CONSTRUCTING THE 2-ELEMENT AGDS PROTOCOL BASED ON THE DISCRETE LOGARITHM PROBLEM

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

[1]Faculty of Information Technology - Duy Tan University, Da Nang 550000, Vietnam
[2]Department of Information Technology, Ha Noi, Vietnam
[3]St. Petersburg Institute for Informatics and
Automation of Russian Academy of Sciences, St. Petersburg, Russia

ABSTRACT

It is considered a group signature scheme in frame of which different sets of signers sign electronic documents with hidden signatures and the head of the signing group generates a group signature of fixed size. A new mechanism for imbedding the information about signers into a group signature is proposed. The method provides possibilities for reducing the signature size and to construct collective signature protocols for signing groups. New group signature and collective signature protocols based on the computational difficulty of discrete logarithm are proposed.

KEYWORDS

Groupdigital signature, Collective digital signature, difficult computational problems, Signing group.

1. INTRODUCTION

In modern information technologies, Electronic Digital Signature (EDS) protocols are widely used [1]. The variety of applications of EDS led to the development of special types of EDS protocols: blind signatures [2,3], group digital signatures [4-6], collective digital signatures [7,8], Approved Group Digital Signatures (AGDS) [9], etc. The protocols of the latter two types are of considerable practical interest. In practice, a public key infrastructure deployed at present can be used to support applications of conventional individual EDS. In these types of cryptographic schemes, the EDS is a pair of natural numbers of a sufficiently large size, i.e. is a two-element one, except for the protocols of the AGDS, in which the signature contains three elements (integers). Inclusion of the third number in the EDS is due to the fact that it stores information about all the persons involved in the formation of the electronic document and in generation of the AGDS to the prepared document. This information is accessible only to the head of the group of signers, who can perform the procedure of identification of signers [9,10] (disclosure of the AGDS). However, the storage of such information in the third element of the signature leads to a significant increase in its size.

This article proposes a new mechanism for storing the information necessary for the disclosure of the AGDS and the AGDS protocols with a two-element signature. Elimination of the need to use the third element of the signature is provided by embedding the information about all signers in the randomization parameter of the digital signature scheme based on the computational the difficulty of the discrete logarithm problem. In the developed protocols, the randomizing parameter is generated not by random choice, but by some algorithm generating pseudo-random

values. This parameter is formed as the transformed value of the collective signature of signers, which depends on the secret key of the manager of the signing group (using the manager's secret key defines secrecy of the pseudo-random value containing the information about signers) and on the value of the hash-function value computed from the signed document (using the hash value provides the uniqueness of the pseudo-random value).

2. AGDS PROTOCOL WITH THREE-ELEMENT SIGNATURE

2.1. Approved Group Digital Signatures

The concepts of group EDS [1,11] and collective EDS [3,8] have significant differences. A collective signature is called an EDS, formed by a given set of signers. The signature of the last type proves conclusively that each of the indicated signers has really signed the considered electronic document. A signature of the first type (called group signature) confirms that the electronic document is signed by some collegial organization (signing group), and different subsets of the persons (individual signers) included in the signing group can form group signatures.

When performing the collective signature verification procedure, the public keys of all signers are used. When verifying the authenticity of the group signatures, the fixed public key of the collegial organization is used.

The usual requirements for the group signature protocol are as follows: 1) arbitrary subset of the individual signers has the possibility to sign a document on behalf of the signing group; 2) the manager of the signing group can identify all persons who participated in the process of forming a given specific signature; 3) external persons can't establish a subset of individual signers who have formed any group EDS. The scheme of the approved group EDS [9,10] satisfies additionally the following requirements of practical interest:

1) During the calculation of the group signature the individual signers use personal secret keys that are unknown to the manager and anyone else;
2) The generation of a group EDS is performed in two stages: in the first stage a draft group signature is calculated, and in the second stage the manager transforms the draft group signature into the final group signature (the second stage can be considered as a procedure for approving the signed document);
3) Any non-empty subset of the signer can form a draft group signature to a given electronic document;
4) Only the manager is able to identify the subset of individual signers who participated in the formation of some given signature.

The last requirement in the AGDS protocols is realized by including the third element in the signature, which contains some hidden information about the persons participating in the formation of the group signature (the value of this additional number depends on the signed document and on the manager's secret key).

In the paper [9] it was shown that the AGDS based on the discrete logarithm problem in the ground finite field provides the 80-bit security with the signature size equal to 1280 bits. Implementation [10] of the AGDS based on the computational difficulty of the discrete logarithm problem on the elliptic curves provides the 80-bit security with the digital signature size equal to only 481 bits. Let us consider an AGDS scheme based on computations on an elliptic curve (EC).

2.2. AGDS Scheme Based on Computations on an Elliptic Curve

Suppose it is given an EC satisfying the standard security requirements and the point G has the large prime order q. The group manager calculates his public key as the point L = zG, where z is his private secret key. Each of m signers (members of the signing group) generates his private key k_j and his public key $P_i = k_iG$, i = 1 ,…, m.

The AGDS signature generation procedure includes the following steps:

1. The group manager computes hash value from document M: $H = F_H(M)$,where F_H is some specified hash function, calculates masking coefficients

$$\lambda_i = F_H\left(H||x_{P_i}||F_H\left(H||x_{P_i}||z\right)\right), \quad (1)$$

and sends each value λ_i to the corresponding i-th group member, for i=1, 2, .., m. Then the group manager computes the first element of the group signature

$$U = \lambda_1 P_1 + \lambda_2 P_2 + \ldots + \lambda_m P_m. \quad (2)$$

2. Each i-th individual signer (i = 1, 2, …,m) generates a random number $\rho_i < q$, computes the value $R_i = \rho_i G$ and sends R_i to the group manager.

3. The group manager generates the random number $\rho' < q$ and computes the values

$$R' = \rho' G, \quad (3)$$

$$R = R' + R_1 + R_2 + \ldots + R_m, \quad (4)$$

and

$$e = F_H(M \,||\, x_R \,||\, x_U) \bmod \delta \quad (5)$$

where δ is a large prime having length $|\delta|$ = 160 bits, x_R and x_U are abscissa of points R and U, and e is the second element of the group signature. Then he sends the value e to all group members who have initiated the protocol.

4. Each i-th group member (i = 1, 2, …,m) computes his signature share:

$$s_i = \rho_i - e\lambda_i k_i \bmod q \quad (6)$$

and sends it to the group manager.

5. The group manager verifies the correctness of each share s_i by checking equality

$$R_i = \lambda_i e P_i + s_i G \quad (7)$$

If all signature shares S_i satisfy the last verification equation (7), then he computes his share:

$$s' = \rho' + ze \bmod q \quad (8)$$

and the third element of the group signature:

$$s = s' + s_1 + s_2 + \ldots + s_m \; mod \; q \tag{9}$$

The algorithm outputs the group signature as the triple (U , e, s).

The AGDS verification procedure includes the following steps:

1. The verifier computes the hash-function value from the document M: H = F_H(M). Using the group public key L and signature (U, e, s) he computes value:

$$R^* = sG - e(U + L) \tag{10}$$

2. He computes value:

$$e^* = F_H(M||x_{R^*}||x_U) \text{mod } \delta \tag{11}$$

3. He compares the values e and e^*. If $e^* = e$, then the verifier concludes that the group signature is valid. Otherwise, he rejects the signature.

3. CONSTRUCTING THE AGDS PROTOCOL WITH A TWO-ELEMENT SIGNATURE

3.1. The Two-Element AGDS Protocol

Randomized EDS schemes, which include protocols based on the computational difficulty of the discrete logarithm problem, when performing the digital signature generation procedure use the uniformly random number that is called randomization parameter (the value t in the protocol described in Section 3). The purpose of this parameter is to protect the private key of the signer, i.e. in order to ensure the computational impossibility of finding the secret key from the signature value. This assignment is ideally realized by means of using uniformly random values as the values of the randomization parameter.

Protection of the private secret key of the signer is also provided in the case of using pseudo-random value as the value of the signature randomization parameter, which satisfies the following three requirements: unpredictability, uniqueness, and secrecy.

In the case when the initial values (seeds) of the process of generating pseudo-random values are known the indicated requirements can be quite easily fulfilled. The last remark shows the potential possibility of embedding information about individual signers in the value of the randomization parameter used to form the AGDS.

Indeed, if each document to be signed is unique, then uniqueness and unpredictability can be defined by computing the randomization parameter t as some value dependent on the hash value H from the document. To fulfill the privacy requirement, one can specify the computation of the value t depending on the manager's private secret key z. Thus, using information about signers as a seed of some specified pseudo-random transformation that is performed depending on the values H and z one can calculate the pseudo-random value t, for example, as follows $t = \sigma Hz \bmod q$, where q is a prime number that is the order of the algebraic group above which the signature scheme is defined and σ is the number containing information about signers.

In the simplest case, one can use the list of signers (participating in the formation of the group signature) as the value σ. Using his private key the manager can recover the value t, and hence the value σ, from the signature. Thus, the manager is able to identify the set of signers who participated the formation of the given group signature, but the signers have the possibility to deny their participation in the formation of the disclosed group signature. To prevent such potential possibility the number σ must also contain evidence of the fact that identified set of signers actually participated in the procedure for computing the disclosed AGDS. It is reasonable to use the collective DS to document M, which is generated by the set of individual signers appointed by the manager for signing the document M as the mentioned evidence. Thus, it is possible to propose the following general scheme for the formation of AGDS:

1. A subset of individual signers form a collective signature to the specified electronic document M and transfer it to the head.
2. The manager calculates the randomization parameter, depending on the received value of the collective signature, the value M, and his private secret key.
3. Using the computed pseudo-random value of the randomization parameter, the manager forms his individual EDS to document M, which is taken as AGDS.

In such a scheme it is assumed that the manager's public key is accepted as the public key of the group of signers, which he heads. Let us consider a detailed implementation of the AGDS protocol constructed in accordance with the described general construction scheme.

3.2. Protocol Based on the Problem of Discrete Logarithm on the Finite Field

We denote the bit length of some natural number n as $|n|$. It is quite easy to generate some 2560-bit prime number p such that $p - 1$ contains prime factors r and q of length $|r| = 161$ and $|q| = 256$ bits. It is also quite easy to compute the numbers α and β having orders (modulo p) equal to r and q, respectively.

The protocol with two-element AGDS is described as follows:

Each j-th signer generates his private secret key as a random number x_j and calculates his public key $y_j = \alpha^{x_j} \bmod p$; $j = 1,2, 3, \ldots, g$); g is the number of signers excluding the manager. The manager selects his private secret key in the form of the random value $z < q$ and computes his public key $L = \alpha^z \bmod p$, which is accepted as the public key of the group signer, i.e. the value L is used when verifying the authenticity of the group signature.

The procedure for forming a group signature to the electronic document M by a subset of some m individual signers with public keys $y_i = \alpha^{x_i} \bmod p$, where $i = 1,2, \ldots, m$, includes the following steps:

1. Individual signers form a collective digital signature to the document M:

   1.1. Each i-th signer generates a random number $t_i < r$ and sends the value

$$R_i = \alpha^{t_i} \bmod p \tag{12}$$

   to the other signers ($i = 1,2, \ldots, m$).

   1.2. Signers calculate the values:

$$R_{col} = (R_1 R_2 \dots R_m) \bmod p = \alpha^{t_1+t_1+\dots+t_m} \bmod p \quad (13)$$

and

$$E_{\text{col}} = F_H(M \,||\, R_{\text{col}}) \bmod 2^{80}, \quad (14)$$

where F_H is some specified hash function. The value E_{col} is the first element of the collective EDS.

1.3. Each *i*-th signer calculates his share of the signature

$$S_i = E_{\text{col}}(t_i + x_i E_{\text{col}}) \bmod r, \quad (15)$$

where $i = 1,2, \dots, m$, and sends it to the other signers.

1.4. The signers calculate the second element of the collective EDS in the form of the number

$$S_{\text{col}} = (S_1 + S_2 + \dots + S_m) \bmod r. \quad (16)$$

Then they give the signature (E_{col}, S_{col}), the length of which is $|E_{\text{col}}| + |S_{\text{col}}| \approx 240$ bit, to the manager.

2. The manager verifies the authenticity of the signature (E_{col}, S_{col}) by means of the verification of the equation

$$R_{\text{col}} = y_{\text{col}}^{-E_{\text{col}}} \alpha^{E_{\text{col}}^{-1} S_{\text{col}}} \bmod p, \quad (17)$$

where

$$y_{\text{col}} = (y_1 y_2 \dots y_m) \bmod p. \quad (18)$$

If the collective signature is genuine, then he calculates the pseudo-random number

$$T = (E_{\text{col}} \,||\, S_{\text{col}})^{z^*} H_z \bmod \text{q}, \quad (19)$$

Where $z^* = \min\{z_i: z_i = z + i;\ \gcd(z_i, q - 1) = 1;\ i = 0, 1, 2, \dots\}\}$, and $H_z = F_H(M, z) \bmod q$.

3. Then the manager calculates the values

$$R = \alpha^T \bmod p, \quad (20)$$

$$E = F_H(M \,||\, R) \bmod 2^{128} \quad (21)$$

And

$$S = E(T + zE) \bmod q, \quad (22)$$

where (E, S)is the group signature, whose size is | E | + | S | = 384 bits.

The procedure for disclosing the AGDS (identification of signers) is carried out by the manager as follows. By the value of the group signature (E, S) and the value $H_z = F_H(M, z) \bmod q$, the manager calculates the value

$$T = SE^{-1} - zE \bmod q, \tag{23}$$

and then the value of the collective signature

$$E_{\text{col}} || S_{\text{col}} = (TH_z{}^{-1})^{z^{-1} \bmod (q-1)}. \tag{24}$$

Next, it performs the procedure for authentication of the collective EDS for all possible values of the collective public key, i.e. for all possible subsets of potential signatories. The collective public key, for which the verification procedure of the EDS confirms the authenticity of the collective signature, uniquely identifies all signers related to the disclosed AGDS. The fact that the head indicates a collective signature passing the authentication procedure by their collective key proves unambiguously that they did form the given collective signature (the probability of random coincidence is negligible).

3.3. Protocol Based on the Problem of Discrete Logarithm on Elliptic Curves

The AGDS protocol can be constructed using computations on elliptic curves (EC). Suppose two curves EC1 and EC2 having orders $\#E_1$ and $\#E_2$ are defined over the ground finite field $GF(p)$. Suppose also that the 256-bit prime number w divides $\#E_1$, i.e. $w|\#E_1$, and 520-bit prime number q divides $\#E_2$, i.e. $q|\#E_2$. Suppose that for the first and second EC there are given the points G_1 and G_2, the order of which is w and q, respectively. The private secret key of the i-th signer is formed as a random number $k_i<w$, and the corresponding public key is computed in the form of the point $P_i = t_iG_1$. The manager computes his public key L using the formula $L = zG_2$, where z is his private secret key ($z < q$). The proposed AGDS protocol on the basis of the Russian digital signature standard GOST R 34.10-2012 is described as follows.

1. A subset m of ordinary signers forms a collective signature to the document M:

   1.1. Each i-th signer generates a random number $t_i < w$and sends the point EC1

   $$R_i = t_iG_1 \tag{25}$$

   to the other signers (i = 1,2, …, m).

   1.2. The signers calculate the point

   $$R_{\text{col}} = R_1 + R_2 + \ldots + R_m, \tag{26}$$

   the value

   $$r_{col} = x_R \bmod w, \tag{27}$$

   where x_R is the first coordinate of the point R_{col}, and the value of the first element of the collective signature:

   $$e_{\text{col}} = F_H(M \,||\, x_R) \bmod w. \tag{28}$$

1.3. Each *i*-th signer calculates his share of the signature

$$s_i = (t_i + e_{col}k_i)\ mod\ w \tag{29}$$

and sends the value s_i to the other signers.

1.4. The signers calculate the second element of the collective EDS

$$s_{\text{col}} = (s_1 + s_2 + \ldots + s_m)\ mod\ w. \tag{30}$$

Then they directed the signature (e_{col}, s_{col}) to the head (the signature length is $|e_{\text{col}}| + |s_{\text{col}}| = 512$ bits, where the bit length of the number x is denoted as $|x|$).

2. The manager verifies the authenticity of the signature (e_{col}, s_{col}), by the verification equation

$$R_{\text{col}} = s_{\text{col}}G - e_{\text{col}}P_{\text{col}}, \tag{31}$$

Where

$$P_{\text{col}} = P_1 + P_2 + \ldots + P_m. \tag{32}$$

If the collective signature is genuine, then he calculates a pseudo-random number

$$t^* = (e_{\text{col}} \| s_{\text{col}})^{z^*} H_z \mod q, \tag{33}$$

where $z^* = \min\{z_i: z_i = z + i;\ \gcd(z_i, q - 1) = 1;\ i = 0, 1,,...\}$, and $H_z = F_H(M, z) \mod q$.

3. Then the manager computes the point

$$R^* = t^* G_2, \tag{34}$$

the first element of the group signature as the number:

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

and its second element

$$s^* = t^* + e^* z\ mod\ q \tag{36}$$

A group EDS is a pair (e^*, s^*), whose size is equal to $|e^*| + |s^*| = 776$ bits, and security is equal to$\approx 2^{256}$multiplication operations modulo p having the length $|p| \approx 520$ bits.

4. COLLECTIVE SIGNATURE PROTOCOL FOR SIGNING GROUPS

The proposed method of embedding information about signers in the pseudo-random value of the randomization parameter leads to the construction of AGDS protocols, which are computationally indistinguishable by signatures from the protocols of the individual EDS (for anybody, except the manager of the signing group). Even a subset of signers who participated in the formation of the AGDS can't show that this signature was formed using their collective signature to the specified document.

The noted in distinguish ability of the group signature from the individual signature of the manager means that the known protocols of the collective EDS for individual signers [7,8] can be applied for the cases of the formation of a single collective signature to a given document *M*, shared by i) an arbitrary number of signing groups (collective EDS schemes for signing groups) and ii) an arbitrary number of signing groups and an arbitrary number of individual signers (schemes of combined collective EDS).

5. EVALUATE THE SECURITY OF THE ALGORITHM

Security of the AGDS protocol based on the signature standard GOST R34.10-2012 against known attacks is defined by the security of the GOST.

However, it should be estimated security against attack performed by a coalition of the sets of signers participating in the procedure of the formation of the AGDS. Suppose the signers form two different collective signatures $(e_{\text{col}}\|s_{\text{col}})_1$ and $(e_{\text{col}}\|s_{\text{col}})_2$ to the same document and the manager computes two different group signatures (e_1^*, s_1^*) and (e_2^*, s_2^*). Then the signers can compose the following system of three equations with three unknowns z, t_1^*, and t_2^*:

$$\begin{cases} s_1 = t_1^* + ze_1 \bmod q; \\ s_2 = t_2^* + ze_2 \bmod q; \\ \frac{t_1^*}{t_2^*} = \left(\frac{(e_{col} \,||\, s_{col})_1}{(e_{col} \,||\, s_{col})_2}\right)^{z+1} \bmod q \end{cases} \tag{37}$$

Even in the case of the known value *i* (one should suppose the value *z* be known since the value *i* is a small integer) solving this system of equations is difficult since it contains one exponentiation equation and the modulus *q* is sufficiently large.

6. CONCLUSION

A new method of embedding information about signers in the AGDS protocol was proposed, on the basis of which the AGDS protocols with a two-element signature were first developed. This method allows reducing the length of EDS for a given level of security. In the developed protocols, the signature is formed as an individual EDS by the manager of the signing group. Only the manager can open the signature and identify those who participated in the formation of a group signature. When using the proposed approach for the formation of AGDS, the protocols of collective EDS [3,7,8] are easily extended to cases when a single collective signature is formed by i) an arbitrary number of the signing groups (collective signatures for signing groups) and ii) signing groups and individual signers (combined protocols of collective signature).

The proposed protocols and protocols of the latter two types can be implemented by analogy with protocols breaking of which requires simultaneous solving two different computationally difficult problems [12], but this question is of interest for a separate study.

REFERENCES

[1] Shah F., Patel H.,*"A Survey of Digital and Group Signature"*, International Journal of Computer Science and Mobile Computing, Vol.5 Issue.6, P. 274-278, (2016).

[2] Camenisch J.L., Piveteau J.M., Stadler M.A.,*"Blind Signatures Based on the Discrete Logarithm Problem"*, Advances in Crypology – EUROCRYPT'94 Proc, Lecture Notes in Computer Science. Springer Verlang, Vol. 950,P. 428–432, (1995).

[3] Moldovyan A.A., Moldovyan N.A.,*"Blind Collective Signature Protocol Based on Discrete Logarithm Problem",*Int. Journal of Network Security, Vol. 11, No. **2**, P. 106–113, (2010).

[4] Qi Su, Wen-Min Li, *"Improved Group Signature Scheme Based on Quantum Teleportation"*, International Journal of Theoretical Physics, Vol. 53, No. **4**, P. 1208, (2016).
[5] Alamélou Q, Blazy O, Cauchie S., Gaborit Ph.,*"A code-based group signature scheme",* Designs, Codes and Cryptography, Vol. 82, No **1-2**, P. 469–493, (2017).
[6] San Ling, Khoa Nguyen, Huaxiong Wang, *"Group signature from lattices: simpler, tighter, shorter, ring-based",* Proc. of 18th IACR International Conference on Practice and Theory in Public-Key Cryptography,P.427-449, (2015).
[7] Moldovyan N.A,*"Blind Signature Protocols from Digital Signature Standards"*, Int. Journal of Network Security, Vol. 13, No. **1**, P. 22–30, (2011).
[8] Duy H.N., Binh D.V., Minh N.H., Moldovyan N.A. *"240-bit collective signature protocol in a non-cyclic finite group"*, 2014 International conference on Advanced Technologies for Communications (ATC),Hanoi, P. 467 – 470, (2014). (DOI 10.1109/ATC.2014.7043433)
[9] Moldovyan A.A., Moldovyan N.A., *"Group signature protocol based on masking public keys",* Quasigroups and related systems, Vol. 22, P. 133-140, (2014).
[10] Moldovyan N.A., Nguyen Hieu Minh, Dao Tuan Hung, Tran Xuan Kien,*"Group Signature Protocol Based on Collective Signature Protocol and Masking Public Keys Mechanism"*, International Journal of Emerging Technology and Advanced Engineering, Vol. 6, Issue. 6, P. 1-5, (2016).
[11] Phong Q. Nguyen, Jiang Zhang, Zhenfeng Zhang, *"Simpler efficient group signature from lattices",* Proc. of 18th IACR International Conference on Practice and Theory in Public-Key Cryptography, P.401-426, (2015).
[12] Berezin A. N., Moldovyan N. A., Shcherbakov V. A.,*"Cryptoschemes Based on Difficulty of Simultaneous Solving Two Different Difficult Problems"*, Computer Science Journal of Moldova, Vol. 21,No.**2**(62), P. 280-290, (2013).

AUTHORS

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 (2021) 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.

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

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).