ELLIPTIK EGRI CHIZIQLAR KRIPTOGRAFIYASINING UMUMIY FUNKSIONAL AHAMIYATI

Toshboyeva Feruza To`lqin qizi

Toshkent davlat iqtisodiyot universiteti

So`nggi yillarda ochiq kalitli kriptotizimlarning paydo bo`lishi rivojlanayotgan axborot texnologiyalari bilan birgalikda matematikaning bir nechta yangi sohalari ham ochildi.Zamonaviy kriptografiyaning eng istiqbolli vositalaridan biri elliptik egri chiziqlardan foydalanish kirib kela boshladi.Bu nafaqat matematiklar orasida, balki yangi kriptotizimlar bilan shug`ullanuvchi muhandislar, axborot xavfsizligiga ma’sul shaxslar, idora xodimlari va kompyuter olimlari tomonidan ham yangi qiziqish uyg`otdi.

Kriptografiyada elliptik egri chiziqlar(boshqacha qilib aytganda elliptik egri chiziqlarning matematik xususiyatlariga asoslangan shifrlash usuli) dan foydalanishning ko`plab samarali va qiziqarli tomonlari, masalan, butun sonlarni faktorizatsiya qilish, elliptic egri chiziqlardagi nuqtalarni topish kabilar jalb qilishi mumkin.

Elliptik egri chiziqlarni birinchi bo`lib Koblits(1987) va Miller(1986) taklif qilgan[1].Elliptik egri chiziqqa asoslangan kriptotizimlar avvaliga mobil elektron biznes xavfsizligi uchun ishlab chiqilgan bo`lib keyinchalik esa ko`plab faoliyatlarda qo`llab quvvatlandi.

Elliptik kriptografiyaga alohida qiziqish quyidagi sabablar bilan bog‘liq:

- birinchidan, 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 algoritmlarning yuzaga kelishi.Elliptik egri chiziqlar gruppasida esa silliqlik tushunchasi nuqtalarga tegishli bo‘lib, tezkor kriptotahlillash algoritmlarini tuzish imkoniyatini bermaydi;

- ikkinchidan, EECh gruppasida nisbatan qisqa kalit uzunligi asosida kriptotizimlar ishlab chiqarish imkoniyati mavjudligi. Bular simsiz kommunikasiyalarda va resurs

cheklangan hollarda (smartkartalar, mobil qurilmalar) asosiy hisoblanadi. Masalan, 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 [5-7].

Elliptik egri chiziqlar kubik egri chiziqlarning turiga mansub bo`lib, uning yechimlari topologic jihatdan torusga ekvivalent bo`lgan fazo mintaqasi bilan chegaralangan.Umumiy holatda kubik egri chiziqlarning dastlabki ko`rinishi quyidagicha bo`ladi:

$$Ax^3 + Bx^2y + Cxy^2 + Dy^3 + Ex^2 + Fxy + Gx^2 + Hx + Iy + J = 0$$

Elliptik egri chiziq uning xususiy ko`rinishi bo`lgani uchun quyidagicha yozish mumkin:

$y^2 = x^3 + ax + b$[2]

Elliptik egri chiziqqa asoslangan Diffie-Hellman algoritmi quyidagi bosqichlarda amalga oshiriladi:

Ijrochilar (X va Y) elliptik egri chiziq E va modul p ustida ishlash uchun kelishishadi.X va Y o'zining maxfiy kalitlarini (a va b) tanlaydi, ularning har biri [1, p-1] oralig'ida bo'lishi kerak.X va Y o'zining umumiy kalitlarini hisoblash uchun elliptik egri chiziq ustida nuqta ko'paytirish amalini ishlatadi: X = a * G va Y = b * G, G elliptik egri chiziqning nuqtasi.X va Y o'zining maxfiy kalitlari va qabul qilgan umumiy kalitlarini ishlatib, o'zaro kalitni hisoblaydilar: K_X = a * B va K_Y = b * A. Bu yerda, K_X va K_Y bir xil bo'lishi kerak.

Diffie-Hellman kriptografik protokoli, ikki tomondoshlar o`rtasidagi xavfsiz kalit almashishni ta'minlovchi bir usul hisoblanadi. Bu protokol, maxfiy kalit kriptografisidan foydalanib, ikki tomon orasida umumiy kalit hosil qilishni ta'minlaydi.Diffie-Hellman protokoli, har bir tomonning birer gizli va ochiq kaliti bor. Har bir tomon o'zining ochiq kalitini boshqa tomon bilan almashadi va so'ng maxfiy kalitlarini ishlatib umumiy kalitni hosil qiladi. Ushbu umumiy kalit keyingi simmetrik kalitli shifrlash algoritmalarida ishlatilishi mumkin.Diffie-Hellman

protokolining xavfsizligi, modulyar arifmetik hisoblashining matematikaviy xususiyatlaridan kelib chiqadi. Ushbu xususiyatlar saldirlarga qarshi kalitni baxtli qirg'ishlariga qarshi himoya qiladi.Lekin, Diffie-Hellman protokoli xavfsizligi boshqa faktorlar bilan ham tasir etilishi mumkin, masalan, amaliy qo'llanish va tuzilish xatoliklari kabi. Shuning uchun, protokolni to'g'ri shaklda qo'llash va tuzilish juda muhimdir. Qulay keladigan kalit boshqaruvining, kalit uzunligining va boshqa xavfsizlik chora-tadbirlari kabi yaxshi kriptografik amallarni qo'llash ham muhimmu.Natijada, Diffie-Hellman protokoli to'g'ri tarzda qo'llanilganda, xavfsiz kalit almashishni ta'minlash uchun samaraliusul hisoblanadi. Lekin, amaliy qo'llanish va tuzilish xatoliklari kabi boshqa faktorlar ham hisobga olinishi kerak.

Elliptik egri chiziqqa asoslangan shifrlash va deshifrlash algoritmlari anchagina yuqori darajada xavfsizlikka ega bo`lib u o`zining maxfiylik kalitlari qisqaligi bilan ancha samarali hisoblanadi.Bundan tashqari kalitlar orasidagi o`zaro almashtirishlar osonlik bilan amalga oshiriladi.Elliptik egri chiziqqa asoslangan shifrlash hozirgi kunda juda ko`p faoliyatlarda foydalanilmoqda, shuningdek mobil qurilmalarda axborot xavfsizligida ham.Har bir narsaning afzalligi va kamchiligi bo`lgani kabi EECH da nuqtani to`g`ri toppish va hisoblash muammosi mavjud.

Foydalanilgan adabiyotlar

1.Elliptic curves and their applications to cryptography.Andreas Enge,Universitat Augsburg, Germany

2.Kriptografiyaning matematik asoslari. O‘quv qo‘llanma D.Y.Akbarov, P.F.Xasanov, X.P.Xasanov, O.P.Axmedova, I.U.Xolimtayeva Toshkent 2018.

3. Koblitz, Neal. Elliptic curve cryptosystems. Mathematics of Computation 48 (1987), 203-209. [One of the original articles that proposed the use of elliptic curves for cryptography. The other is by Victor Miller.

4. Yusupova, S. M. "ELLIPTIK EGRI CHIZIQQA ASOSLANGAN KRIPTOTIZIMLAR."INNOVATION IN THE MODERN EDUCATION SYSTEM3.30 (2023): 533-541.

5. Хасанов Х.П. Криптографические системы на базе эллиптических кривых с параметром Ахборот-коммуникациялар: Тармоқлар – Технологиялар – Ечимлар. – Т.: №4, 2008.

6. Алгоритмические основы эллиптической криптографии / Болотов А.А. Гашков С.Б. Фролов А.В., Часовских А.А. – Москва МЭИ, 2000. – 100 с.

7. Элементарное введение в эллиптическую криптографию: алгебраические и алгоритмические основы / Болотов А.А. Гашков С.Б. Фролов А.В., Часовских А.А. – Москва МЭИ, 2006. – 328 с.