The American Journal of Engineering and Technology
(ISSN – 2689-0984
Published: April 30, 2021 | Pages: 102-107
Doi: https://doi.org/10.37547/tajet/Volume03Issue04-16

IMPACT FACTOR
2021: 5. 705
OCLC - 1121105677

Algorithm Of The Electronic Digital Subscript On The Basis Of The Composition Of Computing Complexities

Davlatali Egitaliyevich Akbarov
Doctor Of Physics And Mathematics, Associate Professor, Department Of Mathematics Kokand Pedagogical Institute, Republic Of Uzbekistan

Shukhratjon Azizjonovich Umarov
Senior Teacher, Department Of Information Technology, Fergana Branch Of The Tashkent University Of Information Technologies Named After Muhammad Al-Khwarizmi, Republic Of Uzbekistan

Abbosjon Erali Ugli Toychiboyev
Student, Department Of Computer Engineering, Fergana Branch Of The Tashkent University Of Information Technologies Named After Muhammad Al-Khwarizmi, Republic Of Uzbekistan

ABSTRACT

In article the new algorithm of a digital signature in composition of the existing difficulties is developed: discrete logarithming in a final field, decomposition of rather large natural number on simple multipliers, additions of points with rational coordinates of an elliptic curve. On the basis of a combination of difficulties of discrete logarithming on a final field with the characteristic of large number, decomposition of rather large odd number on simple multipliers and additions of points of an elliptic curve develops algorithm of a digital signature for formation. The conventional scheme (model) of a digital signature covers three processes: generation of keys of EDS; formation of EDS; check (authenticity confirmation) of EDS. The idea of a design of the offered algorithm allows modifying and increasing crypto stability with addition to other computing difficulties. It is intended for use in systems of information processing of different function during forming and confirmation of authenticity of digital signature.

KEYWORDS

Algorithm, electronic digital signature, simple multipliers, elliptic curve, hash value, Euler function, generation, correctness, crypto stability

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].

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 [8-9].

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 $de1 \equiv \bmod \varphi(n)$ 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 mod$n \neq 1$, and also q is not a divider $\varphi(n)$.
Open keys are: $y=g^{axd}$ mod$n$ 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 [10-11]:

1. Open keys: *y* - generated by a rule $y=g^{axd}$ mod*n*, and 1<*x*<*q* where confidential keys *x* and *d*, are known only to the signed person; *e* – generated from comparison *de*1 ≡mod $\varphi(n)$; *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).

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).

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≤ 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.

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:

$[k]G = s^{-1}H(M)\rho\,[+]\quad s^{-1}r\rho x - a_3 q\ G = [$ $s^{-1}H(M)\rho]G +\quad [s^{-1}r\rho][x]G - [a_3][q]G =$ $[u_1]G + [u_2]Q$.

On the other hand:

$[u_1]G + [u_2]Q = [s^{-1}H(M)\rho - a_1 q]G + [$ $s^{-1}r\rho - a_2 q][x]G = \quad = [s^{-1}H(M)\rho]G + [$ $s^{-1}r\rho x]G - [a_1 + a_2 x][q]G = [s^{-1}H(M)\rho +$ $s^{-1}r\rho x]G =$
$= [s^{-1}(H(M)\rho + r\rho x)]G = [k]G$.

Thus, the algorithm correctness is proved.

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.

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., and KS Anil Kumar. "Security and performance enhancement of fingerprint biometric template using symmetric hashing" Computers & Security 90 (2020): 101714.
2. Akbarov D.E., Umarov Sh.A. "Applying logical operations and table replacements in modeling basic transformations of

symmetric block encryption algorithms." International Journal of Mechanical and Production Engineering Research and Development 10.3 (2020): 15041–15046.

3. Akbarov D. E., Umarov S. A. An Electronic Digital Signature Algorithm Based on a Composition of Computational Difficulties: Discrete Logarithm, Factorization, and Addition of Points of an Elliptic Curve //Common Information about the Journal A&SE. – 2020. – T. 10. – C. 10.
4. 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. – №. 52. – C. 2.
5. Johnson, Don, Alfred Menezes, and Scott Vanstone. "The elliptic curve digital signature algorithm (ECDSA)." International journal of information security 1.1 (2001): 36-63.
6. Kazmirchuk, Svitlana, Ilyenko Anna, and Ilyenko Sergii. "Digital signature authentication scheme with message recovery based on the use of elliptic curves." International Conference on Computer Science, Engineering and Education Applications. Springer, Cham, 2019.
7. Klokov, I. A., Andreeva, K. A., Polushkina, I. A. "Application of the algorithm of encryption of electronic-digital signature." Наука и просвещение: актуальные вопросы, достижения и инновации. (2020): 43-45.
8. Norouzi, Mohammad, and David J. Fleet. "Minimal loss hashing for compact binary codes." ICML. 2011.
9. Weng, Zhenyu, and Yuesheng Zhu. "Concatenation hashing: A relative position preserving method for learning binary codes." Pattern Recognition 100 (2020): 107151.
10. Агибалов, Геннадий Петрович, and Ирина Анатольевна Панкратова. "Элементы теории статистических аналогов дискретных функций с применением в криптоанализе итеративных блочных шифров." Прикладная дискретная математика 3 (9) (2010).
11. Рацеев, Сергей Михайлович, and Андрей Михайлович Иванцов. "О НЕКОТОРЫХ СВОЙСТВАХ КРИПТОГРАФИЧЕСКИХ ХЕШ-ФУНКЦИЙ." Автоматизация процессов управления 2 (2019): 53-58.
12. Akbarov D.E. Umarov Sh.A. Working out the new algorithm enciphered the data with a symmetric key. Siberian Federal University. Engineering & Technologies. 2016, 9(2), 214-224 p, DOI: 10.17516/1999-494X-2016-9-2-214-224.
13. Akbarov D. E. Umarov Sh.A. The hash function algorithm with new basic transformations. News of the National Technical University of Ukraine" Kyiv Polytechnic Institute". Seriya: Priladobuduvannya. – 2016. – №. 51. – C. 1.
14. Akbarov D.E. Umarov Sh.A. The Application of Logical Operations and Tabular Transformations in the Base Accents of Hash Function Algorithms. Computer Reviews Journal Vol 6 (2020) ISSN: 2581-6640. Page 11-18.
15. 15. Akbarov D.E. Umarov Sh.A. Applying logical operations and table replacements in modeling basic transformations of symmetric block encryption algorithms. International Journal of Mechanical and

Production Engineering Research and Development (IJMPERD) Vol. 10, Issue 3, Jun 2020, 15041–15046 DOI: 10.24247/ijmperdjun20201433.

16. Abdurakhmonova, M. M., ugli Mirzayev, M. A., Karimov, U. U., & Karimova, G. Y. (2021). Information Culture And Ethical Education In The Globalization Century. *The American Journal of Social Science and Education Innovations*, *3*(03), 384-388.

17. Karimov, U., & Abdurakhmon, A. (2017). INNOVATIVE INFORMATION TECHNOLOGY IN EDUCATION. *Форум молодых ученых*, (5), 9-12.

18. Karimov, U., & Kasimov, I. (2018). THE IMPORTANCE OF MODERN INFORMATION TECHNOLOGIES IN DEVELOPMENT OF DISTANCE EDUCATION. In *Перспективные информационные технологии (ПИТ 2018)* (pp. 1186-1187).

19. Karimov, U., Kaxarov, S., Yokubjonov, S., & Ziyodov, D. (2018). USING NEW INFORMATION TECHNOLOGIES IN DISTANCE LEARNING SYSTEM. In *НОВАЯ ПРОМЫШЛЕННАЯ РЕВОЛЮЦИЯ В ЗЕРКАЛЕ СОВРЕМЕННОЙ НАУКИ* (pp. 9-11).

20. Каримов, У. (2017). ИНФОКОМТЕХНОЛОГИИ (ИКТ) ФОРМИРОВАНИЕ ДУХОВНЫХ ХАРАКТЕРИСТИК ЛИЧНОСТИ. In *Перспективные информационные технологии (ПИТ 2017)* (pp. 1160-1163).

21. Каримов, У. У. (2017). РОЛЬ СРЕДСТВ МАССОВОЙ ИНФОРМАЦИИ В ПРОЦЕССЕ ГЛОБАЛИЗАЦИИ. In *Перспективные информационные технологии (ПИТ 2017)* (pp. 1189-1192).

22. Каримов, У., & Каримова, Г. (2018). ГЕОПОЛИТИЧЕСКАЯ КОНКУРЕНЦИЯ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ. In *Перспективные информационные технологии (ПИТ 2018)* (pp. 1368-1372).

23. Umarov Sh.A. Use of Chebyshev polynomials in digital processing of signals. International Journal of Advanced Research in Science, Engineering and Technology. Vol. 6, Issue 2, February 2019.

24. Umarov Sh.A., Axmedov Z., Tolipov N. About an incorrect task for a biharmonic equation in a ball. Polish Science Journal. Issue 12 (33). Part 2. P.373-376.