TRƯỜNG ĐẠI HỌC AN GIANG

**KHOA CÔNG NGHỆ THÔNG TIN**



Tiểu luận học phần

AN TOÀN HỆ THỐNG VÀ AN NINH MẠNG

**TÊN TIỂU LUẬN**

# TÌM HIỂU GIẢI THUẬT MÃ HÓA CP-ABE

Thành viên: Giáo viên hướng dẫn:

Võ Phát Thành - DTH216157 TS: Lê Hoàng Anh

Ngô Thanh Phong - DTH216080

Nguyễn Trường Vũ - DTH216251

12/2024

**MỤC LỤC**

[TÌM HIỂU GIẢI THUẬT MÃ HÓA CP-ABE 1](#_Toc184741031)

[1. GIỚI THIỆU 4](#_Toc184741032)

[2. THUẬT TOÁN 4](#_Toc184741033)

[2.1. Khái niệm 4](#_Toc184741034)

[2.1. Các công thức toán học trong CP-ABE 5](#_Toc184741035)

[3. DEMO 11](#_Toc184741036)

[3.1. Khởi tạo các giá trị PK: 11](#_Toc184741037)

[3.2. Tạo MK: 11](#_Toc184741038)

[3.3. Tạo hàm mã hóa thông tin: 12](#_Toc184741039)

[3.4. Hàm tạo đa thức ngẫu nhiên: 12](#_Toc184741040)

[3.5. Hàm tính giá trị của một đa thức tại một điểm z: 12](#_Toc184741041)

[3.6. Hàm tạo SK: 13](#_Toc184741042)

[3.7. Hàm giải mã: 13](#_Toc184741043)

[3.8 Hàm giải mã từng node: 14](#_Toc184741044)

[3.9. Hàm main: 15](#_Toc184741046)

[3.10. Kết quả: 16](#_Toc184741047)

[4. KẾT LUẬN 16](#_Toc184741048)

[4.1.Ưu điểm 16](#_Toc184741049)

[4.2. Khuyết điểm 16](#_Toc184741050)

[4.3. Ứng dụng: 17](#_Toc184741051)

[Tài liệu tham khảo 18](#_Toc184741052)

**DANH MỤC HÌNH**

[Hình 1: Public Key 5](#_Toc184741053)

[Hình 2: Ciphertext 6](#_Toc184741054)

[Hình 3: Secret Key 7](#_Toc184741055)

[Hình 4: Giải mã node 8](#_Toc184741056)

[Hình 5: Node không thể giải mã 8](#_Toc184741057)

[Hình 6: Tính cho node không phải lá 9](#_Toc184741058)

[Hình 7: Cách tính A tại root 9](#_Toc184741059)

[Hình 8: Công thức giải mã M 9](#_Toc184741060)

[Hình 9: Tạo Key ủy thác 10](#_Toc184741061)

[Hình 10: Khởi tạo 11](#_Toc184741062)

[Hình 11: Tạo Master Key 11](#_Toc184741063)

[Hình 12: Mã hóa 12](#_Toc184741064)

[Hình 13: Tạo đa thức 12](#_Toc184741065)

[Hình 14: Tính đa thức 12](#_Toc184741066)

[Hình 15: Tạo khóa cá nhân 13](#_Toc184741067)

[Hình 16: Giải mã 13](#_Toc184741068)

[Hình 17: Giải mã tại node 14](#_Toc184741069)

[Hình 18: main 15](#_Toc184741070)

[Hình 19: kết quả 16](#_Toc184741071)

# GIỚI THIỆU

Trong kỷ nguyên công nghệ, với sự phát triển không ngừng của công nghệ số song song với đó là nỗi lo về an toàn thông tin khi mà bản thân thông tin cũng trở thành một loại tài sản khi sử dụng không gian mạng. Bên cạnh đó sự tiện ích của điện toán đám mây trong việc tiết kiệm chi phí cũng đã giúp doanh nghiệp tăng phần nào lợi nhuận. Với những ưu điểm như lưu trữ được lượng dữ liệu lớn điện toán đám mây cũng không khỏi có những nhược điểm về vấn đề an toàn vì ta không thể nào chắc chắn dữ liệu sẽ không bị tấn công, lấy cắp nhằm mục đích trục lợi trong hoàn cảnh máy chủ bị hư hại và liệu rằng quyền truy cập của người dùng có thật sự hiệu quả. Do đó việc áp dụng mã hóa dữ liệu là điều cần thiết để đảm bảo tính bảo mật và toàn vẹn của thông tin. Giải thuật mã hóa (encryption algorithm) là một tập hợp các quy tắc hoặc quy trình được sử dụng để biến đổi dữ liệu (thông điệp, tệp tin, hoặc sensitive data) từ dạng plain text sang dạng mã hóa (cipher text) nhằm bảo vệ thông tin khỏi việc truy cập trái phép. Dữ liệu đã mã hóa chỉ có thể được giải mã và đọc bởi những người hoặc hệ thống có khóa hoặc thông tin cần thiết để giải mã.Một trong những giải thuật có độ tin tưởng cao trong việc mã hóa giữ liệ đó chính là giải thuật mã hóa dựa trên thuộc tính (ciphertext policy attribute-based encryption: CP-ABE).

# 2. THUẬT TOÁN

## 2.1. Khái niệm

* Trong nhiều hệ thống phân tán, một người dùng chỉ có thể truy cập đến dữ liệu nếu sở hữu một tập hợp các ủy nhiệm hoặc thuộc tính. Hiện nay, phương pháp duy nhất để thi hành chính sách trên là sử dụng một server tin cậy để lưu trữ dữ liệu và làm trung gian trong việc quản lý quyền truy cập. Tuy nhiên, nếu server lưu trữ dữ liệu bị tổn hại, thì tính bí mật của dữ liệu lưu trữ ở đó cũng bị xâm phạm.
* Khái niệm mã hóa dựa trên thuộc tính (Attribute-based Encryption - ABE) được đề xuất bởi Sahai và Waters, trong bài báo “Mã hóa dựa trên định danh mờ Fuzzy IBE”. Trong mã hóa dựa trên thuộc tính, một bên tham gia sẽ mã hóa một tài liệu sử dụng cho tất cả những người dùng cùng sở hữu một tập hợp thuộc tính nào đó. Trong hệ thống CP- ABE, khóa riêng của người dùng sẽ được liên kết với một số tùy ý các thuộc tính, được diễn đạt dưới dạng các xâu. Mặt khác, khi một bên mã hóa thông báo trong hệ thống này, họ xác định một cấu trúc truy cập có liên quan đến các thuộc tính. Một người dùng chỉ có thể giải mã một bản mã nếu các thuộc tính của người dùng thỏa mãn cấu trúc truy cập. Ở mức toán học, trong hệ thống CP- ABE cấu trúc truy cập được mô tả dưới dạng monotonic access tree, ở đó các nút của cấu trúc truy cập được tạo bởi threshold gates và “the leaves” là những thuộc tính. Ví dụ, trong một khoa giảng dạy về khoa học máy tính, một văn bản được mã hóa và dùng cho tất cả hệ thống của khoa. Trong trường hợp này, người ta sẽ mã hóa cả các định danh {"khoa", "hệ thống"}. Bất kỳ người dùng nào có định danh chứa tất cả các thuộc tính trên mới có thể giải mã được văn bản. Với việc sử dụng mã hóa dựa trên thuộc tính chính sách hướng bản mã (CP- ABE) dữ liệu mã hóa có thể được giữ bí mật, thậm chí khi server dữ liệu không còn đáng tin cậy và phương pháp này cũng an toàn đối với Tấn công thông đồng (collusion attacks).[1]

## 2.1. Các công thức toán học trong CP-ABE

Giải thuật mã hóa CP-ABE dựa trên 4 thuật toán[2], [3]: Setup, Encrypt, KeyGen, and Decrypt. Thêm vào đó có 1 thuật toán được bổ sung là Delegate.

* Setup (Khởi tạo): Thuật toán chỉ nhận vào tham số bảo mật ẩn và outputs là các tham số công khai (PK) và một master key (MK). Thuật toán sẽ chọn một nhóm song tuyến tính G0​​ có bậc nguyên tố p với phần tử sinh g. Tiếp theo, nó sẽ chọn hai số mũ ngẫu nhiên α,β∈Zp​. Khóa công khai sẽ được public như sau:

Với:

Hình 1: Public Key

**G₀** là một nhóm có bậc (số phần tử ) r là số nguyên tố, là chiều dài của khóa, là nhóm hữu hạn có cấp nguyên tố p, được chọn sao cho có ánh xạ song tuyến tính e. Là nền tảng cho các phép toán mã hóa và giải mã trong hệ thống.

**g** là phần tử sinh của nhóm G₀. Tất cả các thành phần khác trong hệ thống được sinh ra từ g và được công khai như một phần của khóa công khai PK.

**α,β∈Zp** là một số nguyên ngẫu nhiên được chọn trong tập các số nguyên modulo 𝑝, bảo mật của hệ thống phụ thuộc vào việc giữ bí mật giá trị α,β.

**h=gβ** là một thành phần của khóa công khai PK, được sử dụng trong quá trình mã hóa.

**f=g1/β** được sử dụng để xác minh thuộc tính hoặc giải mã trong các thuật toán liên quan và chỉ sử dụng trong ủy quyền.

**e(g,g)α** là kết quả của ánh xạ song tuyến tính e, được tính từ g và α

Và khóa bí mật master key cũng được tính là MK = (β,gα).

* Encrypt (Mã hóa): Thuật toán mã hóa nhận đầu vào là tham số công khai (PK), thông điệp M và một cấu trúc truy cập A trên tập hợp các thuộc tính. Thuật toán sẽ mã hóa M và tạo ra bản mã CT, sao cho chỉ những người dùng sở hữu tập thuộc tính thỏa mãn cấu trúc truy cập A mới có thể giải mã thông điệp. Chúng ta giả định rằng bản mã CT ngầm chứa cấu trúc truy cập A. Quy trình được thực hiện như sau:

1. **Chọn đa thức cho mỗi nút**:  
   Thuật toán chọn một đa thức qx cho từng nút x (bao gồm cả lá) trong cây T. Các đa thức này được chọn từ trên xuống, bắt đầu từ nút gốc R.

* Bậc của đa thức qx được đặt bằng dx ​= kx​ − 1, trong đó kx​ là giá trị ngưỡng của nút x.

1. **Định nghĩa đa thức tại nút gốc**:

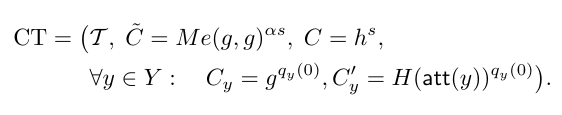
* Tại nút gốc R, thuật toán chọn một giá trị ngẫu nhiên s∈Zp​ và đặt qR​(0)=s.
* Sau đó, thuật toán chọn ngẫu nhiên s∈Zp​ điểm khác để hoàn toàn xác định đa thức qR.

1. **Định nghĩa đa thức tại các nút khác**:

* Với bất kỳ nút nào x khác nút gốc, thuật toán đặt qx​(0)=qparent(x)​(index(x)), trong đó:
  + parent(x) là nút cha của x.
  + index(x) là chỉ số xác định vị trí của x trong danh sách các con của nút cha.
* Sau đó, thuật toán chọn ngẫu nhiên dx điểm khác để xác định hoàn toàn đa thức qx.

1. **Tạo bản mã**:

* Gọi Y là tập hợp các nút lá trong cây T.
* Bản mã được xây dựng bằng cách cung cấp cấu trúc truy cập cây T và tính toán các giá trị liên quan dựa trên T.

Cụ thể các bước tiếp theo sẽ tính toán chi tiết giá trị của bản mã, đảm bảo thông điệp M chỉ có thể được giải mã nếu cấu trúc truy cập T được thỏa mãn.

Hình 2: Ciphertext

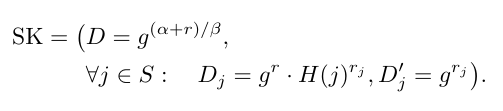
Với:

* **T**: Cấu trúc truy cập (Access structure) đảm bảo rằng chỉ những người dùng có tập thuộc tính phù hợp với T mới giải mã được.
* **C~=M\*e(g,g)αs** là thành phần mã hóa thông điệp M và s là tham số ngẫu nhiên được chọn trong quá trình mã hóa
* **C=hs** giữ vai trò liên kết giữa tham số ngẫu nhiên sss và khóa công khai h, trong đó h là thành phần công khai của PK.
* Với mỗi thuộc tính y∈Y:
  + **Cy =gqy(0)** là thành phần dựa trên một hàm qy​(x) tại điểm x=0. Dùng để mã hóa thông tin liên quan đến thuộc tính y bằng cách sử dụng hàm bí mật qy(x).
  + **Cy​’=H(att(y))qy​(0)** là hành phần phụ thuộc vào giá trị băm H(att(y)), tương ứng với thuộc tính y.
* Key Generation (Tạo khóa): Thuật toán tạo khóa nhận đầu vào gồm khóa chính (master key) MK và một tập hợp các thuộc tính S mô tả khóa. Thuật toán sẽ tạo ra và xuất ra khóa riêng (private key) SK. Quy trình thực hiện như sau:

1. **Chọn giá trị ngẫu nhiên**:

* Thuật toán chọn một giá trị ngẫu nhiên r∈Zp​​.
* Sau đó, với mỗi thuộc tính j∈S, chọn ngẫu nhiên một giá trị rj​∈Zp​.

1. **Tính toán khóa**:

* Khóa được tính dựa trên các giá trị r và rj, cùng với các thành phần liên quan đến hệ thống (như khóa công khai hoặc các tham số cụ thể).

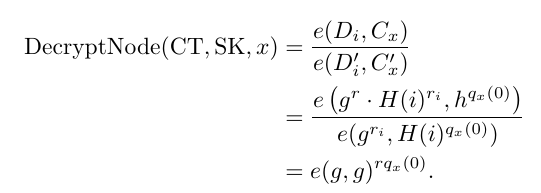
Hình 3: Secret Key

Với:

* **D=g(α+r)/β​**: Là thành phần chung, được tính từ các tham số công khai và các giá trị ngẫu nhiên, đảm bảo rằng khóa bí mật của người dùng là hợp lệ khi kết hợp với các tham số công khai. Trong đó:
  + g: Là phần tử sinh của nhóm G0​.
  + α: Là tham số bí mật được chọn trong quá trình thiết lập khóa công khai.
  + r: Là một giá trị ngẫu nhiên được chọn trong quá trình tạo khóa bí mật.
  + β: Là tham số công khai từ khóa công khai (public key).
* **Dj​=grH(j)** và **Dj′=grj​** là các thành phần tương ứng với từng thuộc tính j của người dùng, chứa các giá trị bí mật được tính từ thuộc tính của người dùng và các giá trị ngẫu nhiên r và rj ,​liên quan đến từng thuộc tính, giúp xác định xem người dùng có quyền giải mã thông điệp hay không, tùy thuộc vào việc người dùng có thuộc tính j hay không. Trong đó:
  + H(j): Là hàm băm (hash function) áp dụng lên thuộc tính j, và giá trị H(j) sẽ có giá trị phụ thuộc vào thuộc tính cụ thể của người dùng.
  + r: Là giá trị ngẫu nhiên được chọn khi tạo khóa bí mật. Mỗi thuộc tính sẽ có giá trị rrr riêng biệt.
  + rj​: Là một giá trị ngẫu nhiên riêng biệt cho thuộc tính j. Đây là một giá trị bí mật liên quan đến thuộc tính j.
* Decrypt (Giải mã): Thuật toán giải mã nhận đầu vào gồm tham số công khai PK, bản mã CT (chứa chính sách truy cập A), và khóa riêng SK tương ứng với một tập hợp thuộc tính S. Nếu tập thuộc tính S thỏa mãn cấu trúc truy cập A, thuật toán sẽ giải mã bản mã và trả về thông điệp M. Cụ thể, chúng ta định nghĩa một thuật toán đệ quy **DecryptNode(CT, SK, x)**, trong đó đầu vào gồm ciphertext CT=(T, C~,C,∀y∈Y:Cy,C’y), khóa bí mật SK liên kết với một tập thuộc tính S, và một nút x trong cây T.

Trường hợp 1: Nút lá

Nếu nút x là nút lá, ta định nghĩa i=att(x) và quy trình giải mã sẽ như sau:

* Nếu i∈S, ta tính:

Hình 4: Giải mã node

Với:

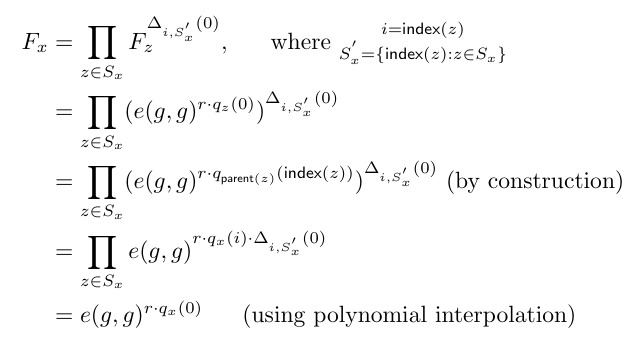
* Cx​ và C’x là các thành phần của bản mã CT, với x là thuộc tính mà người dùng muốn giải mã.
* Cx​=hqx​(0) là thành phần của bản mã được mã hóa với tham số qx(0), liên quan đến thuộc tính x
* C’x​ là thành phần liên quan đến ánh xạ các thuộc tính, có thể được mã hóa theo các thông số khác của hệ thống.
* Di​ và D’i​ là các phần của khóa bí mật SK, được tính toán từ các thuộc tính người dùng và các giá trị bí mật của người dùng đó.
* Di​=gri​⋅H(i)ri​ là thành phần liên quan đến thuộc tính i, và ri là tham số ngẫu nhiên được sử dụng trong khóa bí mật.
* D’i​=gri​ là một phần khác trong khóa bí mật, được tính toán từ thuộc tính i và giá trị ngẫu nhiên ri​.
* Nếu i∉S, ta định nghĩa:

(nghĩa là không thể giải mã)

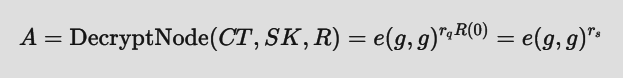
Hình 5: Node không thể giải mã

Trường hợp 2: Không phải nút lá

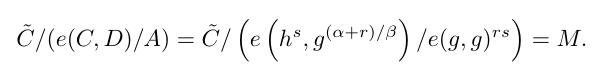
Khi x là nút không phải lá, thuật toán tiếp tục như sau:

* Đối với tất cả các nút z là con của x, gọi đệ quy **DecryptNode(CT, SK, z)** và lưu trữ kết quả vào Fz​.
* Xác định một tập hợp Sx​ là tập hợp con kx-phần tử của các nút con z sao cho Fz=⊥. Nếu không tồn tại một tập hợp như vậy, tức là không thỏa mãn yêu cầu và hàm trả về ⊥.
* Nếu có, ta tính như sau:

Hình 6: Tính cho node không phải lá

Sau khi đã định nghĩa hàm **DecryptNode**, thuật toán giải mã bắt đầu bằng cách gọi hàm này tại nút gốc R của cây T. Nếu cây được xác nhận bởi tập thuộc tính S, ta có:

Hình 7: Cách tính A tại root

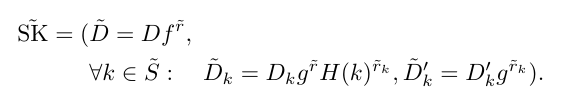
Thuật toán sau đó giải mã thông điệp bằng cách tính:

Hình 8: Công thức giải mã M

Với:

* C~ là một thành phần của bản mã, được mã hóa từ thông điệp M kết hợp với các tham số ngẫu nhiên như α,β,s
* e(C,D) Là phép toán song tuyến tính được tính từ thành phần C trong bản mã và D trong khóa bí mật. Thành phần này giúp tạo điều kiện giải mã thông điệp M, bằng cách loại bỏ các tham số không cần thiết.
* hs: Là giá trị tính từ tham số h (thuộc khóa công khai) lũy thừa s (giá trị ngẫu nhiên của bản mã).
* g(α+r)/β: Là một phần trong phép mã hóa, phụ thuộc vào tham số ngẫu nhiên r, tham số hệ thống α,β.
* e(g,g)rs Là giá trị tính toán từ tham số ngẫu nhiên r và s, được mã hóa trong bản mã.
* M: Đây là thông điệp gốc cần được giải mã.
* Delegate (Ủy quyền): Thuật toán ủy quyền nhận đầu vào gồm khóa bí mật (secret key) SK cho một tập hợp các thuộc tính S và một tập hợp con của S. Thuật toán sẽ xuất ra khóa bí mật mới cho tập hợp các thuộc tính trong tập con của S có dạng:

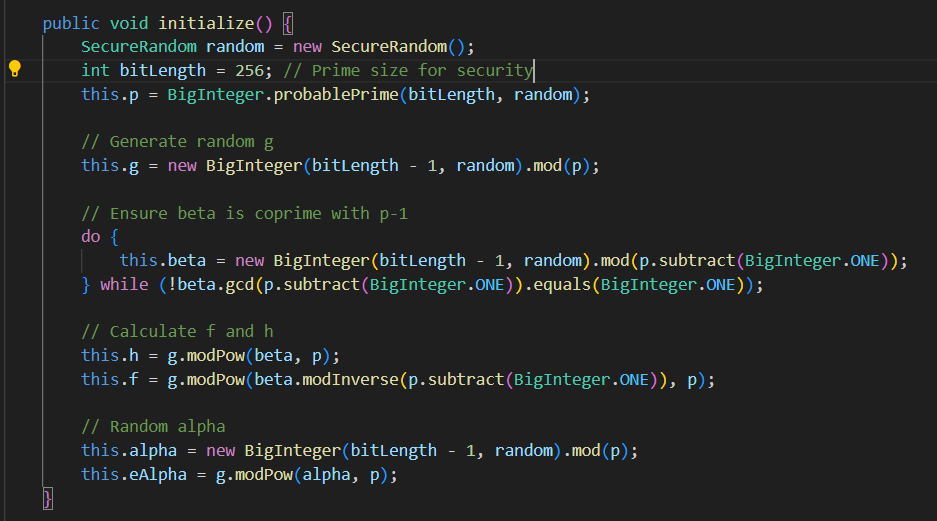
Hình 9: Tạo Key ủy thác

Với:

* D: Thành phần chính của khóa bí mật ban đầu SK, được tạo từ tham số hệ thống α,β và các giá trị ngẫu nhiên r trong quá trình sinh khóa.
* fr~:
* f=g1/β là một tham số trong khóa công khai PK.
* r~ là giá trị ngẫu nhiên mới được chọn trong quá trình tạo khóa ủy quyền. Nó đảm bảo rằng khóa được ủy quyền vẫn giữ được tính bảo mật.
* D~: Thành phần mới trong khóa bí mật ủy quyền SK~, được điều chỉnh bởi fr~.
* D~k​:
* Thành phần tương ứng với thuộc tính k∈S~ trong khóa bí mật ủy quyền.
* Dk: Thành phần tương ứng với k trong khóa bí mật ban đầu.
* gr~: Phần điều chỉnh từ giá trị ngẫu nhiên mới r~.
* H(k)r~k​: Băm thuộc tính k được lũy thừa với giá trị ngẫu nhiên rk​~, tăng cường tính bảo mật.
* D~′k​:
  + - * Thành phần bổ sung cho thuộc tính k trong khóa bí mật ủy quyền.
      * D’k: Thành phần tương ứng trong khóa bí mật ban đầu.
      * gr~k​: Điều chỉnh từ giá trị ngẫu nhiên rk​~​.

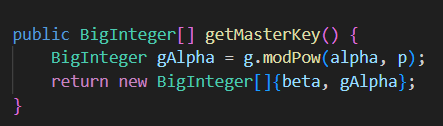
# 3. DEMO

## 3.1. Khởi tạo các giá trị PK:



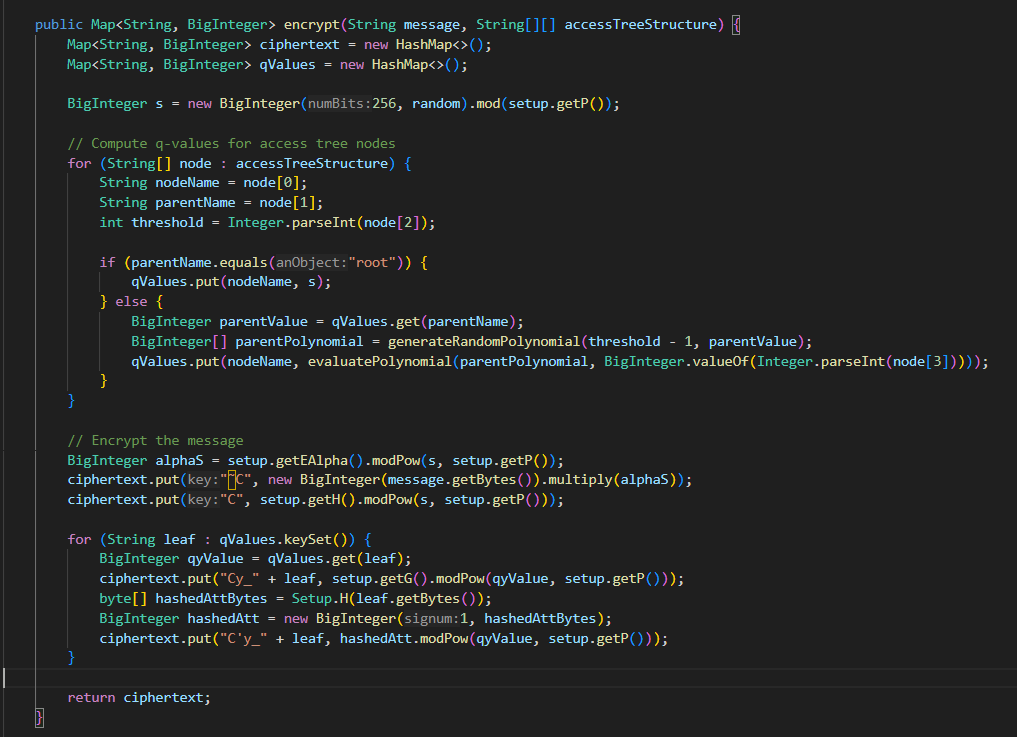
Hình 10: Khởi tạo

## 3.2. Tạo MK:



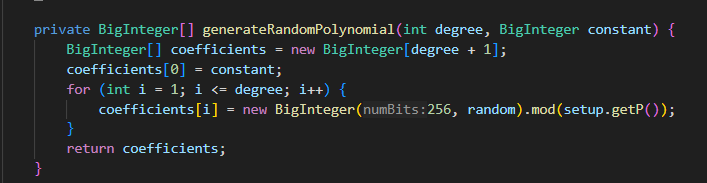
Hình 11: Tạo Master Key

## 3.3. Tạo hàm mã hóa thông tin:



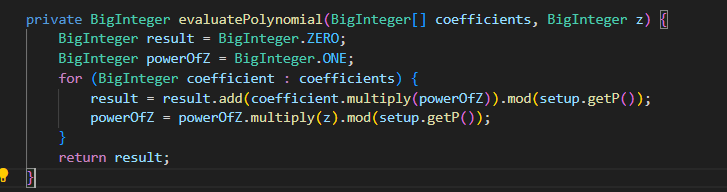
Hình 12: Mã hóa

## 3.4. Hàm tạo đa thức ngẫu nhiên:



Hình 13: Tạo đa thức

## 3.5. Hàm tính giá trị của một đa thức tại một điểm z:



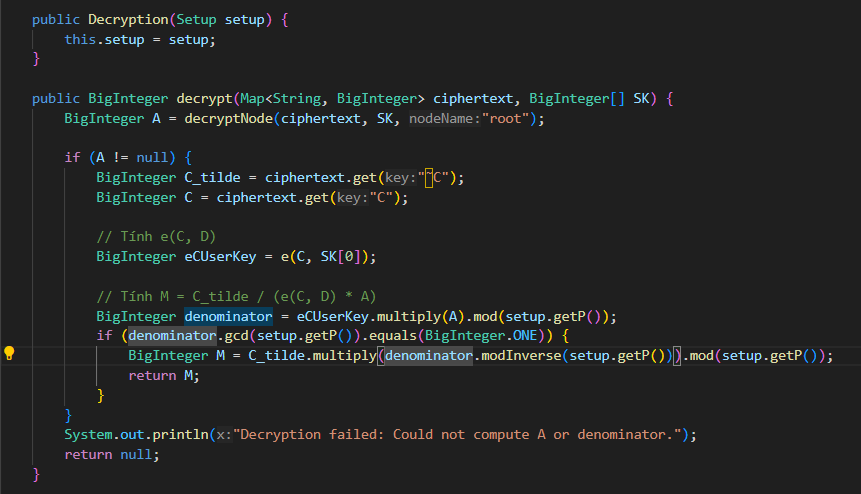
Hình 14: Tính đa thức

## 3.6. Hàm tạo SK:



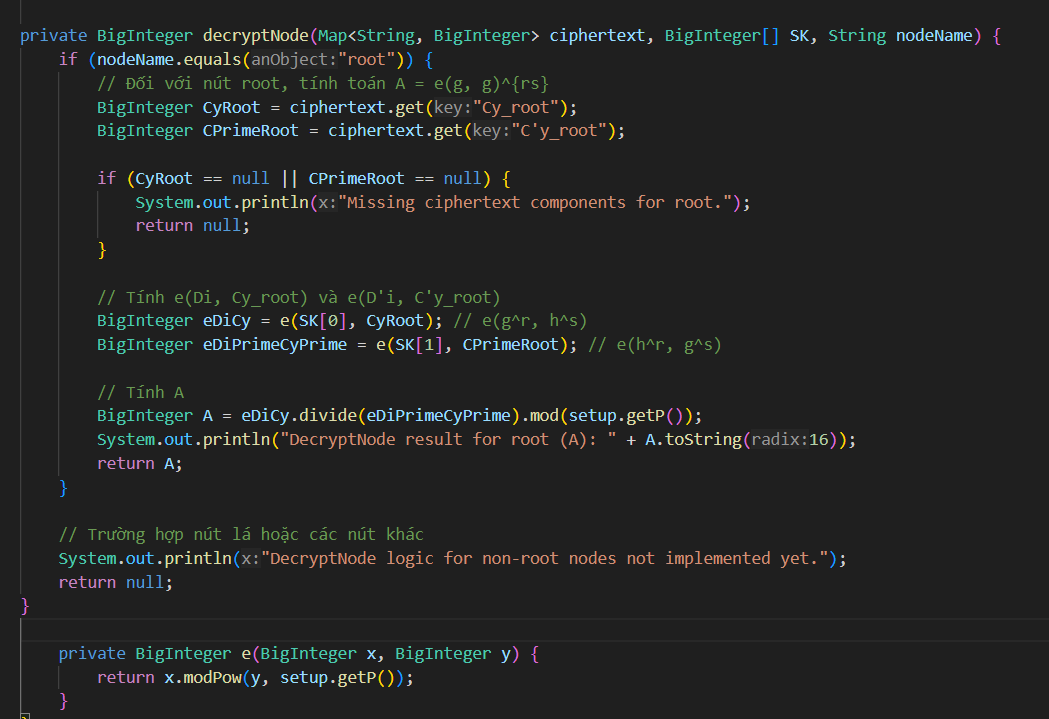
Hình 15: Tạo khóa cá nhân

## 3.7. Hàm giải mã:



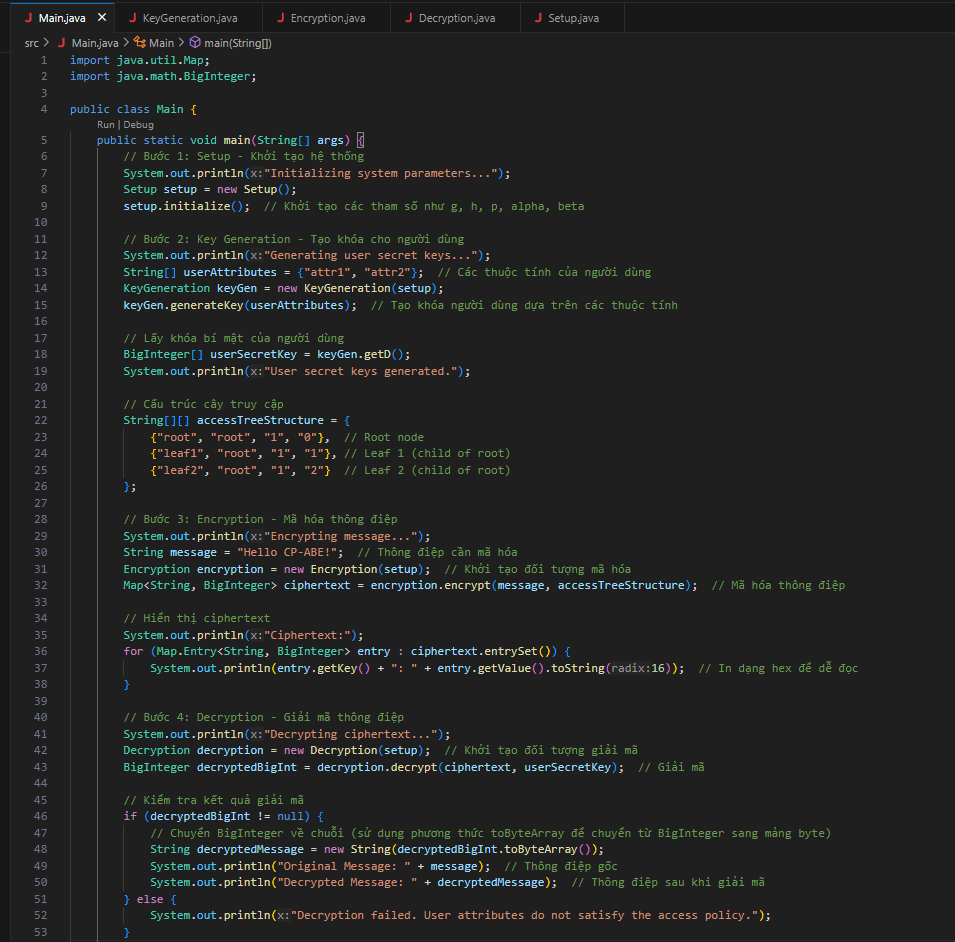
Hình 16: Giải mã

## 3.8 Hàm giải mã từng node:



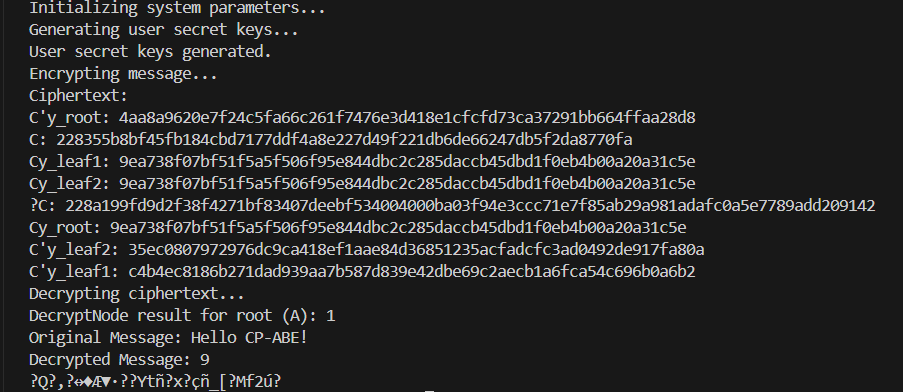
Hình 17: Giải mã tại node

## 3.9. Hàm main:



Hình 18: main

## 3.10. Kết quả:



Hình 19: kết quả

# 4. KẾT LUẬN

Hệ thống mã hóa dựa trên thuộc tính với cấu trúc truy cập cây (**CP-ABE**) là một giải pháp hiệu quả và linh hoạt để đảm bảo an toàn thông tin trong các hệ thống phân tán, đặc biệt là trong môi trường đòi hỏi quản lý truy cập dựa trên chính sách như điện toán đám mây.

Mặc dù CP-ABE có nhiều ưu điểm, nhưng hệ thống này cũng tồn tại một số hạn chế như hiệu suất giảm khi số lượng thuộc tính hoặc độ phức tạp của chính sách truy cập tăng. Tuy nhiên, với những cải tiến và tối ưu hóa trong tương lai, CP-ABE sẽ tiếp tục là một trong những giải pháp tiềm năng trong lĩnh vực bảo mật dữ liệu hiện đại.4

## 4.1. Ưu điểm

* Kiểm soát truy cập linh hoạt: Cho phép định nghĩa chính sách truy cập phức tạp dựa trên thuộc tính của người dùng, đảm bảo dữ liệu chỉ được truy cập bởi những người dùng có quyền hợp lệ.
* Bảo mật cao: Dữ liệu được mã hóa theo chính sách truy cập, đảm bảo rằng ngay cả khi khóa công khai bị lộ, dữ liệu vẫn không bị giải mã nếu không có khóa bí mật phù hợp.
* Không cần liên lạc với bên thứ ba: Người dùng không cần liên hệ với máy chủ quản lý quyền để xác minh, giảm thiểu rủi ro và độ trễ.
* Ứng dụng rộng rãi: Thích hợp cho các hệ thống phân tán như điện toán đám mây, Internet of Things (IoT), và các môi trường yêu cầu chia sẻ dữ liệu an toàn.

## 4.2. Khuyết điểm

* Hiệu suất thấp trên tập dữ liệu lớn: Quá trình mã hóa và giải mã yêu cầu nhiều phép tính song tuyến tính, gây tốn kém tài nguyên tính toán, đặc biệt với các thiết bị có cấu hình thấp.
* Quản lý khóa phức tạp: Khi số lượng người dùng và thuộc tính tăng, việc quản lý và phân phối khóa bí mật trở nên khó khăn.
* Hạn chế trong việc cập nhật chính sách: Nếu chính sách truy cập thay đổi, cần mã hóa lại dữ liệu, điều này không hiệu quả với lượng dữ liệu lớn.
* Vấn đề với người dùng rời khỏi hệ thống: Khi một người dùng rời khỏi hệ thống hoặc mất quyền truy cập, việc thu hồi quyền của họ khó thực hiện mà không ảnh hưởng đến toàn bộ hệ thống.
* Tăng chi phí lưu trữ: Ciphertext trong CP-ABE thường lớn hơn đáng kể so với dữ liệu gốc, làm tăng yêu cầu lưu trữ.

## 4.3. Ứng dụng:

**Chia sẻ dữ liệu an toàn trong mạng IoT (Internet of Things)**:

* Đảm bảo dữ liệu được truyền giữa các thiết bị IoT được mã hóa để tránh bị đánh cắp hoặc chỉnh sửa bởi các tác nhân độc hại.
* Sử dụng các giao thức bảo mật hiện đại như TLS hoặc DTLS trong việc trao đổi dữ liệu giữa các thiết bị.

**Quản lý quyền truy cập tài liệu**:

* Thiết lập các cấp độ quyền truy cập rõ ràng cho từng nhóm người dùng hoặc cá nhân dựa trên vai trò và trách nhiệm của họ.
* Sử dụng hệ thống xác thực đa yếu tố (MFA) để tăng cường bảo mật khi truy cập vào tài liệu quan trọng.

**Bảo vệ hồ sơ y tế điện tử (Electronic Medical Records - EMRs)**:

* Sử dụng các tiêu chuẩn bảo mật y tế như HIPAA hoặc ISO 27799 để đảm bảo an toàn thông tin.
* Mã hóa toàn bộ hồ sơ y tế điện tử khi lưu trữ và truyền tải để tránh rủi ro rò rỉ dữ liệu.
* Đảm bảo chỉ những nhân viên y tế có quyền hạn cụ thể mới có thể truy cập vào các phần thông tin phù hợp của hồ sơ bệnh nhân.

# 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] Tắt T., “HỆ MÃ HÓA DỰA TRÊN THUỘC TÍNH MỚI HỖ TRỢ TÍNH CHẤT PHI TẬP TRUNG HÓA”.

[3] A. T. T. Tin, “Mã hóa dựa trên thuộc tính - An Toàn Thông Tin,” An Toan Thong Tin. Accessed: Dec. 10, 2024. [Online]. Available: http://antoanthongtin.gov.vn/gp-mat-ma/chi-tiet-bai-viet-cua-100371