ELLIPTIK EGRI CHIZIQLAR ASOSIDA SHIFRLASH ALGORITIMLARINING SAMARADORLIGINI OSHIRISH

Sattorov Asadullo Shonazar o‘g‘li
Xorazm viloyati Urganch shahri Urganch raqamli texnoligiyalar texnikumi maxsus fan o‘qituvchisi
E-mail: asadullosattarov10@gmail.com

Annotatsiya: *Ushbu tezisda elliptik egri chiziqlar (ECC) asosidagi shifrlash algoritimlarining samaradorligini oshirish yo‘nalishlari, uning afzalliklari va amaliy qo‘llanilish imkoniyatlari tahlil qilinadi. ECCning an’anaviy kriptotizimlardan ustun jihatlari, optimallashtirish texnikalari hamda zamonaviy tahdidlarga nisbatan barqarorligini ta’minlash mexanizmlari yoritilgan.*

Kalit so‘zlar: *ECC, elliptik egri chiziqlar, kriptografiya, RSA, skalyar ko‘paytirish, Curv e25519, Montgomery Ladder, post-kvant kriptografiya.*

Kirish

Elliptik egri chiziqlar kriptografiyasi (ECC) zamonaviy ochiq kalitli kriptotizimlarning eng samarali yo‘nalishlaridan biri hisoblanadi. ECCning asosiy ustunligi — kichik bitli kalitlar orqali yuqori xavfsizlik darajasini ta’minlashidir. U resurslar cheklangan qurilmalarda — mobil telefonlar, IoT tizimlari, aqlli sensorlar, to‘lov qurilmalari va davlat xizmatlari tizimlarida keng qo‘llanilmoqda.

Elliptik egri chiziqlar (ECC — Elliptic Curve Cryptography) zamonaviy kriptografik tizimlarning eng samarali va xavfsiz yo‘nalishlaridan biri hisoblanadi. ECCning asosiy ustunligi — kichik kalitlar uzunligida yuqori xavfsizlik darajasini ta’minlashi, hisoblash murakkabligining pastligi va resurslar cheklangan muhitlarda samarali ishlashidir. Aynan shu xususiyatlar ECCni mobil qurilmalar, IoT tizimlari, aqlli sensorlar, moliyaviy tranzaksiyalar va hukumat darajasidagi axborot almashinuvi jarayonlarida keng qo‘llanilishiga sabab bo‘lmoqda.

Eccning afzalliklari

An’anaviy ochiq kalitli kriptotizimlardan biri bo‘lgan RSA algoritmi xavfsizlik darajasini oshirish uchun juda katta bitli kalitlarni talab qiladi. Masalan, 2048-bitli RSA bilan teng xavfsizlikni ECC atigi 224–256 bitli kalit orqali ta’minlay oladi. Bu esa ma’lumotni shifrlash tezligini oshiradi, tarmoq trafigini kamaytiradi, saqlash uchun zarur bo‘lgan xotira hajmini optimallashtiradi va energiya sarfini sezilarli darajada pasaytiradi. Shuning uchun ECC resurslar cheklangan tizimlar uchun eng optimal yechimlardan biri sifatida qaraladi.

Samaradorlikni oshirish texnik yo‘nalishlari

Elliptik egri chiziqlar asosida kriptografiyani samaradorligini oshirishda bir nechta texnik yo‘nalishlar mavjud. Ulardan biri — kalit generatsiyasi va nuqtalar arifmetikasini optimallashtirishdir. Nuqtalarni qo‘shish va skalyar ko‘paytirish amallari ECC algoritmlarining eng resurs talab qiladigan jarayonlari hisoblanadi. Bu amallarni Montgomery, Edwards yoki Twisted Edwards kabi tez ishlovchi egriliklarda bajarish natijasida algoritmning umumiy ishlash tezligi oshiriladi. Shuningdek, wNAF, Sliding Window, Montgomery Ladder kabi optimallashtirilgan skalyar ko‘paytirish usullari qo‘llanilganda hisoblash vaqtini sezilarli kamaytirish mumkin.

ECCning samaradorligini oshirishning yana bir yo‘nalishi — himoya mexanizmlarini kuchaytirishdir. Yon-kanal hujumlari (Side-Channel Attacks), vaqt bo‘yicha tahlil (Timing Attacks) va differensial quvvat tahlili (DPA) kabi hujumlar ECCga bevosita tahdid solishi mumkin. Ularga qarshi barqaror ishlash uchun randomizatsiya, nuqtalarni maskalash, constant-time arifmetika va kalitlarni qayta ishlab chiqish kabi himoya strategiyalaridan foydalaniladi. Bu yondashuvlar ECCni nafaqat tezkor, balki amaliy jihatdan xavfsiz kriptotizimga aylantiradi.

Hozirgi tendensiyalar va amaliyot

Bugungi kunda blokcheyn, elektron hukumat, elektron imzo, to‘lov tizimlari va 5G infratuzilmasida ECCning ulushi ortib bormoqda. Ayniqsa, kvant hisoblash tahdidlari fonida ECCning yangi avlod variantlari — post-kvant ECC modifikatsiyalari bo‘yicha ilmiy tadqiqotlar kuchaymoqda. Hozirda standartlashtirilgan Curve25519, Curve448 kabi egriliklar xavfsizlik va samaradorlikning eng yaxshi muvozanatini taqdim etadi, shuning uchun ularning amaliy qo‘llanilishi kengaymoqda.

Yuqoridagilardan kelib chiqib, elliptik egri chiziqlar asosidagi kriptografiya zamonaviy axborot xavfsizligi tizimlarida yuqori samaradorlik va ishonchlilikni ta’minlay oladigan eng istiqbolli yo‘nalishlardan biri ekanligi isbotlanadi. ECCning matematik asoslari, optimallashtirilgan arifmetikasi, kuchli xavfsizlik modeli va kichik kalitlari uni raqamli xavfsizlik infratuzilmasining asosiy bo‘g‘iniga aylantirmoqda.

Foydalanilgan adabiyotlar

1. Hankerson, D., Menezes, A., & Vanstone, S. Guide to Elliptic Curve Cryptography. Springer, 2004.

2.Koblitz, N. Elliptic Curve Cryptosystems. Mathematics of Computation, 1987.

3.Miller, V. S. Use of Elliptic Curves in Cryptography. Advances in Cryptology — CRYPTO ’85, Springer, 1986.

4.Bernstein, D. J. Curve25519: New Diffie–Hellman Speed Records. Public Key Cryptography (PKC), 2006.