ELEKTRON RAQAMLI IMZO ALGORITMLARI TAHLILI

I.S.Olimov,
Tashkent university of information technologies named after Muhammad al- Khwarizmi
E-mail: iskandar.olimov@mail.ru

X.I. Ibrohimov
Tashkent university of information technologies named after Muhammad al- Khwarizmi

Annotatsiya: *Bu maqolada elektron imzo algoritmlari haqida umumiy ma'lumotlar berilgan, shu bilan birga elektron raqam imzoni shakllantirish va tekshirish, undan tashqari elektron raqamli imzo algoritmlari va ularni tahlili keltirilgan.*

Kalit so'zlar: *ERI, blokcheyn texnologiyasi,RSA, GOST R 34.10-2001, DSA.*

KIRISH

Hozirgi kunda Ma'lumotlar yaxlitligini ta'minlashda bir qator zamonaviy usullari mavjud:

Xesh funksiyalar: Ma'lumotni xeshlash uning yaxlitligini kafolatlash maqsadida amalga oshirilib, agar Ma'lumot uzatilishi davomida o'zgarishga uchrasa, uni aniqlash imkoni mavjud bo'ladi.

Xatolarni aniqlash va tuzatish kodlari: Ushbu kodlar uzatilgan yoki saqlangan Ma'lumotlardagi xatolarni aniqlash va tuzatish uchun ishlatiladi. Masalan, Hamming kodlari va Reed-Solomon kodlari. Ma'lumotlarga ortiqcha Ma'lumotlarni kiritish orqali ushbu kodlar xatolarni aniqlashi va tuzatishi mumkin.

Raqamli imzolar: Raqamli imzolar yaxlitlik va autentifikatsiyani ta’minlash uchun assimetrik kriptografiyadan foydalanadi. Elektron raqamli imzo jo‘natuvchining shaxsiy kaliti yordamida yaratiladi va uni jo‘natuvchining ochiq kaliti yordamida tekshirish mumkin. Agar imzo haqiqiy bo‘lsa, u Ma’lumotlarning yaxlitligi va haqiqiyligini ta’minlaydi.

Merkle daraxtlari: Merkle daraxtlari, shuningdek, xesh daraxtlari sifatida ham tanilgan, katta Ma’lumotlar to‘plamlarini samarali tekshirish imkonini beruvchi Ma’lumotlar tuzilmalari. Ular Ma’lumotlarni kichikroq bloklarga ajratadilar, har bir blok uchun xeshlarni hisoblaydilar.

Blokcheyn texnologiyasi: Dastlab Bitcoin kabi kriptovalyutalar uchun taqdim etilgan blokcheyn texnologiyasi o‘ziga xos Ma’lumotlar yaxlitligi xususiyatlari tufayli turli sohalarda e’tiborni tortdi. Blokcheyndagi har bir blok zanjirni tashkil etuvchi oldingi blokning kriptografik xeshini o‘z ichiga oladi.

O‘zbekiston Respublikasining Elektron raqamli imzo to‘g‘risidagi qonunida elektron raqamli imzoga quyidagichata’rif berilgan:

Elektron raqamli imzo

“*Elektron raqamli imzo (ERI)* — elektron hujjatdagi mazkur elektron hujjat axborotini elektron raqamli imzoning yopiq kalitidan foydalangan holda, maxsus o‘zgartirish natijasida hosil qilingan, hamda elektron raqamli imzoning ochiq kaliti yordamida elektron hujjatdagi axborotda xatolik yo‘qligini aniqlash va elektron raqamli imzo yopiq kalitining egasini identifikatsiya qilish imkoniyatini beradigan imzo”.

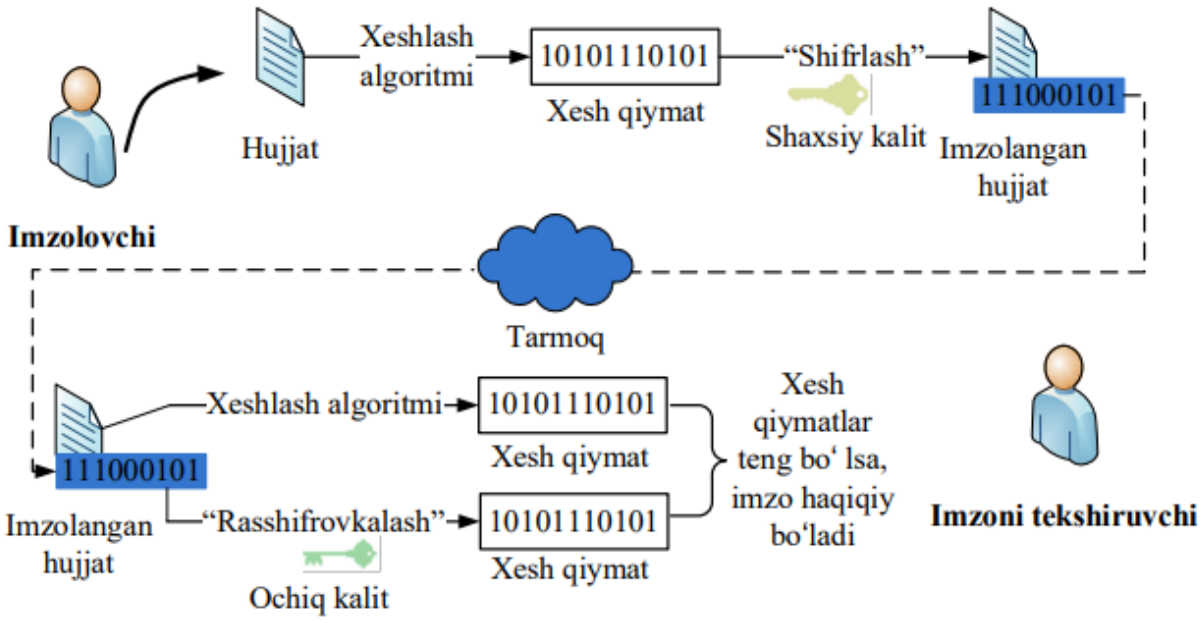
Elektron raqamli imzo oddiy qo‘lda qo‘yiluvchi imzo kabi, faqat elektron hujjatlarda qo‘yiladi va imzo qo‘yilgan Ma’lumotning yaxlitligini ta’minlaydi va imzolovchining qo‘yilgan imzodan bosh tortmasligini (rad etmasligini) kafolatlaydi. Axborot xavfsizligida *rad etish* muammosi mavjud, unga ko‘ra foydalanuvchi hujjatni imzolaganini rad etadi (ya’ni, men imzolamadim deb turib oladi). Mazkur muammoni oldini olishda aynan elektron raqamli imzo tizimlaridan foydalaniladi.

Shunday qilib, ERI tizimlari nafaqat Ma’lumot yaxlitligini ta’minlaydi, balki imzolovchining majburiyatlardan tonishiga yo‘l qo‘ymaydi (yoki rad etishni oldini oladi). Shu sababli, ERI tizimlari Ma’lumotlar yaxlitligini ta’minlovchi simmetrik kriptotizimlarga asoslangan MAC tizimlaridan ajralib turadi.

MAC tizimlarida xesh qiymatni qayta hisoblay olmaslik uchun, matnga kalit biriktirilgan bo‘lsa, ERI tizimlarida Ma’lumotning xesh qiymati shaxsiy kaliti bilan “shifrlash” amalga oshiriladi va ERI hosil qilinadi. Ushbu xabarni “rasshifrovkalash” uchun esa tomonning ochiq kalitini bilishning o‘zi yetarli. Demak, oddiy imzo tizimiga o‘xshash (oddiy imzo tizimida bir kishi imzo qo‘yadi va qolganlardan uning haqiqiyligini tekshirish talab etiladi). ERI tizimida ham shaxsiy kalit egasi xabarni imzolaydi, qolganlar esa, uning ochiq kalitidan foydalanib, imzoni haqiqiyligini tekshiradi.

Agar A tomon xabar M ga imzo qo‘ygan bo‘lsa, u holda imzo

$S = [M]_A$ shaklida ifodalanadi (xuddi ochiq kalitli kriptografiyada shaxsiy kalit bilan rasshifrovkalash kabi). ERI tizimlarini yaratish ikkita muolajadan iborat: *ERIni shakllantirish* va *ERIni tekshirish* (1-rasm).



1-rasm. Elektron raqamli imzo sxemasi

Hozirda ERI tizimini yaratishning bir nechta yo‘nalishlari mavjud. Bu yo‘nalishlarni uchta guruhga bo‘lish mumkin:

1) ochiq kalitli shifrlash algoritmlariga asoslangan;
2) simmetrik shifrlash algoritmlariga asoslangan;
3) imzoni hisoblash va uni tekshirishning maxsus algoritmlariga asoslangan raqamli imzo tizimlaridir.

Ochiq kalitli shifrlash algoritmlariga asoslangan ERI

Ishonchli bardoshli kriptoalgoritmlar mutaxasislar tomonidan yechilishi murakkab deb tan olingan matematik masalaga asoslanadi. Ishonchli bardoshli kriptoalgoritmlar turkumi tarkibiga kiruvchi yetarli katta sonni tub ko‘paytuvchiga ajratish ***(TKA) matematik*** murakkabligiga asoslangan ***RSA*** shifrlash algoritmi keltirishimiz mumkin [1];

RSA shifrlash algoritmi. Diffi va Xelman kritografiya sohasida yangicha yondashishni targ‘ib qilib, ochiq kalitli kriptotizimlarning barcha talablariga javob beradigan kriptografik algoritm yaratish taklifi bilan chiqdi. Birinchilardan bo‘lib bunga javoban 1978 yil Ron Rayvets (Ron Rivest), Adi Shamir (Adi Shamir) va Len Adlmen (Len Adlmen)lar shu vaqtgacha tan olingan va amaliy keng qo‘llanib kelingan ochiq kalitli shifrlash algoritm sxemasini taklif qildi va bu algoritm ularning nomi sharafiga RSA algoritmi deb ataldi. RSA algoritmi faktorlash murakkabligiga asoslangan shifrlash algoritmi hisoblanadi [1,2].

Tizimning har bir i- foydalanuvchisi (e_i, d_i) - kalitlar juftligini yaratadi. Buning uchun yetarli katta bo‘lgan p va q - tub sonlari olinib (bu sonlar mahfiy tutiladi), $n = pq$ - soni va Eyler funksiyasining qiymati $\varphi(n)=(p-1)(q-1)$ hisoblanadi (bu son ham maxfiy tutiladi). So‘ngra, $(e_i, \varphi(n))=1$ shartni qanoatlantiruvchi, ya’ni $\varphi(n)$ -soni bilan o‘zaro tub bo‘lgan e_i -son bo‘yicha d_i -soni ushbu $e_i d_i = 1 \bmod \varphi(n)$ formula orqali hisoblanadi. Bu $(e_i; d_i)$ –juftlikda e_i - ochiq kalit va d_i - mahfiy kalit deb e’lon qilinadi.

Shundan so‘ng i - foydalanuvchidan j - foydalanuvchiga shifrlangan Ma’lumotni imzolagan holda jo‘natishi quyidagicha amalga oshiriladi:

– *shifrlash qoidasi:* $M^{e_j} \bmod n = C$, bu yerda M - ochiq Ma’lumot, C – shifrlangan Ma’lumot;

– *deshifrlash qoidasi:* $C^{d_j} \bmod n = M^{e_j d_j} \bmod n = M$;

– *ERI ni hisoblash:* $H(M)^{d_i} \bmod n = P_i$,

Bu yerda i - foydalanuvchining P_i - imzosi M - Ma’lumotning $H(M)$ - xesh funksiya qiymati bo‘yicha hisoblangan;

ERI ni tekshirish: $(P_i)^{e_i} \bmod n = H(M)^{e_i d_i} \bmod n = H(M)$, agar $H(M) = H(M_1)$ bo‘lsa (bu yerda M_1 -deshifrlangan Ma’lumot), u holda elektron hujjat haqiqiy, aks holda haqiqiy emas, chunki xesh funksiya xossasiga ko‘ra $M = M_1$ bo‘lsa ularning xesh qiymatlari ham teng bo‘ladi.

Ma’lumotni maxfiy uzatish protokoli:

$\left[M \cup H(M)^{d_i}\right]^{e_j} \bmod n = \left[M \cup P_i\right]^{e_j} \bmod n = C$;

Maxfiy uzatilgan Ma’lumotni qabul qilish protokoli:

$C^{d_j} \bmod n = \left[M \cup P_i\right]^{e_j d_j} \bmod n = M \cup P_i$, umuman qaraganda dastlabki Ma’lumot o‘zgartirilgan bo‘lishi mumkin, shuning uchun $C^{d_j} \bmod n = M_1 \cup P_i$ bo‘lib, natijada, xesh qiymat imzo bo‘yicha ushbu ifoda $(P_i)^{e_i} \bmod n = H(M)^{e_i d_i} \bmod n = H(M)$ bilan hisoblanadi va qabul qilib olingan Ma’lumotning xesh qiymati $H(M_1)$ bo‘lsa, u holda $H(M) = H(M_1)$ bo‘lganda elektron hujjat haqiqiy, aksincha bo‘lsa qalbaki hisoblanadi.

Elliptik egri chiziqlarga asoslangan elektron raqamli imzo algoritmlari

Elliptik egri chiziqlarga asoslangan kriptotizimlar kriptografiyaga 1985 yilda V.Miller va N.Koblis tomonidan tadbiq qilingan. Assimmetrik kriptografik algoritmlarning ko‘pchiligi chekli maydonda diskret logarifmlash masalasining murakkabligiga asoslangan bo‘lib, bu algoritmlarni elliptik egri chiziqlarga o‘tkazish masalasi alohida izlanish talab etadi. Quyida xalqaro standart sifatida qabul qilingan EC DSA va GOST R 34.10-2001 elliptik egri chiziqlarga asoslangan elektron raqamli imzo algoritmlari ko‘rib o‘tiladi [3].

Elektron raqamli imzo algoritmining boshlang'ich parametrlari. Qaralayotgan algoritmning asosiy parametrlari xarakteristikasi p-tub sondan iborat bo'lgan chekli maydonda aniqlangan E-elliptik egri chiziq va shu chiziqda olingan katta tub tartibga ega bo'lgan $G \in E(F_p)$-bazaviy nuqta hisoblanadi.

Bu chiziq quyidagi tenglama bilan beriladi:

$$y^2 = x^3 + ax + b(\mathrm{mod}\ p).$$

Turli (a,b) parametrlar juftligi izomorf elliptik egri chiziqlarni aniqlaydi. Tenglamaning muhim parametrlari esa mos ravishda diskriminant $d = -16(4a^3 + 27b^2) \neq 0$ va invariant $j = 1728(4a)^3/d$ ko'rinishda bo'ladi. Tenglamaning koeffisiyentlari a va b ma'lum j invariant bo'yicha quyidagicha aniqlanadi:

bu yerda

$$k \equiv \frac{j}{1728 - j}(\mathrm{mod}\ p), \quad j \neq 0, \quad j \neq 1728$$

Elliptik egri chiziqning G nuqtasi $F_p : G = (x_G, y_G)$ maydondan olingan (x_G, y_G) elementlar juftligi bilan aniqlanadi. Bu nuqtani hisoblashning yagona aniq usuli yo'q. Shuning uchun tanlash usuli bilan – biror x-qiymat olinadi va F_p maydonda $x^3 + ax + b$ ifodaning qiymati hisoblanib, bu qiymat biror sonni kvadrat ildizi bo'lishi yoki bo'lmasligi tekshiriladi. Agarda kvadrat ildiz mavjud bo'lsa, bu idiz y deb olinadi. Kvadrat ildiz mavjudligi $\left(\frac{x^3+ax+b}{p}\right)$ simvoli yordamida tekshiriladi [4,6].

Kriptografik bardoshli raqamli imzo tizimini olish uchun quyidagi shartlar bajarilishi kerak:

– elliptik egri chiziq supersingulyar bo'lmasligi kerak, $\#E(F_p) \neq p + 1$;

– $p^k \neq 1(\mathrm{mod}\, n)$ barcha $k \in \{1, \ldots, C\}$ lar uchun, bu yerda C yetarli katta son, qaysiki F_{p^C} maydonda diskret logarifmlashni hisoblash vaqt nuqtai nazaridan mumkin bo'lmasin (odatda $C = 20$ qilib tanlanadi);

– elliptik egri chiziq anomal bo'lmasligi kerak, ya'ni $\#E(F_p) \neq p$;

– elliptik egri chiziqning rasional koordinatali nuqtalari soni *m* quyidagi shartni qanoatlantirsin:

$\#E(F_p) = m$, $m = tq$, bu yerda q - katta tub son, $t \in N$ va $t \geq 1$.

Hozirda maxsus chiziqlar sinflariga mavjud bo‘lgan hujumlardan himoyalanishning mavjud usuli - E - Elliptik egri chiziqni yuqoridagi shartlarni qanoatlantiruvchi qilib olishdan iboratdir [1,5].

Ushbu parametrlar foydalanuvchilar guruhi uchun umumiy bo‘lishi mumkin. Imzoni generasiya qilish va tekshirish uchun ishlatiladigan individual parametrlar – maxfiy va ochiq kalitlar deb nomlanadi.

– imzo qo‘yish kaliti (mahfiy kalit) – bu $[0; q]$ intervaldagi ihtiyoriy d soni;

– imzoni tekshirish kaliti (ochiq kalit) – bu elliptik egri chiziqdagi $Q = [d]G$ nuqta;

– bundan tashqari raqamli imzo algoritmida *h* - xesh-funksiyadan ham foydalaniladi.

DSA ERI algoritmi

1991 yilda NIST (National Institute of Standard and Technology) tomonidan DSA (Digital Signature Algorithm) algoritmiga asoslangan DSS (Digital Signature Standard) ERI standarti yaratildi. Ushbu algoritm chekli maydonda diskret logarifmlash muammosiga asoslangan. Xesh funksiya sifatida SHA1 standartidan foydalanilgan.

Ochiq va yopiq kalitlar

1. Maxfiy kalit

Imzoni shakllantirish:

1. Imzolanuvchi *M* Ma’lumotni imzolashda quyidagi ketma – ketliklar bajariladi:

a. *p* – tub son tanlanadi ($2^{1023} < p < 2^{1024}$ va bit uzunligi 64 ga karrali);

b. *q* – tub son tanlanadi ($2^{159} < q < 2^{160}$ va *p-1* ning bo‘luvchisi);

c. $0 < h < p$ va $h^{(p-1)/q} \bmod p > 1$ shartlarni qanoatlantiruvchi *h* kattalik asosida $g = h^{(p-1)/q} \bmod p$ butun son hisoblanadi;

d. x – maxfiy kalit orqali, $y = q^x \ mod \ p$ ochiq *kalit hisoblanadi* (bu yerda: 0<x<q);

2. Ma’lumot jo‘natuvchisi tasodifiy k sonini tanlaydi ($0<k<q$ shart bilan). Ushbu kattalik imzo shakllantirilgandan so‘ng o‘chirib tashlanadi.

3. M Ma’lumotni imzolari quyidagilarga teng bo‘ladi:

$r = g^k \ mod \ p \ mod \ q,$

$s = k^{-1}(xr + H(M)) \ mod \ q.$

Hosil qilingan kattaliklar (r, s) Ma’lumot M ga qo‘shib imzoni tekshiruvchi tomonga yuboriladi.

Imzoni tekshirish jarayoni:

Qabul qilingan M’ Ma’lumot va unga qo‘yilgan imzo (r’, s’) asosida imzoni tekshirish jarayoni amalga oshiriladi. Bu ikki bosqichdan iborat. Agar imzo birinchi bosqichdagi tekshiruvdan o‘ta olmasa, unda ikkinchi bosqichga o‘tmaydi.

Qabul qilingan imzolar uchun $0 < s' < q$ yoki $0 < r' < q$ shart tekshiriladi. Bu shart bajarilsa ikkinchi bosqichga o‘tiladi [5,6].

1. Ikkinchi bosqich quyidagilardan iborat:

a. $v = (s')^{-1} (mod \ q)$ hisoblanadi.

b. $z_1 = H(M') \ v \ mod \ q, \ z_2 = r' \ v \ mod \ q$ qiymatlar hisoblanadi.

c. Shundan so‘ng $u = g^{z_1} y^{z_2} \ mod \ p \ mod \ q$ qiymat hisoblanadi.

d. Agar $r' = u$ tenglik bajarilsa, u holda qo‘yilgan elektron raqamli imzo haqiqiy ($M = M'$) bo‘ladi. Aks holda imzo qalbaki deb topiladi.

- *Parametrlarni generatsiyalash*

– $H = 9_{10} = 1001_2$;

– xesh qiymat uzunligi 4 ga tengligi uchun $q = 11_{10} = 1011_2$ tanlash mumkin.

– shuningdek, $p = 23$ ni tanlash mumkin, ya’ni $23 - 1 = 22 = q * 2$;

– bundan tashqari, $g = 2^2 = 4$.

- *Kalitlarni hosil qilish*

– shaxsiy kalit uchun: $x = 7$;

– u holda ochiq kalit quyidagiga teng bo‘ldi: $y = g^x mod p = 4^7 mod 23 = 16384 mod 23 = 8$.

- *Xabarni imzolash*

– $k = 3$ deb tanlaylik;

– u holda $r = (g^k mod p) mod q = (4^3 mod 23) mod 11 = 7$;

– $r \neq 0$ bo‘lganligi bois, keying qadamga o‘tamiz;

– $s = k^{-1}(H(m) + x * r) mod q = 4(9 + 7 * 7) mod 11 = 1$, ya’ni $3^{-1} mod 11 = 4$.

– $s \neq 0$ bo‘lganligi bois, keyingi qadamga o‘tamiz:

– Imzo jufti $(r, s) = (7,1)$ ga teng.

- *Imzoni tekshirish*

– $w = s^{-1} mod q = 1^{-1} mod 11 = 1$;

– $u_1 = H(m) * w \; mod \; q = 9 * 1 \; mod \; 11 = 9$;

– $u_2 = r * w \; mod \; q = 7 * 1 \; mod \; 11 = 7$;

– $v = (g^{u_1} * y^{u_2} \; mod \; p) mod \; q = (4^9 * 8^7 \; mod \; 23) mod \; 11 = 7$;

– $v = r$ bo‘lganligi bois, imzo to‘g‘ri.

ERI algoritmlari tahlili

1-jadval

ERI algoritmlari tahlili jadvali

Belgilar	***O‘z Dst 1092:2005***	***DSA***	***GOST R 24.10-2001***
Algebraik Struktirasi	Parametrli Algebra	Chekli oddiy maydon	Chekli oddiy maydon, aniqlangan EECh
Modul tipi va o‘lchami	Tub son p> 2^{255} (afzalligi: tezkorlikda)	Tub son 2^{511}<p <2^{1024}	Tub son, p>2^{255}
Protseduralarda foydalanilgan asosiy amallar	Parametrli ko‘paytirish; Parametr bilan darajaga oshirish.	Ko‘paytirish Ko‘shish Darajaga oshirish Teskarilash	Ko‘shish Inkor Ko‘p martalik ko‘shish (kamchili: amallarning murakkbligida)
Daraja asosi tipi	Maxfiy - g. (afzalligi: diskret logarifm masalasini qo‘shish	Oshkora - g. (kamchiligi : diskret logarifmlash masalasini kushish osonligida)	Oshkora - p (kamchiligi: EECh diskret logarifmlash masalasini ko‘shish

	murakkabligida)		osonligida)
ERI uzunligini qisqartirishga yondoshuv	Faktor ((p-1) ning tub ko‘paytuvchisi) dan foydalanish $2^{254}<q<2^{256}$	Faktordan foydalanish $2^{511}<q<2^{1024}$	Siklik gruppaning tartibidan foydalanish $2^{254}<q<2^{256}$ q-gruppa tartibi
Yopiq kalit shakli	Juftliklar(r, s) μ=0, (r,s,y1) μ=1. Kamchiligi μ=1	Juftlik(r,s)	Juftlik(r,s)
Bardoshlilik	μ=1 da daraja parametrning muammosining murakkabligiga asoslangan (afzalligi:RSA ga nisbatan bardoshli)	Modullar (512-1024) bit bo‘landa diskret logarifmlashning murakkab	Modul 255 bitdan kata bo‘lganda EECh da diskret logarifmlashning murakkabligiga asoslangan.
Tekshirish kaliti shakli	Juftlik (y,z) μ=0, (y,z,y1) μ=1 da (afzalligi: soxta imzoni aniqlashda)	Juftlik (s, y)	Parametr - Q
Imzoni tekshirish natijasi shakli	Xesh funksiya qiymati yoki xeshlashdan foydalanilmagan dagi xabar bloki (afzalligi: xeshlanishi shart bo‘lmagan qisqa xabarlarni uzutmaslik mumkinligi)	Ijobiy yoki salbiy	Ijobiy yoki salbiy
Foydalaniladi gan mezon	1. Seans kalitisiz (μ=0 2. Seans kaliti bilan (s=1) (afzalligi: yangi imkoniyatlar tug‘ilishida)	Seans kalitisiz	Seans kalitisiz

Ushbu jadvalda hozirda keng qo‘llanilayotgan bardoshli sanalgan ERI standartlari keltirilgan.

Yuqoridagi jadvallardan ko‘rinib turibdiki, har bir kriptotizim o‘ziga tegishli bo‘lgan ochiq va yopiq kalitlarga ega hisoblanib bu parametlar kriptotizimni bardoshliligiga hissa qo‘shuvchi eng muhim parametrlardir.

Xulosa

Mazkur maqolada Elektron raqamli imzo algoritmlari tahlili qilingan bo‘lib, unda ma’lumotlar yaxlitligini ta’minlash usullari, elektron raqamli imzo algoritmlari haqida ma’lumot ya’ni electron raqamli imzoni shakllantirish, tekshirish va undan tashqari elektron raqamli imzo algoritmlari tahlili keltirlgan.

Foydalanilgan adabiyotlar ro‘yxati

1. Kheshaifaty, Nafisah, and Adnan Gutub. "Preventing multiple accessing attacks via efficient integration of captcha crypto hash functions." *Int. J. Comput. Sci. Netw. Secur.(IJCSNS)* 20.9 (2020): 16-28.

2. Xu, Cong, Jingru Sun, and Chunhua Wang. "A novel image encryption algorithm based on bit-plane matrix rotation and hyper chaotic systems." *Multimedia Tools and Applications* 79.9-10 (2020): 5573-5593.

3. Hunt, Gareth, and H. E. Payne. "Image Reconstruction with Few Strip-Integrated Projections: Enhancements by Application of Versions of the CLEAN Algorithm." *Astronomical Data Analysis Software and Systems VI*. Vol. 202. No. 25. 1997.

4. Latif, S., Idrees, Z., Ahmad, J., Zheng, L., & Zou, Z. (2021). A blockchain-based architecture for secure and trustworthy operations in the industrial Internet of Things. *Journal of Industrial Information Integration*, *21*, 100190.

5. Olimov I. S., Karimov A. A., Ibrohimov X. I. ELLIPTIK EGRI CHIZIQQA ASOSLANGAN DIFFI XELMAN ALGORITMLARI YORDAMIDA KALITLARNI GENERATSIYALASH //RESEARCH AND EDUCATION. – 2023. – T. 2. – №. 5. – C. 427-432.

6. Salimboyevich O. I. et al. Making algorithm of improved key generation model and software //2020 International Conference on Information Science and Communications Technologies (ICISCT). – IEEE, 2020. – C. 1-3.