UDK 681.3

An Electronic Digital Signature Algorithm Based on a Composition of Computational Difficulties: Discrete Logarithm, Factorization, and Addition of Points of an Elliptic Curve

D.E. Akbarov[1], *Sh.A. Umarov*[2]
[1]Kokand Pedagogical Institute, Kokand, Uzbekistan
[2] Ferghana branch of Tashkent University of Information Technologies named after Muhammad Al-Khwarizmi, Ferghana, Uzbekistan

Abstract: The article developed a new algorithm for electronic digital signature in the composition of existing difficulties: discrete logarithm in a finite field, decomposition of a sufficiently large natural number into prime factors, addition of points with rational coordinates of the elliptic curve. Based on a combination of the complexities of a discrete logarithm on a finite field with a large number characteristic, decomposition of a sufficiently large odd number into prime factors, and addition of points of an elliptic curve, an electronic digital signature algorithm is developed for generating. The generally recognized scheme (model) of electronic digital signature covers three processes: generation of digital signature keys; EDS formation; verification (confirmation of authenticity) of electronic digital signature. The design idea of the proposed algorithm allows you to modify and increase cryptographic strength with the addition of other computational difficulties. It is intended for use in information processing systems for various purposes in the formation and authentication of electronic digital signatures.

Key words: algorithm, electronic digital signature, prime factors, elliptic curve, hash value, Euler function, generation, correctness, cryptographic strength

INTRODUCTION

The electronic digital subscript in the electronic document, received because of special transformations of the information of the given electronic document with usage. Of the closed key of an electronic digital subscript and allowing by means of an open key of an electronic digital subscript establishes the lack of distortion of the information in the electronic document and identifies the owner of the closed key of an electronic digital subscript.

Existing algorithms of an electronic digital subscript is developed based on one of computing complexity: expansions on prime factors, a discrete taking the logarithm, and addition of points of an elliptic curve and [1-5].

1. PROBLEM STATEMENT

In this article on the basis of a combination of complexities of the discrete logarithm on the final field with the great number, expansions of enough big odd number on prime factors and additions of points of an elliptic curve develops Algorithm of the Electronic Digital Subscript (AEDS) for shaping and acknowledgement of authenticity of an electronic digital subscript (EDS) under the set message (the electronic document), transmitted on not protected telecommunication channels of the general use [7-9].

2. SOLUTION OF STATEMENT OF A PROBLEM

Following labels are used:

M - the message;

H (M) - hash-value of message *M*;

p_1, q_1 - big enough prime numbers, i.e. $p_1 > 2512$ and $q_1 > 2512$;

$n = p_1 q_1$ - the great number suffices;

$\varphi(n)$ - Euler's function;

a - an integral number defined from equality $ed - a\varphi(n)=1$;

d, *x* - integral numbers - closed keys of EDS;

k - signed a chosen random number from an interval $1 < k < q$;

e, *y* - integral numbers and *Q*- a point on an elliptic curve - open keys of EDS;

G- a base point on the chosen elliptic curve;

q - a prime number defining an order of a base point *G*;

(r, s, γ) - triple of integral numbers, an electronic digital subscript under *the M* message;

The conventional scheme (model) of an electronic digital subscript envelops three processes [6-7]:

- Generation of keys of EDS;
- Shaping EDS;
- Check (authenticity acknowledgement) EDS.

The basic mathematical definitions and the requirements superimposed on plants of algorithm of a digital subscript are given below.

For a subscript of message *M*, the signing by generating keys: *e*- opened and *d*- confidential of comparison $de1 \equiv \mod \varphi(n)$ where the great number suffices $n=p_1q_1$, p_1q_1 – unknown prime numbers (satisfying to conditions $p_1>2512$, $q_1>2512$), $\varphi(n)$ - Euler's function, for accuracy $p_1>q_1$, let gets out a random number *k* and *x*, and $1<k<q$, *q* - a prime

number and $q<q_1$, $1<x<q$ and
NOD (x, n)=1, the parameter $g<n$ gets out on condition NOD(q, n)=1 and $g^q \bmod n \neq 1$, and also q is not a divider $\varphi(n)$.

Open keys are: $y=g^{axd} \bmod n$ the number an is defined from equality $ed - a\varphi(n)=1$ and $Q=[x]G$, where G- the base point having an order q (where q - a prime number), on the chosen elliptic curve.

In algorithm of EDS it is used following parameters [10-12]:

1) Open keys: y - generated by a rule $y=g^{axd} \bmod n$, and $1<x<q$ where confidential keys x and d, are known only to the signed person; e – generated from comparison $de1 \equiv \bmod \varphi(n)$; Q - an elliptic curve point generated by a rule $Q=[x]G$, where G- the base point having an order q, on the chosen elliptic curve;
2) Hashing function $H(M)$ which under the initial message (text) M forms an integral number in a range from 1 to q, i.e. $1<H(M)<q$.
3) Each user of AEDS should possess personal keys:

a) d, x - integral numbers - closed keys of EDS and signed a chosen random number k from an interval $1<k<q$;

b) y - an integer and Q - a point on an elliptic curve - open keys of EDS.

The prime number q is opened and can be the general for group of users.

Processes of shaping of an electronic digital subscript under the message of the user and authenticity acknowledgement.

For realization of the given processes, it is necessary, that to all users parameters of algorithm of an electronic digital subscript were known. Besides, each user to have closed key of EDS (d, x) and open key of EDS (e, y, Q).

For creation of an electronic digital subscript under *the* M message, it is necessary to fulfil following operations (pitches).

3. ALGORITHM SUBSCRIPT GENERATION

Input data: message M, initial parameters, confidential and discovery keys.

Output data: a subscript (r, s, γ).

Pitches of algorithm of generation of a subscript:

1. To calculate value $H(M)$ according to M, i.e. $h=H(M)$.

2. On the chosen random number k (to keep it a secret and to destroy at once after deriving subscripts) it is calculated: $[k]G=(x_1,y_1)$.

3. It is calculated: $r = g^{x_1 d} \bmod n \bmod q$.

4. It is calculated: $\rho = g^d \bmod n$.

5. It is calculated: $s = [k^{-1}(H(M)\rho + r\rho x)] \bmod q$.

6. It is calculated: $\gamma = (g^{-ax}\rho) \bmod n$.

7. A subscript is triple: (r, s, γ).

Further the signed message is transmitted a receiving leg.

For acknowledgement of authenticity of EDS under received message M it is necessary to fulfil following operations (pitches).

4. ALGORITHM SUBSCRIPT CHECK

Input data: message M, initial parameters, an open key of check of a subscript and a subscript to M - triple (r, s, γ).

Output data: the statement that a subscript valid or not the valid.

1. If conditions $1 \le r, s < q$ also $1 \le \gamma < n$ are broken, «a subscript not valid» and to finish algorithm work.

2. To calculate value $H(M)$ according to M, i.e. $h=H(M)$.

3. To calculate: $w = y^e \bmod n$.

4. To calculate: $\beta = w\gamma \bmod n = \rho \bmod n = \rho$ as $\rho < n$.

5. To calculate: $u_1 = [s^{-1}H(M)\beta] \bmod q = s^{-1}H(M)\rho - a_1 q$.

6. To calculate: $u_2 = (s^{-1}r\beta) \bmod q = s^{-1}r\rho - a_2 q$.

7. To calculate: $[u_1]G + [u_2]Q = (x_2, y_2)$.

8. If $u = \beta^{x_2} \bmod n \bmod q = r$, a subscript valid, differently the void.

5. CORRECTNESS OF AEDS

For the correctness proof it is necessary to show to justice equality: $[u_1]G + [u_2]Q = (x_2, y_2) = (x_1, y_1) = [k]G$. Really, from expression

$$s = (H(M)\rho + r\rho x)\ k^{-1} \bmod q$$

We discover:

$$k = [s^{-1}(H(M)\rho + r\rho x)] \bmod q =$$

$$[s^{-1}H(M)\rho + s^{-1}r\rho x] \bmod q =$$

$$s^{-1}H(M)\rho + s^{-1}r\rho x - a_3 q.$$

Then:

$$[k]G = s^{-1}H(M)\rho\ [+]\ s^{-1}r\rho x - a_3 q\ G =$$

$$[s^{-1}H(M)\rho]G + [s^{-1}r\rho][x]G - [a_3][q]G =$$

$$[u_1]G + [u_2]Q.$$

On the other hand:

$$[u_1]G + [u_2]Q = [s^{-1}H(M)\rho - a_1 q]G + [$$

$$s^{-1}r\rho - a_2 q][x]G = [s^{-1}H(M)\rho]G + [s^{-1}r\rho x]G -$$

$$[a_1 + a_2 x][q]G = [s^{-1}H(M)\rho + s^{-1}r\rho x]G =$$

$$= [s^{-1}(H(M)\rho + r\rho x)]G = [k]G.$$

Thus, the algorithm correctness is proved.

6. THE ANALYSIS OF OUTCOMES

Crypto stability existing AEDS it is based on one of having computing complexities. In offered AEDS, its cryptographic firmness is based on several complexities: evaluations of a discrete taking the logarithm in a final field, solutions of a problem of expansion of enough big odd number to prime factors, realizations of addition operation of points of the elliptic curve set in a final field. It considerably raises crypto stabilities.

7. CONCLUSION

The idea of a design of offered algorithm allows modifying and raising crypto stabilities with adding of other computing complexities. It is intended for use in data reduction systems of different function at shaping and acknowledgement of authenticity of an electronic digital subscript.

REFERENCES

[1] Ajish S., AnilKumar K. S. Security and Performance Enhancement of Fingerprint Biometric Template Using Symmetric Hashing. Computers & Security. – 2020. – С. 101714. DOI: 10.1016/j.cose.2020.101714

[2] Górski G., Wojsa M. New Encryption Method with Adaptable Computational and Memory Complexity Using Selected Hash Function. International Conference on Information Systems Architecture and Technology. – Springer, Cham, 2019. – С. 209-218. DOI: 10.1007/978-3-030-30440-9_20

[3] M. Norouzi, D.M. Blei. Minimal loss hashing for compact binary codes. Proceedings of the 28th International Conference on Machine Learning (2011), pp. 353-360

[4] Vostrov G. Dynamic processes of hash function formation in a system of finite fields = Динамічні процеси формування хеш-функцій в системі кінцевих полів. G. Vostrov, O. Ponomarenko. Electrotechnic and Computer Systems = Електротехнічні та комп'ютерні системи. Науково-технічний журнал. – 2018. – № 28(104). – С. 233-239.

[5] Weng Z., Zhu Y. Concatenation hashing: A relative position preserving method for learning binary codes. Pattern Recognition. – 2020. – Т. 100. – С. 107151. DOI: 10.1016/j.patcog.2019.107151

[6] Agibalov G. P., Pankratova I. A. Elements of the theory of statistical analogues of discrete functions using iterative block ciphers in cryptanalysis. Prikl. 2010. No. 3 (9). 51-68. (in Russian).

[7] Akbarov D.E. Akhborot hafsizligini tamminlashning cryptographics usullari wa ularning аnиllanylish. Uzbekiston marcassi. - 2009. - T. 432. (in Russian).

[8] Akbarov D.E., Umarov Sh.A. The hash function subscript. algorithm with new basic transformations. News of the National Technical University of Ukraine "Kyiv Polytechnic Institute". Seriya: Priladobuduvannya. 2016. No. 51 (1). S. 100-108. DOI: https://doi.org/10.20535/1970.51(1).2016.78112. (in Russian).

[9] Akbarov D.E., Khasanov H.P. Algorithm for electronic digital signature based on the composition of complexities. (Gup "Unicon.Uz"). (in Russian).

[10] Akbarov D.E., Umarov Sh.A. New symmetric key block data encryption algorithm. Newsletter of the National Technical University of Ukraine "Kyiv Polytechnic Institute". Seriya: Priladobuduvannya. 2016. No. 52 (2). S. 82-91. DOI: https://doi.org/10.20535/1970.52(2).2016.92963. (in Russian).

[11] Karondeev A. M. Addition modulo 2n in block encryption. PDM. Appendix, 2015, No. 8, 62–63. DOI: https://doi.org/10.17223/2226308X/8/22. (in Russian).

[12] Raceev S. M., Ivantsov A. M. About some properties of cryptographic hash functions. Automation of control processes. - 2019. - No. 2. - S. 53-58. doi: 10.35752 / 1991-2927-2019-2-56-53-58. (in Russian).

Davlatali Egitalievich Akbarov - Doctor of Physics and Mathematics, Associate Professor of the Department of "Mathematics" of the Kokand Pedagogical Institute.
Tel.: +998993684304,
E-mail: sht00357@gmail.com

Republic of Uzbekistan, Kokand city Turon 23

Shukhratjon Azizjonovich Umarov - Senior Lecturer, Department of Information Technology, Ferghana branch of the Tashkent University of Information Technology named after Muhammad Al-Khwarizmi,
Tel .: +998913961130.
E-mail: sh.umarov81@mail.ru

Republic of Uzbekistan, Ferghana, st. Mustakillik 185.

The paper has been received on 05.05.2020.