TRANG THÔNG TIN LUẬN ÁN TIẾN SĨ

Tên đề tài luận án tiến sĩ: ***Về một thuật toán sinh số giả ngẫu nhiên dựa trên phương pháp tạo dãy phi tuyến lồng ghép với bậc lớn***

Chuyên ngành: Kỹ thuật Điện tử

Mã số: 9.52.02.03

Họ và tên NCS: **Đặng Vân Trường**

Người hướng dẫn khoa học:

GS.TSKH. Nguyễn Xuân Quỳnh

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

NHỮNG KẾT QUẢ MỚI CỦA LUẬN ÁN:

Dãy giả ngẫu nhiên dựa trên m-dãy là bài toán luôn được quan tâm trong thời gian qua, các dãy này đã có nhiều ứng dụng trong kỹ thuật điện tử-viễn thông và bảo mật thông tin. Thông qua việc nghiên cứu kiến trúc và các đặc điểm, tính chất của dãy phi tuyến lồng ghép cùng với các yêu cầu của việc ứng dụng dãy phi tuyến lồng ghép ứng dụng trong việc bảo mật thông tin, luận án đưa ra giải pháp cho việc sử dụng dãy phi tuyến lồng ghép bảo đảm các yêu cầu về bảo mật mà vẫn có thể thực hiện được trong điều kiện thực tế. Các đóng góp mới của quá trình nghiên cứu thể hiện trong luận án như sau:

(1) Đề xuất một giải pháp sinh dãy phi tuyến lồng ghép dựa trên kỹ thuật phân rã theo bước và kỹ thuật tính một phần thứ tự lồng ghép. Giải pháp này có thể ứng dụng trong cài đặt thực tế để sinh ra một đoạn có kích thước tùy ý của dãy phi tuyến lồng ghép.

(2) Đề xuất một thuật toán hiệu quả để sinh dãy phi tuyến lồng ghép với bậc lớn, phân tích đánh giá thuật toán đã đề xuất về độ phức tạp tính toán, độ phức tạp lưu trữ và kết quả tính toán thực nghiệm. Thuật toán có độ phức tạp tính toán tiệm cận với $O(n^3)$ với n là bậc của đa thức sinh m-dãy. Bằng cách khai thác một đặc điểm của tham số của dãy lồng ghép, thuật toán này có lợi thế lớn hơn so với thuật toán bình phương và nhân thông thường.

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

Từ những đề xuất đưa ra trong luận án, ta có một phương án khả thi để có thể ứng dụng dãy lồng ghép phi tuyến trong bảo mật thông tin trong thực tế với mức độ bảo mật cao mà không yêu cầu năng lực xử lý cũng như tài nguyên tính toán quá lớn. Ngoài việc ứng dụng dãy phi tuyến lồng ghép trong kỹ thuật mật mã, còn rất nhiều lĩnh vực kỹ thuật có thể ứng

dụng dãy phi tuyến lồng ghép như một bộ tạo dãy giả ngẫu nhiên với các mục đích khác nhau.

Các vấn đề cần tiếp tục nghiên cứu

Việc đề xuất một thuật toán mật mã mới cần phải xem xét rất kỹ về tính an toàn của thuật toán trên nhiều khía cạnh trước khi có thể đưa vào sử dụng thực tế, cần có các nghiên cứu sâu hơn về việc phân tích mã đối với dãy lồng ghép và phi tuyến lồng ghép, cũng như dãy luân phiên phi tuyến lồng ghép

Một công việc khác cần tiếp tục nghiên cứu là giải pháp để cài đặt hiệu quả các dãy trên GF(p^n) với số p nguyên tố lớn (p>2) trên cả hai môi trường: phần mềm máy tính và các thiết bị xử lý trực tiếp bằng phần cứng. Ta cũng cần nghiên cứu về việc sử dụng hiệu quả dãy đầu ra trên GF(p^n) ví dụ như một phương pháp chuyển đổi dữ liệu từ hệ q-phân sang hệ nhị phân.

Xác nhận của đại diện tập thể	**Nghiên cứu sinh**
Người hướng dẫn khoa học	
GS.TSKH. Nguyễn Xuân Quỳnh	**Đặng Vân Trường**