XXI ASRDA INNOVATSION
TEXNOLOGIYALAR, FAN VA TA'LIM
TARAQQIYOTIDAGI DOLZARB MUAMMOLAR
Volume 03, Issue 04, 2025

NOSIMMETRIK KRIPTOTIZIMLAR UCHUN KALIT KRIPTOBARDOSHLIGINI OSHIRISH USULINI ASOSLASH

Allanazarova Davlatoy Farxod qizi
Termiz davlat universiteti, Kompyuter tizimlari va ularning dasturiy ta’minoti mutaxassisligi magistranti

Annotatsiya: Ushbu maqolada nosimmetrik kriptotizimlarda kalitlar xavfsizligini ta’minlashda muhim bosqich bo‘lgan tub sonlarni generatsiya qilish muammosi tahlil qilinadi. Tub sonlarning taqsimlanishi va chastotalari matematik jihatdan tadqiq qilinadi hamda bu asosda kalit kriptobardoshligini oshirish uchun rekursiv yondashuvga asoslangan yangi metod taklif etiladi. Fibonachchi ketma-ketligi, primitiv rekursiv funksiyalar va signum funktsiyasi asosida algoritmik yechim ishlab chiqiladi. Taklif etilgan usulning matematik asoslari va nazariy afzalliklari ko‘rsatib berilgan.

Kalit so‘zlar: nosimmetrik kriptotizim, tub sonlar, chastota, rekursiv funksiyalar, Fibonachchi, kalit xavfsizligi, kriptobardoshlik.

Nosimmetrik kriptotizimlar – zamonaviy raqamli xavfsizlikning tayanchidir. Bu tizimlarda ishlatiladigan kalitlarning xavfsizligi ko‘pincha katta tub sonlarning ishonchli generatsiyasiga bog‘liq. Tub sonlarning tabiiy sonlar to‘plamida notekis taqsimlanganligi sababli, ularni yaratish jarayoni ehtimolli bo‘lib qolmoqda. Shuning uchun matematik asoslangan yangi metodologiyalarni joriy qilish zarur. Ushbu maqolada tub sonlarning chastotasini aniqlash orqali ularni generatsiya qilishda foydalaniladigan matematik model asoslanadi va rekursiv yondashuv orqali kalitning kriptobardoshligini oshirish imkoniyati ko‘rib chiqiladi.

Sonni tubligini aniqlovchi ko’pgina usullar va algoritmlarning tadqiqi shuni ko’rsatdiki, tub sonlarni generatsiya qilishda qo’llaniladigan barcha algoritmlar ma’lum ehtimollik bilan tub sonni hosil qiladi va ular hal qiluvchi ahamiyat kasb etdi. Yuqorida ta’kidlanganidek, tub sonlarni generatsiya qilish nosimmetrik kriptotizimlarni loyihalashda asosiy bosqichlardan biri bo’lib, ular asosida modul arifmetikasining hal qiluvchi elementi - moduli shakllantiriladi.

Natural sonlar to’plamida tub sonlar notekis taqsimlangan bo’lib, sonlar qiymati ortib borgani sari u diapazondagi tub sonlar soni kamayib boradi. Quyidagi 1-jadvalda

uzunligi 100 ta sonni o’z ichiga olgan turli diapazondagi mavjud tub sonlarining soni keltirilgan

1-jadval

Turli diapazondagi mavjud tub sonlarning soni

Diapazoni	**Tub sonlar soni**
1-100	25
100-200	21
200-300	16
300-400	16
400-500	17
500-600	14
600-700	16
700-800	14
800-900	15
900-1000	14
1000-1100	16
1100-1200	12
1200-1300	15
1300-1400	11

Endi tub sonlarning paydo bo’lish chastotasining sonli oraliq uzunligiga bog’liqligini ko’rib chiqamiz. Tub sonlarni paydo bo’lish chastotasini ketma-ket hisoblash sxemasida qaralayotgan oraliq uzunligini o’sha oraliqda uchraydigan tub sonlar soniga bo’lib topiladi. Masalan, 1 dan 100 gacha bo’lgan birinchi diapazonni qaraydigan bo’lsak, bu yerda uchraydigan tub sonlar miqdori 25 edi, demak, chastotani ν bilan belgilaydigan bo’lsak, birinchi diapazondagi tub sonning paydo bo’lish chastotasi $\nu = \frac{25}{100}$=0,25 ga teng bo’lar ekan. 1-200 gacha bo’lgan ikkinchi sonli

diapazonni ko'radigan bo'lsak, unda tub sonning paydo bo'lish chastotasi $\nu = \frac{25+21}{100+100}$=0,23 ga teng bo'ladi. 1-300 gacha bo'lgan uchinchi sonli diapazonni ko'radigan bo'lsak, unda tub sonning paydo bo'lish chastotasi $\nu = \frac{25+21+16}{100+100+100}$=0,21 ga teng bo'ladi va hokazo davom ettirsak, quyidagi 2-jadvalni hosil qilamiz.

2-jadval

Tub sonlarning paydo bo'lish chastotalari

Diapazoni	**Tub sonlar soni**	**Umumiy soni**	**Chastotasi**
1-100	25	25	0,25
1-200	21	46	0,23
1-300	16	62	0,206667
1-400	16	78	0,195
1-500	17	95	0,19
1-600	14	109	0,181667
1-700	16	125	0,178571
1-800	14	139	0,17375
1-900	15	154	0,171111
1-1000	14	168	0,168
1-1100	16	184	0,167273
1-1200	12	196	0,163333
1-1300	15	211	0,162308
1-1400	11	222	0,15871

Yuqorida keltirilgan jadvallarni tahlil qilib quyidagi xulosalarga kelish mumkin:

- tub sonlarni paydo bo'lish chastotasining eng katta qiymati 0,25 ga teng bo'lib, unga birinchi diapazonda erishiladi;
- tub sonlarni taqsimlanishida hech qanday qonuniyat ko'zga tashlanmaydi;

- oraliq uzunligi ortib borishi bilan undagi tub sonlar miqdori ham ortib boradi;
- oraliq uzunligi ortib borishi bilan unda tub sonlarni uchrash chastotasi kamayib boradi.

Nosimmetrik kriptotizimlarda kalit generatsiya qilish masalasi katta tub sonlarni generatsiya qilish masalasi bilan chambarchas bog'liq bo'lganligi tufayli, bu natural sonlar to'plamida tub sonlarni taqsimlanishi muammosini o'rganishni talab etadi.

Rekursiv funktsiya (lotincha rekursio - qaytarish) – bu sonli argumentning sonli funktsiyasi bo'lib, funktsiyaning ko'rinishida funktsiyaning o'zidan foydalaniladi. Ya'ni bunda $f(n)$ ni hisoblash uchun $f(n-1), f(n-2),...$ dan foydalaniladi. Ixtiyoriy p uchun hisoblash yakunlanishi uchun ba'zi bir p lar uchun funktsiyaning qiymati rekursiv bo'lmasdan aniqlanishi talab qilinadi (masalan $n=0, 1$ uchun).

Rekursiv funktsiyaga misol qilib Fibonachchi sonining n- hisoblovchi quyidagi funktsiyani ko'rish mumkin:

$$F = \begin{cases} F(0) = 1; \\ F(1) = 1; \\ F(n) = F(n-1) + F(n-2), \qquad n > 1. \end{cases}$$

Ushbu keltirilgan formuladan foydalanib $F(n)$ ni qiymatini ixtiyoriy n natural son uchun chekli qadamda topishi mumkin. Bunda kerakli qiymatni topish uchun $F(n-1), F(n-2),..., F(2)$ qiymatlarni hisoblash kerak bo'ladi.

Rekursiya - bu funktsiya berishning shunday usuliki, bunda argumentning ixtiyoriy qiymati uchun aniqlanuvchi funktsiyaning qiymati muayyan usulda aniqlaniyotgan funktsiyaning kichik argumentlari orqali ifodalanadi. Primetiv rekursiya umumiy rekursiyaning eng oddiy ko'rinishlaridan biridir.

Ta'rif. Faraz qilaylik, $\alpha_1(x), ..., \alpha_s(x)$ barcha yerda aniqlangan funktsiya bo'lib, x ning barcha qiymatlarida quyidagi shartlarni qanoatlantirsin: $\alpha_i(x+1) \leq x \ (i=1,...,s)$.

$f(x_1,...,x_{n+1})$ funktsiya $g(x_1,...,x_n)$, $h(x_1,...,x_n, y, z_1, ..., z_s)$ funktsiyalardan va yordamchi funktsiya $\alpha_1, ..., \alpha_s$ dan rekursiya qaytarilishi yordamida hosil qilinadi deyiladi, agar $x_1,...,x_n, y$ o'zgaruvchilarning barcha qiymatlari uchun

$f(x_1,...,x_n,0) = g(x_1,...,x_n)$,

$f(x_1,...,x_n,y+1) = h(x_1,...,x_n, y, f(x_1,...,x_n, \alpha_1(y+1),..., f(x_1,...,x_n, \alpha_s(y+1)))$.

Teorema. Barcha yerda aniqlangan $g(x_1,...,x_n)$, $h(x_1,...,x_n, y, z_1, ..., z_s)$ funktsiyalardan va yordamchi funktsiya $\alpha_1, ..., \alpha_s$ dan hosil bo'luvchi f funktsiya yuqoridagi ta'rifda keltirilgan shartlarni qanoatlantirsa, qaytarilish rekursiyasi yordamida o'sha funktsiya $g(x_1,...,x_n)$, $h(x_1,...,x_n, y, z_1, ..., z_s)$ funktsiyalardan va yordamchi funktsiya g, h, α_i va sodda funktsiyalar 0, s, I^n_m o'rinlashtirishlar operatsiyalari va primetiv rekursiya olinishi mumkin.

Tahlilda ba'zan $sg\ x$ (signum x) funktsiyasidan foydalaniladi. Bu funktsiya x ning haqiqiy musbat qiymatlari uchun +1, haqiqiy manfiy qiymatlari uchun -1 ga va x=0 uchun 0 qiymatga ega bo'ladi. Bu funktsiyani faqat x ning natural qiymatlari uchun ko'radigan bo'lsak, u quyidagicha aniqlanadi:

$$sg\ x=\begin{cases}0, & agar \quad x=0\\ 1, & agar \quad x>0.\end{cases}$$

Quyidagicha aniqlanuvchi $\overline{sg}$ funktsiyani kiritamiz:

$$\overline{sg}=\begin{cases}1, & agar \quad x=0\\ 0, & agar \quad x>0.\end{cases}$$

$\overline{sg}$ funktsiya 1- sg bilan ustma-ust tushadi.

sg va $\overline{sg}$ funktsiyalar primetiv rekursiv sxemalarni qanoatlantiradi:

$sg\ 0=0$, $\overline{sg}\ 0=1$,

$sg\ (x+1)=1$, $\overline{sg}\ (x+1)=0$

Misol sifatida 0, 1, 1, 2, 3, 5, 8, 13, 21, ... sonli ketma ketlikni keltirish mumkin, bu ketma–ketlik Fibonachchi ketma-ketligi nomi bilan mashhur. Bu ketma-ketlikning uchinchi hadidan boshlab barcha keyingi hadlari undan oldin keladigan ikkita hadning yig'indisiga teng. Agar fibonachchi sonli ketma-ketligining p-hadini $F(p)$ bilan belgilasak, u holda $F(0)=0, F(1)=1, F(p+2)=F(p)+F(p+1)$ yoki $F(0)=0, F(p+1)=F(p)+F(p-1)+\overline{sg}n$ hosil bo'ladi. Bundan ko'rinib turibdiki, $F(p)$ funktsiya $g(x)=0, h(x, y, z_1, z_2)=\overline{sg}u+z_1+z_2$ funktsiyalardan va yordamchi funktsiyalar $\alpha_1(y)=y-1$, $\alpha_2(y)=y-2$ qaytish rekursiyasi yordamida hosil bo'ladi. Bu yerda qo'llanilgan barcha funktsiyalar primitiv rekursiv bo'lgani uchun F ham primitiv rekursiv bo'ladi.

Tub sonlarning notekis taqsimlanganligi nosimmetrik kriptotizimlarda kalit xavfsizligini zaiflashtiradi. Ushbu maqolada taklif etilgan rekursiv model bu muammoni hal qilish uchun muhim yechim hisoblanadi. Primitiv rekursiv funksiyalar va Fibonachchi ketma-ketligidan foydalanish orqali ishonchli, barqaror va boshqariladigan kalitlar generatsiyasi mumkin. Kelgusida bu yondashuv real tizimlarda testdan o'tkazilishi mumkin.

Foydalanilgan adabiyotlar ro'yxati

1. Alferov A.P., Zubov A.Yu., Kuzmin A.S., Cheremushkin A.V. Osnovы kriptografii. Uchebnoe posobie/ Izd.:Gelios ARV, 2001. – 480 s.
2. Akbarov D.Ye., Xasanov P. F., Xasanov X. P., Axmedova O. P. "Kriptografiyaning matematik asoslari" – Toshkent, 2010 – 210 bet.
3. ISO/IEC 11770 -1. "Key management – Introduction".
4. ISO/IEC 11770 -2. "Key management – Symmetric techniques".
5. ISO/IEC 11770 -3. "Key management – Asymmetric techniques".

6. Menezes A., van Oorschot R., Vanstone S. Handbook of Applied Cryptography. - CRC Press, 1996. – 780 rr.

7. Moldovyan A.A., Moldovyan N.A., Guts N.D., Izotov B.V. Kriptografiya. Skorostnыe shifrы. Sankt – Peterburg «BXV-Peterburg» 2002.

8. Bryus Shnayer. Prikladnaya kriptografiya. Protokolы, algoritmы, isxodnыe tekstы na yazыke SI – Moskva: TRIUMF, 2002.

9. Akbarov D.Ye. «Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qo’llanilishi» - T.: «O’zbekiston markasi», 2009. - 424 b.