TRANG THÔNG TIN LUẬN ÁN TIẾN SĨ

Tên đề tài luận án tiến sĩ: **Nghiên cứu giải pháp nâng cao hiệu quả sử dụng mật mã đường cong elliptic trên các thiết bị tính toán nhúng.**

Chuyên ngành: Kỹ thuật điện tử

Mã số: 9.52.02.03

Họ và tên NCS: **Phạm Văn Lực**

Người hướng dẫn khoa học:

1. PGS. TSKH. Hoàng Đăng Hải

2. TS. Lều Đức Tân

Cơ sở đào tạo: Học viện Công nghệ Bưu chính Viễn thông

NHỮNG KẾT QUẢ MỚI CỦA LUẬN ÁN:

Các hệ thống nhúng dựa trên vi xử lý ARM đang được ứng dụng rộng rãi trên nhiều dòng thiết bị hiện nay như: Thiết bị di động, máy tính bảng, thiết bị IoT, các thiết bị mật mã…. Đặc điểm chung của hệ thống nhúng là hạn chế về tài nguyên và năng lực xử lý. Các hệ thống nhúng thường có kích thước nhỏ hơn, khả năng xử lý yếu hơn, bộ nhớ nhỏ hơn và yêu cầu tiêu thụ ít năng lượng do sử dụng nguồn pin. Việc triển khai các giải pháp an toàn bảo mật thông tin cho các hệ thống nhúng có thêm nhiều thách thức so với các hệ thống máy tính truyền thống.

Hệ mật đường cong Elliptic (ECC) đã được đề xuất sử dụng cho các hệ thống nhúng do kích thước khóa nhỏ hơn nhiều so với các hệ mật khóa công khai khác. Các lược đồ mã hóa dựa trên ECC đã được đề xuất điển hình là lược đồ thỏa thuận khóa Diffie Hellman trên đường cong elliptic (ECDH) và thuật toán chữ ký số trên đường cong elliptic (ECDSA). ECC có nhiều ưu việt và phù hợp cho bảo mật dữ liệu trên các thiết bị nhúng. Tuy nhiên, việc nghiên cứu cải tiến các thuật toán ECC đảm bảo cân bằng giữa an toàn và hiệu quả trong các hệ thống nhúng có tài nguyên hạn chế vẫn đang là vấn đề có nhiều thách thức (thực thi, đáp ứng thời gian thực, tài

nguyên sử dụng...)

Luận án tập trung vào nghiên cứu các giải pháp cải tiến về hiệu quả khi triển khai các thuật toán, lược đồ thỏa thuận khóa, chữ ký số dựa trên hệ mật đường cong Elliptic trên các hệ thống, vi xử lý nhúng (chủ yếu là dòng ARM Cortex-A) được sử dụng phổ biến trong thực tiễn.

Các kết quả mới của luận án như sau:

1) Đề xuất phương pháp nhân phân tầng hai số hạng trên trường hữu hạn dựa trên hai thuật toán nhân cơ bản là thuật toán nhân theo phương pháp phổ thông và thuật toán nhân theo phương pháp Karatsuba. Với phương pháp phân tầng, luận án đã xây dựng được thuật toán nhân có chi phí tốt nhất trong các trường hợp cụ thể cũng như đưa ra công thức để xác định chi phí của thuật toán đó. Thuật toán đề xuất đã được kiểm chứng về tính hiệu quả trên nền vi xử lý nhúng ARMv7 và ARMv8.

2) Đề xuất, cải tiến thuật toán nhân vô hướng (nhân giữa một điểm và một số nguyên dương) của hệ mật đường cong Elliptic trên trường nguyên tố dựa trên đề xuất cải tiến thuật toán NAF và đề xuất nâng cao hiệu quả của các phép toán số học (cộng điểm, nhân đôi điểm) theo phương pháp thực hiện song song hai phép nhân.

CÁC ỨNG DỤNG, KHẢ NĂNG ỨNG DỤNG TRONG THỰC TIỄN HOẶC NHỮNG VẤN ĐỀ CÒN BỎ NGỎ CẦN TIẾP TỤC NGHIÊN CỨU:

Các đề xuất nâng cao hiệu quả về sử dụng mật mã đường cong elliptic trên thiết bị nhúng trong luận án sẽ góp phần tăng cường khả năng bảo mật thông tin trên các thiết bị nhúng, ngăn chặn tấn công nghe lén và rò rỉ thông tin cá nhân. Các kết quả của luận án có ý nghĩa đặc biệt trong lĩnh vực an ninh quốc phòng: Khả năng mềm dẻo ở tùy biến tham số, thuật toán được bản địa hóa, khả năng đáp ứng thời gian thực của các phần mềm bảo mật.

Liên quan đến những đề xuất mới của luận án, có thể liệt kê những vấn đề cần nghiên cứu trong các công trình tiếp theo như sau:

1) Thuật toán nhân phân tầng được xây dựng trên trên cơ sở hai thuật toán cơ

bản là thuật toán theo phương pháp phổ thông và thuật toán nhân theo phương pháp Karatsuba. Tuy nhiên, cần có những nghiên cứu đề xuất thuật toán phân tầng dựa trên các thuật toán cơ sở khác (như Montgomery) cũng như cho phép toán khác như: modulo, bình phương...

2) Nghiên cứu, nâng cao hiệu quả các các lược đồ, thuật toán mật mã dựa trên ECC cho các hệ vi xử lý nhúng khác như dòng ARM Cortex-M.

3) Nghiên cứu đảm bảo an toàn chống lại tấn công kênh kề cho các thuật toán mật mã của hệ mật ECC hoạt động trên nền vi xử lý nhúng.

Xác nhận của tập thể **Người hướng dẫn khoa học**	**Nghiên cứu sinh**
PGS. TSKH. Hoàng Đăng Hải	**Phạm Văn Lực**