TRANG THÔNG TIN LUẬN ÁN TIẾN SĨ

Tên đề tài luận án tiến sĩ: **Mã mạng trên một số cấu trúc đại số**

Chuyên ngành: Kỹ thuật điện tử

Mã số: 9.52.02.03

Họ và tên NCS: **Phạm Long Âu**

Người hướng dẫn khoa học:

1. TS. Ngô Đức Thiện

2. TS. Nguyễn Lê Cường

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

NHỮNG KẾT QUẢ MỚI CỦA LUẬN ÁN:

Với các lợi ích của kỹ thuật mã mạng nhằm nâng cao hiệu quả của hệ thống truyền tin và với một số phương pháp mã mạng khác nhau mà các nhà nghiên cứu đi trước đã thực hiện, nghiên cứu sinh lựa chọn nghiên cứu về lĩnh vực kỹ thuật mã mạng và đề xuất ý tưởng xây dựng kỹ thuật mã mạng bằng phương pháp mới, dựa trên một số cấu trúc đại số. Sau quá trình nghiên cứu, tìm hiểu, nghiên cứu sinh đã đề xuất các phương thức mã mạng trên một số cấu trúc đại số thông dụng như: các phép toán trên vành số, các nhóm cộng trên đường cong elliptic, vành đa thức, trường đa thức và các nhóm nhân trên trường GF… Ngoài ra, với lợi ích giảm phiên liên lạc của mã mạng có thể kết hợp với một số hệ mã công khai (mật mã khóa bất đối xứng). Trong nội dung luận án, nghiên cứu sinh đề xuất thêm giải pháp sử dụng hai hệ mật khóa công khai Omura-Massey và ElGamal kết hợp với phương pháp mã mạng mà nghiên cứu sinh đã đề xuất để có được một mô hình mã mạng an toàn (có bảo mật). Những đóng góp mới của quá trình nghiên cứu thể hiện trong luận án như sau:

1. Nghiên cứu sinh đã tập trung nghiên cứu đề xuất xây dựng một số phương pháp mã mạng trên một số cấu trúc đại số mới như: (1) mã mạng xây dựng trong vành số, trường số, trong đó có phép cộng, phép nhân và kết hợp phép cộng và phép nhân; (2) mã mạng xây dựng trên trường đa thức, vành đa thức, trong đó có phép cộng, phép nhân và kết hợp phép cộng và phép nhân; (3) mã mạng xây dựng

trên đường cong Elliptic. Cụ thể là:

- Phương pháp mã mạng dựa trên phép cộng của các vành số;
- Phương pháp mã mạng dựa trên phép nhân của vành số;
- Phương pháp mã mạng Affine trên vành số;
- Phương pháp mã mạng trên vành đa thức;
- Phương pháp mã mạng bằng phép nhân trên trường đa thức;
- Phương pháp mã mạng Affine trên trường đa thức;
- Phương pháp mã mạng dựa trên đường cong elliptic;
- Phương pháp mã mạng dựa trên nhóm cộng Zp;
- Phương pháp mã mạng dựa trên GF(p).

Các nghiên cứu, đề xuất này mang tính mới, khác so với các phương pháp mã mạng của các nhà khoa học đã nghiên cứu trước đây, nhưng vẫn đảm bảo được các tiêu chí về giảm phiên truyền, tăng thông lượng theo yêu cầu của kỹ thuật mã mạng.

2. Nghiên cứu sinh cũng đã tập trung nghiên cứu lý thuyết về hai hệ mật khóa công khai Omura-Massey và ElGamal để từ đó đề xuất xây dựng phương pháp "Mã mạng an toàn dựa trên hai hệ mật Omura-Masey và Elgamal trên vành số" nhằm kết hợp ưu điểm của việc giảm phiên truyền dẫn (của mã mạng) với các hệ mật mã công khai, để tạo ra một mã mạng an toàn. Các bước của mô hình này tóm tắt như sau: Bước 1: xác thực bảo mật dùng hệ mật ElGamal; Bước 2: giải mã và xác thực, kết hợp (che giấu) bản tin bằng mặt nạ cộng hoặc nhân; Bước 3: phát quảng bá bằng hệ mật O-M.

Ưu điểm của mô hình đề xuất đó là: (1) Sử dụng được ưu điểm của mã mạng là giảm số phiên truyền dẫn giữa các nút truyền trên mạng (tăng thông lượng), tăng độ ổn định của việc truyền tin; (2) thông tin truyền trong mạng được bảo mật an toàn nhờ các hệ mật khóa công khai. Độ an toàn của các hệ mật khóa công khai dựa trên bài toán logarit rời rạc, đã được chứng minh là bài toán an toàn với trường hợp số nguyên tố lớn.

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

Hiện nay, kỹ thuật mã mạng vẫn là một kỹ thuật mới, một lĩnh vực khó trên thế giới. Các nhà nghiên cứu vẫn chưa đưa ra được nhiều phương thức mã hóa mang lại hiệu quả cao. Đặc biệt, các đơn vị nghiên cứu chưa xây dựng được hệ thống mô phỏng kiểm tra - "*Simulation testbed*" của toàn bộ hệ thống viễn thông để có thể nhanh chóng thử nghiệm một kết quả lý thuyết bằng mô phỏng thực nghiệm. Hơn nữa, khi hướng đến phát triển công nghệ thực tiễn trong lĩnh vực này ta chưa có các thiết bị cho phép kiểm nghiệm thực tế các kết quả nghiên cứu của kỹ thuật mã mạng.

Từ những nội dung trên, trong thời gian tới nghiên cứu sinh định hướng sẽ tiếp tục nghiên cứu, phân tích sâu hơn để có thể đánh giá đầy đủ tính hiệu quả các phương thức, thuật toán mã mạng mà nghiên cứu sinh đã đề xuất. Đặc biệt là việc viết các chương trình cho các thuật toán đã đề xuất và xây dựng hệ thống kiểm thử thông qua mô phỏng bằng các phần mềm rồi tiến tới mô phỏng trong thực tế để có thể đưa các phương thức mã mạng vào trong thực tế nhằm nâng cao hiệu quả truyền tin.

Ngoài ra, với những kiến thức mà nghiên cứu sinh đã có được trong quá trình thực hiện luận án này, nghiên cứu sinh sẽ tiếp tục nghiên cứu và hợp tác với các đồng nghiệp đang nghiên cứu trong lĩnh vực mã mạng để có thể đưa ra được nhiều phương thức, thuật toán mã mạng mới hiệu quả hơn và đưa vào ứng dụng trong thực tế.

Xác nhận của đại diện tập thể **Người hướng dẫn khoa học**	**Nghiên cứu sinh**
TS. Ngô Đức Thiện	**Phạm Long Âu**