KRIPTOGRAFIYADA MATEMATIKA ELEMENTLARINING QO‘LLANILISHI

Noraliyev Sanjarbek Nurislom o‘g‘li,
“Yosh chegarachilar” harbiy akademik litseyi
o‘qituvchisi,
Termiz, O‘zbekiston.
E-mail: sanjarnoraliyev@gmail.com

Annotatsiya: Diskret matematika zamonaviy kriptografiyaning nazariy asosini tashkil etuvchi eng muhim ilmiy yo‘nalishlardan biridir. Tub sonlar nazariyasi, modulyar arifmetika, tugallangan maydonlar, kombinatorika, ehtimollar nazariyasi, graf strukturalari, panjara (lattice) nazariyasi, mantiqiy algebra va algoritmlar nazariyasi kabi diskret sohalar zamonaviy shifrlash algoritmlarining ichki mexanizmlarini shakllantiradi. Shifrlash jarayonida qo‘llaniladigan har bir matematik amal - bu bitlar ustida bajariladigan chegaralangan, diskret arifmetikadan iborat bo‘lib, aynan shu diskretlik kriptosistemalarning deterministik, ishonchli va xavfsiz bo‘lishini ta’minlaydi. Ushbu maqolada kriptografiyaning turli yo‘nalishlarida diskret matematikaning tutgan o‘rni keng qamrovda tahlil qilinadi.

Kalit so‘zlar: diskret matematika, modulyar arifmetika, tub sonlar nazariyasi, diskret logarifm, elliptik egri chiziqlar, tugallangan maydonlar, kombinatorika, ehtimollar nazariyasi, tuzilmalangan graflar, LFSR, hash funksiyalari, kolliziya ehtimoli, kalit fazosi, panzara nazariyasi, LWE, Ring-LWE, NTRU.

Kirish

Kriptografiya - bu ma’lumotni himoyalash, uzatish va qayta ishlashning nazariy hamda amaliy mexanizmlarini o‘rganuvchi fan bo‘lib, uning asosida to‘liq diskret matematik strukturalar yotadi. Zamonaviy axborot xavfsizligi tizimlarining barchasi - shifrlash algoritmlari, imzo sxemalari, autentifikatsiya protokollari, tasdiqlash mexanizmlari - bitta umumiy xususiyatga ega: ular diskret obyektlar va diskret amallar asosida qurilgan.

Kriptografiyaning tub mohiyati - cheklangan, diskret strukturalar ichida murakkab matematik masalalar yaratish va ularni hal qilishni qiyinlashtirishdan iborat. Masalan, RSA algoritmining xavfsizligi ikkita katta tub sonning ko‘paytmasini faktorlashning murakkabligiga tayansa, Diffie–Hellman protokoli diskret logarifm masalasining yechilishi qiyinligiga asoslanadi. AES algoritmi baytlar ustida tugallangan maydonida bajariladigan chiziqli va nolinear akslantirishlarga tayanadi. Hash funksiyalarining kolliziya ehtimoli tug‘ilgan kun paradoksiga bog‘lanadi. Post-kvant kriptografiyada esa panjara strukturalari asosiy rolga aylangan bo‘lib, ular diskret bo‘linishlar va vektor fazolar ustida aniqlanadi.

Diskret matematikaning kriptografiyadagi o‘rni quyidagi yirik yo‘nalishlarda yaqqol namoyon bo‘ladi:

- sonlar nazariyasi va modulyar arifmetika - RSA, ElGamal, DSA, DH;
- chekli maydonlar nazariyasi - AES, SNOW, GCM va ko‘plab oqimli shifrlarda;
- kombinatorika va ehtimollar - kolliziya ehtimoli, kalit fazosining murakkabligi, tasodifiy generatorlar;
- graflar nazariyasi - LFSR holatlar grafigi, blok shifrlarning topologik modeli;
- panjara nazariyasi - LWE, NTRU, Ring-LWE kabi post-kvant algoritmlar;
- algoritmlar nazariyasi - faktorlash, DLP, qidiruv, qisqartirish algoritmlari.

Bu yo‘nalishlarning barchasi kriptografiyaning nafaqat matematik asosini, balki amaliy islashi, xavfsizlik chegaralari, algoritmik barqarorligi va hujumlarga qarshi chidamliligini belgilaydi. Yana bir muhim jihat shundaki, zamonaviy xavfsizlik talablarining kuchayishi bilan birga, diskret matematikaning roli yanada ortib bormoqda. Klassik

sonlar nazariyasidan tortib, panjara nazariyasi kabi zamonaviy strukturalargacha bo‘lgan barcha diskret yo‘nalishlar kelajakdagi kriptotizimlarning shakllanishiga, ayniqsa post-kvant muhitida, asos bo‘lib xizmat qilmoqda.

Shu sababli ushbu maqola kriptografiyaning turli qatlamlarida diskret matematika elementlarining qanday ishlatilishini chuqur va tizimli tahlil qilishni o‘z oldiga maqsad qilib qo‘yadi.

Adabiyotlar tahlili va metodoligiya.

1. Diskret matematikaning kriptografik poydevordagi o‘rni

Diskret matematika raqamlar, to‘plamlar, kombinatsiyalar va mantiqiy strukturalar ustida ishlaydi. Aynan shu tizimlar kriptografiyaning ham nazariy, ham amaliy mexanizmlarini belgilaydi. Shifrlash algoritmlari diskret obyektlar - butun sonlar, bitlar, vektorlar, graf tugunlari, polinomlar, modulyar arifmetika elementlari - asosida quriladi.

Diskret tuzilmalar kriptografiyada quyidagi yo‘nalishlarda asosiy rol o‘ynaydi:

- modulyar arifmetika va sonlar nazariyasi: RSA, DH, ECDH
- tugallangan maydonlar: AES, GCM, stream cipherlar
- kombinatorika va ehtimollar: kalit fazosi, hujum ehtimoli, kolliziyalar
- graf nazariyasi: blok shifrlardagi bog‘lanishlar, topologik xususiyatlar
- bo‘linishlar nazariyasi: panjara (lattice) kriptografiyasi
- algoritmlar nazariyasi: faktorlash, diskret logarifm, panjara qisqartirish

2. Sonlar nazariyasi va modulyar arifmetikaning kriptografiyadagi roli

2.1. Modulyar arifmetika

Modulyar arifmetika ko'plab ochiq kalitli algoritmlarning asosiy mexanizmi hisoblanadi. Asosiy amal:

$$a \equiv b \ (\mathrm{mod} n)$$

ko'rinishidagi kongruentsiyalar asosida quriladi. RSA algoritmi quyidagi ikki amalni ishlatadi:

$$C = M^e \ \mathrm{mod} n, M = C^d \ \mathrm{mod} n.$$

Bu yerda $n = pq$ ikkita katta tub sonning ko'paytmasi hisoblanadi [1].

2.2. Diskret logarifm masalasi

Diskret logarifm masalasi (DLP):

$$g^x \equiv h \ (\mathrm{mod} p)$$

berilgan bo'lsa, x ni topish juda murakkab hisoblanadi [2]. Bu murakkablik quyidagi protokollarning xavfsizligini ta'minlaydi:

- Diffie-Hellman
- ElGamal
- DSA
- Elliptik egri chiziqlar asosidagi kriptografiya (ECDLP)

2.3. Elliptik egri chiziqlar

Elliptik egri chiziqlar:

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

tenglamasi bilan aniqlanib, p tub son bo'lganda F_p ustida ishlaydi [3]. ECC quyidagilarni ta’minlaydi:

- kichik kalitlar bilan yuqori xavfsizlik,
- tezroq hisoblash,
- mobil qurilmalar uchun samaradorlik.

3. Tugallangan maydonlar: blok va oqimli shifrlardagi qo'llanishi

3.1. AES va GF(2^8)

AES baytlari $\boldsymbol{F_{2^8}}$ maydonida ko'riladi. Bayt ustidagi barcha operatsiyalar - qo'shish, ko'paytirish, teskari element topish - tugallangan maydon arifmetikasi orqali aniqlanadi [4].

AESda:

SubBytes - maydon elementining teskari elementiga asoslanadi;

MixColumns - $\boldsymbol{F_{2^8}}$ dagi matritsali o'zgarish;

AddRoundKey - XOR orqali bajariladi.

3.2. Oqimli shifrlar va LFSR

LFSRlar $\boldsymbol{F_2}$ ustida ishlaydi:

$$s_{k+1} = a_1 s_k + a_2 s_{k-1} + \cdots + a_n s_{k-n}$$

Bu to'liq diskret algebraik struktura bo'lib, chiziqli arifmetika asosida quriladi [5].

4. Kombinatorika va ehtimollar kriptografiyada

4.1. Kalit fazosi va kombinatorik murakkablik

Kalit fazosining kattaligi:

$$|\mathcal{K}| = 2^n$$

bo'lganda, qo‘pol kuch (brute-force) hujumi 2^{n-1} operatsiyani talab qiladi [6].

4.2. Kolliziyalar ehtimoli - Tug'ilgan kun paradoksi

Hesh funksiyalarida kolliziya ehtimoli:

$$\Pr(\text{kolliziya}) \approx 1 - e^{-k^2/2N}.$$

$N = 2^n$ bo'lsa, taxminan $2^{n/2}$ ta urinishda kolliziya topiladi [7]. Shu tamoyil hash funksiyalarining kuchini baholashda asosiy rol o'ynaydi.

5. Graf nazariyasining kriptografiyada qo‘llanilishi

- blok shifrlarning raund tarmoqlari graf strukturasiga ega;
- S-qutilar graf morfizmlar orqali tahlil qilinadi;
- oqimli shifrlarda LFSR holatlar grafigi de Bruijn grafga ekvivalent [8];
- tarmoq xavfsizligida autentifikatsiya protokollari graflar ustida isbotlanadi.

6. Panjara (lattice) nazariyasi va post-kvant kriptografiya

6.1. Panjara bazisi va qisqartirish algoritmlari

Panjara:

$$L(B) = \{Bx \mid x \in \mathbb{Z}^n\}$$

tenglama orqali aniqlanadi [9].

6.2. LWE va uning diskret mohiyati

LWE tenglamasi:

$$As + e = b \ (\mathrm{mod} q),$$

bu yerda A - diskret matritsa, s - maxfiy vektor, e - kichik shovqin [10].

Diskret struktura tufayli:

- kvant hujumlariga qarshi barqarorlik,
- katta o'Ichamli to'plamlar,
- diskret tasodifiylik yuqori darajada.

7. Diskret algoritmlar: faktorlash, ECDLP, LWE

Quyidagi algoritmlar to'liq diskret jarayonlarga tayangan:

- Pollard Rho
- Shanks algoritmi
- Shor algoritmi (kvant)
- Babai rounding
- BKZ va LLL panjara qisqartirish algoritmlari

Natijalar

Quyidagi 1-jadvalda diskret matematika elementlarining asosiy kriptografik vazifalarini yig‘ma ko‘rinishda taqdim etilgan.

1-jadval. Diskret matematikaning kriptografiyadagi roli bo‘yicha tahlil

Soha	**Rol**	**Xavfsizlikka ta’siri**	**Namuna**
Sonlar nazariyasi	Modulyar arifmetika, tub sonlar	Faktorlash va DLP murakkabligi	RSA, DH
Tugallangan maydonlar	Bitlar va baytlar ustida algebra	Diffuziya, nolinearlik	AES, SNOW
Kombinatorika	Kalit fazosi, kolliziya	Bruteforce va kolliziya murakkabligi	Hash funksiyalar
Graf nazariyasi	Strukturaviy modellar	Raund bog‘lanishlari	LFSR, blok shifrlar
Panjara nazariyasi	Ochiq kalit konstruksiyasi	Post-kvant barqarorlik	LWE, NTRU

Xulosa

Ushbu maqolada kriptografiyada diskret matematika elementlarining o‘rni, qo‘llanilishi va amaliy ahamiyati chuqur tahlil qilindi. O‘tkazilgan tahlillar shuni ko‘rsatdiki, kriptografiya - bu asosan diskret matematik strukturalarga tayanadigan ilmiy fan bo‘lib, uning xavfsizlik darajasi ham, ishlash samaradorligi ham, hujumlarga chidamliligi ham aynan shu diskret tuzilmalar sifatiga bevosita bog‘liqdir.

Birinchidan, sonlar nazariyasi va modulyar arifmetika ochiq kalitli kriptotizimlarning poydevorini tashkil etadi. RSA, Diffie–Hellman, ElGamal, DSA kabi algoritmlar aynan tub sonlar, modulyar eksponentlash, diskret logarifmlar va kongruentsiyalar nazariyasiga asoslanadi. Ushbu tizimlarning kuchi sonlar ustida aniqlangan murakkab masalalarning yechimi amaliy jihatdan juda qiyin bo‘lishiga tayanadi.

Ikkinchidan, tugallangan maydonlar nazariyasi simmetrik shifrlash algoritmlarida markaziy rol o‘ynaydi. AES, GCM, SNOW kabi algoritmlarda har bir bayt va bit ustida bajariladigan arifmetikaning to‘liq

matematik modeli aynan diskret maydonlarga tayangan holda yaratiladi. Bu maydonlar chiziqli va chiziqsiz akslantirishlarni mukammal tarzda ifodalashga imkon beradi, natijada yuqori diffuziya va xavfsizlik ta’minlanadi.

Uchinchidan, kombinatorika va ehtimollar nazariyasi hash funksiyalari, tasodifiy sonlar generatorlari, kolliziya ehtimoli, brute-force murakkabligi, tug‘ilgan kun paradoksiga asoslangan xavfsizlik baholarida asosiy manba sifatida namoyon bo‘ladi. Kriptotizimlarning muhim jihatlari - masalan, kalitlar soni, hujumchi uchun qidiruv maydoni, ehtimoliy tahdidlarni baholash - aynan kombinatorik o‘lchamlar orqali aniqlanadi.

To‘rtinchidan, graf nazariyasi blok shifrlardagi raund strukturalarini modellashtirish, oqimli shifrlardagi holat mashinalarini tavsiflash, LFSRlar va murakkab bog‘lanishlarni tahlil qilishda muhim vosita dir. Graflar orqali algoritmning ichki bog‘lanish darajasi, murakkablik chuqurligi va tahlilga bo‘lgan bardoshlilik o‘lchanadi.

Beshinchidan, zamonaviy kriptografiyada eng dolzarb yo‘nalishlardan biri bo‘lgan panjara nazariyasi (lattice theory) post-kvant davr uchun mo‘ljallangan kriptografik sxemalarning matematik asosini yaratadi. LWE, Ring-LWE, NTRU kabi algoritmlar diskret vektor fazolari, bo‘linish strukturalari va panjaralar ustida aniqlangan murakkab algebraik masalalarga tayanadi. Panjaralar ustida ishlashning murakkabligi, ayniqsa kvant kompyuterlari sharoitida ham barqaror bo‘lishi ushbu yondashuvlarning strategik ahamiyatini oshiradi.

Yakuniy natija sifatida shuni aytish mumkinki: diskret matematika kriptografiyaning barcha yo‘nalishlari - simmetrik shifrlashdan tortib ochiq kalitli tizimlargacha, hash funksiyalaridan tortib post-kvant algoritmlargacha - uchun yagona umumiy poydevor bo‘lib xizmat qiladi.

Diskret tuzilmalar qat’iy, nazariy jihatdan asoslangan, formal tarzda tasvirlanadigan bo‘lgani uchun kriptografik tizimlarning barqarorligi, ishonchliligi va isbotlangan xavfsizligi aynan shu matematik modelga tayanadi. Va eng muhimi, kelajakdagi kriptografiya - xususan kvant kompyuterlari davrida - aynan diskret matematikaning yanada chuqur tadqiqi va rivojlantirilgan variantlariga muhtoj bo‘ladi.

Foydalanilgan adabiyotlar

[1] R. L. Rivest, A. Shamir and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[2] N. Koblitz, *A Course in Number Theory and Cryptography*, 2nd ed. New York, NY, USA: Springer, 1994.

[3] W. Diffie and M. Hellman, “New directions in cryptography,” *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[4] T. ElGamal, “A public key cryptosystem and a signature scheme based on discrete logarithms,” *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472, 1985.

[5] V. S. Miller, “Use of elliptic curves in cryptography,” in *Advances in Cryptology — CRYPTO’85*, Springer, 1986, pp. 417–426.

[6] N. Koblitz, “Elliptic curve cryptosystems,” *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987.

[7] J. Daemen and V. Rijmen, *The Design of Rijndael: AES—The Advanced Encryption Standard*, Springer, 2002.

[8] National Institute of Standards and Technology (NIST), “FIPS PUB 197: Advanced Encryption Standard (AES),” 2001.

[9] S. Lin and D. J. Costello, *Error Control Coding*, 2nd ed. Prentice-Hall, 2004.

[10] J. L. Massey, “Shift-register synthesis and BCH decoding,” *IEEE Transactions on Information Theory*, vol. 15, no. 1, pp. 122–127, 1969.