Mật mã trên đường cong Elliptic Curves cho thiết bị IoT

Sinh viên thực hiện
Đặng Quang Trung - 20134145

Giảng viên hướng dẫn
TS Trần Vĩnh Đức

Ngày 18 tháng 5 năm 2018

Nội dung trình bày

1. Cở sở lý thuyết
   - Hệ mã khóa công khai
   - Giao thức Diffe-Hellman
2. Đường cong elliptic
3. Chứng thư số ẩn
4. Kết quả

1. Cở sở lý thuyết
   - Hệ mã khóa công khai
   - Giao thức Diffe-Hellman
2. Đường cong elliptic
3. Chứng thư số ẩn
4. Kết quả

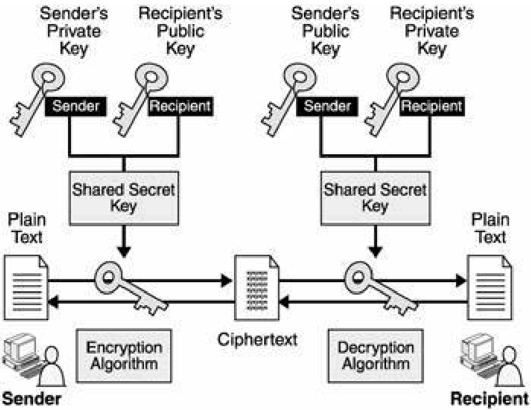
Tại sao cần có mật mã?

Ứng dụng

- Thương mại điện tử:
  - Chữ ký điện tử.
  - Mã hóa thông tin giao dịch.
- Mạng xã hội:
  - Mã hóa tin nhắn, văn bản,thư điện tử, ...
- Banking
  - Xác thực người dùng
  - Mã hóa giao dịch, thông tin khách hàng.
  - . . . .

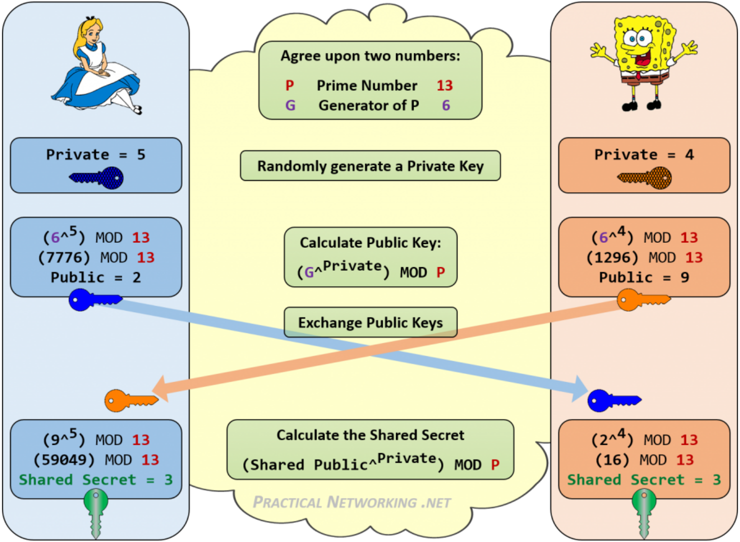
1. Cở sở lý thuyết
   - Hệ mã khóa công khai
   - Giao thức Diffe-Hellman
2. Đường cong elliptic
3. Chứng thư số ẩn
4. Kết quả

Sơ đồ hệ mã khóa công khai



1. Cở sở lý thuyết
   - Hệ mã khóa công khai
   - Giao thức Diffe-Hellman
2. Đường cong elliptic
3. Chứng thư số ẩn
4. Kết quả

Diffe-Hellman



1. Cở sở lý thuyết
   - Hệ mã khóa công khai
   - Giao thức Diffe-Hellman
2. **Đường cong elliptic**
3. Chứng thư số ẩn
4. Kết quả

Định nghĩa

Một đường cong elliptic curve được xác định bởi phương trình đường cong

- **phương trình dạng Weierstrass**

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

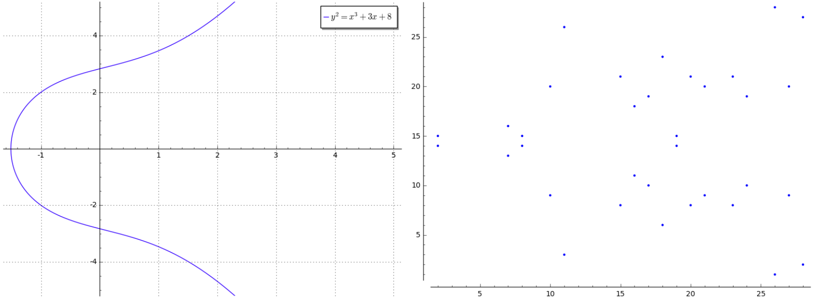
  với điều kiện $A, B \in \mathbb{F}$ thỏa mãn $4A^3 + 27B^2 \neq 0$.

- **phương trình dạng Montgomery**

$$M_{A,B} : By^2 = x^3 + Ax^2 + x$$

  với điều kiện $A \in \mathbb{F} \setminus \{-2, 2\}, B \in \mathbb{F} \setminus \{0\}$ và $B(A^2 - 4) \neq 0$

Elliptic trên trường hữu hạn



(a) elliptic trên trường số thực elliptic trên trường hữu hạn $\mathbb{F}_{29}$

Hình: Đường cong elliptic dạng $y^2 = x^3 + 3x + 8$

- Đường cong elliptic có điểm giả định $\mathcal{O}$ ở vô cùng được gọi là điểm cơ sở.

Luật trên đường cong elliptic hữu hạn

Trên đường cong elliptic có 2 phép toán quan trọng là:

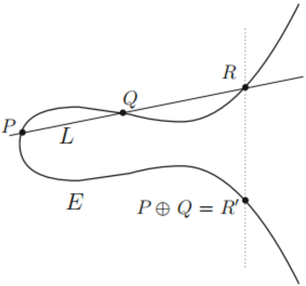
- Phép cộng (Add)
- Phép nhân đôi và cộng (Double-And-Add)

Phép cộng 2 trên đường cong elliptic(E) thoả mãn tính chất:

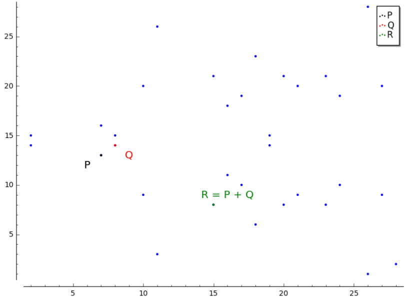
- Phần tử đơn vị: $P + \mathcal{O} = \mathcal{O} + P = P \; \forall P \in E$.
- Phần tử nghịch: $P + (-P) = \mathcal{O} \; \forall P \in E$.
- Kết hợp: $(P + Q) + R = P + (Q + R) \; \forall P, Q, R \in E$.
- Giao hoán: $P + Q = Q + P \; \forall P, Q \in E$.

Hay nói cách khác tập các điểm thuộc E với luật cộng tạo thành nhóm *Abelian*.

Phép cộng trên đường cong elliptic



(a) $P + Q (P \neq Q)$

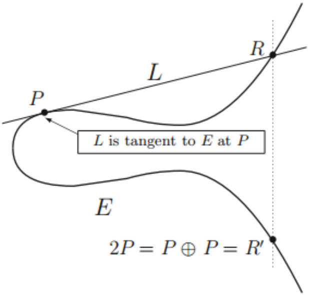


(b) $P + Q (P \neq Q)$ trên $\mathbb{F}_{29}$

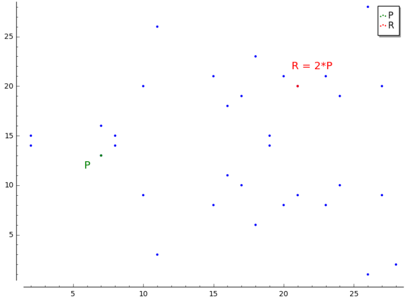
Đường cong elliptic dạng $y^2 = x^3 + 3x + 8$

- $P(7, 13) + Q(8, 14) = R(15, 8)\ (mod\ 29) \in E(\mathbb{F}_{29})$.

Phép cộng trên đường cong elliptic



(a) $P + P([2]P)$

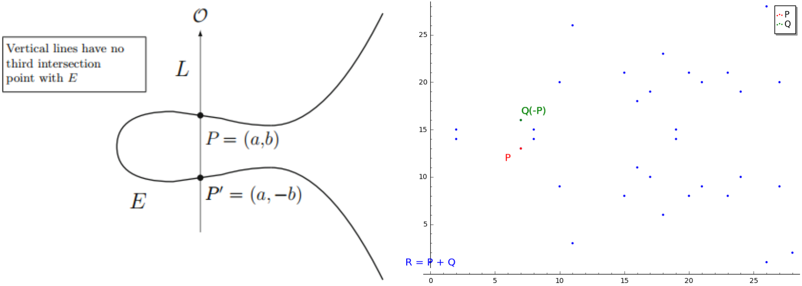


(b) $P + P([2]P)$ trên $\mathbb{F}_{29}$

Đường cong elliptic dạng $y^2 = x^3 + 3x + 8$

- $P(7,13) + P(7,13) = 2P(7,13) = R(21,20)\ (mod 29) \in E(\mathbb{F}_{29})$

Phép cộng trên đường cong elliptic



(a) $P + (-P)$ (b) $P + (-P)$ trên $\mathbb{F}_{29}$

Đường cong elliptic dạng $y^2 = x^3 + 3x + 8$

- $P(7,13) + P'(7,15) = \mathcal{O} \in E(\mathbb{F}_{29})$
    - $-P(7,13) = P'(7,-13) = P'(7,15)\ (mod\ 29)$
- $P + \mathcal{O} = P\ \forall P \in E(\mathbb{F}_{29})$

Double-And-Add

Phép toán $Q = nP$ với $n \in \mathbb{F}_p$.

$$Q = \underbrace{P + P + \ldots + P}_{n\ add}$$

Vấn đề:

- Nếu n lớn thì tốc độc tính $Q = nP$ sẽ rất lâu.

Ta có thể biểu diễn n thành:

$$n = n_0 + n_1 \cdot 2 + n_2 \cdot 4 + n_3 \cdot 8 + \ldots + n_r \cdot 2^r$$

với $n_0, n_1, \ldots, n_r \in \{0, 1\}$. Nếu $n_r = 1$ ta có thể tính:

$$Q_0 = P, Q_1 = 2Q_0, Q_2 = 2Q_1, \ldots, Q_r = 2Q_{r-1}$$

Chú ý rằng Q_i chỉ gấp 2 lần Q_{i-1} hay $Q_i = 2^i P$.Phép cộng sẽ được tính:

$$nP = n_0 Q_0 + n_1 Q_1 + n_2 Q_2 + \ldots + n_r Q_r$$

Điểm sinh trên đường cong

Cho G là một điểm nằm trên E và có cấp là n (hay $nG = \mathcal{O}$). Khi đó các phần tử của đường cong sẽ biễu diễn bởi:

$$G, 2G, 3G, 4G, \ldots, nG$$

với $nG = \mathcal{O}$ là điểm cơ sở.

Ví dụ

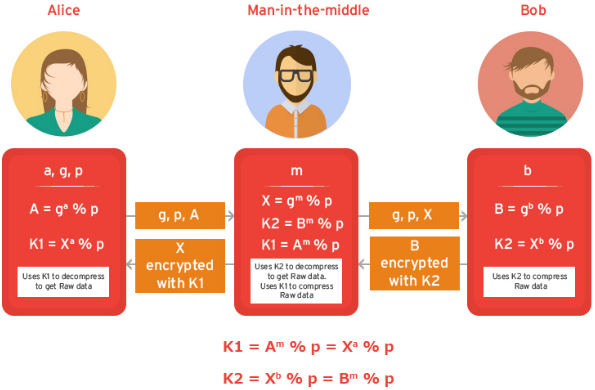
Cho pt $y^2 = x^3 + 3x + 8$, ta có điểm sinh $G = (19, 15)$ có cấp $n = 35$

$G = (19, 15)$	$2G = (15, 8)$	$3G = (18, 23)$	$4G = (27, 20)$
$5G = (21, 20)$	$6G = (17, 19)$	$7G = (26, 28)$	$8G = (20, 8)$
$9G = (10, 9)$	$10G = (23, 21)$	$11G = (11, 26)$	$12G = (24, 10)$
$13G = (16, 11)$	$14G = (28, 2)$	$15G = (7, 16)$	$16G = (2, 15)$
$17G = (8, 14)$	$18G = (8, 15)$	$19G = (2, 14)$	$20G = (7, 13)$
$21G = (28, 17)$	$22G = (16, 18)$	$23G = (24, 19)$	$24G = (11, 3)$
$25G = (23, 8)$	$26G = (10, 20)$	$27G = (20, 21)$	$28G = (26, 1)$
$29G = (17, 10)$	$30G = (21, 9)$	$31G = (27, 9)$	$32G = (18, 6)$
$33G = (15, 21)$	$34G = (19, 14)$	$35G = \mathcal{O}$	

Diffe-Hellman trên đường cong Elliptic

1. Cở sở lý thuyết
   - Hệ mã khóa công khai
   - Giao thức Diffe-Hellman
2. Đường cong elliptic
3. Chứng thư số ẩn
4. Kết quả

Tại sao cần chứng thư số ẩn?



Tấn công MITM

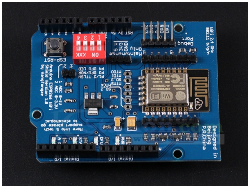
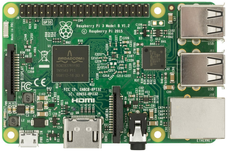
Kết quả thu được

- Tìm hiểu được một số nguyên lý mã công khai, hàm băm, chữ ký điện tử.
- Hiểu được lý thuyết về đường cong elliptic.
- Hiểu được các bước cơ bản xây dựng một đường cong elliptic và ứng dụng trong thuật toán trao đổi khóa và tạo chứng thư số.
- Nắm được một số kiểu tấn công như timing-attack, tấn công xen giữa.
- . . .

Hạn chế

- Chưa tìm hiểu được một cách đầy đủ và chi tiết về đường cong elliptic trên trường hữu hạn F_{2^m} với 2 dạng cơ sở normal và polinomial.
- Ứng dụng truyền file và chứng thư số chưa có giao diện đẹp mắt và mới chỉ thử nghiệm trên một máy.
- . . .

Hướng Phát triển

Hình: arduino, esp-12(esp8266), raspberry pi – các thiết bị dùng trong phát triển sản phẩm IoT

- Tốc độ tính toán trên đường cong Elliptic nhanh.
- Lưu trữ và trao đổi khóa nhỏ gọn.
- Tính an toàn bảo mật cao.