Computers, Materials & Continua
DOI: 10.32604/cmc.2022.024677
Article

Tech Science Press

New Representative Collective Signatures Based on the Discrete Logarithm Problem

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: 27 October 2021; Accepted: 10 December 2021

Abstract: The representative collective digital signature scheme allows the creation of a unique collective signature on document M that represents an entire signing community consisting of many individual signers and many different signing groups, each signing group is represented by a group leader. On document M, a collective signature can be created using the representative digital signature scheme that represents an entire community consisting of individual signers and signing groups, each of which is represented by a group leader. The characteristic of this type of letter is that it consists of three elements (U, E, S), one of which (U) is used to store the information of all the signers who participated in the formation of the collective signature on document M. While storing this information is necessary to identify the signer and resolve disputes later, it greatly increases the size of signatures. This is considered a limitation of the collective signature representing 3 elements. In this paper, we propose and build a new type of collective signature, a collective signature representing 2 elements (E, S). In this case, the signature has been reduced in size, but it contains all the information needed to identify the signer and resolve disputes if necessary. To construct the approved group signature scheme, which is the basic scheme for the proposed representative collective signature schemes, we use the discrete logarithm problem on the prime finite field. At the end of this paper, we present the security analysis of the AGDS scheme and a performance evaluation of the proposed collective signature schemes.

Keywords: Elliptic curve; signing group; individual signer; collective signature; group signature

1 Introduction

To ensure the security of transactions on the network, people often use authentication systems based on digital signatures. Digital signatures [1] not only help authenticate the origin of information,

but also help check the integrity of information as it is transmitted from source to destination. In addition, digital signatures also help prevent the repudiation of a communication partner.

In order to meet many different authentication requirements in practice, many types of digital signature schemes have been researched and published such as single digital signature scheme [2], multiple digital signature scheme [3], blind digital signature scheme [4,5], group digital signature scheme [6–9], collective signature scheme [10], blind collective digital signature scheme [11], representative collective signature scheme [12].

It is known that a group signature is a multi-signature formed by a group of signers under the control of the group leader (who manages the signing group). This type of signature usually consist of two components, or pairs of two sufficiently large integers (E and S). A group signature scheme must meet the following minimum requirements: i) A set (subnet) of any individual signers the individual, selected from a group of members, can generate a signature, representing the signing group, on document M; ii) The signing group manager can identify everyone who participated in the group signature formation process of the signing group they manage, and only the group manager can do this; and iii) Persons outside of the signing group cannot establish a subset of individual signers so that these people create group signatures representing the signing group.

The Approved Group Digital Signatures (AGDS) type proposed by us [13], to serve as the basic scheme for the representative collective signature scheme, also satisfies the following additional conditions: i) No anyone in the signing group, including the group manager, knows the private key used by the individual signers in the group signature formation process; ii) Group signatures are formed in two stages: First, each individual signer generates the associated parameters and their shared personal signature and then passes it all on to the group manager. The group manager then checks the validity of each signature received by the shared individuals, if all are valid then the manager proceeds to generate the final group signature, from the shared signatures and signature of the administrator himself. This is why this signature is called a consent group signature.

Therefore, to meet the above conditions, the approved group signature has been designed in the form of a set of three components U, E, and S [10]. The U component is used to store information of all participating members participating in the formation of group signatures, as the basis for the identification of the signer later. Obviously, it is necessary to save the information of those who participated in the formation of the group signature, but it makes the size of the group signature significantly increase, which is considered a limitation of this group signature scheme. Because the representative collective signature scheme is built on the basis of the AGDS scheme, this is also a limitation of the three-component representative collective signature (U, E, S).

To overcome this limitation, we change the AGDS schema, and subsequently change the representative collective signature scheme, so that it allows the creation of group signatures and representative collective signatures consisting of only sets of 2 components (E, S) [13]. Of course, it still contains all the necessary information so that it can later be identified who participated in the creation of the signing group's group signature. This information is contained in the random component (R), which is used to form the E component of the group signature, the ultimate representative collective signature.

In three-element grouping signature schemes [13], the random parameter (R) is formed from a randomly chosen numeric value (t). In a 2-component grouping signature protocol, since the information of all the signers involved in the signature generation process is embedded in the random parameter (R), the random value (T) is not chosen in the random way that it is generated by some pseudo-random value generator algorithm. The random parameter in this case not only satisfies the requirements of uniqueness, secrecy, and unpredictability but also ensures the function of protecting

the private keys of the participants in the group signature generation process of the signing group. The pseudo-random number generation algorithm used in the group signature schemes below fulfills this.

The AGDS generation procedure in this case, which generates a 2-component group signature, is performed through the following steps:

1. The set of individual signers together create a collective signature on the document M to be signed. Then, send the newly created collective signature (E_{col}, S_{col}) to the group manager.
2. The group manager uses the received collective signature (E_{col}, S_{col}), document M, and his private key z to compute a pseudo-random value T, according to a predefined algorithm.
3. Using the calculated pseudo-random value, the group manager computes the random component of the group signature (R), and then computes the two components of the team leader's signature (E, S) on document M This is also the group signature of the whole group signing on document M.

Thus, we reduce the size of the group signature and the representative collective signature [10] by not using the U element to contain the signer information, but embedding this information in the random parameter R. That is the group signature and the representative collective signature are reduced to two elements (E, S), but still contain all the necessary information to serve the identification of the signer later.

In this paper, we use the difficult problem of the discrete logarithm on prime finite fields to build both forms of collective signature schema representing 2 components: i) Collective signature shared by multiple signing groups and ii) Collective signatures shared by multiple signing groups and many individual signers. The collective signature scheme and the consent group signature scheme are used as the basis for the proposed collective signature scheme.

2 Related Basis Digital Signature Schemes

2.1 The Collective Signature Scheme Based on the Discrete Logarithm Problem (The CDS-2.1 Scheme)

This part uses the digital signature scheme described in [10] as the basic scheme to build a collective signature scheme on document M for a collective consisting of m signers. Secret key x_j and public key y_j of the j-th signer meet the conditions: $x_j < p$ and $y_j = x_j^k \ mod \ p$; (where j = 1, 2, ..., m).

The input parameters are chosen as follows: Choose a sufficiently large prime number $|p| \sim 2560$ *bites*, $p - 1$ which contains the factors r and q, $|r| = 161$ *bites* and $|q| = 256$ *bites*. Choose α and β with degrees (*modulo p*) of r and q, respectively.

The main procedures of the collective signature scheme on the document M are described below.

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

Includes the following stages:

1. Each *j-th* signer performs the following steps:
   - Choose a random value t_j, satisfying: $t_j < p$
   - Calculate the value of the random component R_j using the formula:

$$R_j = \alpha^{t_j} \ mod \ p \tag{1}$$

   - Send R_j to all other signers in the signing collective.
2. A certain signer, or all signers, in the signing collective does:

– Calculate the value of the common (public) random component of the collective R using the following formula:

$$R = \prod_{j=1}^{m} R_j \ mod \ p \tag{2}$$

– Calculate the first component E of the collective signature using the following formula:

$$E = F_H(M \ || \ R) \ mod \ 2^{80} \tag{3}$$

where F_H is a pre-specified compression function. "||" is the string concatenation operator.

3. Each *j-th* signer goes on to:
   – Calculate the value of the individual share component S_j using the formula

$$S_j = E(t_j + x_j E) \bmod r \tag{4}$$

   – Send S_j to all other signers in the signing collective.
4. A certain person, or all signers, in the signing collective calculates the second component of the S collective signature using the following formula:

$$S = S_1 + S_2 + \ldots + S_m \ mod \ r \tag{5}$$

So the value pair (E, S) is the collective signature of the signing collective consisting of m signers on document M.

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

To verificate the validity of the signature received with the document M, the verifier performs the following step:

1. Calculate the public key y using the following formula:

$$y = \prod_{j=1}^{m} y_j \ mod \ p \tag{6}$$

2. Calculate the value of the random parameter R^* using the following formula:

$$R^* = y^{-E} \alpha^{E^{-1} S} \ mod \ p \tag{7}$$

3. Calculate the value of the component E^* using the following formula:

$$E^* = F_H(M||R^*) \ mod \ 2^{80} \tag{8}$$

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-2.1 scheme:**

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

Conspicuously, the test expression $E^* = E$ always exists

$$R^* = y^{-E}\alpha^{E^{-1}S} \ mod \ p$$
$$= \alpha^{\sum_{i=1}^{m} -x_i E \ E^{-1}E\left(\sum_{i=1}^{m} t_i + x_i E\right)} \ mod \ p$$
$$= \alpha^{\sum_{i=1}^{m} t_i} \ mod \ p$$
$$= \prod_{i=1}^{m} R_i \bmod p = R$$

as $R^* = R$, $E^* = F_H(M||R^*) = F_H(M||R) = E$

Thus, the test expression $E^* = E$ always exists This proves that the correctness of the signature check procedure, or the correctness of the CDS-2.1 scheme, is always guaranteed.

2.2 The Approved Group Signature Scheme Based on the Discrete Logarithm Problem (The GDS-2.2 Scheme)

This section describes the two-component approved group signature scheme. The signing group in this case consists of m signers and one who plays the role of group manager. The input parameters are selected as shown in the CDS-2.1 scheme. M is the document that needs to have a group signature on it.

Each signer generates a random secret number to serve as the private key. The public key y_j is calculated by the formula: $y_j = \alpha^{x_j} \ mod \ p; j = 1, \ 2, \ 3, \ldots, m$; The group manager (GM) also chooses a random secret number z, $z < q$, as the private key. GM's public key is: $Y = \alpha^z \ mod \ p$. This Y is also the public key of the signing group.

The main procedures of the two-component approved group signature scheme on the document M are described below.

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

The group signature in this case is formed through two stages:

i) Creating a collective signature on document M, made by a collective of m individual signers;
ii) On the basis of the collective signature that has just been created, the group manager creates a group signature of 2 components, representing the whole signing group

1. Individual signers create a collective signature on the document *M:*

1.1. Each i signer generates a random number t_i, $t_i < r$, and then computes R_i:

$$R_i = \alpha^{t_i} \bmod p \tag{9}$$

Then send R_i to the other signers in the signing group ($i = 1, 2, \ldots, m$).

1.2. Any signer in the group, or all, calculate R_{col}:

$$R_{col} = (R_1 R_2 \ldots R_m) \bmod p = \alpha^{t_1 + t_1 + \ldots + t_m} \bmod p \tag{10}$$

And calculate E_{col} :

$$E_{\text{col}} = F_H(M \ || \ R_{\text{col}}) \ mod \ 2^{80} \tag{11}$$

where: F_H is a given hash function, the value of E_{col} is the first element in the collective signature.

1.3. Each i signer calculate the personal share value S_i:

$$S_i = E_{\text{col}}(t_i + x_i E_{\text{col}}) \bmod r \tag{12}$$

Then, sends S_i to other signers in the signing group.

1.4. Any signer in the signing group, or all, calculate S_{col}:

$$S_{\text{col}} = (S_1 + S_2 + \ldots + S_m) \bmod r \tag{13}$$

So the tuple (E_{col}, S_{col}) is the collective signature of a signing group of m members. The length of the signature is: $|E_{\text{col}}| + |S_{\text{col}}| \approx 240$ bit.

This collective signature is forwarded to the group manager,

2. The group manager checks the validity of the received collective signature (E_{col}, S_{col}) by checking the precision of the following expression:

$$R_{\text{col}} = y_{\text{col}}^{-E_{\text{col}}} \alpha^{E_{\text{col}}^{-1} S_{\text{col}}} \bmod p \tag{14}$$

where:

$$y_{\text{col}} = (y_1 y_2 \ldots y_m) \bmod p \tag{15}$$

If the collective signature is valid, the group manager will calculate the pseudo-random value T:

$$T = (E_{\text{col}} \,||\, S_{\text{col}})^{z^*} H_z \; mod \; q \tag{16}$$

where: $H_z = F_H(M,\ z) \; mod \; q$ and

$$z^* = \min\{z_i:\ z_i = z + i;\ \gcd(z_i,\ q-1) = 1;\ i = 0,\ 1,\ 2, \ldots\} \tag{17}$$

3. The group manager calculates the values R, E and S as follows:

$$R = \alpha^T \bmod p, \tag{18}$$

$$E = F_H(M \,||\, R) \; mod \; 2^{128} \tag{19}$$

$$S = E(T + zE) \bmod q \tag{20}$$

Thus, the tuple (E, S) is the two-component approved group signature of the signing group including m signers and the group manager on the document M.

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

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

1. Calculate the value of the random parameter R^* using the following formula:

$$R^* = Y^{-E} \; \alpha^{E^{-1} S} \; mod \; p \tag{21}$$

2. Calculate the value of component E^* using the following formula:

$$E^* = F_H(M||R^*) \; mod \; 2^{128} \tag{22}$$

3. 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 GDS-2.2 scheme:**

The correctness 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 collective signature test formula R_{col} and iii) The existence of the test expression $E^* = E$. Detailed as follows:

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

It is easy to see that the shared signature checking formula is always correct:

$$\begin{aligned} R_j &= y_i^{-E}\, \alpha^{E^{-1}S_i} \bmod q \\ &= \alpha^{-x_i E}\, \alpha^{E^{-1}E(t_i + x_i E)} \\ &= \alpha^{t_i} = R_j \end{aligned}$$

b) The correctness of the formula for checking collective signatures:

It is easy to see that the collective signature checking formula is always correct:

$$\begin{aligned} R_{col} &= y_{col}^{-E_{col}} \alpha^{E_{col}^{-1} S_{col}} \bmod p \\ &= \alpha^{\sum_{i=1}^{m} -x_i E}\, \alpha^{E^{-1}E\left(\sum_{i=1}^{m} t_i + x_i E\right)} \bmod p \\ &= \alpha^{\sum_{i=1}^{m} t_i} \bmod p \\ &= \prod_{i=1}^{m} R_i \bmod p = R_{col} \end{aligned}$$

c) The correctness of the group signature checking procedure:

Conspicuously, the signature checking expression $E^* = E$ always exists:

$$\begin{aligned} R^* &= Y^{-E}\, \alpha^{E^{-1}S} \bmod p \\ &= \alpha^{-zE}\, \alpha^{E^{-1}E(T+zE)} \bmod p \\ &= \alpha^{T} \bmod p = R \end{aligned}$$

And calculates:

$$\begin{aligned} E^* &= F_H(M||R^*) \bmod 2^{128} \\ &= F_H(M||R) \bmod 2^{128} = E \end{aligned}$$

Thus, the expression $E^* = E$ always exists: This proves that the correctness of the signature checking procedure, or the correctness of the GDS-2.2 scheme is always guaranteed.

3 Constructing the Proposed Collective Digital Signature Schemes Based on the Discrete Logarithm Problem on Prime Finite Field

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

This scheme generates a collective signature for g signing groups, with the public key of each group manager (GM), and the public key of each signing group: $Y_j = X_j^k \ mod \ p$; with $j = 1,\ 2,\ \ldots,\ g$, and X_j is the secret key of j-th GM.

Suppose that the j-th group consists of m_j individual signers. M is a document to be signed on.

The protocol of collective signatures for signing groups is descibed as follows:

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

Including these following steps:

1. Each j-th group generates a group signature according to the GDS-2.2 signing group scheme above and then send R_j to all the remaining groups in the signing pool.
2. A certain GM in the collective, or all, calculates the values of R and E by the following formulas:

$$R = \prod_{j=1}^{g} R_j \ mod \ p \tag{23}$$

$$E = F_H(M||R) \ \ mod \ 2^{128} \tag{24}$$

E is the first component of the collective signature.

3. GM of each j-th signing group continues to execute:
   - Calculate the shared composition S_j of the signing group:

$$S_j = E(T_j + z_j E) \bmod q \tag{25}$$

   - Send S_j to all other GM in the signing group.
4. A certain GM in the collective, or all, does the final works:
   - Verify the precision of the shared component S_j of each signing group by the following formula:

$$R^* = Y_j^{-E} \alpha^{E^{-1} S_j} \ mod \ p \tag{26}$$

   - If all S_j satisfied the test formula, then the third element S of the collective signature is calculated by the formula:

$$S = \sum_{j=1}^{g} S_j \ mod \ p \tag{27}$$

Thus, the value par (E, S) is the collective digital signature, two components, of a collective of g signing groups on the document M.

- **The procedure to verification the collective digital signature for *g* group signing on the document M:**

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

1. Calculate collective public key Y_{col} using the formula:

$$Y_{col} = \prod_{j=1}^{g} Y_j \ mod \ p \tag{28}$$

2. Calculate the R^* using the following formula:

$$R^* = Y_{col}^{-E} \alpha^{E^{-1}S} \ mod \ p \tag{29}$$

3. Calculate the E^* using the following formula:

$$E^* = F_H(M||R^*) \ mod \ 2^{128} \tag{30}$$

4. Compare E^* with E. If $E^* = E$: The received signature is valid; otherwise, it is invalid and will be rejected.

- **The proof of the correctness of the RCS.01-3.1 scheme:**

The precision of this representative collective signature scheme is shown through: i) The existence of a shared signature verification formula shared by the signing team leaders; and ii) Existence of the test expression in the signature check procedure.

a) Prove the correctness of the member's signature:

It is easy to see that the shared signature checking formula S_j shared by the signing team leaders always exists:

$$\begin{aligned} R_j^* &= Y_j^{-E} \ \alpha^{E^{-1}S_j} \ mod \ p \\ &= \alpha^{-z_j E} \ \alpha^{E^{-1}E(T_j + z_j E)} \ mod \ p \\ &= \alpha^{T_j} \ mod \ p = R_j \end{aligned}$$

b) Prove the correctness of the last signature:

Conspicuously, the signature check expression $E^* = E$ always exists:

$$R^* = Y_{col}^{-E}\alpha^{E^{-1}S} \ mod \ p$$

$$= \prod_{j=1}^{g}(Y_j^{-E})\alpha^{E^{-1}\sum_{j=1}^{g} S_j} \bmod p$$

$$= \prod_{j=1}^{g}(\alpha^{-z_jE})\alpha^{E^{-1}\sum_{j=1}^{g} E(T_j+z_jE)} \bmod p$$

$$= \prod_{j=1}^{g}(\alpha^{-z_jE})\prod_{j=1}^{g}(\alpha^{T_j+z_jE}) \bmod p$$

$$= \prod_{j=1}^{g}\alpha^{T_j} \ mod \ p = \prod_{j=1}^{g} R_j \bmod p = R$$

as $R^* = R$:

$$E^* = F_H(M||R^*) \ mod \ 2^{128}$$

$$= F_H(M||R) \ \ mod \ 2^{128} = E$$

Thus, the expression $E^* = E$ always exists: This proves that the correctness of the signature checking procedure scheme is always guaranteed.

From (a) and (b): The correctness of the RCS.01-3.1 scheme is guaranteed.

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

Suppose there is a signing collective consisting of *g* signing groups and *m* individual signers, and want to create a representative collective signature on the document M. Assume that the *j-th* signing group consists of *m* signing members (m_j), these people are designated to participate in the formation of the group signature of the *j-th* signing group (j = 1, 2, ..., g), and each individual signer is considered as a one-member signing group.

The input parameters, secret key, public key ... are selected and calculated as the scheme RCS.01-3.1.

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

Including these steps:

1a. The GM of each group performs:
  - Generate a group signature according to the scheme for the GDS-2.2 signing group above and then send R_j to all GM of the signing groups in the signing collective.
  - R_j is the shared component of the *j-th* signing group used to generate a random parameter of the collective signature.

1b. Each *j-th*:
- Choose a random number t_j and calculate the random value R_j using the following formula:

$$R_j = \alpha^{t_j} \ mod \ p \tag{31}$$

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

2. A GM or an individual signer in the collective calculates the values of R and E by using the following formula:

$$R = \prod_{j=1}^{g+m} R_j \tag{32}$$

$$E = F_H(M||R) \ mod \ 2^{128} \tag{33}$$

where: $j = 1,\ 2,\ 3,\ \ldots,\ g+m$. E is the first element of the signature.

3a. GM of each j-th group will:
- Calculate the shared component S_j of the j group by using the following formula:

$$S_j = E(T_j + z_j E) \bmod q \tag{34}$$

- Send S_j to other GM-s and other individual signers in the signing collective.

3b. Each *j-th* individual signer j ($j = g+1,\ g+2,\ \ldots,\ g+m$) will:
- Calculate their shared component S_j by the following formula:

$$S_j = E(t_j + x_j E) \bmod q \tag{35}$$

- Send S_j to other GM-s and other individual signers in the signing collective.

4. A GM or an individual signer in the signing collective will:
- Check the validity of each S_j by using the following formula:

$$R_j = Y_j^{-E} \ \alpha^{E^{-1} S_j} \ mod \ p \tag{36}$$

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

$$R_j = y_j^{-E} \ \alpha^{E^{-1} S_j} \ mod \ p \tag{37}$$

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

- If all the conditions are satisfied, the third component of the group signature will be calculated by the formula:

$$S = \sum_{j=1}^{g+m} S_j \ mod \ p \tag{38}$$

Thus, the value pair (E, S) is a collective signature, two components, of a collective consisting of g signing groups and m individual signers on the document M. It represents this collective signing.

- **The procedure for verification the collective digital signature for multiple signing groups and 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 by using the following formula:

$$Y_{col} = \prod_{j=1}^{g} Y_j \prod_{j=g+1}^{g+m} y_j \ mod\ p \tag{39}$$

2. Calculate the random parameter value by using the following formula:

$$R^* = Y_{col}^{-E} \alpha^{E^{-1}S} \ mod\ p \tag{40}$$

3. Calculate the E^* using the following formula:

$$E^* = F_H(M||R) \ mod\ 2^{128} \tag{41}$$

4. Compare E^* with E. If $E^* = E$: The received signature is valid; otherwise, it is invalid and will be rejected.

- **The proof of the correctness of the RCS.02-3.2 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; ii) The existence of the signature test formula shared S_j by each individual signer and iii) The existence of the test expression $E^* = E$.

a) The correctness of the formula to check the shared signature of m group managers:

Conspicuously, the formula for checking the shared signature of each group manager always exists:

$$\begin{aligned} R_j^* &= Y_j^{-E}\, \alpha^{E^{-1}S_j} \ mod\ p \\ &= \alpha^{-z_jE}\, \alpha^{E^{-1}E(T_j+z_jE)} \ mod\ p \\ &= \alpha^{T_j} \ mod\ p = R_j \end{aligned}$$

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

Conspicuously, the formula for checking the shared signature of each group manager always exists:

$$\begin{aligned} R_j^* &= y_j^{-E} \alpha^{E^{-1}S_j} \ mod\ p \\ &= \alpha^{-x_jE}\, \alpha^{E^{-1}E(T_j+x_jE)} \ mod\ p \\ &= \alpha^{t_j} \ mod\ p = R_j \end{aligned}$$

c) The correctness of the procedure for checking the representative collective signature:

Conspicuously, the signature checking expression $E = E^*$ always exists.

$$
\begin{aligned}
R^* &= Y_{col}^{-E}\alpha^{E^{-1}S} \; mod \; p \\
&= \prod_{j=1}^{g} Y_j^{-E} \prod_{j=g+1}^{g+m} y_j^{-E} \alpha^{E^{-1}\sum_{j=1}^{g+m} S_j} \bmod p \\
&= \prod_{j=1}^{g} (Y_j^{-E}\alpha^{E^{-1}S_j}) \prod_{j=g+1}^{g+m} (y_j^{-E}\alpha^{E^{-1}S_j}) \bmod p \\
&= \prod_{j=1}^{g} R_j \prod_{j=g+1}^{g+m} R_j \bmod p \\
&= \prod_{j=1}^{g+m} R_j \bmod p = R
\end{aligned}
$$

and calculate:

$$
\begin{aligned}
E^* &= F_H(M \parallel x_{R^*} \parallel x_U) \; mod \; \delta \\
&= F_H(M \parallel x_R \parallel x_U) \; mod \; \delta \\
&= E
\end{aligned}
$$

Thus, the expression $E^* = E$ always exisits: This proves that the precision of the signature checking precedure, or the precision of the RCS.02-3.2 scheme is always guaranteed.

From (a), (b) and (c): The correctness of the RCS.02-3.2 scheme is guaranteed.

4 Security Analysis and Performance Evaluation

4.1 Security Advantages of the Proposed Collective Signature Schemes

The approved group signature and the approved group signature scheme has the following security advantages:

- The group signature in this paper is built based on the discrete logarithm problem on the prime finite field, so it inherits all the security advantages of this difficult problem. The same is true for the group approved digital signature scheme.
- Signing group members and the group manager can both use a pair of their private key and public key for both purposes: Forming private signatures and participating in group signature formation. As a result, this scheme can be fully deployed on existing PKI (Public Key Infrastructure) systems [14].
- The signer's private key and secret keys are not used directly in the group signature formation process, nor are they passed on to the group manager and other members of the signing group. In this case, the security and privacy of the values involved are guaranteed.
- Using the group manager's public key Y as the public key of the signing group makes it possible both to check the validity of the signature (of the verifier) and to change the set of participants that form the signature (of the group manager) have become much more convenient.
- The random parameters t_i is treated as the second secret key of the signing group member. Unlike the first secret key, the private key, t_i randomly chosen for each signature generation, i.e., it is used only once. This results in also a random and unique R component in each

group signature generated on document M. The "single-use" here enables the signing collective to generate different signatures across documents are different, although they still use the same original public key and private key pair. Thus, it is difficult for an attacker to use the signature collection method of the signing group on different documents to find out the secret components in the received signature set.

The proposed representative collective signature scheme is built on the basis of the approved group signature scheme, so it fully inherits the advantages of this scheme.

4.2 Performance of the Proposed Collective Signature Schemes

We evaluate the computational performance of the two-element 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.

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 [15]: $T_h \approx T_m,\ T_s \approx 29T_m,\ T_{inv} \approx 240T_m,\ T_e \approx 240T_m, T_{sqrt} \approx 290T_m$.

Information from Tab. 1 shows that the time cost for signature generation and signature checking of a two-element representative signature scheme is not much reduced compared to a three-element scheme [10], of course, if both Both schemes are built on the same difficult problem and/or the same digital signature standard. The advantage of the new representative collective signature scheme is that it still produces a shorter collective signature, but still ensures the security level and meets the basic requirements of a representative collective signature scheme.

Table 1: Time cost of the proposed collective signature scheme: RCS.01-3.2 and RCS.02-3.3

The scheme	Time for the signature generation	Time for the signature verification
RCS.01-3.1	$E = \left[\sum_{j=1}^{g}(244m_j + 1204) + 1\right] T_m$ $S = (724g)T_m$ $Sum = \left[\sum_{j=1}^{g}(244m_j + 1928) + 1\right] T_m$	$(723 + g)T_m$
RCS.02-3.2	$E = \left[\sum_{j=1}^{g}(244m_j + 1204) + 241m + 1\right] T_m$ $S = (724g + 724m)T_m$ $Sum = \left[\sum_{j=1}^{g}(244m_j + 1928) + 965m + 1\right] T_m$	$(723 + g + m)T_m$

5 Discussion

The pseudo-random number generation algorithm T [13] that we use is guaranteed to contain all the information of everyone who participated in informing the signature and it is also easy to identify the signer later. Indeed, when it comes to identifying those who have previously participated in the formation of the consent group signature, the group manager only needs to perform the following steps:

– Use the group signature (E, S) to recalculate T by using the following formula:

$$T = SE^{-1} - zE \bmod q \tag{42}$$

– Calculate:

$$H_z = F_H(M,\ z)\ mod\ q, \tag{43}$$

– And then recalculate the collective signature value using the formula:

$$E_{\text{col}}||S_{\text{col}} = (TH_z^{-1})^{z^{-1}\ mod\ (q-1)} \tag{44}$$

– Select a signing group (subset) consisting of any m members from the signing collective (this is a group of signers selected from the signing collective, they are assigned the task of creating a collective signature on document M): Use public key of this signing group to generate the collective public key. Use the newly computed collective public key to recalculate the $E_{col}||S_{col}$: If this value is equal to the $E_{col}||S_{col}$ of (44), it is the people in this signing group who participated in the generation of the set signature body of collective sign; Otherwise, the group manager will choose another signing group and do the same until they find a signing group whose public key results in a matching E_col||S_col value pair (44). That is, iterate until the identifier is signed by the signers who have participated in the creation of the collective signature, then stop (Here accepted: The probability of coincidence is negligible).

6 Conclusion

A representative collective signature is a form of signature formed by a group of signatures whose members are drawn from different signing groups and/or are from individuals of the same level with the signatories. It is a requirement of this type of signature that it contains information regarding all signers who participated in the signing process. This information is needed for the identification of the signer and to solve the "repudiation" responsibility issue later. We have proposed and implemented a representative collective signature scheme that only has two components (E, S) while still meeting the requirements for a representative scheme.

In [13], we proposed a approved group signature protocol that entails two components. The advantages of this protocol are i) All signer information is embedded in the collective signature (E_{col}, S_{col}), precisely in the pseudo-random parameter T; ii) The group manager can easily identify all those who participated in the formation of the group's consent group signature, this is possible thanks to the special structure of the parameter T; and iii) Only the group manager can perform the "opening" of the group signature to identify the signer since only this person knows must know the secret key z, a very important component in T.

In addition to having the same security advantages of the three-component signature scheme and the consensus group signature protocol, the two-component collective signature scheme also exhibits the following capabilities: i) Helps to create signatures of shorter size, equal to $|E| + |S|$, but keeping the same level of security; ii) Helps to reduce time costs for signature generation and signature

checking process. To achieve these advantages, the U component is removed from the signature, with the information of all signers whose signatures were used to form the signature stored in a pseudo-random parameter.

In this paper, we use the discrete logarithm problem on a prime finite field to build the proposed collective signature, hence the signature size and time cost for the signature formation/checking process not significantly reduced. We have reason to believe that, if we use the discrete logarithm problem on the elliptic curve [16,17], combined with the GOST R34.10-2012 signature standard [18,19], to build a collective signature scheme representing two components, signature size, and associated time costs will be greatly reduced. This is our future work.

Funding Statement: We received funding for this research from Duy Tan University, Danang, 550000, 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] National Institute of Standards and Technology, "Digital signature standard," in *FIPS Publication 186-3*, 2009.
[2] J. Pieprzyk, T. Hardjono and J. Seberry, *Fundamentals of Computer Security*. Berlin: Springer-Verlag, 2003.
[3] K. Itakura and K. Nakamura, "A public key cryptosystem suitable for digital multisignatures," *NEC Research and Development*, vol. 71, pp. 1–8, 1983.
[4] 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*, vol. 950, Berlin Heidelberg New York, Springer-Verlag, pp. 428–432, 1995.
[5] D. Chaum, "Blind signatures for untraceable payments," in *Proc. Advances in Cryptology–CRYPTO'82*, Plenum Press, pp. 199–203, 1983.
[6] Q. Alamélou, O. Blazy, S. Cauchie and P. Gaborit, "A Code-based group signature scheme," *Designs, Codes and Cryptography*, vol. 82, no. 1–2, 2017.
[7] 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, 2016.
[8] A. A. Moldovyan and N. A. Moldovyan, "Group signature protocol based on masking public keys," *Quasigroups and Related Systems*, vol. 22, pp. 133–140, 2014.
[9] 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.
[10] 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*, India, 2018.
[11] 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.
[12] 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," vol. 13, no. 4, pp. 59–69, 2021.
[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] H. Yong, C. Fugui and Q. Peixin, "Research on digital signature based on digital certificate," in *Proc: Proc. of 14th Youth Conf. on Communication*, Scientific Research, pp. 467–470, 2009.

[15] C. Popescu, "Blind signature and BMS using elliptic curves," *Studia Univ Babes–Bolyai*, Informatica, pp. 43–49, 1999.
[16] A. A. Bolotov, S. B. Gashkov and A. B. Frolov, "Elementary introduction to elliptic curve cryptography," in *Cryptography Protocols on the Elliptic Curves*, KomKniga, Moskow, 2006.
[17] D. Johnson, A. J. Menezes and S. Vanstone, "The elliptic curve digital signature algorithm," *Certicom*, 2001.
[18] Government Committee of the Russia for Standards, "GOST R34.10-2012: Russian Federation Standard," *Cryptographic Data Security, Produce and Check Procedures of Electronic Digital Signature*, 2012.
[19] A. Beresneva, A. Epishkina, O. Isupova, K. Kogos and M. Shimkiv, "Special digital signature schemes based on GOST R 34.10-2012," in *Proc: Electrical and Electronic Engineering Conf. (EIConRusNW)*, IEEE NW Russia Young Researchers, 2016.