THIẾT KẾ VÀ ĐÁNH GIÁ THUẬT TOÁN SHA3-256 TỐI ƯU TRÊN FPGA

DẤU VÂN TAY SỐ CHO THÀNH PHỐ THÔNG MINH

Phạm Ngô Tuấn Tú - Nguyễn Đình Khánh Vy
Nguyễn Tài Anh Tuấn - Huỳnh Trang Vĩnh San

GIỚI THIỆU

Hiện thực kiến trúc Keccak theo mô hình sponge Nhằm giảm độ trễ, tối ưu diện tích logic và công suất tiêu thụ trong các hệ thống bảo mật theo thời gian thực.

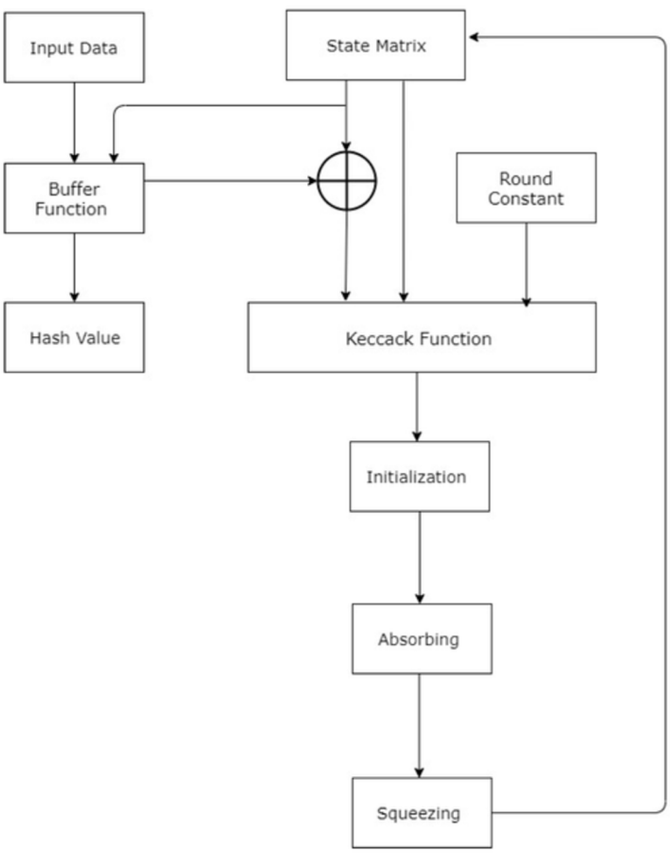
NGUYÊN LÝ CỐT LÕI

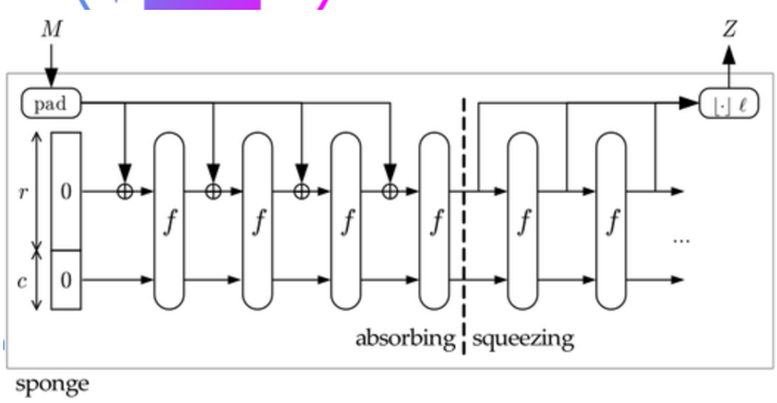
SHA-3 sử dụng kiến trúc sponge gồm 2 giai đoạn:

- Hấp thụ dữ liệu đầu vào qua phép XOR
- Hoán vị Keccak-f, sau đó trích xuất dần đầu ra.

Keccak-f gồm 24 vòng biến đổi phi tuyến, sử dụng các phép logic đơn giản, tối ưu cho phần cứng.

KIẾN TRÚC HỆ THỐNG





sponge

ỨNG DỤNG

Xác thực mật khẩu (Hash + Salt)
Kiểm tra tính toàn vẹn (Checksum)
Giao thức bảo mật: TLS/SSL, IPsec
Blockchain: Ethereum