4. Các cấu trúc toán học nâng cao

Ngày 22 tháng 7 năm 2025

1 Đường cong Elliptic (Elliptic Curves)

Định nghĩa:
Đường cong elliptic là tập hợp các điểm (x, y) thỏa mãn phương trình:

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

với a, b là các hằng số.

Ngoài các điểm (x, y) thoả mãn phương trình trên, còn có một điểm đặc biệt gọi là **điểm vô cực** (point at infinity), ký hiệu là O, đóng vai trò phần tử đơn vị trong nhóm.

Nhóm trên đường cong elliptic:
Các điểm trên đường cong có thể được cộng với nhau bằng một phép toán hình học, gọi là *point addition*. Phép cộng này có các tính chất:

- **Tính đóng:** Tổng hai điểm trên đường cong vẫn thuộc đường cong.
- **Tính giao hoán:** $P + Q = Q + P$
- **Tính kết hợp:** $P + (Q + R) = (P + Q) + R$
- **Phần tử đơn vị:** $P + O = P$
- **Phần tử nghịch đảo:** Nếu $P = (x, y)$ thì $-P = (x, -y)$

Cộng điểm (Point addition):
Đường thẳng nối hai điểm P và Q cắt đường cong tại điểm thứ ba R', khi đó:

$$P + Q = -R'$$

Nhân vô hướng (Scalar multiplication):

$$kP = \underbrace{P + P + \ldots + P}_{k \text{ lần}}$$

Là phép toán quan trọng trong mật mã elliptic curve cryptography (ECC).

2 Căn bậc nhất (Roots of Unity)

Trên một trường hữu hạn $\mathbb{F}_p$, tập các điểm trên đường cong elliptic là hữu hạn, gồm điểm vô cực và hữu hạn điểm (x, y) khác.

Căn bậc nhất:

Một điểm P có *bậc* n nếu:

$$nP = O$$

với n là số nguyên dương nhỏ nhất thỏa mãn.

Các căn bậc nhất là các điểm mà khi cộng chính nó n lần sẽ trở lại điểm vô cực.

Bậc của điểm là yếu tố quan trọng trong mật mã và sơ đồ chứng minh zero knowledge.

3 Phép ghép đôi (Pairing)

Phép ghép đôi là một ánh xạ:

$$e : G_1 \times G_2 \to G_T$$

với G_1, G_2, G_T là các nhóm elliptic hoặc nhóm hữu hạn khác.

Tính chất quan trọng:

- **Song tuyến (Bilinearity):**

$$e(P, Q + R) = e(P, Q) \cdot e(P, R), \quad e(P + S, Q) = e(P, Q) \cdot e(S, Q)$$

- **Không suy biến (Non-degeneracy):** Nếu P là phần tử sinh của G_1, tồn tại $Q \in G_2$ sao cho $e(P, Q)$ là phần tử sinh của G_T.
- **Tính khả thi (Computability):** Có thuật toán hiệu quả để tính $e(P, Q)$ với mọi $P \in G_1$, $Q \in G_2$.

Phép ghép đôi thường được sử dụng trong các sơ đồ mật mã hiện đại như zk-SNARKs.

4 Đồng cấu nhóm (Group Homomorphisms)

Là ánh xạ giữa hai nhóm cùng loại, bảo toàn phép toán nhóm.

Cho hai nhóm $(A, *)$ và $(B, \cdot)$, ánh xạ $f : A \to B$ là *đồng cấu nhóm* nếu:

$$f(x * y) = f(x) \cdot f(y)$$

Đồng cấu giúp duy trì cấu trúc đại số trong biến đổi, rất quan trọng trong mật mã và các giao thức ZKP.

5 Ý nghĩa trong Zero Knowledge Proofs (ZKP)

- Đường cong elliptic và phép ghép đôi là nền tảng cho các cam kết nhỏ gọn và chứng minh hiệu quả.
- Các phép toán nhóm hỗ trợ xây dựng chứng minh với tính ràng buộc và ẩn danh.
- Scalar multiplication và căn bậc nhất là nền tảng tạo khóa mật mã và cấu trúc chứng minh.

Tóm lại:

Mục này giới thiệu các cấu trúc đại số nâng cao như đường cong elliptic, căn bậc nhất, phép ghép đôi, và đồng cấu nhóm — là các công cụ toán học cốt lõi cho việc xây dựng các sơ đồ chứng minh Zero Knowledge an toàn và hiệu quả.