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,
elektron pochta: feruzatoshboyeva35@gmail.com.

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

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.

ADABIYOTLAR SHARHI

Elliptik egri kriptografiyasi (EEC) zamonaviy kriptografiyaning eng dolzarb sohalaridan biri bo‘lib, uning xavfsizlik jihatlari ko‘plab ilmiy tadqiqotlar va amaliy dasturlarga asos bo‘lgan.Jumladan, **Koblitz, N. (1987) “**Elliptic Curve Cryptosystems”, **Menezes, A. (1993) “**Elliptic Curve Public Key Cryptosystems”, **Smart, N. (1999), Galbraith, S. (2012), Bernstein, D. (2006) va** Mavlonov, R.X. (2020), Kadirov, A.Sh. (2021), Yuldashev, F.A. (2022) kabi olimlarimiz ko’pgina izlanishlar olib borganlar.Bu sohada izlanishlar, tadqiqotlar bugungi kunda ham davom etmoqda.

TADQIQOT METODOLOGIYASI

Ushbu maqolani yoritishda O‘zbekiston Respublikasi tomonidan sohaga doir qabul qilingan qarorlar, olimlarning adabiyotlari, ilmiy tadqiqot ishlari hamda yurtimiz doirasida ushbu sohaga aloqador jarayonlar, amaliyotlar analiz va sintez qilgan holda tadqiq etildi.

ASOSIY QISM

1. Elliptik egri chiziqlarda DLP ta’rifi

Berilgan elliptik egri chiziq E ustida aniqlangan va P — egri chiziqdagi generator nuqta bo‘lsin. Agar Q∈⟨P⟩ bo‘lsa, ya’ni Q=kP, bu yerda k — noma’lum butun son.DLP quyidagicha ifodalanadi:

Q=kP

Bu muammo “qiyin” deb hisoblanadi va ECC asosidagi kriptotizimlarning asosidir.

2. Shanks (Baby-Step Giant-Step) algoritmi

1. Prinsipi: Ushbu algoritm kuchli xotira evaziga DLP ni hal qilishni tezlashtiradi.
2. Ishlash tartibi:
1. $M=\sqrt{n}$ deb belgilaymiz, bu yerda n – guruhning tartibi.
2. P nuqtaning jP ko‘rinishidagi m ta “baby-step” hosil qilinadi.
3. So‘ngra Q−imP kabi “giant-step” lar orqali moslik topiladi.
3. Murakkabligi:

- Vaqt: $O(\sqrt{n})$
- Xotira: $O(\sqrt{n})$

---

3. Pollard’s Rho algoritmi

1. Prinsipi: Bu usul tasodifiy yurishlar orqali kolliziya (ikki xil ifodalanish) topishga asoslangan.
2. Afzalliklari:
- Xotira jihatdan tejamli: faqat bir nechta nuqtani saqlaydi.
- Parallel ishlash imkoniyati mavjud.
3. Murakkabligi:
- Vaqt: $O(\sqrt{n})$
- Xotira: O(1)

4. MOV hujumi (Menezes-Okamoto-Vanstone)

1. Prinsipi: DLP ni ECC dan ketma-ket juftliklar orqali oxir-oqibat oddiy ko‘paytma guruhiga o‘tkazadi.
2. Chegaralari:
- Faqat maxsus turlaridagi egri chiziqlarda ishlaydi (masalan, past embedding darajali egri chiziqlar).
- Supersingular egri chiziqlar ko‘pincha MOV hujumiga nisbatan zaif.
3. Murakkabligi:
- Vaqt: $O(\sqrt{n})$, lekin ko‘pincha qo‘llanilishi cheklangan.

4. Algoritmlar taqqoslanishi

Algoritm	Vaqt murakkabligi	Xotira talabi	Amaliyligi	Cheklovlar
Shanks	$O(\sqrt{n})$	$O(\sqrt{n})$	Tez, lekin xotiraga talab katta	Xotira cheklovli tizimlarda mos emas
Pollard's Rho	$O(\sqrt{n})$	O(1)	Juda samarali va moslashuvchan	Sekinroq bo‘lishi mumkin
MOV hujumi	$O(\sqrt{n})$	O‘rtacha	Faqat ayrim egri chiziqlarda ishlaydi	Hujum faqat past embeddingda mumkin

Index Calculus algoritmi - bu diskret logarifm muammosini hal qilish uchun ishlatiladigan matematik algoritmdir. Ushbu algoritm katta tub maydonlar yoki sonlar guruhi ustida diskret logarifm hisoblashni tezlashtirishga yordam beradi.

Index Calculus algoritmining asosiy prinsiplari

1. Faktorizatsiya usuli
   - Algoritm berilgan tub sonlar ustida oddiy elementlar to‘plamini yaratadi.
   - Har bir element faktorizatsiya qilingan ko‘rinishda yoziladi.
2. Chiziqli tenglamalar tizimi hosil qilish
   - Diskret logarifmlarni hisoblash uchun faktorizatsiya natijasida hosil bo‘lgan chiziqli tenglamalar yechiladi.
   - Bunda matritsalar va algebraik metodlar qo‘llaniladi.
3. **Gauss usuli orqali yechim topish**
   - Matritsa asosida **Gauss eliminatsiya usuli** yordamida aniq natijaga erishiladi.
   - Ushbu usul orqali **diskret logarifm** tez hisoblanadi.

Kriptografiyaga ta’siri

- **RSA va ECC tizimlariga hujum qilish** Index Calculus algoritmi **katta maydonlardagi** diskret logarifmlarni tez hisoblashga yordam beradi, bu esa ba’zi **kriptografik tizimlarga tahdid** solishi mumkin.
- **Xavfsizlik tekshiruvi** Ushbu algoritm **ECC va RSA sistemalarining mustahkamligini sinash** uchun qo‘llaniladi.
- **Kriptografik protokollarni optimallashtirish** ba’zi **zamonaviy shifrlash tizimlarida** hisoblash jarayonlarini tezlashtirish uchun ishlatiladi[11-12].

Index Calculus algoritmi **diskret logarifm muammosini hal qilishning eng samarali usullaridan biri** bo‘lib, **katta sonlar bilan tezkor ishlash** imkonini beradi. Index calculusni elliptik egri chiziqlarga to‘g‘ridan-to‘g‘ri qo‘llab bo‘lmasada, uni modifikatsiyalash orqali ba’zi hollarda qo‘llab samarali yechimlar olish mumkin.Bu masala yuzasidan ilmiy ishlar, tadqiqotlar olib borilmoqda.

XULOSA

Elliptik egri chiziqlar kriptografiyasida diskret logarifm muammosi (DLM) zamonaviy kriptotizimlarning xavfsizligini ta’minlovchi asosiy matematik

muammolardan biri hisoblanadi hamda diskret logarifm muammosi ECC xavfsizligining asosidir. Ushbu muammo hisoblash jihatdan juda murakkab bo‘lib, hozirgi klassik kompyuterlar uchun uni samarali yechish imkonsizdir. Aynan shu murakkablik EEChK asosida qurilgan kriptografik tizimlarning mustahkamligini ta’minlaydi. EEChDLMning murakkabligi Pollard’s Rho, Index Calculus, va Shor algoritmi kabi usullar yordamida tahlil qilinadi. Klassik hisoblash usullari bu muammoni yechishda juda sekin ishlaydi, lekin kvant hisoblash texnologiyalarining rivojlanishi bilan Shor algoritmi orqali EEChDLMni samarali yechish mumkin bo‘lib qolishi ehtimoli mavjud. Har bir algoritmning o‘ziga xos ustunliklari va cheklovlari mavjud. Amaliy kriptografik tizimlarda, ayniqsa Pollard’s Rho algoritmi eng ko‘p qo‘llaniladi, chunki u kam xotira talab qiladi va parallel ishlash imkonini beradi. MOV hujumi esa ECC’dagi ba’zi zaifliklarni aniqlashda qo‘llanadi va egri chiziqlarni tanlashda ehtiyotkorlikni talab qiladi. Shanks algoritmi esa nazariy jihatdan muhim, lekin katta xotira kerakligi sababli amaliyotda kam qo‘llaniladi.

Shuni ta’kidlash kerakki elliptik egri chiziqlar kriptografiyasi hozirda eng ishonchli kriptotizimlardan biri bo‘lib, u bank tizimlari, blockchain (Bitcoin, Ethereum) va davlatlararo xavfsiz aloqalarda qo‘llanilmoqda. Biroq, DLP ni sindirish usullarining rivojlanishi va kvant hisoblashning paydo bo‘lishi tufayli, bu sohada doimiy yangilanish va innovatsiyalar talab qilinadi. Kelajakda ECC ning yangi variantlari yoki butunlay boshqa kriptografik usullar paydo bo‘lishi mumkin

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.