5. Ứng dụng vào Zero Knowledge Proofs (ZKP)

Ngày 22 tháng 7 năm 2025

1 Tổng quan về Zero Knowledge Proofs

Zero Knowledge Proof (ZKP) là một giao thức tương tác giữa **prover** (người chứng minh) và **verifier** (người kiểm chứng) cho phép prover chứng minh một khẳng định là đúng mà không tiết lộ bất kỳ thông tin nào khác ngoài tính đúng của khẳng định đó.

Mục tiêu: Đảm bảo rằng verifier chỉ biết khẳng định đúng, mà không biết cách chứng minh hay bất kỳ dữ liệu nhạy cảm nào liên quan.

2 Các bước chính trong quá trình tạo chứng minh ZKP

- **Biến đổi bài toán (Arithmetization):** Chuyển đổi bài toán logic hoặc tính toán thành hệ thống các ràng buộc đại số hoặc đa thức.
- **Biểu diễn dưới dạng đa thức:** Các ràng buộc được thể hiện bằng các đa thức mô tả mối quan hệ giữa các biến.
- **Giao tiếp tương tác:**
  - Prover tính toán để chứng minh các ràng buộc được thỏa mãn tại các điểm do verifier chọn ngẫu nhiên.
  - Verifier nhận các giá trị đa thức tại các điểm đó cùng bằng chứng, mà không cần biết toàn bộ đa thức.
- **Biến giao thức tương tác thành không tương tác:** Dùng *Fiat–Shamir heuristic* để tạo điểm kiểm tra ngẫu nhiên từ đầu vào và transcript trước đó.

  Điều này cho phép tạo chứng minh một lần duy nhất mà không cần tương tác nhiều lượt.

3 Sử dụng cam kết đa thức trong ZKP

Cam kết đa thức (*Polynomial Commitment Schemes*) cho phép prover cam kết một đa thức mà không tiết lộ nó.

Prover có thể chứng minh giá trị tại điểm bất kỳ mà vẫn giữ bí mật toàn bộ đa thức, bảo đảm:

- **Tính ràng buộc (binding)**
- **Tính ẩn danh (hiding)**

Việc này giúp verifier xác minh ràng buộc đại số mà không biết toàn bộ dữ liệu.

4 Ý nghĩa của các cấu trúc toán học trong ZKP

- **Đường cong elliptic và phép ghép đôi:**
  - Giúp xây dựng cam kết và bằng chứng ngắn gọn, hiệu quả.
  - Ví dụ: *KZG commitments* dựa trên đường cong elliptic.
- **Đa thức và phép nội suy:** Dùng để biểu diễn và kiểm tra các ràng buộc logic phức tạp bằng cách đánh giá đa thức tại các điểm.
- **Giao thức tương tác:** Xây dựng chứng minh với các tính chất:
  - **Completeness (Đầy đủ):** Nếu khẳng định đúng, prover sẽ thuyết phục được verifier.
  - **Soundness (Độ tin cậy):** Nếu khẳng định sai, prover không thể lừa verifier.
  - **Zero knowledge (Không tiết lộ):** Không rò rỉ bất kỳ thông tin nào ngoài tính đúng.

5 Ví dụ minh họa

Trong các hệ thống như **PLONK** hoặc **SNARKs**:

- Bài toán được biểu diễn bằng hệ đa thức.
- Prover cam kết đa thức bằng sơ đồ KZG trên đường cong elliptic.
- Verifier chọn điểm ngẫu nhiên.
- Prover trả lời giá trị đánh giá và bằng chứng tương ứng.
- Verifier xác minh tính hợp lệ mà không cần biết toàn bộ đa thức.

6 Tổng kết quy trình

1. Bắt đầu từ bài toán logic hoặc tính toán.
2. Biến đổi thành đa thức và các ràng buộc đại số.
3. Prover cam kết đa thức.
4. Verifier chọn ngẫu nhiên điểm kiểm tra.
5. Prover trả lời giá trị và bằng chứng.
6. Verifier xác minh và đưa ra quyết định chấp nhận hoặc bác bỏ.

Toàn bộ quá trình này đảm bảo rằng prover có thể chứng minh tính đúng mà không tiết lộ bí mật nào.

Tóm lại

Mục này giải thích cách các công cụ toán học như đa thức, cam kết đa thức, đường cong elliptic, phép ghép đôi và giao thức tương tác được kết hợp để xây dựng các chứng minh **Zero Knowledge Proofs**, đảm bảo tính bảo mật và minh bạch trong các hệ thống mật mã hiện đại.