TRÍCH YẾU LUẬN ÁN TIẾN SỸ KỸ THUẬT

Tên tác giả: **Trần Văn Toàn**

Tên luận án: **Nghiên cứu nâng cao hiệu năng RO PUF dùng trong bảo mật phần cứng.**

Thuộc chuyên ngành: Kỹ thuật Điện tử

Mã số chuyên ngành: 9 52 02 03

Cơ sở đào tạo: Học viện Kỹ thuật Quân sự

1. Mục đích nghiên cứu của luận án

Luận án nghiên cứu các giải pháp nâng cao hiệu năng mạch PUF dao động vòng (RO PUF), dùng trong phát triển các ứng dụng bảo mật phần cứng. Cụ thể, nghiên cứu sinh đề xuất mô hình trích xuất đặc trưng cục bộ của mạch RO PUF, ứng dụng trong định danh và xác thực thiết bị; nghiên cứu các kỹ thuật ổn định chuỗi bit ra đáp ứng RO PUF; đồng thời phát triển các mạch ứng dụng và thực nghiệm kiểm chứng kết quả trên FPGA.

Đối tượng, phạm vi và phương pháp nghiên cứu:

Đối tượng nghiên cứu: Mạch RO PUF

Phạm vi nghiên cứu:

- Về lý thuyết, nghiên cứu mô hình thống kê của tần số mạch RO PUF, tham số định lượng phẩm chất RO PUF và tính khả thi của các ứng dụng RO PUF cụ thể.

- Về thực nghiệm, phát triển các ứng dụng của mạch RO PUF trong việc tách và xác thực ID cho thiết bị, tạo chuỗi bit ra ổn định và duy nhất, phục vụ mã hóa bảo mật.

Phương pháp nghiên cứu:

- Khảo sát các nghiên cứu đã có, tập trung vào RO PUF trên các phương diện như mô hình toán, phương pháp xây dựng mạch vật lý, cơ chế tạo dữ liệu đáp ứng, các ứng dụng của RO PUF trong bảo mật phần cứng.

- Đánh giá khả năng phát triển các ứng dụng của phần cứng thực thi thiết kế PUF, cụ thể là các họ FPGA Xilinx Spartan-3E, Spartan-6 và Artix-7.

- Thử nghiệm mạch phần cứng thực thi thiết kế RO PUF trong các điều kiện môi trường khác nhau.

- Phân tích thống kê dữ liệu thực nghiệm, rút ra kết luận về đặc tính vật lý cần nghiên cứu.

- Sử dụng các công cụ hỗ trợ thiết kế và mô phỏng trong thiết kế logic số: Xilinx ISE, Xilinx Vivado, Mentor Graphics Modelsim; phần mềm tính toán và mô phỏng Matlab-Simulink.

2. Các kết quả chính

- Xây dựng mô hình thống kê của tần số RO, phân tích định tính và định lượng mức độ ảnh hưởng của nhiệt độ môi trường, điều kiện hoạt động lên các thành phần trong tần số RO.

- Đề xuất sơ đồ tách và xác thực ID cho thiết bị sử dụng mạch RO PUF thực thi trên FPGA, trong đó sử dụng các tham số khoảng cách và mức ngưỡng xác thực dựa trên độ đo Euclid. So với các kết quả nghiên cứu đã có, phương pháp đề xuất đã nâng cao độ tin cậy xác thực ID lên vài bậc độ lớn.

- Đề xuất các phương pháp ổn định chuỗi bit tạo ra bởi RO PUF để có thể tạo khóa mã hoặc tạo mã khởi tạo, phục vụ các ứng dụng mã hóa hoặc tạo số ngẫu nhiên.

Hà Nội, ngày tháng 4 năm 2023

T/M TẬP THỂ HƯỚNG DẪN	**NGHIÊN CỨU SINH**
PGS. TS. Hoàng Văn Phúc	**Trần Văn Toàn**