TRANG THÔNG TIN LUẬN ÁN TIẾN SĨ

Tên đề tài luận án tiến sĩ:

Nghiên cứu hệ mật hạng nhẹ trên vành đa thức ứng dụng vào thiết bị có tài nguyên hạn chế

Chuyên ngành: **Kỹ thuật điện tử**

Mã số: **9.52.02.03**

Họ và tên NCS: **Hoàng Mạnh Thắng**

Người hướng dẫn khoa học: **GS.TS. Nguyễn Bình**

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

NHỮNG KẾT QUẢ MỚI CỦA LUẬN ÁN

1. Xây dựng được hệ mật CBC-QRHE (Hệ mật lai ghép dựa trên thặng dư bậc hai và các phần tử liên hợp của vành đa thức chẵn có khả năng chống tấn công bằng bản rõ chọn trước). Với khả năng chống tấn công bằng bạn rõ chọn trước (CPA), hệ mật CBC-QRHE được coi là đã đảm bảo độ an toàn. Ngoài ra, về mặt lý thuyết, các thuật toán giải mã và mã hóa của hệ mật CBC-QRHE có độ phức tạp tính toán O(n), và về mặt thực tế, các module của hệ mật đã được cài đặt trên thiết bị có tài nguyên hạn chế, và đã đã được đánh giá là hiệu quả hơn hệ mật nguyên gốc. Như vậy, hệ mật CBC-QRHE được coi là phù hợp với thiết bị có tài nguyên hạn chế.

2. Xây dựng được hệ mật OM-CA (Hệ mật Omura-Massey trên vành đa thức có hai lớp kề Cyclic có nhận thực). Hệ mật OM-CA tuy chưa được thử nghiệm trên thiết bị thực, nhưng về mặt lý thuyết, thuật toán giải mã và mã hóa của hệ mật OM-CA có độ phức tạp tính toán O(n), có thể coi là hệ mật mã có khả năng phù hợp với thiết bị có tài nguyên hạn chế. Ngoài ra, trong quá trình xây dựng hệ mật OM-CA, tác giả đã đề xuất bốn phương pháp bổ sung tính nhận thực vào các hệ mật trên vành đa thức.

3. Xây dựng được hệ mật OM-PI (Hệ mật Omura-Massey trên vành đa thức có hai lũy đẳng nguyên thủy). Hệ mật OM-PI cũng chưa được thử nghiệm trên thiết bị thực, tuy nhiên, về mặt lý thuyết, hệ mật OM-PI có độ phức tạp tính toán là O(n), tương tự như hệ mật OM-CA, OM-PI cũng được coi là phù hợp với thiết bị có tài nguyên hạn chế. Một trong những kết quả quan trọng khác khi xây dựng hệ mật OM-PI là đã làm rõ được tính chất tựa đẳng cấu giữa vành đa thức hai lũy đẳng nguyên thủy với trường hữu hạn GF(p), đây là nền tảng toán học để xây dựng hệ mật OM-PI.

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

Về mặt lý thuyết, phương pháp nghiên cứu trong luận án có thể được áp dụng để tiếp tục nghiên cứu, xây dựng các hệ mật mã hạng nhẹ khác theo hai hướng tiếp cận như sau: một là sử dụng vành đa thức để cải tiến các hệ mật đang có thành hệ mật mã hạng nhẹ, hai là sử dụng vành đa thức để xây dựng hệ mật mã hạng nhẹ mới. Về mặt ứng dụng, 3 hệ mật trong luận án cần phải bổ sung thêm các bước nghiên cứu nhằm chứng minh hiệu năng, độ tương thích, tính khả dụng trước khi đưa vào ứng dụng trong thực tế.

Vậy, có một số vấn đề mở, cần tiếp tục nghiên cứu như sau:

1. Mở rộng và hoàn thiện lý thuyết về ứng dụng vành đa thức trong mật mã nói chung, mật mã hạng nhẹ nói riêng. Đặc biệt các ứng dụng của vành đa thức hai lũy đẳng nguyên thủy trong cải tiến, xây dựng các hệ mật mã hạng nhẹ mới.
2. Cài đặt và đánh giá hệ mật CBC-QRHE, OM-CA, OM-PI trên các thiết bị có tài nguyên hạn chế phổ biến trên thị trường, đa dạng cấu trúc như FPGA, ASIC.
3. Đưa các hệ mật CBC-QRHE, OM-CA, OM-PI vào trong các ứng dụng trong thực tế, thực hiện chức năng đảm bảo an toàn bảo mật thông tin khi trao đổi dữ liệu giữa các thiết bị IoT.

Xác nhận của khoa Kỹ thuật điện tử 1	**Nghiên cứu sinh**
Phó trưởng khoa phụ trách	
TS. Nguyễn Trung Hiếu	**Hoàng Mạnh Thắng**