ELLIPTIK EGRI CHIZIQLAR KRIPTOGRAFIYASI

Shahriyorov Ikrom Ibrohim o'g'li
Mirzo Ulug'bek nomidagi O'zbekiston Milliy Universiteti
"Amaliy matematika va inkellektual texnologiyalar" fakulteti
"Kripotografiya va kriptoanaliz" yo'nalishi 2-bosqich magistranti.
E-mail: shahriyorovikrom6@gmail.com

ANNOTATSIYA

Elliptik egri chiziqlar kriptografiyasi kriptografiyaning mustaqil bir bo'limi hisoblanib, chekli maydonlardagi elliptik egri chiziqlarga asoslangan nosimmetrik kriptotizimlarni o'rganadi.

Kalit so'zlar: Elliptik egri chiziqlar, shifrlash, shifrni ochish, algoritm, logarifmlash, yopiq kalit.

Ko'plab oshkora kalitli kriptografik mahsulotlar va standartlar deyarli an'anaviy mavqega erishgan RSA va El Gamal algoritmlariga asoslangan. So'nggi vaqtlarda kriptotahlil usullarining va hisoblash texnikasining keskin rivojlanishi tizimlarning ishonchli himoyasi uchun kalit bitlari sonining ham katta bo'lishiga olib keldi, bu esa an'anaviy tizimlarni qo'llovchi tizimlar ilovasini yuklanish vaqtining ortishiga olib keldi. Bu o'z navbatida katta tranzaksiyalarni himoyalash talab etiladigan, elektron tijoratga ixtisoslashgan aloqa tugunlarida ko'plab muammolarni keltirib chiqardi. Shu bois an'anaviy mavqega erishgan tizimlarga raqib bo'lgan elliptik egri chiziqlarga asoslangan kriptografiya vujudga keldi.

Elliptik egri chiziqlar kriptografiyasi — kriptografiyaning mustaqil bir bo'limi hisoblanib, chekli maydonlardagi elliptik egri chiziqlarga asoslangan nosimmetrik kriptotizimlarni o'rganadi. Elliptik egri chiziqlar kriptografiyasining asosiy afzalligi hozirgi kungachaelliptik egri chiziqlardagi nuqtalar gruppasini diskret logarifmlash

masalasi asosida subeksponensial algoritmlarni echishga qaratilgan muammoning aniqlanmaganligi hisoblanadi.

Kriptotizimlarni yaratishda elliptik egri chiziqlardan foydalanish bir-biridan mustaqil ravishda Nil Koblis va Viktor Millerlartomonidan 1985 yilda tavsiya etilgan.

Nosimmetrik kriptotizimlar kriptobardoshligi bir qator matematikmasalalarning echish murakkabligiga asoslangan. Ilk ochiq kalitli kriptotizim, ya'ni algoritm RSAning kriptobardoshligi murakkab sonlarni tub ko'paytuvchilarga ajratish muammosiga asoslanganligidadir. Elliptik egri chiziqlarda xuddi shu kriptobardoshlikda RSAga nisbatan kalit o'lchami qisqa bo'ladi, bu ma'lumotni saqlash va uzatishda sezilarli darajada sarfning kamayishiga olib keladi.

Misol uchun RSA-2005 konferensiyasida Milliy xavfsizlik agentligi –Suite B‖ ni yaratishda faqat elliptik egri chiziqli algoritmlardan foydalanilganligini bayon qilgan.

Shunday qilib, elliptik egri chiziqlarga asoslangan kriptografik tizimlarning an'anaviy tizimlarga nisbatan afzalligi, ularda foydalaniladigan kalit uzunligi razryadi kichik bo'lganda ham, ekvivalent himoya bilan ta'minlashidadir. Bu esa qabul qiluvchi va uzatuvchi moslama protsessorlarining yuklanish vaqtini kamaytiradi.

Elliptik egri chiziqlar quyidagi ko'rinishdagi tenglamalar yordamida beriladi:

$$y^2 + axy + by = x^3 + cx^2 + dx + g,$$

bunda a, b, c, d butun sonlar.

Elliptik egri chiziq O deb belgilangan maxsus bo'lmagan (cheksizlikdagi nuqta, nol element) elementni o'z ichiga oladi.

Elliptik egri chiziq ta'rifidan agar uchta nuqta bir to'g'ri chiziqda ètsa, ularning yig'indisi O ekanligi kelib chiqadi. Bu ta'rifdan elliptik egri chiziq nuqtalarining qo'shishni quyidagi qoidalari kelib chiqadi:

1. Qo'shishda O nol elementi sifatida qatnashadi, ya'ni $O=-O$ bo'lib, elliptik egri chiziqning ixtiyoriy nuqtasi uchun $R+O=R$.

2. Vertikal chiziq elliptik egri chiziqni bir xil x absissali ikkita nuqtada kesib o'tadi. Bu chiziq egri chiziqni cheksizlik nuqtasida ham kesib o'tadi. Shuning uchun

$P_1+P_2+O=O$ va $P_1=-P_2$, bunda $P_1=(x,y)$, $P_2=(x,-y)$. "Manfiy" ishorali nuqta bu x koordinatasi xuddi o'sha qiymatga,u koordinatasi esa ishorasi bo'yicha qarama-qarshi qiymatga ega bo'lgan nuqtadir.

3. Turli x koordinatali Q va R nuqtalarni qo'shish uchun, bu ikki nuqta orqali to'g'ri chiziq o'tkaziladi va bu to'g'ri chiziqning elliptik egri chiziq bilan kesishgan uchinchi nuqtasi P_1 topiladi. Agar bu nuqtalarning birortasida to'g'ri chiziq elliptik egri chiziqqa urinma bo'lmaydigan bo'lsa, u holda bu to'g'ri chiziqning EECh bilan faqat bitta kesishish nuqtasi topiladi. Bunda $Q + R = -P_1$.

4. Q nuqtani ikkilantirish uchun Q nuqtadan urinma o'tkazish kerak va boshqa S kesishish nuqtasini topish kerak. Bunda $Q + Q = 2Q = -S$.

Qo'shishning yuqorida keltirilgan xossalari qo'shishning barcha oddiy xossalariga, masalan, kommutativlik va assotsiativlik qonunlariga bo'ysunadi.

Elliptik egri chiziqning R nuqtasini k songa ko'paytirish R nuqtaning k ta nusxasining yig'indisi shaklida aniqlangan. $2P = P + P$, $3P = P + P + P$ va hokazo.

r - tub sonli modul bo'yicha elliptik gruppa kriptografiyada alohida qiziqish kasb etadi. Bunday gruppa quyidagicha aniqlanadi. Ikkita manfiy bo'lmagan va p dan kichik bo'lgan butun a va b sonlar tanlanadi, bunda

$$4a^3 \square 27b^2 \bmod p \square 0$$

Shart bajarilsin, u holda $E_p(a,b)$ r modul bo'yicha elliptik gruppani bildiradi. Bu gruppaning elementlari manfiy bo'lmagan r dankichik (x,u) sonlarjuftligi bo'lib, cheksizlikdagi O nuqta bilan $y^2 \square (x^3 \square ax \square b)(\bmod p)$ shartni qanoatlantiradi.

Elliptik gruppa uchun $(0,0)$ dan (r,r) gacha bo'lgan, kvadrati manfiy son bo'lmagan r modul bo'yicha tenglamani qanoatlantiradigan faqat butun qiymatlar qaraladi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI: (REFERENCES)

1. Akbarov D. E. "Axborot xavfsizligini ta'minlashning kriptografik usullari va ularning qo'llanilishi" – Toshkent, 2008

2. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии.[уточнить]

3. Б. А. Фороузан. Схема цифровой подписи Эль-Гамаля // Управление ключами шифрования и безопасность сети / Пер. А. Н. Берлин. — Курс лекций.

4. http://www.hozir.org/el-gamal-shifrlash-algoritmi.html