INFORMATION OF THE DOCTORAL THESIS

Thesis title: "Network Coding based on some algebraic structures"

Speciality: Electronic Engineering

Code: 9.52.02.03

PhD. Candidate: Pham Long Au

Scientific supervisors:

1. PhD. Ngo Duc Thien
2. PhD. Nguyen Le Cuong

Training institution: Posts and Telecommunications Institute of Technology

NEW FINDINGS OF THE THESIS

With the benefits of network coding techniques to improve the efficiency of the communication system and with a number of different network coding methods that previous researchers have implemented, the PhD student chooses to study in the field of network coding techniques and propose ideas to build network coding techniques by new methods, based on some algebraic structures. After research, the PhD student has proposed network coding methods on some common algebraic structures such as: operations on number rings, additive groups on elliptic curves, polynomial rings, polynomial field and multiplicative groups on the GF field… In addition, with the benefit of reduced communication sessions, the network cipher can be combined with some public cryptography (asymmetric key cryptography). In the content of the thesis, the PhD student proposes more solutions using two public key cryptosystems Omura-Massey and ElGamal in combination with the network encryption method proposed by the PhD student to obtain a secure network encryption model (with security). The new contributions of the research process shown in the thesis are as follows:

1. The PhD student has focused on researching and proposing to build some network coding methods on some new algebraic structures such as: (1) network coding built in number ring, number field, including addition, multiplication and combination of addition and multiplication; (2) network coding built on polynomial field, polynomial ring, including addition, multiplication and combination of addition and multiplication; (3) network coding built on Elliptic curve. Detail:

- Network coding method is based on the addition of number ring;
- Network coding method based on multiplication of number ring;
- Affine network coding method on number ring;
- Network coding method on polynomial ring;
- The network coding method by multiplying on the polynomial field;
- Affine network coding method on polynomial field;
- Network coding method based on elliptic curve;
- Network coding method based on Zp plus group;
- Network coding method based on GF(p).

These studies and proposals are new, different from the network coding methods previously studied by scientists, but still ensure the criteria of reducing transmission sessions and increasing throughput as required by the network coding techniques.

2. The PhD student also focused on theoretical research on two public-key cryptosystems Omura-Massey and ElGamal, thereby proposing to build a method "Secure network cipher based on two ciphers Omura-Masey and Elgamal on number ring" to combine the advantages of reduced session transmission (of the network coding) with public ciphers, to create a secure network coding. The steps of this model are summarized as follows: Step 1: secure authentication using the ElGamal cryptosystem; Step 2: decrypt and authenticate, combine (hide) the message by adding or multiplying mask; Step 3: broadcast using O-M cryptosystem.

The advantages of the proposed model are: (1) The advantage of the network coding is to reduce the number of transmission sessions between the transmitting nodes on the network (increasing throughput), increasing the stability of the communication; (2) The information transmitted in the network is kept safe by public key cryptosystems. The security of public-key cryptosystems is based on the discrete logarithm problem, which has been shown to be secure in the case of large primes.

APPLICATIONS, PRACTICAL APPLICABILITY AND MATTES NEED FURTHER STUDIES

Currently, network coding techniques is still a new technique, a difficult field in the world. Researchers have yet to come up with many highly efficient encryption methods. In particular, research units have not built a test simulation system of the entire telecommunications system to be able to quickly test a theoretical result by experimental simulation. Moreover, when aiming to develop practical technology in this field, we do not have the equipment that allows to practically test the research results of network coding techniques.

From the above content, in the coming time, the oriented PhD student will continue to research and analyze more deeply to be able to fully evaluate the effectiveness of the network encryption methods and algorithms proposed by the PhD student. Especially, writing programs for the proposed algorithms and building a test system through simulation by software and then moving to simulation in reality to be able to put network coding methods into reality to improve communication efficiency.

In addition, with the knowledge that the PhD student has acquired during the implementation of this thesis, the PhD student will continue to research and cooperate with colleagues who are researching in the field of network coding to be able to bring many new methods, network cipher algorithms are more effective and put into practice.

Confirmation of representative Scientific supervisor	**PhD. Candidate**
PhD. Ngo Duc Thien	**Pham Long Au**