OQIMLI SHIFRLARNING MATEMATIK MODELI VA XAVFSIZLIK MEZONLARI

Rahmatullayev Ilhom Raxmatullayevich

Toshkent Kimyo xalqaro universiteti Samarqand filiali
E-mail: ilhom9001@gmail.com

K E Y W O R D S

Oqimli shifr; chekli holat modeli; Boolean funksiya; chiziqli murakkablik; holatni tiklash; statistik sinov; nonce; autentifikatsiya.

A B S T R A C T

Oqimli shifrning statistik jihatdan tasodifiyga o‘xshash chiqishi uning kriptografik xavfsizligini o‘z-o‘zidan ta’minlamaydi. Mazkur maqolada ushbu farq chekli holat modeli, Boolean mezonlar, chiziqli murakkablik, holatning kuzatiluvchanligi va protokol shartlarini birlashtiruvchi qayta tekshiriladigan audit orqali miqdoriy asoslanadi. Tadqiqotda chiziqli LFSR16 hamda kvadratik filtrli QF16 nazorat generatorlari to‘liq holatlar fazosida tekshirildi; ChaCha20 esa amaliy taqqoslash obyekti sifatida olindi. Har bir generator uchun 16 384 bitdan iborat 256 ta chiqish oynasi, jami 12 582 912 bit tahlil qilindi. QF16 ning nochiziqligi 32 512, bir bitli empirik entropiyasining o‘rtachasi 0,999972 bo‘lishiga qaramay, uning chiziqli murakkabligi atigi 136 ga tengligi va keyingi 512 bitni xatosiz bashorat qilish mumkinligi aniqlandi. Uchta tanlangan statistik sinovga Holm tuzatishi qo‘llanganda QF16 hamda ChaCha20 uchun bir xil — 255/256 — rad etilmagan oynalar soni olindi. Barcha 65 535 boshlang‘ich holatni sanash QF16 holatini bir qiymatli aniqlash uchun zarur va yetarli kuzatuv uzunligi 29 bit ekanini ko‘rsatdi; 28 bitda qoladigan yagona noaniq juftlik ham topildi. Nonce takrorlanishi va shifrmatnni o‘zgartirish tajribalari maxfiylik hamda yaxlitlik talablari alohida tekshirilishi lozimligini tasdiqladi. Natijalar statistik ko‘rsatkichlarni xavfsizlik darajasi sifatida talqin qilish o‘rniga, dalil turi va amal qilish chegarasi ko‘rsatilgan ko‘p bosqichli baholashdan foydalanish zarurligini asoslaydi.

Kirish

Oqimli shifrlashda ochiq matn kalit oqimi bilan birlashtiriladi, biroq himoyaning sifati bu sodda amalga emas, kalit oqimini hosil qiluvchi tizimning tuzilishiga bog‘liq. Shannonning maxfiylik haqidagi nazariyasi axborot-nazariy himoya bilan cheklangan resursli raqibga qarshi himoyani ajratishga asos beradi [1]. Amaliy generator esa cheklangan maxfiy holatdan uzun ketma-ketlik chiqaradi. Shuning uchun chiqishdagi nollar va birlar muvozanati, uzun davr yoki murakkab ko‘rinadigan formula xavfsizlikning yakuniy isboti bo‘la olmaydi [2].

Baholashdagi asosiy metodik muammo turli mazmundagi ko‘rsatkichlarni bir-birining o‘rnida ishlatishdir. Masalan, empirik entropiyaning birga yaqinligi ba’zan kalitni tiklash qiyinligi bilan tenglashtiriladi; statistik sinovdan o‘tish esa algoritmga qarshi samarali hujum mavjud emasligining dalili sifatida ko‘rsatiladi. NIST SP 800-22 statistik tahlilni kriptotahlil o‘rniga qo‘ymaslikni ta’kidlaydi [3]. NISTning 2022-yildagi qayta ko‘rib chiqish qarorida ham ushbu to‘plamning vazifasi va kriptografik generatorlarni baholashdagi noto‘g‘ri qo‘llanishini aniqlashtirish zarurati qayd etilgan [4].

Bundan tashqari, algoritmning to‘g‘ri ishlashi protokolning to‘g‘ri ishlashiga teng emas. Nonce — bitta kalit ostida takrorlanmasligi talab etiladigan ochiq qiymat — shifrlash modelining ajralmas qismidir [5]. ChaCha20 spetsifikatsiyasi ham parametrlar, blok hisoblagichi va autentifikatsiya bilan birlashtirish tartibini alohida belgilaydi [6]. Demak, mezonlar faqat chiqish ketma-ketligi bilan chegaralansa, amaliy xavfsizlikka bevosita ta’sir qiluvchi shartlar tahlildan tashqarida qoladi.

Ishning maqsadi oqimli shifrni matematik modeldan tekshiriladigan hujum natijasigacha izchil baholash usulini ishlab chiqish va uning foydasini nazorat misollarida ko‘rsatishdan iborat. Tadqiqot yangi sanoat shifri yaratishni yoki ChaCha20 ni buzishni da’vo qilmaydi. Uning hisoblash hissasi kvadratik filtrli aniq generator

(cc) BY

uchun to‘liq kuzatiluvchanlik chegarasini topish, bu chegarani shartli entropiya va bashorat natijalari bilan bog‘lash hamda statistik saralashning cheklanishini bir xil tajriba tartibida ko‘rsatishdir. Barcha sonli natijalar ushbu ish uchun bajarilgan dasturiy hisoblashlardan olingan; adabiyotdagi natijalar alohida havola bilan beriladi.

Adabiyotlar sharhi

Rueppelning oqimli shifrlar nazariyasida ketma-ketlik davri, registr tuzilishi va chiziqli murakkablik alohida xususiyatlar sifatida qaraladi [2]. Massey taklif etgan sintez algoritmi berilgan prefiksni hosil qiladigan eng qisqa chiziqli rekurrent bog‘lanishni topishga imkon beradi [7]. Bu yondashuvning muhim afzalligi tekshiruvning hujumga yaqinligidir: topilgan rekurrent qoida keyingi, sintezda ishlatilmagan bitlarni ham bashorat qilsa, natija oddiy statistik og‘ishdan kuchliroq dalilga aylanadi. Biroq cheklangan prefiks uchun topilgan qiymatni butun cheksiz oqimning murakkabligi deb qabul qilish mumkin emas.

Boolean funksiyalar tahlili boshqa darajadagi savolni hal qiladi. Carlet nochiziqlik, algebraik daraja, korrelyatsion immunitet, algebraik immunitet va tarqalish xossalarini turli hujum mexanizmlariga bog‘laydi [8]. Siegenthalerning korrelyatsion immunitet tushunchasi ayrim kirishlar bilan chiqish o‘rtasidagi statistik bog‘liqlikni nazorat qiladi [9]. Ammo bu xossa kirishlar taqsimoti haqidagi shartlarga tayanadi. Registr holatlarining vaqt bo‘yicha bog‘langan ketma-ketligini mustaqil tekis Boolean kirishlar bilan tenglashtirish noto‘g‘ri; filtrning yaxshi lokal xossasi butun generatorning yaxshi dinamik xossasini kafolatlamaydi.

Courtois va Meier chiziqli qayta bog‘lanishli generatorlarga qarshi algebraik tenglamalardan foydalanish yo‘lini ko‘rsatgan [10]. Tezkor algebraik hujumlarda esa filtrning o‘z darajasi bilan cheklanmasdan, uni past darajali funksiyaga ko‘paytirganda hosil bo‘ladigan munosabatlar ham tekshiriladi [11]. Bu natijalar baholash uchun muhim: yuqori nochiziqlik soni past darajali tenglamalar yoki kichik monomlar fazosi mavjudligini bartaraf etmaydi. Mazkur maqoladagi QF16 aynan shunday farqni to‘liq sanash mumkin bo‘lgan kichik modelda ko‘rsatishga xizmat qiladi.

Dinur va Shamirning kub hujumi ochiq o‘zgaruvchilarning tanlangan to‘plami bo‘yicha yig‘indilar yordamida maxfiy o‘zgaruvchilar haqidagi munosabatlarni ajratishga asoslanadi [12]. Ushbu yo‘nalishda Trivium muhim tadqiqot obyektidir; uning to‘liq spetsifikatsiyasi va boshlang‘ich aralashtirish tartibi alohida berilgan [13]. Zhang va Sun 2024-yilda 820 hamda 832 boshlang‘ich raundgacha qisqartirilgan Trivium variantlari uchun mos ravishda 2^{45} va 2^{49} ma’lumot talab qiladigan, vaqt baholari 2^{46} va 2^{50} dan kichik hujumlarni keltirgan [14]. Bu sonlar mualliflar bergan murakkablik baholaridir; ularni barcha oracle so‘rovlari to‘liq bajarilgan tajriba vaqti deb talqin qilish mumkin emas. Ularning qisqartirilgan variantga tegishliligi to‘liq 1152 boshlang‘ich raundli Trivium buzilganini anglatmaydi.

Nonce asosidagi formal yondashuv takrorlanmas ochiq parametrni raqib modeliga kiritadi [5]. Amaliy spetsifikatsiya darajasida ChaCha20–Poly1305 maxfiylikni autentifikatsiya bilan birlashtiradi [6]. NISTning 2025-yilda yakunlangan SP 800-232 hujjatida ham cheklangan qurilmalar uchun Ascon-AEAD128 kabi autentifikatsiyalangan shifrlash algoritmi standartlashtirilgan [15]. Ascon bu ishda oddiy oqimli generator sifatida tasniflanmaydi va tajribaga kiritilmaydi; u amaliy himoyani faqat kalit oqimi sifati bilan cheklamaslik zarurligini ko‘rsatuvchi standartlashuv misolidir.

Tahlil qilingan manbalar bir-birini inkor qilmaydi, balki turli darajalardagi dalillarni beradi: ketma-ketlik nazariyasi bashoratni, Boolean tahlil lokal algebraik tuzilishni, kub hujumi ko‘p boshlang‘ich qiymatli bog‘lanishlarni, nonce va AEAD modeli esa foydalanish shartlarini tekshiradi. Ushbu ishda ular yagona vaznli ballga yig‘ilmaydi. Har bir natija o‘z hujum modeli, ma’lumot hajmi va tekshirish chegarasi bilan saqlanadi. Shu jihat maqoladagi auditni faqat testlar ro‘yxatini yoki algoritmlar tavsifini takrorlashdan farqlaydi.

Oqimli shifrlash bo‘yicha muallifning avvalgi tadqiqotlari ushbu ishning metodologik bazasini kengaytiradi. Dastlab oqimli shifrlarning paydo bo‘lish sabablari va ularning kriptografik

(cc) BY

tizimlardagi o‘rni tahlil qilingan [17]; keyingi ishlarda yangi kalit oqimi generatorining kriptotahlili [18], mavjud oqimli algoritmlarning qiyosiy ko‘rsatkichlari [19] va differensial hamda algebraik kriptotahlil orqali bardoshlilikni baholash [20] ko‘rib chiqilgan. Dasturiy realizatsiyaga yo‘naltirilgan yechimlar [21], NewHSA apparat oqimli shifrining tasodifiylik va apparat samaradorligi [22], shuningdek A5/1 algoritmining boshlang‘ich holatini tiklashga qaratilgan yangi kriptotahliliy yondashuvlar [23] mazkur maqoladagi ‘statistik xossa – strukturaviy bardoshlilik – amaliy protokol xavfsizligi’ ajratilishini mantiqan davom ettiradi.

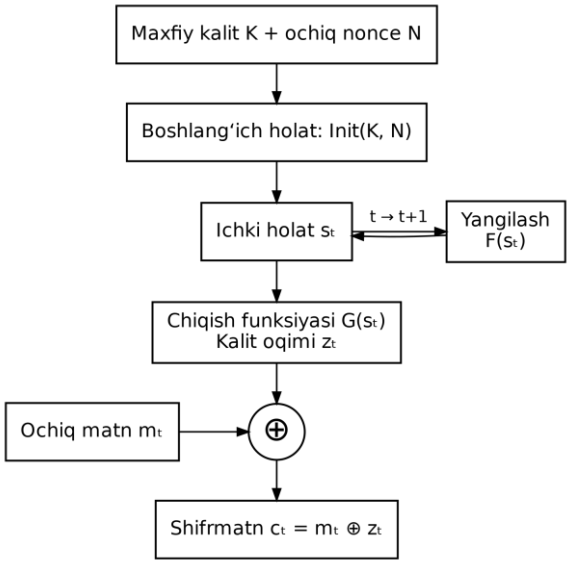
Metodologiya

1.1. Chekli holat modeli va raqib imkoniyatlari

Sinxron oqimli shifr $K \in \{0,1\}^k$ maxfiy kalit, $N \in \{0,1\}^v$ ochiq nonce va $s_t \in \{0,1\}^s$ ichki holat orqali ifodalanadi. Bir bitli chiqish uchun model quyidagicha yoziladi:

$$\begin{aligned} s_0 &= Init(K, N), \\ s_{t+1} &= F(s_t), \quad z_t = G(s_t), \\ c_t &= m_t \oplus z_t. \end{aligned} \tag{1}$$

Bu yerda m_t va c_t mos ravishda ochiq matn hamda shifrmatn bitlaridir. So‘zli yoki blok hisoblagichli algoritm ham hisoblagichni holatga kiritish orqali shu abstraksiyaga moslashtiriladi. Modelni o‘z-o‘zidan sinxronlanuvchi shifrga o‘zgartirmasdan qo‘llash mumkin emas: bunday holatda holat yangilanishiga oldingi shifrmatn ham kiradi. Ushbu ish sinxron model bilan cheklanadi. 1-rasmda maxfiy holat, chiqish va shifrlash amali orasidagi bog‘lanish ko‘rsatilgan.



1-rasm. Sinxron oqimli shifrning holat–chiqish modeli.

Deterministik boshlang‘ich yuklashda, K va N mustaqil bo‘lsa, holat hamda chiqishning axborot miqdori quyidagicha chegaralanadi:

$$H(S_0 \mid N) \le H(K) \le k. \tag{2}$$

Shu sababli 256 bitli kalitdan hosil qilingan katta ichki holat avtomatik ravishda holat uzunligicha maxfiy entropiya bermaydi. Ayni paytda (2) hisoblash bilan cheklangan raqibning muvaffaqiyatini bevosita baholamaydi. Ochiq nonce maxfiy entropiyani oshirmaydi, lekin bir kalit bilan turli oqimlarni ajratish vazifasini bajaradi. Umumiy F uchun uzun davr ham avtomatik emas: chekli holat tizimi qisqa siklga yoki o‘tkinchi qismdan keyingi siklga tushishi mumkin.

Formal ajratish o‘yinida raqib D bir kalit ostida takrorlanmagan nonce qiymatlariga so‘rov beradi. Haqiqiy oracle shifr oqimini, ideal oracle esa har bir yangi nonce uchun mustaqil tekis bitlarni qaytaradi [5]. T vaqt, q so‘rov va jami σ bit resurslari uchun ustunlik:

$$Adv_D(T, q, \sigma) = |p_{real} - p_{ideal}|. \tag{3}$$

Bu yerda $p_b = \Pr[D^{\mathcal{O}_b} = 1]$ va $b \in \{\text{real}, \text{ideal}\}$. Statistik sinovdagi p-qiymat (3) dagi ustunlik emas. Xavfsizlik haqidagi xulosa raqibning algoritmi va resurslariga bog‘lanishi kerak. Tajribada kuzatilgan kalit oqimi ma’lum

(cc) BY

ochiq matn holatiga mos keladi: $z = m \oplus c$. Boshlang‘ich holatni tiklash, chiqishni bashorat qilish va shifrmatnni o‘zgartirish alohida natija sifatida baholanadi.

1.2. Nazorat generatorlari va Boolean mezonlar

Chiziqli nazorat generatori LFSR16 da holat bitlari $x_0, \dots, x_{15}$ deb olinadi; x_0 butun sonning eng kichik razryadiga mos keladi. Yangilanish va chiqish:

$$x_i' = x_{i+1} \quad (0 \le i < 15),$$
$$x_{15}' = x_0 \oplus x_2 \oplus x_3 \oplus x_5, \tag{4}$$
$$g(x) = x_0.$$

Mos rekurrent ko‘phad $P(X) = X^{16} + X^5 + X^3 + X^2 + 1$. Nolinchi holat ishlatilmaydi. Maksimal davr faqat ko‘phad nomiga tayangan holda qabul qilinmadi: barcha 65 535 noldan farqli holatning bitta siklda kelishi dasturiy sanash bilan tekshirildi.

Ikkinchi nazorat generatori QF16 shu holat yangilanishini saqlaydi, ammo chiqishga kvadratik filtr qo‘llaydi:

$$f(x) = x_0 \oplus x_{15} \oplus \oplus_{j=1}^{7} x_{2j-1}x_{2j}. \tag{5}$$

QF16 ataylab audit nazorati sifatida tanlangan; u amaliy foydalanishga taklif qilinadigan shifr emas. Filtr barcha 16 o‘zgaruvchini ishlatadi, lekin holat hajmi o‘zgarmaydi. Haqiqiylik jadvalidagi barcha 2^{16} kirish uchun algebraik normal shakl, Walsh spektri va bir bitli hosilalar hisoblandi. Nochiziqlikning ta’rifi [8]:

$$W_f(a) = \sum_{x \in \mathbb{F}_2^{16}} (-1)^{f(x) \oplus a \cdot x},$$
$$NL(f) = 2^{15} - 1/2 \max_a \left| W_f(a) \right|. \tag{6}$$

Algebraik immunitet $AI(f)$ — $fh = 0$ yoki $(f \oplus 1)h = 0$ tengliklardan birini qanoatlantiradigan noldan farqli h ning eng kichik darajasi [8, 10]. Bu ishda darajasi birgacha bo‘lgan potensial annihilyatorlar $1, x_0, \dots, x_{15}$ bazisining filtr nol va birga teng to‘plamlaridagi rangini topish orqali tekshirildi. SAC mezoni uchun $D_i f(x) = f(x) \oplus f(x \oplus e_i)$ ning birga teng bo‘lish ulushi to‘liq sanaldi.

Uchinchi obyekt ChaCha20 ning 20 raundli, 256 bitli kalit va 96 bitli nonce bilan ishlaydigan RFC 8439 parametrizatsiyasidir [6]. Boshlang‘ich blok hisoblagichi birga teng. U nazorat generatorlarining o‘lchami bilan tenglashtirilmaydi: vazifa tezlik reytingi tuzish emas, bir xil kuzatuv testlari turli kriptografik tuzilishlarga qanday munosabat bildirishini ko‘rsatishdir.

1.3. Chiziqli murakkablik va kuzatiluvchanlik

$L(n)$ berilgan n bitli prefiksni hosil qila oladigan eng qisqa chiziqli rekurrent qoida uzunligi sifatida Berlekamp–Massey algoritmi bilan topildi [7]. Birinchi 512 bitda topilgan qoida keyingi 512 bitni rekursiv bashorat qilishda qo‘llandi. Bashoratda haqiqiy keyingi bitlar qayta kirish sifatida berilmadi. Shu bilan modelni moslashtirish va tekshirish ma’lumotlari ajratildi.

Chiziqli holat yangilanishida kvadratik filtrni monomlar fazosiga ko‘tarish mumkin. Darajasi birdan yoki ikkidan iborat monomlar keyingi taktda yana shu monomlarning chiziqli kombinatsiyasiga aylanadi; $x_i^2 = x_i$ tengligi darajani oshirmaydi. (4) va (5) da doimiy had yo‘qligi sababli mazkur invariant fazoning o‘lchami:

$$D = \binom{16}{1} + \binom{16}{2} = 136, \qquad L \le D. \tag{7}$$

Shunday qilib, chiqish funksiyasi nochiziqli bo‘lsa ham, kengaytirilgan koordinatalarda generator ko‘pi bilan 136 o‘lchamli chiziqli kuzatuvga ega. Bu standart monomlar orqali chiziqlashtirishning mazkur modelga qo‘llanishidir, yangi umumiy teorema emas. Amalda $L = 136$ bo‘lishi alohida sintez hamda to‘liq davr bo‘yicha tekshiruv bilan aniqlanadi.

Holatning kuzatiluvchanligi uchun barcha $Q = 65\,535$ boshlang‘ich holat tekis ehtimolli deb

(cc) BY

olinadi. r bitli chiqish prefiksi y ni beradigan holatlar soni c_y, turli prefikslar soni B_r bo‘lsin. Deterministik kuzatuvdan keyingi shartli entropiya va optimal bir martalik holat taxmini ehtimoli:

$$H(S_0 \mid Z^r) = \frac{1}{Q} \sum_{y:c_y>0} c_y \, log_2 c_y,$$
$$P_{guess}(S_0 \mid Z^r) = \frac{B_r}{Q}. \quad (8)$$

(8) ning asosi sodda: berilgan y uchun mos c_y holat teng ehtimolli, shuning uchun shartli entropiya $\log_2 c_y$, eng yaxshi bitta taxmin muvaffaqiyati esa $1/c_y$ ga teng. Ularni c_y/Q ehtimol bilan o‘rtachalash keltirilgan ifodalarni beradi. Bir qiymatli aniqlanadigan holatlar ulushi esa boshqa ko‘rsatkichdir:

$$u_r = \frac{\left|\{s_0 : c_{Z^r(s_0)} = 1\}\right|}{Q}. \quad (9)$$

$r \geq \lceil \log_2 Q \rceil$ bo‘lganda chiqish taqsimoti bilan r bitli tekis taqsimot $\mathcal{U}_r$ orasidagi to‘liq variatsion masofa ham aniq topiladi:

$$\Delta(P_{Z^r}, \mathcal{U}_r) = 1 - \frac{B_r}{2^r}. \quad (10)$$

Chunki qo‘llab-quvvatlovchi to‘plamdagi har bir ehtimol $c_y/Q \geq 1/Q \geq 2^{-r}$; tekis taqsimotning ushbu to‘plamdan tashqaridagi massasi aynan (10) ga teng. Bu resurs bilan cheklanmagan ajratish natijasidir. Katta kalitli har qanday deterministik generator uchun ham uzun chiqishda tayanch to‘plam kichik bo‘lishi mumkin, lekin unga a’zolikni samarali tekshirish alohida masala. QF16 uchun fazo kichikligi sababli bu farqni amaliy lug‘at orqali ishlatish mumkin.

1.4. Tajriba tartibi va statistik ishlov

Har bir obyekt uchun 256 ta, har biri 16 384 bitli oyna hosil qilindi. LFSR16 va QF16 uchun 256 ta turli noldan farqli holat takrorlanmas tanlash orqali olindi; ChaCha20 uchun 256 ta turli kalit–nonce juftligi yaratildi. Qayta bajarish urug‘i «OSMM-XM-v1-20261011». SHAKE256 faqat parametrlarni deterministik hosil qilish uchun ishlatildi; u sinalayotgan shifr emas. Bayt ichidagi bitlar kichik razryaddan katta razryadga o‘qildi. Parametrlar va chiqishlar uchun tekshirish xeshlari elektron ilovada saqlandi.

Tanlangan tekshiruvlar NIST SP 800-22 ta’rifidagi bir bitli chastota, 128 bitli bloklar chastotasi va seriyalar soni sinovlaridir [3]. Masalan, □ birlar ulushi bo‘lsa, monobit sinovi va marginal entropiya:

$$p_{mono} = erfc\left(\frac{|\sum_t (2z_t - 1)|}{\sqrt{2n}}\right),$$
$$\hat{H}_1 = -\hat{p} log_2 \hat{p} \quad (11)$$
$$-(1-\hat{p}) log_2 (1-\hat{p}).$$

Blok sinovida 128 ta blokning har biri 128 bitdan iborat; bu eksplorativ parametr tanlovi bo‘lib, standartning barcha parametr tavsiyalarini qamragan validatsiya emas; $\chi^2 = 4M \sum_j (\hat{p}_j - 1/2)^2$ va to‘ldiruvchi gamma funksiyasi ishlatildi. Seriyalar sinovining birlar ulushiga oid dastlabki sharti ham tekshirildi. Bu uchta yo‘naltiruvchi sinov bo‘lib, to‘liq NIST STS to‘plami bajarilgani yoki sertifikat olingani da’vo qilinmaydi. $\hat{H}_1$ esa ketma-ketlikning qo‘shma, shartli yoki min-entropiyasi emas.

Bitta oynadagi uchta p-qiymat uchun oilaviy daraja $\alpha = 0{,}01$ qilib belgilandi. Holmning ketma-ket rad etish tartibida kichikdan kattaga saralangan qiymatlar $\alpha/3$, $\alpha/2$ va α chegaralari bilan birinchi rad etilmagan gipotezagacha solishtiriladi [16]. «Holm bo‘yicha rad etilmadi» degani uchala gipotezadan hech biri rad etilmaganini bildiradi; bu har bir xom p-qiymat kamida 0,01 bo‘lishi bilan bir xil shart emas.

Nazorat generatorlarining oynalari bir davrning turli fazalaridir; ular qisman ustma-ust tushishi va o‘zaro bog‘liq bo‘lishi mumkin. Shu sababli ularning o‘tish ulushlariga mustaqil Bernulli kuzatuvlari kabi ishonch oralig‘i hisoblanmadi. ChaCha20 bashorat aniqligi uchun esa 256 oqimning har biridagi 512 bitlik aniqlik alohida kuzatuv birligi sifatida olindi va

(cc) BY

oqimlararo o‘zgaruvchanlikdan Student usulidagi 95 foizlik oraliq hisoblandi. Bu deterministik namunani mustaqil kalitlar tanlanishiga yaqin model sifatida qarashga tayangan tavsifiy oraliqdir.

Hisoblash muhiti: Python 3.13.5, NumPy 2.3.5, SciPy 1.17.0 va cryptography 46.0.4. ChaCha20 RFC 8439 ning 2.3.2-bo‘limidagi nazorat vektori bilan, qo‘shimcha 10 ta ko‘p blokli misolda esa mustaqil Python realizatsiyasi bilan tekshirildi. Berlekamp–Massey natijalari alohida sodda realizatsiya bilan 10 tasodifiy ketma-ketlikda va QF16 da solishtirildi. Ushbu tekshiruvlar algoritmlarning kodga noto‘g‘ri ko‘chirilishidan keladigan xatolarni kamaytirishga xizmat qiladi; ular formal dastur verifikatsiyasi emas.

Natijalar

2.1. Lokal Boolean xossalar va global tuzilish

To‘liq sanashda LFSR16 hamda QF16 ning davri 65 535 ga teng chiqdi. QF16 chiqish davri holat davrining haqiqiy bo‘luvchisiga qisqarmasligi 65 535 sonining 3, 5, 17 va 257 tub bo‘luvchilari bo‘yicha tekshirildi. Demak, keyingi zaifliklar qisqa davr yoki nol holatning noto‘g‘ri ishlatilishidan kelib chiqmagan.

1-jadval.

QF16 filtrining to‘liq hisoblangan Boolean ko‘rsatkichlari

Ko‘rsatkich	Aniq natija
Haqiqiylik jadvali og‘irligi	32 768 / 65 536
Algebraik daraja	2
Maksimal |Walsh|	512
Nochiziqlik NL	32 512
Korrelyatsion immunitet	1
Algebraik immunitet AI	2
SAC: x_0 va x_{15} bo‘yicha	1,0
SAC: qolgan 14 kirishda	0,5

1-jadvaldagi katta nochiziqlik filtrning barcha mezonlarda kuchli ekanini bildirmaydi. Uning Walsh spektridagi noldan farqli eng kichik vaznli niqob ikki razryadli; bu birinchi tartibli korrelyatsion immunitetni beradi, ikkinchi tartibini bermaydi. Maksimal korrelyatsiya amplitudasi $512/65\,536 = 1/128$. Bu lokal amplituda tayyor kalitni tiklash hujumi murakkabligi sifatida talqin qilinmaydi.

Filtr nol va birga teng bo‘lgan to‘plamlarda affine bazis matritsalarining rangi ikkalasida ham 17 chiqdi. Shunday qilib, noldan farqli affine annihilyator yo‘q. Boshqa tomondan, $f(f \oplus 1) = 0$ va $\deg(f) = 2$ bo‘lgani uchun $AI(f) \leq 2$; ikki natija birgalikda $AI(f) = 2$ ni beradi. x_0 yoki x_{15} almashsa chiqish doimo almashishi esa SAC ning to‘liq bajarilmasligini ko‘rsatadi. Katta NL qiymati past algebraik immunitet va chiziqli strukturalarni yashira olmagan.

2.2. Statistik tekshiruv va bashorat orasidagi tafovut

2-jadval.

256 oynada statistik gipotezalar rad etilmagan holatlar soni

Sinov	LFSR16	QF16	ChaCha20
Monobit, α=0,01	256	256	254
Blok, M=128	223	254	253
Seriyalar	256	256	254
Holm, 3 sinov	239	255	255

Dastlabki uch qator xom p-qiymatlar uchun; oxirgi qator oilaviy tuzatishdan keyingi hisob. Har bir ustunda 256 oyna mavjud.

2-jadvalda QF16 va ChaCha20 Holm bo‘yicha aynan bir xil 255/256 natija berdi. LFSR16 da esa bloklar chastotasi ko‘proq og‘ishni aniqladi. Bu sinovlar ayrim strukturalarni sezishi mumkinligini, lekin barcha xavfli strukturalarni topmasligini ko‘rsatadi. Hatto QF16 uchun uch sinovning yakuniy o‘tish ulushi 99,6094 foiz bo‘lsa ham, quyida berilgan bashorat hujumi to‘liq muvaffaqiyatli bo‘ldi.

3-jadval.

Empirik entropiya va chiziqli bashorat natijalari

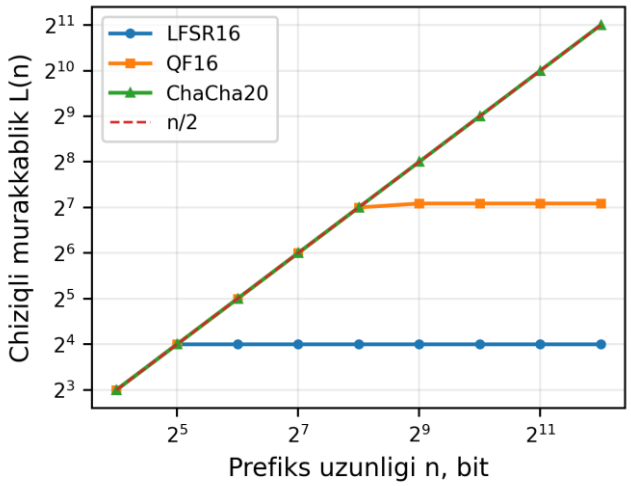
Ko‘rsatkich	LFSR16	QF16	ChaCha20
O‘rtacha H_1	0,999963	0,999972	0,999954

(cc) BY

Ko‘rsatkich	LFSR16	QF16	ChaCha20
L(4096), mediana	16	136	2048
L(4096), oraliq	16–16	136–136	2044–2052
512 bitni bashorat qilish	100%	100%	50,1640%

Bashorat uchun faqat oldingi 512 bit ishlatilgan. H_1 marginal chastotadan hisoblangan, xavfsizlik biti emas.

QF16 ning o‘rtacha marginal entropiyasi ChaCha20 nikidan ham kattaroq chiqdi. Biroq uni «yaxshiroq shifr» deb baholash mutlaqo teskari xulosaga olib kelgan bo‘lardi: QF16 ning 256 ta oynasida keyingi 512 bitning barchasi topildi. ChaCha20 uchun o‘rtacha aniqlik 50,1640 foiz, oqimlararo standart og‘ish 2,1064 foiz punkt, 95 foizlik tavsifiy oraliq esa 49,9048–50,4233 foiz bo‘ldi. Oraliq 50 foizni qamrab oladi; mazkur bashorat usuli uchun ishonchli ustunlik kuzatilmadi.



2-rasm. 256 oqim bo‘yicha chiziqli murakkablik medianasi.

2-rasmda LFSR16 profili 16 da, QF16 profili esa 136 da to‘xtaydi. ChaCha20 ning kuzatilgan prefikslaridagi qiymatlar o‘sishda davom etadi. QF16 uchun dastlabki 272 bitdan darajasi 136 bo‘lgan rekurrent ko‘phad topilib, uning tengligi 65 535 bitli butun davr bo‘yicha, siklik tutashishlar bilan birga tekshirildi. Natija (7) dagi yuqori chegaraning aynan erishilganini tasdiqlaydi. ChaCha20 uchun esa 4096 bitda olingan L(n) ni butun oqimning chiziqli murakkabligi yoki 256 bitli xavfsizlik isboti deb qabul qilishga asos yo‘q.

2.3. Holatni tiklashning aniq chegarasi

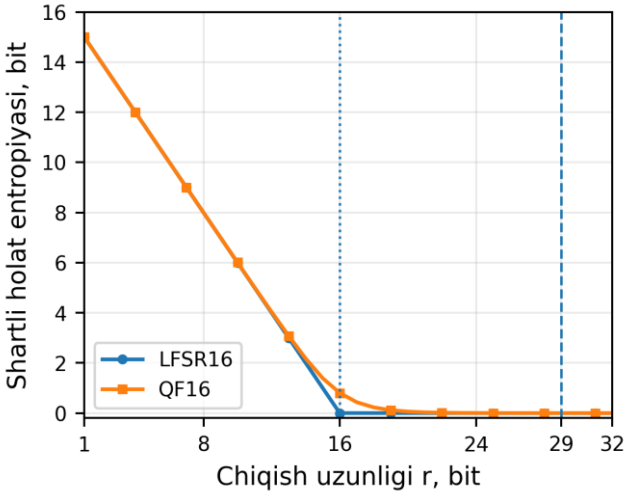
Kuzatiluvchanlik tajribasi statistik oynalardan mustaqil ravishda barcha 65 535 holatda bajarildi. LFSR16 holati birinchi 16 chiqish biti bilan bir qiymatli aniqlandi. QF16 uchun asosiy qiymatlar 4-jadvalda keltirilgan. Undagi ehtimollar tanlanma bahosi emas, butun holatlar fazosidagi aniq ulushlardir.

4-jadval.

QF16 holatining chiqish orqali kuzatiluvchanligi

r, bit	B_r	Pguess	$H(S_0\|Z^r)$, bit
16	41 911	0,639521	0,804841
20	63 595	0,970397	0,059835
24	65 421	0,998260	0,003479
28	65 534	0,999985	0,000031
29	65 535	1,000000	0
32	65 535	1,000000	0

16 bit kuzatilganda holatning o‘rtacha qolgan entropiyasi atigi 0,804841 bit bo‘lgan, lekin faqat 24 614 holat bir qiymatli ajralgan: $\square_{16} = 0{,}375586$. Optimal taxmin ehtimoli esa 0,639521. Demak, shartli entropiya, bir qiymatli tiklanish ulushi va eng yaxshi taxmin ehtimoli bir xil mezon emas; ularni bitta «aniqlik» nomi bilan almashtirish muhim axborotni yo‘qotadi.



3-rasm. Barcha boshlang‘ich holatlar uchun chiqish kuzatilgandan keyin qoladigan shartli entropiya.

(cc) BY

QF16 da 28 bitdan keyin faqat bitta noaniq juftlik qoldi: 52 253 va 15 143 sonli boshlang‘ich holatlar. Ularning umumiy 28 bitli prefiksi «1011111000000100111101111111»; keyingi bit birinchisida 0, ikkinchisida 1. 29 bitda esa barcha prefikslar turlicha bo‘ldi. Shuning uchun mazkur filtr va holat yangilanishi uchun barcha holatlarni bir qiymatli ajratadigan eng kichik uzunlik aynan 29 bitdir. Bu natija boshqa kvadratik filtrlar yoki zamonaviy oqimli shifrlarga avtomatik ko‘chirilmaydi.

Tiklash lug‘atida har bir yozuvga 32 bitli prefiks va 16 bitli holat ajratilsa, sof ma’lumot hajmi $65\,535 \times 6 = 393\,210$ bayt bo‘ladi. Bu Python obyektlari, saralash buferi va indeks xarajatlarini o‘z ichiga olmaydi. Sodda oldindan hisoblash $65\,535 \times 29 = 1\,900\,515$ chiqish biti hisobini talab qiladi; saralash xarajati bundan alohida. Binobarin, QF16 uchun (10) dagi nazariy farqlanish kichik lug‘at bilan amalga oshiriladigan holatni tiklashga aylanadi.

32 bitli chiqishda QF16 taqsimotining tekis taqsimotdan masofasi $1 - 65\,535/2^{32} = 0{,}9999847414$. Bir vaqtning o‘zida 16 384 bitli oynalarning marginal entropiyasi deyarli birga teng. Bunda ziddiyat yo‘q: $\hat{\square}_1$ bitta bitning chastotasini o‘lchaydi, (8) va (10) esa butun so‘zdagi birgalikdagi tuzilishni hisobga oladi. Aynan shu farqni hisoblash bilan ochib berish statistik natijani kriptografik dalildan ajratishga imkon beradi.

2.4. Nonce va yaxlitlik bo‘yicha nazorat tajribalari

Bir xil kalit, nonce va hisoblagich bilan ikki xabar shifrlanganda bir xil oqim takrorlanadi. XOR ning xossasidan:

$$c^{(1)} \oplus c^{(2)} = m^{(1)} \oplus m^{(2)},$$
$$m^{(2)} = c^{(1)} \oplus c^{(2)} \oplus m^{(1)}. \quad (12)$$

128 baytli xabarlardan iborat 256 tajribada ikkinchi xabar shu tenglik bilan to‘liq tiklandi. Bu ChaCha20 yadrosining zaifligi emas, takrorlanmas nonce shartining buzilishidir. Xuddi shuningdek, autentifikatsiyasiz oqimli shifrlashda $c' = c \oplus \delta$ yuborilishi $m' = m \oplus \delta$ ga olib keladi. Shifrmatndagi boshqariladigan bitta bit o‘zgarishi barcha 256 tajribada ochiq matnning shu bitiga ko‘chdi.

5-jadval.

128 baytli xabarlarda protokol nazoratlari

Nazorat holati	Natija
Nonce takrori: ikkinchi xabar to‘liq tiklandi	256/256
Oddiy ChaCha20: bit o‘zgarishi matnga o‘tdi	256/256
AEAD: o‘zgargan shifrmatn rad etildi	256/256
AEAD: o‘zgargan teg rad etildi	256/256
AEAD: o‘zgargan AAD rad etildi	256/256

AEAD — ChaCha20–Poly1305. AAD shifrlanmaydigan, ammo autentifikatsiyalanadigan qo‘shimcha ma’lumotdir.

ChaCha20–Poly1305 bilan to‘g‘ri xabarlarning barchasi muvaffaqiyatli ochildi. Shifrmatn, autentifikatsiya tegi va AAD alohida o‘zgartirilgan 768 holatning barchasi rad etildi. Bu ma’lum sinov vektorlari uchun yaxlitlik tekshiruvi ishlaganini ko‘rsatadi, lekin tajriba sonidan juda kichik soxtalashtirish ehtimoli yoki umumiy kriptografik isbotni chiqarib bo‘lmaydi. AEAD ishlatilganda ham nonce ni takrorlashga ruxsat berilmaydi [6].

Tasodifiy tanlanadigan ν bitli nonce lar uchun q ta tanlashda kamida bitta takrorlanish ehtimoli mustaqil tekis tanlash farazida quyidagicha hisoblanadi:

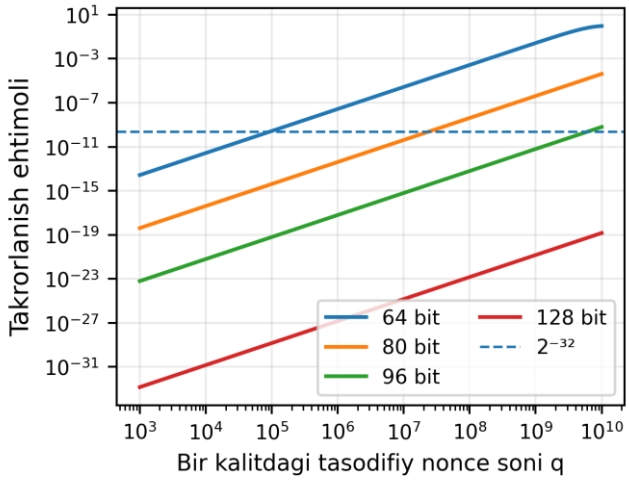
$$P_{coll} = 1 - \prod_{j=0}^{q-1}(1 - j/2^{\nu}),$$
$$P_{coll} \approx 1 - e^{-q(q-1)/2^{\nu+1}}, \quad (13)$$
$$P_{coll} \le \frac{q(q-1)}{2^{\nu+1}}.$$

(cc) BY dtai.uz

6-jadval.

$q = 2^{32}$ bo‘lganda tasodifiy nonce takrorlanish xavfi

Nonce uzunligi	Pcoll, eksponensial yaqinlashuv
64 bit	0,39346934
80 bit	$7{,}6294 \times 10^{-6}$
96 bit	$1{,}1642 \times 10^{-10}$
128 bit	$2{,}7105 \times 10^{-20}$



4-rasm. Tasodifiy nonce tanlashda takrorlanish xavfining o‘sishi.

6-jadvaldagi kichik ehtimol ham spetsifikatsiyadagi takrorlanmaslik talabini bekor qilmaydi. Hisoblagichni qayta yuklashda yo‘qotish, klonlangan qurilmalarda bir xil holatdan boshlash yoki parallel jo‘natuvchilarni ajratmaslik tasodifiy tanlash modeliga kirmaydi. Shu sababli amaliy audit faqat nonce uzunligini emas, uning ajratilishi, doimiy saqlanishi, jo‘natuvchilar o‘rtasida bo‘linishi va kalit yangilanishi tartibini ham tekshirishi kerak. Bular maqoladagi ehtimol formulasidan chiqadigan foydalanish xulosalari bo‘lib, alohida qurilmada bajarilgan sinov natijalari emas.

Muhokama

Natijalar uchta mantiqiy darajani aniq ajratadi. Birinchi darajada (5) filtr balans va katta nochiziqlikka ega. Ikkinchi darajada xuddi shu filtr chiziqli holatga qo‘yilganda 136 o‘lchamli monomlar fazosidan tashqariga chiqmaydi va rekurrent bashoratga yengiladi. Uchinchi darajada esa 29 bitli chiqish butun boshlang‘ich holatni ajratadi. Shuning uchun lokal Boolean xossalar, ketma-ketlikning statistik ko‘rinishi va global kriptografik xatti-harakatni bitta xulosa ostida birlashtirish mumkin emas.

Chiziqli murakkablikning 16 dan 136 ga ortishi 8,5 baravar o‘sishdir, ammo bu «xavfsizlik 8,5 baravar oshdi» degani emas. Holat fazosi hamon 65 535 elementdan iborat, lug‘at hujumi esa to‘liq ishlaydi. Xuddi shuningdek, 272 bit rekurrent qoidani topishga yetgani haqidagi natija bilan 29 bit holatni tiklashga yetgani haqidagi natija bir-biriga zid emas. Birinchisi noma’lum chiziqli bog‘lanishni sintez qiladi, ikkinchisi esa oldindan ma’lum F va G uchun barcha holatlar lug‘atidan foydalanadi. Hujum maqsadi va oldindan hisoblash imkoniyati turlicha.

Ishdagi matematik natijalar tanlangan nazorat modeliga kuchli dalil beradi: holatlar fazosi to‘liq qamrab olingan, 28 bitdagi qarshi misol topilgan va 29 bitdagi injektivlik sanash bilan tasdiqlangan. ChaCha20 haqidagi natija esa bunday to‘liqlikka ega emas. Uning ulkan kalit fazosi sanalmagan; faqat 256 kalit–nonce juftligidagi tanlangan testlar va oddiy chiziqli bashorat bajarilgan. Shuning uchun QF16 uchun «zaiflik ko‘rsatildi», ChaCha20 uchun esa «ushbu tekshirish doirasida chiziqli bashorat ustunligi aniqlanmadi» degan ikki xil hukm qo‘llanadi.

Adabiyotdagi qisqartirilgan Trivium hujumlari bilan taqqoslashda ham shu intizom saqlanadi [13, 14]. Raund soni, ochiq o‘zgaruvchilarni tanlash imkoniyati, oracle so‘rovlari va oldindan hisoblash xarajati ko‘rsatilmasdan keltirilgan murakkablik soni noto‘g‘ri tasavvur uyg‘otadi. QF16 ustida olingan kichik fazoli lug‘at hujumini Trivium yoki ChaCha20 ga qarshi yangi hujum deb nomlash mumkin emas. Maqolaning natijasi tayyor shifrlarni buzish emas, xavfsizlik dalillarini to‘g‘ri qatlamlash va zaif nazoratni ishonchli aniqlashdir.

Taklif qilinayotgan qaror tartibida statistik saralash faqat dastlabki nuqsonlarni aniqlaydi. Keyingi bosqichlarda tuzilishga mos hujum, holat yoki kalitni tiklash, mustaqil bo‘lakdagi bashorat va protokol xatolari tekshiriladi. Ulardan birida bajariladigan hujum ko‘rsatilsa, yuqori entropiya yoki ko‘p testdan o‘tish bu natijani kompensatsiya qilmaydi. Biror mezon tekshirilmagan bo‘lsa, u «bajarildi» emas, «baholanmagan» holatida

(cc) BY

saqlanadi. Bu qoida vaznli xavfsizlik reytingidagi asossiz ijobiy xulosalarni kamaytiradi.

Mazkur yondashuv yangi generatorni baholashda hujum sharoitlari pasportini talab qiladi: maxfiy va ochiq parametrlar, kuzatiladigan chiqish hajmi, raqibga ma’lum funksiyalar, oldindan hisoblash hamda xotira resurslari aniq yozilishi lozim. Apparat samaradorligi uchun takt chastotasi, texnologik norma va maydon; dasturiy tezlik uchun protsessor, kutubxona va o‘lchash tartibi kerak bo‘ladi. Bu ishda bunday o‘lchovlar bajarilmagani sababli tezlik, energiya yoki apparat maydoni bo‘yicha ustunlik da’vo qilinmaydi.

Xulosa

Oqimli shifrning xavfsizligini asoslash uchun matematik model, hisoblash bilan cheklangan raqib va foydalanish shartlari birgalikda belgilanishi lozim. Mazkur ishda ushbu talab QF16 nazorat generatorining to‘liq tahlili bilan miqdoriy ko‘rsatildi: balanslangan, 32 512 nochiziqlikka ega filtr 136 chiziqli murakkablik bilan cheklanadi, 272 bitdan rekurrent bog‘lanishi topiladi va 29 bitli kuzatuvdan barcha 65 535 boshlang‘ich holati bir qiymatli tiklanadi. 28 bitda qolgan yagona noaniq juftlik minimal chegaraning zarurligini ham tasdiqlaydi.

QF16 hamda ChaCha20 ning tanlangan statistik tekshiruvlarda bir xil 255/256 natija berishi statistik o‘tish ulushidan kriptografik bardoshlilikni chiqarib bo‘lmasligini ko‘rsatdi. Shu bilan birga, nonce takrorlanishida xabarlarning 256/256 holatda tiklanishi va autentifikatsiyasiz shifrmatnning boshqariladigan o‘zgarishi protokol mezonlarini alohida tekshirish zarurligini tasdiqladi. Natijada tavsiya etilayotgan audit yakuniy bitta ballni emas, har bir xulosa uchun tekshirilgan dalil, hujum resursi va amal qilish chegarasini beradi. Bu yondashuv yangi oqimli generatorlarni baholashda asossiz xavfsizlik da’volarini kamaytiradigan qayta bajariladigan ilmiy asos vazifasini bajaradi.

Foydalanilgan adabiyotlar

1. Shannon, C. E. Communication Theory of Secrecy Systems. Bell System Technical Journal, 28(4), 656–715 (1949). DOI: 10.1002/j.1538-7305.1949.tb00928.x.
2. Rueppel, R. A. Analysis and Design of Stream Ciphers. Springer, Berlin, Heidelberg (1986). DOI: 10.1007/978-3-642-82865-2.
3. Rukhin, A. et al. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST SP 800-22 Rev. 1a (2010). DOI: 10.6028/NIST.SP.800-22r1a.
4. NIST. Decision to Revise NIST SP 800-22 Rev. 1a. CSRC, 19 April 2022. Rasmiy xabar; murojaat sanasi: 11.10.2026. [CSRC]
5. Rogaway, P. Nonce-Based Symmetric Encryption. Fast Software Encryption — FSE 2004, LNCS 3017, 348–358. Springer (2004). DOI: 10.1007/978-3-540-25937-4_22.
6. Nir, Y., Langley, A. ChaCha20 and Poly1305 for IETF Protocols. RFC 8439 (2018). DOI: 10.17487/RFC8439.
7. Massey, J. L. Shift-register synthesis and BCH decoding. IEEE Transactions on Information Theory, 15(1), 122–127 (1969). DOI: 10.1109/TIT.1969.1054260.
8. Carlet, C. Boolean Functions for Cryptography and Error-Correcting Codes. In: Crama, Y., Hammer, P. L. (eds.), Boolean Models and Methods in Mathematics, Computer Science, and Engineering, 257–397. Cambridge University Press (2010). DOI: 10.1017/CBO9780511780448.011.
9. Siegenthaler, T. Correlation-immunity of nonlinear combining functions for cryptographic applications. IEEE Transactions on Information Theory, 30(5), 776–780 (1984). DOI: 10.1109/TIT.1984.1056949.
10. Courtois, N. T., Meier, W. Algebraic Attacks on Stream Ciphers with Linear Feedback. EUROCRYPT 2003, LNCS 2656, 345–359. Springer (2003). DOI: 10.1007/3-540-39200-9_21.
11. Courtois, N. T. Fast Algebraic Attacks on Stream Ciphers with Linear Feedback. CRYPTO 2003, LNCS 2729, 176–194. Springer (2003). DOI: 10.1007/978-3-540-45146-4_11.

(cc) BY *dtai.uz*

12. Dinur, I., Shamir, A. Cube Attacks on Tweakable Black Box Polynomials. EUROCRYPT 2009, LNCS 5479, 278–299. Springer (2009). DOI: 10.1007/978-3-642-01001-9_16.
13. De Cannière, C., Preneel, B. Trivium. In: New Stream Cipher Designs, LNCS 4986, 244–266. Springer (2008). DOI: 10.1007/978-3-540-68351-3_18.
14. Zhang, M., Sun, Y. A New Practical Cube Attack via Recovering Numerous Superpolys. IACR Transactions on Symmetric Cryptology, 2024(4), 38–63 (2024). DOI: 10.46586/tosc.v2024.i4.38-63.
15. Turan, M. S., McKay, K., Kang, J., Kelsey, J., Chang, D. Ascon-Based Lightweight Cryptography Standards for Constrained Devices: Authenticated Encryption, Hash, and Extendable Output Functions. NIST SP 800-232 (2025). DOI: 10.6028/NIST.SP.800-232.
16. Holm, S. A Simple Sequentially Rejective Multiple Test Procedure. Scandinavian Journal of Statistics, 6(2), 65–70 (1979). JSTOR: 4615733.
17. Rahmatullayev, I. R. Oqimli shifrlash algoritmlari va ularni vujudga kelish sabablari. International Journal of Theoretical and Applied Issues of Digital Technologies, 2(2), 119–128 (2022).
18. Khudoykulov, Z. T., Rakhmatullayev, I. R. A new key stream encryption algorithm and its cryptanalysis. Scientific and Technical Journal of Namangan Institute of Engineering and Technology, 8(1), 146–157 (2023).
19. Xudoyqulov, Z. T., Rahmatullayev, I. R. Mavjud oqimli shifrlash algoritmlarining qiyosiy tahlili. Al-Farg‘oniy avlodlari, 1(1), 129–134 (2024).
20. Rahmatullayev, I. R. Oqimli shifrlash algoritmlari bardoshliligini differensial va algebraik kriptotahlil usullari yordamida baholash. Digital Transformation and Artificial Intelligence, 2(1), 64–70 (2024).
21. Rahmatullayev, I. R., Boyquziyev, I. M., Omonov, A. A. Oqimli shifrlash uchun dasturiy yechimlar. Digital Transformation and Artificial Intelligence, 2(4), 28–38 (2024).
22. Rahmatullayev, I. NewHSA oqimli shifrlash algoritmining xususiyatlari. Al-Farg‘oniy avlodlari, 1(2), 100–105 (2025). DOI: 10.5281/zenodo.15580990.
23. Rakhmatullaev, I., Abdurakhimov, B. New approaches to assessing the resilience of the A5/1 stream cipher algorithm. International Journal of Theoretical and Applied Issues of Digital Technologies, 8(1), 122–128 (2025). DOI: 10.62132/ijdt.v8i1.240.

(cc) BY