ELLIPTIK EGRI CHIZIQLAR KRIPTOGRAFIYASINING ZAMONAVIY XAVFSIZLIKDAGI ROLI

Toshboyeva Feruza To‘lqin qizi
Toshkent davlat iqtisodiyot universiteti
feruzatoshboyev35@gmail.com

Annotatsiya: Elliptik egri chiziq kriptografiyasi (ECC) zamonaviy kriptografiyadagi eng kuchli va samarali kriptografik usullardan biridir. Maqolada ECC chekli maydon ustidagi elliptik egri chiziqlar, uning xavfsizligida elliptik egri chiziq diskret logarifm muammosi (ECDLP), elliptik egri chiziq Diffi-Xellman (ECDH) kalit almashish protokollari, elliptik egri chiziq kriptografiyasidan foydalanishning ijobiy va salbiy tomonlari va uning zamonaviy xavfsizlikdagi roli haqida batafsil ma’lumot berilgan.

Kalit so‘zlar: Asimmetrik kriptografiya, elliptik egri chiziq kriptografiyasi (ECC), elliptik egri chiziq raqamli imzo algoritmi (ECDSA), elliptik egri chiziq Diffi-Xellman algoritmi (ECDH).

Kirish

Ochiq kalit kriptografiya asosan shifrlash va shifrni ochish uchun matematik hisob-kitoblardan foydalanadi. Ochiq kalitli kriptografiya an’anaviy kriptografiyadan ko‘ra zamonaviyroq bo‘lib, uning xavfsizligi an’anaviy kriptografiyanikiga qaraganda kuchliroqdir, sababi uning kalit hajmi katta va shifrlash/deshifrlash jarayonlari ko‘proq hisoblashni talab qiladi [1]. Biroq, ochiq kalitli kriptografiya an’anaviy kriptografiyaning o‘rnini to‘liq egallamaydi, chunki u juda ko‘p hisob-kitoblarni talab qiladi, shuning uchun uni faqat elektron raqamli imzo va kalitlarni boshqarishda qo‘llash samaralidir.

ECC chekli maydon ustidagi elliptik egri chiziqlar nuqtalarining guruh operatsiyalariga asoslanadi. Uning xavfsizligi elliptik egri chiziq diskret logarifm muammosini (ECDLP) hal qilishning murakkabligiga asoslanadi [2]. Elliptik egri chiziqlar bir nechta maqsadlarda qo‘llaniladi masalan, elliptik egri chiziq kriptografiyasi (ECC), elliptik egri chiziq raqamli imzo algoritmi (ECDSA) va elliptik egri chiziq Diffi-Xellman (ECDH) kalit almashish protokollarida. Elliptik egri chiziq kriptografiyasidan foydalanishning ijobiy va salbiy tomonlari mavjud. Ijobiy va salbiy tomonlarini tushunish uchun uning zamonaviy xavfsizlikdagi rolini o‘rganish va undan foydalanish bo‘yicha asosli qarorlar qabul qilish muhimdir.

ECC RSA kabi ochiq kalitli tizimlar bilan bir xil xavfsizlik darajasiga erisha oladi, shu jumladan qisqaroq kalit uzunliklari, xotirani qisqartirish, o‘tkazish qobiliyatini kamaytirish va tezroq hisoblash imkoniyatlariga ega [3].

Elliptik egri chiziqlarning asosiy matematikasi xavfsizlik uchun mustahkam poydevor yaratadi, yaxshi tanlangan egri chiziq bo‘yicha elliptik egri chiziq diskret logarifm muammosiga (ECDLP) qarshi ma’lum hujumlar yo‘q.

RSA va ECC (elliptik egri chiziq kriptografiyasi) algoritmlari ochiq va shaxsiy kalit juftliklari orqali xavfsiz aloqaning ta’minlaydi, lekin ular buni tubdan boshqacha yo‘llar bilan amalga oshiradilar, bu esa ba’zi muhim farqlarga olib keladi [6,7]. ECC, RSAga qaraganda ancha qisqa kalit uzunliklari bilan bir xil darajadagi xavfsizlikni ta’minlaydi. Bu uning eng katta afzalliklaridan biri hisoblanadi va quyidagi 1-jadvalda turli kriptotizimlarda foydalaniladigan kalit uzunliklari solishtirilgan [8].

1-jadval. Turli kriptotizimlarda kalit uzunliklari solishtirma jadvali

Simmetrik kriptotizimlar (kalit uzunligi, bit)	ECC tizimlari (n uzunligi, bit)	RSA/DSA (modul uzunligi, bit)
56	112	512
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	512	15360

Kriptografiyada eng muhim muammolardan biri bu diskret logarifm muammosi (DLP) hisoblanadi. Klassik guruhlarda bo‘lgani kabi, elliptik egri chiziqlarda ham DLP asosida samarali va xavfsiz kriptotizimlar barpo qilinmoqda. Elliptik egri chiziqlar (ECC) asosida qurilgan tizimlar kichik kalit o‘lchamida yuqori xavfsizlikni ta’minlashi bilan ajralib turadi. Elliptik egri diskret logarifm muammosi (ECDLP) zamonaviy kriptografiyada, ayniqsa elliptik egri chiziqqa asoslangan tizimlarda asos bo'lib xizmat qiladi. Aslini olganda, ECDLP Q=[d]P tenglamadagi d ko‘rsatkichini aniqlashni o‘z ichiga oladi, bu yerda P ma’lum elliptik egri chiziqdagi nuqta va Q xuddi shu egri chiziqdagi boshqa nuqtadir. Bu vazifa hatto nuqtalarning koordinatalarini bilish bilan ham juda qiyin.

Xulosa

Elliptik egri chiziq kriptografiyasi zamonaviy kriptosistemalar uchun mustahkam matematik asos bo‘lib, qisqa kalit uzunliklari bilan yuqori darajadagi xavfsizlikni ta’minlaydi. Amaliy jihatdan ECDH TLS/SSL, VPN va boshqa ko‘plab xavfsizlik protokollarida keng qo‘llanilmoqda. IoT qurilmalari,

mobil ilovalar, blockchain texnologiyalari va post-kvant kriptografiyasi sohalarida ECC ning ahamiyati tobora o‘sib bormoqda.

ECDH protokoli hozirgi va yaqin kelajakda xavfsiz kalit almashishning eng ishonchli va samarali usullaridan biri bo‘lib qolishiga ishonch hosil qilish mumkin. Uni to‘g‘ri amalga oshirish va zamonaviy standartlarga rioya qilish orqali ma’lumotlarning maxfiyligi va xavfsizligini yuqori darajada saqlash mumkin.

FOYDALANILGAN ADABIYOTLAR

1. Kumar, A., Tyagi, S. S., Rana, M., Aggarwal, N., and Bhadana, P. ‘A comparativestudy of public key cryptosystem based on ECC and RSA’. International Journal on Computer Science and Engineering, vol. 35, pp. 1904–1909, 2011.
2. Bao, Jiaxu. “Research on the security of elliptic curve cryptography.” 2022 7th International Conference on Social Sciences and Economic Development (ICSSED 2022). Atlantis Press, 2022.
3. Hankerson, D., Menezes, A., & Vanstone, S. (2004). Guide to Elliptic Curve Cryptography. Springer.
4. Neal Koblitz. Elliptic curve cryptosystems. Mathematics of Computation, 48:203-209, 1987.
5. National Institute of Standards and Technology (2013) Digital Signature Standard (DSS). (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 186-4. https://doi.org/10.6028/NIST.FIPS.186-4
6. C. Paar and J. Pelzl, Understanding Cryptography, Springer-Verlag Berlin Heidelberg, (2010).
7. K. Rabah, Theory and Implementation of Elliptic Curve Cryptography, Journal of Applied Sciences, vol 5(4), 604-633, (2005).
8. L.D. Singh and K.M. Singh, Implementation of Text Encryption using Elliptic Curve Cryptography, Procedia Computer Science vol 54, 73-82, (2015)