TRANG THÔNG TIN LUẬN ÁN TIẾN SĨ

- Tên đề tài luận án tiến sĩ: ***Nghiên cứu phát triển một số lược đồ chữ ký số mù, chữ ký số tập thể mù dựa trên các chuẩn chữ ký số***
- Chuyên ngành: Kỹ thuật máy tính
- Mã số: 9.48.01.06
- Họ và tên NCS: Nguyễn Tấn Đức
- Người hướng dẫn khoa học:
  1. PGS. TS Nguyễn Hiếu Minh
  2. TS. Ngô Đức Thiện.
- Cơ sở đào tạo: Học viện Công nghệ Bưu chính Viễn thông

NHỮNG KẾT QUẢ MỚI CỦA LUẬN ÁN:

1) Đề xuất giao thức ký số mù mới dựa trên độ khó của bài toán logarit rời rạc modulo một hợp số nguyên $n = p*q$. Giao thức mới sử dụng hai vấn đề khó làm tăng độ an toàn do giảm xác xuất phá vỡ tiềm năng vì các giải pháp tiềm năng phải giải quyết đồng thời hai vấn đề khó về tính toán như: (1) phân tích hợp số n chứa hai số nguyên tố chưa được biết p, q, và (2) Tìm logarit rời rạc modulo các số nguyên tố p, q. Giao thức được thiết kế là trên cơ sở sử dụng các nhóm hữu hạn không vòng hai chiều. Khi chọn các tham số có 80-bit an toàn thì chữ ký có kích thước 240 bits.

2) Đề xuất hai lược đồ chữ ký số tập thể mù dựa trên chuẩn GOST R34.10-94 và lược đồ Schnorr, hai lược đồ chữ ký số tập thể mù dựa trên chuẩn GOST R34.10-2012 và lược đồ EC-Schnorr. Các lược đồ đề xuất dựa trên các chuẩn và lược đồ chữ ký số đã được chứng minh đảm bảo an toàn. Sau đó mở rộng chức năng để xây dựng các lược đồ chữ ký số tập thể mù, điều này giúp kế thừa tính an toàn, đồng thời có hiệu năng tính toán tốt hơn một số lược đồ chữ ký số đề xuất trước đây.

3) Đề xuất lược đồ chữ ký số mới dựa trên độ khó của bài toán phân tích một số nguyên và bài toán logarit rời rạc. Sau đó mở rộng để xây dựng lược đồ chữ ký mù đơn và tập thể mù, mà để phá vỡ lược đồ này yêu cầu phải giải đồng thời hai bài toán khó. Lược đồ mới đề xuất dựa trên lược đồ RSA và Schnorr. Lược đồ đề xuất được chứng minh đảm bảo tính đúng, tính mù, tính không chối bỏ, ngẫu nhiên. Các lược đồ xuất an toàn và có hiệu năng tính toán tốt, và do đó có thể ứng dụng được trong thực tế.

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

- Luận án đã đề xuất một số lược đồ chữ ký số mù, chữ ký số tập thể mù có thể được sử dụng trong các ứng dụng có yêu cầu tính ẩn danh như thanh toán trực tuyến, bầu cử trực tuyến,… góp phần đáp ứng những yêu cầu cấp bách về chuyển đổi số của Việt Nam hiện nay.

- Tuy nhiên, cần tiếp tục nghiên cứu đề xuất các dạng lược đồ chữ ký số mù dựa trên hai bài toán khó đối với các ứng dụng đòi hỏi yêu cầu về tính an toàn cao trong hệ thống có hạ tầng hạn chế về nguồn lực tài nguyên như các thiết bị công nghiệp 4.0 như IoT,...

Xác nhận của người hướng dẫn khoa học	**Nghiên cứu sinh**
PGS.TS Nguyễn Hiếu Minh; TS. Ngô Đức Thiện	Nguyễn Tấn Đức