COLLECTIVE SIGNATURE PROTOCOLS FOR SIGNING GROUPS BASED ON PROBLEM OF FINDING ROOTS MODULO LARGE PRIME NUMBER

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

Generally, digital signature algorithms are based on a single difficult computational problem like prime factorization problem, discrete logarithm problem, elliptic curve problem. There are also many other algorithms which are based on the hybrid combination of prime factorization problem and discrete logarithm problem. Both are true for different types of digital signatures like single digital signature, group digital signature, collective digital signature etc. In this paper we propose collective signature protocols for signing groups based on difficulty of problem of finding roots modulo large prime number. The proposed collective signatures protocols have significant merits one of which is connected with possibility of their practical using on the base of the existing public key infrastructures.

KEYWORDS

Collective digital signature, group digital signature, signing group, finding roots modulo.

1. INTRODUCTION

Digital signature (DS) protocols are widely used in information technologies to process electronic legal messages and documents. The DS protocols are based on DS schemes that represent a mathematical technique applied in public-key cryptography to validate the authenticity of digital messages or documents. Such validation is connected with the fact that DS as some redundant information can be computed only with using the private key that is known only to one person, i.e. to the signer. Verification of the signature validity is performed with signer's public key that is known publicly. To solve a variety of different practical tasks, different types of signatures are proposed: Individual signature [1,8]; Blind signature [2,3]; Collective signature [4,7]; Group signature [5,10].

The group signature refers to a signature formed on behalf of a group of signers (signing group) headed by a person called group manager or leader [11].The group digital signature (GDS) to an electronic message is generated by a group member. To verify the group signature, group public key needs to be used. Except the group manager, nobody can disclose which particular group member signed the document. The group signature has the following important properties: Only group members can sign a document; Group manager, who has both document and valid group signature can reveal the group members signed the document; And, non-group members could not reveal the original signers, who generate the group signature [14].

The collective signature refers to a signature generated with participation of each of the individual signers included in some declared set of signers. Validity of collective signature to some electronic document *M* means that *M* is signed by each of them. To generate a collective digital signature (CDS) it is needed each of the mentioned individual signers use his private key. The procedure of the verification of CDS is performed using public keys of each signer. The CDS protocols can be practically used on the base of the public key infrastructure (PKI) existing on practice to support the widely used individual DS protocols. In addition, another merit of the CDS protocols relates to possibility to implement them using many official DS standards [12], for example the Russian standard GOST R 34.10–2012 [13].

Combining the main properties of CDS and GDS in the frame of some single DS protocol [15] is very actual in the following cases: when an electronic document is to be processed and signed by several different signing groups; when an electronic document is to be processed and signed by several different signing groups and by several different individual signers. In this paper we propose the collective signature protocol for both cases, namely: Collective digital signature protocol for signing groups and Protocol of collective digital signature for group and individual signers.

Generally, digital signature algorithms are based on a single difficult computational problem like prime factorization problem, discrete logarithm problem, elliptic curve problem or are based on the hybrid combination of prime factorization problem and discrete logarithm problem. We based on difficulty of the problem of finding roots modulo large prime number [16] to design our proposed collective signature protocols.

2. COLLECTIVE DIGITAL SIGNATURE BASED ON PROBLEM OF FINDING ROOTS MODULO LARGE PRIME NUMBER

2.1. Digital Signature Protocol

New hard computational problem described in [16] is used in the digital signature scheme (DSS) described below. It uses the prime modulus having the structure $p = Nk^2 + 1$, where k is a large prime ($|k| \geq 160$ bits) and N is such even number that the size of p satisfies the condition $|p| \geq 1024$ bits.

A random value x is selected as a private key. The public key y is computed using the formula $y = x^k \bmod p$. The signature represents a pair of the numbers S and E. The size of S is equal to $|p| \geq 1024$ bits and size of E is equal to $|\delta| \geq 160$ bits, where δ is some specified prime number. Suppose a message M is given.

The signature generation procedure is performed as follows:

1. Select at random a value $t < p - 1$ and calculate:

$$R = t^k \bmod p \tag{1}$$

2. Using some specified hash function $F_H(M)$ calculate the hash value H corresponding to the message M and compute the first element of the signature

$$E = f(R, M) = RH \bmod \delta, \tag{2}$$

where δ is a large prime that is a parameter of the signature generation algorithm. For example, it is acceptable to use a randomly selected prime δ such that|δ|= 160. The function $F_H(M)$ is also a part of the DSS. For example, one can use the hash function SHA-1 recommended by US National Institute of Standards and technology (NIST).

3. Calculate the second element of the signature:

$$S = x^{f(R,M)}t \bmod p \tag{3}$$

The signature verification procedure is performed as follows:

1. Using the signature (E, S) compute:

$$R = S^k y^{-E} \bmod p \tag{4}$$

2. Calculate:

$$E' = f(R; M) = RH \bmod \delta \tag{5}$$

3. Compare E' with E. If $E' = E$, then the signature is valid.

The signature length is equal to

$$|E| + |S| = |\delta| + |p| \approx |p|.$$

The random value t plays the role of one-time secret key. It is unacceptable to use the same value t for the formation of signatures to two different documents, since in this case the private key can be calculated. Indeed, let (R, S_1) and (R, S_2) are the signature to the messages M_1 and M_2, respectively. We have

$$S_1 = y^{f(R,M_1)}.R \bmod p \tag{3a}$$

and

$$S_2 = y^{f(R,M_2)}.R \bmod p \tag{3b}$$

Therefore

$$\frac{S_1^k}{S_2^k} = y^{f(R,M_1)-f(R,M_2)} \tag{6}$$

therefore

$$x = \left(\frac{S_1}{S_2}\right)^{1/\left(f(R,M_1)-f(R,M_2)\right)} \bmod p \tag{7}$$

2.2. Collective Signature Protocol

Using the previously described digital signature scheme one can propose the following collective signature protocol.

Suppose the *j*-th user owns the public key y_j depending on his private key $x_j < p$ as follows: $y_j = x_j^k \bmod p$, where $j = 1,2,\ldots, s$.

Suppose an electronic document *M* is given and *m*(*m* < *s*) users owning the public keys $y_{\alpha 1}$, $y_{\alpha 2}$, …, $y_{\alpha m}$ should sign it simultaneously.

The following protocol produces the collective digital signature:

1. Each α_jth user selects at random a value$t_{\alpha_j} < p$and computes the public value:

$$R_{\alpha_j} = t_{\alpha_j}^{k} mod p \tag{8}$$

where *j = 1,2, …, m.*

2. Some of the users (or one of them) calculate the common randomization value:

$$R = \prod_{j=1}^{m} R_{\alpha_j} mod p \tag{9}$$

and then calculate the first part of the CDS:

$$E = f(R, M)$$

where *f* is a specified compression function. For example, we will use the following function:

$$E = RH \; mod \; \delta \tag{10}$$

where δ is a large prime having length |δ|= 160 bit and *H* is a hash value computed from the message *M.*

3. Using the values R and t_{α_j}each α_jth user computes its share in the CDS:

$$S_{\alpha_j} = x_{\alpha_j}^{f(R,M)} t_{\alpha_j} \; mod \; p \tag{11}$$

that is supposed to be available to all users of the group.

4. Calculate the second element of the CDS:

$$S = \prod_{j=1}^{m} S_{\alpha_j} \; mod \; p \tag{12}$$

Thus, the CDS is computed with 2m modulo exponentiations. The CDS length is fixed and equals to$|S| + |\delta|$.

The CDS verification procedure is performed as follows.

1. Compute the collective public key y:

$$y = \prod_{j=1}^{m} y_{\alpha_j} \; mod \; p \tag{13}$$

2. Using the CDS (E; S) compute value R'

$$R' = S^{k} y^{-E} \; mod \; p \tag{14}$$

3. Compute $E' = f(R', M) = R'H \; mod \; \delta$
4. Compare values *E′*and *E*.

If *E′* = *E*, then the signature is valid. Otherwise the signature is false.

3. COLLECTIVE DIGITAL SIGNATURE FOR SIGNING GROUPS BASED ON PROBLEM OF FINDING ROOTS MODULO LARGE PRIME NUMBER

The GDS protocol presupposes the formation of a digital signature to some electronic document on behalf of some collegial body (group of signers, i.e. signing group), which is headed by a group manager. Each representative of a group of signers generates his private key *x* and his public key $y = x^k \bmod p$. The public key *Y* of the group manager is a public key of the group and is calculated as follows $Y = X^k \bmod p$, where *X* is manager's private key. The value *Y* is also the public key of the group, i.e. the value *Y* is used to verify authenticity of the GDS.

Let *m* group members (having public keys $y_i = x_i^k \bmod p$and corresponding private keys x_i , *i = 1, 2, …, m*) wish to sign the document *M*.

The group signature protocol is described as follows:

- ***Signature generation:***

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

$$\lambda_i = F_H(H \,||\, y_i ||\, F_H(H \,||y_i||\, X)) \tag{15}$$

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:

$$U = \prod_{i=1}^{m} y_i^{\lambda_i} \bmod p \tag{16}$$

2. Each *i*-th group member (*i = 1, 2, …, m*) generates a random number $t_i < p-1$, computes the value:
3.

$$R_i = t_i^k \bmod p \tag{17}$$

and sends R_i to the group manager.

4. The group manager generates the random number $T < p-1$ and computes the values
5.

$$R' = T^k \bmod p, \tag{18}$$

$$R = R' \prod_{i=1}^{m} R_i \bmod p = (T . \prod_{i=1}^{m} t_i)^k, \tag{19}$$

and

$$E = F_H(M||R||U) \bmod \delta, \tag{20}$$

whereδ is a large prime having length $|\delta|$= 160 bit,*E* is the second element of the group signature. Then he sends value *E* to all group members who have initiated the protocol.

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

$$S_i = x_i^{E\lambda_i} . t_i \bmod p \tag{21}$$

and sends it to the group manager.

7. The group manager verifies the correctness of each share S_i by checking equality
8.

$$R_i = S_i^k y_i^{-E\lambda_i} \bmod p \quad (22)$$

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

$$S' = X^E . T \bmod p \quad (23)$$

and the third element of the group signature

$$S = S' . \prod_{i=1}^{m} S_i \bmod p \quad (24)$$

- ***Signature verification:***

The 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 *Y* and signature (*U, E, S*) he computes value:

$$R^* = S^k (YU)^{-E} \bmod p \quad (25)$$

2. He computes value
3.

$$E^* = F_H(M \,||\, R^* \,||\, U) \quad (26)$$

4. Compares the values *E* and E.

If E* = E, then the verifier concludes that the group signature is valid. Otherwise, he rejects the signature.

- **Proof of correctness**:

Let us show that the proposed protocol generating the CDS (U, e, s) works correctly.
Substituting the value:

$$S = S' . \prod_{i=1}^{m} S_i \bmod p,$$
$$Y = X^k \bmod p$$
$$\text{And } U = \prod_{i=1}^{m} y_i^{\lambda_i} \bmod p$$

in the right part of the verification equation (25):

$$R^* = S^k (YU)^{-E} \bmod p$$

we get: $R^* = S^k (YU)^{-E} \bmod p$

$$= (X^E . T \prod_{i=1}^{m} x_i^{E\lambda_i} . t_i)^k \; (X^k . T \prod_{i=1}^{m} y_i^{\lambda_i})^{-E}$$

$$= X^{kE}.(T\prod_{i=1}^{m} x_i^{E\lambda_i}.t_i)^{k} X^{-kE}.(T\prod_{i=1}^{m} y_i^{k\lambda_i})^{-E}$$
$$= T^k.\prod_{i=1}^{m} t_i{}^k \bmod p = R$$

It is easy to see that the value:

$$D = \prod_{i=1}^{m} S_i \bmod p \quad (27)$$

can be considered as a "group pre-signature" approving of which is performed by the group manager with adding his signature share *S'*. The value is actually calculated analogously to the computation of the collective signature in the protocols [5,6]. The main difference between the described GDS protocol and collective DS protocols [5,6] is using the masking coefficients λ_i at time of generating the collective public key *U*, which is used as the first element of the GDS. The value *U* conserves the information about all group members who participated in the process of generating the GDS. It is easy to see that only the group manager can open the GDS, using the value *U*, since only he can compute the masking values λ_i.

In the protocol developed in this paper it is also used the mechanism of the formation of the collective DS. Namely, this mechanism is used in the following two ways: i) to form a pre-signature and ii) to form a collective signature shared by several signing groups.

Let *g* signing groups with public keys$Y_j = X_j^k \bmod p$, where *j = 1,2, …, g*; X_j is the secret key of the *j*-th group manager, have intention to sign the document *M*.

Suppose also the *j*-th signing group includes m_j active individual signers (persons appointed to act on behalf of the *j*-th signing group). The protocol of collective signature for group signers is described as follows.

The signature generation procedure relating to the proposed collective DS protocol for signing groups:

1. Within the framework of the GDS protocol described above, the manager of each *j*-group of signers (*j = 1, 2,.., g*) generates masking parameters λ_{ji} for the signers of his group and computes the value:

$$U_j = \prod_{i=1}^{m_j} y_{ji}^{\lambda_{ji}} \bmod p \quad (28)$$

(where $i = 1,2,\ldots, m_j$) as the *j*-th share in the first element of the collective group signature and the randomizing parameter:

$$R_j = R'_j \prod_{i=1}^{m_j} R_{ji} \bmod p \quad (29)$$

Then he sends values U_j and R_j to all other managers.

2. Each *j*-th group manager (*j = 1, 2, …, g*) computes values

$$U = \prod_{j=1}^{g} U_j \bmod p, R = \prod_{j=1}^{g} R_j \bmod p, \quad (30)$$

And

$$E = F_H(M||R||U) \bmod \delta, \tag{31}$$

where δ is a large prime having length |δ|= 160 bit, *E* and *U* are the first and second elements of the group signature.

3. Each *j*-th group manager (*j = 1, 2, …, g*) computes signature share of his group

$$S_j = S'_j \prod_{i=1}^{m_j} S_{ji} \bmod p, \tag{32}$$

where S_{ji} is the signature share of the ith individual signer in the ith signing group, and sends it to other group managers.

4. Each *j*-th group manager can verify the correctness of each share S_j by checking equality
5.

$$R_j = S_j^k (Y_j U_j)^{-E} \bmod p. \tag{33}$$

If all shares S_j satisfy the last verification equation, then the third element S of the collective signature is computed:

$$S = \prod_{j=1}^{g} S_j \bmod p \tag{34}$$

The tuple (*U, E, S*) generated by the above procedure presents the collective signature (to the document *M*) shared by g signing groups.

- **Signature Verification:**

The signature verification procedure relating to the proposed collective DS protocol for signing groups:

1. Compute the collective public key shared by all signing groups:

$$Y_{col} = \prod_{j=1}^{g} Y_j \bmod p = (\prod_{j=1}^{g} X_j)^k \bmod p \tag{35}$$

2. Compute the value:

$$R^* = S^k (U Y_{col})^{-E} \bmod p \tag{36}$$

3. Compute the value:

$$E^* = F_H(M \,||\, R^* \,||\, U) \tag{37}$$

4. Compare the values *E* and E*.

If E* = E, then one concludes that the group signature is valid. Otherwise, the signature is rejected.

- **Proof of correctness:**

Substituting the value:

$$S = \prod_{j=1}^{g} S_j \bmod p, U = \prod_{j=1}^{g} U_j \bmod p,$$

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

in the right part of the verification equation (36):

$$R* = S^{k}(UY_{col})^{-E} \bmod p$$

we get:

$$\begin{aligned} R^{*} &= \overset{g}{S^{k}}(UY_{col})^{-E} \bmod p \\ &= (\prod_{j=1}^{g} S_j)^{k} (\prod_{j=1}^{g} U_j \prod_{j=1}^{g} Y_j)^{-E} \bmod p \\ &= \prod_{j=1}^{g} S_j{}^{k}(U_j Y_j)^{-E} \bmod p \\ &= \prod_{j=1}^{g} R_j \bmod p = R \end{aligned}$$

The first element *U* of the collective signature contains information about all group members of each signing group who signed the document *M*. The identification procedure (the disclosure of the group signature) is carried out by analogy with the procedure for disclosing the group signature described in [9]. It should be noted that the procedure for identifying individual signers requires the participation of the group managers of each group that share the collective signature. At the same time, the computational complexity of this procedure is relatively high and rapidly increases with the growth of number of the signing groups that share collective signature.

In the proposed collective DS scheme the signature verification procedure includes the steps of the verification procedure in the group signature scheme and an additional initial step for computing the collective public key (step 1). In the signature verification equation it is used the collective public key Y_{col} instead of the group public key.

4. PROTOCOL OF COLLECTIVE DIGITAL SIGNATURE FOR GROUP AND INDIVIDUAL SIGNERS

Another important practical scenario relates to the processing document *M* by several individual signers and by several group signers. Construction of the collective signature protocol (in Section 2) for such case can be implemented in full correspondence with the collective signature protocol for group signers described in Section 3, if it is accepted an agreement that for individual signers the value U_j is equal to 1.

It is evident that only all group managers act in the procedure of disclosing the collective group signature (identification of the individual signers acted in the frame of each group signer).

5. CONCLUSION

In paper [16], Nicolay A. Moldovyan based on difficulty of finding the k^{th} roots in the finite fields GF(p) such that $p = Nk^2 + 1$, where k is sufficiently large prime having the size $|k| > 160$ bits and N is even number such that the size of p is $|p| > 1024$ bits, to propose a collective digital signature scheme. This is the basis for us design collective signature protocols for signing groups based on problem of finding roots modulo large prime numbers: Collective digital signature for signing groups and Collective digital signature for group and individual signers. Both are extensions of collective digital signatures that combine the advantages of group digital signatures

and collective digital signatures. Their size does not depend on the number of members involved in the formation of the final signature. In each turn, we presented the signature generation process, the signature verification process, as well as demonstrate the correctness of this verification process.

We also set all our hope on our future work to develop the collective signature schemes of the proposed types, in which the signature contains only two elements E and S.

REFERENCES

[1] National Institute of Standards and Technology,*"Digital Signature Standard*",FIPS Publication 186-3, (2009).

[2] Chaum D.,"*Blind Signatures for Untraceable Payments*", Advances in Cryptology: Proc. of CRYPTO'82, Plenum Press, p. 199–203, (1983).

[3] Camenisch J.L., Piveteau J.-M. and Stadler M.A,"*Blind Signatures Based on the Discrete Logarithm Problem*", In: Advances in Crypology – EUROCRYPT'94 Proc, Lecture Notes in Computer Science, Springer-Verlag, Berlin Heidelberg New York, Vol. 950, 428–432, (1995).

[4] Minh N. H., Binh D. V., Giang N. T. and Moldovyan N. A. "*Blind Signature Protocol Based on Difficulty of Simultaneous Solving Two Difficult Problems*", Applied Mathematical Sciences,No.**6,** 6903–6910, (2012).

[5] Moldovyan N.A, "*Blind Signature Protocols from Digital Signature Standards*", Int. Journal of Network Security,No. **13**, 22–30, (2011).

[6] Moldovyan N.A,"*Blind Collective Signature Protocol*", Computer Science Journal of Moldova,No. **19**, 80–91, (2011).

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

[8] Pieprzyk J., HardjonoTh. and Seberry J.,"*Fundamentals of Computer Security*", Springer-verlag, Berlin, (2003).

[9] Moldovyan A.A. and Moldovyan N.A,"*Group signature protocol based on masking public keys*,Quasigroups and related systems, No. **22**, 133–140, (2014).

[10] Seetha R. and Saravanan R,"*Digital Signature Schemes for group communication: A Survey*", International Journal of Applied Engineering Research, No.**11**, 4416–4422, (2016).

[11] Enache A.-C,"*About Group Digital Signatures*", Journal of Mobile, Embedded and Distributed Systems, No.**IV,** 193–202, (2012).

[12] International Standard ISO/IEC 14888-3:2006(E), *Information technology –Security techniques – Digital Signatures with appendix – Part 3: Discrete logarithm based mechanisms*.

[13] GOST R 34.10-2001 and Russian Federation Standard, Information Technology,"*Cryptographic data Security. Produce and check procedures of Electronic Digital Signature*", Government Committee of the Russia for Standards, (2012).

[14] Rajasree R.S,"*Generation of Dynamic Group Digital Signature*", International Journal of Computer Applications, No.**98**, 1–5, (2014).

[15] Moldovyan N.A., Nguyen Hieu Minh, Dao Tuan Hung and Tran Xuan Kien,"*Group Signature Protocol Based on Collective Signature Protocol and Masking Public Keys Mechanism*", International Journal of Emerging Technology and Advanced Engineering, No.**6**, 1–5, (2016).

[16] Moldovyan N.A,"*Digital Signature Scheme Based on a New Hard Problem*", Computer Science Journal of Moldova, No.**16**, 163–18, (2008).

AUTHORS

Tuan Nguyen Kim was born in 1969, received B.E., and M.E from Hue University of Sciences in 1994, and from 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).