Đường cong Elliptic

(trước và sau quantum)

Main Author , 2nd Author, 3rd Author

School of Computer Science
University of Windsor

Ngày 19 tháng 4 năm 2022

Table of Contents

Introduction

Definition

Ta định nghĩa bài toán logarit rời rạc trên một nhóm với phép nhân các số nguyên theo modulo p, $\mathbb{Z}_{/\mathbb{Z}_p}$, như sau:
Cho $g, a \in \mathbb{Z}_{/\mathbb{Z}_p}$, với a là phần tử của nhóm cyclic có phần tử sinh g, tìm số nguyên k thỏa mãn:

$$g^k \equiv a \pmod{p} \tag{1}$$

Definition

Ta định nghĩa bài toán phân tích rời rạc như sau: Cho một số nguyên N, có ước là hai số nguyên tố lớn p và q. Tìm p và q.

Preliminaries

[Vishwanath and Nagappan, 2010]

Definition

Một *nhóm* là một cấu trúc đại số bao gồm:

- Một tập phần tử G
- Một toán tử đóng $(\cdot)$ trên tập G thỏa mãn tính chất kết hợp. Nghĩa là $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, với mọi $a, b, c \in G$.
- Một phần tử đơn vị 1, để $a \cdot 1 = a$ với mọi $a \in G$.
- Tồn tại phần tử nghịch đảo $a^{-1} \in G$ nếu $a \in G$ để $a^{-1} \cdot a = 1$.

Một *nhóm* thỏa mãn thêm điều kiện toán tử hai ngôi có thêm tính giao hoán (hay $a \cdot b = b \cdot a$) là nhóm giao hoán hoặc *nhóm Abel*

Example

Với tập số nguyên $\mathbb{Z}$ được trang bị toán tử $+$ và xem số 0 như phần tử đơn vị, xem các cặp số nguyên có dấu ngược nhau là các cặp nghịch đảo, ta có một *nhóm*.
Ngược lại, tập số tự nhiên $\mathbb{N}$ không phải một nhóm vì không định nghĩa được phần tử nghịch đảo.

Definition

Cho nhóm G được trang bị toán tử $(\cdot)$ với phần tử đơn vị 1. Với mỗi $a \in G$, *bậc* của a, là số nguyên n nhỏ nhất thỏa mãn:

$$\underbrace{a \cdot a \cdot a \cdot \ldots \cdot a}_{n} = 1 \tag{2}$$

Tập $\{a, a^2, a^3, a^4, \ldots, a^n\}$ là nhóm cyclic con của G có bậc n, a được gọi là *phần tử sinh* của nhóm đó.

Definition

Một *trường* là một cấu trúc đại số bao gồm:

- Tập G là tập đóng dưới phép cộng và phép nhân.
- Phép cộng và phép nhân phải có tính kết hợp trên tập G.
- Phép cộng và phép nhân phải có tính giao hoán trên tập G.
- Tồn tại phần tử nghịch đảo cho cả phép cộng và phép nhân.
- Phép nhân có tính chất phân phối đối với phép cộng: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.
- Phần tử đơn vị của phép cộng và phép nhân phải khác nhau.

Preliminaries

Definition

Tính đặc trưng của trường F là số n nhỏ nhất thỏa mãn tổng của n phần tử 1 bằng 0. Kí hiệu $char(F) = n$.

Example

Nếu tính đặc trưng của F, $char(F)$, là 2 và phần tử đơn vị là 1, thì $1 + 1 = 0$.
Nếu $char(F) = 3$ thì $1 + 1 + 1 = 0$.

Preliminaries

Definition

Trường Galois là trường bao gồm một tập hữu hạn phần tử.

Example

Tập số nguyên theo modulo số nguyên tố p, $\mathbb{Z}_{/\mathbb{Z}_1}$ là một trường Galois. Với p phần tử, 0 đến $p-1$, kí hiệu $GF(p)$.

Phần còn lại, ta sẽ đề cập nhiều hơn đến trường của số nguyên tố $GF(p)$, tổng quát hơn là $GF(p^n)$.

Definition

Một đường cong elliptic $E(F)$ là một tập điểm trên trường F, thỏa mãn phương trình có dạng:

$$y^2 + a_1xy + a_2y = x^3 + a_3x^2 + a_4x + a_5 \tag{3}$$

Trong đó $a_1, a_2, a_3, a_4, a_5 \in F$.

Nếu ta giả sử tính đặc trưng của F khác 2, hay $1 + 1 = 2 \neq 0$, phương trình có thể viết lại dưới dạng:

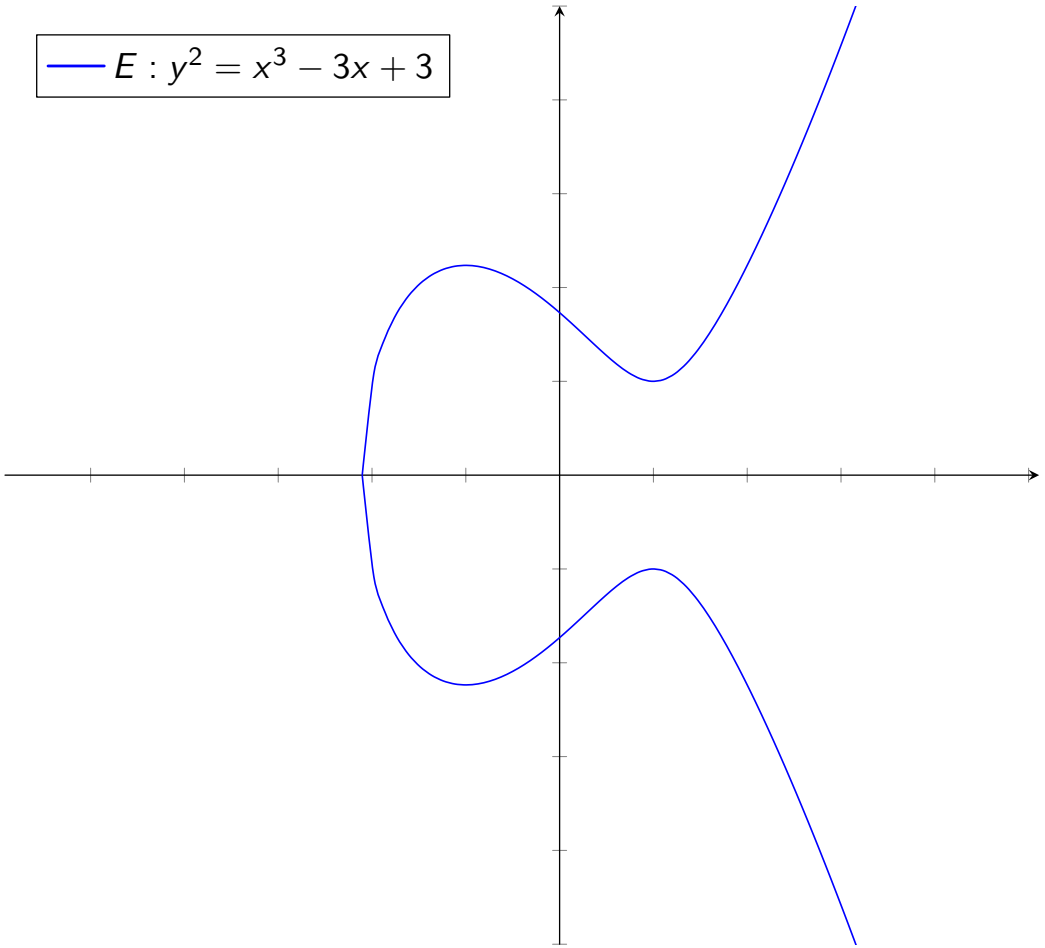
$$y^2 = x^3 + a_3x^2 + a_4x + a_5 \tag{4}$$

Phương trình có thể rút gọn hơn nữa nếu tính đặc trưng của trường khác 3, ta được phương trình đơn giản hơn, được gọi là phương trình Weierstrass.

$$y^2 = x^3 + ax + b \,|_{a=a_4, b=a_5} \tag{5}$$

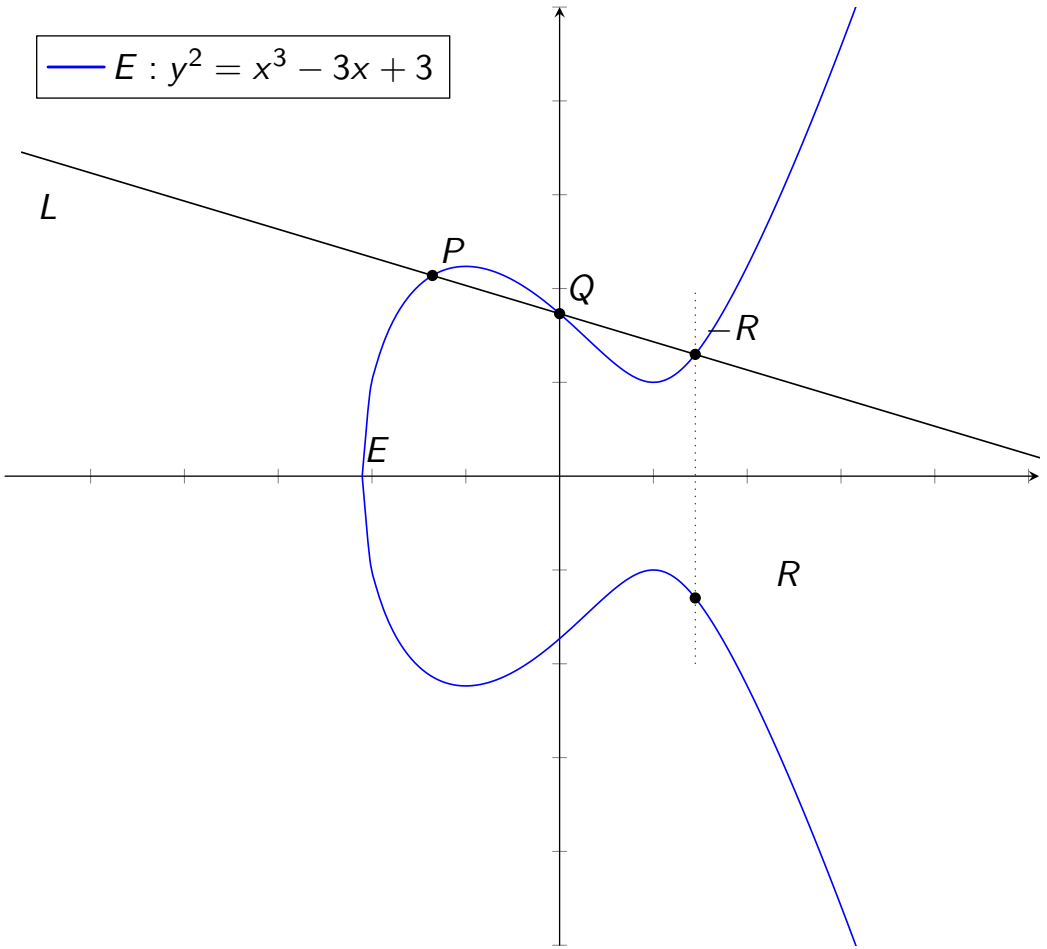
Đồ thị

Hình: Đường cong Elliptic E trên $\mathbb{R}^2$



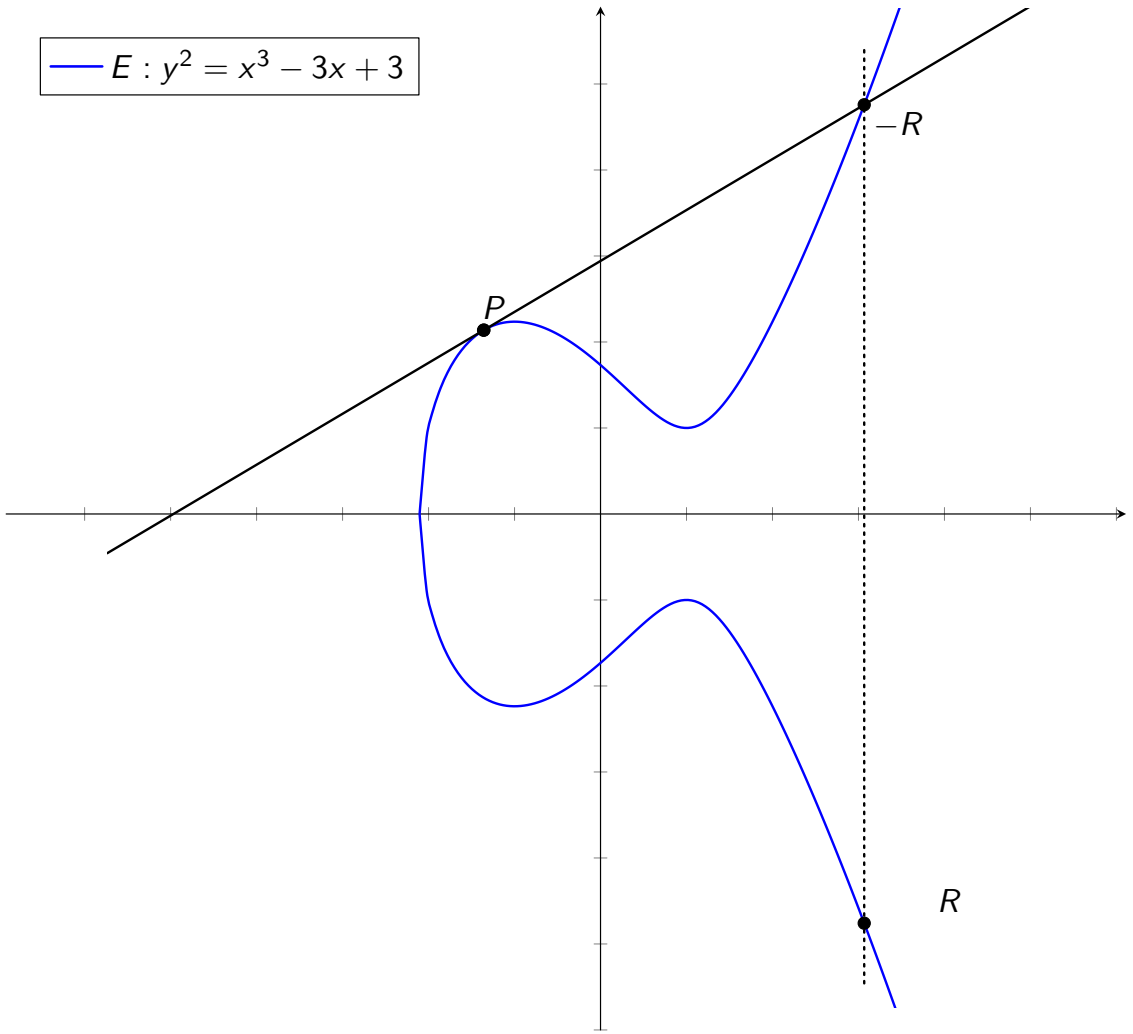
Đồ thị

Hình: Cộng hai điểm P và Q trên E



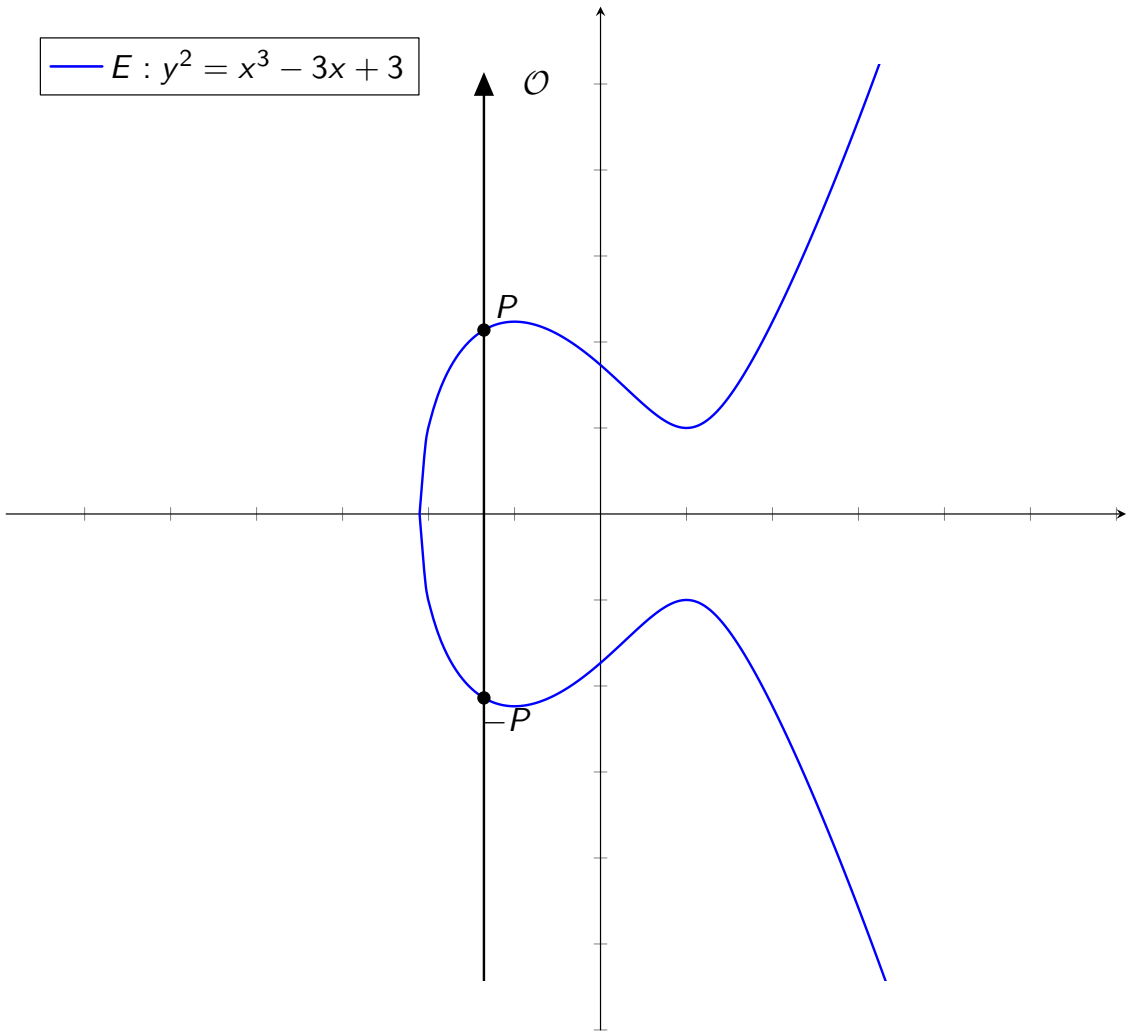
Đồ thị

Hình: Cộng hai điểm P và P trên E



Đồ thị

Hình: Cộng hai điểm P và $-P$ trên E



Tính $P + Q$ nếu $P(x_1, y_1)$ và $Q(x_2, y_2)$ phân biệt

Để sau

Tính $P + Q$ nếu $P(x_1, y_1)$ và $Q(x_2, y_2)$ phân biệt

Sử dụng phép cộng này, ta định nghĩa phép *nhân vô hướng* trên nhóm G

Definition

Phép *nhân vô hướng* trên nhóm G là phép cộng một điểm nhiều lần.

$$nP = \underbrace{P + P + \ldots + P}_{n} \tag{6}$$

Thuật toán nhân đôi và cộng

Algorithm 1: Nhân đôi và cộng

input : n, P
output: $R = nP$
begin
  $Q \leftarrow P$
  $E \leftarrow \mathcal{O}$
  while $n > 0$ **do**
    if $n \equiv 1 \pmod 2$ **then**
      $R \leftarrow R + Q$
    else
      $R \leftarrow R + Q$
      $Q \leftarrow 2 \cdot Q$
      $n \leftarrow \lfloor \frac{n}{2} \rfloor$
    end
  end
  return R
end

Corollary

Vì $nP + mP = \underbrace{P + P + P + \ldots + P}_{n} + \underbrace{P + P + P + \ldots + P}_{m} = (n + m)P$

nên khi cộng 2 bội của P ta thu được bội khác của P. Tập hợp các bội của P là một nhóm cyclic với bậc k, trong đó P là phần tử sinh.

Theorem (Định lý Lagrange)

Nếu H là nhóm con của nhóm hữu hạn G, thì bậc (số phần tử) của G chia hết cho bậc của H.

Corollary

Nếu bậc của nhóm hữu hạn G là số nguyên tố p thì bậc của nhóm con H là 1 hoặc p.
Nếu bậc của H là p, mọi điểm thuộc G đều là phần tử sinh của nhóm con H

Bài toán logarit rời rạc đối với đường cong elliptic

Definition

Cho đường cong elliptic E trên trường hữu hạn F, và nhóm G bao gồm tập các điểm trên E được định nghĩa với phép $+$. Cho điểm $P, Q \in G$ sao cho Q là bội của P, hay $Q = kP$ với k là số nguyên. Bài toán logarit rời rạc được định nghĩa như sau:

Cho trước 2 điểm $P, Q \in G$.
Tìm số nguyên k nhỏ nhất thỏa mãn $kP = Q$.

k gọi là logarit rời rạc của Q theo cơ sở P.

Bài toán logarit rời rạc đối với đường cong elliptic

Xét trường hữu hạn $\mathbb{F}_p$ bao gồm các số nguyên theo modulo p, trong đó p là số nguyên tố. Kí hiệu $E(\mathbb{F}_p^2)$ là tập điểm của $\mathbb{F}_p^2$ nằm trên đường cong E. Điểm $P = (x, y) \in \mathbb{F}_p^2$ khi và chỉ khi, với mọi $a, b \in \mathbb{F}_p$, biểu thức được thỏa mãn:

$$y^2 \equiv x^3 + ax + b \pmod{p} \tag{7}$$

$E(\mathbb{F}_p^2)$ là một nhóm abel với phép toán $+$ được định nghĩa ở trên.

Bài toán logarit rời rạc đối với đường cong elliptic

Xét trường hữu hạn $\mathbb{F}_p$ bao gồm các số nguyên theo modulo p, trong đó p là số nguyên tố. Kí hiệu $E(\mathbb{F}_p^2)$ là tập điểm của $\mathbb{F}_p^2$ nằm trên đường cong E. Điểm $P = (x, y) \in \mathbb{F}_p^2$ khi và chỉ khi, với mọi $a, b \in \mathbb{F}_p$, biểu thức được thỏa mãn:

$$y^2 \equiv x^3 + ax + b \pmod{p} \tag{8}$$

$E(\mathbb{F}_p^2)$ là một nhóm abel với phép toán $+$ được định nghĩa ở trên.

$$| G | = | E(\mathbb{F}_p^2) | = h \cdot k,$$

trong đó k là số nguyên tố và là bậc của nhóm sinh bởi P, h nên nhỏ.

Thuật toán tìm tham số đường cong trên trường $\mathbb{F}_p$

Algorithm 2: Tìm tham số đường cong

input : p
output : $out = (p, a, b, P, k, h)$
begin
1. Chọn ngẫu nhiên đường cong E, hay ngẫu nhiên a, b
2. Dùng thuật toán Schoof để tìm bậc của G
3. Tìm ước nguyên tố k lớn của $\mid G \mid$. Đảm bảo h đủ nhỏ và k đủ lớn với $h \cdot k = \mid G \mid$
4. **if** *k không đủ lớn* **then**
   Trở lại bước 1, tìm đường cong mới.
   end
5. Chọn ngẫu nhiên $P \in G$ và tính kP bằng thuật toán nhân đôi và cộng.
6. **if** $kP \neq 1$ **then**
   k không phải bậc của nhóm con sinh bởi P, trở lại bước 6 tìm điểm P khác.
   end
7. **return** (p, a, b, P, k, h)

end

Một số đường cong đặc biệt

- Đường cong Koblitz trên trường nhị phân:

$$y^2 + xy = x^3 + ax^2 + 1 \text{ với } a \in \{0, 1\} \text{ trên trường } GF(2^m)$$

  với m là số nguyên tố
- Đường cong Weierstrass trên trường số nguyên tố:

$$y^2 = x^3 + ax + b$$

  với $a, b \in \mathbb{F}_p$ Được cho rằng đem lại hiệu quả bảo mật cao hơn đường Koblitz hay đường nhị phân dù chi phí tính toán tốn kém hơn.

NIST đã cung cấp một vài đường cong để sử dụng trong ECC. 3 trường $\mathbb{F}_p$ với các số p cụ thể: $2^{607} - 1, 2^{521} - 1, 180 * (2^{127} - 1)^2 + 1$, với độ bảo mật tương ứng giảm dần.

Trao đổi khóa Diffe-Hellman

Tạo tham số công khai	
Cả hai chấp nhận cùng sử dụng (p, a, b, P, k, h)	
Thực hiện tính toán bí mật	
Alice	Bob
Chọn bí mật một số nguyên n_A Tính $Q_A = n_A P$	Chọn bí mật một số nguyên n_B Tính $Q_B = n_B P$
Trao đổi giá trị công khai	
Alice gửi Q_A cho Bob $Q_B \longleftarrow$	$\longrightarrow Q_A$ Bob gửi Q_B cho Alice
Tiếp tục thực hiện tính toán bí mật	
Alice	Bob
Tính $n_A Q_B \pmod p$	Tính $n_B Q_A \pmod p$
Khóa bí mật của cả hai là $n_A n_B P$	

Chữ ký số

Alice muốn gửi tin nhắn m cho Bob
Cả hai chấp nhận cùng sử dụng (p, a, b, P, k, h)
n_A, Q_A tương ứng là khóa bí mật và công khai Alice
Alice chọn một số n làm khóa tạm thời
Alice tính $Q = nP$, đặt r là tọa độ x của điểm Q Tính $s = n^{-1}(m + rn_A)$ Gửi cặp (r, s) cho Bob $\longrightarrow$
Bob tính $u_1 = s^{-1}m \pmod{k}$ $u_2 = s^{-1}r \pmod{k}$ $Q = u_1P + u_2Q_A$ kiểm tra nếu $r = x_Q$ thì đúng là Alice.

Bài toán của Sony

Proposition

Nếu n trong thuật toán chữ ký số không đổi, ta có thể khôi phục khóa bí mật từ chữ ký của Alice.

Chứng minh.

Ta có 2 bộ chữ ký của Alice là (r_1, s_1) và (r_2, s_2). Vì $r = x_Q$ mà $Q = nP$, nên với n không đổi, ta có $r_1 = r_2$. Lại có;

$$s_1 - s_2 = n^{-1}(m_1 + rn_A) - n^{-1}(m_2 + rn_A) = n^{-1}(m_1 - m_2) \pmod{k}$$

nên

$$n = (m_1 - m_2)(s_1 - s_2)^{-1} \pmod{k}$$

Sau khi tính được n, ta tính được

$$n_A = r^{-1}(s_1 n - m_1) \pmod{k}$$

Tấn công Pollard Rho

Algorithm 3: Tìm chu trình của Floyd

input : P, Q

output: $out = (a, b, c, d)$

begin

Sinh ra dãy S, mỗi phần tử là một cặp (a, b)

Khởi tạo con trỏ $it_1 = 0$ và $it_2 = 0$

while $aP + bQ \neq cP + dQ$ **do**

$it_1 \leftarrow it_1 + 1$

$it_2 \leftarrow it_2 + 1$

$(a, b) \leftarrow S[it_1]$

$(c, d) \leftarrow S[it_2]$

end

return (a, b, c, d)

end

Tấn công Pollard Rho

Algorithm 4: Pollard Rho

input : P, Q

output: n thỏa mãn $nP = Q$

begin

$(a, b, c, d) \leftarrow Floyd(P, Q)$

$n \leftarrow (a - c)(d - b)^{-1}$

return n

end

Độ phức tạp thời gian: $O(\sqrt{k})$ hoặc $2^{O(b)}$ với b là số bit của k.

References I

Vishwanath, K. V. and Nagappan, N. (2010).
Characterizing cloud computing hardware reliability.
SoCC '10, pages 193–204, New York, NY, USA. Association for Computing Machinery.