ELLIPTIK EGRI CHIZIQLARNING KRIPTOGRAFIYADA QO'LLANILISHI

Boyquziyev Ilhom Mardonaqulovich[1], Saydullayev Eldorjon Ismatillo o'gli[2], Rahmatullayev Ilhom Raxmatullayevich[2]

[1]Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalar universiteti
[2]Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalar universiteti Samarqand filiali
E-mail: Ilhom9001@gmail.com

K E Y W O R D S

Ochiq kalitli kriptotizim, bir tomonlama funksiya, faktorizatsiya, diskret logorifmlash, ryukzak, Veyershtrass tenglamasi, elleptik egri chiziq (EECh).

A B S T R A C T

Mazkur maqolada ochiq kalitli kriptotizimlar asosini tashkil qiluvchi murakkabliklarga asoslangan masalalar, ushbu murakkabliklarga asoslangan asimmetrik algoritmlar, elliptik egri chiziqlar hamda chekli maydonda ularning ratsional nuqtalarini aniqlash masalalari yoritilgan. Shuningdek, ushbu murakkablikka asoslangan EC DSA 2000 ERI standartida imzoni generatsiya qilish va tekshirish jarayoni hamda algoritmning korrektligi keltirilgan.

Kirish

1976-yilda U.Diffi va M.Ye.Xellmanning «**Kriptografiyada yangi yo'nalish**»[6], deb nomlangan maqolasini e'lon qilishlari bilan ochiq kalitli kriptotizimlar sohasida ilmiy ishlarning rivojlanishi yangi pog'onaga ko'tarildi. Ular maxfiy aloqa tizimlarida ma'lumotlarni shifrlash va shifrmatnni ochiq matnga o'girishda maxfiy kalitni maxsus aloqa tarmog'i orqali uzatilishi zarur bo'lmaydigan ilmiy-amaliy uslub asoslarini yaratib, bugungi kunda ham tobora rivojlanib borayotgan *ochiq kalitli kriptografiya davrini* boshlab berdi. Shuningdek, R.K.Merkli ham U.Diffi va M.Ye.Xellman bilan deyarli bir paytda boshqa ilmiy jurnalda chop qilish uchun tadqiqot natijalarini taqdim etgan lekin nashriyotda uzoq vaqt e'lon qilinmasdan qolgan maqolasida ham *ochiq kalitli shifrlash* g'oyasining asoslarini keltirib o'tgan [7].

Kriptografik tizim qanchalik murakkab va ishonchli murakkablikga ega algoritmga asoslangan bo'lmasin, uning amaliy qo'llanishida foydalanuvchilarga *kalitlarni taqsimlash* muammosi dolzarb bo'lib qolaveradi. Bu muammoni yechish uchun, klassik hamda zamonaviy fan va texnika, xususan, oliy matematika fani yutuqlariga asoslangan holda *ochiq kalitli kriptotizimlar* yaratish yo'nalishi vujudga keldi. Ochiq kalitli kriptotizimlarning qo'llanilishining umumiy mohiyati quyidagilardan iborat:

1. Foydalanuvchilarning har biri uchun ma'lum qoida bilan bog'langan ikkita kalit yaratiladi (generatsiya qilinadi).
2. Generatsiya qilingan (yaratilgan) kalitlardan biri ochiq kalit sifatida e'lon qilinadi, ikkinchisi esa maxfiy holda saqlanadi.
3. Ochiq matn ma'lumotni oluvchi foydalanuvchining ochiq kaliti bilan shifrlanib, shu foydalanuvchiga uzatiladi, bunda shifrmatnni va u shifrlangan ochiq kalitni bilgan holda unga mos keluvchi maxfiy kalitni yoki ochiq matnni aniqlashning imkoniyati mavjud emas.
4. Shifrmatn orqali ochiq matnni aniqlash faqat kriptogrammaning haqiqiy egasigagina ma'lum bo'lgan maxfiy kalit bilan amalga oshiriladi.

Asosiy qism

Ochiq kalitli kriptotizimlar teskarisi mavjud bo'lmagan yoki teskarisini aniqlash zamonaviy fan va texnika yutuqlaridan foydalangan holda ham juda katta moddiy sarf-harajatlar bilan va yetarlicha ko'p vaqt sarflash bilan amalga oshiriladigan bir tomonli funksiyalar funksiyalarga yoki algoritmlarga asoslanadi. Bir tomonli funksiyalar quyidagi xossaga ega bo'ladi[11-12]: berilgan x-qiymatda $f(x)$

© *I.M.Boyquziyev, E.I.Saydullayev, I.R.Rahmatullayev.*

funksiyaning qiymati y yetarli darajada oson hisoblanadi, ammo biror noma'lum x-qiymatda funksiyaning qiymati $y = f(x)$ ma'lum bo'lsa, x-qiymatni topishning ham moddiy jihatdan ham vaqt nuqtayi nazaridan yetarli darajadagi imkoni mavjud emas.

Ochiq kalitli kriptotizimlar ularning asosini tashkil etuvchi bir tomonli funksiyalar bilan farqlanadi.

Ochiq kalitli kriptotizimlar simmetrik kriptotizimlar algoritmlariga nisbatan murakkab bo'lgan hisoblash akslantirishlariga asoslanganligi sababli, ulardan aksariyat hollarda kalitlarni taqsimlashda foydalaniladi, katta hajmli ma'lumotlarni uzatishda asosan simmetrik kriptotizimlar qo'llaniladi.

Yuqorida ta'kidlanganidek, asimmetrik (ochiq kalitli) kriptotizmlarda ochiq va yopiq kalitlar shunday matematik qonuniyatlar bilan bog'langan bo'ladiki, ochiq kalitdan foydalangan holda maxfiy kalitni aniqlash masalasi yechilishi qiyin yoki effektiv algoritmi mavjud bo'lmagan matematik masalalarni yechishning murakkabliklariga asoslanadi. Masalan, yetarlicha katta razryadli sonni tub sonlar ko'paytmasi shaklida ifodalash yoki chekli maydonda diskret logarifmlash masalalarini yechish [1,4,13].

Mavjud asimmetrik kriptotizimlar asosan matematikada yechishning samarali usullari mavjud bo'lmagan quyidagi masalalarning murakkabliklariga asoslanadi[20-25]:

- Berilgan sonni tub ko'paytuvchilarga ajratish (faktorizatsiya)muammosi (RSA, Vilyams, Polig-Xellman) [1,4,8,13];
- Chekli maydonda diskret logarifmlash (DSA, EL-GAMAL, GOST 34.10-94) [1,8,26-27];
- Chekli maydonda chiziqli tenglamalar sistemasini yechish (Mak-Elis shifrlash algoritmi) [1,8];
- "Ryukzak " muammosi (Merkl-Xellman shifrlash algoritmi) [4,27];
- Chekli maydonda aniqlangan elliptik egri chiziq nuqtalari ustida amallar bajarish (ECDSA 2000, GOST R 34.10-2001) [4, 25].

Hozirgi kunda chekli maydonda aniqlangan elliptik egri chiziqlar kriptografiya sohasiga keng tatbiq etilmoqda.

1-ta'rif: Biror K-maydonda olingan elliptik egri chiziq deb, quyidagi Veyershtrass tenglamasi deb ataluvchi tenglik orqali aniqlanuvchi

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (1)$$

egri chiziqqa aytiladi, bu yerda $a_1, a_2, a_3, a_4, a_6 \in K$.

Elliptik egri chiziq odatda E yoki E/K bilan belgilanadi va elliptik egri chiziqqa tegishli nuqtalar, yani (1) tenglama yechimlari shu elliptik egri chiziqning affin nuqtalari deyiladi.

2-ta'rif: $P(x_0, y_0) \in E$ nuqta elliptik egri chiziqning silliq nuqtasi deyiladi, agar

$$f(x_0, y_0) = y_0^2 + a_1x_0y_0 + a_3y_0 - x_0^3 - a_2x_0^2 - a_4x_0 - a_6$$

bo'lib, quyidagi shartlardan bittasi o'rinli bo'lsa:

$$f_x'(x_0, y_0) \neq 0 \ \ yoki \ \ f_y'(x_0, y_0) \neq 0 \quad (2)$$

Quyida elliptik egri chiziqlarning umumiy kanonik ko'rinishi keltirilgan

$$y^2 = x^3 + ax^2 + bx + c \ , \ (3)$$

bu erda $a, b, c \in Z$ (a, b, c - butun sonlar) va ko'phad $p(x) = x^3 + ax^2 + bx + c$ karrali ildizga ega emas deb qaraladi.

Oldindan shuni aytish lozimki, hozirgi kunda $y^2 = x^3 + ax^2 + bx + c$,

tenglamaning barcha ratsional echimlarini aniqlash usuli matematikada noma'lumligicha qolib kelmoqda. Lekin, quyidagi ikkita usuldan foydalanib, ratsional echimlarni topish mumkin.

1-usul. Tanlangan $y^2=x^3+ax+b$ tenglamaga x_i qiymatlarni berib, tenglamaning o'ng tomoni to'la kvadrat tashkil qilish tekshiriladi. Agar biror x_k qiymatda tenglikni o'ng tomonidagi ifodaning

© I.M.Boyquziyev, E.I.Saydullayev, I.R.Rahmatullayev.

qiymati to‘la kvadrat tashkil qilsa, u holda tenglamaga tegishli nuqta koordinatalarini

$$(x_k ; y_k = \pm\sqrt{x_k^3 + ax_k + b}\ )\ (4)$$

juftliklar bilan fiksirlanadi.

2- usul. Bu usulda nuqta koordinatalari (x; y) va tenglamaning bitta a –koeffistientini fiksirlab: (a; x; $y \in R$) ,

$$b=y^2-x^3-ax\ (5)$$

formula orqali b–koeffistient hisoblab topiladi va uning asosida tenglama quriladi. Elliptik egri chiziq koeffistientlarini olingan ratdional koordinatali nuqta orqali aniqlashning bunday usuli samarali hisoblanadi.

$P+Q$ yig’indi nuqta koordinatasini hisoblash formulasini keltirib chiqarish mumkin. $P+Q$ nuqta R – nuqtani Ox - o‘qiga simmetrik ko‘chirishdan hosil bo‘ladi. Natijada, yig‘indi nuqtaning koordinatalari (u,v), deb belgilansa, bu koordinatalar quyidagi formulalar orqali topiladi:

$$u = k^2 - a - x_1 - x_2,$$

$$v = -ku - d = -(k(u - x_1) + y_1)$$

chunki $u = x_3$, $v = -y_3$. Bu formulada k - koeffistienti qiymatining o‘rniga $\frac{y_1 - y_2}{x_1 - x_2}$ qo‘yilsa, quyidagi tengliklar hosil bo‘ladi:

$$\begin{cases} v = \dfrac{y_1 - y_2}{x_1 - x_2}(-u + x_1) - y_1, \\ u = \dfrac{(y_1 - y_2)^2}{(x_1 - x_2)^2} - (a + x_1 + x_2) \end{cases} (6)$$

Bu erda, $x_1 \neq x_2$.

Agar $x_1 = x_2$ bo’lsa, u holda kesuvchi to‘g‘ri chiziq o‘rniga urinma o‘tkazilib, quyidagi formulalar keltirib chiqariladi:

$$\begin{cases} u = -2x_1 - a + \dfrac{(3x_1^2 + 2ax_1 + b)^2}{4y_1^2}, \\ v = -y_1 - \dfrac{3x_1^2 + 2ax_1 + b}{2y_1}(u - x_1). \end{cases} (7)$$

Shunday qilib, hech bo‘lmasa bitta P - ratsional nuqta elliptik egri chiziqdagi nuqta bo‘lsa, u holda (6), (7) - formulalar orqali $[2]P$-ni topish uchun, $[3]P=P+P$, $[3]P$-ni topish uchun, $[3]P=[2]P+P$, shu kabi $[4]P=[3]P+P$, $[5]P=[4]P+P$ va hokazolarni topishimiz mumkin bo‘ladi.

Shuni alohida ta’kidlash kerakki, keltirilgan (6) va (7) formulalar (3) tenglamaga nisbatan keltirib chiqarildi. Endi elliptik egri chiziqning (EECh) kriptografiyada keng qo‘llaniladigan

$$y = x^3 + ax + b$$

tenglamasi uchun ratsional nuqtalarini qo‘shish formulalari keltirib o‘tiladi:

$$\begin{cases} u = \dfrac{(y_1 - y_2)^2}{(x_1 - x_2)^2} - x_1 - x_2, \\ v = -y_1 + \dfrac{y_1 - y_2}{x_1 - x_2}(x_1 - u). \end{cases}$$

bu erda, $x_1 \neq x_2$.

Agar $x_1 = x_2$ bo‘lsa, u holda

$$\begin{cases} u = \dfrac{(3x_1^2 + a)^2}{4y_1^2} - 2x_1, \\ v = -y_1 - \dfrac{3x_1^2 + a}{2y_1}(x_1 - u). \end{cases}$$

Oldindan berilgan $y^2 = x^3 + ax^2 + bx + c$ - EECh ratsional nuqtalarini topishning samarali usulini aniqlash hozirgi kunda sonlar nazariyasining muammolaridan biri hisoblansada, egri chiziqqa tegishli bitta nuqta topilsa, qolganlari (6), (7) formulalar orqali aniqlanadi.

© I.M.Boyquziyev, E.I.Saydullayev, I.R.Rahmatullayev.

EECh nuqtalarini qo‘shish jarayonida quyidagi ikkita holat bo‘lishi mumkin:

1. Biror n –qadamda $[n]P = 0_E$ tenglik bajarilishi mumkin;
2. $[2]P$, $[3]P$, $[4]P$ va hokazo $[n]P$ – nuqtalar har xil qiymatga ega bo‘lishi mumkin.
3. *3-ta’rif:* Agar barcha $m < n$ holatlarda $[m]P \neq 0_E$ bajarilib, $[n]P = 0_E$ bo’lsa, u holda P – nuqta n – chekli tartibga ega deyiladi.

O‘tgan asrning 80-yillarida EECh katta sonlarni faktorlash algoritmlarini tuzish sohasida qo‘llanila boshladi va bu qo‘llanishlar orqali kriptografiya sohasiga kirib keldi (nosimmetrik tizimlar, psevdotasodifiy sonlarni generastiyalash). Elliptik kriptografiyada haqiqiy burilish 1985-yilda N.Koblist va V.Miller ilmiy ishlari chop etilgandan so‘ng yuz berdi. Shu damdan boshlab mashhur jahon kritologlari elliptik kriptografiya bilan shug‘ullana boshladilar

1-jadval.

Kriptotahlil murakkabliklari bo‘yicha ma’lumotlar

Almashtirish moduli uzunligi	EECh gruppasida kriptotahlil murakkabligi	RSA modulini faktorlash murakkabligi
192 bit	$2^{95,82} \approx 10^{29,21}$	$2^{40,41} \approx 10^{12,32}$
256 bit	$2^{127,82} \approx 10^{39}$	$2^{40,56} \approx 10^{14,5}$
512 bit	$2^{255,82} \approx 10^{78}$	$2^{65,15} \approx 10^{19,86}$
1024 bit	$2^{511,82} \approx 10^{156}$	$2^{88,47} \approx 10^{27}$

Kriptografiyada chekli algebraik strukturalarda, masalan, chekli maydonlarda berilgan EEChdan keng foydalaniladi. Tub maydon *GF(p)* da berilgan EECh

$$y^2 = x^3 + ax + b \pmod p \qquad (10)$$

taqqoslamaning $P = (x, y)$ nuqtalari (echimlari) to‘plamini tashkil etadi. Bu yerda a va b kattaliklari $4a^3 + 27b \neq 0 \pmod p$ shartini qanoatlantiruvchi doimiylar, $p>3$. To’plam gruppani tashkil etishi uchun unga cheksiz uzoqlashgan $0_E=(x,\infty)$ nuqta birlashtiriladi, natijada gruppa tashuvchisi $E=\{4 \text{ echimlari}\} U\{0\}$ ko’rinishni oladi. Mazkur gruppaning kriptografiya uchun asosiy amali nuqtalarni takroran m marta qo‘shish amali $[m]P$ bo’lib, uni $[m]$ ga ko‘paytirish deb ataladi va u rekursiv suratda amalga oshiriladi. Ochiq kalitli kriptografiyada yaratilgan ko‘pchilik algoritmlarning EEChli analoglari ishlab chiqilgan. Elliptik egri chiziqli kriptotizimlar kriptobardoshliligi EEChda diskret logarifmlash muammosining murakkabligi bilan belgilanadi.

Quyida ushbu murakkablikka asoslangan EC DSA 2000 ERI standartida imzoni generatsiya qilish va tekshirish jarayoni hamda algoritmning korrektligi keltirilgan.

Imzo generasiya qilish algoritmi. Boshlang‘ich ma’lumotlar: m ma’lumot, berilgan parametrlar va imzo kaliti. Natija: imzo (r, s).

1. $1 \le k \le n-1$ intervaldan tasodifiy k soni tanlansin, bu yerda G nuqta tartibi $n > \max\{2^{160}, 4\sqrt{p}\}$ shartni qanoatlantiruvchi tub son bo‘lishi kerak.
2. $(x_1, y_1) := [k]G$ hisoblansin.
3. $r := x_1 \bmod n$ hisoblansin.
4. Agar $r = 0$ bo‘lsa, u holda 1-qadamga borilsin.
5. $z := k^{-1} \bmod n$ hisoblansin.
6. $e := h(m)$ hisoblansin.
7. $s := z(e + dr) \bmod n$ hisoblansin.
8. Agar $s = 0$ bo‘lsa, u holda 1-qadamga borilsin.
9. m ma’lumot imzosi - (r, s) juftligidan iborat.

Imzoni tekshirish algoritmi. Boshlang‘ich ma’lumotlar: m ma’lumot, berilgan parametrlar, imzoni tekshirish kaliti va m ma’lumot imzosi.

Natija: imzo haqiqiyligi yoki qalbakiligi haqidagi tasdiq.

© I.M.Boyquziyev, E.I.Saydullayev, I.R.Rahmatullayev.

1) Agar $1 \le r, s \le n-1$ shart bajarilmasa, u holda imzo qalbaki va imzoni tekshirish algoritmi tugatiladi.
1. $e := h(m)$ hisoblansin.
2. $w := s^{-1} \bmod n$ hisoblansin.
3. $u_1 := ew \bmod n$ hisoblansin.
4. $u_2 := rw \bmod n$ hisoblansin.
5. $X := [u_1]G + [u_2]Q = (x_1, y_1)$ hisoblansin.
6. Agar $r = x_1 \bmod n$ shart bajarilsa, u holda imzo haqiqiy, aks holda imzo qalbaki va imzoni tekshirish algoritmi tugatiladi.

Imzo algoritmining korrektligi. Isbot qilishimiz kerakki, generasiya qilish algoritmi orqali qo'yilgan ixtiyoriy imzo, uni tekshirish algoritmi orqali solishtirilganda to'g'ri natijaga erishiladi.

Imzoni generatsiya qilish algoritmidan olingan r va s parametrlar n butun songa bo'lingandagi qoldiq sifatida olinganligi uchun $n-1$ qiymatdan katta bo'lmaydi. Ikkinchi tomondan esa to'rtinchi va sakkizinchi qadamlariga ko'ra, bu parametrlar 0 dan farqli qiymatga ega bo'ladi. U holda, imzoni tekshirish algoritmining 1-qadamida berilgan shart r va s parametrlar uchun har doim o'rinli bo'lishi shart.

Imzoni generatsiya qilish algoritmining beshinchi va yettinchi qadamlaridan foydalanib, $ks \equiv e + dr (mod\, n)$ tenglikka ega bo'lamiz . U holda $w := s^{-1} \, mod\, n$ (imzoni tekshirish algoritmning uchinchi qadami) ekanligidan $k \equiv we + wdr (mod\, n)$ kelib chiqadi. Algoritm shartiga ko'ra, G nuqta n tartibga ega, natijada:

$$[k]G = [we + wdr]G = [we]G + [wr][d]G = [we]G + [wr]Q = [u_1]G + [u_2]Q = X.$$

Demak, imzoni tekshirish algoritmining 6-qadamidan olinadigan X nuqta $[k]G$ nuqtaga teng bo'ladi. X nuqtaning birinchi koordinatasi x_1 va uning $\bmod n$ bo'yicha qoldig'i r ga teng (imzoni generasiya qilish algoritmining 3-qadamiga ko'ra). Ya'ni, algoritm korrektligi isbotlandi.

Misol: F_p maydonda $y^2 = x^3 + 13x + 17$ tenglamaga nisbatan parametrlar tanlansin. Maydon xarakteristikasi p = *1000003* bo'lsin. Boshlang'ich nuqta sifatida *G(439;1900)* nuqtani olamiz. U holda tanlangan *G(439;1900)* –bazaviy nuqtaning berilgan $y^2 = x^3 + 13x + 17$ -elliptik egri chiziqdagi tartibi algoritm talabiga ko'ra, tub *va n=500933* ga teng. Endi algoritm keyingi qadamlariga muvofiq ochiq va maxfiy kalitlarni tanlaymiz.

Imzo qo'yish kaliti (maxfiy kalit) sifatida – $[0;n]$ intervaldagi ixtiyoriy $d = 63289$ sonini olamiz.

Imzoni tekshirish kaliti (ochiq kalit) sifatida elliptik egri chiziqdagi $Q = [d]G$ nuqta, ya'ni $Q = [63289]G = (168708; 576959)$.

Bundan tashqari raqamli imzo algoritmida xesh funksiya qiymatidan h ham foydalaniladi. Ushbu misolda xesh qiymat sifatida *h=86347* qiymatdan shartli ravishda foydalanamiz.

Xulosa

Elliptik egri chiziqlarga asoslangan kriptotizimlar kriptografiyaga 1985-yilda V.Miller va N.Koblis tomonidan tadbiq qilingan. Kriptografik algoritmlarning ko'pchiligi faktorizatsiyalash va chekli maydonda diskret logarifimlash masalalarining murakkabligiga asoslangan bo'lib, bu algoritmlarni elliptik chiziqlarga o'tkazish masalasi alohida izlanish talab etadi. Keyingi tadqiqot ishlarida bu murakkabliklarga asoslangan algoritmlarni elliptik egri chiziqlarga o'tkazish hamda elliptik egri chiziqlarning ratsional nuqtalarini aniqlash masalalariga yo'naltirilgan algoritmlar bo'yicha izlanishlar olib borish ko'zda tutulgan.

Foydalanilgan adabiyotlar

1. Alferov A.AN, Zubov A.Yu., Kuzmin A.S., Cheryomushkin A.V Osnovы kriptogarfii. M.: Gelios ARV, 2002. 2-ye izd.
2. D.Ye. Akbarov, V.V. Yasinskiy. Matematika v stanovlenii nauki kriptologii. –Kiyev.: Politexnika, 2001.-42 s.
3. D.Ye. Akbarov, Sh.Z.Nuriyev, Sh.Sh.Axmadaliyev. Kriptografiya asoslarida matematika. Farg'ona, 2003. -48 b.
4. D.Ye. Akbarov. Kriptografiya, standartы algoritmov kriptograficheskoy zaщitы

© I.M.Boyquziyev, E.I.Saydullayev, I.R.Rahmatullayev.

informatsii i ix prilojeniya. Izdatelstvo SNB, Tashkent, 2007g.-189s.
5. Akbarov D.Ye., Kuryazov D.M., Jumaniyazov M.O. «O'zbekiston Respublikasi davlat standartlari, xeshlash funksiyasi, ma'lumotlarni shifrlash va elektron raqamli imzo algoritmlari tahlili natijalari» ILMIY-TADQIQOT ISHI BO'YICHA HISOBOT (yakuniy), reg. № 8/150, 21.11.06y., 100 bet.
6. W. Diffie and M.E. Hellman, "New directions in cryptography" IEEE Trans. Informat. Theory, vol. IT-22, pp. 644-654, Nov. 1976.
7. R. C. Merkle, "Secure communication over insecure channels", Comm. ACM, pp. 294-299, Apr. 1978.
8. B.Shnayer. Prikladnaya kriptografiya. Izdatelstvo TRIUMF, Moskva, 2002-816s.
9. K.E. Shenon. Teoriya svyazi v sekretnых sistemax. V kn.: K.E. Shenon. Rabotы po teorii informatsii i kibernetike. M.: IL, 1963, tom 1. - S. 333-402.
10. K.E. Shenon. Teoriya svyazi v sekretnых sistemax. V kn.: K.E. Shenon. Rabotы po teorii informatsii i kibernetike. M.: IL, 1963, tom 2. -S. 243-332.
11. D.M. Kuryazov. Novыy variant algoritma ESP DSA s uvelicheniyem stoykosti. Materialы 4-y nauchno-prakticheskoy konferensii molodых uchenых SNB RUz."Aktualnыye problemы obespecheniya natsionalnoy bezopasnosti RUz" (16-iyunya 2006 g., gorod Tashkent), str.188-192.
12. D.M. Kuryazov, M.I. Zulpuqarov Telekommunikatsiya tarmog'ida himoyalangan elektron axborot almashinuvini tashkil etish mexanizmlari. Materialы 5-y nauchno- prakticheskoy konferensii molodых uchenых SNB RUz. "Aktualnыye problemы obespecheniya natsionalnoy bezopasnosti RUz" str.142-144.
13. D.M. Kuryazov. Sonlar nazariyasi elementlarining asimmetrik kriptotizimlar asoslarida qo'llanishlari. Izdatelstvo SNB, Tashkent, 2007 g.74s.
14. Zulpuqarov M.I. ELLIPTIK EGRI CHIZIQLARGA ASOSLANGAN ELEKTRON RAQAMLI IMZO ALGORITMLARI PARAMETRLARINI HISOBLASH. Axborot xavfsizligi yo'nalishi bo'yicha magistr darajasidagi DISSERTATSIYA**.** 2007-yil. 86 bet.
15. Koblitz N. "Elliptic Curve Cryptosystems", Mathematics of Computation, 48, 1987, pp.203-209.
16. Miller V. Use of elliptic curves in cryptography // Advances in cryptology – CRYPTO'85 (Santa Barbara, Calif., 1985). 1986 (Lecture Notes in Comput. Sci.: V.218). P. 417-426.
17. N. Koblis. Kurs teorii chisel i kriptografii.– M.Nauchnoye izd.TVP, 2001g.–261 s.
18. Moldavyan A.A., Moldavyan N.A. Kriptografiya ot primitivov k sintezu algoritmov. Sankt – Peterburg "BXV-Peterburg" 2004g. 448s.
19. Moldavyan A.A., Moldavyan N.A., Gus N.D., Izotov B.V. "Kriptografiya. Skorostnыe shifrы" Sankt-Peterburg. "BXV-Peterburg" 2002g. 439 s.
20. Moldavyan A.A., Moldavyan N.A. Vvedeniye v kriptosistemы s otkrытым klyuchom. Sankt – Peterburg "BXV-Peterburg" 2005g. 288s.
21. Rostovsev A.G., Maxovenko Ye. B., Teoreticheskaya kriptografiya. NPO "Professional", Sankt-Peterburg. 2004g. - 478 s.
22. Vasilenko O.N.Teoretiko-chislovыe algoritmы v kriptografii. – M., MSNMO, 2003. – 328 s.
23. www. cryptography.ru.
24. www. cryptology.com.
25. Xarin Yu.S., Bernik V.I., Matveev G.V., Agiyevich S.G. "Matematicheskiye i komyuternыe osnovы kriptologii" OOO "Novoye znaniye" 2003 g. 381 s.
26. Chmora A.L. "Sovremennaya prikladnaya kriptografiya" Moskva. "Gelios ARV" 2002g. 244 s.

© *I.M.Boyquziyev, E.I.Saydullayev, I.R.Rahmatullayev.*