Ý TƯỞNG CUỘC THI THIẾT KẾ VI MẠCH: LÕI MÃ HÓA ASCON TỐI ƯU CHO THIẾT BỊ IOT

Nguyễn Hữu Học 22520486 . Nguyễn Đình Lê Mạnh 22520848
Lương trùng Dương 22520301 . Lê Trọng Điền 22520246

1. TỔNG QUAN Ý TƯỞNG

Ý tưởng của chúng tôi là thiết kế một lõi vi mạch chuyên dụng (Hardware IP Core) để tăng tốc mã hóa và giải mã sử dụng thuật toán ASCON. Lõi này sẽ tích hợp liền mạch vào các hệ thống trên chip (SoC) của thiết bị IoT, cung cấp khả năng bảo mật mạnh mẽ mà vẫn đảm bảo hiệu suất cao và tiêu thụ năng lượng thấp, phù hợp với môi trường hạn chế của IoT.

2. LÝ DO THỰC HIỆN

a) Được NIST Lựa Chọn làm Tiêu Chuẩn Mới: ASCON là người chiến thắng chính thức trong cuộc thi Lightweight Cryptography của NIST (Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ). Điều này khẳng định tính bảo mật đã được kiểm chứng, hiệu suất tối ưu và khả năng chấp nhận rộng rãi trong tương lai, giảm thiểu rủi ro khi triển khai.

b) Hiệu Suất Vượt Trội trên Tài Nguyên Hạn Chế: ASCON được thiết kế đặc biệt để hoạt động hiệu quả trên các vi điều khiển 8-bit, 16-bit và 32-bit. Khi được triển khai bằng phần cứng, nó có thể đạt được

c) Bảo Mật Toàn Diện (Authenticated Encryption with Associated Data - AEAD): Tính bảo mật dữ liệu (Confidentiality): Đảm bảo thông tin không bị đọc trộm. Xác thực dữ liệu và tính toàn vẹn (Authentication & Integrity): Đảm bảo dữ liệu không bị thay đổi và đến từ nguồn đáng tin cậy. Khả năng AEAD này giúp đơn giản hóa giao thức bảo mật và giảm thiểu overhead so với việc sử dụng riêng rẽ mã hóa và MAC.

d) Khả Năng Chống Tấn Công Kênh Phụ (Side-Channel Attack - SCA): ASCON được thiết kế với các đặc tính giúp chống lại các cuộc tấn công kênh phụ (như phân tích công suất, phân tích thời gian) – những mối đe dọa thực tế đối với các thiết bị nhúng. Việc triển khai phần cứng có thể tận dụng và củng cố thêm các biện pháp chống SCA.

3. QUY TRÌNH THỰC HIỆN

Giai đoạn 1: Nghiên cứu và lên ý tưởng chi tiết

Phân tích yêu cầu: Xác định rõ đối tượng thiết bị IoT , yêu cầu về thông lượng, độ trễ, diện tích chip và ngân sách năng lượng.
Nghiên cứu thuật toán ASCON: Đọc kỹ tài liệu chính thức của NIST về ASCON-AEAD128 và ASCON-AEAD128a.

Giai đoạn 2: Thiết kế RTL (REGISTER-TRANSFER LEVEL)

Xây dựng cấu trúc module: Chia lõi ASCON thành các module nhỏ, dễ quản lý và kiểm tra.

Giai đoạn 3: Mô phỏng và xác minh chức năng

Viết Testbench
Sử dụng Test Vector.
Mô phỏng hồi quy (Regression Simulation)
Đo lường độ bao phủ (Coverage Analysis)

Giai đoạn 4: Thiết kế máy gia tốc ASSCON-P

Tổng hợp (Synthesis): Dùng công cụ EDA (ví dụ:Cadence genus) để chuyển đổi mã RTL thành netlist (mạng các cổng logic) dựa trên một thư viện công nghệ cụ thể (ví dụ: 65nm, 40nm, 28nm cho IoT). Đặt các ràng buộc về tần số hoạt động, diện tích chip và tiêu thụ năng lượng để tối ưu hóa.

Giai đoạn 5: Kiểm tra và đánh giá thực tế (POST-SILICON VALIDATION)

Kiểm tra tính hợp lệ của bố cục (DRC/LVS): Đảm bảo bố cục tuân thủ các quy tắc thiết kế của xưởng đúc chip và khớp với netlist.

4. KẾT LUẬN

Thiết kế lõi mã hóa ASCON không chỉ là một bài toán kỹ thuật mà còn là một bước tiến quan trọng trong việc nâng cao bảo mật cho hệ sinh thái IoT. Bằng cách cung cấp một giải pháp mã hóa hiệu quả, nhỏ gọn và an toàn, dự án này sẽ góp phần xây dựng một tương lai nơi dữ liệu IoT được truyền tải và xử lý một cách đáng tin cậy, ngay cả trong các môi trường tài nguyên hạn chế nhất.