240-bit Collective Signature Protocol in a Non-cyclic Finite Group

Duy H.N
Department of Information Technology
Ha Noi, Viet Nam
aimezthngocduy207@yahoo.com

Minh N.H
Le Qui Don Technical University
Ha Noi, Viet Nam
hieuminhmta@ymail.com

Binh D.V
Military Information Technology Institute
Ha Noi, Viet Nam
binhdv@gmail.com

Moldovyan N.A
St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences, 14 Liniya, 39, St. Petersburg 199178, Russia (nmold@mail.ru)

***Abstract*—The article describes a collective digital signature protocol based on the difficulty of the discrete logarithm problem modulo a composite number that is a product of two strong primes having the 2:1 size ratio. The usage of difficult problems provide signature protocol with security improvement, because the probability to break the protocol has been reduced significant. This can be achieved due to the appearance of breakthrough solutions in the area of the factoring problem and the discrete logarithm modulo a prime problem. One of the features of the protocol is using the non-cyclic finite group. After selecting appropriate parameters which provide 80-bit security, the size of the proposed collectively signature is 240 bits and is not dependent on the number of signers.**

Keywords—cryptographic protocol, digital signature, collective signature, factorization problem, discrete logarithm problem, public key.

I. INTRODUCTION

In automated information systems digital signatures (DS) to electronic documents are usually computed using the public-key DS protocols. The DS algorithms used in practice are based on the computational difficulty of the following three problems: i) factoring a composite integer $n = qr$, where q and r are two strong primes [1] (for example, RSA [2], Rabin DS algorithm [3], the signature scheme [4-6]); ii) finding the discrete logarithm modulo a large prime p [7] ; iii) finding the discrete logarithm on an elliptic curve (EC) of special type (the DS standards ECDSA [8]). Among DS schemes representing significant practical interest one can mention the collective DS (CDS) protocols based the difficulty of the discrete logarithm problems [9-11]. The CDS protocols extend the application areas of the public-key DS technology in practical informatics. Security of the DS protocols is due to the following two facts i) the best known algorithms for forging a signature are computationally infeasible and ii) the probability of the appearing of a breakthrough algorithm, which is used to solve the computationally difficult problem put into the base of the protocols in the foreseeable future, is negligibly small. In order to improve security DS protocols in [12-14] propose such design of the protocols that forging a signature requires to solve simultaneously two independent computationally difficult problems, i.e., factorization problem (FP) and the discrete logarithm (modulo a prime) problem (DLP). However, in the proposed protocols in [12-14], the signature size is more than 1024 bits. An alternative approach [15], which is based on the use of computational complexity of the DLP modulo a composite number n that is difficult for factoring the decomposition of modules, provides 3 solutions. Those are reducing the size of the signature, increasing a performance of the protocol and extending types of the cryptographic protocols based on the computational difficulty of the simultaneous solving the FP and DLP modulo a prime problems. Justification of the cryptoschemes based on the computational difficulty of solving simultaneously two independent hard problems, is connected with the term of integrated security parameter, W/P ratio[12], where W is the computational difficulty of the hard problem put into the base of the cryptoscheme, and P is the probability of the appearance in near future a breakthrough algorithm for solving that problem. Thus, raising the value W or/and reducing the value P will increase(s) the integrated security parameter. If breaking a public key cryptoscheme requires solving simultaneously two independent hard problems, the probability P will be significantly reduced. In this paper, using the approach by [15], we proposes a design of the collective DS protocols based on the computational difficulty of the DLP modulo $n = pq$, where p and q are two strong primes such that their size ratio is 2:1. A peculiarity of the proposed protocol consists in using computation in a finite non-cyclic subgroup G of the multiplicative group $\mathbb{Z}_n^*$. First, it is constructed the protocol of individual (ordinary) signature based on difficulty of the DLP mod n and then the individual signature

978-1-4799-6956-2/14/$31.00 ©2014 IEEE

scheme is modified into the collective DS using the approach proposed in [9,10].

II. Basic Parameters of Cryptographic Scheme

Initially, 240-bit signature scheme is constructed (the base DS scheme) and then it is used as the base DS algorithm while designing the collective DS protocol in frame of the approach proposed in papers [9, 10]. In the base DS scheme, there is a used noncyclic subgroup G of the multiplicative group $\mathbb{Z}_n^*$ of a finite ring $\mathbb{Z}_n$ where n is a natural number equal to the product of two strong primes q and p having the size $|q| \approx \lambda$ bits, $|p| \approx 2\lambda$ bits, correspondingly. The parameter λ is selected depending on the required security level, for example, $\lambda \approx 512$ bits in the case of 80-bit security and $\lambda \approx 1232$ bits in the case of 128-bit security. Numbers q and p are secret and have the following structure: $p = N_p r + 1$ and $q = N_q r + 1$, where N_p and N_q are two large even numbers; r is a ρ-bit prime number (for the resistance equal to 2^W modular multiplication operations, we should choose the value $\rho \geq W$). The used subgroup G has the order r^2 and it is generated by two integers α and β that generate two different cyclic subgroups of $\mathbb{Z}_n^*$, each of them having the prime order r. In [16], the authors proposed a probabilistic procedure for finding the values α and β, such that the probability that they belong to the same cyclic subgroup of order r is negligible. Although that procedure suites well for practical applications, it is not deterministic. In this paper, we implement the following deterministic algorithm for finding values α and β that guaranteed set a noncyclic primary subgroup G having an order equal to r^2.

A. Algorithm 1

1. Generate a value γ having order equal to r modulo p.
2. Generate a value δ having order equal to r modulo q.
3. Select at random values $0 < h < r$ and $0 < k < r$ and find the value α that satisfies the following system of congruences:

$$\begin{cases} \alpha \equiv \gamma^k \bmod p \\ \alpha \equiv \delta^h \bmod q \end{cases}. \quad (1)$$

4. Select at random values $0 < g < r$ and $0 < m < r$ satisfying the condition $gh \neq km \bmod r$, and find the solution β of the following system of congruences:

$$\begin{cases} \beta \equiv \gamma^g \bmod p \\ \beta \equiv \delta^m \bmod q \end{cases}. \quad (2)$$

This algorithm outputs the values α and β that belong to different cyclic subgroups having order r, so the products (modulo n) of all possible powers of the values α and β compose a primary subgroups having order r^2. Indeed, the order of α and β is equal to r, since the following formulas holds:

$$\left\{\left\{\alpha^r \equiv \gamma^{kr} \equiv 1 \bmod p\right\} \cup \left\{\alpha^r \equiv \delta^{hr} \equiv 1 \bmod q\right\}\right\} \Rightarrow \alpha^r \equiv 1 \bmod n; \quad (3)$$

$$\left\{\left\{\beta^r \equiv \gamma^{gr} \equiv 1 \bmod p\right\} \cup \left\{\beta^r \equiv \delta^{mr} \equiv 1 \bmod q\right\}\right\} \Rightarrow \beta^r \equiv 1 \bmod n. \quad (4)$$

In addition, the following statement also holds.

B. Statement 1.

Algorithm 1 outputs the values α and β such that inequality $\alpha \neq \beta^d \bmod n$ holds for all values $d \in \{1, 2, \ldots, r\}$.

Proof. It is obvious that the inequality $\alpha \neq \beta^r \bmod n$. Suppose that for some value $d \in \{1, 2, \ldots, r-1\}$ the equality $\alpha = \beta^d \bmod n$ holds.

From (1) one can get the following:

$\{\beta^d \equiv \gamma^k \bmod p\} \Rightarrow \{\beta \equiv \gamma^{k/d} \bmod p\}$ and

$\{\beta^d \equiv \delta^h \bmod q\} \Rightarrow \{\beta \equiv \gamma^{h/d} \bmod q\}$

From (2) one can get the following:

$\{\gamma^g \equiv \gamma^{k/d} \bmod p\} \Rightarrow \{g \equiv k/d \bmod r\}$ and

$\{\delta^m \equiv \delta^{h/d} \bmod q\} \Rightarrow \{m \equiv h/d \bmod r\}$.

Therefore we have $\{d \equiv k/g \bmod r\}$ and $\{d \equiv h/m \bmod r\}$, hence $km \equiv hg \bmod r$. This contradicts condition $gh \neq km \bmod r$, used in step 4 of the algorithm when choosing g and m. The assertion is proved.

Thus, due to Statement 1 the product (mod n) of all possible powers of the values α and β generate r^2 different values of the form $\alpha^i \beta^j \bmod n$, each of which has order equal to r: $\left(\alpha^i \beta^j\right)^r \equiv \alpha^{ir} \beta^{jr} \equiv 1 \cdot 1 \equiv 1 \bmod n$.

In the proposed collective DS protocol below it is assumed that the parameters n, α, β, and r are generated by some trusted party using randomly selected strong primes p and q having the size providing the required security value. After the computation the parameters n, α, β, and r the secret values p and q are destroyed. Each user generates her/his private key as a pair of the random integers x and w ($1 < x < r$; $1 < w < r$) and to compute the public key y in accordance with the following formula: $y = \alpha^x \beta^w \bmod n$.

C. The ρ-bit signature generation procedure is performed as follows:

1. Select at random values $k < r$ and $t < r$ and calculate $R = \alpha^k \beta^t \bmod n$.
2. Using some specified 2ρ-bit hash function $F_H(M)$ calculate the hash value H corresponding from the message M. Interpret the value $F_H(M)$ as a concatenation of two ρ-bit numbers: $F_H(M) = H_1 \| H_2$.
3. Calculate the first ρ-bit element E of the signature: $E = F_H(M, R) \bmod r$.
4. Calculate the second ρ-bit element S of the signature: $S = \dfrac{k + xE}{H_1} \bmod r$.
5. Calculate the third ρ-bit element U of the signature: $U = \dfrac{t + wE}{H_2} \bmod r$.

The triples of numbers (E, S, U) is the signature to the electronic document M. The signature length is fixed and equals to 3ρ.

D. Verification of the DS is performed using the public key y as follows:

1. Compute the value $F_H(M) = H_1||H_2$.
2. Compute $\tilde{R} = y^{-E}\alpha^{SH_1}\beta^{UH_2} \bmod n$ and $\tilde{E} = F_H\left(M, \tilde{R}\right) \bmod r$.
3. Compare values E' and E. If $E' = E$, then the signature is valid. Otherwise the signature is false.

The value ρ should be consistent with the size of the modulus n, which is equal to 3λ bits, and both the value ρ and the value λ are chosen depending on the required security of the protocol. To provide 80-bit (128-bit) security we should use the parameters ρ ≥ 80 (ρ ≥ 128) and λ ≥ 512 (λ ≥ 1232).

III. Collective Signature Protocol

Using the previously described DSS we can propose the following 3ρ bit collective signature protocol. Suppose the ith user owns the public key y_i depending on his private key (x_i, w_i) as follows: $y_i = \alpha^{x_i}\beta^{w_i} \bmod n$, where $i = 1, 2, \ldots, s$. Given an electronic document M and m ($m < s$) users owning the public keys $y_1, y_2, \ldots, y_m$ should sign it simultaneously.

Compute the collective public key y: $y = \prod_{i=1}^{m} y_i \bmod n.$

A. The following protocol produces the collective digital signature (CDS):

1. Each i-th user selects at random values k_i and t_i, and computes the public value $R_i = \alpha^{k_i}\beta^{t_i} \bmod n$, where $i = 1, 2, \ldots, m$ and sends R_i to all signers.
2. One of them calculates the common randomization value: $R = \prod_{i=1}^{m} R_i \bmod n.$
3. Calculate the first ρ-bit element of the CDS:

   $E = F_H(M, R, y) \bmod r$, where $F_H(M, R) = H_1||H_2$.
4. Each signer computes its shares signature S_i and U_i using the hash function values H_1 and H_2 corresponding to the document and the value E, is given below:

$$S_i = \frac{k_i + x_i E}{H_1} \bmod r,$$

$$U_i = \frac{t_i + w_i E}{H_2} \bmod r.$$

5. Calculate the second element of the CDS:

$$S = \sum_{i=1}^{m} S_i = \frac{\sum_{i=1}^{m} k_i + E\sum_{i=1}^{m} x_i}{H_1} \bmod r.$$

6. Calculate the third element of the CDS:

$$U = \sum_{i=1}^{m} U_i = \frac{\sum_{i=1}^{m} t_i + E\sum_{i=1}^{m} w_i}{H_2} \bmod r.$$

The triples of numbers (E, S, U) is the CDS to document M. The CDS length does not depend on the number of signers and equals to 3ρ.

B. Verification of the CDS is performed using the collective public key y computed as product of the public keys of all signers:

1. Calculate $F_H(M) = H_1||H_2$.
2. Compute the collective public key $y = \prod_{i=1}^{m} y_i \bmod n.$
3. Calculate $\tilde{R} = y^{-E}\alpha^{SH_1}\beta^{UH_2} \bmod n$ and $\tilde{E} = F_H\left(M, \tilde{R}, y\right) \bmod r$.
4. Compare values $\tilde{E}$ and E. If $\tilde{E} = E$, then the signature is valid. Otherwise the signature is false.

Correctness proof of the described CDS protocol is as follows.

Substituting the value U and S in the right part of the verification equation $\tilde{R} = y^{-E}\alpha^{SH_1}\beta^{UH_2} \bmod n$ we get:

$$\tilde{R} \equiv y^{-E}\alpha^{SH_1}\beta^{UH_2} \equiv \left(\prod_{i=1}^{m} y_i\right)^{-E} \alpha^{H_1\sum_{i=1}^{m} S_i}\beta^{H_2\sum_{i=1}^{m} U_i} \equiv$$

$$\equiv \left(\alpha^{\sum_{i=1}^{m} x_i}\beta^{\sum_{i=1}^{m} w_j}\right)^{-E} \alpha^{H_1\sum_{i=1}^{m} S_i}\beta^{H_2\sum_{i=1}^{m} U_i} \equiv$$

$$\equiv \alpha^{-E\sum_{i=1}^{m} x_i}\beta^{-E\sum_{i=1}^{m} w_j}\alpha^{H_1\frac{\sum_{i=1}^{m} k_i + E\sum_{i=1}^{m} x_i}{H_1}}\beta^{H_2\frac{\sum_{i=1}^{m} t_i + E\sum_{i=1}^{m} w_i}{H_2}} \equiv$$

$$\equiv \alpha^{-E\sum_{i=1}^{m} x_i}\beta^{-E\sum_{i=1}^{m} w_i}\alpha^{\sum_{i=1}^{m} k_i + E\sum_{i=1}^{m} x_i}\beta^{\sum_{i=1}^{m} t_i + E\sum_{i=1}^{m} w_i} \equiv$$

$$\equiv \alpha^{\sum_{i=1}^{m} k_i}\beta^{\sum_{i=1}^{m} t_i} \equiv \prod_{i=1}^{m}\alpha^{k_i}\beta^{t_i} \equiv \prod_{i=1}^{m} R_i \equiv R \bmod n$$

$$\Rightarrow \tilde{R} = R$$

$$\Rightarrow \tilde{E} = E.$$

The last equality proves the correctness of the protocol developed by the collective DS. Thus, the collective DS that is formed using the private keys of all signers is recognized by the signature verification procedure as a valid CDS.

IV. Conclusion

In this paper, we proposed a new collective DS protocol with the 3ρ-bit signature size which provides ρ-bit security. The

protocol is the first that is based on the computational difficulty of the DLP modulo a composite number $n = pq$. The prime factors p and q satisfies condition $p \approx q^2$ that is difficult for factoring. Solving the used computational problem is as difficult as simultaneous solving the FP and the DLP modulo prime p [15]. Therefore the proposed protocol can be considered as a cryptoscheme having significantly higher integrated security parameter W/P introduced in [12]. The individual signature scheme described in Section 2 can be also put into the base of the blind DS and blind CDS protocols detailed consideration of which represents an individual work.

REFERENCES

[1] J. Gordon, "Strong primes are easy to find," Advances in cryptology – EUROCRYPT'84, Springer-Verlag LNCS, 1985, vol. 209, pp. 216–223

[2] R.L. Rivest , A. Shamir , and L.M.A. Adleman, " Method for Obtaining Digital Signatures and Public Key Cryptosystems," Communications of the ACM, 1978, vol. 21, n. 2, pp. 120-126.

[3] M.O. Rabin, "Digitalized signatures and public key functions as intractable as factorization," Technical report MIT/LCS/TR-212, MIT Laboratory for Computer Science, 1979.

[4] A.A. Moldovyan, D.N. Moldovyan, L.V. Gortinskaya, "Cryptoschemes based on new signature formation mechanism," Computer Science Journal of Moldova. 2006, vol. 14, no. 3(42), pp. 397-411.

[5] N.A. Moldovyan, "Short Signatures from Difficulty of Factorization Problem," Int. Journal of Network Security, 2009, vol. 8, no. 1, pp. 90-95.

[6] A.A. Moldovyan, N.A. Moldovyan, V.A. Shcherbakov, " Short signatures from difficulty of the factoring problem," Buletinul Academiei de Stiinte a Republicii Moldova. Matematica, 2013, no. 2(72)-3(73), pp. 27-36.

[7] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Transactions on Information Theory, 1985, vol. it-31, no. 4, pp. 469–472.

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

[9] N.A. Moldovyan, A.A. Moldovyan, "Blind Collective Signature Protocol Based on Discrete Logarithm Problem," Int. Journal of Network Security, 2010, vol. 11, no. 2, pp. 106-113.

[10] N.A. Moldovyan, "Blind Signature Protocols from Digital Signature Standards," Int. Journal of Network Security, 2011, vol. 12, no. 3, pp. 202-210.

[11] N.A. Moldovyan, "Blind Collective Signature Protocol," Computer Science Journal of Moldova, 2011, vol. 19, no. 1, pp. 80–91.

[12] N.H. Minh, D.V. Binh, N.T. Giang, N.A. Moldovyan, "Blind Signature Protocol Based on Difficulty of Simultaneous Solving Two Difficult Problems," Applied Mathematical Sciences, 2012, vol. 6, no. 139, pp. 6903 – 6910.

[13] N.M.F. Tahat, S.M.A. Shatnawi, E.S. Ismail, "New Partially Blind Signature Based on Factoring and Discrete Logarithms," Journal of Mathematics and Statistics, 2008, vol. 4 (2), p. 124-129.

[14] N.M.F. Tahat, E.S. Ismail, R.R. Ahmad, "A New Blind Signature Scheme Based On Factoring and Discrete Logarithms," International Journal of Cryptology Research, 2009, vol.1 (1), pp.1-9.

[15] A.N. Berezin, N.A. Moldovyan, V.A. Shcherbakov, "Cryptoschemes Based on Difficulty of Simultaneous Solving Two Different Difficult Problems," Computer Science Journal of Moldova, 2013, vol. 21, no. 2(62), pp. 280-290.

[16] A.A. Moldovyan, N.A. Moldovyan, E.S. Novikova, "Blind 384-bit Digital Signature Scheme," // Proceedings of the International workshop, Methods, Models, and Architectures for Network Security MMM ACNS 2012, October 17, St.Petersburg, Russia / Lect, Notes in Computer Science, Berlin: Springer-Verlag, 2012, vol. 7531, pp. 77-83.