INFORMATION OF DOCTORAL DISSERTATION

Dissertation title: Some advanced encryption schemes with flexible decryption right

Major: Informatinon system

Code:9.48.01.04

Ph.D candidate: Trịnh Văn Anh

Scientific supervisors:

1.Professor Dr Nguyen Binh

2. Dr Ho Van Huong.

Training institution: Posts and Telecommunications Institute of Technology

I. NEW CONTRIBUTIONS OF THE THESIS

Thesis has three main contributions:

1. Propose a new efficient multi-channel broadcast encryption (MCBE) scheme in the public key setting. Note that all existing MCBE schemes [47,15] are in the secret key setting, that means only the authority can encrypt messages.

2. Propose a new ciphertext policy attribute-based encryption (CP-ABE) scheme with constant-size ciphertext. Compare with all existing CP-ABE schemes which have the same constant-size ciphertext property, my proposed CP-ABE scheme has shorter secret key size but weaker security level.

3. Based on the existing CP-ABE scheme [42], the third contribution of the thesis is to propose a new CP-ABE scheme which supports the searchable encryption property. My proposed CP-ABE scheme is the first scheme which doesn't need the trusted authority (third party) to generate the trapdoor.

II. FUTURE RESEARCH

1. Propose a new MCBE scheme in public key-setting with constant-size ciphertext and shorter secret key size;

2. Propose a new decentralized MCBE scheme, note that currently there still doesn't exist any decentralized MCBE scheme;

3. Propose a new CP-ABE scheme with constant size of both ciphertext and secret key. Note that there already exists broadcast encryption scheme with constant size of both ciphertext and secret key, therefore it is possible to design a such CP-ABE scheme.

SUPERVISOR	PhD STUDENT
Professor Dr Nguyen Binh; Dr. Ho Van Huong	Trinh Van Anh

PROMOTION OF THE THESIS

Ph.D candidate: Trịnh Văn Anh

Dissertation title: Some advanced encryption schemes with flexible decryption right

Major: Informatinon system

Code: 9.48.01.04

Training institution: Posts and Telecommunications Institute of Technology

I. Goals of the thesis

Thesis concentrates on researching three types of schemes, Broadcast encryption (BE) scheme, Multi-channel broadcast encryption (MCBE) scheme and Attribute-based encryption (ABE) scheme, to achieve the following goals:

1. To understand the state of the arts of three types of schemes: BE scheme, MCBE scheme and ABE scheme;
2. Propose a new MCBE scheme which can overcome the weaknesses of existing MCBE schemes such as slow decrytion and is in secret key setting;
3. Propose a new ABE scheme which has interesting properties such as constant-size ciphertext, supporting searchable encryption, acceptable secret key size and acceptable decryption time.

II. Researching methods

1. Understand techniques of constructing all existing efficient BE, MCBE schemes;
2. To research how to construct a new MCBE scheme based on existing efficient BE schemes, particularly based on the Delerablee scheme [25] and some improvements of [55, 56];
3. Understand techniques of constructing all existing efficient attribute-based encryption (ABE) schemes;
4. To research how to construct a new ABE scheme from techniques of constructing existing efficient BE and MCBE schemes, particularly focus on constructing ABE scheme with constant-size ciphertext and supporting searchable encryption;
5. Research the security level of some existing ABE schemes.

III. Main contributions of the thesis

Main contributions of the thesis:

1. Propose a new efficient multi-channel broadcast encryption (MCBE) scheme in the public key setting. Note that all existing MCBE schemes [47,15] are in the secret key setting, that means only the authority can encrypt messages.
2. Propose a new ciphertext policy attribute-based encryption (CP-ABE) scheme with constant-size ciphertext. Compare with all existing CP-ABE schemes which have the same constant-size ciphertext property, my proposed CP-ABE scheme has shorter secret key size but weaker security level.
3. Based on the existing CP-ABE scheme [42], the third contribution of the thesis is to propose a new CP-ABE scheme which supports the searchable encryption property. My proposed CP-ABE scheme is the first scheme which doesn’t need the trusted authority (third party) to generate the trapdoor.

Conclusion:

Advanced encryption schemes, such as BE, MCBE and ABE schemes, have found many practical applications, particularly in pay-TV application, social network application (facebooks, twitter,...), cloud storage application, … However, currently there are still many unsolved problems of these schemes related to the efficiency and security. This thesis contributes a step forward to resolve the aforementioned problems of these schemes.

SUPERVISOR	PhD STUDENT
Professor Dr Nguyen Binh; **Dr**. Ho Van Huong	Trinh Van Anh