On Functionality Extension of the Digital Signature Standards

Minh H. Nguyen[1], Duy N. Ho[1], Dung H. Luu[1], Alexander A. Moldovyan[2], and Nikolay A. Moldovyan[2]
[1]Le Qui Don Technical University, Ha Noi, Viet Nam
[2]St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences
14 Liniya, 39, St. Petersburg 199178, Russia
hieuminhmta@ymail.com, nmold@cobra.ru

Abstract - **There are proposed collective signature, blind signature, and collective blind signature protocols based on the digital signature generation and verification procedures specified by Russian and Belarusian signature standards. The protocols are characterized in computing the randomization parameter of the collective signature depending on the collective public key. Due to this novel feature the proposed protocols provide integrity of the collective signature.**

Keywords - **Digital signature, collective digital signature, blind signature, digital signature standards, discrete logarithm problem, multi-signature schemes, public key, finite group**

I. INTRODUCTION

One of the important objectives of the information security systems is providing authentication of the electronic documents and messages. Usually this problem is solved with digital signatures (DS)[1]. In some special cases, for example in the voting systems and in the electronic cash technologies, there is required to provide the anonymity of the users presenting electronic messages for signing. To solve this problem the blind signature schemes are used [2]. The properties of the blind signatures are [3]: i) the signer can not to read the document during process of signature generation; ii) the signer can not correlate the signed document with the act of signing.

The problem of providing the second property is known as anonymity (or untraceability) problem. To solve this problem there are used specially designed DS algorithms. There are known blind signature schemes based on difficulty of the factorization problem [3] and on difficulty of finding discrete logarithm [4]. Usually, the blind signature scheme is designed on the basis of some known DS algorithm, for example the RSA algorithm [5] or DS algorithm [4]. To provide the anonymity of the signature and hash function value (or message submitted for signing) there are used so called *blinding factors*. Prior to submit a hash function value (or message M) for signing the user U computes the hash function value H and multiplies H (or M) by a random number (blinding factor). Then the user submits the blinded hash function value (or blinded document) for signing. The signer signs the blinded value H (or M) producing the blinded signature that is delivered to user U. The user divides out the blinding factor producing the valid signature to the original hash function value (or directly to the original document).

Another type of DS protocols interesting for practical application are multi-signature schemes [6, 7] among which the collective DS protocols represent special interest. There are known collective DS protocols based on the difficulty of finding large prime roots modulo a 1024-bit prime [8] and on the difficulty of the discrete logarithm problem [9]. In the first case the protocol produces a fixed size collective DS for arbitrary number of signers, however the DS length is sufficiently large, actually, 1184 bits. In the second case the 320-bit collective DS is produced.

It seems that the collective DS protocols are promising for application in the electronic cash systems in which the electronic banknotes are issued by several banks. However it should be solved the anonymity problem for collective DS schemes. Besides, is reasonable to implement such protocols on the base of the official digital signature standards.

Previously the collective, blind, and blind collective signature protocols were implemented using the Russian signature standards GOST R 34.10-94 and GOST R 34.10-2001 [10, 13, 15]. However those protocols have not provide the collective signature integrity and the are possible some attacks producing a reduced collective signature from the initially generated one [14]. Besides, blind signature protocols use four blinding parameters.

In the present paper there are designed the collective, blind, and blind collective DS protocols using the Belarusian DS standard STB 1176.2-9 [11] as underlying signature scheme. The are also proposed new variants of the blind and blind collective DS protocols based on the Russian DS standard GOST R 34.10-2001.

II. BLIND COLLECTIVE SIGNATURE PROTOCOL BASED ON BELARUSIAN STANDARD

A. Belarusian Signature Standard STB 1176.2-9

Belarusian signature standard STB 1176.2-9 [11] is based on difficulty of finding discrete logarithm in the finite group order of which contains large prime factor q. The size of the factor q should be equal to $h \geq 160$ bits. The standard specifies the finite group as follows. Select prime p such that its size is $l \leq 1024$ bits. The group includes all numbers of the set $\{1, 2, \ldots, p-1\}$. The group operation "$*$" is defied with formula:

$$u*v = uv\mu^{-1} \bmod p,$$

where u and v are the group elements and $\mu = 2^{l+2}$. The standard specifies ten security levels corresponding to balanced pairs of the values h and l (see Table I). The exponentiation operation is denoted as follows:

$$\underbrace{a*a*...*a}_{k \text{ times}} = a^{(k)}.$$

In the STB 1176.2-9 signature scheme the public key is computed using formula $y = g^{(x)}$, where y is the q order element of the group and x is the secret key ($1 < x < q$).

The signature generation procedure includes the following steps:

1. Generate a random number k ($1 < k < q$) and compute $T = g^{(k)}$.

2. Concatenate the value T and message M to be signed: $M' = T||M$.

3. Using the specified hash function F_H compute the hash value from M': $e = F_H(M') = F_H(T||M)$, where || denotes the concatenation operation.

4. Compute the value $s = k - xe \bmod q$.

The pair of numbers (e, s) is the signature to message M.

The signature verification is performed as follows:

1. If $1 < s < q$ and $0 < e < q$, then go to step 2. Otherwise the signature is false.

2. Compute values $T^{\bullet} = g^{(s)} * y^{(e)}$ and $e^{\bullet} = F_H(T^{\bullet}||M)$.

3. If $e^{\bullet} = e$, then the signature is valid, otherwise the signature is false.

TABLE I.

Security level	h, bits	l, bits	Security level	h, bits	l, bits
1	143	638	6	208	1534
2	154	766	7	222	1790
3	175	1022	8	235	2046
4	182	1118	9	249	2334
5	195	1310	10	257	2462

B. Collective DS Protocol using the DS Standard STB 1176.2-9

Suppose that m users should sign the given message M. The collective DS protocol works as follows.

1. Each of the users generates his individual random value k_i and computes $T_i = g^{(k_i)}$.

2. It is computed the common randomization parameter as the product $T = T_1 * T_2 * \ldots * T_m$.

3. It is computed the collective public key y of the specified set of signers $y = y_1 * y_2 * \ldots * y_m$, where $y_1, y_2, \ldots$, and y_m are are the individual public keys of signers $i = 1, 2, ..., m$.

4. Using the common randomization parameter T, the collective public key, and specified hash function F_H it is computed the first element e of the collective DS: $e = F_H(T||M||y)$.

5. Each of the users computes his share s_i in the second element of the collective DS: $s_i = k_i - x_i e \bmod q$, where $i = 1, 2, ..., m$.

6. The second element s of the collective DS (e, s) is computed as follows $s = \sum_{i=1}^{m} s_i \bmod q$.

Size of the value s is equal to h, since it is computed modulo prime q. The total size of the signature (e, s) is $h + h'$, where h' is the bit size of the specified hash function.

The signature verification is performed exactly as it is described in subsection A except the collective DS verification uses the collective public key $y = y_1 * y_2 * \ldots * y_m$.

The proposed collective DS protocol works correctly. Indeed,

$$T^{\bullet} = g^{(s)} * y^{(e)} = g^{\left(\sum_{i=1}^{m} s_i\right)} \left(y_i\right)^e =$$
$$= g^{\left(\sum_{i=1}^{m} (k_i - x_i e)\right)} * g^{\left(e \sum_{i=1}^{m} x_i\right)} =$$
$$= g^{\left(\sum_{i=1}^{m} k_i\right)} = g^{(k_1)} * g^{(k_2)} * ... * g^{(k_m)} = T \Rightarrow$$
$$\Rightarrow \quad e^{\bullet} = F_H\left(T^{\bullet} \,||\, M \,||\, y\right) = F_H\left(T \,||\, M \,||\, y\right) = e.$$

Since the equality $e^{\bullet} = e$ holds, then the collective signature produced with the protocol satisfies the verification procedure, i.e. the described collective signature protocol is correct.

C. Blind Collective Signature Protocol based on Belarusian DS Standard

Suppose some user U is intended to get a blind collective DS (corresponding to message M) of some set of m signers using a blind signature generation procedure. To solve this problem the user can apply the following protocol.

1. Each signer generates a random value $k_i < q$ and computes $T_i = g^{(k_i)}$, and sends the value T_i to each of the signers.

2. It is computed the common randomization parameter as the product $\overline{T} = T_1 * T_2 * \ldots * T_m$.

3. The value $\overline{T}$ is send to user U.

4. User U generates random values $\tau < q$ and $\varepsilon < q$ and computes the collective public key $y = y_1 * y_2 * \ldots * y_m$, the values $T = \overline{T} y^{(\tau)} g^{(\varepsilon)}$ and $e = F_H\left(T \,||\, M \,||\, y\right)$. The value e is the first element of the blind collective DS.

5. User U calculates the value $\overline{e} = e - \tau \bmod q$ and sends the value $\overline{e}$ to the signers.

6. Each signer using his individual value k_i and his secret key x_i computes his share in the blind collective DS: $\overline{s}_i = k_i - x_i \overline{e} \bmod q$.

7. It is computed the second part $\bar{s}$ of the blind collective DS: $\bar{s} = \bar{s}_1 + \bar{s}_2 + ... + \bar{s}_m \bmod q$.

8. User U computes the second parameter of the blind collective DS: $s = \bar{s} + \varepsilon \bmod q$.

The pair of numbers (e, s) is the blind collective signature to message M.

The signature verification procedure is exactly the same as described in the case of the collective DS based on Belarusian standard (see subsection B). The signature (e, s) is a valid collective DS corresponding to the message M.

Indeed, using the collective public key $y = y_1 * y_2 * \ldots * y_m = g^{\left(\sum_{i=1}^{m} x_i\right)}$ we get

$$\begin{aligned} T^{\bullet} &= g^{(s)} * y^{(e)} = g^{\left(\varepsilon + \sum_{i=1}^{m} s_i\right)} * y^{(\bar{e}+\tau)} = \\ &= g^{(\varepsilon)} g^{\left(\sum_{i=1}^{m} \bar{s}_i\right)} * y^{(\bar{e})} * y^{(\tau)} = \\ &= g^{\left(\sum_{i=1}^{m} (k_i - x_i \bar{e})\right)} * y^{(\bar{e})} * y^{(\tau)} * g^{(\varepsilon)} = \\ &= g^{\left(\sum_{i=1}^{m} k_i\right)} * g^{\left(-\bar{e}\sum_{i=1}^{m} x_i\right)} * y^{(\bar{e})} * y^{(\tau)} * g^{(\varepsilon)} = \\ &= \bar{T} * y^{(\tau)} * g^{(\varepsilon)} = T \;\Rightarrow\; e^{\bullet} = e. \end{aligned}$$

Thus, the protocol yields a valid blind collective DS (e, s) that is known to user U and unknown to each of the signers. The protocol provides anonymity of the user in the case when the message M and blind collective signature (e, s) will be presented to the signers. Anonymity means that the signers are not able to correlate the disclosed signature with only one act of the blind signing, if the signers have participated in two or more procedures of blind signing. Indeed, it is easy to show that arbitrary signature (e, s) can be get from any of the blind signatures $(\bar{e}, \bar{s})$ recorded by the signers with some random parameters τ and ε: $\tau = e - \bar{e} \bmod q$ and $\varepsilon = s - \bar{s} \bmod q$.

In the particular case $m = 1$ we have usual blind signature scheme based on the STB 1176.2-9 standard.

III. Collective and Blind Collective Signature Protocol based on Russian Signature Standard

A. Collective DS Protocol based on GOST R 34.10-2001

Russian signature standard GOST G 34.10-2001 [12]. The standard specifies the DS algorithm based on the elliptic curves (ECs) defined over the ground field $GF(p)$ with the following equation

$$y^2 = x^3 + ax + b \bmod p,$$

where $a,b \in GF(p)$ and y and x are coordinates of the EC points. Suppose it is given an EC satisfying the requirements by the standard and the point G the order of which is a large prime q.

Each of m signers generates his private key k_j and his public key $Q_j = k_j G, j = 1, \ldots, m$.

The collective DS protocol using GOST R 34.10-2001 is described as follows:

1. Each of signers selects a random value t_j and computes the EC point $R_j = t_j G, j = 1, \ldots, m$.

2. It is computed the collective public key Q as the sum of all individual public keys $Q = Q_1 + Q_2 + \ldots + Q_m$.

3. It is computed the following digest of all points R_j: $R = R_1 + R_2 + \ldots + R_m$ and the value $r = x_Q x_R \bmod q$, where x_R (x_Q) is the abscissa of the EC point R (Q). The value r is the first part of the collective DS.

3. Each user computes his share in the collective DS as follows $s_j = (rk_j + t_j e) \bmod q$, where $e = H \bmod q$ and H is the hash function value computed from the document to be signed.

4. The second part of the signature is $s = s_1 + s_2 + \ldots + s_m \bmod q$.

The collective signature is (r, s).

To verify a collective DS one is to perform the following steps.

1. Compute the collective public key as the point

$$Q = Q_1 + Q_2 + \ldots + Q_m.$$

2. Compute the EC point

$$R^* = (se^{-1} \bmod q)G + ((q - r)e^{-1} \bmod q)Q.$$

3. Compute the value $r^* = x_Q x_{R^*} \bmod q$ and compare r^* and r. If $r^* = r$, then the collective DS is valid.

B. Blind Collective Signature Protocol based on GOST R 34.10-2001

Below it is supposed that some user U is intended to get a blind collective DS using a blind signature generation procedure.

1. Each of signers selects a random value t_j and computes the EC point $R_j = t_j G, j = 1, \ldots, m$.

2. It is computed the collective public key Q as the sum of all individual public keys $Q = Q_1 + Q_2 + \ldots + Q_m$.

3. It is computed the following digest of all points R_j: $\bar{R} = R_1 + R_2 + \ldots + R_m$. The point $\bar{R}$ is sent to user U.

4. User U generates random values $\tau, \varepsilon \in \{1, 2, \ldots, q - 1\}$ and computes the point $R = \bar{R} + \tau Q + \varepsilon G$, the values $r = x_Q x_R \bmod q$ and $\bar{r} = (r/e + \tau) \bmod q$, where $e = H \bmod q$; H is the hash function value computed from the given message M. The value r is the first element of the blind collective DS.

5. User U sends the value $\bar{r}$ to the signers.

6. Each of the signers computes his share in the blind collective DS as follows $\bar{s}_j = (\bar{r} k_j + t_j) \bmod q$.

7. It is computed the second part $\bar{s}$ of the blind collective DS: $\bar{s} = \bar{s}_1 + \bar{s}_2 + \ldots + \bar{s}_m \bmod q$. The value $\bar{s}$ is send to user U.

8. User U computes the second part of the blind collective signature as follows $s = e(\overline{s} + \varepsilon) \bmod q$.

The pair of numbers (r, s) is the blind collective signature to message M.

The blind collective DS verification procedure is described in subsection A.

As compared with the previous version of the blind collective DS protocol based on the GOST R 34.10-2001 [13] the proposed protocol is characterized in computing the randomization parameter r depending on the collective public key and in using only two randomization parameters (instead of four randomization parameters in [13]).

In the particular case $m = 1$ we have usual blind signature scheme based on the GOST R 34.10-2001.

IV. Discussion

The proposed protocols based on the Belarusian DS standards are novel. The protocols based on the Russian DS standard represent new improved versions of the protocols proposed earlier in [13]. The new versions of the protocols based on GOST R 34.10-2001 contain important feature that consists in computing the signature randomization parameter depending on the collective public key. The correctness and security of the proposed version of the protocols can be proved analogously with the proof presented in [13] for earlier versions of such protocols. However security analysis of [13] considers the post signature formation attacks. To prevent attacks undertaken during the signature formation process [14] in the new versions of the collective and blind collective DS protocols the is used a novel mechanism of computing the signature randomization parameter.

The proposed collective DS protocols possess the following advantages:

i) the DS length is sufficiently small and does not depend on number of signers (the collective DS length is equals to the length of individual DS provided by the underlying DS algorithm),

ii) the standard public key infrastructure (PKI) is used, except the public key correctness procedure should be evidently specified while a public key is registered;

iii) the protocol is based on the DS algorithm recommended by official state standard ,

iv) the protocol can be efficiently used in practice for simultaneous signing a contract.

V. Conclusion

The Russian and Belarusian DS standards are sufficiently flexible and provide possibility of natural extension of their functionality, i.e. to implement the collective, blind, and blind collective DS protocols. The feature of the proposed protocols is computing the signature randomization parameter depending on the collective public key. This mechanism imparts the signature integrity property to the proposed protocols.

References

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

[2] B. Schneier, "Applied Cryptography," Second Edition, John Wiley & Sons, Inc. New York, 1996.

[3] D. Chaum, "Blind Signature Systems," U.S. Patent # 4,759,063. 19 July 1988.

[4] D. Chaum, "Security without identification: Transaction systems to make big brother obsolete," Communications of the AMS, vol. 28, no 10, pp. 1030-1044, 1985.

[5] D. Pointcheval and J. Stern, "Security Arguments for Digital Signatures and Blind Signatures," Journal of Cryptology, vol. 13, p. 361-396, 2000.

[6] R. L. Rivest, A. Shamir, and L. M. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Communications of the ACM, vol. 21, no 2, pp. 120-126, 1978.

[7] Min-Shiang Hwang and Cheng-Chi Lee, "Research Issues and Challenges for Multiple Digital Signatures," International Journal of Network Security, vol. 1. no 1, pp. 1-7, 2005.

[8] A. Boldyreva, "Efficient Threshold Signature, Multisignature and Blind Signature Shemes Based on the Gap-Diffi-Hellman-Group Signature Sheme," Springer-Verlag Lecture Notes in Computer Science, vol. 2139, pp. 31-46, 2003.

[9] N. A. Moldovyan, "Digital Signature Scheme Based on a New Hard Problem," Computer Science Journal of Moldova, vol. 16, no 2(47), pp. 163-182, 2008.

[10] N. H. Minh, N. A. Moldovyan, N. L. Minh, "New Multisignature Protocols Based on Randomized Signature Algorithms," 2008 IEEE International Conference on Research, Innovation and Vision for the Future in computing & Communication Technologies. University of Science - Vietnam National University, Ho Chi Minh City, July 13-17, 2008. Proc. pp. 23.pdf.

[11] Kharin Yu.S., Bernik V.I., Matveev G.V., Aguievich S.V. "Mathematic and computer foundations of cryptology," Novoe znanie, Minsk, 2003.- 381 p. (in Russian).

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

[13] N. A. Moldovyan, “Blind Signature Protocols from Digital Signature Standards,” Int. Journal of Network Security. 2011. Vol. 13. No. 1. pp. 22–30.

[14] M. Rjasko, M. Stanek, “Attacking M&M Signature Scheme,” (eprint.iacr.org/2010/308.pdf).

[15] Nguyen H. Minh, and Nikolay A. Moldovyan, “Protocols for Simultaneous Signing Contracts,” 2009 International Conference on Advanced Technologies for Communications, Hai Phong, Vietnam, October 12-14, 2009, pp. 31-34.