THÔNG TIN LUẬN ÁN TIẾN SĨ

I. Thông tin chung

Tên đề tài luận án:

NGHIÊN CỨU VÀ XÂY DỰNG
LƯỢC ĐỒ CHỮ KÝ SỐ TẬP THỂ ĐẠI DIỆN

Chuyên ngành: **KHOA HỌC MÁY TÍNH**

Mã số: **948 01 01**

Họ và tên NCS: **NGUYỄN KIM TUẤN**

Người hướng dẫn khoa học:

1. TS. Hồ Ngọc Duy

2. PGS.TS Đoàn Văn Ban

Cơ sở đào tạo: **Trường Đại học Duy Tân**

II. Những kết quả chính của luận án

1. Đã đề xuất được một loại lược đồ chữ ký số tập thể mới có tính thực tế cao, đó là, chữ ký số tập thể đại diện. Có 2 dạng lược đồ chữ ký số tập thể đại diện: i) Chữ ký số tập thể cho các nhóm ký và ii) Chữ ký số tập thể cho các nhóm ký và các cá nhân ký.

2. Đã xây dựng được 4 lược đồ chữ ký số tập thể đại diện dựa trên các bài toán logarit rời rạc: Trên trường nguyên tố hữu hạn (2 lược đồ); Trên đường cong Elliptic sử dụng chuẩn ECDSA (2 lược đồ).

3. Đã xây dựng được 4 lược đồ chữ ký số tập thể đại diện dựa trên bài toán khó mới, bài toán tìm căn modulo số nguyên tố lớn, với các modulo nguyên tố có cấu trúc đặc biệt khác nhau: $p = Nt_0t_1t_2 + 1$ (2 lược đồ) và $p = Nk^2 + 1$ (2 lược đồ).

4. Đã đề xuất và xây dựng được 4 lược đồ chữ ký số tập thể đại diện 2 thành phần dựa trên các bài toán logarit rời rạc: Trên trường nguyên tố hữu hạn (2 lược đồ); Trên đường cong Elliptic sử dụng chuẩn GOST R34.10-2012 (2 lược đồ).

5. Đã đề xuất được 2 lược đồ chữ ký số tập thể đại diện dựa trên đồng thời hai bài toán khó: Bài toán phân tích số nguyên lớn thành các thừa số nguyên tố và Bài toán logarit rời rạc trên trường hữu hạn nguyên tố, sử dụng chuẩn chữ ký Schnorr.

III. Những đóng góp của luận án

Những đóng góp khoa học của luận án bao gồm:

a. Phát hiện và lược đồ hóa được hai yêu cầu chứng thực dựa vào chữ ký số khá phổ biến trong thực tế hiện nay. Đó là: i) Chứng thực được thực hiện cho nhiều nhóm thành viên khác nhau, mỗi nhóm gồm nhiều thành viên, trong đó một người đóng vai trò trưởng nhóm và ii) Chứng thực được thực hiện cho nhiều nhóm thành viên và nhiều thành viên đơn lẻ khác nhau.

Từ đó đề xuất được một loại chữ ký số tập thể mới - "**chữ ký số tập thể đại diện"** - có tính thực tế và cấp thiết cao. Có hai dạng lược đồ chữ ký số tập thể đại diện: i) Lược đồ chữ ký số tập thể cho các nhóm ký và ii) Lược đồ chữ ký số tập thể cho các nhóm ký và các cá nhân ký. Các lược đồ này được hình thành dựa trên sự kết hợp những ưu điểm của lược đồ chữ ký số nhóm và lược đồ chữ ký số tập thể nên ưu điểm và khả năng ứng dụng của nó là khá cao.

b. Kết quả nghiên cứu cho thấy, hoàn toàn có thể: i) Sử dụng một bài toán khó hoặc sử dụng đồng thời hai bài toán khó, như IFP, DLP, ECDLP, PFRM (Một vấn đề khó mới), v.v. và ii) Dựa vào các chuẩn chữ ký số và các lược đồ chữ ký số chuẩn phổ biến, như: Schnorr, DSA, ECDSA, GOST R34.10-2001, v.v. để xây dựng các lược đồ chữ số tập thể đại diện được đề xuất trong luận án này.

Điều này cũng chứng tỏ hiệu quả sử dụng, tính an toàn và tính khả thi của các lược đồ chữ ký số đề xuất ở đây là có thể ghi nhận và tin dùng.

c. Nguyên lý hoạt động của các lược đồ chữ ký số đề xuất chứng tỏ những lược đồ này hoàn toàn có thể triển khai trên các hạ tầng PKI hiện có. Người sử dụng vẫn sử dụng cặp khóa private key và public key để tham gia vào hệ thống xác thực dựa trên chữ ký số tập thể nhưng vẫn đảm bảo tính bí mật và tính riêng tư của cặp khóa bất đối xứng mà họ sở hữu.

Như vậy, kết quả nghiên cứu của LA đã đóng góp cho cộng đồng hai dạng lược đồ chữ ký số tập thể mới có tính thực tế, cập thiết và ứng dụng cao. Luận án cũng đã công bố các lược đồ chữ ký số cụ thể của hai dạng lược đồ đề xuất. Cơ sở toán học, tính đúng đắn, tính an toàn và hiệu năng tính toán của các lược đồ này cũng đã được chỉ ra.

IV. Khả năng ứng dụng trong thực tế

Nguyên lý hoạt động của các lược đồ chữ ký số đề xuất chứng tỏ những lược đồ này hoàn toàn có thể triển khai trên các hạ tầng PKI hiện có. Người sử dụng vẫn sử dụng cặp khóa private key, public key để tham gia vào hệ thống xác thực dựa trên chữ ký số tập thể nhưng vẫn đảm bảo tính bí mật và tính riêng tư của cặp khóa bất đối xứng mà họ sở hữu.

NCS tin rằng, những kết quả được công bố trong luận án này hoàn toàn có thể áp dụng vào thực tế, đáp ứng được các yêu cầu chứng thực cho cả một tập thể gồm nhiều cấp độ chức năng của nhiều ứng dụng trao đổi thông tin trên không gian mạng hiện nay.

V. Hướng nghiên cứu tiếp theo

Trong tương lai, NCS sẽ tiếp tục nghiên cứu và phát triển luận án theo các hướng cụ thể sau đây:

- Nghiên cứu để đề xuất một dạng bài toán khó mới mà có thể sử dụng để xây dựng lược đồ chữ ký số tập thể đại diện và một số dạng lược đồ chữ ký số khác như chữ ký số nhóm, chữ ký số tập thể, chữ ký số tập thể mà, v.v..
- Nghiên cứu để xây dựng các ứng dụng xác thực dựa trên lược đồ chữ ký số tập

thể đại diện mà nó có thể hỗ trợ cho các yêu cầu chứng thức, có tính tập thể, của nhiều bài toán có yêu cầu xác thực khác nhau trong thực tế.

- Triển khai các ứng dụng xác thực, chứng thực dựa trên chữ ký số tập thể đại diện trên hạ tầng PKI hiện có.

Qua quá trình nghiên cứu về chữ ký số tập thể đại diện, với những kết quả đạt được cho đến thời điểm hiện tại, NCS có đầy đủ cở sở để tin rằng những hướng nghiên cứu tiếp theo cũng sẽ mang đến những kết quả khả quan.

Đà Nẵng, ngày 25 tháng 11 năm 2022

Xác nhận của đại diện người HDKH	**Nghiên cứu sinh**
TS. HỒ NGỌC DUY	**NGUYỄN KIM TUẤN**

DANH MỤC CÔNG TRÌNH CỦA TÁC GIẢ

[CT1] **Nguyen Kim Tuan**, Ho Ngoc Duy, "*Xây dựng sơ đồ chữ ký tập thể mù trên cơ sở hệ mật Schnorr",* Journal of Science & Technology of Duy Tan University, 2015.

[CT2] **N. K. Tuan**, V. L. Van, N. A. Moldovyan and H. N. Duy, A. A. Moldovyan, "*Collective signature protocols for signing groups",* Information Systems Design and Intelligent Applications. Advances in Intelligent Systems and Computing (Scopus), INDIA, pp.78-87, 2017.

[CT3] **N. K. Tuan**, N. A Moldovyan, H. N Duy, T. T. V. Lam, V. L. Van*, "New protocols of collective digital signature based on Elliptic curve",* Hội thảo quốc gia: Một số vấn đề chọn lọc của Công nghệ thông tin và truyền thông - Chủ đề: An ninh không gian mạng, Quy Nhơn, pp.57-67, 2018.

[CT4] **Tuan Nguyen Kim**, Duy Ho Ngoc, Nikolay A. Moldovyan, *"Constructing the 2-element AGDS protocol based on the discrete logarithm problem",* International Journal of Network Security & Its Applications, vol.13, no.4, pp.13-22, 2021.

[CT5] **Tuan Nguyen Kim**, Duy Ho Ngoc, Nikolay A. Moldovyan, *"Collective signature protocols for signing groups based on problem of finding roots modulo large prime number",* International Journal of Network Security & Its Applications, vol.13, no.4, pp.59-69, 2021.

[CT6] **Tuan Nguyen Kim**, Nguyen Tran Truong Thien, Duy Ho Ngoc, Nikolay A. Moldovyan. *"Constructing New Collective Signature Schemes Based on Two Hard Problems Factoring and Discrete Logarithm"*, International Journal of Computer Networks & Communications, vol.14, no.2, pp.115-133, 2022 (Scopus).

[CT7] **Tuan Nguyen Kim**, Duy Ho Ngoc, Nikolay A. Moldovyan, "*New Collective Signatures Based on The Elliptic Curve Discrete Logarithm Problem*", Computers, Materials & Continua, vol.73, no.1, pp.595-610, 2021 (SCI/Q2).

[CT8] **Tuan Nguyen Kim**, Duy Ho Ngoc, Nikolay A. Moldovyan, "*New Representative Collective Signatures Based on The Discrete Logarithm Problem*", Computers, Materials & Continua, vol.73, no.1, pp.783-799, 2021 (SCI/Q2).

[CT9] **Tuan Nguyen Kim**, Duy Ho Ngoc, Nikolay A. Moldovyan, "*Constructing Collective Signature Schemes Using Problem of Finding Roots Modulo",* Computers, Materials & Continua, vol.72, no.1, pp.1105-1122, 02/2022 (SCI/Q2).

[CT10] **Tuan Nguyen Kim**, Duy Ho Ngoc, Nikolay A. Moldovyan, *"Constructing New Representative Collective Signature Using The GOST R34.10-2012 Digital Signature Standard"***,** Journal of Communication, vol.17, no.6, pp.478-485, 2022 (SCI/Q3).

[CT11] **Tuan Nguyen Kim**, Duy Ho Ngoc, Nin Ho Le Viet, Nikolay A. Moldovyan, *"The New Collective Signature Schemes Based on Two Hard Problems Using Schnorr's Signature Standard"*, Journal of Advances in Information Technology, vol.14, no.1, pp.77-84, 2022 (SCI/Q3).

[CT12] **Tuan Nguyen Kim**, Duy Ho Ngoc, Nikolay A. Moldovyan, *"Constructing Representative Collective Signature Protocols Using The GOST R34.10-1994 Standard",* Computers, Materials & Continua, vol.74, no.6, pp.1475-1491, 2022 (SCI/Q2).

Nghiên cứu sinh

NGUYỄN KIM TUẤN