INFORMATION OF DOCTORAL DISSERTATION

Dissertation title: ***"Research and development some blind digital signature schemes and blind collective digital signature schemes based on digital signature standards"***

Major: Computer Engineering

Code: 9.48.01.06

Ph.D candidate: Nguyen Tan Duc

Scientific supervisors:

1. Assoc.Prof.Dr. Nguyen Hieu Minh.
2. Dr. Ngo Duc Thien.

Training institution: Posts and Telecommunications Institute of Technology

THE NEW SCIENTIFIC FINDINGS

1. Propose new blind digital signature protocol based on the difficulty of the discrete logarithm problem modulo a composite number $n = p*q$. New protocol use of the two difficult problem provides increased security of the signature protocol due to reducing the probability of the potential breaking the protocols, which is connected with potential appearance of the breakthrough solutions of the following two computationally difficult problems: (1) factoring composite number n containing two unknown prime divisors p, q và (2) finding discrete logarithm modulo primes p, q. The designed protocols are based on using finite groups possessing two-dimensional cyclicity. When selecting parameters providing 80-bit security, the signature size in the proposed blind protocols is equal to 240 bits.

2) Propose two blind multisignature schemes (BMSs) based on the GOST R34-10.94 standard and the Schnorr digital signature scheme and two BMSs based on the GOST R34-10.2012 digital signature standard and the EC-Schnorr digital signature scheme. Proposed BMSs are based on digital signature standards and digital signature schemes that have been proven to ensure security. Then expanding the functionality to construct the BMSs. This helps new BMSs inherit some advantages of the security of the signature schemes that had been proven in practice and they have better computational performance than previously proposed schemes.

3) Propose a new signature scheme from two difficult problems IFP and DLP. Then expanding to propose a single blind signature scheme and a blind multi-signature scheme, which requires the simultaneous breaking of two independent difficult problems, these are based on the RSA signature scheme and Schnorr signature scheme. It has been proved to be correct, blind, unforged, random. My proposed blind multi-signature signature scheme are safe and present high performance, therefore, they can be applied in practice.

APPLICATIONS, PERSPECTIVES AND FUTURE RESEARCH:

- Our proposed blind signature schemes and blind multi-signature schemes are safe and present high performance; therefore, they can be applied in practice such as the proposed schemes can be applied in election systems and digital cash schemes.

- However, it is necessary to continue researching and proposing the types of blind digital signature scheme based on two difficult problems for applications requiring high security in systems with limited resources such as industrial equipment 4.0, IoT, etc.

SUPERVISOR	PhD STUDENT
Assoc. Prof Dr. Nguyen Hieu Minh; Dr. Ngo Duc Thien	Nguyen Tan Đuc