Constructing New Representative Collective Signature Using the GOST R34.10-2012

Tuan Nguyen Kim[1], Duy Ho Ngoc[2], and Nikolay A. Moldovyan[3]
[1] School of Computer Science - Duy Tan University, Da Nang, 550000, Vietnam
[2] Department of Information Technology, Ha Noi, 100000, Vietnam
[3] ITMO University, St.Petersburg, Russia
Email: nguyenkimtuan@duytan.edu.vn; hoduy027@gmail.com; nmold@mail.ru

***Abstract*–**A representative collective signature is a signature created by a collective of multiple signing groups. The basic requirement for this signature is that it must include information about all participants involved in the signing process of a given document. The U component in the 3-component collective signature (including U, E, S) is used to satisfy this requirement. In this paper, we propose a new form of representative collective signature consisting of only two components (e, s), then, the information of all signers is contained in the pseudo-random parameter R. The purpose of this is both to reduce the size of the signature, as well as ensure that the manager of the signing group has enough information to identify the signer and to prevent "disclaimer" during a dispute. In the proposed collective signature scheme, we use the GOST R34.10-2012 digital signature standard to develop a consensus group signature scheme based on the discrete logarithm problem on the Elliptic curve. This scheme allows the generation of a representative collective signature: i) Only 512 bits in length, but still achieves security level 2^{512} and ii) Significantly reduced computational performance (in comparison to the representative collective signature that represents the three components).

***Index Terms*–**GOST R34.10-2012 signture standard, collective digital signature, group digital signature, EC discrete logarithm problem, pseudo-random parameter

I. Introduction

Digital signatures [1] are one of the major applications of asymmetric cryptosystems. Currently, there are many digital signature-based authentication systems deployed in cyberspace. Not only do these systems meet the requirements of information exchange partner authentication and information origin authentication, but they also ensure the integrity of information transmitted on the network and address the issue of “disclaimer” of responsibility when a dispute arises over liability.

The first studied and standardized form of digital signature was the single digital signature [2], which was created only by a private signer, who possessed the asymmetric key pair, the private key, and the public key. Therefore, a single signature only authenticates the person who created the signature on the signed document.

A signature generated by a signer is validated by using their public key. A blind digital signature [3], [4] is also a form of a single digital signature, but the signer is not allowed to see the contents of the document they are asked to sign. To meet the authentication requirements of a collective signing, multiple different types of digital signatures have been researched and published such as collective digital signature [5]-[7], blind collective signature [8]-[10], consenting group digital signature, blind group digital signature [11], representative collective signature [10], [12]... Representative collective signature is a type of signature formed from a collective signing in which the members of this collective are representatives for other signing groups, each signing group consists of many members. This collective also has individual signers, they do not belong to any signing group, they are considered as representatives of the signing group with no members. The representative group signature scheme is developed from the advantages of the collective signature scheme and the group signature scheme.

Digital multi-signature [13] types such as group signatures, collective signatures, and representative collective signatures are all made up of a certain number of signers. Each member of the group indirectly contributes to the creation of a unique signature for the group using their secret values and private keys. Validation of all members of this signing group is performed only once on their shared signature. The public key of the signer set, formed from the public key of those who participated in creating the group signature, or the public key of the representative used in this authentication process.

The basic requirement of multi-signature schemes, namely group signatures and representative collective signatures, is to store the information of all members who have participated in the formation of the signature of the group or the collective. This information is necessary for the identification of the signer and the subsequent resolution of the signer's "disclaimer". The storage of this information must ensure that, when there is a conflict or "disclaimer" related to the group signature or the generated representative collective signature, the group manager signs it, and only with this person, it is easy to perform the "opening" of the signature to accurately identify all those who participated in the process of forming the collective signature of the signing group or the signing group.

Manuscript received November 14, 2021; revised May 18, 2022.
Corresponding author email: nguyenkimtuan@duytan.edu.vn
doi:10.12720/jcm.17.6.478-485

Therefore, most group signatures and representative collective signatures are designed with 3 components, one of which is used to store signer information, this is to increase the size of the signature. increased significantly, this is considered a limitation of this 3-component signature. We think that group signatures [12] and collective signatures representing two components can overcome this limitation.

The new type of representative collective signature scheme that we propose allows the creation of a 2-component collective signature, but still fully stores the information of all who participated in the formation of the common signature of the signing collective. In this scheme, we use a pseudo-random parameter t to contain the signer information. The random number generator algorithm is designed to ensure the "opening" of the signature for later identification of the signer.

In this study, we first construct a two-component consent group signature scheme, then create a two-component collective signature scheme based on it. We rely on the discrete logarithm problem on Elliptic curves [14], [15] and use the GOST R34.10-2012 digital signature standard [16]-[18] to build these types of schemes. Both forms of two-component collective signature schemes have been developed following this approach: i) Collective signatures are shared by multiple signing groups, and ii) Collective signatures are shared by many signing groups and many individual signers. As shown in the research, compared with the three-component collective signature scheme, the proposed schemes not only reduce the size of the signature and improve computational performance but also guarantee the security level and satisfy the requirement of storing signer's information.

II. The Related Basis Digital Signature Scheme

The basic scheme of two-component collective signature schemes is a two-component group signature scheme, so we must first construct a group signature scheme of this type.

The group signature scheme in this section is built based on the elliptic curve discrete logarithm problem using the GOST R 34.10-2012 signature standard.

Suppose: Two curves EC1 and EC2 have degrees #E1 and #E2, defined in the prime finite field GF(p); w and q are two prime numbers of magnitude 256 and 520 bits respectively, satisfying w|#E1 and q|#E2; G1 is a point of degree w on the EC1 curve and G2 is a point of order q on the EC2 curve; The signing group consists of m members, excluding the group leader.

The private key of the *j-th* signer is a random number k_i, $k_i < w$. This person's corresponding public key is $P_i = k_i G_1$. The private key and the public key of the group manager are z $(z < q)$ and L, satisfying $L = zG_2$. L is also the public key of the signing group.

This scheme (The GDS-2.2 schme) includes the following procedures:

- *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.

Specifically as follows:

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

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

$$R_i = t_i G_1 \quad (1)$$

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

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

$$R_{\text{col}} = R_1 + R_2 + \ldots + R_m \quad (2)$$

and

$$r_{col} = x_R \bmod w \quad (3)$$

where x_R is the first coordinate of the point R_{col}.

Then calculate e_{col}:

$$e_{\text{col}} = F_H(M||x_R) \bmod w \quad (4)$$

where F_H is a given hash function.

The value of e_{col} is the first element in the collective signature. Then, sent e_{col} to the other signers in the signing group.

1.3. Each *i* signer calculate the personal share value s_i:

$$s_i = (t_i + e_{col} k_i) \bmod w \quad (5)$$

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

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

$$s_{\text{col}} = (s_1 + s_2 + \ldots + s_m) \bmod w \quad (6)$$

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:

$$R_{\text{col}} = s_{\text{col}} G_1 - e_{\text{col}} P_{\text{col}} \quad (7)$$

where:

$$P_{\text{col}} = P_1 + P_2 + \ldots + P_m \quad (8)$$

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

$$t = (e_{\text{col}} \,||\, s_{\text{col}})^{z^*} H_z \bmod q, \quad (9)$$

where:

$$H_z = F_H(M, z) \bmod q \quad (10)$$

and

$$z^* = \min\{z_i: z_i = z + i;\ \gcd(z_i, q-1) = 1;\ i = 0, 1, 2, \dots\} \quad (11)$$

3. The group manager calculates the values *R*, *e* and *s* as follows:

$$R = tG_2 \quad (12)$$

$$e = F_H(M||x_R) \bmod w \quad (13)$$

$$s = t + ez \bmod q \quad (14)$$

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:

$$R^* = sG_2 - eL \quad (15)$$

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

$$e^* = F_H(M||R^*) \bmod w \quad (16)$$

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:

$$\begin{aligned} R_i^* &= s_i G_1 - e_{col} P_i \\ &= (t_i + e_{col} k_i) G_1 - e_{col} k_i G_1 \\ &= tG_1 = R_i \end{aligned}$$

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

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

$$\begin{aligned} R_{col}^* &= s_{col} G_1 - e_{col} P_{col} \\ &= (s_1 + s_2 + \cdots + s_m) G_1 \\ &\qquad - e_{col}(P_1 + P_2 + \cdots + P_m) \\ &= \big((t_1 + e_{col} k_1) + \cdots + (t_m + e_{col} k_m)\big) G_1 \\ &\qquad - e_{col}(k_1 G_1 + \cdots + k_m G_1) \\ &= t_1 G_1 + \cdots + t_m G_1 \\ &= R_1 + \cdots + R_m = R_{col} \end{aligned}$$

c) The correctness of the group signature checking procedure:

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

$$\begin{aligned} R^* &= sG_2 - eL \\ &= (t + ez)G_2 - ezG_2 \\ &= tG_2 = R \end{aligned}$$

and calculates:

$$\begin{aligned} e^* &= F_H(M||R^*) \bmod w \\ &= F_H(M||R) \bmod w = e \end{aligned}$$

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.

III. The Proposed Group Digital Signature Schemes

In this section, we propose and build a new form of representative collective signature, which is a two-component representative collective signature. We use the GOST R34.10-2012 digital signature standard and the discrete logarithm problem on the elliptic curve to build this scheme. The group signature scheme described in section II is the basic scheme of this scheme.

A. Constructing the Two-Element Collective Digital Signature Scheme for Signing Groups (The RCS.01-3 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: $L_j = z_j G_2$; with $j = 1, 2, \dots, g$, and z_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:

$$R = \sum_{j=1}^{g} R_j \quad (17)$$

and

$$r = x_R \bmod w, \quad (18)$$

where x_R is the first coordinate of the point R_{col}, calculate e:

$$e = F_H(M||x_R) \bmod w \quad (19)$$

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:

$$s_j = t_j + ez_j \ mod \ q \quad (20)$$

- 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:

$$R_j^* = s_j G_2 - eL_j \quad (21)$$

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

$$s = \sum_{j=1}^{g} s_j \ mod \ w \quad (22)$$

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:

$$L_{col} = L_1 + L_2 + \ldots + L_g \quad (23)$$

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

$$R_{\text{col}}^* = sG_2 - eL_{\text{col}} \quad (24)$$

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

$$e^* = F_H(M||x_{R^*}) \ mod \ w \quad (25)$$

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 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:

$$\begin{aligned} R_j^* &= s_j G_2 - eL_j \\ &= (t_j + ez_j)G_2 - ez_j G_2 \\ &= t_j G_2 = R_j \end{aligned}$$

b) Prove the correctness of the last signature:

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

$$\begin{aligned} R^* &= sG_2 - sL_{\text{col}} \\ &= (s_1 + s_2 + \cdots + s_g)G_2 \\ &\quad - e(L_1 + L_2 + \cdots + L_g) \\ &= \left((t_1 + ez_1) + \cdots + (t_g + ez_g)\right)G_2 \\ &\quad - e(z_1 G_2 + \cdots + z_g G_2) \\ &= t_1 G_1 + \cdots + t_g G_2 \\ &= R_1 + \cdots + R_g = R \end{aligned}$$

as $R^* = R$:

$$\begin{aligned} e^* &= F_H(M||x_{R^*}) \ mod \ w \\ &= F_H(M||x_R) \ mod \ w = e \end{aligned}$$

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 scheme is guaranteed.

B. Constructing the Two-Element Collective Digital Signature Scheme for Signing Groups and Individual Signers (The RCS.02-3 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 $(j = 1, 2, \ldots, g)$, 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.

- *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 radom value R_j using the following formula:

$$R_j = t_j G_2 \quad (26)$$

- 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:

$$R = R_1 + R_2 + \ldots + R_{g+m} \quad (27)$$

And

$$r = x_R \ mod \ w$$

where x_R is the first coordinate of the point R_{col}. Calculate e:

$$e = F_H(M||x_R) \ mod \ w \quad (28)$$

where $j = 1, 2, 3, \dots, g + m$. 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:

$$s_j = t_j + ez_j \ mod \ q \quad (29)$$

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

3b. *Each j-th* individual signer j ($j = g + 1, g + 2, \dots, g + m$) will:

- Calculate their shared component S_j by the following formula:

$$s_j = \left(t_j + ek_j\right) mod \ q \quad (30)$$

- 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:

$$R_j^* = s_j G_2 - eL_j \quad (31)$$

with $j = 1, 2, \dots, g + m$ and

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

$$s = s_1 + s_2 + \dots + s_{g+m} \ mod \ w \quad (32)$$

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:

$$L_{col} = L_1 + L_2 + \dots + L_{g+m} \quad (33)$$

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

$$R^* = sG_2 - eL_{\text{col}} \quad (34)$$

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

$$e^* = F_H(M||x_{R^*}) \ mod \ w \quad (35)$$

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 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:

$$\begin{aligned} R_j^* &= s_j G_2 - eL_j \\ &= \left(t_j + ez_j\right)G_2 - e_{col} z_j G_2 \\ &= t_j G_2 = R_j \end{aligned}$$

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:

$$\begin{aligned} R_j^* &= s_j G_2 - eL_j \\ &= \left(t_j + ek_j\right)G_2 - e_{col} k_j G_2 \\ &= t_j G_2 = R_j \end{aligned}$$

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

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

$$\begin{aligned} R^* &= sG_2 - eL_{col} \\ &= \left(s_1 + s_2 + \dots + s_{g+m}\right)G_2 \\ &\qquad - e\left(L_1 + L_2 + \dots + L_{g+m}\right) \\ &= \Big(\left(t_1 + ez_1\right) + \dots + \left(t_g + ez_g\right) \\ &\qquad + \left(t_{g+m} + ek_{g+1}\right) \dots \\ &\qquad + \left(t_{g+m} + ek_{g+m}\right)\Big) G_2 \\ &\qquad - e\left(z_1 G_2 + \dots + z_g G_2 + k_{g+1} G_2\right. \\ &\qquad \left. + \dots + k_{g+m} G_2\right) \\ &= t_1 G_1 + \dots + t_{g+m} G_2 \\ &= R_1 + \dots + R_{g+m} = R \end{aligned}$$

and calculate:

$$\begin{aligned} e^* &= F_H(M \parallel x_{R^*}) \ mod \ w \\ &= F_H(M \parallel x_R) \ mod \ w = e \end{aligned}$$

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 scheme is always guaranteed.

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

IV. Security Analysis and Performance Evaluations

A. Security Advantages of the Proposed Collective Signature Schemes

The 2-component consent group signature and the 2-component consent group signature scheme in this study have the following security advantages:

- The system was developed using the discrete logarithm problem on an elliptic curve and the GOST R34.10-2012 digital signature standard, so it retains all the advantages of this difficult problem and cryptographic system. The security level of the GOST R34.10-2012

digital signature standard has been verified, so the group signature scheme here is feasible and has a high level of trust.

- When forming a group signature, no private and/or private keys need to be exchanged between members of the signing group and/or between a member of the signing group and the group manager, these values are used indirectly. Thereby: i) Confidentiality and privacy of related values are always guaranteed, and ii) This group signature-based authentication system can be deployed in the Internet environment.
- Any member of the signing group can use their key pair, private key, and public keys, for various purposes such as forming a private signature, participating in the formation of group signatures, participating in a form into collective signatures… It is the same for group managers. Thanks to this, the group signature scheme espouses two components that are easy to deploy on top of existing PKI infrastructures [19].
- Using the group leader's public key L in the consent group signature validation procedure ensures i) This verification process is simpler, as it is performed only once; ii) The responsibility of the group leader is higher, and iii) Independent of the change in the set of members participating in the group signature formation process.
- The parameter t is treated as the second secret key of each signing group member. Unlike the first secret key, the private key k, t is generated randomly for each signature generation, which means it only needs to be used once. This also means that the value of the R component always ensures randomness and uniqueness in each group signature generated on document M. This enables a signing collective to generate multiple signatures. Different group signatures may appear on different documents. There is no doubt that every member here uses the same private and public key pair. Because of this, hackers have a hard time identifying the secret components of the signatures they receive using different group signatures, or the signatures of a signing group, on a variety of documents.

The two-component collective signature scheme proposed in this paper is built based on the two-component consensus group signature scheme, so it also has the same security advantages as above.

B. Performance of the Proposed Collective Signature Schemes

The computational performance of the two-component representative collective signature schemes proposed in this paper is evaluated by calculating the time cost that each scheme needs for the signature generation process of the signing collective on document M (Signature Generation Procedure) and is needed for signature validation on document M (Signature Checking Procedure).

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

The computational cost for the two signed regression schemes is as follows:

TABLE I: TIME COST OF THE SIGNATURE SCHEMES

The scheme	Time cost	
	For the signature generation	For the signature verification
RCS. 01-3	$E = [\sum_{j=1}^{g}(29m_j + 329) + 1]T_m$ $S = (59g)T_m$ $Sum = [\sum_{j=1}^{g}(29m_j + 388) + 1]T_m$	$(59 + g)T_m$
RCS. 02-3	$E = [\sum_{j=1}^{g}(30m_j + 329) + 29m + 1]T_m$ $S = (59g + 59m)T_m$ $Sum = [\sum_{j=1}^{g}(29m_j + 388) + 88m + 1]T_m$	$(59 + g + m)T_m$

Information from Table I shows the time cost for the signature generation procedure and signature checking procedure of the two-component collective signature scheme is built based on the discrete logarithm problem on the Elliptic curve and the GOST R34.10-2012 digital signature standard: i) Corresponds to the 3-component schema of the same type built on the same difficult problem; ii) Is much more reduced with schemas of the same type but built on other difficult problems. This proves that the proposed collective signature form not only significantly reduces the signature size but also meets the requirements of a representative collective signature scheme and is easy to deploy according to different digital signature standards.

V. DISCUSSION

In this paper, the process of generating consent group signatures is distinctive from that of previously-published group signatures. First, the signing group which consists of m members excluding the team leader is fully proactive in coordinating together to create a two-component collective signature of the group (e_{col}, s_{col}), and then sends the signature to the manager. Next, the manager checks the validity of the collective signature received, using the formula $R_{\text{col}} = s_{\text{col}}G_1 - e_{\text{col}}P_{\text{col}}$ (7). If it is valid, the team leader uses his private key z and a predefined algorithm to generate a pseudo-random parameter t, $t = (e_{\text{col}} \,||\, s_{\text{col}})^{z^*} H_z \; mod \; q$ (9), as well as the two components of the group signature (e, s). While the signature generated in this case represents the signed group of members and the group leader, it is still considered the personal signature of the group leader. The group leader's public key L is used to verify the validity of this signature. This procedure has the following advantages: i) If there is a forgery of a member or a member's signature during the

formation of the collective signature, this will be detected by the group leader when verifying the validity of the collective signature received; ii) The group leader is entirely responsible for ensuring the validity of the collective signature, even if this represents the signature of the group as a whole; and iii) The group leader holds the accountability, as only the group leader is authorized to "open" the group signature and identify the participants.

We have succeeded in saving the information of all the signers in the pseudo-random parameter t, whereby the signature size is significantly shortened, from the three-component group signature (U, e, s) to a two-component group signature (e, s). The algorithm for generating t has proven that it contains all the information the team leader needs for identifying the signer and solving the "disclaimer" problem later. This can also be done only by the group leader because you must recalculate t to open the signature, and to do this you must have the private key of the group leader z.

Apparently, the size of the 2-component consent group signature is only 776 bits ($|e^*| + |s^*| = 256 \text{ bits} + 520 \text{ bits} = 776 \text{ bits}$) and the security level is 2^{256} modulo multiplications, with $|p| \approx 520$ bits.

The two-component collective signature schemes proposed in this paper are built based on the two-component group signature scheme, so the above analysis is completely consistent with this proposed scheme.

VI. Conclusion

Thus, we have developed and installed two types of representative collective signatures using two components in this study. This study presents a two-component signature scheme that uses the pseudo-random parameter T to store the information of all those involved in the creation of the collective signature on the document M. The algorithm for generating t shows that when a signature dispute arises, only the group administrator has sufficient information to identify all signers and/or resolve the responsible disclaimer of any signer.

Based on the research, the following conclusions have been reached: i) A two-component representative collective signature has a smaller size than a three-component collective signature of the same type while maintaining the same security level; ii) The time cost of signature generation and signature checking process of the proposed collective signature scheme is much lower than that of the similar 3-component scheme; iii) From the consent group signature 2 components can be built: 2-component collective signature for many signing groups and 2-component collective signature for many signing groups and many individual signers.

This paper proposes a two-component consensus group signature scheme and a two-component representative collective signature scheme based on discrete logarithmic problems on the Elliptic curve and the GOST R34.10-2012 digital signature standard. Since the collective signature inherits all of the security advantages from the cryptosystem based on the elliptic curve as well as the GOST R34.10-2012 standard for digital signatures, in this case, it is considered a high level of security. In the future, we will study to build this scheme according to ECDSA [21] and GOST R34.10-2001 standards, the purpose is to demonstrate the feasibility of the new representative collective signature scheme that we propose.

Funding Statement

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

Conflict of Interest

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

Author Contributions

All authors contributed to the formation of this article. Specifically as follows: Author Tuan Nguyen Kim builds the representative collective signature schemes and proves the correctness of these schemes; Author Nikolay A. Moldovyan builds the two-component group signature scheme and designed an algorithm to generate pseudo-random number t; Author Duy Ho Ngoc analyzes security and evaluates the performance of the proposed schemes…; all authors had approved the final version.

References

[1] J. Pieprzyk, T. Hardjono, and J. Seberry, "Fundamentals of computer security," *Springer-Verlag*, Berlin, 2003.

[2] National Institute of Standards and Technology, "Digital signature standard," *FIPS Publication 186-3*, 2009.

[3] 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, Springer-Verlag, Berlin Heidelberg New York, 1995, pp. 428–432.

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

[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, 2017.

[6] 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.

[7] A. A. Moldovyan and N. A. Moldovyan, "Group signature protocol based on masking public keys," *Quasigroups and Related Systems*, 2014, pp. 133-140.

[8] 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*, no. 6, pp. 1-5, 6 2016.

[9] 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.
[10] 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.
[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, "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.
[13] K. Itakura and K. Nakamura, "A public key cryptosystem suitable for digital multisignatures," *NEC Research and Development*, vol. 71, pp. 1-8, 1983.
[14] 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.
[15] D. Johnson, A. J. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *Certicom*, 2001.
[16] 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.
[17] 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 Conference* (EIConRusNW), IEEE NW Russia Young Researchers, 2016.
[18] A. Komarova, A. Menshchikov, and T. Klyaus, "Analysis and comparison of electronic digital signature state standards GOST R34.10-1994, GOST R34.10-2001 and GOST R34.10-2012," in *Proc. 10th International Conference*, Jaipur, India, 2017.
[19] S. Selvakumaraswamy and U. Govindaswamy, "Efficient transmission of PKI certificates using ECC and its variants," *The International Arab Journal of Information Technology*, vol. 13, no. 1, pp. 38-43. 2016.
[20] C. Popescu, "Blind signature and BMS using elliptic curves," *Studia Univ Babes–Bolyai*, Informatica, pp. 43-49, 1999.
[21] J. Lee, H. Kim, Y. Lee, S. M. Hong, and H. Yoon, "Parallelized scalar multiplication on elliptic curves defined over optimal extension field," *International Journal of Network Security*, vol. 4, pp. 99-106, 2017.

Duy Ho Ngoc was born in 1982. He received his Ph.D. in Cybersecurity in 2007 from LETI University, St. Petersburg, RussiaFederation. He has authored more than 45 scientific articles in cybersecurity.

Tuan Nguyen Kim was born in 1969, received B.E, and M.E from Hue University of Sciences in 1994, and Hanoi University of Technology in 1998. He has been a lecturer at Hue University since 1996. From 2011 to the present he is a lecturer at School of Computer Science, Duy Tan University, Da Nang, Vietnam. His main research interests include Computer Network Technology and Information Security.

Nikolay A. Moldovyan is an honored inventor of Russian Federation (2002), a laboratory head at St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences, and a Professor with the St. Petersburg State Electrotechnical University. His research interests include computer security and cryptography. He has authored or co-authored more than 60 inventions and 220 scientific articles, books, and reports. He received his Ph.D. from the Academy of Sciences of Moldova (1981).