6. Khái quát quá trình tạo chứng minh Zero Knowledge

Ngày 22 tháng 7 năm 2025

1 Quá trình tạo chứng minh – Các bước chính

Quá trình tạo chứng minh Zero Knowledge (ZK proof) là chuỗi các bước toán học và tương tác giữa **prover** (người chứng minh) và **verifier** (người kiểm chứng):

- **Mô tả bài toán bằng DSL (Domain Specific Language):**
  Bài toán được viết dưới dạng ngôn ngữ chuyên biệt, sử dụng các phép toán và ràng buộc logic để hỗ trợ quá trình chuyển đổi đại số.
- **Arithmetisation – Chuyển đổi sang ràng buộc đại số:**
  Biểu diễn bài toán dưới dạng hệ thống các ràng buộc đại số (constraint system), thường là các biểu thức đa thức.
- **Biểu diễn hệ ràng buộc bằng đa thức:**
  Chuyển ràng buộc thành các đa thức để áp dụng cam kết đa thức và kiểm tra bằng đánh giá tại điểm.
- **Tương tác prover–verifier:**
  - Verifier chọn ngẫu nhiên các điểm đánh giá.
  - Prover gửi bằng chứng cho thấy các đa thức thỏa ràng buộc tại các điểm đó.
  - Verifier kiểm tra mà không cần biết toàn bộ đa thức.
- **Fiat–Shamir heuristic:**
  Biến giao thức tương tác thành không tương tác bằng cách tạo điểm ngẫu nhiên từ hàm băm (*hash function*) thay vì tương tác thực tế.

2 Vai trò của thông tin bất đối xứng

Có sự bất đối xứng trong thông tin giữa hai bên:

- **Prover:** Biết toàn bộ bí mật, dữ liệu đầu vào, và đa thức.
- **Verifier:** Chỉ biết một phần thông tin và tự chọn điểm kiểm tra.

Prover phải thuyết phục verifier mà không tiết lộ thêm bất kỳ thông tin nào — đảm bảo tính *zero knowledge*.

3 Bảo đảm tính đúng đắn và bảo mật

- **Tính đúng đắn (Completeness):**
  Prover trung thực luôn có thể thuyết phục verifier chấp nhận.
- **Tính chống giả mạo (Soundness):**
  Prover gian lận không thể lừa verifier nếu khẳng định sai.
- **Tính không tiết lộ (Zero knowledge):**
  Verifier không học được gì ngoài việc xác nhận khẳng định là đúng.

4 Sơ đồ tóm tắt quy trình

Bài toán (DSL) $\rightarrow$ Ràng buộc đại số $\rightarrow$ Biểu diễn đa thức $\rightarrow$ Prover $\leftrightarrow$ Verifier $\rightarrow$ Fiat–Shamir heuristic $\rightarrow$

5 Tính chất và thách thức trong quá trình tạo chứng minh

- **Độ ngắn gọn:**
  Bằng chứng phải đủ nhỏ để verifier có thể kiểm tra nhanh.
- **Hiệu quả tính toán:**
  Prover có thể tốn nhiều tính toán, nhưng verifier cần xác minh nhanh.
- **Độ tin cậy:**
  Xác suất prover gian lận mà vẫn được chấp nhận phải cực thấp.

Tóm lại

Phần này mô tả tổng quan quy trình tạo chứng minh Zero Knowledge: từ việc mô tả bài toán bằng DSL, chuyển đổi sang dạng đại số, tương tác chứng minh và xác minh, cho đến việc loại bỏ tương tác bằng Fiat–Shamir heuristic. Đây là khung khái niệm giúp hiểu cơ chế hoạt động hiệu quả và bảo mật của ZKP.