ĐẠI HỌC QUỐC GIA TP. HỒ CHÍ MINH

**TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN**

**CÔNG NGHỆ CHUỖI KHỐI**

**(BLOCKCHAIN)**

**Báo Cáo Về Hệ Mật Mã**

**Dựa Trên Đường Cong Elliptic**

**NGUYỄN TRẦN KHÁNH NGUYÊN (**MSHV: 21C11017)

**GitHub: https://github.com/nguyennguyen6bk/blockchain\_lab1\_ecc**

**TP. HỒ CHÍ MINH – 2023**

MỤC LỤC

[Phần 1 : Giới Thiệu Về Đường Cong Elliptic 1](#_Toc126360059)

[1.1. Tổng quan về đường cong Elliptic 2](#_Toc126360060)

[1.2. Cộng các điểm trên đường cong Elliptic 2](#_Toc126360061)

[1.3. Nhân vô hướng các điểm trên đường cong Elliptic 3](#_Toc126360062)

[Phần 2 : Hệ Mật Dựa Trên Đường Cong Elliptic và Những Ứng Dụng 4](#_Toc126360063)

[2.1. Bài toán Logarithm rời rạc 4](#_Toc126360064)

[2.2. Tương đương với hệ Diffie – Hellman (Trao đổi khóa) 4](#_Toc126360065)

[2.3. Tương đương với hệ Massey – Omura (Mã hóa) 5](#_Toc126360066)

[2.4. Tương đương với hệ ElGamal (Chữ ký số) 5](#_Toc126360067)

[2.5. Tương đương với hệ RSA 6](#_Toc126360068)

[KẾT LUẬN 7](#_Toc126360069)

# 

# Phần 1 : Giới Thiệu Về Đường Cong Elliptic

Trong vài thập kỷ gần đây, đường cong elliptic đóng vai trò quan trọng đối với lý thuyết số và mật mã. Mật mã đường cong elliptic (ECC) được giới thiệu lần đầu vào năm 1991 bởi các công trình nghiên cứu độc lập của Neals Koblitz và Victor Miller. Độ an toàn của ECC dựa vào bài toán logarit rời rạc trên nhóm các điểm của đường cong elliptic (ECDLP). Đối với bài toán logarit rời rạc trên trường hữu hạn hoặc bài toán phân tích số, tồn tại các thuật toán dưới dạng dạng hàm mũ để giải các bài toán này (tính chỉ số hoặc sàng trường số). Tuy nhiên, đối với bài toán ECDLP cho đến nay vẫn chưa tìm được thuật toán dưới hàm mũ để giải.

# Tổng quan về đường cong Elliptic

Trong [toán học](https://vi.wikipedia.org/wiki/To%C3%A1n_h%E1%BB%8Dc), một đường cong Elliptic là một đường cong đại số phẳng được định nghĩa bằng phương trình có dạng:

(1.1)

Trong đó *a* và *b* là các hằng số. Các giá trị x, y, a, b thường là các giá trị trên một trường nào đó, ví dụ như R(số thực), Q(Số hữu tỷ), C(số phức), hoặc trường hữu hạn Fq, với q=p^n trong đó p là số nguyên tố với n >= 1. Đường cong (1.1) có định thức . Đường cong này sẽ suy biến và không có đủ 3 nghiệm phân biệt khi , trong phần này chúng ta chỉ xét các đường cong có .

# Cộng các điểm trên đường cong Elliptic

Xét hai điểm P = (, ) và Q = (, ) trên đường cong Elliptic E. Phép cộng giữa hai điểm trên đường cong E được định nghĩa như sau:

(1.2)

Với = -R’ là giao điểm của đường cong E và đường thẳng đi qua P và Q.

Nếu xp = xq và yp = - yq thì ta định nghĩa P + Q = ∞.

Trong đó , , với:

Vậy nếu tức là , ta có:

Nếu P = Q tức là , ta có:

Chart, line chart

Description automatically generated

Hình 1. Tổng hai điểm của đường cong Elliptic

# Nhân vô hướng các điểm trên đường cong Elliptic

Phép nhân một số nguyên k với một điểm P thuộc đường cong Elliptic E là điểm Q được xác định bằng cách cộng k lần điểm P và dĩ nhiên Q E: k P = P + P + P……+ P (k phép cộng điểm P). Vì vậy nếu G là một điểm thuộc đường cong Elliptic E thì với mỗi số nguyên dương k luôn dễ dàng xác định được điểm Q = kG.

Khi tổng các điểm P và Q trên đường cong Elliptic E được chỉ ra trong Hình 1. Kết quả được xác định là điểm S thu được bằng cách đảo ngược dấu của tọa độ y của điểm R’, trong đó R’ là giao điểm của E và đường thẳng đi qua P và Q. Nếu P và Q ở cùng một vị trí, đường thẳng là tiếp tuyến của E tại P. Ngoài ra, tổng điểm tại vô cực và điểm P được xác định là chính điểm P.

# Phần 2 : Hệ Mật Dựa Trên Đường Cong Elliptic và Những Ứng Dụng

# Bài toán Logarithm rời rạc

Định nghĩa: Bài toán Logarithm rời rạc trên đường cong Elliptic (ECDLP): *Cho đường cong E trên trường hữu hạn , điểm P ∈ E() với bậc n(nP = O = ∞)và điểm Q ∈ E(), tìm số nguyên k ∈ [0,n−1] sao cho Q = kP . Số nguyên k được gọi là Logarithm rời rạc của Q với cơ sở P , và thường được viết là k = .*

Bất kỳ một hệ mật khóa công khai nào cũng phải sử dụng một bài toán khó để xây dựng hàm một chiều. Ý nghĩa một chiều ở đây có nghĩa là tính thuận thì dễ (thuật toán giải trong thời gian đa thức) và tính ngược thì khó (thuật toán giải với thời gian không phải là đa thức - thường là hàm mũ hoặc nửa mũ). Các tham số của Hệ mật dựa trên đường cong Elliptic (ECC) cần phải được lựa chọn cẩn thận để tránh được các tấn công đối với bài toán ECDLP. Thuật toán vét cạn để giải bài toán ECDLP là lần lượt tính thử các điểm P,2P,3P,... cho đến khi điểm mới tính được đúng bằng điểm Q. Trong trường hợp xấu nhất sẽ phải cần đến n bước thử, trung bình thường là n/2 là đạt được điểm Q, do đó cần phải chọn n đủ lớn để bài toán vét cạn là không khả thi (n ≥).Thuật toán tốt nhất hiện nay để tấn công bài toán ECDLP là sự kết hợp của thuật toán Pohlih-Hellman và Pollard’s rho, thuật toán này có thời gian tính là O(), với p là ước số nguyên tố lớn nhất của n do đó phải chọn số n sao cho nó chia hết số nguyên tố p lớn nhất có đủ lớn để giải bài toán này là không khả thi.

# Tương đương với hệ Diffie – Hellman (Trao đổi khóa)

Hai bên A và B cần tạo khóa phiên bí mật trao đổi trong một kênh truyền công khai, hai bên cùng thỏa thuận điểm cơ sở *P* trên *E* . Bên A tạo khóa bí mật và gửi giá trị cho bên B, ngược lại bên B tạo khóa bí mật nhân với *P* sau đó gửi lại cho A. Khi đó khóa phiên của bên A sẽ là , và của bên B sẽ là . Dễ dàng nhận thấy , khóa này chỉ riêng hai bên A và B có thể tính được. Xem sơ đồ dưới đây:

Diagram

Description automatically generated with medium confidence

*Đánh giá bảo mật:* Để tìm được khóa chia sẻ hoặc , Hacker buộc phải tìm được cả 2 khóa bí mật ,, trong khi chỉ có thể bắt được thông tin trên đường truyền là và , khi biết P , Hacker buộc phải giải bài toán Logarithm rời rạc và và đây là bài toán khó không giải được trong thời gian đa thức.

# Tương đương với hệ Massey – Omura (Mã hóa)

Text, letter

Description automatically generated with medium confidence

Dễ dàng nhận thấy:

Text

Description automatically generated with medium confidence

*Đánh giá bảo mật:* Muốn phá khóa trong lược đồ này, điều kiện đầu tiên phải tìm được giá trị , để tìm được các giá trị này phải lần lượt giải 2 bài toán Logarithm rời rạc và , và đây là 2 bài toán chưa giải được trong thời gian đa thức.

# Tương đương với hệ ElGamal (Chữ ký số)

1. A và B chọn công khai một đường cong Elliptic E trên Fq với q = p ^r và p là một số nguyên tố và một điểm cơ sở ngẫu nhiên P thuộc E.
2. A chọn ngẫu nhiên một số nguyên ra và tính raP; B cũng chọn ngẫu nhiên một số nguyên rb và tính rbP.
3. Để gửi một thông điệp M cho B, A chon ngẫu nhiên một số nguyên k và gửi cặp (kP, M+k(rbP)).
4. Để đọc M, B tính:

M + k(rbP) – rb(kP) = M

Người thứ ba nếu giải được bài toán logarithm rời rạc trên E dĩ nhiên có thể xác định rb từ các thông tin được công bố P và rbP. Nhưng, như ta đã biết, không có cách nào hiệu quả để tính logarithm rời rạc, vì thế hệ thống rất an toàn.

# Tương đương với hệ RSA

RSA cũng có những điểm tương đương với hệ mã đường cong Elliptic như sau:

1. N = pq là khóa công khai và là tích của hai số nguyên tố lớn p và q.
2. Chọn ngẫu nhiên hai số nguyên a và b thỏa xác định một đường cong Elliptic cho cả mod p lẫn mod q.
3. Mã hóa một thông điệp P, chỉ phải thi hành eP mod N, với e là khóa công khai. Để giải mã, ta cần biết một số điểm trên E mod cho cả p lẫn q.

# KẾT LUẬN

Báo cáo hướng đến việc giới thiệu về hệ mật mã dựa trên đường cong Elliptic. Thể hiện các phép cộng và nhân trên đường cong trong trường hữu hạn. Nêu lên được mối liên hệ tương đương giữa hệ mã ECC với các hệ mã khác dùng trong nhiều mục đích khác nhau như là: Trao đổi khóa, Xác thực – Chữ ký số, Mã hóa – Giải mã.