VIETNAM NATIONAL UNIVERSITY, HANOI
VNU UNIVERSITY OF ENGINEERING AND TECHNOLOGY

SOCIALIST REPUBLIC OF VIETNAM
Independence – Freedom – Happiness

INFORMATION ON DOCTORAL THESIS

1. Full name : Mai Manh Trung 2. Sex: Male

3. Date of birth: December 29th, 1978 4. Place of birth: Nam Dinh

5. Admission decision number: 867/QĐ-ĐT Dated: November 8th, 2016

6. Changes in academic process: ....

(List the forms of change and corresponding times)

7. Official thesis title: Research and application of lightweight cryptography on smart devices

8. Major: Computer Science 9. Code: 9480101.01

10. Supervisors:

- Assoc.Prof.Dr. Do Trung Tuan
- Dr. Le Phe Do

11. Summary of the **new findings** of the thesis:

- The thesis has proposed cryptography algorithms on elliptic curve.

4) Cryptography algorithm on elliptic curve – CECC

The idea of the algorithm is based on the idea of CAESAR cipher, using a K symmetric key, the K key is a numeric value. The thesis combines this idea with features and operations on elliptic curves to propose cryptographic algorithms on elliptic curves – CECC.

5) Cryptography algorithm on elliptic curve – AECC

The idea of the algorithm is based on the AFFINE cipher idea, using a K symmetric key, the K key is a key pair K(u, v). The thesis combines this idea with features and operations on elliptic curves to propose cryptographic algorithms on elliptic curves – AECC.

6) Cryptography algorithm on elliptic curve – VECC

The idea of the algorithm is based on the Vigenere cipher idea, using a K symmetric key, the K key is a text string value. The thesis combines

this idea with features and operations on elliptic curves to propose cryptographic algorithms on elliptic curves – VECC.

- The thesis develops two elliptic curve cryptography to encrypt Vietnamese text;
- The thesis tested on devices with limited computing power.

12. Practical applicability, if any: .....

13. Further research directions, if any:

- Research models of lightweight cryptographic systems using a combination of the SPN and Feistel structures to design new lightweight block cipher algorithms.
- Propose new algorithms for cryptography on elliptic curves, applied to e-government and digital signatures.
- Research the relationship between elliptic curve cryptography and steganography in images.

14. Thesis-related publications:

1. Lê Phê Đô, **Mai Mạnh Trừng**, Lê Trung Thực, Nguyễn Thị Hằng, Vương Thị Hạnh, Nguyễn Khắc Hưng, Đinh Thị Thúy, Lê Thị Len, *"Nghiên cứu một số hệ mật mã nhẹ và ứng dụng trong IoT"*, Tạp chí Nghiên cứu khoa học và Công nghệ Quân Sự, chủ đề "Những tiến bộ Khoa học trong lĩnh vực An ninh-An toàn thông tin", 137-147, số đặc san 5-2017.
2. Lê Phê Đô, **Mai Mạnh Trừng**, Nguyễn Khắc Hưng, Trần Văn Mạnh, Lê Trung Thực, Lê Thị Len, Nguyễn Thị Hằng *"Cải tiến mã khối nhẹ LED và NOEKEON"*, Kỷ yếu hội thảo Quốc gia lần thứ XX, "Một số vấn đề chọn lọc của CNTT & TT", 8-12, 2017.
3. **Mai Mạnh Trừng**, Lê Phê Đô, Lê Trung Thực, Trần Văn Mạnh, Lê Thị Len, Nguyễn Thị Hằng, Nguyễn Khắc Hưng, *"Nghiên cứu các cuộc tấn công hệ mật mã nhẹ PRESENT",* Kỷ yếu Hội thảo lần thứ II, "Một số vấn đề chọn lọc về An toàn An ninh Thông tin", 1-6, Thành phố H.C.M, 2017.
4. **Mai Mạnh Trừng**, Đỗ Trung Tuấn, Lê Phê Đô, Lê Trung Thực, Đào Thị Phương Anh, "*Xây dựng hệ mật mã đường cong elliptic với khóa đối xứng Affine để mã hóa giải mã văn bản tiếng Việt*", Kỷ yếu Hội nghị KHCN Quốc gia lần thứ XIII về Nghiên cứu cơ bản và ứng dụng Công nghệ thông tin (FAIR), 724-732, Nha Trang, ngày 8-9/10/2020.
5. **Mai Mạnh Trừng**, Lê Trung Thực, Đào Thị Phương Anh, *"Ứng dụng phân tích dữ liệu và phân lớp giám sát NAÏVE BAYES phát hiện gian lận trong thanh toán trực tuyến"*, TNU Journal of Science and Technology, ISSN: 1859-2171 e-ISSN: 2615-9562, 225 (06): 157-164, 2020.
6. **Mai Manh Trung**, Le Phe Do, Le Trung Thuc, Dao Thi Phuong Anh, "*Proposing an elliptic curve cryptosystem with the symmetric key for Vietnamese text encryption and decryption*", International Journal of Advanced Trends in Computer Science and Engineering**,** ISSN 2278-3091, Volume 9, No.3, May - June 2020 **(SCOPUS).**
7. **Mai Manh Trung**, Do Trung Tuan, Le Phe Do, "*Building an elliptic curve cryptography to encode and decode Vietnamese texts*", Computer Science and Communication Engineering, VNU Journal of Science, 44-51, Vol.36, No. 2, 2020.
8. Nguyen Van Tanh, Ngo Quang Tri, **Mai Manh Trung**, "*The solution to improve information security for IoT networks by combining lightweight encryption protocols",* Indonesian

Journal of Electrical Engineering and Computer Science, Vol. 23, No. 3, ISSN: 2502-4752, DOI: 10.11591/ijeecs.v23.i3.pp1727-1735, September 2021 **(SCOPUS).**

9. **Mai Manh Trung**, Do Trung Tuan, Le Phe Do, "*Building elliptic curve cryptography with public key to encrypt Vietnamese text*", Journal of science and technology on information security, Special Issue CS (I5), pp 119-126, 2022.
10. **Mai Manh Trung**, Le Phe Do, Do Trung Tuan, Nguyen Van Tanh, Ngo Quang Tri, *"Design a cryptosystem using elliptic curves cryptography and sysmetry key"*, International Journal of Electrical and Computer Engineering (IJECE), Vol. 13, No. 2, pp. 1734~1743, ISSN: 2088-8708, DOI: 10.11591/ijece.v13i2.pp1734-1743, April 2023 **(SCOPUS).**

Date: November 7th, 2023

Signature: ……

Full name: Dr. Le Phe Do

Date: November 5th, 2023

Signature: ……

Full name: Mai Manh Trung