn đề như vậy, trong một hệ thống mã hóa thuộc tính tùy ý, ta có thể định nghĩa một tập các thuộc tính. Ví dụ, Trong công ty FPT có dự án e-Health (e-H), Phòng kỹ thuật (PKT), Phòng chăm sóc khách hàng (PCS), Nhân viên (NV), Trưởng phòng (TP),. . . là các thuộc tính. Nếu người dùng X thuộc phòng kỹ thuật, là nhân viên và tham gia dự án e-Health thì sẽ nhận các thuộc tính là PKT, e-H, NV và nhận khóa bí mật tương ứng với các thuộc tính này. Công ty FPT khi mã hóa văn bản chỉ đơn giản là thực hiện việc mã hóa trong đó quy định rằng những nhân viên của hai phòng này và làm trong dự án e-Health có thể giải mã được mà không cần biết cụ thể là nhân viên nào. Điều kiện giải mã có thể được mô tả bằng một biểu thức boolean như sau:

(NV and PKT and e-H) or (NV and PCS and e-H) Khi một nhân viên mới thuộc một trong hai phòng này tham gia dự án, người này sẽ nhận thêm thuộc tính là Dự án e-Health và nhận khóa bí mật tương ứng, hiển nhiên nhân viên mới này sẽ có khả năng giải mã vì đáp ứng được điều kiện giải mã.

## 3.2. Hệ mã hóa dựa trên thuộc tính thứ nhất do nghiên cứu sinh đề xuất

Trong phần này nghiên cứu sinh đề xuất một hệ mã hóa dựa trên thuộc tính có các ưu điểm sau:

• Hệ có độ dài bản mã Hdr chỉ là 3 phần tử (tối ưu nhất trong các hệ mã dựa trên thuộc tính hiện có hiện nay);

• Hệ hỗ trợ chính sách giải mã là một biểu thức boolean, mà cụ thể là có dạng CNF;

• Tốc độ mã hóa và giải mã là hiệu quả. Để giải mã người dùng cần tình *2m* pairings. Để chi tiết hơn tôi cài đặt và trình bày so sánh hệ của luận án với các hệ hiện có trong bảng 2.2.

Tuy nhiên điểm yếu của hệ mã của luận án là:

• Độ dài của khóa bí mật vẫn dài. Cụ thể là độ dài của khóa bí mật là tuyến tính với *N* trong đó *N* là tích của số các thuộc tính trong hệ thống *n* và số các mệnh đề *m* trong biểu thức CNF;

• Độ dài của khóa công khai vẫn dài, và số lượng tối đa thuộc tính có trong hệ thống là giới hạn;

• Hệ chỉ đạt an toàn *selective security*-CPA.

### 3.2.1 Ý tưởng xây dựng

Ý tưởng chính là biến đổi một hệ mã hóa quảng bá đa kênh thành một hệ mã hóa dựa trên thuộc tính CP-ABE. Với mục đích đó tác giả xem mỗi tập $S_i$ trong hệ MCBE luận án đề xuất trình bày ở chương 3 như một mệnh đề $\tilde{\beta}_i$ trong biểu thức boolean CNF (là chính sách giải mã - *access policy*). Khóa phiên *K* trong hệ CP-ABE lúc này chính là tích của tất cả các khóa phiên con trong hệ MCBE. Cụ thể khóa phiên $K = \prod_{i=1}^{t} e(g,h)^{k.\beta_i}$

Tiếp theo tác giả xem mỗi chỉ số $i \in \{1, \ldots, n\}$ trong hệ MCBE như là một thuộc tính trong hệ CP-ABE. Ngoài ra để cho mỗi thuộc tính có thể được dùng lại nhiều lần trong chính sách bản mã, mỗi thuộc tính có *m* bản sao, tức là nếu một thuộc tính khi được dùng lại thì sẽ dùng một bản sao khác, như vậy mỗi thuộc tính có thể dùng lại tối đa m lần, m là số tối đa các mệnh đề trong biểu thức boolean CNF. Nếu một người dùng trong hệ CP-ABE sở hữu một thuộc tính $i \in \{1, \ldots, n\}$, người dùng đó sẽ nhận khóa bí mật tương ứng với chỉ số $\{i, j\}_{j=1,\ldots,m}$ trong hệ MCBE.

Để có khả năng giải mã (tức là tính khóa phiên *K*), người dùng phải tính được tất cả các khóa phiên con $e(g,h)^{k.\beta_i}, i = 1, \ldots, t$. Điều đó dẫn đến rằng người dùng chỉ có khả năng giải mã khi người dùng đó sở hữu tập thuộc tính thỏa mãn chính sách bản mã. Để giải quyết vấn đề hợp tác giải mã của các người dùng mà mỗi người dùng trong số đó không có quyền giải mã, dùng một thành phần ngẫu nhiên khác nhau sao cho mỗi lần tạo khóa bí mật cho người dùng *u*.

### 3.2.2 Hệ mã đề xuất và so sánh

Hệ mã được xây dựng như sau.

**Khởi tạo** $(1^{\lambda}, n, \{S_u\}_{u \in \mathcal{U}})$: giả sử rằng $\lambda$ là tham số an toàn, *n* là số tối đa các thuộc tính trong hệ thống. Ký hiệu *m* là số tối đa các mệnh đề trong biểu thức boolen CNF, đặt $N = m \cdot n$. Mỗi người dùng u sở hữu một tập các thuộc tính $S_u \subset \{1, \ldots, n\}$. Mỗi thuộc tính $A_i$, $i = 1, \ldots, n$, có *m* bản sao của chính nó, đặt $\mathcal{B} = \{A_{11}, \ldots, A_{n,m}\}$ là tập tất cả các thuộc tính, ký hiệu $\mathcal{B}_u = (A_{i,j} \in \mathbb{Z}_p^*)_{\substack{i \in S_u \\ j=1,\ldots,m}}$. Giả thuật tạo ra tham số công khai cho hệ thống và

khóa bí mật cho người dùng $u \in \mathcal{U}$ như sau (lưu ý ở đây là gộp luôn giải thuật khởi tạo và tạo khóa):

Giải thuật đầu tiên tạo ra hệ thống bilinear map $D = (p, \mathbb{G}, \widetilde{\mathbb{G}}, \mathbb{G}_T, e)$, chọn ngẫu nhiên $h \xleftarrow{\$} \widetilde{\mathbb{G}}, g \xleftarrow{\$} \mathbb{G}$ và $\alpha, \gamma, \beta_1, \dots, \beta_m \xleftarrow{\$} \mathbb{Z}_p^*$ . Tiếp theo, giải thuật cho đầu ra tham số an toàn của hệ thống

$$\text{param} = \left(D, \mathcal{B}, \{h^{\alpha^j}\}_{j=0,\dots,N}, \{h^{\beta_j}\}_{j=1,\dots,m}, g^{\alpha}, \{e, (g,h)^{\gamma\beta_i}\}_{i=1,\dots,m}\right) \qquad (3.14)$$

Để tạo ra khóa bí mật $sk_u$, giải thuật đầu tiên chọn ngẫu nhiên $s_u \xleftarrow{\$} \mathbb{Z}_p^*$, sau đó tính

$$sk_u = \left( \{g^{\overline{\alpha+A_{i,j}}}\}_{\substack{i\in S_u \\ j=1,\dots,m}}, \{h^{\alpha^i \beta_j s_u}\}_{\substack{i=0,\dots,N \\ j=1,\dots,m}}, g^{s_u+\gamma} \right) \qquad (3.15)$$

Chú ý rằng $sk_u$ cũng bao gồm $S_u$.

**Mã hóa** (param, $\tilde{\beta} = \tilde{\beta}_1 \wedge \cdots \wedge \tilde{\beta}_t$) : Đầu vào của giải thuật là khóa công khai param và chính sách mã hóa $\tilde{\beta}$ (*access policy*).

Giải thuật đầu tiên chọn ngẫu nhiên $k \in \mathbb{Z}_p^*$ sau đó tính khóa phiên:

$$K = e(g,h)^{k\gamma \sum_{i=1}^{t} \beta_i}$$

Chú ý rằng $t \le m$ và giải thuật có $\{e(g,h)^{\gamma\beta_i}\}_{i=1,\dots,m}$ từ param.

Để tính bản mã Header, giải thuật tính Hdr = ($C_1$, $C_2$, $C_3$), trong đó

$$C_1 = g^{-\alpha.k} \quad C_2 = h^{k \sum_{i=1}^{t} \beta_i}$$

Và

$$C_3 = h^{k.\prod_{i\in\tilde{\beta}_1}(\alpha+A_{i,1})\dots\prod_{i\in\tilde{\beta}_t}(\alpha+A_{i,t})}$$

Cuối cùng giải thuật cho đầu ra $K$ và bản mã Hdr = ($C_1$, $C_2$, $C_3$) bao gồm cả $\tilde{\beta}$.

**Giải mã** ($sk_u$, Hdr, param): Giải thuật đầu tiên kiểm tra xem $S_u$ có thỏa mãn $\tilde{\beta}$ không? nếu không giải thuật trả về $\perp$. Ngược lại giải thuật tính khóa phiên thành phần $K_1$ như sau:

Giải thuật đầu tiên chọn $i' \in (\tilde{\beta}_1 \cap S_u)$ sau đó tính $K'_1 = h^{\emptyset}$ trong đó

$$\emptyset = \frac{\beta_1 s_u}{\alpha} \left( \prod_{\substack{i\in\tilde{\beta}_1 \\ i\neq i'}} (\alpha + A_{i,1}) \dots \prod_{i\in\tilde{\beta}_t} (\alpha + A_{i,t}) - \prod_{\substack{i\in\tilde{\beta}_1 \\ i\neq i'}} A_{i,1} \dots \prod_{i\in\tilde{\beta}_t} A_{i,t} \right) \qquad (3.17)$$

Chú ý rằng giải thuật cũng có thể tính $K'_1$ từ $\left\{h^{\alpha^i \beta_j s_u}\right\}_{\substack{i=0,\dots,N \\ j=1,\dots,m}}$. Đặt

$$B_1 = \prod_{\substack{i\in\tilde{\beta}_1 \\ i\neq i'}} A_{i,1} \dots \prod_{i\in\tilde{\beta}_t} A_{i,t}$$

Giải thuật tính

$$K_1 = \left( e(C_1 K'_1) \,.\, e(g^{\overline{\alpha+A_{i',1}}}, C_3) \right) \qquad (3.18)$$

$$= \left( e\left(g^{-\alpha.k} h^{\theta}\right) . e\left( g^{\overline{\alpha+A_{i',1}}}, h^{k.\prod_{i\in\tilde{\beta}_1}(\alpha+A_{i,1})\dots\prod_{i\in\tilde{\beta}_t}(\alpha+A_{i,t})} \right) \right) \qquad (3.19)$$

$$= \left( e(g,h)^{k\beta_1 s_u \prod_{\substack{i \in \widetilde{\beta}_1 \\ i \neq i'}} A_{i,1} \ldots \prod_{i \in \widetilde{\beta}_t} (\alpha + A_{i,t})} \right)^{\frac{1}{B_1}} \quad (3.20)$$

$$= e(g,h)^{k\beta_1 s_u} \quad (3.21)$$

Tương tự, giải thuật tính $K_2, \ldots, K_t$ , và sau đó

$$K' = \prod K_i = e(g,h)^{k s_u \sum_{i=1}^{t} \beta_i} \quad (3.22)$$

Cuối cùng, giải thuật tính

$$K = \frac{e(g^{s_u+\gamma}, C_2)}{K'} = \frac{e\left(g^{s_u+\gamma}, h^{k\sum_{i=1}^{t}\beta_i}\right)}{e(g,h)^{k s_u \sum_{i=1}^{t} \beta_i}} = e(g,h)^{k\gamma \sum_{i=1}^{t} \beta_i} \quad (3.23)$$

**So sánh với các hệ mã khác**

Để đánh giá độ hiệu quả của hệ mã hóa dựa trên thuộc tính đề xuất, tác giả lập bảng sau 3.1 so sánh với các hệ mã hóa dựa trên thuộc tính hiện có mà có cùng tính chất là có độ dài bản mã là hằng số, trong đó:

• **Header là độ dài của bản mã Hdr**; **S-key** là độ dài khóa bí mật; **P-key** là độ dài khóa công khai;

• **Acce Policy** là chính sách giải mã;

• **Setting** là kiểu mã hóa bí mật (**Secret-key**) hay công khai (**Public-key**).

| | Acce Policy | CNF | S-key | P-key | Setting |
|---|---|---|---|---|---|
| [27] | AND-gates | *O*(1) | *O*(1) | $O(n^2)$ | Public-key |
| [35] | Threshold | *O*(1) | *O(n)* | *O(n)* | Public-key |
| [8] | LSS | *O*(1) | $O(k^4.\ell^4)$ | $O(k^2.\ell^2)$ | Public-key |
| [4] | LSS | *O*(1) | $O(n.\ell^2)$ | *O(n.ℓ)* | Public-key |
| [6] | LSS | *O*(1) | $O(n.\ell^2)$ | *O(n.ℓ)* | Public-key |
| [15]-3 | CNF | *O*(1) | *O(m.n)* | *O(m.n)* | Secret-key |
| [15]-4 | CNF | *O*(1) | *O(m.n)* | *O*(1) | Secret-key |
| [52] | LSS | O(ℓ) | *O(k)* | *O*(1) | Public-key |
| [5] | LSS | O(ℓ) | *O(k)* | *O*(1) | Public-key |
| Hệ mã CP-ABE đề xuất | CNF | O(1) | $O(m^2.n)$ | *O(m.n)* | Public-key |

*Bảng 3.1 So sánh các hệ mã hóa dựa trên thuộc tính đã có với hệ mà hóa đề xuất. n là số tối đa các thuộc tính trong hệ thống, m là số tối đa các mệnh đề trong CNF access policy (chính sách truy cập liên kết thông thường), k là số tối đa các thuộc tính trong một khóa bí mật (số tối đa các thuộc tính mà một người dùng có thể sở hữu), ℓ là số dòng trong ma trận LSS, tương đương với n. LSS là ma trận tuyến tính chia sẽ khóa bí mật (linear secret sharing), có dạng như một biểu thức Boolean.*

Hệ mã nghiên cứu sinh đề xuất lợi thế là hệ mã hóa công khai.

Cài đặt hệ CP-ABE đề xuất ở trên bằng ngôn ngữ C và dùng thư viện PBC [40]. Mã nguồn của chương trình cài đặt có ở địa chỉ

*https://github.com/tranvinhduc/MCBE*

Tác giả cài đặt trên máy tính xách tay với bộ vi xử lý Intel Core i7-4600U @ 2.1 GHz. Đo kết quả trung bình 1000 lần. Trên máy tính này thư viện PBC tính một Parings khoảng 0.9ms, một phép mũ trên đường cong elliptic của nhóm $\mathbb{G}$ khoảng xấp xỉ 1.3ms.

Với hệ CP-ABE, thời gian chủ yếu khi mã hóa là để tính $C_2$ và $C_3$, với tương ứng cần $m$ và $N$ phép mũ trong nhóm $\mathbb{G}$. Hầu hết thời gian giải mã là để tính $K_1, K_2, \ldots, K_m$ trong đó $m$ là số các mệnh đề trong một chính sách giải mã (access policy). Với mỗi $K_i$ cần $N$ phép mũ trong $\mathbb{G}$.

Cài đặt dùng chính sách giải mã (access policy) $\tilde{\beta}$ có dạng biểu thức CNF sau:

$$\tilde{\beta} = \tilde{\beta}_1 \wedge \ldots \wedge \tilde{\beta}_m, \ \left|\tilde{\beta}\right| = N, \ \left|\tilde{\beta}_i\right| = N/m$$

Bảng 3.2 mô tả kết quả cài đặt hệ CP-ABE của nghiên cứu sinh. Kết quả cài đặt thực nghiệm đúng với kết quả phân tích ở trên

Tóm lại thực nghiệm đã chỉ ra rằng hệ CP-ABE của nghiên cứu sinh đáp ứng được yêu cầu về sự hiệu quả khi triển khai trong thực tế.

| m | N | Mã hóa | Giải mã |
|---|---|---|---|
| 10 | 20 | 27ms | 237ms |
| 10 | 40 | 54ms | 510ms |
| 10 | 80 | 107ms | 1.03s |
| 20 | 40 | 55ms | 1.04s |
| 20 | 80 | 103ms | 2.01s |
| 20 | 160 | 209ms | 4.1s |
| 25 | 50 | 68ms | 1.6s |
| 25 | 100 | 127ms | 3.1s |
| 25 | 200 | 259ms | 6.4s |

*Bảng 3.2: Kết quả thực nghiệm cài đặt hệ CP-ABE đề xuất. m là số mệnh đề trong biểu thức boolean CNF (dạng liên kết thông thường), N là số các thuộc tính trong hệ thống.*

## 3.3. Đề xuất thứ hai về hệ mã hóa dựa trên thuộc tính

### 3.3.1. Ý tưởng xây dựng và So sánh

Hiện nay dữ liệu của các công ty/doanh nghiệp thường được mã hóa và lưu trên các đám mây (Cloud storage). Để đảm bảo tính linh động thì trong các hệ mã hóa hiện có, mã hóa dựa trên thuộc tính thường được chọn. Trong khi hàng ngày công ty/doanh nghiệp vẫn cần phải làm việc trên khối dữ liệu đã được mã hóa này, ví dụ tìm kiếm dữ liệu. Có hai cách công ty/doanh nghiệp có thể làm:

**Phương pháp thứ nhất** là công ty/doanh nghiệp sẽ cung cấp toàn bộ khóa bí mật cho một máy chủ (Cloud Server) nào đó có năng lực mạnh để giải mã toàn bộ dữ liệu của mình, sau đó tìm kiếm dữ liệu trên dữ liệu đã được giải mã đó rồi trả về kết quả cho công ty/doanh nghiệp. Tuy nhiên phương pháp này có nhược điểm là máy chủ đó sẽ biết được toàn bộ nội dung dữ liệu của công ty/doanh nghiệp, điều mà không một công ty/doanh nghiệp nào mong muốn;

**Phương pháp thứ hai** là công ty/doanh nghiệp tự lấy về hoàn toàn dữ liệu và giải mã, sau đó tìm kiếm trên dữ liệu đã được giải mã. Phương pháp này hiển nhiên là không hợp lý vì năng lực máy tính của công ty/doanh nghiệp là không đáp ứng được. Để giải quyết vấn đề này,một hướng nghiên cứu mở rộng của ABE hiện nay đang rất được quan tâm là vấn đề tìm kiếm trên dữ liệu đã được mã hóa [11,14,23,24,34,37,45,57,59]. Với hướng nghiên cứu này công ty/doanh nghiệp chỉ cung cấp một phần thông tin của khóa bí mật gọi là cửa sập cho máy chủ, để máy chủ dựa vào đó tìm kiếm dữ liệu cần thiết trên khối dữ liệu đang được mã hóa của doanh nghiệp. Sau khi tìm được các bản mã tương ứng doanh nghiệp muốn tìm sẽ gửi trả về cho doanh nghiệp, doanh nghiệp sẽ dùng khóa bí mật của mình để giải mã các bản mã này. Với phương pháp như vậy máy chủ chỉ biết được thông tin là cửa sập và các bản mã, và từ các thông tin này không thể biết được nội dung thực sự dữ liệu của doanh nghiệp. Trong khi doanh nghiệp vẫn tận dụng được sức mạnh tính toán của máy chủ. Kỹ thuật này cũng được áp dụng vào rất nhiều ứng dụng khác ví dụ như ứng dụng định hướng chuyển tiếp Email của các Gateway.

Trong luận án này nghiên cứu sinh đề xuất một hệ mã hóa dựa trên thuộc tính đồng thời có tính chất tìm kiếm trên dữ liệu đã được mã hóa. Hệ của nghiên cứu sinh có ưu và nhược điểm sau:

- Đề xuất của nghiên cứu sinh tích hợp một mã hóa dựa trên thuộc tính và một hệ cho phép tìm kiếm trên dữ liệu đã được mã hóa. Tức là trong hệ của nghiên cứu sinh người dùng chỉ cần sở hữu một khóa bí mật duy nhất cho cả hai hệ, cũng như hệ thống chỉ cần một khóa công khai param duy nhất cho cả hai hệ thống. Lưu ý rằng trong một số hệ khác hai hệ này là tách biệt do đó sẽ kém hiệu quả hơn;

- Trong hệ thống của nghiên cứu sinh người dùng có thể tự mình tạo ra của sập (trapdoor). So với các hệ khác để tạo ra cửa sập người dùng thường phải nhờ trợ giúp từ một bên thứ 3 dẫn đến phức tạp và kém an toàn hơn;

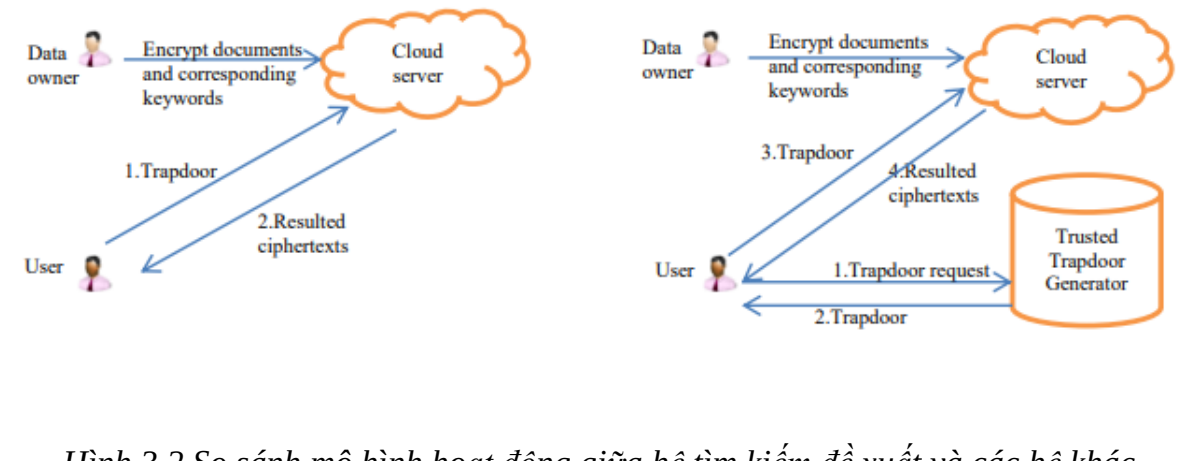
- Về độ hiệu quả, do hệ của nghiên cứu sinh được xây dựng dựa trên hệ CP-ABE [42] nên cũng kế thừa cơ bản các tính chất của hệ này như độ dài khóa bí mật ngắn, độ dài bản mã ngắn, tốc độ giải mã nhanh và hỗ trợ hệ thống phân phối khóa an toàn (multi-authority);

- Tuy nhiên hệ của nghiên cứu sinh có những nhược điểm sau:

• Hệ nghiên cứu sinh không đạt được an toàn cho cửa sập. Lưu ý rằng cho đến nay chỉ có duy nhất hệ [24] đạt được một phần tính chất này;

• Độ dài khóa công khai cũng như cửa sập còn dài;

• Tốc độ tìm kiếm dữ liệu vẫn chưa thực sự hiệu quả. Nghiên cứu sinh so sánh mô hình hoạt động hệ của nghiên cứu sinh với một số hệ hiện có trong hình 3.2




*Hình 3.2 So sánh mô hình hoạt động giữa hệ tìm kiếm đề xuất và các hệ khác*

### 3.4.2. Hệ mã đề xuất dựa trên thuộc tính thứ 2 của nghiên cứu sinh

Hệ đề xuất của nghiên cứu sinh được mô tả chi tiết như sau:

**Khởi tạo** $(v, \mathcal{B})$: Giả sử $N = |\mathcal{B}|$ là số tối đa các thuộc tính có trong hệ thống, $(p, \mathbb{G}, \mathbb{G}_T, e(\cdot,\cdot))$ là một hệ thống Billinear Map. Thuật toán chọn ngẫu nhiên một phần tử sinh $g \in \mathbb{G}$, và các giá trị $a, \alpha, \lambda \in \mathbb{Z}_p$, tính $g^a, g^\alpha, g^\lambda$. Thuật toán tiếp tục tạo ra $2N$ phần tử trong nhóm $\mathbb{G}$ tương ứng với $N$ thuộc tính trong hệ thống

$h_1, \ldots, h_N, \tilde{h}_1, \ldots, \tilde{h}_N$. Giả sử $\mathcal{H}, \tilde{\mathcal{H}}$ là các hàm băm sao cho $\mathcal{H} : \{0,1\}^* \to \mathbb{G}$ và

$\tilde{\mathcal{H}} : \mathbb{G}_T \times \{0,1\}^* \to \mathbb{Z}_p$. Giả sử tập hợp các từ khóa có trong hệ thống là $W = (\omega_1, \omega_2, \omega_3, \ldots)$, trong đó mỗi $\omega_i \in \{0,1\}^*$. Lưu ý rằng tập $W$ là không giới hạn, chúng ta có thể thêm mới từ khóa bất kỳ lúc nào nếu muốn. Để cho đơn giản về mặt ký hiệu, thuật toán bỏ qua $W$ trong danh sách tham số hệ thống. Cuối cùng, khóa bí mật của hệ thống là $\text{MSK} = (g^\alpha, \lambda)$ và khóa công khai của hệ thống là:

$$\text{param} = (g, g^a, g^\lambda, e(g,g)^\alpha, h_1, \ldots, h_N, \tilde{h}_1, \ldots, \tilde{h}_N, \mathcal{H}, \tilde{\mathcal{H}})$$

**Tạo Khóa** $(u, \mathcal{B}(u), \text{MSK}, \text{param})$ : Giả sử $\mathcal{B}(u)$ là tập thuộc tính của người dùng $u$ Giải thuật tạo khóa chọn $s_u \xleftarrow{\$} \mathbb{Z}_p$ , tính khóa bí mật cho người dùng $u$ là $d_{u0} = (d_{u_0}, d'_{u_0}, \{d_{u_i}\}_{i\in B(u)}, \lambda)$ , trong đó

$$d_{u_0} = g^{\alpha} \cdot g^{a \cdot s_u}, d'_{u_0} = g^{s_u}, \{d_{u_i} = h_i^{s_u}\}_{i\in\mathcal{B}(u)} .$$

Người dùng $u$ chỉ cần giữ bí mật $d_{u_0}$và $\lambda$ , phần còn lại của khóa có thể lưu giữ ở bất kỳ đâu không cần giữ bí mật, điều đó có nghĩa là khóa bí mật mà người dùng cần lưu giữ có chỉ là hai phần tử do đó có độ dài là rất ngắn.

**Mã Hóa** $(\mathcal{M}, \mathbb{A}, param)$ : Đầu vào của giải thuật là dữ liệu $\mathcal{M}$ , chính sách mã hóa $\mathbb{A}$, và khóa công khai của hệ thống param . Giải sử rằng $\mathbb{A}$ là biểu thức boolean $\beta$ và kích thước của $\beta$ là $|\beta|$ . Đầu tiên giải thuật mã hóa biểu diễn $\beta$ dưới dạng biểu thức dạng DNF $\beta = (\beta_1 \vee \cdots \vee \beta_m)$ , trong đó mỗi $\beta_i$ là một tập các thuộc tính, $i = 1, \ldots, m$.

Thuật toán chọn ngẫu nhiên giá trị $s \xleftarrow{\$} \mathbb{Z}_p$ , Tính $C, C_0$ như sau

$$C = \mathcal{M} \cdot e(g,g)^{\alpha \cdot s}, C_0 = g^s .$$

Tiếp theo, giải thuật so sánh giữa giá trị $m$ và $|\beta|$ , nếu $m \leq |\beta|$ giải thuật tính

$$C_1 = (g^a) \prod h_i)^s, \ldots, C_m = (g^a \prod_{i\in\beta_m} h_i)^s$$

Ngược lại, giải thuật xây dựng ma trận $M$ biểu diễn biểu thức $\beta$ , và một ánh xạ $\rho$ sao cho $(M, \rho) \in (\mathbb{Z}_p^{\ell\times n}, \mathcal{F}([\ell] \to [N]))$ . Giải thuật sau đó chọn một vector ngẫu nhiên $\vec{v} = (s, \mathcal{Y}_2, \ldots, \mathcal{Y}_n) \in \mathbb{Z}_p^n$ . Cho $i = 1, \ldots, \ell$ , tính $\lambda_i = \vec{v} \cdot M_i$ , trong đó $M_i$ là vector tương ứng với dòng thứ $i$ của ma trận $M$ . Giải thuật tiếp tục tính

$$C_i = g^{a.\lambda_i} h_{\rho(i)}^{-s}, i = 1, \ldots, \ell.$$

Cuối cùng, giải thuật cho đầu ra hoặc là $ct = (C, C_0, \ldots, C_m)$ cùng với mô tả của $\beta$ trong trường hợp $m \leq |\beta|$ , hoặc là $ct = (C, C_0, \ldots, C_\ell)$cùng với mô tả của $(M, \rho)$ trong trường hợp ngược lại.

**Giải Mã** $(ct, d_u, \text{param})$ : Thuật toán với đầu vào là khóa bí mật $d_u$, bản mã $ct$ và khóa công khai của hệ thống param, trước tiên sẽ phân tích bản mã $ct$, kiểm tra xem số phần tử có trong bản mã $ct$. Nếu số phần tử chính xác là $m + 1$ phần tử, thuật toán sẽ biểu diễn $ct$ dưới dạng $(C_0, C_1, \ldots, C_m)$, sau đó tìm chỉ số $j$ sao cho $\beta_j \subset \mathcal{B}(u)$ , và tính

$$\frac{e(C_0, d_{u_0} \prod_{i\in\beta_j} d_{u_i})}{e(d'_{u_0}, C_j)} = \frac{e(g^s, g^{\alpha} (g^a \prod_{i\in\beta_j} h_i)^{s_u})}{e(g^{s_u}, (g^a \prod_{i\in\beta_j} h_i)^s)} = e(g,g)^{\alpha\cdot s} = K$$

Cuối cùng tính $\mathcal{M} = C \cdot K^{-1}$ .

Ngược lại, thuật toán tạo ra tập $I \subset \{1,2,\ldots,\ell\}$ sao cho $I = \{i : \rho(i) \in B(u)\}$ . Đặt $\{\omega_i \in \mathbb{Z}_p\}_{i\in I}$ là tập các hằng số sao cho nếu $\{\lambda_i\}$ là các giá trị chia sẽ đúng của bất kỳ thành phần bí mật $s$ tương ứng với ma trận $M$ thì $\sum_{i\in I} \omega_i \lambda_i = s$ . Chú ý rằng từ mối liên hệ $\sum_{i\in I} \omega_i M_i = (1,0,\ldots,0)$ trong đó $M_i$ là dòng thứ $i$ của ma trận $M$ , thuật toán có thể tính được các hằng số này. Thuật toán tiếp tục biểu diễn $ct$ dưới dạng $(C, C_0, \ldots, C_\ell)$và tính

$$e(\prod_{i\in I} C_i^{-\omega_i}, d'_{u_0}) \cdot e(C_0, d_{u_0} \prod_{i\in I} d_{u_{\rho(i)}}^{-\omega_i}) = K.$$

sau đó tính $\mathcal{M} = C \cdot K^{-1}$.

**Tính Cửa Sập** $(d_u, W_i = (\widetilde{\omega}_{i_1}, \ldots, \widetilde{\omega}_{i_k}), \text{param})$: Giả sử rằng mỗi $\widetilde{\omega}_{i_j} \in \{0,1\}^*, j \in [k]$, là một sự kết hợp của tập các từ khóa, ví dụ "$Diabetes||Age: 30$".

Người dùng ngẫu nhiên chọn các giá trị $r_1, \ldots, r_k \in \mathbb{Z}_p$, tính cửa sập $\text{tds} = (\{\text{tds}_{0,j}, \text{tds}_{1,j}, \{\text{tds}_{2,j,\ell}\}_{\ell\in\mathcal{B}_u}\}_{j\in[k]}, \text{tds}_0, \{\text{tds}_i\}_{i\in\mathcal{B}(u)}, \widetilde{W}_i)$

$$= (\{g^{\alpha} g^{as_u} g^{ar_j} (\{g^{\alpha}\mathcal{H}(\widetilde{w}_{i_j}))^{\wedge}, g^{r_j}, \{\tilde{h}_{\ell}^{r_j}\}_{\ell\in\mathcal{B}_u}\}_{j\in[k]}, g^{s_u}, \{h_i^{s_u}\}_{i\in\mathcal{B}_u}, \widetilde{W}_i).$$

trong đó $\widetilde{W}_i$ là giá trị mô tả của $W_i$. Người dùng sau đó gửi $(\{\text{tds}_{0,j}\}_{j\in[k]}, \widetilde{W}_i)$ cho máy chủ (cloud server), và lưu giữ công khai phần còn lại của tds. Như vậy độ dài của cửa sập sẽ tuyến tính với số lượng sự kết hợp của các từ khóa mà người dùng muốn tìm kiếm.

**Mã Hóa Từ Khóa** $(\mathcal{KF}, \mathbb{A}', \text{param},)$ : Giả sử rằng chính sách mã hóa là $\mathbb{A}' = \beta = (\beta_1 \vee \cdots \vee \beta_m)$ và $\mathcal{KF} = (kf_1 \vee \cdots \vee kf_{m'})$, trong đó mỗi $\beta_i$ là một tập các thuộc tính và $kf_i$ là một sự kết hợp của các từ khóa. Chú ý rằng $\beta_i \neq \beta_j, kf_{i'} \neq kf_{j'}, \forall i,j \in [m], i', j' \in [m']$.

Thuật toán chọn ngẫu nhiên $s \xleftarrow{\$} \mathbb{Z}_p$, sau đó tính

$$C_0 = g^s, C_1 = (g^a \prod_{i\in\beta_1} h_i)^s, \ldots, C_m = (g^a \prod_{i\in\beta_m} h_i)^s,$$
$$\tilde{C}_1 = (g^a \prod_{i\in\beta_1} \tilde{h}_i)^s, \ldots, \tilde{C}_m = (g^a \prod_{i\in\beta_m} \tilde{h}_i)^s.$$

Tiếp theo, tính

$$X_i \; e(g,g)^{\alpha\cdot s} \cdot e(g, g^a \mathcal{H}(kf_i))^{\wedge\cdot s}, i = 1, \ldots, m',$$

sau đó tính.

$$K_1 = \widetilde{\mathcal{H}}(X_1, kf_1), \ldots, K_{m'} = \widetilde{\mathcal{H}}(X_{m'}, kf_{m'}).$$

Cuối cùng, thuật toán cho đầu ra

$$ct' = (C_0, \ldots, C_{,}, \tilde{C}_1, \ldots, \tilde{C}_m, K_1, \ldots, K_{m'})$$

cùng với bản mô tả của $\beta$.

**Tìm Kiếm** $(\text{tds}, ct', \text{param})$: Máy chủ (cloud server) tìm $\ell \in [m]$ sao cho $\beta_\ell \subset \mathcal{B}(u)$, sau đó tính $(X_j, Y_j), j = 1, \ldots, k$

$$X_j = \frac{e(C_0, \text{tds}_{0,j} \prod_{i\in\beta_\ell} \text{tds}_i \cdot \text{tds}_{2,j,i})}{e(\text{tds}_0, C_\ell) \cdot e(\text{tds}_{1,j}, \tilde{C}_\ell)}$$

$$= \frac{e(g^s, g^{\alpha} g^{as_u} g^{ar_j} g^{a\wedge}\mathcal{H}(\widetilde{w}_{ij})^{\wedge} \prod_{i\in\beta_\ell} h_i^{s_u} \tilde{h}_i^{r_j}}{e(g^{s_u}, (g^a \prod_{i\in\beta_\ell} h_i)^s) \cdot e(g^{r_j}, (g^a \prod_{i\in\beta_\ell} \tilde{h}_i)^s)}$$

$$= e(g,g)^{\alpha\cdot s} \cdot e\left(g, g^a \mathcal{H}\left(\widetilde{w}_{i_j}\right)\right)^{\wedge\cdot s},$$

$Y_j = \mathcal{H}(X_j, \widetilde{w}_{i_j})$.

Nếu tồn tại một cặp $(i,j), i \in [m'], j \in [k]$ sao cho $K_i = Y_j$ thì máy chủ cho đầu ra là "yes". Ngược lại máy chủ cho đầu ra là "no". Chú ý rằng, máy chủ không cần thiết phải tính rất cả các cặp $(X_j, Y_j), j = 1, \ldots, k$ , miễn là máy chủ tìm được một cặp $(i,j), i \in [m'], j \in [k]$ sao cho$K_i = Y_j$ , máy chủ cho đầu ra là "yes" và dừng lại.

**Tính đúng đắn**: Chúng ta thấy rằng nếu tồn tại một cặp $\widetilde{w}_{i_j} \in W_i$ và $kf_t \in \mathcal{KF}$ sao cho $\widetilde{w}_{i_j} = kf_t$ , thì

$$X_t = e(g,g)^{\alpha \cdot s} \cdot e(g, g^a \mathcal{H}(kf_t))^{\lambda \cdot s} = e(g,g)^{\alpha \cdot s} \cdot e(g, g^a \mathcal{H}(\widetilde{w}_{i_j}))^{\lambda \cdot s} = X_j ,$$

có nghĩa là

$$K_t = \widetilde{\mathcal{H}}(X_t, kf_t) = \widetilde{\mathcal{H}}(X_j, \widetilde{w}_{i_j}) = Y_j .$$

### 3.5. Kết luận chương 3

Trong chương này nghiên cứu sinh đã trình bày về hệ mã hóa dựa trên thuộc tính. Với các hệ mã hóa dựa trên thuộc tính tham số quan trọng nhất đó là độ dài của bản mã, trong chương này nghiên cứu sinh đã trình bày hai đóng góp trong hệ mã hóa dựa trên thuộc tính do nghiên cứu sinh đề xuất, hệ thứ nhất có tính chất là độ dài bản mã chỉ là hằng số, cụ thể chỉ là hai phần tử tối ưu nhất trong các hệ mã đang có hiện nay. Phần tiếp theo nghiên cứu sinh trình bày về hệ mã hóa dựa trên thuộc tính thứ hai do nghiên cứu sinh đề xuất, hệ này có hỗ trợ tính chất là tìm kiếm trên dữ liệu đã được mã hóa.

## KẾT LUẬN

Các hệ mã hóa với quyền giải mã linh động như mã hóa quảng bá, hệ mã hóa quảng bá đa kênh hay mã hóa dựa trên thuộc tính đang được sử dụng rộng rãi trong thực tế hiện nay, đặc biệt trong các ứng dụng như truyền hình trả tiền, chia sẽ files, social network (facebooks, twitter,...), lưu trữ an toàn dữ liệu trên đám mây cho mọi loại ứng dụng như e-Health, chính phủ điện tử, ... Tuy nhiên vẫn còn nhiều vấn đề mở đối với ba loại hệ mã hóa này mà các nhà nghiên cứu hiện nay vẫn chưa giải quyết được. Trong luận án này đóng góp cụ thể đối với lĩnh vực này như sau:

1. Đóng góp thứ nhất: Đề xuất một lược đồ mã hóa quảng bá đa kênh dựa trên hệ Delerablee [25] có độ hiệu quả và an toàn tương tự như hệ [47, 15] nhưng ở dạng mã hóa công khai, không còn ở dạng bí mật. Được công bố tại công trình số 4.

2. Đóng góp thứ hai: Đề xuất lược đồ CP-ABE mới, có khóa bí mật ngắn hơn các hệ CP-ABE khác. Các hệ khác có cùng tính chất, độ dài bản mã là hằng số. Điểm yếu của đề xuất so với các hệ mã này là, có mức độ an toàn yếu hơn các hệ khác cso cùng tính chất. Nội dung đề xuất được công bố tại công trình số 4.

3. Đóng góp thứ 3: Đề xuất mới, dựa trên hệ ABE hiện có [42], xây dựng một lược đồ ABE mới hỗ trợ tìm kiếm trên dữ liệu đã được mã hóa; được công bố tại công trình số 2.

**Các hướng nghiên cứu tiếp theo NCS đề xuất như sau**:

1. Xây dựng MCBE có độ dài khóa bí mật ngắn hơn các hệ hiện có mà vẫn giữ được độ dài bản mã là hằng số.

2. Xây dựng phi tập trung hóa MCBE, hiện nay vẫn chưa tồn tại hệ phi tập trung hóa MCBE nào.

3. Xây dựng CP-ABE có tính chất là cả đội dài bản mã và độ dài khóa bí mật đều là hằng số. Lưu ý rằng, các hệ mã hóa quảng bá đã có tính chất này nên tồn tại hệ CP-ABE như vậy là khả thi

## CÁC CÔNG TRÌNH CÔNG BỐ TRONG LUẬN ÁN

1.Trinh Viet Cuong, Trinh Van Anh, Do Thi Thu Hien, Do Thi Thanh Hien, Tran Cam Van, Tran Vinh Duc. Anonymous Key Leakage Attack on Attribute-based Encryption. *Kỷ yếu hội thảo quốc gia @ năm 2018.*

2. Van Anh Trinh, Viet Cuong Trinh. A Ciphertext-policy Attribute-based Searchable Encryption Scheme in Non-interactive Model. *Journal of Computer Science and Cybernetics, Volume 35, Pages 233-249, 2019,*

3. Van Anh Trinh, Viet Cuong Trinh. One-Verifier Signature Scheme and Its Applications. *In Proceeding of The 10th International Symposium on Information and Communication Technology - SoICT 2019, December 4 – 6, 2019, Ha Noi - Ha Long Bay, Viet Nam.*

4. Minh Ha Le, Vinh Duc Tran, Van Anh Trinh, Viet Cuong Trinh. Compacting Ciphertext in Multi-Channel Broadcast Encryption and Attribute-Based Encryption. *Theoretical Computer Science, Volume 804, 12 January 2020, Pages 219-235. (ISI-SCIE)*