INFORMATION OF THE DOCTORAL THESIS

Thesis title: **Researching solutions to improve the efficiency of using elliptic curve cryptography on embedded computing devices.**

Speciality: **Electronic Engineering**

Code: **9.52.02.03**

Name of PhD Candidate: **Pham Van Luc**

Scientific supervisors:

1. Assoc. Prof, PhD **Hoang Dang Hai**
2. PhD **Leu Duc Tan**

Training institution: Posts and Telecommunications Institute of Technology

NEW FINDINGS OF THE THESIS

Currently, ARM-based embedded systems are being widely applied on many devices such as: mobile devices, tablets, IoT devices, cryptographic devices.... The common features of embedded systems are resource constrained devices and low performance. Embedded systems typically have small size, weaker performance, small memory, and less energy consumption due to the use of battery power. Deploying information security solutions for embedded systems presents more challenges than for traditional computer systems.

Elliptic curve cryptography (ECC) has been proposed for embedded systems due to its much smaller key size compared to other public key cryptosystems. The typical proposed ECC-based encryption schemes are Diffie Hellman key agreement schemes on elliptic curve (ECDH) and digital signature algorithms on elliptic curve (ECDSA). ECC has many advantages and is suitable for implementation on embedded devices. However, the research and improvement of ECC algorithms to ensure the balance between security and efficiency in embedded systems with limited resources are still challenging issues regarding performance, real-time response, resource usage...

This thesis focuses on researching solutions to improve efficiency in deploying algorithms, key agreement schemes, and digital signatures based on elliptic curve cryptography on embedded systems and processors, which are commonly used in practice.

The new contributions of this thesis are as follows:

1. Proposing a two-term stratified multiplication method on a finite field based on two basic multiplication algorithms, which are the multiplication algorithm according to the standard method and the multiplication algorithm according to the Karatsuba method. With the stratification method, the thesis has built a multiplication algorithm with the best cost in specific cases as well as a formula to determine the cost of that algorithm. The proposed algorithm has been tested for efficiency on ARMv7 and ARMv8 embedded processors.

2. Proposing and improving the scalar multiplication algorithm (multiplying between a point and a positive integer) of the elliptic curve cryptosystem on the prime field based on the proposal to improve the NAF algorithm and the proposal to improve the efficiency of arithmetic operations (adding points, doubling points) by the method of performing dual multiplications in parallel.

APPLICATIONS, PRACTICAL APPLICABILITY AND MATTERS NEED FURTHER STUDIES

Proposals to improve the efficiency of using elliptic curve cryptography on embedded devices in the thesis will contribute to enhancing information security on embedded devices, preventing eavesdropping attacks and personal data leak. The results of the thesis have special significance in the field of national defense and security according to flexibility in parameter customization, localized algorithms, real-time responsiveness of security software.

Regarding the new proposals of the thesis, it is possible to list the issues that need to be studied in the next works as follows:

1. The stratified multiplication algorithm is built on the basis of two basic

algorithms: the school method and the Karatsuba method. However, there is a need for research that allows the stratification algorithm to use other basic algorithms (such as Montgomery) as well as other operations such as modulo, squared, etc.

2. Research on improving efficiency of ECC-based cryptographic schemes and algorithms for other embedded microprocessors such as ARM Cortex-M series.

3. Research on ensuring security against side-channel attack for cryptographic algorithms of ECC cryptosystems based on embedded microprocessors.

Confirmation of representative Scientific supervisor	**PhD. Candidate**
Assoc. Prof. DSc. PhD. Hoang Dang Hai	**Pham Van Luc**