MAVJUD NOSIMMETRIK KRIPTOTIZIMLARNING BARDOSHLILIGI

Xolbekov Umarali Zokir o‘g‘li

Jizzax politexnika instituti “ICHJA va B” kafedrasi, assistenti

umaralixolbekov@gmail.com

Annotatsiya: *Diskret logarifmlash va faktorlash muammolarini yechishga qaratilgan sonli maydon va halqalarda n moduli bo‘yicha sonlar silliqligi xossasidan foydalanadigan umumlashgan g‘alvir usuliga asoslangan tezkor algoritmlari ishlab chiqilgan.*

Kalit so‘zlar*: EECh (elliptik egri chiziqlar), smart-kartalar, mobil qurilmalar, kriptografiya, kriptoanaliz, kripto bardoshlilik, Koblits va Xasse teoremalari, Diffi-Xelmana algoritmi, spetsifikatsiyalash, RSA, (RSAP), (QRP), (SQROOT), diskret logarifm, (GDLP), Diffi-Xellman, (DHP), Diffi-Xellman, (GDHP) va (SUBSET-SUM) kvadratik chegirma.*

Аннотация: *Разработаны быстрые алгоритмы на основе обобщенного метода Гальвира, использующие свойство гладкости чисел по модулю n в числовых полях и циклах, направленные на решение задач дискретного логарифмирования и факторизации.*

Ключевые слова: *EECh (эллиптические кривые), смарт-карты, мобильные устройства, криптография, криптоанализ, криптотолерантность, теоремы Коблица и Хассе, алгоритм Диффи-Хельмана, спецификация, RSA, (RSAP), (QRP), (SQROOT), дискретный логарифм, (GDLP), Диффи-Хеллмана, (DHP), Диффи-Хеллмана, (GDHP) и (SUBSET-SUM) квадратичное вычитание.*

Abstract: *Fast algorithms based on the generalized Galvir method using the property of smoothness of numbers modulo n in numerical fields and loops aimed at solving discrete logarithmization and factoring problems have been developed.*

Keywords: *EECh (elliptic curves), smart cards, mobile devices, cryptography, cryptanalysis, crypto tolerance, Koblitz and Hasse theorems, Diffie-Helmana algorithm, specification, RSA, (RSAP), (QRP), (SQROOT), discrete logarithm, (GDLP), Diffi-Hellman, (DHP), Diffi-Hellman, (GDHP) and (SUBSET-SUM) quadratic subtraction.*

EECh (elliptik egri chiziqlar) gruppasida esa silliqlik tushunchasi aniqlanmaganligi ularda tezkor kriptotahlillash algoritmlarini tuzish imkoniyatini bermaydi;

- ikkinchidan, EECh (elliptik egri chiziqlar) gruppasida nisbatan qisqa kalit uzunligi asosida kriptotizimlar ishlab chiqarish imkoniyati mavjudligi. Bular simsiz kommunikatsiyalarda va resurs cheklangan hollarda (smart-kartalar, mobil qurilmalar) asosiy hisoblanadi.

Masalan, EECh (elliptik egri chiziqlar) gruppasida tuzilgan kalitning binar uzunligi *150* dan *350* gacha bo‘lgan qurilmalarda an’anaviy qurilmalardagi kalitning binar uzunligi *600* dan *1400* gacha bo‘lgandagidek kriptografik bardoshlilik darajasiga erishiladi.

Yuqorida keltirilgan sabablar AQSh va Rossiya Federatsiyasida amaldagi standartlarni elliptik kriptografiyaga oid standartlar bilan almashtirishga olib keldi. Hozirgi kunda EECh (elliptik egri chiziqlar) larga asoslangan algoritmlar ko‘plab xalqaro, milliy va sohaga oid standartlar qatoridan o‘rin olgan. Elliptik kriptografiyada foydalanish uchun asosan $GF(2^m)$ maydonida aniqlangan singulyar yoki $GF(p)$ maydonida aniqlangan nosupersingulyar EECh (elliptik egri chiziqlar) lardan foydalanish tavsiya etiladi. Barcha hollarda EECh (elliptik egri chiziqlar) gruppasida katta tartibga ega bo‘lgan elementlar mavjudligiga ishonch hosil qilish muhimdir.

Kriptografiyada chekli algebraik strukturalarda, masalan, chekli maydonlarda berilgan EECh (elliptik egri chiziqlar) dan keng foydalaniladi. Tub maydon $GF(p)$ da berilgan elliptik egri chiziq $y^2\ q\ x^3\ Qa*xQb\ (mod\ p)$ (1.1)

Taqqoslamaning $P\ q\ (x, y)$ nuqtalari (yechimlari) to‘plamini tashkil etadi. Bu erda a va $b\ 4*a^3\ Q27*b \neq 0\ (mod\ p)$ shartini qanoatlantiruvchi doimiylar, $p>3$. To‘plam gruppani tashkil etishi uchun unga cheksiz uzoqlashgan $0q(x,\infty)$ nuqta birlashtiriladi, natijada gruppa tashuvchisi $Eq\{1.1\ yyechimlari\}\ U\{0\}$ 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. Umuman olganda eliptik egri chiziqlarda ko‘paytma degan tushuncha yo‘q, faqat qo‘shish amali mavjud.

Agar elliptik egri chiziqda joylashgan ixtiyoriy nuqtani ikkinchi nuqta bilan qo‘shadigan bo‘lsak unda uchinchi nuqtaga ega bo‘lamiz va bu nuqta xam shu egri chiziqqa tegishli bo‘ladi.

Qo‘shish amalini xosil qilish uchun Koblits va Xasse teoremalaridan foydalangan xolda keltirilib chiqariladi. Elliptik egri chiziqda ikki nuqtani qo‘shishda quyidagi formula o‘rinli bo‘ladi:

$$\forall(x_1, y_1) \in E(x_2, y_2) \in E, x_1 \neq x_2 (x_1, y_1) + (x_2, y_2) = (x_3, y_3)$$

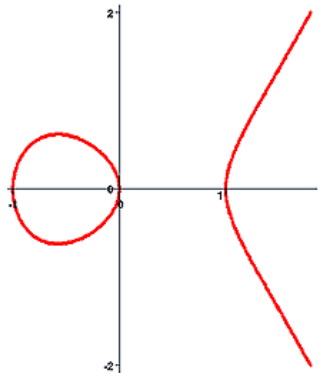
Bu yerda,

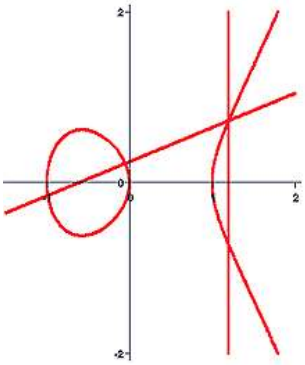
$$x_3 = \lambda^2 - x_1 - x_2,$$

$$y_3 = \lambda(x_1 - x_3) - y_1,$$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

Quyidagi rasmda yuqoridagi formulani geometrik tasviri keltirilgan, yahni egri chiziqda joylashgan ikki nuqtani kesib o‘tgan to‘g‘ri chiziq albatta uni uchinchi nuqtada xam kesib o‘tadi.





Elliptik egri chiziqni kriptografiyada qo‘llash uchun esa bir nuqtani o‘ziga qayta qo‘shish amalini bajarish kerak, bu degani tanlangan nuqtaga urinma o‘tqazish degan tushunchani beradi. Shunda Y=XG ni boshqacha qilib Y=G+G+G+G+G+G… deb yozish mumkin G Lar soni X ga teng bo‘ladi.

Urinma uchun qo‘shish formulasi quyidagi ko‘rinishga ega bo‘ladi:

$$\forall(x_1, y_1) \in E, y_1 \neq 0, (x_1, y_1) + (x_1, y_1) = (x_3, y_3)$$

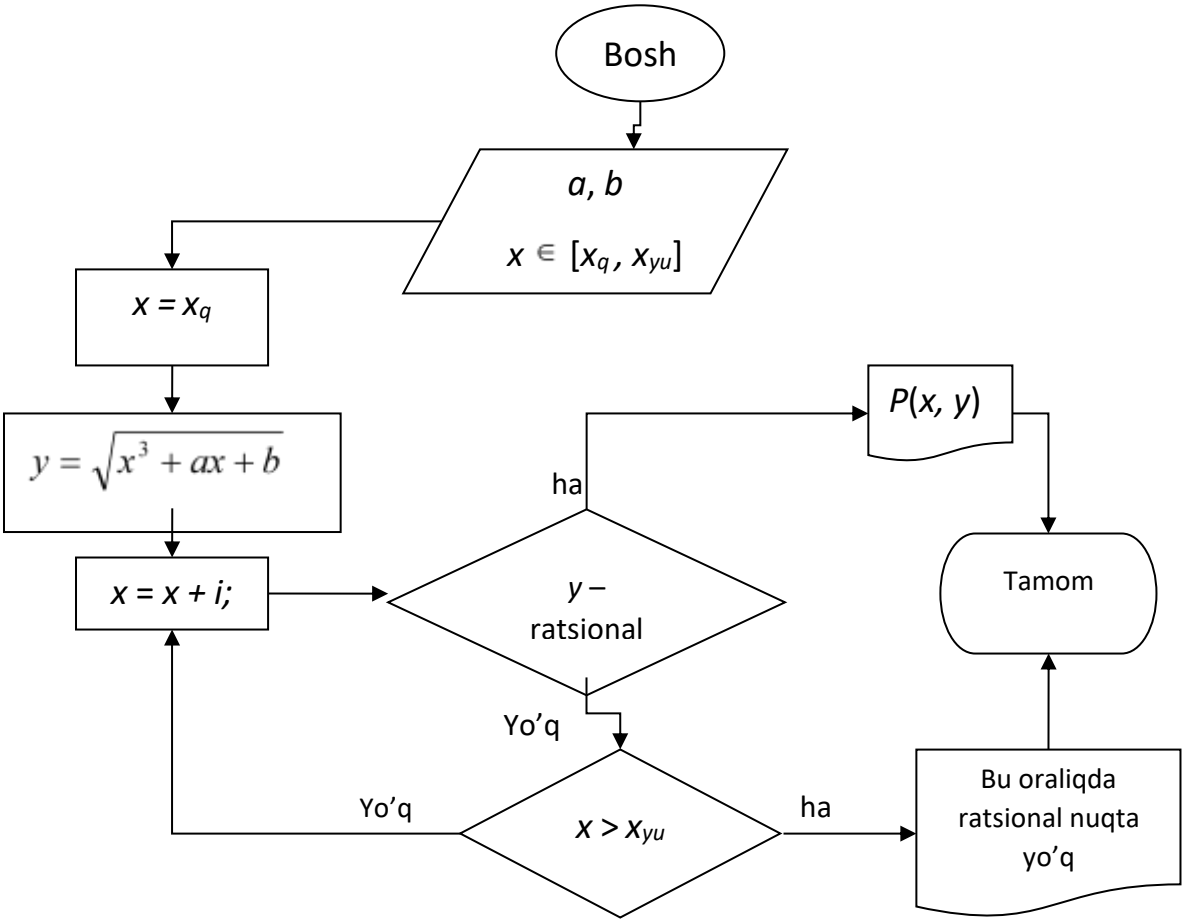
Bu erda:

$$x_3 = \lambda^2 - 2x_1,$$

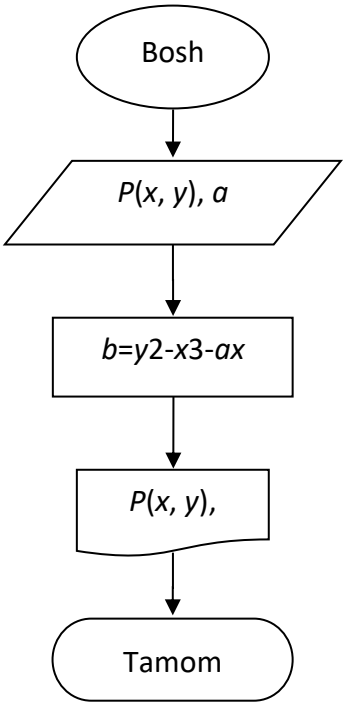
$$y_3 = \lambda(x_1 - x_3) - y_1$$

$$\lambda = \frac{3x_1^2 + a}{2y_1}$$

Quyidagi - rasmda elliptik egri chiziqning ratsional nuqtalarini topish blok-sxemasi keltirilgan.



1-rasm. Ratsional nuqtalarni topish sxemasi. (kirilchaga o‘tkazib qo‘ying.)
Quyidagi zaruriy shartlar qo‘yilganda ratsional nuqtalarni topish keltirilgan.



2-Rasm. Ratsional nuqtalarni topish (shart qo‘yilganda).

Kriptografiyada elliptik egri chiziqlardan nosimmetrik tizimlarda ishlatilib kelinmoqda. Xususan Diffi-Xelmana algoritmining analogi sifatida ishlatib kelinmoqda.

EECh (elliptik egri chiziqlar) gruppasida har qanday kriptografik algoritmni tuzish tizim parametrlarini spetsifikatsiyalashdan boshlanib, kriptografik algoritmni tuzish va uni sinab ko‘rish bilan yakunlanadi.

Yuqorida aytib o‘tilgan muammolardan tashqari boshqa muammolar ham mavjud bo‘lib, ularga RSA (RSAP), kvadratik chegirma (QRP), n moduli bo‘yicha kvadrat ildiz (SQROOT), umumlashgan diskret logarifm (GDLP), Diffi-Xellman (DHP), Diffi-Xellmanning umumlashgan (GDHP) va qismto‘plam-yig‘indisi (SUBSET-SUM) muammolari va daraja parametri muammosi ham kiradi.

Daraja parametri muammosi o‘zbekistonlik olimlar tomonidan kiritilgan bo‘lib, bir tomonlama funktsiyaga qo‘shimcha maxfiylik - *R* parametri kiritishga asoslanadi.

Mavjud nosimmetrik kriptotizimlar bardoshliligini ta’minlashga asos bo‘lgan murakkab muammo (masala) turi bo‘yicha quyidagicha tasniflanadi:

faktorlash muammosining murakkabligiga asoslangan kriptotizimlar;

diskret logarifm muammosining murakkabligiga asoslangan kriptotizimlar;

elliptik egri chiziqda diskret logarifm muammosining murakkabligiga asoslangan kriptotizimlar;

boshqa muammolarga asoslangan kriptotizimlar.

Bu keltirilgan har bir masalaning yechilishi bugungi kun hisoblash qurilmalari imkoniyatlaridan to‘la foydalanilganda ham murakkab va qiyin bo‘lgan yoki umuman yyechib bo‘lmasligi nazariy jihatdan isbotlangan masalalarga olib keladi.

Mavjud nosimmetrik kriptoalgoritmlar orasida xalqaro va davlat standartlari maqomiga ega bo‘lgan ERI algoritmlarining ko‘pchiligi faktorlash (RSA, ESIGN), diskret logarifmlash (DSA, GOST R 34.10–94), EECh (elliptik egri chiziqlar) da diskret logarifmlash (GOST R 34.10-2001, EC-DSA-2000, EC-KCDSA, EC-GDSA va DSTU 4145-2002) va daraja parametri (O‘z DSt 1092:2005, O‘z DSt 1092:2009) muammolarining murakkabligiga asoslangan algoritmlardir.

Xulosa: Shunday qilib, nosimmetrik kriptotizimlarga asoslangan algoritmlar boshqa kriptotizimlar algoritmlariga nisbatan murakkabroq hisoblash jarayonlariga asoslanadi. Shuning uchun ham zamonaviy axborot tizimlarida ochiq kalitli shifrlash algoritmlaridan keng foydalanidi. Ularga misol qilib, RSA, El Gamal va elliptik egri chiziqlarga asoslangan algoritmlarni keltirish mumkin.

Foydalanilgan adabiyotlar ro‘yxati

1. Akbarov D.E. Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qo‘llanishlari. Toshkent. “O‘zbekiston markasi “, 2009. - 432 b.

2. O‘z DSt 1092:2009 «Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari».

5. Брюс Шнаер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ - Москва: ТРИУМФ, 2002.

6. Xasanov X.P. Takomillashgan diamatritsalar algebralari va parametrli algebra asosida kriptotizimlar yaratish usullari va algoritmlari. - Toshkent, 2008. 208 b.