SUMARY OF THE THESIS

I. General Information

Thesis Title:

RESEARCH AND CONSTRUCTION
REPRESENTATIVE DIGITAL SIGNATURE SCHEMES

Specialization: **COMPUTER SCIENCE**

Code: **948 01 01**

Full Name of PhD Student: **NGUYEN KIM TUAN**

Science Instructor:

1. PhD. **HO NGOC DUY**
2. Assoc Prof. PhD **DOAN VAN BAN**

Training Institution: **DUY TAN UNIVERSITY**

II. The main results of the thesis

1. A new type of highly practical collective digital signature scheme has been proposed, that is, a representative collective digital signature. There are two types of representative collective signature schemes: i) Collective digital signatures for signing groups and ii) Collective digital signatures for signing groups and individual signings.

2. Four representative collective digital signature schemes have been built based on discrete logarithmic problems: On a finite prime field (2 schemes); On Elliptic curve using standard ECDSA (2 schemes).

3. Four representative collective digital signature schemes have been built based on a new difficult problem, the problem of finding the modulo roots of large prime numbers, with prime modulos with different special structures: $p = Nt_0t_1t_2 + 1$ (2 schemes) and $p = Nk^2 + 1$ (2 schemes).

4. Proposed and built four collective digital signature schemes representing 2 components based on discrete logarithmic problems: On a finite prime field (2 schemes); On Elliptic curve using the standard GOST R34.10-2012 (2 diagrams).

5. Two representative collective digital signature schemes have been proposed based on two difficult problems at the same time: The problem of analyzing large integers into prime factors and the problem of discrete logarithms on prime finite fields, using Schnorr's signature standard.

III. The scientific contributions of the thesis

The scientific contributions of the thesis include:

a. Detecting and schematizing two authentication requests based on digital signatures is quite common in today's practice. These are: i) Authentication is performed for different groups of members, each group consists of many members, in

which one person acts as the group leader, and ii) Authentication is performed for many groups of members and many members. different single tablets.

From there, a new type of collective digital signature - "representative collective digital signature" - is proposed with high practicality and urgency. There are two types of representative collective digital signature scheme: i) Collective digital signature scheme for signing groups and ii) Collective digital signature scheme for signing groups and individual signings. These schemes are formed based on the combination of advantages of group digital signature scheme and collective digital signature scheme, so its advantages and applicability are quite high.

b. The research results show that it is possible to: i) Use one difficult problem or use two difficult problems simultaneously, such as IFP, DLP, ECDLP, PFRM (A New Difficult Problem), etc. and ii) Based on popular digital signature standards and standard digital signature schemes, such as: Schnorr, DSA, ECDSA, GOST R34.10-2001, etc. to build representative collective numerical schemes proposed in this thesis.

This also proves that the usability, security and feasibility of the digital signature schemes proposed here are recognisable and reliable.

c. The operating principle of the proposed digital signature schemes proves that these schemes can be deployed on existing PKI infrastructures. Users still use the private key and public key pair to participate in the collective digital signature-based authentication system but still ensure the secrecy and privacy of the asymmetric key pair they own.

Thus, the research results of the thesis have contributed to the community two new types of collective digital signature schemes that are practical, relevant and highly applicable. The thesis has also published specific digital signature schemes of the two proposed schemes. The mathematical basis, correctness, security and computational performance of these schemes have also been shown.

IV. Practical applicability

The operating principle of the proposed digital signature schemes proves that these schemes can be deployed on existing PKI infrastructures. Users still use the private key and public key pairs to participate in the collective digital signature-based authentication system but still ensure the secrecy and privacy of the asymmetric key pair they own.

PhD student believes that the results published in this thesis can be fully applied in practice, meeting the authentication requirements for a collective of many functional levels and information exchange applications in today's cyberspace.

V. Further research directions

In the future, the PhD student will continue to research and develop the thesis in the following specific directions:

- Research to propose a new type of difficult problem that can be used to build a representative collective digital signature scheme and some other types of digital

signature schemes such as group digital signatures, collective digital signatures, collective digital signatures, etc.

- Research to build authentication applications based on representative collective digital signature scheme that can support collective, certificate requirements, of many problems with different authentication requirements in practice.
- Deploy authentication and authentication applications based on representative collective signatures on existing PKI infrastructure.

Through the research on representative collective digital signatures, with the results achieved up to now, the researcher has sufficient grounds to believe that further research directions will also yield positive results.

Da Nang, November 25, 2022

Science Instructors *(surrogate)*	**PhD Student**
PhD. HO NGOC DUY	**NGUYEN KIM TUAN**

THE PUBLICATIONS OF THE AUTHOR

[CT1] **Nguyen Kim Tuan**, Ho Ngoc Duy, "*Xây dựng sơ đồ chữ ký tập thể mù trên cơ sở hệ mật Schnorr",* Journal of Science & Technology of Duy Tan University, 2015.

[CT2] **N. K. Tuan**, V. L. Van, N. A. Moldovyan and H. N. Duy, A. A. Moldovyan, "*Collective signature protocols for signing groups",* Information Systems Design and Intelligent Applications. Advances in Intelligent Systems and Computing (Scopus), INDIA, pp.78-87, 2017.

[CT3] **N. K. Tuan**, N. A Moldovyan, H. N Duy, T. T. V. Lam, V. L. Van*, "New protocols of collective digital signature based on Elliptic curve",* Hội thảo quốc gia: Một số vấn đề chọn lọc của Công nghệ thông tin và truyền thông - Chủ đề: An ninh không gian mạng, Quy Nhơn, pp.57-67, 2018.

[CT4] **Tuan Nguyen Kim**, Duy Ho Ngoc, Nikolay A. Moldovyan, *"Constructing the 2-element AGDS protocol based on the discrete logarithm problem",* International Journal of Network Security & Its Applications, vol.13, no.4, pp.13-22, 2021.

[CT5] **Tuan Nguyen Kim**, Duy Ho Ngoc, Nikolay A. Moldovyan, *"Collective signature protocols for signing groups based on problem of finding roots modulo large prime number",* International Journal of Network Security & Its Applications, vol.13, no.4, pp.59-69, 2021.

[CT6] **Tuan Nguyen Kim**, Nguyen Tran Truong Thien, Duy Ho Ngoc, Nikolay A. Moldovyan. *"Constructing New Collective Signature Schemes Based on Two Hard Problems Factoring and Discrete Logarithm"*, International Journal of Computer Networks & Communications, vol.14, no.2, pp.115-133, 2022 (Scopus).

[CT7] **Tuan Nguyen Kim**, Duy Ho Ngoc, Nikolay A. Moldovyan, "*New Collective Signatures Based on The Elliptic Curve Discrete Logarithm Problem*", Computers, Materials & Continua, vol.73, no.1, pp.595-610, 2021 (SCI/Q2).

[CT8] **Tuan Nguyen Kim**, Duy Ho Ngoc, Nikolay A. Moldovyan, "*New Representative Collective Signatures Based on The Discrete Logarithm Problem*", Computers, Materials & Continua, vol.73, no.1, pp.783-799, 2021 (SCI/Q2).

[CT9] **Tuan Nguyen Kim**, Duy Ho Ngoc, Nikolay A. Moldovyan, "*Constructing Collective Signature Schemes Using Problem of Finding Roots Modulo",* Computers, Materials & Continua, vol.72, no.1, pp.1105-1122, 02/2022 (SCI/Q2).

[CT10] **Tuan Nguyen Kim**, Duy Ho Ngoc, Nikolay A. Moldovyan, *"Constructing New Representative Collective Signature Using The GOST R34.10-2012 Digital Signature Standard"***,** Journal of Communication, vol.17, no.6, pp.478-485, 2022 (SCI/Q3).

[CT11] **Tuan Nguyen Kim**, Duy Ho Ngoc, Nin Ho Le Viet, Nikolay A. Moldovyan, *"The New Collective Signature Schemes Based on Two Hard Problems Using Schnorr's Signature Standard"*, Journal of Advances in Information Technology, vol.14, no.1,pp.77-84, 2022 (SCI/Q3).

[CT12] **Tuan Nguyen Kim**, Duy Ho Ngoc, Nikolay A. Moldovyan, *"Constructing Representative Collective Signature Protocols Using The GOST R34.10-1994 Standard",* Computers, Materials & Continua, vol.74, no.6, pp.1475-1491, 2022 (SCI/Q2).

PhD Student

TUAN NGUYEN KIM