ISSN 2181-3187

ELLIPTIK EGRI CHIZIQLARDA NUQTALARNI TOPISH MUAMMOSIGA ASOSLANGAN SHIFRLASH

Axrorbek Otaqo'ziyev Abdunazar o'g'li
Mirzo Ulug'bek nomidagi O'zbekiston milliy universiteti Jizzax filiali.
Axborot xavfsizligi (sohalar bo'yicha)
998-91-603-12-75

Annotatsiya: ushbu maqola shifrlashning maftunkor olamiga kirib boradi, xususan elliptik egri chiziqlardan foydalanishga qaratilgan. Bu elliptik egri kriptografiyaning matematik asosini va uning raqamli aloqani ta'minlashdagi ahamiyatini tushuntiradi.

Kalit so'zlar: Elliptik egri chiziqlar, nuqtalarni hisoblash muammosi, kodlash, cheklangan maydonlar, kriptografiya, sonlar nazariyasi.

Elliptik egri chiziqlar zamonaviy kriptografiyada xavfsiz aloqa va shifrlash protokollari uchun asos bo'lib xizmat qiladigan keng dasturlarni topdi. Ushbu domendagi asosiy muammo bu nuqta sonini aniqlashdir elliptik egri chiziq cheklangan maydon ustida aniqlangan, ko'pincha nuqta hisoblash muammosi. Ushbu muammoning samarali echimlari xavfsiz elliptik egri chiziqli kriptografik tizimlar uchun juda muhimdir. Ushbu maqolada biz nuqtalarni hisoblash muammosini hal qilishda kodlash texnikasining rolini o'rganamiz. Biz mavjud usullarni har tomonlama ko'rib chiqamiz va turli kodlash strategiyalarining nuqtalarni hisoblash algoritmlari samaradorligiga ta'sirini tahlil qilish uchun eksperimental natijalarni taqdim etamiz.

Ushbu bo'limda biz nuqtalarni hisoblash muammosini hal qilishda ishlatiladigan turli xil kodlash usullarini muhokama qilamiz. Biz turli xil kodlash strategiyalariga tayanadigan Schoof algoritmi va SEA (Schoof-Elkies-Atkin) kabi klassik usullarni ko'rib chiqamiz. Bundan tashqari, biz kodlashdagi so'nggi yutuqlarni, jumladan Montgomeri vakolatxonasini va Edvards egri chiziqlarini o'rganamiz. Biz ushbu texnikalarning batafsil tahlilini taqdim etamiz, ularning kuchli va zaif tomonlarini ta'kidlaymiz.

Elliptik egri kriptografiya - elliptik egri chiziqlarning matematik xususiyatlariga asoslangan mashhur shifrlash texnikasi. Elliptik egri kriptografiya nisbatan kichik kalit o'lchamlari bilan kuchli xavfsizlikni ta'minlaydi, bu uni turli xil ilovalar, jumladan, xavfsiz aloqa va raqamli imzolar uchun mos qiladi.

ISSN 2181-3187

Elliptik egri chiziq deb, quyidagi Veyershtrass tenglamasi deb ataluvchi tenglik orqali aniqlanuvchi

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (3.1)$$

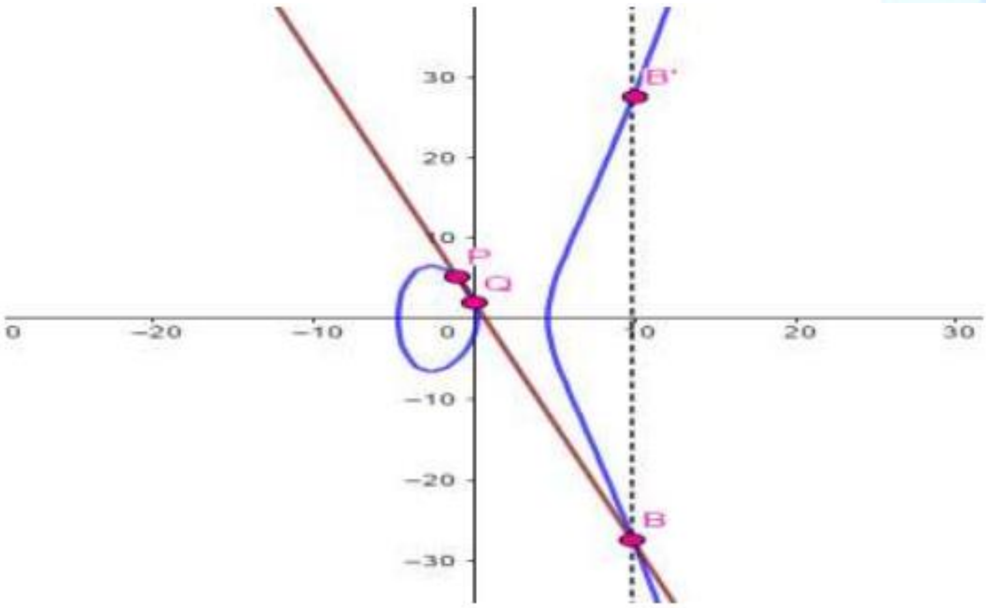
egri chiziqqa aytiladi, bu yerda a_1, a_2, a_3, a_4, a_6 – haqiqiy sonlar. [1. 204-b]

Biz quyidagi,

$y^2 = x^3 - 22x + 4$ elliptik egri chiziqda $P(0;2)$, $Q(-1;5)$ nuqtalar mavjudligini bilganimiz holda uning boshqa ratsional koordinatali nuqtalarini aniqlaylik.

Buning uchun, bu nuqtalar orqali to’g’ri chiziq o’tkazaylik. U holda, o’tkazilgan chiziq, egri chiziqni uchinchi nuqtada kesib o’tadi. Bu $B(x_3, y_3)$ nuqta Ox o’qiga simmetrik ko’chiriladi va hosil bo‘lgan $B'(x_3, -y_3)$ nuqta, P va Q nuqtalarning elliptik egri chiziq ustida yig‘indisi deb e’lon qilamiz:

$$B^{`}(x_3, -y_3) = P(x_1, y_1) + Q(x_2, y_2)$$



Tasdiq. Agar $P(x_1, y_1), Q(x_2, y_2) \in E$ nuqtalar ratsional koordinatali bo’lsa, u holda $B(x_{3,} y_3)$ nuqta koordinatalari ham ratsional bo’ladi. [1.209-b]

Isboti. $P(x_1, y_1)$, $Q(x_2, y_2) \in E$ nuqtalar orqali o’tuvchi to’g’ri chiziqning umumiy ko’rinishi:

$y = kx + d$

ISSN 2181-3187

ifodaga ega bo'lib, bu yerda k, d - koeffisientlar. $P(x_1,y_1)$, $Q(x_2,y_2)$ – nuqtalar $y = kx + d$ chiziqqa tegishli. Bundan esa:

$$\begin{cases} y_1 = kx_1 + d \\ y_2 = kx_2 + d \end{cases}, \qquad y_1 - y_2 = k(x_1 - x_2) \text{ va } k = \frac{y_1 - y_2}{x_1 - x_2}$$

$$d = y_1 - kx_1 = y_1 - \left(\frac{y - y_2}{x - x_2}\right) \cdot x_1 = \frac{y_2 x_1 - y_1 x_2}{x_1 - x_2}$$

ekanligi kelib chiqadi.

$y = kx + d$ to'g'ri chizig'i tiklab olindi. Demak, $y = 2 - 3x$ to'g'ri chiziq P va Q nuqtalardan o'tuvchi to'g'ri chiziq. Keyingi qadamda $y = kx + d$ ifoda

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

elliptik egri chiziqning tenglamasiga qo'yilsa, to'g'ri chiziq va elliptik egri chiziqning 3- nuqtasini topa olamiz, ya'ni:

$$(kx + d)^2 = x^3 + ax^2 + bx + c,$$

$$x^3 + (a - k^2)x^2 + (b - 2kd)x + c - d^2 = 0,$$

$$(2 - 3x)^2 = x^3 - 22x + 4$$

Demak, $y^2 = x^3 - 22x + 4$ elliptik egri chiziqda mavjud 3- ratsional

u holda uchinchi tartibli tenglama uchun Viyet teoremasiga ko'ra:

$$x_1 + x_2 + x_3 = k^2 - a = 9$$

tenglik o'rinli bo'lib, bu oxirgi tenglikda x_1, x_2 ratsional sonlar bo'lganligi uchun, x_3 ham ratsional son bo'ladi. Xuddi shuningdek,

$$y_3 = kx_3 + d$$

ifodaga ko'ra, y_1 sonining ham ratsional ekanligi kelib chiqadi.

Bu keltirilgan tasdiq isbotidan esa $P + Q$ yig'indi nuqta koordinatasini hisoblash formulasi keltirilib chiqariladi. $P + Q$ nuqta R nuqtani Ox o'qiga simmetrik ko'chirishdan hosil bo'lar edi. Natijada, yig'indi nuqtaning koordinatalari (u, v) deb belgilansa, bu koordinatalar quyidagi formulalar orqali topiladi, chunki, $u = x_3$, $v = -y_3$.

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

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

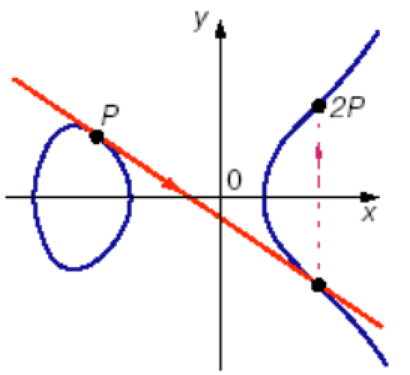
ISSN 2181-3187

$B(10,28)$ nuqta topildi. Endi, umumiy holda, B nuqtani aniqlaylik. Buning uchun, yuqoridagi formulada k koeffisientning qiymati o'rniga qo'yilsa, ushbu:

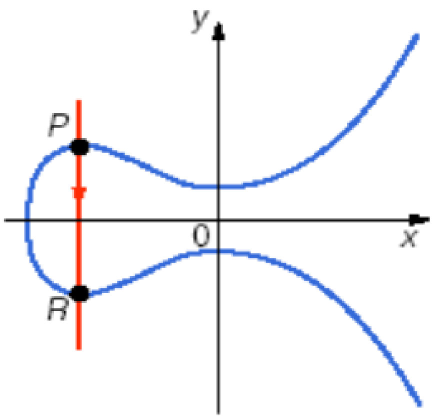
$$\begin{cases} v = \dfrac{y_1 - y_2}{x_1 - x_2}(-u + x_1) - y_1 \\ u = (\dfrac{y_1 - y_2}{x_1 - x_2})^2 - (a + x_1 + x_2) \end{cases}$$

tengliklarga ega bo'linadi, bu yerda $x_1 \neq x_2$.

$P + P = ?$ qanday amalga oshirilishi haqida to'xtalaylik. Buning uchun elliptik egri chiziqdagi P-nuqta orqali urinma to‘g‘ri chiziq o‘tkaziladi. Bu urinma elliptik egri chiziq grafigidagi ikkinchi qismni (giperbola qismida) biror nuqtada kesib o‘tadi. Ana shu kesib o‘tgan nuqtani Ox-o‘qiga nisbatan simmetrik ko‘chiriladi va bu nuqta $2P$ deb elon qilinadi: So‘ngra, $3P$-ni topish uchun, $3P = P + 2P$, shu kabi $4P = P + 3P$, $5P = 4P + P$ va hokazolar amalga oshiriladi.



Har doim ham $P(x_1,y_1)$ va $Q(x_2,y_2)$ nuqtalar orqali o‘tuvchi to‘g‘ri chiziq elliptik egri chiziqni uchinchi nuqtada kesib o‘tavermaydi. Masalan, $P(x_1,y_1)$ va $Q(x_1,-y_1)$ nuqtalardan o‘tuvchi to‘g‘ri chiziq Ox -o‘qiga perpendikulyar bo‘lib, u elliptik egri chiziqni uchinchi nuqtada kesib o‘tmaydi:



Bunday holda o‘tkazilgan to‘g‘ri chiziq elliptik egri chiziqni cheksizlikda kesib o‘tadi deb qabul qilinib, cheksizlikdagi barcha nuqtalar bitta nol nuqtaga birlashtirilgan deb hisoblanadi, ya’ni cheksizlikdagi barcha nuqtalar, elliptik egri chiziq nuqtalari ustida aniqlangan qo‘shish amaliga nisbatan, haqiqiy sonlarni qo‘shishdagi nol qiymati kabi xossaga ega. Bevosita hisoblashlar bilan ko‘rsatish mumkinki, elliptik egri chiziq nuqtalarini qo‘shish amali Abel gruppasini tashkil etadi, yani elliptik egri chiziqqa tegishli bo‘lgan a,b,c – nuqtalar uchun:

1) kommutativlik $a+b=b+a$;
2) assotsiativlik $(a+b)+c=(b+c)+a$;
3) nol elementining mavjudligi $a+E=a$;
4) teskari (qarama - qarshi) elementning mavjudligi $a+(-a)=E$

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

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

Shunday qilib, hech bo’lmasa bitta P ratsional nuqta elliptik egri chiziqdagi nuqta bo’lsa, u holda yuqoridagi formula yordamida $2P,\ 3P,\ 4P, \ldots$ va hokazolarni topishimiz mumkin bo’ladi.

Misol. Elliptik egri chiziq $y^2 = x^3 - 13$, unga tegishli nuqta $P(17;-70)$ berilgan bo’lsa, bu nuqtaning yig’indisini ifodalovchi nuqtalar topilsin. *2P=?, 3P=?, 4P=?, 5P=?*

Yechish. (1) va (2) formuladan foydalanilsa,

$$y^2 = x^3 + ax^2 + bx + c, \qquad a = 0, b = 0, c = -13$$

$$u = -2x_1 - a + \frac{(3x_1^2 + 2ax_1 + b)^2}{4y_1^2} = -2\cdot 17 - 0 + \frac{(3\cdot 17^2 + 2\cdot 0\cdot 17 + 0)^2}{4\cdot(-70)^2}$$

$$= 4\frac{6889}{19600}$$

$$v = -y_1 - \frac{3x_1^2 + 2ax_1 + b}{2y_1}(u - x_1) = -8\frac{906837}{2744000},$$

Javob. $2P = \left(4\frac{6889}{19600};\ -8\frac{906837}{2744000}\right).$

Demak, elliptik egri chiziqda yotuvchi kamida bitta ratsional nuqtani bilganimiz holda qolgan istalganicha ratsional nuqtalarni topish imkoniyati

mavjud. Tanlab olingan elliptik egri chiziqda tartibi yetarli katta bo‘lib, bu tartibni aniqlovchi son tub son bo‘lishi samarali amaliy tadbiqlarga asos bo‘ladigan ratsional koordinatali nuqtalarni toppish masalasi yechimi muhimdir.

$$y^2 mod p = (x^3 + ax + b) mod p$$

ISSN 2181-3187

Bu yerda *$(4a^3+27b^2)$ modp≠0, x,y,a,b* – maydonda aniqlangan elliptik egri chiziq, p-tub son.

Aniqlangan maydonda nuqtalarni qo'shish va ikkilantirish:

Nuqtalarni qo'shish	Nuqtalarni ikkilantirish
$x_R = (\lambda^2 - x_p - x_Q) modp$ $y_R = (\lambda(x_p - x_R) - y_p) modp$ $\lambda = \frac{y_Q - y_P}{x_Q - x_P} modp$	$x_R = (\lambda^2 - 2x_P) modp$ $y_R = (\lambda(x_P - x_R) - y_P) modp$ $\lambda = \frac{3x_P^2 + a}{2y_P} modp$

Elliptik egri chiziqlarga asoslangan shifrlash algoritmlari.

$\boldsymbol{E_p(a,b), p} - tub\ son.$ C – E EEChdagi iyotiyoriy nuqta	
Alisa	**Bob**
α (α <p) va E EECHda A nuqta olinadi. $A_1 = \alpha(C + A),\ A_2 = \alpha A$ α, A – maxfiy kalit A_1, A_2 – ochiq kalit $A_b = \alpha * B_2$ – Bob uchun Alisaning maxsus ochiq kaliti	β (β<p) va E EECHda B nuqta olinadi. $B_1 = \beta(C + B),\ B_2 = \beta B$ β, B – maxfiy kalit B_1, B_2 – ochiq kalit $B_a = \beta * A_2$ – Alisa uchun Bobning maxsus ochiq kaliti
Deshifrlash	**Shifrlash**
$M = E_2 - (\alpha E_1 + \alpha B_1 + B_a)$	$E_1 = \gamma * C;$ $E_2 = M + (\beta + \gamma)A_1 - \gamma A_2 + A_b$ γ – matnning har bir bayti uchun ixtiyoriy tanlanadi

ISSN 2181-3187

Misol

$y^2 = x^2 + 2x + 9 \quad y^2 = (x^2 + 2x + 9)\text{mod}37 \quad E_{37}(2,9)$

{ ∞,(5,25), (1,30), (21,32), (7,25), (25,12), (4,28), (0,34), (16,17), (15,26), (27,32), (9,4),(2,24), (26,5), (33,14), (11,17), (31,22), (13,30), (35,21), (23,7), (10,17), (29,6), (29,31), (10,20), (23,30), (35,16),(13,7), (31,15), (11,20), (33,23), (26,32),(2,13), (9,33), (27,5), (15,11), (16,20), (0,3), (4,9), (25,25), (7,12), (21,5), (1,7), (5,12), }

Kalit generatsiyasi

$Alice \qquad C = (9,4) \qquad$ Bob

$\alpha = 5,\ \text{A} = (10,20) \qquad \beta = 7, \text{B} = (11,20)$

$A_1 = \alpha(C + A) = 5[(9,4) + (10,20)] = (1,7) \qquad B_1 = \beta(C + B) = (11,17)$

$A_2 = \alpha * A = (33,23) \qquad B_2 = \beta * B = (23,30)$

$A_b = \alpha * B_2 = (15,11) \qquad B_a = \beta * A_2 = (2,13)$

Shifrlash / Deshifrlash

$M = attack$ – ochiq matn $\qquad \alpha = (5,25)$

*	a	b	c	d	e	f	g	h
∞	(5,25)	(1,30)	(21,32)	(7,25)	(25,12)	(4,28)	(0,34)	(16,17)
I	j	k	l	m	n	o	p	q
(15,26)	(27,32)	(9,4)	(2,24)	(26,5)	(33,14)	(11,17)	(31,22)	(13,30)
r	s	t	u	v	w	x	y	z
(35,21)	(23,7)	(10,17)	(29,6)	(29,31)	(10,20)	(23,30)	(35,16)	(13,7)

1	2	3	4	5	6	7	8	9	0
(31,15)	(11,20)	(33,23)	(26,32)	(2,13)	(9,33)	(27,5)	(15,11)	(16,20)	(0,3)
#	@	!	&	$	%				
(4,9)	(25,25)	(7,12)	(21,5)	(1,7)	(5,12)				

Shifrlash

$\gamma = 8,\ \alpha$ – xarfi uchun

$E_1 = \gamma * C = (1,30) = b\ (jadval\ bo'yicha) \qquad (b,5)$

$E_2 = \text{M} + (\beta + \gamma)A_1 - \gamma A_2 + A_b = (2,13) = 5\ (jadval\ bo'yicha)$

$\gamma = 12,\ t$ – xarfi uchun, $\text{t} = (10,17)$

$E_1 = \gamma * C = (21,32) = c\ (jadval\ bo'yicha) \qquad (c,1)$

$E_2 = \text{M} * (\beta + \gamma)A_1 - \gamma A_2 + A_b = (2,24) = 1(jadval\ bo'yicha)$

Shifr matn = {b, 5; c, 1; #, j; v, b; b, p; @, f}

ISSN 2181-3187

Deshifrlash

$\{b,5;\ c,1;\ \#,j;\ v,b;\ b,p;\ @,f\} =$

$\{(1{,}30),(2{,}13),(21{,}32),(2{,}24),(4{,}9),(27{,}32),(29{,}31),(1{,}30),(1{,}30),(31{,}22),(25{,}25),(4{,}28)\}$

$$M = E_2 - (E_1 + B_1 + B_A) = (5{,}25) = a$$

$$M = E_2 - (E_1 + B_1 + B_A) = (10{,}17) = t$$

$$M = E_2 - (E_1 + B_1 + B_A) = (10{,}17) = t$$

$$M = E_2 - (E_1 + B_1 + B_A) = (5{,}25) = a$$

$$M = E_2 - (E_1 + B_1 + B_A) = (21{,}32) = c$$

$$M = E_2 - (E_1 + B_1 + B_A) = (9{,}4) = k$$

Ushbu bo'limda biz eksperimental natijalarimizning oqibatlari va ularning elliptik egri kriptografiya va sonlar nazariyasi bilan bog'liqligini muhokama qilamiz. Biz ish vaqti, xotiradan foydalanish va amalga oshirish qulayligi kabi omillarni hisobga olgan holda turli xil kodlash texnikasi o'rtasidagi kelishuvlarni tahlil qilamiz. Shuningdek, biz nuqtalarni hisoblash algoritmlari samaradorligini yanada oshirish uchun potentsial optimallashtirish va parallellashtirish strategiyalarini o'rganamiz.

Xulosa:

Bizning tadqiqotimiz elliptik egri chiziqlardagi nuqtalarni hisoblash muammosini hal qilishda kodlash texnikasining muhim rolini ta'kidlaydi. Biz kodlash strategiyasini tanlash algoritmlarning samaradorligiga sezilarli ta'sir ko'rsatishi va kriptografik ilovalar uchun potentsial ta'sir ko'rsatishi mumkinligini ko'rsatdik. Soha rivojlanishda davom etar ekan, kelajakdagi tadqiqotlar yangi kodlash usullarini ishlab chiqish va elliptik egri kriptografiya va sonlar nazariyasini yanada rivojlantirish uchun mavjudlarini optimallashtirishga qaratilishi mumkin.

Kelajakdagi tadqiqotlar uchun takliflar: Elliptik egri bilan bog'liq muammolarni kodlash texnikasi sohasida kelajakdagi tadqiqotlar uchun bir nechta yo'nalishlarni taklif qilamiz. Bularga quyidagilar kiradi:

- Nuqtalarni hisoblash algoritmlari samaradorligini yanada oshirishi mumkin bo'lgan yangi kodlash usullarini o'rganish.

-Elliptik egri diskret logarifm muammosi kabi elliptik egri bilan bog'liq boshqa masalalarda kodlash strategiyalarini qo'llashni o'rganish.

-Real vaqtda dasturlar uchun kodlashning afzalliklaridan foydalanish uchun apparat tezlatgichlari va parallelizatsiya texnikasini ishlab chiqish.

- Elliptik egri chiziqlarga asoslangan kriptografik tizimlarda turli xil kodlash tanlovlarining xavfsizlik oqibatlarini o'rganish.

Ushbu tadqiqot yo'nalishlariga murojaat qilib, biz elliptik egri chiziqlardagi murakkab muammolarni hal qilishda kodlash texnikasining rolini tushunishni davom

ISSN 2181-3187

ettirishimiz mumkin, natijada yanada samarali va xavfsiz kriptografik echimlarga olib keladi.

Foydalanilgan adabiyotlar:

1. U.R.Xamdamov, Dj.B.Sultanov, S.S.Parsiyev, U.M.Abdullayev Operatsion tizimlar. (O‘quv qo‘llanma)
2. Бабаш А.В., Шанкин Г.П. История криптографии. Часть I. – Москва: Лори Гелиос АРВ, 2002. – 240 с.
3. Бабаш А.В., Шанкин Г.П., Криптография – Москва: Лори Гелиос АРВ, 2002. – 512 с.