ELLIPTIK EGRI CHIZIQLAR KRIPTOGRAFIYASIDA DISKRET LOGARIFM MUAMMOSI VA UNI TADQIQ QILISH

Toshboyeva Feruza To‘lqin qizi

Toshkent davlat iqtisodiyot universiteti “Oliy va amaliy matematika” kafedrasi assistenti

Annotatsiya. *Diskret logarifm muammosi ko'plab kriptografik tizimlarning asosini tashkil qiladi.Ushbu maqolada elliptik egri chiziqlar kriptografiyasida DLP va uni samarali hal qilishning bir nechta usullari tadqiq qilinib yoritib berilgan.Shu bilan birga tahliliy natijalar va xulosa keltirilgan.*

Kalit so‘zlar: *kriptografiya, DLP(dikret logarifm muammosi), algoritm, Shanks (Baby-Step Giant-Step), Pollard’s Rho, MOV, index hisoblash, protokol, egri chiziq nuqtasi, shifrlash, xavfsizlik, raqamli imzo*

KIRISH

Kriptografiya - bu xabarlarning maxfiyligini ta’minlash uchun kompyuter algoritmi bilan ifodalanishi mumkin bo'lgan aqlli matematik tenglamalarni o‘rganadigan rivojlanayotgan soha. Ushbu maqola elliptik egri chiziqlar kriptografiyasida diskret logarifm muammosi bo‘yicha asosiy tadqiqotni taqdim etadi. U elliptik egri chiziq ortidagi matematikani kriptotizimda qo'llanilishiga moslashtiradi. Xulosa qilib aytganda, elliptik egri chiziq 3-darajali ikki o‘zgaruvchan ko‘phaddagi nuqtalarni o‘rganishdir. Egri chiziq chegarali maydon ustida aniqlanganda, qo‘shish amali bilan ta’sir etuvchi nuqtalar to‘plami chekli guruh strukturasini hosil qiladi. Aylanma nuqtalar sifatida ham tanilgan, ular kodlangan xabarlarni ifodalash uchun ishlatiladi. Shifrlash va dekodlash nuqtani bir xil to'plamdagi boshqa nuqtaga aylantiradi. Kontseptual tushunishdan tashqari, muhokamalar elliptik egri chiziqlar kriptotizimning xavfsizligi va samaradorligi masalalariga qaratilgan.

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. Mazkur maqolada ECC dagi DLP ni hal qilishga qaratilgan asosiy algoritmlar – **Shanks (Baby-Step Giant-Step), Pollard’s Rho, Index calculus** va **MOV (Menezes-Okamoto-Vanstone) hujumi** – ko‘rib chiqiladi va ularning samaradorligi taqqoslanadi.

Elliptik egri kriptotizimlari ECDLP (elliptik egri chiziqli diskret logarifm muammosiga asoslangan chekli maydonlar ustidagi elliptik egri kriptografiya (ECC), ularning xavfsizligi uchun nP nuqtasi berilgan musbat sonni topish muammosi, bu yerda P egri chiziqdagi nuqta), kriptografiyaning kuchli tarmog‘i hisoblanadi. Cheklangan sohadagi diskret logarifm (DL) sonlar nazariyasidagi NP-to‘liq muammolardan biri bo‘lib, elliptik egri chiziqlar va kriptografiya kabi bir qancha sohalarda qo'llaniladi. Bu muammo Martin Hellman, Tonelli Shanks, Jon M.Pollard, Adleman kabi bir qancha mualliflar tomonidan ko‘tarilgan. Bundan tashqari, uni hal qilish uchun Pohlig Hellman algoritmi, Baby-Step, Giant-Step algoritmi, Rho-Pollard algoritmi va Index hisoblash algoritmlari kabi ko'plab usullar taklif qilingan. ECC samaradorligi, kuchli xavfsizlik xususiyatlari va autentifikatsiya protokoli dizayni, kalitlarni yaratish protokoli, kalitlarni almashish protokoli, raqamli imzolar, xesh funktsiyalari, bulutli hisoblash, blokcheynlar va Internet texnologiyalari kabi dolzarb sohalarda xavfsizlikni isbotlash kabi qisqaroq kalitlari (kamroq xotira talablari va tezroq maydon arifmetik operatsiyalari) tufayli turli xil xavfsizlik dasturlarida keng qo‘llaniladi [1-3]. Bizning ushbu maqoladagi maqsadimiz chekli maydonlar va uning xavfsizlik dasturlari bo'yicha elliptik egri kriptografiyani (ECC) keng va sinchkovlik bilan o‘rganishni taqdim etish, shuningdek, elliptik egri chiziqdagi arifmetikani va bu egri operatsiyalar kriptografik tizimlarning ishlashini aniqlashda qanchalik muhimligini muhokama qilishdir.

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.

Elliptik egri kriptografiyadagi xavfsizlik ECDLP ni hal qilishning juda murakkabligiga bog'liq. Baby-step Giant-step va Pollard’s rho kabi an’anaviy algoritmlar keng o‘lchamni ta’minlash uchun elliptik egri parametrlari sinchkovlik bilan tanlangan bo‘lsa, bu muammoni samarali hal qilish uchun kurashadi. ECDLP dan foydalanadigan kriptografik tizimlar turli xil zamonaviy xavfsizlik protokollarida, jumladan shifrlash va raqamli imzolar uchun Elliptik Egri Kriptografiya (ECC) keng tarqalgan. Shunga qaramay, ushbu tizimlarning samaradorligi elliptik egri parametrlarni sinchkovlik bilan tanlashga va tegishli kriptografik algoritmlarni to‘g‘ri amalga oshirishga bog‘liqligini ta’kidlash juda muhimdir.

Foydalanilgan adabiyotlar

1. **Koblitz N.** (1987). *Elliptic Curve Cryptosystems*. Mathematics of Computation, **48**(177), 203–209.

2. **Miller V. S.** (1985). *Use of Elliptic Curves in Cryptography*. In *Advances in Cryptology — CRYPTO ’85* (pp. 417–426).

3. **Silverman J. H.** (2009). *The Arithmetic of Elliptic Curves* (2nd ed.). Springer.

4. **Hankerson D., Menezes A., & Vanstone S.** (2004). *Guide to Elliptic Curve Cryptography*.

5. **Pollard J. M.** (1978). *Monte Carlo Methods for Index Computation (mod p)*. Mathematics of Computation, **32**(143), 918–924.

6. **Shanks D.** (1971). *Class number, a theory of factorization and genera*. Proceedings of Symposia in Pure Mathematics, **20**, 415–440.

7. **Menezes A., Okamoto T., & Vanstone S. A.** (1993). *Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field*. IEEE Transactions on Information Theory, **39**(5), 1639–1646.

8. **Washington L. C.** (2008). *Elliptic Curves: Number Theory and Cryptography* (2nd ed.). Chapman and Hall/CRC.

9. **Bernstein D. J., Lange T.** (2007). *Faster Addition and Doubling on Elliptic Curves*. In *Advances in Cryptology — ASIACRYPT 2007*, Springer.

10. **Galbraith S. D.** (2012). *Mathematics of Public Key Cryptography*. Cambridge University Press.

11. **Henri Cohen. A Course in Computational Algebraic Number Theory**

12. **Crandall & Pomerance. Prime Numbers: A Computational Perspective**

13. **Шеннон К.** Теория и связи в секретных системах. Работы по теории информации и кибернетике. – М.: Иностранная лит. 1963. – 243 б.

14. **Washington L. C**. (2008). *Elliptic Curves: Number Theory and Cryptography*.

15. **Menezes A. J.,** Vanstone, S. A., & Oorschot, P. C. (1996). *Handbook of Applied Cryptography*.

16. **F.T.Toshboyeva,** ELLIPTIK EGRI CHIZIQLAR KRIPTOGRAFIYASIDA DISKRET LOGARIFM MUAMMOSI VA UNI TADQIQ QILISH.