NOVATEUR PUBLICATIONS
INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY
[IJIERT] ISSN: 2394-3696 Website: ijiert.org
VOLUME 9, ISSUE 12, Dec. -2022

ELECTRONIC DIGITAL SIGNATURE PROTOCOL OF AN ASYMMETRIC ENCRYPTION ALGORITHM BASED ON THE COMPLEXITY OF PERFORMING ACTIONS ABOUT ELLIPTIC CURVE POINTS AND MULTIPLICATION OF MATRICES WITH A PARAMETER ON A FINAL FIELD

Akhmadaliev Shakhobidin Sharifovich
Kokand State Pedagogical Institute
Senior Teacher
Tel: 97 337-74-06 e-mail: 356_qabul_2009@mail.ru

ANNOTATION
In article the report of the electronic digital signature on the basis of asymmetric algorithm of the enciphering based on complexity of performance of operation of addition of points with rational co-ordinates of an elliptic curve on a final field at which, in process formation of the digital signature possibility a choice of any number from the signed is provided is developed.

Keywords: matrix, field, multiplication, rational coordinate point, elliptic curve, complexity, asymmetry, encryption, algorithm, protocol, digital signature

The disadvantage of the EDS based on the public key encryption algorithm is that it is possible to create only one digital signature corresponding to the given M - information. Because the checksum NY (M)= NY corresponding to the given M -data always has the same value and the result of encryption and decryption always has the same expression because the calculation of the hash function value is based on the keyless algorithm. $H(M) = H$ is divided. This situation makes it difficult to use such EDS algorithms.

Specially developed (created) EDS calculation formulation and its verification algorithms are free from the above-mentioned shortcomings. Because in these algorithms, the value of the hash function of the information to be signed, in addition to the secret key of the signer, a parameter chosen by the signer is also used in forming the EDS.

Article presented to your attention, a symmetric encryption algorithm [4] was created based on the complexity of the parametric multiplication of matrices and the complexity of operations on the points of the elliptic curve in a finite field. together with the given HF, using a parameter chosen by the signer practical application methods and protocols will be developed for the implementation of electronic digital signature, verification of the integrity of information and solutions for ensuring its authentication .

This point are calculated through a known point $R_{m\times n} = R_{il} = [x_{il}]G$ belonging to the selected elliptic curve G - with rational coordinates of sufficiently large order, where x_{il} - are the unknowns. Then we declare (p, G, A $_{mxn}$,R $_{mxn}$) - four as public key, x_{il} and unknowns as secret key.

Cryptosystem j - user t - to user $M = M_{n\times m}$ - encrypts public information and sends it with a digital signature depending on its hash value as follows:

1 $M =$. - its hash value $M_{n\times m}$ H (M)= H ($M_{n\times m}$)= $H_{n\times m}$ = H according to the hash-function algorithm of the selected open data .

R -numeric signature j on this hash-value is formed by the user x_{il}^{j}'s private key and a number chosen by him k_1:

a) Randomly selecting j a number known only to the user , k_1 = $(x_{il}^{jk_1}(G), y_{il}^{jk_1}(G))$ - points are found on the elliptic curve, and the $R_{m\times n}^{jk_1} = [k_1]G + R_{m\times n}^{j} = [k_1 + x_{il}^{j}]G$ - coordinates of these points on the Ax axis (or -coordinates on the $x_{il}^{jk_1}(G)$ Moon axis $y_{il}^{jk_1}(G)$) $R_{il}^{jk_1} = x_{il}^{jk_1}(G)$ (or $R_{il}^{jk_1} = y_{il}^{jk_1}(G)$ or $R_{il}^{jk_1} = f(x_{il}^{jk_1}(G), y_{il}^{jk_1}(G))$) is accepted as

b) Encryption $A_{n\times m}^{j}$ is performed in the form ® H = $A_{n\times m}^{j} + H_{n\times m} + A_{n\times m}^{j} R_{m\times n}^{jk_1} H_{n\times m} \left(\mathrm{mod}\, p\right)$ = $P_{n\times m}$ = P and a digital signature is formed.

3. The information M to be signed and its digital signature are P combined to obtain M ||P = M' - extended electronic document.

4. By j randomly selecting t a number known only to the user, points k are found $(x_{il}^{tk}(G), y_{il}^{tk}(G))$ on the elliptic curve according to the $R_{m\times n}^{tk} = [k]R_{m\times n}^{t} = [k][x_{il}^{t}]G = [kx_{il}^{t}]G$ user's public key , $R_{m\times n}^{t} = R_{il}^{t} = [x_{il}^{t}]G$ and the coordinates of these points on the Ax axis $x_{il}^{tk}(G)$ (or on the Moon axis $y_{il}^{tk}(G)$ -coordinates) $R_{il}^{tk} = x_{il}^{tk}(G)$ (or $R_{il}^{tk} = y_{il}^{tk}(G)$ or $R_{il}^{tk} = f(x_{il}^{tk}(G), y_{il}^{tk}(G))$) are $R^{tk}{}_{m\times n}$ taken as elements of the matrix.

5. $A_{n\times m}^{t}$ By performing the encryption in the form $C_{n\times m} = (w_{n\times m}; d_t = [k]G; d_p = [k_1]G)$ ® $M'_{n\times m}$ = $A_{n\times m}^{t} + M'_{n\times m} + A_{n\times m}^{t} R_{n\times m}^{tk} M'_{n\times m} \left(\mathrm{mod}\, p\right)$ = , a $w_{n\times m}$ triplet is sent as ciphertext.

Cipher has received the t information $C_{n\times m} = (w_{n\times m}; d_t = [k]G; d_p = [k_1]G)$ - the user performs the decryption as follows:

1. Only the elements of the t matrix are calculated using the elements of the secret key $[x_{il}^{t}]d = [x_{il}^{t}][k]G = [x_{il}^{t}k]G = D_{m\times n}^{tk}$ known to the user. x_{il}^{t}

2. Open is the matrix $A_{n\times m}^{t}$ = $(I_{n\times n} + A_{n\times m}^{t} D_{m\times n}^{tk})^{-1}(-A_{n\times m}^{t}) \bmod p$ which is the parametric inverse of the key $(A_{n\times m}^{t})^{\backslash -1}$.

3. $R = D_{n\times m}^{tk}$ Decryption is performed by performing this value substitution operation:

$$(A_{n\times m}^{t})^{\backslash -1} \text{®}\ w_{n\times m} = (I_{n\times n} + A_{n\times m}^{t} D_{m\times n}^{tk})^{-1}(-A_{n\times m}^{t}) \text{®} (A_{n\times m}^{t} + M'_{n\times m} + A_{n\times m}^{t} R_{m\times n}^{tk} M'_{n\times m})$$

$$\left(\mathrm{mod}\, p\right) = (I_{n\times n} + A_{n\times m}^{t} R_{m\times n}^{tk})^{-1}(-A_{n\times m}^{t}) + (A_{n\times m}^{t} + M'_{n\times m} + A_{n\times m}^{t} R_{m\times n}^{tk} M'_{n\times m}) +$$

$$+ (I_{n\times n} + A^t_{n\times m}R^{tk}_{m\times n})^{-1}(-A^t_{n\times m})\, R^{tk}_{m\times n}\, (A^t_{n\times m} + M'_{n\times m} + A^t_{n\times m}R^{tk}_{m\times n}M'_{n\times m}) (\text{mod p}) =$$

$$= (I_{n\times n} + A^t_{n\times m}R^{tk}_{m\times n})^{-1}(-A^t_{n\times m})\, (I_{m\times m} + R^{tk}_{m\times n}A^t_{n\times m}) + A^t_{n\times m} + (I_{n\times n} + A^t_{n\times m}R^{tk}_{m\times n})M'_{n\times m}$$

$$+ (I_{n\times n} + A^t_{n\times m}R^{tk}_{m\times n})^{-1}(-A^t_{n\times m})R^{tk}_{m\times n}\, (I_{n\times n} + A^t_{n\times m}R^{tk}_{m\times n})M'_{n\times m} (\text{mod p})$$

If all the diagonal elements of the matrices in the expression of this last equality are non-zero, and all other elements are zero (such matrices have the property of commutativity), then the equality does not change even if they are exchanged in the terms involving matrix products. This equality holds for such matrices:

$$(A^t_{n\times m})^{\backslash -1} \circledR\ w_{n\times m} = (I_{n\times n} + A^t_{n\times m}R^{tk}_{m\times n})^{-1}(-A^t_{n\times m})\, (I_{m\times m} + R^{tk}_{m\times n}A^t_{n\times m}) + A^t_{n\times m} +$$

$$+ (I_{n\times n} + A^t_{n\times m}R^{tk}_{m\times n})M'_{n\times m} + (I_{n\times n} + A^t_{n\times m}R^{tk}_{m\times n})^{-1}(-A^t_{n\times m})R^{tk}_{m\times n}\, (I_{n\times n} + A^t_{n\times m}R^{tk}_{m\times n})M'_{n\times m}$$

$$(\text{mod p}) = (-A^t_{n\times m})(I_{n\times n} + A^t_{n\times m}R^{tk}_{m\times n})^{-1}\, (I_{m\times m} + R^{tk}_{m\times n}A^t_{n\times m}) + A^t_{n\times m} + +$$

$$(I_{n\times n} + A^t_{n\times m}R^{tk}_{m\times n})M'_{n\times m} + (-A^t_{n\times m})R^{tk}_{m\times n}(I_{n\times n} + A^t_{n\times m}R^{tk}_{m\times n})^{-1}\, (I_{n\times n} + A^t_{n\times m}R^{tk}_{m\times n})M_{n\times m} \text{ (mod}$$

$$\text{p)} = -A^t_{n\times m} + A^t_{n\times m} + M'_{n\times m} + A^t_{n\times m}R^{tk}_{m\times n}M'_{n\times m} - A^t_{n\times m}R^{tk}_{m\times n}\, M'_{n\times m} (\text{ mod p}) = M'_{n\times m}.$$

In general, if the matrices participating in these equality expressions are chosen so that they have the property of commutativity, the decoding process mentioned above can be easily implemented. Here

$$M'_{n\times m} = M_{n\times m} \,||\, P_{n\times m} \text{ and } P_{n\times m} = A^j_{n\times m} + H_{n\times m} + A^j_{n\times m}R^{jk_1}_{m\times n}H_{n\times m} \left(\text{mod } p\right) = A^j_{n\times m} \circledR\ H = P$$

taking into account that the process of determining the correctness of the electronic digital signature continues as follows:

4. j - $R^j_{m\times n}$ added to the user's $R^{jk_1}_{m\times n} = [k_1]G + R^j_{m\times n} = [k_1 + x^j_{il}]G$ public key $d_p = [k_1]G$ $R^{jk_1}_{il} = g^{x^j_{il}+k_1} \bmod p = D^{jk_1}_{il}$ is calculated, $D^{jk_1}_{n\times m}$ -matrix is generated.

5. Open is the matrix $A^j_{n\times m} = (I_{n\times n} + A^j_{n\times m}D^{jk_1}_{m\times n})^{-1}(-A^{jk_1}_{n\times m}) \bmod p$ which is the parametric inverse of the key $(A^j_{n\times m})^{\backslash -1}$.

6. $R = D^{jk_1}_{n\times m}$ Decryption is performed by performing this value substitution operation:

$$(A^j_{n\times m})^{\backslash -1} \circledR\ w_{n\times m} = (I_{n\times n} + A^j_{n\times m}D^{jk_1}_{m\times n})^{-1}(-A^j_{n\times m}) \circledR (A^j_{n\times m} + H_{n\times m} + A^j_{n\times m}R^{jk_1}_{m\times n}H_{n\times m}) \left(\text{mod } p\right) =$$

$$(I_{n\times n} + A^t_{n\times m}R^{jk_1}_{m\times n})^{-1}(-A^t_{n\times m}) + (A^t_{n\times m} + H_{n\times m} + A^t_{n\times m}R^{jk_1}_{m\times n}H_{n\times m}) +$$

$$+ (I_{n\times n} + A^j_{n\times m}R^{jk_1}_{m\times n})^{-1}(-A^j_{n\times m})\, R^{jk_1}_{m\times n}\, (A^j_{n\times m} + H_{n\times m} + A^j_{n\times m}R^{jk_1}_{m\times n}H_{n\times m}) (\text{mod p}) =$$

$$= (I_{n\times n} + A^j_{n\times m}R^{jk_1}_{m\times n})^{-1}(-A^j_{n\times m})\, (I_{m\times m} + R^{jk_1}_{m\times n}A^j_{n\times m}) + A^j_{n\times m} + (I_{n\times n} + A^t_{n\times m}R^t_{m\times n})H_{n\times m} +$$

$$+ (I_{n\times n} + A^j_{n\times m}R^{jk_1}_{m\times n})^{-1}(-A^j_{n\times m})R^{jk_1}_{m\times n}\, (I_{n\times n} + A^j_{n\times m}R^{jk_1}_{m\times n})H_{n\times m} (\text{mod p})$$

Taking into account that only the diagonal elements of the matrices in the expression of this last equality are not all zero, and all other elements are zero (such matrices have the property of commutativity), using the fact that the equality does not change even if their positions are changed in the terms involving matrix products, we can approach this equality has:

$$(A_{n\times m}^{j})^{\backslash -1}\text{®}\ w_{n\times m}=(I_{n\times n}+A_{n\times m}^{j}R_{m\times n}^{jk_1})^{-1}(-A_{n\times m}^{j})\,(I_{m\times m}+R_{m\times n}^{jk_1}A_{n\times m}^{j})+A_{n\times m}^{j}+$$

$$+(I_{n\times n}+A_{n\times m}^{j}R_{m\times n}^{jk_1})H_{n\times m}+(I_{n\times n}+A_{n\times m}^{j}R_{m\times n}^{jk_1})^{-1}(-A_{n\times m}^{j})R_{m\times n}^{jk_1}\,(I_{n\times n}+A_{n\times m}^{t}R_{m\times n}^{t})H_{n\times m}\ (\text{mod p}$$

$$)=(-A_{n\times m}^{j})(I_{n\times n}+A_{n\times m}^{j}R_{m\times n}^{jk_1})^{-1}\,(I_{m\times m}+R_{m\times n}^{jk_1}A_{n\times m}^{j})+A_{n\times m}^{j}+(I_{n\times n}+A_{n\times m}^{j}R_{m\times n}^{jk_1})H_{n\times m}+$$

$$(-A_{n\times m}^{j})R_{m\times n}^{jk_1}(I_{n\times n}+A_{n\times m}^{jt}R_{m\times n}^{jk_1})^{-1}\,(I_{n\times n}+A_{n\times m}^{j}R_{m\times n}^{jk_1})H_{n\times m}\ (\text{mod p})=-A_{n\times m}^{j}+A_{n\times m}^{j}++$$

$$H_{n\times m}+A_{n\times m}^{j}R_{m\times n}^{jk_1}H_{n\times m}\ H_{n\times m}+A_{n\times m}^{j}R_{n\times m}^{jk_1}H_{n\times m}-A_{n\times m}^{t}R_{m\times n}^{t}\ H_{n\times m}(\ \text{mod p})=H_{n\times m}.$$

7 . t- the part of the extended document M_1 generated as a result of the decryption of the $M_1^{/}$ encrypted information by the user $C_{n\times m}$ is hashed: H (M_1) = M_1 | | P_1 H ($M_{1n\times m}$)= H_1

8. H_1 = If H ($M_{1n\times m}$)= H $_{n\times m}$ = H , the electronic document is considered complete (authentic) and the authenticity of its source also follows from the authenticity of its electronic digital signature.

Is possible to distribute the secret keys to the users of the information and communication network in the open communication channel by putting information about the key instead of -information in the algorithms of EDS protocols M [1-3].

In the proposed EDS algorithm, in addition to the private key of the signer, a parameter chosen by the signer was also used. Therefore , this EDS algorithm has the same properties as EDS algorithms based on the formation and verification of a specially designed (created) digital signature calculation.

Foydalanilgan adabiyotlar ro‘yxati

1. Alferov A. P., Zubov A. Ю., Kuzmin A. S., Cheremushkin A. V. Osnovы kriptografii: Uchebnoe posobie, 2-e izd. –M.: Gelios ARV, 2002.-480 s.
2. Shnayer B. Prikladnaya kriptografiya. Protokolы, algoritmы, isxodnыe tekstы na yazыke Si. –M.: izdatelstvo TRIUMF, 2003 - 816 s.
3. Akbarov D.E. Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qo‘llanilishi – Toshkent, “O‘zbekiston markasi”, 2009 – 434 bet.
4. Xasanov P.F., Akbarov D. E., Axmadaliev Sh. Sh. Parametrli algebra amallaridan foydalanib mavjud hisoblash murakkabliklari asosida yangi asimmetrik algoritmlar yaratish usullari. //Infokommunikatsii: Seti-Texnologii-Resheniya. -1(9)/2009. -s. 31-35.
5. Siddikov I. M., Sh S. O. ABOUT ONE INNOVATION METHOD OF LOCALIZATION OF INDEPENDENT DIGITAL DEVICES //E-Conference Globe. – 2021. – С. 204-205.
6. Khaidarova, S. "Sql-expressions That Manage Transactions." JournalNX: 307-310.
7. Хонбобоев, Хакимжон Икромович, and Дилшод Улугбекович Султанов. "РУКОВОДСТВО НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТЬЮ СТУДЕНТОВ ПРИ ОБУЧЕНИИ ПРЕДМЕТАМ ИНФОРМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ." Актуальные научные исследования в современном мире 12-1 (2016): 63-65.
8. Хонбобоев, Хакимжон Октамович, Фозилжон Усибхонович Полатов, and Мухаммад-Анасхон Хакимжонович Икромов. "Tasviriy san’atni oqitishda interfaol metodlardan foydalanish." Молодой ученый 3-1 (2016): 22-23.
9. Shukhratovich, Shirinov Feruzjon. "The Field of Computer Graphics and Its Importance, Role and Place in The Information Society." Texas Journal of Multidisciplinary Studies 4 (2022): 86-88.

10. Muydinovich, Rasulov Inom. "The Role of Digital Technologies in Growing Secondary School Students to the Profession." Eurasian Scientific Herald 6 (2022): 137-142.
11. Muydinovich, Rasulov Inom. "The Role of Digital Technologies in Growing Secondary School Students to the Profession." Eurasian Scientific Herald 6 (2022): 137-142.
12. Йулдошев, Уткир, and Уктамжон Жуманкузиев. "Определение ведущих педагогических закономерностей и основополагающих принципов формирования информационной культуры детей школьного возраста." Общество и инновации 2.5/S (2021): 68-76.
13. Mamadjanova, S. V. "DESIGN FEATURES OF VIRTUAL LEARNING ENVIRONMENTS." European International Journal of Multidisciplinary Research and Management Studies 2.06 (2022): 1-5.
14. Toshpulatov, Raximjon I. "MODERN METHODS AND TENDENCIES IN TEACHING INFORMATION TECHNOLOGY." International Journal of Pedagogics 2.09 (2022): 43-46.
15. Jo‘rayev, M. (2022). Professional ta’lim jarayonida fanlararo uzvilik va uzliksizlikni ta’minlash o‘quvchilari kasbiy tayyorgarligining muhim omili sifatida. Zamonaviy dunyoda amaliy fanlar: Muammolar va yechimlar, 1(29), 43-46.
16. Shirinov F., Mamasoliyev A. A GENERAL DESCRIPTION OF THE HARDWARE AND SOFTWARE ENVIRONMENT USED TO ORGANIZE COMPUTER-BASED LEARNING PROCESSES //Euro-Asia Conferences. – 2021. – Т. 3. – №. 1. – С. 63-65.
17. Tokhirovna, Khakimova Yoqutkhon. "Stages Of Implementation Of Distance Learning In Higher Education." Texas Journal of Philology, Culture and History 1 (2021): 38-39.
18. Normatov, R. N., M. M. Aripov, and I. M. Siddikov. "Analysis Method of Structural-complex System Indicators by Decomposition Into Subsystems." JournalNX 7.04 (2021): 68-71.
19. Shirinov F., Mamasoliyev A. AN INTELLIGENT COMPUTER NETWORK-BASED LEARNING PROCESS MANAGEMENT SYSTEM //Euro-Asia Conferences. – 2021. – Т. 3. – №. 1. – С. 55-57.
20. Juraev, M. M. (2022). The value of open mass competitions in the process of digitalization of extracurricular activities of schoolchildren. Web of Scientist: International Scientific Research Journal, 3(10), 338-344.
21. Abdunazarova, Dilfuza Tukhtasinovna, Maxfuza Madraximova, and Shuhrat Madrahimov. "SOLVING EQUATIONS IS FOUNDATIONAL FOR MIDDLE AND HIGH SCHOOL MATH." Scientific Bulletin of Namangan State University 3.5 (2021): 7-10.
22. Aripov M.M. Structural methods for program testing. Journal of Positive School Psychology. Vol.6, No 10, 2022, p.3428-3431.