Computers, Materials & Continua
DOI: 10.32604/cmc.2022.025653
Article

Tech Science Press

Constructing Collective Signature Schemes Using Problem of Finding Roots Modulo

Tuan Nguyen Kim[1,*], **Duy Ho Ngoc**[2] **and Nikolay A. Moldovyan**[3]

[1]School of Computer Science, Duy Tan University, Da Nang, Vietnam
[2]Department of Information Technology, Ha Noi, Vietnam
[3]ITMO University, St. Petersburg, Russia
*Corresponding Author: Tuan Nguyen Kim. Email: nguyenkimtuan@duytan.edu.vn

Received: 30 November 2021; Accepted: 30 December 2021

Abstract: Digital signature schemes are often built based on the difficulty of the discrete logarithm problems, of the problem of factor analysis, of the problem of finding the roots modulo of large primes or a combination of the difficult problems mentioned above. In this paper, we use the new difficult problem, which is to find the w^{th} root in the finite ground field $GF(p)$ to build representative collective signature schemes, but the chosen modulo p has a special structure distinct $p = Nt_0t_1t_2 + 1$, where N is an even number and t_0, t_1, t_2 are prime numbers of equal magnitude, about 80 *bits*. The characteristics of the proposed scheme are: i) The private key of each signer consists of 2 components (K_1, K_2), randomly selected, but the public key has only one component (Y) calculated by the formula $Y = K_1^{w_1}K_2^{w_2}$; $w_1 = t_0t_1$ and $w_2 = t_0t_2$; and ii) The generated signature consists of a set of 3 components (e, S_1, S_2). We use the technique of hiding the signer's public key Y, which is the coefficient λ generated by the group nanager, in the process of forming the group signature and representative collective signature to enhance the privacy of all members of the signing collective.

Keywords: Computing roots; finding roots modulo; collective signature; signing collective; signing group

1 Introduction

Digital signatures [1] play an important role in authentication systems in today's cyberspace. Other network security services such as ensuring the integrity of information transmitted on the network, preventing the disclaimer of responsibility of a communication partner, etc also need the support of digital signatures [2]. It can be said that digital signatures contribute to making cyberspace safer and more reliable. Therefore, digital signatures and digital signature schemes are increasingly interested in research by cryptographic scientists.

Digital signatures is not only used to authenticate a single signer, but it can also support authentication for a collective, or a group, consisting of many different members. These people work together to create a single signature that represents an entire signing group or a group of signatures. Currently, there are many forms of digital signatures and digital signature schemes, in order to meet many different authentication models, which have been researched, published and applied in practice such as: Single digital signatures, group digital signatures [3–6], collective digital signatures [7–9], blind digital signatures [10,11], blind collective digital signatures [12], representative collective signatures [13]. The types of signatures generated by a set of signers are often referred to as multi-signatures [14,15].

The group signature is a signature representing a signing group, the signature formation is controlled by the group manager, the group manager's public key is used to verify the validity of the group signature of the signing group. The collective signature is a signature that represents a signing collective, signature formation is done by all members of the collective, the public key is used to check the validity of the collective signature is formed the public key of all members who participated in creating the signature. A collective signature on document M is considered valid when it is formed by the participation of all members of that signing collective. Representative collective signatures is a new form of collective signature, we rely on the advantages of the group signature scheme and the collective signature scheme to develop the representative collective signature scheme.

A representative collective signature [8,9] is formed from a signing collective consisting of: i) Many groups of members, called signing groups, each group is represented by a group manager; and ii) A number of single individuals, known as individual signers, who do not belong to any group, but are functionally equivalent to the group leaders in this collective. Thus, a single representative collective signature can authenticate all members of a multi-level functional collective who are the creators of this representative collective signature. There are three difficult problems commonly used to build digital signature schemes, which are: i) The problem of parsing a composite number into prime factors [16]; ii) Discrete logarithm problem on prime finite field [17]; and iii) Discrete logarithm problem on Elliptic curves [18,19].

The problem of finding modulo roots in finite fields is a new difficult problem, introduced by Nikolay A. Moldovyan in [17]. According to the author, the problem of finding the k^{th} prime modulo root (with a prime modulo being a large prime p, has the special structure $p = Nk^2 + 1$, $|p| \geq 1024$, N being an even number and k is prime, $|k| \geq 160$) is a hard problem, the estimated difficulty is $O\left(\sqrt{k}\right)$. Digital signature schemes built on this difficult problem can achieve security level 2^{80}, however, the time cost of signature generation and signature checking is an issue that needs to be considered for improvement. According to Nikolay A. Moldovyan, this time cost limitation can be overcome if the difficult problem of finding prime modulo roots is considered in a finite field, with p having the following structure $p = Nt_0t_1t_2 + 1$, where N is an even number; t_0, t_1, t_2 are prime numbers of the same magnitude as 80 bits.

The key pair of the signer in the case of $p = NK^2 + 1$ is (x, y), the private key x is chosen at random, the public key y is calculated by the formula $y = x^k \ mod\ p$. But in case $p = Nt_0t_1t_2 + 1$ is (K_1, K_2) and Y). That is, the private key consists of two components K_1 and K_2, the public key is still one component Y. This is the difference of the signature schemes described in this paper.

In this paper, we use the difficult problem of finding roots modulo in a finite ground field, with a prime modulo p with the structure $p = Nt_0t_1t_2 + 1$ and a single signature scheme described by Nikolay A. Moldovyan in [20] to build the collective signature scheme and the group signature scheme. From these two basic schemes, we propose and build two types of representative collective signature scheme, proposed by us: i) The collective signature scheme for many signing groups (the RCS.01-3 scheme);

and ii) The collective signature scheme for many signing groups and many individual signers (the RCS.02-3 scheme). These schemes fully inherit the security advantages of the newly created difficult problem and the attack resistance of the basic signature scheme built by Nikolay A. Moldovyan.

2 Constructing the Related Basis Digital Signature Schemes

In this part, we use the problem of finding roots modulo in the finite ground field, with modulo p with the structure $p = Nt_0t_1t_2 + 1$ [20], to build a collective digital signature scheme and a group digital signature scheme. These are the two basic signature schemes that we use to build the proposed collective digital signature schemes.

2.1 The Collective Signature Scheme Based on Problem of Finding Roots Modulo (The CDS-2 Scheme)

Assume there is a collective of m members who sign the document M. The private keys and public keys of each signer in this signing collective are $(K_{1_i},\ K_{2_i})$, $K_{1_i} < p,\ K_{2_i} < p$, and $Y_i = K_{1_i}^{w1}K_{2_i}^{w2}$, with $w_1 = t_0t_1, w_2 = t_0t_2, t_0 \approx\ t_1 \approx\ t_2 \approx 80$ bits and $i = 1,\ 2, \ldots, m$. Note that the signer's private key is a tuple of two components.

The collective public key used in the verification of the collective signature is calculated by the formula $Y = \prod_{i=1}^{m} Y_i\ mod\ p$. F_H is a pre-specified one-way secure hash function.

The process of checking the validity of a collective signature is the same as that of an individual signature [20]. The following are the procedures of the scheme:

- **The procedure for generating the collective digital signature on the document M**

Includes the following stages:

1. Each i-*th* signer performs the following steps:

– Generate pairs of random numbers T_{1_i} and T_{2_i} (act as a pseudo-secret key)
– Calculate the value of R_i according to the formula:

$$\mathrm{R_i = T_{1_i}^{w_1}T_{2_i}^{w_2}\ mod\ p} \tag{1}$$

– Send R_i to all other signers in the signing collective

2. A certain signer, or all, in the signing collective does:

– Calculate the value R according to the formula:

$$\mathrm{R = \prod\nolimits_{i=1}^{m} R_i\ mod\ p} \tag{2}$$

R acts as the general random component of the signing collective with the contribution of the random components R_i of each member of this collective.

– Calculate the value e according to the formula:

$$\mathrm{e = F_H(M||R||Y)} \tag{3}$$

– Send e to all other signers in the signing collective

e is the first element of the collective signature.

3. Each i-th signer goes on to:

– Calculate their share signature component S_{1_i} and S_{2_i} according to the formulas:

$$S_{1_i} = T_{1_i} K_{1_i}^{-e} \bmod p \tag{4a}$$

$$S_{2_i} = T_{2_i} K_{2_i}^{-e} \bmod p \tag{4b}$$

– Send S_{1_i} and S_{2_i} to all other signers in the signing collective

4. A certain signer, or all, in the signing collective does the final job: Calculate the second component S_1 and the third component S_2 of the collective signature according to the formulas:

$$S_1 = \prod_{i=1}^{m} S_{1_i} \bmod p \tag{5a}$$

$$S_2 = \prod_{i=1}^{m} S_{2_i} \bmod p \tag{5b}$$

So the triple value $(e,\ S_1, S_2)$ is the collective signature of the signing collective consisting of m signers on document M.

- **The procedure for verification the collective digital signature on the document M**

To check the validity of the signature received with the document M, the verifier performs the following steps:

1. Calculate the value of the collective public key Y according to the formula:

$$Y = \prod_{i=1}^{m} Y_i \bmod p \tag{6}$$

2. Calculate the value of R' according to the formula:

$$R' = Y^e S_1^{w_1} S_2^{w_2} \bmod p \tag{7}$$

3. Calculate the value of e' according to the formula:

$$e' = F_H(M||R'||Y) \tag{8}$$

4. Compare e' with e. If $e' = e$: The received signature is valid; Otherwise, it is invalid and will be rejected.

- **Proof of the correctness of the CDS-2 scheme:**

To prove the correctness of this scheme, we need to prove the existence of the test expression $e' = e$ in the signature checking procedure.

Conspicuously, the test expression $e' = e$ always exists.

Indeed:

$$\begin{aligned} R' &= Y^e S_1^{w_1} S_2^{W_2} \bmod p \\ &= \prod_{i=1}^{m} (K_{1_i}^{w_1} K_{2_i}^{w_2})^e \prod_{i=1}^{m} (T_{1_i} K_{1_i}^{-e})^{w_1} \prod_{i=1}^{m} (T_{2_i} K_{2_i}^{-e})^{w_2} \bmod p \\ &= \prod_{i=1}^{m} T_{1_i}^{w_1} T_{2_i}^{w_2} \bmod p = \prod_{i=1}^{m} R_i \bmod p = R \end{aligned}$$

as $R' = R$ so $e' = F_H(M||R'||Y) = F_H(M||R||Y) = e$

Thus, the test expression $e' = e$ always exists: This proves that the correctness of the signature check procedure, or the correctness of the CDS-2 scheme, is always guaranteed.

2.2 The Group Signature Scheme Based on Problem of Finding Roots Modulo (The GDS-2 Scheme)

Assume there is a group of m members who sign the document M. The private keys and the public key of each signer in this signing group are $(K_{1_i},\ K_{2_i})$, $K_{1_i} < p,\ K_{2_i} < p$, and $Y_i = K_{1_i}^{w1} K_{2_i}^{w2}$, with $w_1 = t_0 t_1$, $w_2 = t_0 t_2$, $t_0 \approx t_1 \approx t_2 \approx 80$ bits and $i = 1,\ 2, \ldots, m$. The private keys and the public key of the group manager (GM) are $K_1',\ K_2'$, $K_1' < p,\ K_2' < p$, $w_1 = t_0 t_1$, $w_2 = t_0 t_2$ and $Y' = K_1^{\prime w1} K_2^{\prime w2}$.

The group public key used in the verification of the group signature is calculated by the formula $Y = \prod_{i=1}^{m} Y_i \ mod\ p$. F_H is a pre-specified one-way secure hash function.

The process of checking the validity of a group signature is the same as that of an individual signature [20]. The following are the procedures of the scheme:

- **The procedure for generating the group digital signature on the document *M***

Includes the following steps:

1. The GM does the following:

- Calculate the hash value of the document M using the formula:

$$\mathrm{H} = \mathrm{F_H(M)} \tag{9}$$

- Calculate mask coefficients λ_i for each signer in the group sign according to the formula:

$$\lambda_\mathrm{i} = \mathrm{F_H(H\ ||\ Y_i ||\ F_H(H\ || Y_i || K_1' || K_2'))} \tag{10}$$

- Send λ_i to each corresponding signer i
- Calculate the first component of the group signature

$$\mathrm{U} = \prod_{\mathrm{i=1}}^{\mathrm{m}} \mathrm{Y_i^{\lambda_i}\ mod\ p} \tag{11}$$

2. Each i-*th* signer in the signing group does:

- Randomly generate pairs of numbers T_{1_i} and T_{2_i} and then calculate R_i according to the formula:

$$\mathrm{R_i} = \mathrm{T_{1_i}^{w1} T_{2_i}^{w2}\ mod\ p} \tag{12}$$

- Send the R_i value to the group manager

3. The GM continues to make:

- Generates a random value pair T_1' and T_2' and calculate the values R', R and e according to the formulas:

$$\mathrm{R'} = \mathrm{T_1^{\prime w_1} T_2^{\prime w_2} mod\ p} \tag{13}$$

$$\mathrm{R} = \mathrm{R'} \prod_{\mathrm{i=1}}^{\mathrm{m}} \mathrm{R_I\ mod\ p} \tag{14}$$

$$\mathrm{e} = \mathrm{F_H(M||R||U)\ mod}\ \delta \tag{15}$$

where δ is a prime number of length $|\delta| = 160$ bits.

- e is the second component of the group signature.

– Send the value of e to all signers in the signing group

4. Each signer i continues to do the following:

– Calculate the shared signature component of S_{1_i}, S_{2_i} according to the formula:

$$S_{1_i} = T_{1_i} K_{1_i}^{-\lambda_i e} \bmod p \tag{16a}$$

$$S_{2_i} = T_{2_i} K_{2_i}^{-\lambda_i e} \bmod p \tag{16b}$$

– Send the value S_{1_i}, S_{2_i} to other signers in the signing group

5. The GM does the final work:

– Check the correctness of the shared signature S_{1_i}, S_{2_i} of all signers in the signing group using the formula:

$$R_i = S_{1_i}^{w_1} S_{2_i}^{w_2} Y_i^{e_i} \bmod p \tag{17}$$

– If all pairs of numbers S_{1_i}, S_{2_i} are satisfied: Calculate the signature component of a personal share according to the following formulas:

$$S_1' = T_1' K_1'^{-e} \bmod p \tag{18a}$$

$$S_2' = T_2' K_2'^{-e} \bmod p \tag{18b}$$

– Calculate the third component S_1 and the fourth S_2 of the group signature according to the following formulas:

$$S_1 = S_1' \prod_{i=1}^{m} S_{1_i} \bmod p \tag{19a}$$

$$S_2 = S_2' \prod_{i=1}^{m} S_{2_i} \bmod p \tag{19b}$$

So the set of values (U, e, S_1, S_2) is the group signature of the signing group on the document M.

- **The procedure for verification the group digital signature on the document *M***

To check the validity of the signature received with the document M, the verifier performs the following steps:

1. Calculate the value of the group public key Y according to the formula:

$$Y' = \prod_{i=1}^{m} Y_i \bmod p \tag{20}$$

2. Calculate the value of R^* according to the formula:

$$R^* = (UY')^e S_1^{w_1} S_2^{w_2} \bmod p \tag{21}$$

3. Calculate the value of e^* according to the formula:

$$e^* = F_H(M||R^*||U) \tag{22}$$

4. Compare the value of e^* with e. If $e^* = e$: The received signature is valid; Otherwise, the received signature is invalid, it is rejected.

- **Proof of the correctness of the GDS-2 scheme:**

To prove the correctness of this scheme, we only need to prove the existence of the check expression $e^* = e$ in the signature check procedure.

Conspicuously, the test expression $e^* = e$ always exists.

We have:

$$\begin{aligned}
R^* &= \left(UY'\right)^e {S_1}^{w_1} {S_2}^{w_2} \bmod p \\
&= \left[\left(K_1'^{w_1} K_2'^{w_2}\right)^e \prod\nolimits_{i=1}^{m} \left({K_{1_i}}^{w_1} {K_{2_i}}^{w_2}\right)^{\lambda_i e}\right] \\
&\quad \left[\left(T_1' K_1'^{-e}\right)^{w_1} \prod\nolimits_{i=1}^{m} \left(T_{1_i} {K_{1_i}}^{-\lambda_i e}\right)^{w_1}\right] \\
&\quad \left[\left(T_2' K_2'^{-e}\right)^{w_2} \prod\nolimits_{i=1}^{m} \left(T_{2_i} {K_{2_i}}^{-\lambda_i e}\right)^{w_2} \bmod p\right] \\
&= T_1'^{w_1} T_2'^{w_2} \prod\nolimits_{i=1}^{m} T_{1_i}^{w_1} T_{2_i}^{w_2} \bmod p \\
&= R' \prod\nolimits_{i=1}^{m} R_i \bmod p = R
\end{aligned}$$

Because of $R^* = R$ so $e^* = F_H(M||R^*||U) = F_H(M||R||U) = e$.

So the expression $e^* = e$ always exists: This proves that the correctness of the signature check procedure, or the correctness of the GDS-2 scheme, is always guaranteed.

3 Constructing the Proposed Collective Digital Signature Schemes Based on Problem of Finding Roots Modulo in the Finite Ground Field

In this section, we use the collective digital signature scheme and the group signature scheme described in Section 2 as the basis schemes to build two types of the proposed collective signature scheme: i) The collective digital signature scheme for many signing groups; and ii) The collective digital signature scheme for many signing groups and many individual signers.

3.1 Constructing the Collective Digital Signature Scheme for Signing Groups (The RCS.01-3 Scheme)

This section uses the two schemes just described above as the basis to build a representative collective signature scheme, the first type: The collective signature for many (*g*) signing groups.

This scheme allows the creation of a collective signature on the document M which represents a signing collective with *g* signing groups, each of which consists of *m* members, which is controlled by the group manager (GM). The signature formation process is run by the group managers.

The input parameters, public keys, and private keys are selected, calculated as the base schemes above. The following are the procedures of the scheme:

- **The procedure for generating the collective digital signature for *g* signing groups on the document M**

1. Each GM in the signing collective does the following:

– Calculate mask coefficients λ_{ji} for the signers in the j-*th* signing group according to the formula:

$$\lambda_{ji} = F_H(H\ ||Y_i||\ F_H(H||\ Y_i||\ K_1'||K_2')) \tag{23}$$

(λ_{ji} is the mask coefficient of the i-*th* signer in the j-*th* signing group)

- Calculate the value of the component U_j of the j-*th* signing group according to the formula:

$$U_j = \prod_{i=1}^{m_j} Y_{ji}^{\lambda_{ji}} \bmod p \tag{24}$$

U_j is considered as the shared value of the j-*th* signing group in the first component of the collective signature for the signing groups.

- Calculate the random component R_j using the formula:

$$R_j = R'_j \prod_{i=1}^{m_j} R_{ji} \bmod p \tag{25}$$

- Send U_j and R_j values to all other GMs in the signing collective

2. A certain GM in the singing collective, or all, computes the values of the U, R and e components of the collective signature according to the following formulas:

$$U = \prod_{j=1}^{g} U_j \bmod p \tag{26}$$

$$R = \prod_{j=1}^{g} R_j \bmod p \tag{27}$$

and

$$e = F_H(M||R||U) \bmod \delta \tag{28}$$

where δ is a large prime $|\delta| = 160$ bits.

U and e are the first and second components of the collective signature.

3. Each GM in the signing collective continues to do:

- Calculate the shared signature S_{1j}, S_{2j} of the j-*th* signing group according to the formula:

$$S_{1j} = S'_{1j} \prod_{i=1}^{m_j} S_{1ji} \bmod p \tag{29a}$$

$$S_{2j} = S'_{2j} \prod_{i=1}^{m_j} S_{2ji} \bmod p \tag{29b}$$

with S_{ji} is the shared signature of the i-*th* individual in the j-*th* group.

- Send S_{1j}, S_{2j} to other GMs in the signing collective

4. A certain GM in the signing collective, or all, does the following:

- Check the correctness of the shared signature S_{1_i}, S_{2_i} of all signing groups in the signing collective using the formula:

$$R_j = (U_j Y'_j)^e S_{1_j}^{w_1} S_{2_j}^{w_2} \bmod p \tag{30}$$

– If all S_{1_i}, S_{2_i} are satisfied: Calculate the third and fourth components S_{1_i}, S_{2_i} of the collective signature according to the formulas:

$$S_1 = \prod_{j=1}^{g} S_{1_j} \bmod p \tag{31a}$$

$$S_2 = \prod_{j=1}^{g} S_{2_j} \bmod p \tag{31b}$$

So set of values (U, e, S_1, S_2) is the collective signature of g signing groups on the document M.

- **The procedure for verification the collective digital signature for *g* signing groups on the document M**

To check the validity of the signature received with the document M, the verifier performs the following steps:

1. Calculate the collective public key of the signing collective Y_{col} according to the formula:

$$Y_{col} = \prod_{j=1}^{g} Y_j^{'} \bmod p \tag{32}$$

2. Calculate the value of the random component R^* according to the formula:

$$R^* = (UY_{col})^e S_1^{w_1} S_2^{w_2} \bmod p \tag{33}$$

3. Calculate the value of e^* according to the formula:

$$e^* = F_H(M||R^*||\ U) \tag{34}$$

4. Compare e^* with e. If $e^* = e$: The received signature is valid; Otherwise, the received signature is invalid, it is rejected.

- **Proof of the correctness of the RCS.01-3 scheme:**

The precision of this representative collective signature scheme is shown through: i) The existence of a shared signature verification formula S_{ji} shared by the signing team leaders R_j; and ii) Existence of the test expression $e^* = e$ in the signature check procedure. Specifically as follows:

a) Prove the correctness of the shared signature check formula:

It is easy to see that the formula for checking shared signature S_{ji} shared by team leaders signing R_j always exists. Indeed:

$$\begin{aligned}
R_j &= \left(U_j Y'_j\right)^e {S_{1_j}}^{w_1} {S_{2_j}}^{w_2} \bmod p \\
&= \left[\left(K'^{w_1}_{1_j} K'^{w_2}_{2_j}\right)^e \prod_{i=1}^{m_j} \left({K_{1_{ji}}}^{w_1} {K_{2_{ji}}}^{w_2}\right)^{\lambda_{ji} e}\right] \\
&\quad \left[\left(T'_{1_j} K'^{-e}_{1_j}\right)^{w_1} \prod_{i=1}^{m_j} \left(T_{1_{ji}} {K_{1_{ji}}}^{-\lambda_{ji} e}\right)^{w_1}\right] \\
&\quad \left[\left(T'_{2_j} K'^{-e}_{2_j}\right)^{w_2} \prod_{i=1}^{m_j} \left(T_{2_{ji}} {K_{2_{ji}}}^{-\lambda_{ji} e}\right)^{w_2} \bmod p\right] \\
&= T'^{w_1}_{1_j} T'^{w_2}_{2_j} \prod_{i=1}^{m_j} T^{w_1}_{1_{ji}} T^{w_2}_{2_{ji}} \bmod p \\
&= R'_j \prod_{i=1}^{m_j} R_{ji} \bmod p = R_j
\end{aligned}$$

b) Proof of correctness of the signature check procedure:

Conspicuously, the signature check expression $e^* = e$ always exists.

We have:

$$\begin{aligned}
R^* &= (UY_{col})^e {S_1}^{w_1} {S_2}^{w_2} \bmod p \\
R^* &= \left(\prod_{j=1}^{g} U_j \prod_{j=1}^{g} Y'_j\right)^{-e} \left(\prod_{j=1}^{g} S_{1_j}\right)^{w_1} \left(\prod_{j=1}^{g} S_{2_j}\right)^{w_2} \bmod p \\
&= \prod_{j=1}^{g} (U_j Y'_j)^e {S_{1_j}}^{w_1} {S_{2_j}}^{w_2} \bmod p \\
&= \prod_{j=1}^{g} R_j \bmod p = R
\end{aligned}$$

Because of $R^* = R$ so $e^* = F_H(M||R^*||U) = F_H(M||R||U) = e$.

So the expression $e^* = e$ always exists: This proves that the correctness of the signature check procedure is always guaranteed.

From (a) and (b): The correctness of the RCS.01-3 scheme is guaranteed.

3.2 Constructing the Collective Digital Signature Scheme for Signing Groups and Individual Signers (The RCS.02-3 Scheme)

This section uses the two schemes just described above as a basis to build a representative collective signature scheme, the second type: The collective signatures for many (g) signing groups and many (m) individual signers.

This scheme allows the creation of a collective signature on document M that represents a signing collective with m individual signers and g signing groups, each of which consists of m members which is controlled by the group manager (GM). The signature formation process is run by the group managers and individual signers.

The input parameters, public keys, and private keys are selected, calculated as the base schemes above. The following are the procedures of the scheme:

- **The procedure for generating the collective digital signature for *g* signing groups and *m* individual signers on the document M**

Includes the following steps:

1a. Each GM in the signing collective does the following:

– Generate mask coefficient λ_{ji} for the signers in the j-*th* signing group according to the formula (23).

(λ_{ji} is the mask coefficient of the i-*th* signer in the j-*th* signing group)

– Calculate the value of the component U_j of the j-*th* sign group according to the formula:

$$\mathrm{U_j = \prod_{i=1}^{m_j} Y_{ji}^{ji} \bmod p} \tag{35}$$

U_j is the shared member of the j-*th* signing group to form the first part of the collective signature.

– Calculate the random parameter R_j of the j-*th* signed group according to the formula:

$$\mathrm{R_j = R_j^{\prime} \prod_{i=1}^{m_j} R_{ji} \bmod p} \tag{36}$$

R_j is a shared member of the j-*th* signing group to generate a random parameter of the collective signature..

– Send U_j and R_j values to all other managers and individual signers in the signing collective.

1b. Each individual who signs the j-*th* performs the following tasks:

– Choose 2 random numbers T_{1_j} and T_{2_j} and calculate the random value R_j according to the formula:

$$\mathrm{R_j = T_{1_j}{}^{w_1} T_{2_j}{}^{w_2} \bmod p} \tag{37}$$

– Send the value R_j to all signers GMs and other individual signers in the signing collective.

2. A GM or a certain individual signing in the collective calculates the values of U, R and e according to the following formulas:

$$\mathrm{U = \prod_{j=1}^{g+m} U_j} \tag{38}$$

$$\mathrm{R = \prod_{j=1}^{g+m} R_j} \tag{39}$$

$$\mathrm{e = F_H(M||R||U) \bmod \delta} \tag{40}$$

where δ is a large prime ($|\delta| = 160$ *bits*); $U_j = 1$ when $j = g + 1,\ g + 2,\ \ldots,\ g + m$).

U and e are the first and second components of the group signature.

3a. Each GM in the signing collective continues to do:

– Calculate the shared component $S_{1_j},\ S_{2_j}$ of group j according to the formula:

$$S_{1_j} = S'_{1_j} \prod_{i=1}^{m_j} S_{1_{ji}} \bmod p \tag{41a}$$

$$S_{2_j} = S'_{2_j} \prod_{i=1}^{m_j} S_{2_{ji}} \bmod p \tag{41b}$$

with $S_{1_{ji}},\ S_{2_{ji}}$ is the shared component of the i-*th* signer in the j-*th* group.

– Send $S_{1_j},\ S_{2_j}$ for GMs and other individual signers in the signing collective.

3b. Each individual signer in the signing collective continues to do:

(the j-th ; $j = g + 1,\ g + 2,\ \ldots,\ g + m$)

– Calculate the share component $S_{1_j},\ S_{2_j}$ according to the formula:

$$S_{1_j} = T_{1_j} K_{1_j}^{-e} \bmod p \tag{42a}$$

$$S_{2_j} = T_{2_j} K_{2_j}^{-e} \bmod p \tag{42b}$$

– Send $S_{1_j},\ S_{2_j}$ to other GMs and individual signers in the signing collective.

4. A GM or an individual in the signing collective doing:

– Check the validity of each $S_{1_j},\ S_{2_j}$ according to the formulas:

$$R_j = (U_j Y'_j)^e {S_{1_j}}^{w_1} {S_{2_j}}^{w_2} \bmod p \tag{43a}$$

with $j = 1,\ 2,\ \ldots,\ g$

and

$$R_j = S_{1_j}^{w_1} S_{2_j}^{w_2} Y_j^{-e} \bmod p \tag{43b}$$

with $j = g + 1,\ g + 2,\ \ldots,\ g + m$

– If all are satisfied: The third component of the group signature will be calculated according to the formulas:

$$S_1 = \prod_{j=1}^{g+m} S_{1_j} \bmod p \tag{44a}$$

$$S_2 = \prod_{j=1}^{g+m} S_{2_j} \bmod p \tag{44b}$$

So the set of values $(U,\ e,\ S_1, S_2)$ is the representative collective signature of a collective consisting of *g* signing groups and *m* individual signers on the document M. This type of signature is also known as collective signature shared by multiple groups and signed by many individuals. It represents this collective signing.

- **The procedure for verification the collective digital signature for *g* signing groups and *m* individual signers on the document M**

To check the validity of the signature received with the document M, the verifier performs the following steps:

1. Calculate the collective public key of the signing collective according to the formula:

$$Y_{col}=\prod_{j=1}^{g} Y_j^{\prime} \prod_{j=g+1}^{g+m} Y_j \bmod p \tag{45}$$

2. Calculate the value of the random parameter R^* according to the formula:

$$R^*= (UY_{col})^e S_1^{w_1} S_2^{w_2} \bmod p \tag{46}$$

3. Calculate e^* using to the formula:

$$e^* =F_H(M \parallel R^* \parallel U) \tag{47}$$

4. Compare e^* with e. If $e^* = e$: The signature received is valid; Otherwise, the received signature is invalid, it is rejected.

- **Proof of the correctness of the RCS.02-3 scheme:**

The precision of this representative collective signature scheme is shown through: i) The existence of a formula to check the shared signature S_j of each signing group R_j^*; ii) The existence of the signature test formula shared S_j by each individual signer R and iii) The existence of the test expression $e^* = e$. Specifically as follows:

a) The correctness of the formula to check the shared signature of each group leader:

It is easy to see that the formula for checking shared signature S_{ji} shared by team leaders signing R_j always exists. Indeed:

$$\begin{aligned}
R_j &= \left(U_j Y_j^{\prime}\right)^e S_{1_j}{}^{w_1} S_{2_j}{}^{w_2} \bmod p \\
&= \left[\left(K_{1_j}^{\prime w_1} K_{2_j}^{\prime w_2}\right)^e \prod_{i=1}^{m_j} \left(K_{1_{ji}}{}^{w_1} K_{2_{ji}}{}^{w_2}\right)^{\lambda_{ji} e}\right] \\
&\quad \left[\left(T_{1_j}^{\prime} K_{1_j}^{\prime -e}\right)^{w_1} \prod_{i=1}^{m_j} \left(T_{1_{ji}} K_{1_{ji}}{}^{-\lambda_{ji} e}\right)^{w_1}\right] \\
&\quad \left[\left(T_{2_j}^{\prime} K_{2_j}^{\prime -e}\right)^{w_2} \prod_{i=1}^{m_j} \left(T_{2_{ji}} K_{2_{ji}}{}^{-\lambda_{ji} e}\right)^{w_2} \bmod p\right] \\
&= T_{1_j}^{\prime w_1} T_{2_j}^{\prime} w_2 \prod_{i=1}^{m_j} T_{1_{ji}}^{w_1} T_{2_{ji}}^{w_2} \bmod p \\
&= R_j^{\prime} \prod_{i=1}^{m_j} R_{ji} \bmod p = R_j
\end{aligned}$$

b) The correctness of the formula to check the shared signature per signer:

It is easy to see that the formula for checking the shared signature S_i shared by the R signing team leaders always exists. Indeed:

$$\begin{aligned} R &= Y_j^e {S_{1_j}}^{w_1} {S_{2_j}}^{w_2} \bmod p \\ &= ({K_{1_j}}^{w_1} {K_{2_j}}^{w_2})^e (T_{1_j} {K_{1_j}}^{-e})^{w_1} (T_{2_j} {K_{2_j}}^{-e})^{w_2} \bmod p \\ &= {T_{1_j}}^{w_1} {T_{2_j}}^{w_2} \bmod p = R \end{aligned}$$

c) The correctness of the representative collective signature check procedure:

Conspicuously, the signature check expression $e^* = e$ always exists.

We see:

$$\begin{aligned} R^* &= (UY_{col})^e {S_1}^{w_1} {S_2}^{w_2} \bmod p \\ &= \left(\prod_{j=1}^{g+m} U_j \prod_{j=1}^{g} Y'_j \prod_{j=g+1}^{g+m} Y_j\right)^{-e} \left(\prod_{j=1}^{g+m} S_{1_j}\right)^{w_1} \left(\prod_{j=1}^{g+m} S_{2_j}\right)^{w_2} \bmod p \\ &= \prod_{j=1}^{g} (U_j Y'_j)^e {S_{1_j}}^{w_1} {S_{2_j}}^{w_2} \prod_{j=g+1}^{g+m} Y_j^e {S_{1_j}}^{w_1} {S_{2_j}}^{w_2} \bmod p \\ &= \prod_{j=1}^{g+m} R_j \bmod p = R \end{aligned}$$

and calculate:

$$\begin{aligned} e^* &= F_H(M \parallel R^* \parallel U) \bmod \delta \\ &= F_H(M \parallel R \parallel U) \bmod \delta \\ &= e \end{aligned}$$

So the expression $e^* = e$ always exists. This proves that the correctness of the signature check procedure, or the correctness of the RCS.02-3 scheme, is always guaranteed.

4 Security Analysis and Performance Evaluation

4.1 Security Advantages of the Proposed Collective Signature Schemes

The group signature scheme we described in Section 2.2 has the following security advantages:

- As the scheme is based on the properties of the prime modulo root problem in a finite field, it inherits the safety level of this difficult problem. The attack resistance of the GDS-2 scheme is completely similar to the basic scheme described by Nikolay A. Moldovyan in [20]. To circumvent this scheme, the attacker must find the prime modulo roots to simultaneously determine the two secret values K_1 and K_2.
- The public key of all signers, including the group manager, is "masked" by the mask parameter λ. The attacker will not be able to determine who in the signing group participated in the signing to form the group signature.
- The U component of the group signature contains information about all members of a signing group who took part in forming the group signature for this signing group. Consequently, when there is a dispute about the group signature, the group leader will be able to identify the signer easily later and resist the "disclaimer".
- There is no need to exchange or share security values, private keys, or secret keys between members of a signing group or between members of a signing group with the manager. Therefore, the Internet environment is sufficient to implement this scheme. In addition, the scheme is also easy to deploy on top of existing PKI (Public Key Infrastructure) systems [21].

- As shown in the 5th step of the signature generation procedure, a group manager only proceeds when he or she believes or has verified that all signatures participating in creating the collective signature are valid. The operation generates the final component (S_1, S_2) of the group signature, by adding the shared signature of the group leader to the product of the shared signatures of all members. This makes it very hard to simulate member signings, or members signing each other's signatures and also shows the representativeness as well as high responsibility of the team manager.

The representative collective signature schemes built in this paper use the CDS-2 collective signature scheme and the GDS-2 group signature scheme as the basic scheme, so it also has the advantages of security and resistance to attacks like these schemes.

4.2 Performance of the Proposed Collective Signature Schemes

We evaluate the computational performance of the proposed representative collective signature schemes by calculating the time cost that the scheme takes for the signature generation process (Signature generation procedure) and the need for the signature verification process (Signature verification procedure). The time costs of representative collective signature schemes proposed in this paper are shown in Tab. 1.

Table 1: Time cost of the proposed collective signature scheme: RCS.01-3 and RCS.02-3

The scheme	Time for the signature generation	Time for the signature verification
RCS.01-3	$\mathrm{U} = \sum_{j=1}^{g} (243\mathrm{m}_j+1)\mathrm{T}_m$ $\mathrm{e} = [\sum_{j=1}^{g}(481\mathrm{m}_j+481)+1]\mathrm{T}_m$ $\mathrm{S}_1 + \mathrm{S}_2 = \sum_{j=1}^{g} (1209\mathrm{m}_j+484)\mathrm{T}_m$ $\mathrm{Sum} = [\sum_{j=1}^{g}(1934\mathrm{m}_j+966)+1]\mathrm{T}_m$	$(724 + \mathrm{g})\mathrm{T}_m$
RCS.02-3	$\mathrm{U} = \sum_{j=1}^{g} (243\mathrm{m}_j+1)\mathrm{T}_m$ $\mathrm{e} = [\sum_{j=1}^{g}(481\mathrm{m}_j+481)+481\mathrm{m} + 1]\mathrm{T}_m$ $\mathrm{S}_1 + \mathrm{S}_2 = [\sum_{j=1}^{g}(1209\mathrm{m}_j+484)+1206\mathrm{m}]\mathrm{T}_m$ $\mathrm{Sum} = [\sum_{j=1}^{g}(1934\mathrm{m}_j+966)+1687\mathrm{m} + 1]\mathrm{T}_m$	$(724 + \mathrm{g} + \mathrm{m})\mathrm{T}_m$

Notations: T_h : Time cost of a hash operation in Z_p; T_s : Time cost of a scalar multiplication in Z_p; T_{inv} : Time cost of a inverse operation in Z_p; T_e : Time cost of an exponent operation in Z_p; T_m : Time cost of a modular multiplication in Z_p.

According to [22]: $\mathrm{T}_h \approx \mathrm{T}_m$, $\mathrm{T}_s \approx 29\mathrm{T}_m$, $\mathrm{T}_{inv} \approx 240\mathrm{T}_m$, $\mathrm{T}_e \approx 240\mathrm{T}_m$,$\mathrm{T}_{sqrt} \approx 290\mathrm{T}_m$.

Information from Tab. 1 shows that the time cost for signature generation and signature checking of a proposed representative signature scheme is not much larger when compared to the new collective digital signature schemes in [8].

5 Disscusion

- The representative collective signature is a new form of collective digital signature, it was proposed by us in 2019 and has been built on many difficult problems and/or different digital signature standards. The research results of this paper show that the proposed scheme can be built on a customized form of a new difficult problem, the problem of finding roots modulo in a finite ground field, with a two-component private key. This proves that the availability of a representative collective signature scheme is very high.
- The signature generation procedure in the proposed representative collective signature scheme shows that it has all the security advantages of the collective signature generation procedure and the group signature generation procedure. This is one of the advantages of the representative collective signature schemes proposed by us.
- The basic requirement for multi-signature schemes is to record the information of everyone who participated in creating the signature of the group or the collective. This information is needed for the identification of the signer and against the signer's "disclaimer of responsibility" in the future. The group signature schemes and the representative collective signature schemes built here have met this requirement, the signer information is contained in the first component of the signature, the U component. The algorithm to identify the signer from the information contained in the U has been described in [6].
- The use of the U-component of the representative collective signature is necessary, but this increases the signature size. This is considered a limitation of the proposed scheme. We have proposed and built a two-component representative collective signature scheme, but we can only implement the scheme based on discrete logarithm problems. We are working to build this improved scheme based on the problem of finding roots modulo large primes.

6 Conclusion

Thus, in this paper, we build a collective signature scheme and a group signature scheme using the single digital signature protocol described in [20] via a two-component private key $(K_1,\ K_2)$. Based on their computational difficulty, all three schemes are formed in order to find the modulo root of a large prime, with a prime modulo $p = Nt_0t_1t_2 + 1$, in a finite ground field.

The two signature schemes described above can then be used as the basis for building two different types of collective signature schemes: i) The collective digital signature scheme for many signing groups; and ii) The collective digital signature scheme for many signing groups and many individual signers. These two schemes fully inherit the attack resistance of the single signature scheme in [20] and the difficulty of finding the modulo root in a finite prime field, so the security of the scheme is always guaranteed. For all schemes built in this study, if the chosen modulo is 1024 bits, their security level will be 80 bits.

In this paper, we analyze and evaluate the proposed schemes based on their security benefits and computational performance. In the future, the design of a collective signature scheme will be based on the computational difficulty of finding roots modulo on the elliptic curve.

Funding Statement: We received funding for this research from Duy Tan University, Danang, Vietnam. https://duytan.edu.vn/.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. Radack, "Updated digital signature standard approved as Federal Information Processing Standard (FIPS) 186-3," in *National Institute of Standards and Technology*, FIPS Publication 186-3, 2009.

[2] J. Pieprzyk, T. Hardjono and J. Seberry, "*Fundamentals of Computer Security*," Berlin: Springer-Verlag, 2003.

[3] D. Chaum and E. Heyst, "Group signatures," in *Advances in Cryptology - EUROCRYPT' 91*, Springer-Verlag, pp. 257–265, 1991.

[4] R. Xie, C. Xu, C. He and X. Zhang, "A new group signature scheme for dynamic membership," *International Journal of Electronic Security and Digital Forensics*, vol. 8, no. 4, pp. 332–351, 2016.

[5] Q. Alamélou, O. Blazy, S. Cauchie and P. Gaborit, "A Code-based group signature scheme," *Designs, Codes and Cryptography*, vol. 82, no. 1-2, pp. 469–493, 2017.

[6] A. A. Moldovyan and N. A. Moldovyan, "Group signature protocol based on masking public keys," *Quasigroups and Related Systems*, vol. 22, no. 1, pp. 133–140, 2014.

[7] N. A. Moldovyan, N. H. Minh, D. T. Hung and T. X. Kien, "Group signature protocol based on collective signature protocol and masking public keys mechanism," *International Journal of Emerging Technology and Advanced Engineering*, vol. 6, no. 6, pp. 1–5, 2016.

[8] N. K. Tuan, V. L. Van, D. N. Moldovyan, H. N. Duy and A. A. Moldovyan, "Collective signature protocols for signing groups," in *Proc. Information Systems Design and Intelligent Applications. Advances in Intelligent Systems and Computing*, Springer, India, vol. 672, pp. 200–208, 2018.

[9] N. K. Tuan, H. N. Duy and N. 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.

[10] J. L. Camenisch, J. M. Piveteau and M. A. Stadler, "Blind signatures based on the discrete logarithm problem," in *Proc. Advances in Cryptology–EUROCRYPT'94, Lecture Notes in Computer Science*, Springer-Verlag, Berlin, Heidelberg, New York, vol. 950, pp. 428–432, 1995.

[11] D. Chaum, "Blind signatures for untraceable payments," in *Proc. Advances in Cryptology–CRYPTO'82*, Plenum Press, pp. 199–203, 1983.

[12] N. A. Moldovyan and A. A. Moldovyan, "Blind collective signature protocol based on discrete logarithm problem," *International Journal of Network Security*, vol. 11, no. 2, pp. 106–113, 2010.

[13] N. K. Tuan, H. N. Duy and N. 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.

[14] K. Itakura and K. Nakamura, "A public key cryptosystem suitable for digital multisignatures," *NEC Research and Development*, vol. 71, pp. 1–8, 1983.

[15] D. M. Tuan, "New elliptic curve digital multi-signature schemes for multi-section messages," in *Proc. Int. Conf. on Computing and Communications Technologies Research-Innovation and Vision for the Future*, Vietnam, pp. 25–28, 2012.

[16] D. Poulakis and R. Rolland, "A digital signature scheme based on two hard problems," in *Computation, Cryptography, and Network Security*, Springer, pp. 441–450, 2015.

[17] N. A. Moldovyan, "Digital signature scheme based on a new hard problem," *Computer Science Journal of Moldova*, vol. 16, no. 2, pp. 163–182, 2008.

[18] A. A. Bolotov, S. B. Gashkov and A. B. Frolov, "Elementary introduction to elliptic curve cryptography," *Cryptography Protocols on the Elliptic Curves*, KomKniga, Moskow, 2006.

[19] R. L. B. Daniel, “Generic groups, collision resistance, and ECDSA,” *ACM Journal: Designs, Codes and Cryptography*, vol. 35, no. 1, pp. 119–152, 2005.

[20] N. A. Moldovyan and V. A. Shcherbacov, “New signature scheme based on difficulty of finding roots,” *Quasigroups and Related Systems*, vol. 20, no. 1, pp. 261–266, 2012.

[21] H. Yong, C. Fugui and Q. Peixin, “Research on digital signature based on digital certificate,” in *Proc. of 14th Youth Conf. on Communication*, Scientific Research, pp. 467–470, 2009.

[22] C. Popescu, “Blind signature and BMS using elliptic curves,” *Studia Univ Babes–Bolyai*, Informatica, pp. 43–49, 1999.