MINISTRY OF EDUCATION AND TRAINING
DUY TAN UNIVERSITY

NGUYEN KIM TUAN

RESEARCH AND CONSTRUCTION REPRESENTATIVE DIGITAL SIGNATURE SCHEMES

SPECIALIZATION: COMPUTER SCIENCE

CODE: 948 01 01

SUMARY OF THE THESIS

SCIENCE INSTRUCTOR:

1. PhD. Ho Ngoc Duy

2. Assoc Prof. PhD Doan Van Ban

DA NANG – 2023

INTRODUCTION

1. Reason for choosing the topic

Currently, there are many types of digital signature schemes that have been researched and published, such as single digital signature scheme, multi-digital signature scheme, blind digital signature scheme, group digital signature scheme, alphanumeric scheme, etc. collective signing, blind collective signature scheme, etc. Authentication systems based on group digital signatures, collective digital signatures, etc. well support applications where i) simultaneous authentication of both the identity of the creator of the information and the identity of the organization of which he is a member, and/or ii) co-authentication the identity of all entities in an organization that generate information.

Up to now, many algorithms, protocols, schemes (Schemes) related to group digital signatures and collective digital signatures have been researched and published. unique number, but it represents an entire group or a collective of participants creating that signature.

Recently, in practice, a new type of (handwritten) signature-based authentication request has appeared in practice, that is, attesting to a whole group of signers. Each member of this collective is identified by their own signature. This identification includes identification of a member: i) to which group of members; ii) Being a single member of the collective; iii) Be the leader of a group of members; etc., significantly as the number of members of the collective increases.

According to the PhD student, if we combine the operating principle of the group signature scheme and the collective signature

scheme, we can build a multi-signer scheme that meets the requirements of collective authentication. of the multi-member authentication problem.

Specifically, first, use the group signature scheme to generate group signatures for groups of members in the collective, and then use the collective signature scheme to generate the collective signature from the signatures of the collectives. group members and signatures of individual individuals. This new scheme supports the creation of a single signature, but with the participation of all members of the signing collective, it represents this signing collective. This can be seen as an extension of the collective signature scheme. The new multi-signer signature can be named "Representative Collective Signature".

With the desire to find out the practical applicability of the published collective digital signature schemes and the published collective digital signature schemes, from that basis, we propose representative collective signature schemes that meet the requirements. For authentication requirements for many current real-world problems, the PhD student chose the topic **"Researching and Building the representative collective digital signature schemes"** to research and present presented in his thesis.

2. Research Objectives and Tasks

The research objectives of the thesis are:

- Propose representative collective digital signature schemes based on a difficult problem and based on two difficult problems. Prove the correctness of the schema; Analyze the level of security (resistance to "attack") and evaluate the performance of the proposed schemes.

- Proposed types of representative collective signature scheme consisting of only 2 components but still meeting the necessary requirements of a collective digital signature.

The research tasks of the thesis are:

- Learn about difficult problems used to build digital signature schemas: Factor analysis problem; Discrete logarithmic problem on prime finite field Z_p; Discrete logarithms on Elliptic curves; The problem of finding the modulo root.
- Learn about international digital signature standards (US DSS, Russian GOST R34.10, etc.) and security standards for some digital signature schemes. Analysis of the operation and security level of a number of digital signature schemes have been published in recent years.
- Learn about single digital signature schemes (RSA, ElGamal, Rabin), group digital signatures, collective digital signatures built on difficult problems: Factor analysis, Discrete Logrit, Find modulo roots. This is the basis for the thesis to propose a representative collective digital signature scheme based on a difficult problem.
- Learn about group digital signature schemes, collective digital signatures built on two difficult problems at the same time.
- From this understanding, the thesis proposes a collective digital signature scheme for signing groups based on two difficult problems simultaneously: Factor Analysis Problem - Discrete Logarithmic Problem.
- Learn the applicability of representative collective signatures in practice.

3. Research content

Research overview:

Research by PhD students:

- Research on advantages and disadvantages of published digital signature schemes. Research on the applicability of group digital signature schemes and collective digital signature schemes. From there, find a way to build a digital signature scheme for the signing collective authentication problem mentioned above (Section 1).
- Research on building representative collective signature schemes based on a difficult problem or on two difficult problems simultaneously: Factoring; Discrete logarithms over prime finite field GP(p) and on Elliptic curves; Find the root modulo of the large prime; etc.
- Prove mathematically the security, complexity and computational performance of the proposed collective digital signature scheme.
- Study the applicability of the proposed representative collective digital signature schemes to electronic transaction and electronic document exchange applications where it requires a level of security, integrity and verifiability. real high.

4. Scientific and Practical significance of the topic

Scientific significance of the topic:

- The topic shows that, based on difficult problems such as: Discrete logarithms on finite prime fields and on Elliptic curves; Find the root modulo of the large prime; Parsing integers into prime factors; etc we can build group signature schemes, representative collective signature schemes according to different digital signature standards, such as: DSS, GOST, etc., ensuring high security.

- The topic also shows that the security level of a collective digital signature scheme depends not only on the difficulty of the applied problem but also on the operation of the protocols used in the application. diagram.

Practical significance of the topic:

- The representative collective digital signature schemes proposed by the topic can completely meet the requirements of authentication, multi-level, and increasingly high level of collective identity of many transactional and information exchange applications. movement in cyberspace.
- The signature schemes proposed by the topic can be deployed based on the existing PKI infrastructure in current digital signature and authentication systems.

5. The layout of the thesis

This thesis consists of 4 chapters:

- **Chapter One: Overview of digital signatures and collective digital signatures**

The basic knowledge related to digital signatures and digital signature schemes are explored and selected to be presented in this chapter. Specifically: Digital signature schema standards; Mathematical basis and difficult problems are often used to build digital signatures; Equivalence and difference between group digital signature and collective signature with representative collective signature.

- **Chapter Two: Building the representative collective digital signature scheme based on discrete logarithmic problems**

This chapter presents representative collective digital signature

schemes, proposed by me, built on: i) Discrete logarithmic problem on prime finite field; ii) Discrete logarithmic problem on Elliptic curve.

- **Chapter Three: Building a representative collective digital signature scheme based on the problem of finding the modulo prime root**

The main content of Chapter Three is representative collective signature schemes based on the problem of finding the roots modulo large primes, where modulo p is a large prime with the structure: i) $p = Nt_0t_1t_2 + 1$ (two-component private key); and $p = Nk^2 + 1$ (one-component private key).

- **Chapter Four: Improved size and security of representative collective signatures**

The representative collective signatures built in chapters one and three have two problems to consider: The size of the signature is large and the level of security is based only on a difficult problem. Limitations and solutions to this problem are pointed out at the beginning of chapter four.

CHAPTER ONE:
OVERVIEW OF DIGITAL SIGNATURES AND COLLECTIVE DIGITAL SIGNATURES

This chapter presents the most basic issues related to digital signatures and digital signature schemes. Collective digital signatures and group digital signatures will be described in detail here. The main content of chapter 1 is the presentation of an actual authentication requirement, which requires a new type of multi-signature to be met, that is, a representative collective signature. The practicality and urgency of this new type of collective signature is presented quite clearly in Section 1.5. The research related to the thesis topic and the research direction of the PhD student are also mentioned in chapter 1. The problem presented at the end of the chapter is the mathematical basis used to build signature schemes. in general and the representative collective letter scheme in particular.

1.1. Representative collective signature

In the section Reasons for choosing the topic, the thesis has pointed out a fairly practical authentication requirement today, which is signature-based (handwritten) authentication for a collective of signers, which includes many groups of members. , each member group has a group leader, and a number of individual members.

Consider the organizational structure of a company in practice, for example, Company A (see Figure 1.4): The Board of Directors of Company A consists of 1 director (Director) and 2 deputy directors (PhD1, Deputy Director2); There are 4 functional units in Company A: A1, A2, A3, A4. Each unit has a unit leader: TrA1,

TrA2, TrA3, TrA4, and several employees of the unit. Employees A1-1 and A1-5 belong to unit A1, employee A2-5 belong to unit A2… When the request for authentication for all personnel in this company is set, it can be considered as a collective. multi-level sign: Director, Deputy Director - Head of unit and staff in the unit. This collective consists of 4 groups of members: A1, A2, A3, A4. The respective team leaders are: TrA1, TrA2, TrA3, TrA4. The individual members are Deputy Director 1 and Deputy Director 2 (here, the role of the Director is not considered). The problem here is: i) How to authenticate all members of Company A with only one signature or ii) How to correctly identify a certain employee of Company A? Company A belongs to any unit or is a single member, whether they are the head of the unit or not, a certain member, a certain unit belongs to the company or not.

If this authentication request is done in the traditional way, that is, every member of this signing group, from the signing group member to the signing team leader and even individual signers, signs the document to be signed. , then the signature verifier's job will be very complicated and time-consuming, because it has to check the validity of each signature of different signer objects, group members, group members, members, etc. single pellet.

The above limitation can be overcome by creating only one signature, representing the whole group of signers, all authentication work for this collective is done only on that one common signature. The following are a few approaches considered to generate a common signature representing a signing collective:

i) Each member of a signing group, generates a signature, and then “joins” it into a signature of the signing group. Then "join" the signatures of the signing groups and the signatures of the individual

members into a common signature for the signing collective. Then the signature verifier's job will be simpler because it only performs on a single signature. But this is not possible in practice, because how to "join" and what will happen when the number of members of the signing collective is large.

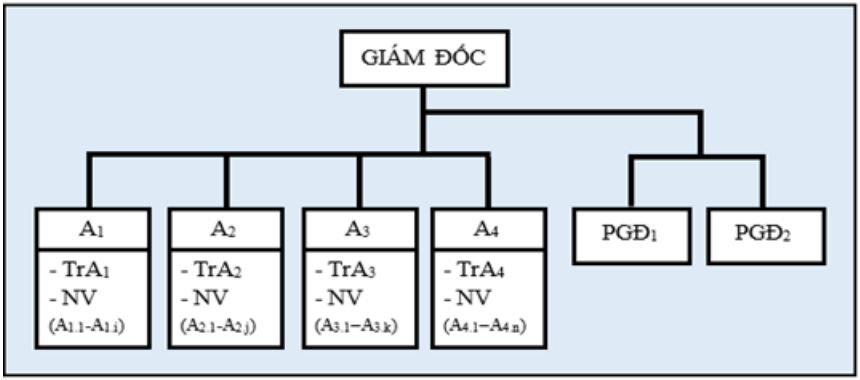

Figure 1.4. Organization chart of Company A (in Vietnamese)

ii) Use only the signature of the team leader as the representative signature of their signing group. The next step is done as above. This way seems feasible in practice because often the number of signing groups and individual signers in a signing collective is not much. But the "trace" of the members of the signing groups does not appear in the final signature of the collective. Thus, the "rejection" ability of this signature-based authentication system cannot be guaranteed.

iii) All members of the collective contribute the relevant information necessary to create a unique signature common to the collective. This signature will be the collective representative in future authentication. Since the collective signature of the collective contains the information of all the members involved in the creation of the signature, the problem of "anti-repudiation", the problem of

determining the origin of the member, which group of members, of This authentication system can be guaranteed. This approach can solve the problem of time and complexity of the signature verifier but is completely impractical in practice.

Thus, the above approaches are difficult to implement in practice, on the handwritten signature system. This has opened up a new research direction that is, building a digital signature scheme that meets the requirements of the authentication problem for a multi-level functional signing collective as stated. This is also the research task of the PhD student in this thesis.

Through initial research, NCS found that, although both the group signature scheme and the collective signature scheme support the creation of a common signature, representing a set of many signers, containing all the necessary information. necessary to trace, identify the member's origin, and prevent "disclaimer" in the future. But both of these schema types can hardly meet the authentication model for members of a multi-level signatories set forth in this thesis. According to NCS, if the advantages of the group signature scheme and the collective signature scheme can be combined, it is possible to build an extended form of collective signature scheme that can meet the requirements of the authentication problem. Multi-functional collective practice has been set up (as analyzed in the section Reasons for choosing the topic). The thesis temporarily names this new type of collective signature scheme as "Representative collective signature scheme".

According to this approach, the above collective authentication problem for Company A can be done through a unique (single) digital signature, but this signature is formed as follows: i) First, each Unit leaders are responsible for generating group signatures for

their units. Membership verification and storage of identifying information of the group members who participated in the creation of this signature are performed by the group leader. In this way, each individual member is also considered a group leader, but their group has no members; ii) Then, from the signatures of groups and individual members, a group leader or any single member or director of the company performs the task of creating collective signatures, representing the collective. can sign. Checking the membership of the participants generating the collective signature is also done here. The necessary relevant information is also stored in the signature of the signing collective; Thus, the collective authentication of Company A only needs to be done on the collective signature of the company. This signature has all the necessary information for tracking, identifying group members/collective members and resisting "disclaimer" when needed.

1.2. Research direction of the PhD student

From the above analysis, the PhD student focuses on the following main contents:

- Build a representative collective signature schema framework, so that it meets both the collective authentication problem and the normative requirements of a multi-signature scheme.
- Use digital signature standards and/or standard digital signature schema formats to build representative collective signature schemes.
- Build a representative collective signature scheme based on a difficult problem or based on two difficult problems. Also looking to change the structure of some input parameters to increase the

difficulty of some schemas.

In the thesis, the PhD student proposes and builds two types of representative collective digital signature schemes: i) Collective signature scheme for signing groups (also known as collective signature scheme shared by multiple signing groups): Provides the ability to authenticate a signing collective which includes many different signing groups and ii) Collective signature scheme for signing groups and individual signings (also known as the signature scheme). collective digital signature scheme shared by many signing groups and many individual signers): Provides the ability to authenticate a signing collective that includes many signing groups and many different individual signers.

Summary of Chapter One:

This chapter of the thesis has presented the following main contents: i) Definitions, concepts, terms, etc. related to digital signatures and digital signature schemes, in particular, group digital signatures and collective digital signatures; ii) Describe a number of standard digital signature schemes and a number of digital signature schemes belonging to American and Russian standards; iii) Presenting the objectives and research direction of the topic: Collective authentication requirements and representative collective signature (main part of chapter 1); iv) The last part of Chapter 1 presents the basic mathematical problems and related difficult problems that the researcher uses to build the proposed schemas in the following chapters of the thesis.

CHAPTER TWO:

BUILDING THE REPRESENTATIVE COLLECTIVE DIGITAL SIGNATURE SCHEME BASED ON DISCRETE LOGARITHMIC PROBLEMS

In this chapter, the PhD student will perform two main tasks simultaneously. First, two new types of collective signature schemes are proposed that allow the creation of a unique representative collective signature, representing a multi-level functional collection, presented in Chapter 1. second, use discrete logarithmic problems to build: i) Collective signature scheme for many signing groups and ii) Collective signature scheme for many signing groups and many individual signers.

2.1. Building representative collective signature scheme based on discrete logarithm problem on prime finite field

Collective signature scheme for multiple signing groups

The collective signature scheme for the following signing groups (Symbol: RCS.01-2.1) is built from the two basic schemes presented in 2.1.1 (CDS-2.1) and 2.1.2 (GDS-2.1). Suppose there is a signing collective consisting of g signing groups, want to create a representative collective signature on document M. Let $\boldsymbol{X_j}$ be the private key of GM of the j[th] signing group $\boldsymbol{j}$ ($\boldsymbol{j = 1, 2, \ldots, g}$) and public corresponding key is $\boldsymbol{Y_j = \alpha^{X_j} \bmod p}$. $\boldsymbol{Y_j}$ is also the public key of the j[th] signing group of this signing group.

Assume that the jth signing group consists of m signing members (denoted by m_j), who are designated to participate in the formation of the group signature of the jth signing group. Each ith member (with $i = 1, 2, \ldots, m_j$) in the jth signing group has a private key of x_{ji} ($|x| \geq 256\ bit$) and a corresponding public key of $y_{ji} = \alpha^{x_{ji}} \bmod p$.

The parameters used in schema protocols include: i) A

sufficiently large prime p (|p|>2048 bits), a prime q (|q|≥256 bits), such that q|p – 1; ii) Some α has degree q modulo p.

Collective signature scheme for multiple signing groups and many individual signers (Symbol: RCS.02-2.1)

a) Collective signature scheme for multiple signing groups according to ECDSA standard (Symbol: RCS.01-2.2)

Suppose there is a signing collective consisting of g signing groups, want to create a representative collective signature on document M. Let z_j be the private key of GM of the j[th] signing group ($j = 1, 2, \ldots, g$) and public The corresponding key is $L_j = z_j G$. L_j is also the public key of the j[th] signing group of this signing group.

Assume that the jth signing group consists of m signing members (denoted by m_j), who are designated to participate in the formation of the group signature of the jth signing group. Each i[th] member (with $i = 1, 2, \ldots, m_j$), in the jth signing group, has a private key of k_{ji} and their corresponding public key is P_{ji}: $P_{ji} = k_{ji} G$.

b) Collective signature scheme for many signing groups and many individual signers according to ECDSA standard (Symbol: RCS.02-2.2)

Suppose there is a signing collective consisting of g signing groups and m individual signers, and want to create a representative collective signature on document M. Suppose the jth signing group includes m signing members (denoted by m_j), this are designated persons participating in the formation of the group signature of the jth signing group $(j = 1, 2, \ldots, g)$and each individual signer is treated as a signing group with only one member. best.

Each i-th signer in the signing group owns a private key of k_{ji} and their respective public key is $P_{ji} = k_{ji} G$, with $i = 1, \ldots, m$. GM of the jth signing group has its private key and public key z_j and L_j ($L_j = z_j G$). L_j is also the public key of the signing group j.

Public key and private key of each individual signer is $L_j = k_j G$ and k_j $(j = g + 1, g + 2, \ldots, g + m)$. In this scheme, the "group signature" corresponding to each individual signer is (O, e, s), where O is the infinity point of the elliptic curve.

2.2. Evaluate the security and computing performance of the representative collective signature scheme that has been built

2.2.1. Resistance to attack from within

For collective signatures, those involved in signature formation are more likely to attack the signature scheme they generate than outsiders.

Therefore, in the following, only two types of attacks based on the common collective signature scheme are presented, which originate from the members of the signing collective themselves.

- First type of attack (Forgery of signature of signer m)
- Second type of attack (Find the private key of signer m)

2.2.2. Evaluation of computational performance of representative collective signature scheme

The thesis evaluates the computational performance of representative collective signature schemes through calculating the time cost that the schema needs for the signature generation process (Signature generation procedure) and needed for the verification process. signature validity (Signature check procedure).

The following are some of the conventions used in the time-costing formulas for the calculations in the two aforementioned procedures: T_h: The computational cost of the hash operation on Z_p; T_s: The computational cost of scalar multiplication on Z_p; T_{inv}: Computational cost of the above inverse Z_p; T_e: Calculation cost of the upper exponent Z_p; T_m: Computational cost of the above multiplication Z_p; T_+: Calculation cost of adding the above points Z_p; Conversion: $T_h \approx T_m, T_s \approx 29T_m, T_{inv} \approx 240T_m, T_e \approx 240T_m$,

$T_+ \approx 0.12T_m$ [15].

The calculation results are given in the following tables:

Table 2.1: Time cost of RCS schemes based on DLP problem

Scheme	Time cost	
	Genarate signature	**Check signature**
RCS.01-2.1	$U = \sum_{j=1}^{g}(243m_j + 1)\,T_m$ $E = [\sum_{j=1}^{g}(241m_j + 240) + 1]T_m$ $S = \sum_{j=1}^{g}(484m_j + 1)\,T_m$ $Sum = [\sum_{j=1}^{g}(968m_j + 242) + 1]T_m$	$(483 + g)T_m$
RCS.02-2.1	$U = \sum_{j=1}^{g}(243m_j + 1)\,T_m$ $E = [\sum_{j=1}^{g}(241m_j + 240) + 240m + 1]T_m$ $S = [\sum_{j=1}^{g}(484m_j + 1) + 482m]T_m$ $Sum = [\sum_{j=1}^{g}(968m_j + 242) + 722m + 1]T_m$	$(483 + g + m)T_m$
RCS.01-2.2	$U = \sum_{j=1}^{g}(32m_j)\,T_m$ $e = [\sum_{j=1}^{g}(29m_j + 29) + 1]\,T_m$ $s = \sum_{j=1}^{g}(61m_j + 1)\,T_m$ $Sum = [\sum_{j=1}^{g}(122m_j + 30) + 1]\,T_m$	$(59 + 0.12g)T_m$
RCS.02-2.2	$U = \sum_{j=1}^{g}(32m_j)\,T_m$ $e = \sum_{j=1}^{g}[(29m_j + 29) + 29m + 1]\,T_m$ $s = [\sum_{j=1}^{g}(61m_j + 1) + 61m]T_m$ $Sum = [\sum_{j=1}^{g}(122m_j + 30) + 90m + 1]\,T_m$	$(59 + 0.12g + 0.12m)T_m$

The data in this table shows that the time cost for signature

generation and signature checking of representative collective signature scheme based on discrete logarithm problem on GF(p) is much higher than signatures and problems of the same type on Elliptic curves. This once again confirms the advantage of Elliptic curve cryptography over other cryptosystems commonly used to build digital signatures and digital signature schemes.

Summary of Chapter Two:

This chapter presents representative collective signature schemes built based on discrete logarithm problem on finite prime field and discrete logarithm problem on Elliptic curve using ECDSA standard. For each problem, two types of representative collective signature schemes are constructed, namely: Collective signature scheme for many signing groups and collective signature scheme for many signing groups and many individual signers. core.

Chapter 2 also details set and group signature schemes. These are the basic schemas that NCS uses to build representative collective signature schemes. The attack resistance, security advantages and computational performance of the built signature schemes are also presented in this chapter.

The publications used in this chapter: [CT3], [CT5], [CT9], [CT14].

CHAPTER THREE:

BUILDING A REPRESENTATIVE COLLECTIVE DIGITAL SIGNATURE SCHEME BASED ON THE PROBLEM OF FINDING THE MODULO PRIME ROOT

In this chapter, in order to strengthen the feasibility of representative collective signature scheme, the PhD student uses the difficult problem of finding the modulo roots of large primes, which is a new type of difficult problem created by Nikolay A. Moldovyan proposed, to build the proposed collective signature scheme. The difficulty of this problem depends heavily on the structure of the prime modulo p, so chapter 3 will study and present the schemas related to the two structures of p: $p = Nk^2 + 1$ (i) and $p = Nt_0t_1t_2 + 1$ (ii). A two-component private key, a new form of key with many security advantages, is used when the schema is built with the structured p prime modulo (ii).

3.1. Building a representative collective digital signature scheme based on the problem of finding the modulo root of a structured large prime $p = Nk^2 + 1$

This section presents two types of representative collective signature schemes, and related basis schemes, based on the difficulty of the problem of finding the modulo roots of large primes, with primes of the structure. special architecture, proposed by Nikolay A. Moldovyan and Victor A. Shcherbacov in [70]. Specifically, $p = Nk^2 + 1$, where k is a large prime ($|k| \geq 160$ bit) and N is an even number such that the magnitude of p satisfies $|p| \geq 1024$ bit.

To generate a private signature based on this difficult problem, the signer must randomly choose a number x as the private key. The

public key y is calculated according to the following formula: $y = x^k \ mod \ p$. The digital signature on document M, which needs to be signed by the signer, is created in this case as a numeric value pair (E, S). The magnitude of S is equal to the magnitude of p, $|p| \geq 1024$ bits, the magnitude of E is equal to the magnitude of δ, $|\delta| \geq 160$ bit, where δ is a prespecified prime number.

3.2. Evaluation of the computational performance of the representative collective signature schemes that have been built

The thesis evaluates the computational performance of representative collective signature schemes through calculating the time cost that the schema needs for the signature generation process (Signature generation procedure) and needed for the verification process. signature validity (Signature check procedure).

Table 3.1: Time cost of RCS schemes based on FRM problem

Scheme	Time cost	
	Generate signture	Check signature
RCS.01-3.1	$U = \sum_{j=1}^{g}(243m_j + 1)\,T_m$ $e = [\sum_{j=1}^{g}(241m_j + 240) + 1]T_m$ $S = \sum_{j=1}^{g}(725m_j + 241)\,T_m$ $Sum = [\sum_{j=1}^{g}(1210m_j + 482) + 1]T_m$	$(481 + g)T_m$
RCS.02-3.1	$U = \sum_{j=1}^{g}(243m_j + 1)\,T_m$ $e = [\sum_{j=1}^{g}(241m_j + 240) + 241m + 1]T_m$ $S = [\sum_{j=1}^{g}(725m_j + 241) + 723m]T_m$ $Sum = [\sum_{j=1}^{g}(1210m_j + 482) + 965m + 1]T_m$	$(481 + g + m)T_m$

RCS.01-3.2	$U = \sum_{j=1}^{g}(243m_j + 1)\,T_m$ $e = [\sum_{j=1}^{g}(481m_j + 481) + 1]T_m$ $S_1 + S_2 = \sum_{j=1}^{g}(1209m_j + 484)\,T_m$ $Sum = [\sum_{j=1}^{g}(1934m_j + 966) + 1]T_m$	$(724 + g)T_m$
RCS.02-3.2	$U = \sum_{j=1}^{g}(243m_j + 1)\,T_m$ $e = [\sum_{j=1}^{g}(481m_j + 481) + 481m + 1]T_m$ $S_1 + S_2 = [\sum_{j=1}^{g}(1209m_j + 484) + 1206m]T_m$ $Sum = [\sum_{j=1}^{g}(1934m_j + 966) + 1687m + 1]T_m$	$(724 + g + m)T_m$

The data in this table show that the representative collective signature scheme built from modulo with structure $p = Nk2 + 1$ has much lower cost than the remaining p structure.

Summary of Chapter Three:

In this chapter, the thesis presents collective signature schemes built based on the problem of root modulo of large prime numbers, with two different structural forms of prime modulo p: i)) $p = Nt_0t_1t_2 + 1$ (with private key consisting of two components); and ii)) $p = Nk^2 + 1$ (with a private key of only one component). For each structure p, the thesis builds two types of schemes: i) Collective signature for many signing groups and ii) Collective signature for many signing groups and many individuals signing. The thesis has also built collective signature schemes and group signature schemes to serve as the basis for representative collective signature schemes.

The publications used in this chapter: [CT4], [CT7], [CT11].

CHAPTER FOUR:

IMPROVED SIZE AND SECURITY OF REPRESENTATIVE COLLECTIVE SIGNATURES

The schema that the PhD student has built still has two issues to consider for improvement: i) Reduce the number of signature components from three to two to reduce the signature size and ii) Increase security of the signature by using two difficult problems simultaneously, instead of using one difficult problem, to build the schema. These two issues will be considered and proposed solutions in chapter four. Thus, chapter four is considered as an extension and completion of chapters two and three.

4.1. Problems and Approaches

Many approaches have been proposed to improve the quality and practical implementation of digital signatures and digital signature schemes, such as increasing key length, reducing signature size, building new difficult problems – based on existing abstract algebraic structures, building signatures based on many difficult problems, using prime modulo with special structure, etc. In this Chapter 4, NCS proposes: i) The type of collective signature represents two components and ii) The type of representative collective signature is based on two difficult problems simultaneously to improve the size and improve the security level for these schemes.

4.2. Building a collective signature scheme representing two components based on DLP on a finite field

a) Collective digital signature scheme for multiple signing groups (Symbol: RCS.01-4.2)

This scheme generates a collective signature for g signing

groups, with the public key of each group manager (GM), and also the public key of each signing group: $Y_j = X_j^k \ mod\ p$; ($j = 1, 2, \dots, g$), and X_j is the private key of the j[th] GM. Assume the j[th] group has m_j signed individuals. M is the document to be signed on.

b) Collective digital signature scheme for many signing groups and many individual signers (Symbol: RCS.02-4.2)

Suppose there is a signing collective consisting of g signing groups and m individual signers, and want to create a representative collective signature on document M. Suppose the jth signing group includes m signing members (denoted by m_j), this are designated persons participating in the formation of the group signature of the jth signing group ($j = 1, 2, \dots, g$) and each individual signer is treated as a signing group with only one member.

4.3. Building a representative collective digital signature scheme based on two difficult problems

The two difficult problems chosen here are: Discrete logarithmic problem over prime finite field $GF(p)$ and Factoring Problem. This combination is formed on the basis of: i) The element modulo p is chosen with a special structure: $p = 2n + 1$, with $n = q'q$; q' and q is a prime number of at least 512 (q' *and* q *is chosen so that 3 is not a divisor of* $q' - 1$ *and* $q - 1$) the primes q' and q are kept secret; and ii) Personal signature scheme built according to Schnorr's signature scheme.

Collective signature scheme for multiple signing groups and many individual signers (Symbol: RCS.02-4.3)

On the basis of the group signature protocol described above and the collective signature scheme for signing groups, this section constructs the collective signature scheme, of a collective of many

signing groups and many individual signers. multiply, on document M.

The signing collective in this case consists of g group of signers and m of individual signers. The input parameter values and the group member's (GM) key values are selected/calculated as above. The private key and public key of the individual signer are: X_j and Y_j. $Y_j = \alpha^{X_j} \, mod \, p$; $(j = g + 1, g + 2, \dots, g + m)$.

4.4. Evaluate the security and computational performance of the built representative collective signature scheme

4.4.1. Security of the base signature scheme

The security of this new scheme depends on the difficulty of simultaneously solving two difficult problems: Discrete logarithmic problem on GF(p) and Prime factorization problem of a large integer. That is, to break this scheme the attacker must first solve the discrete logarithm problem, and then solve the factor analysis problem (see section 4.3.1).

4.4.2. Security of the group signature scheme

With the group signature scheme, there are two main types of attacks: Internal attacks (from members of the signing group themselves) and External attacks (from people who are not signing group members). Formally, the group signature scheme is more vulnerable to internal attacks than external attacks. Since, the external attacker only knows the system parameters, public keys and M documents, while the internal attacker, as a member of the signing group, has more relevant information. to the target of the attack.

The following section considers two common types of attacks on the group signature scheme, which come from the group leader,

so the probability of success is very high.

4.4.3. Security of the representative collective signature scheme

The representative collective digital signature scheme is built on the basis of the collective digital signature scheme and the group digital signature scheme, so it inherits all the security advantages from these two basic schemes.

4.4.4. Evaluation of the computational performance of representative collective signature schemes

The thesis evaluates the computational performance of representative collective signature schemes through calculating the time cost that the schema needs for the signature generation process (Signature generation procedure) and needed for the verification process. signature validity (Signature check procedure).

Table 4.1: Time cost of two-component RCS schemas

Scheme	Time cost	
	Generate signature	Check signature
RCS.01-4.2	$E = [\sum_{j=1}^{g}(244m_j + 1204) + 1]T_m$ $S = (724g)T_m$ $Sum = [\sum_{j=1}^{g}(244m_j + 1928) + 1]T_m$	$(723 + g)T_m$
RCS.02-4.2	$E = [\sum_{j=1}^{g}(244m_j + 1204) + 241m + 1]T_m$ $S = (724g + 724m)T_m$ $Sum = [\sum_{j=1}^{g}(244m_j + 1928) + 965m + 1]T_m$	$(723 + g + m)T_m$

Table 4.2: Time cost of RCS schemes on 2 difficult problems

Scheme	Time cost	
	Generate signature	**Check signature**
RCS.01-4.4	$U = \sum_{j=1}^{g}(243m_j + 1)\,T_m$ $e = [\sum_{j=1}^{g}(241m_j + 240) + 1]T_m$ $S = [\sum_{j=1}^{g}(1254m_j + 1781) + 290]T_m$ $Sum = [\sum_{j=1}^{g}(1738m_j + 2022) + 291]T_m$	$(723 + g)T_m$
RCS.02-4.4	$U = \sum_{j=1}^{g}(243m_j + 1)\,T_m$ $e = [\sum_{j=1}^{g}(241m_j + 240) + 241m + 1]T_m$ $S = [\sum_{j=1}^{g}(1254m_j + 1781) + 1250m + 290]T_m$ $Sum = [\sum_{j=1}^{g}(1738m_j + 2022) + 1491m + 292]T_m$	$(723 + g + m)T_m$

** The notation used in this table has been specified in Chapter 2.*

The data from this table shows that the time cost of both signature generation and signature verification is significantly reduced, compared to three-component signatures of the same type. This table also shows that, with the representative collective signature scheme on two difficult problems, we have to accept the high time cost of signature generation and signature checking in exchange for a high level of security. from both difficult problems, discrete logarithm and factoring.

Summary of Chapter Four:

This chapter has proposed and built two collective signature schemes representing two components (E,S) and two

representative collective signature schemes based on two difficult problems, discrete logarithms and root extraction, with modulo p has a special structure $p = 2n + 1$. All schemes are proven correct and evaluated for performance. The removal of the U component from the signature reduces the size of the signature and reduces the time cost for both signature generation and signature verification.

The publications used in this chapter: [CT1], [CT6], [CT8], [CT10], [CT12].

CONCLUSION

Through the process of implementing the project "Researching and Building a representative collective digital signature scheme", the thesis has the following results and contributions:

1. The main results of the thesis

- 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.

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

- 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: $p = Nt_0t_1t_2 + 1$ (two schemes) and $p = Nk^2 + 1$ (two schemes).

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

- 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.

2. The scientific contributions of the thesis

The scientific contributions of the thesis include:

- 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.

- 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.

- 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.

3. 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	**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 Signature Protocols 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 Signature Schemes 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, n0.6, pp.478-485, 06/2022 (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).
