TRIVIUM, RC4 VA CHACHA OILALARI BO‘YICHA TADQIQOTLAR TAHLILI VA ILMIY BO‘SHLIQ

Rahmatullayev Ilhom Raxmatullayevich[1], Murtazayeva Umida Isakulovna[2]

[1]Toshkent Kimyo xalqaro universiteti Samarqand filiali, Samarqand, O‘zbekiston, ilhom9001@gmail.com
[2]PhD, Energetika va amaliy fanlar kafedrasi dotsenti v.b., Toshkent Kimyo xalqaro universiteti, Toshkent, O‘zbekiston, murtazayeva198202@gmail.com, ORCID: 0000-0002-1801-4465

K E Y W O R D S

oqimli shifr; RC4; Trivium; ChaCha20; kriptotahlil; xavfsizlik zaxirasi; kub testeri; ichki parametrlar

A B S T R A C T

Tadqiqotning maqsadi RC4, Trivium va ChaCha oqimli shifr oilalari bo‘yicha kriptotahlil natijalarini yagona tasnif asosida tahlil qilish va ichki parametrlarni tanlash uchun ilmiy bo‘shliqni aniqlashdir. Metodologiya 40 ta manbani hujum turi, obyekt, murakkablik va nashr maqomi bo‘yicha tanqidiy tahlil qilishni hamda test vektorlari bilan tekshirilgan realizatsiyalarda bir xil seed bilan bajarilgan uchta statistik tajribani birlashtiradi. Xavfsizlik zaxirasi kalitni tiklash va farqlovchi bo‘yicha alohida hisoblandi: Trivium uchun M_key = 0,26 va M_dist = 0,23, ChaCha20 uchun mos ravishda 0,64 va 0,625; RC4 da zaxira yo‘q. N = 224 kalitli tajribada RC4 ikkinchi baytining nolga teng bo‘lish ehtimoli 256 ga ko‘paytirilganda 1,9988 ni (z = 256,2) tashkil etdi; umumiy χ^2 testi 256 pozitsiyadan faqat bittasini rad etdi, maqsadli test esa 16-baytdagi og‘ishni z = 10,5 bilan aniqladi. ChaCha permutatsiyasida bir bitli differensial 3 raundda $\varepsilon = 0{,}198$ bilan saqlandi, 3,5 raundda esa faqat N = 230 tanlanmada $\varepsilon = 2{,}4 \cdot 10^{-4}$ (z = 7,8) bilan aniqlandi. Trivium da kub testerining aniqlash chegarasi kub o‘lchami 1 dan 12 gacha oshganda 425 dan 651 taktga ko‘tarildi. Umumiy testlar va eng yaxshi ixtisoslashgan natijalar orasidagi nisbiy masofa ikkala oilada ham taxminan 0,20 ni tashkil etdi. Ishning hissasi — natijalarni maqomi bilan solishtiruvchi jadvallar, takrorlanadigan aniqlash chegaralari va ichki parametrlarni tanlash bo‘yicha beshta aniq ilmiy bo‘shliq. Natijalar bitta virtual muhitga va tanlangan test budjetiga tegishli; ular xavfsizlik isboti sifatida talqin qilinmaydi.

Kirish

Oqimli shifrlar bo‘yicha adabiyot hajmi katta, ammo uning natijalari bir xil o‘lchovda yozilmagan. Bir ishda to‘liq algoritmga qarshi amaliy ochiq matnni tiklash keltiriladi, boshqasida qisqartirilgan raundli variant uchun nazariy farqlovchi beriladi, uchinchisida esa zaif kalitlar sinfi yoki bog‘langan kalit modeli qabul qilinadi. Bu natijalarni bitta «eng chuqur hujum» jadvaliga yig‘ish algoritmning amaliy xavfsizligi haqida noto‘g‘ri tasavvur hosil qiladi [26, 28, 31].

RC4, Trivium va ChaCha oilalari bu muammoni uch xil holatda ko‘rsatadi. RC4 dasturiy oqimli shifrning klassik namunasi bo‘lib, uning kalit oqimidagi statistik og‘ishlar WEP, WPA-TKIP va TLS protokollariga qarshi amaliy hujumlarga aylangan; natijada TLSda RC4 taqiqlangan [4, 7, 8]. Trivium eSTREAM portfelining apparat profiliga kirgan va ISO/IEC 29192-3 standartiga kiritilgan; uning 1152 taktli initsializatsiyasiga qarshi kub hujumlari 2009-yildan beri raund sonini bosqichma-bosqich oshirib kelmoqda [10–20]. ChaCha20 esa TLS 1.3 va ko‘plab dasturiy kutubxonalarda Poly1305 bilan birga AEAD konstruksiyasi sifatida qo‘llanadi; unga qarshi eng kuchli natijalar qisqartirilgan 7–7,5 raundli variantlarga tegishli [1, 3, 21–31].

O‘zbekistonda raqamli xizmatlar, bank tizimlari va masofaviy monitoring qurilmalarining kengayishi algoritm tanlash masalasini amaliy qiladi. «Shaxsga doir ma’lumotlar to‘g‘risida»gi va «Kiberxavfsizlik to‘g‘risida»gi qonunlar texnik himoya choralarini talab qiladi, lekin aniq oqimli shifrni belgilamaydi [33, 34]. Shu sababli muhandis yoki tizim egasi adabiyotdagi turli maqomdagi natijalarni o‘zi talqin qilishiga to‘g‘ri keladi.

(cc) BY

Tadqiqotning maqsadi RC4, Trivium va ChaCha oilalari bo‘yicha kriptotahlil natijalarini yagona tasnif asosida tahlil qilish va ilmiy bo‘shliqni aniq, tekshiriladigan ko‘rinishda ifodalashdir. Buning uchun uch savol qo‘yildi:

1. Uchta oila bo‘yicha natijalarni hujum modeli, raund soni, ma’lumot va vaqt murakkabligi hamda nashr maqomi bo‘yicha qanday solishtirish mumkin?
2. Oddiy, qayta takrorlanadigan statistik testlar har bir oilada qaysi chuqurlikkacha tasodifiylikdan og‘ishni aniqlaydi va bu chegara adabiyotdagi eng yaxshi natijalardan qancha uzoqda?
3. Mavjud natijalardan amaliy tanlov uchun qanday ilmiy bo‘shliqlar kelib chiqadi?

Ishning hissasi uchta bog‘langan natijadan iborat: hujum modeli va maqomini ajratuvchi taqqoslov jadvali; uchta oila uchun bir xil seed va tekshirilgan realizatsiyada bajarilgan statistik tajribalar (E1–E3); ulardan kelib chiqadigan xavfsizlik zaxirasi ko‘rsatkichi va bo‘shliqlar ro‘yxati. Yangi kriptografik primitiv yoki ilgari noma’lum hujum taklif qilinmaydi.

Adabiyotlar tahlili

Oqimli shifrlarning qiyosiy tahlili va ularga qo‘llanadigan kriptotahlil usullari avvalgi ishlarda umumiy ko‘rinishda ko‘rib chiqilgan [36–38]. Bu yerda uchta oila bo‘yicha natijalarni solishtirishda besh belgi ajratildi: hujum turi (farqlovchi, ochiq matnni tiklash yoki kalitni tiklash), hujum qilingan raund yoki initsializatsiya takti, zarur ma’lumot hajmi, vaqt murakkabligi va nashr maqomi. Bu belgilar bir-birini almashtirmaydi: 2^{51} murakkablikdagi amaliy farqlovchi va 2^{189} murakkablikdagi nazariy kalit tiklash turli xavf darajasini ifodalaydi.

RC4. RC4 256 baytli almashtirish va ikki indeksdan iborat juda sodda dasturiy shifrdir. Fluhrer, Mantin va Shamir kalit jadvali algoritmidagi (KSA) zaifliklarni ko‘rsatgan; bu natija IV kalitga ulangan WEP rejimida kalitni tiklashga olib kelgan [5]. Mantin va Shamir ikkinchi chiqish baytining nolga teng bo‘lish ehtimoli taxminan 2/256 ekanini isbotlagan va undan ommaviy uzatish rejimida farqlovchi qurgan [6]. Sen Gupta va hammualliflar boshlang‘ich baytlarning, jumladan Z_ℓ ning 256 − ℓ qiymatiga og‘ishini nazariy jihatdan asoslagan (ℓ — kalit uzunligi, bayt) [9].

Amaliy burilish TLS bo‘yicha ishlarda yuz berdi. AlFardan va hammualliflar dastlabki 256 bayt og‘ishlaridan foydalanib, bir xil ochiq matn ko‘p marta shifrlanganda uni tiklash mumkinligini ko‘rsatgan [7]. Vanhoef va Piessens yangi uzoq muddatli og‘ishlarni topib, WPA-TKIPni buzgan va HTTPS cookie qiymatini taxminan 75 soatlik hujumda tiklagan [8]. RFC 7465 shundan keyin TLSda RC4ni taqiqlagan [4]. Demak, RC4 bo‘yicha ilmiy masala «buziladimi» emas, balki eski tizimlardan qanday xavfsiz chiqarishdir.

Trivium. Trivium 288 bitli holat, uchta nochiziqli siljish registri, 80 bitli kalit va 80 bitli IVdan foydalanadi; kalit oqimi chiqishidan oldin 1152 takt initsializatsiya bajariladi [10]. U ISO/IEC 29192-3 standartidagi yengil oqimli shifrlardan biri [11]. Asosiy hujum yo‘nalishi — kub hujumi: IV bitlarining bir qismi bo‘yicha yig‘indi olinadi va kalitga bog‘liq «superpolinom» tiklanadi [12, 13].

Kub hujumlarining rivoji initsializatsiya takti bo‘yicha o‘lchanadi. Dinur va Shamir 672 taktli variantda kalitni 2^{19} bit amalida tiklagan va 767 taktli variantni 2^{45} bit amalida buzgan [12]; Fouque va Vannet 784 va 799 taktga yetgan [14]. Bo‘linuvchanlik xossasi va monomial bashorat usullari aniq superpolinomni tiklash chegarasini 842, 848 va 851 taktga ko‘targan [15–17]. Zhang va Sun 820 va 832 taktda amaliy kalit tiklashni berib, ko‘p sonli nochiziqli superpolinomlardan foydalangan [18]. Li va hammualliflar 840 taktda 2^{55} dan past murakkablikdagi amaliy hujumni, 855 taktda esa 2^{74} ta zaif kalit uchun nazariy hujumni e’lon qilgan [19]. He, Hu va Liuning preprinti 852 taktda zaif kalitlar uchun superpolinom tiklashni ko‘rib chiqadi [20]. Kalitni tiklash natijalari 1152 taktli to‘liq Triviumdan kamida 297 takt orqada. Aumasson va hammualliflarning kub testerlari esa 790 taktgacha 2^{30} murakkablikdagi farqlovchini va 885 taktgacha 2^{27} murakkablikdagi notasodifiylikni qayd etgan [13]. Klassik 80 bitli kalit zamonaviy 128 bitli mezonga javob bermaydi.

(cc) BY

ChaCha. ChaCha 512 bitli holatda modulli qo‘shish, aylantirish va XOR (ARX) amallarini bajaradi; ChaCha20 20 raunddan, ya’ni 10 ta ustun va 10 ta diagonal raunddan iborat [1, 2]. Aumasson va hammualliflar ehtimoliy neytral bitlar (PNB) usulini kiritib, 7 raundli ChaCha uchun 2^{248} vaqt va 2^{27} ma’lumot talab qiluvchi kalit tiklashni ko‘rsatgan [21]. Differensial-chiziqli usul keyingi o‘n yillikning asosiy vositasi bo‘ldi: Beierle, Leander va Todo 7 raundli kalit tiklashni $2^{230,86}$ ga, Coutinho va Souza Neto esa $2^{228,51}$ ga tushirgan; ikkinchi ish 6 raund uchun 2^{51} dan kichik murakkablikdagi farqlovchini ham bergan [22, 23]. Bellini va hammualliflar MILP yordamida 7 raundli kalit tiklashni $2^{206,8}$ ga tushirgan [24]. Xu va hammualliflar esa 7 va 7,25 raund uchun mos ravishda $2^{189,7}$ va $2^{223,9}$ murakkablikka erishgan [25].

2023–2026-yillardagi ishlar natija va uning tekshiruvi orasidagi farqni ko‘rsatdi. Dey va Sarkar mavjud ko‘p bitli farqlovchilar ChaCha shifriga emas, faqat ChaCha permutatsiyasiga tegishli ekanini ta’kidlagan [26]. Flórez-Gutiérrez va Todo bit puncturing usulida PNB yondashuvini kuchaytirgan [27]; Tezcan, Leander va Hadipour GPUda qayta hisoblab, ayrim oldingi ChaCha va Ascon baholarini tuzatgan [28]. Beyne va hammualliflar puncturing hujumlarida parametrlarni aniq baholash usulini bergan [29], Ghafoori va Miyaji esa bog‘langan kalitli bumerang modelini 6–7 raundli permutatsiyaga qo‘llagan [30]. Okada va Miyaji 7 raundli farqlovchilarning ma’lumot talabi 2^{128} dan oshishini, shu sababli 6 raundli 2^{51} farqlovchi amaliy jihatdan eng yaxshi bo‘lib qolayotganini qayd etgan [31].

1-jadval.

Uchta oila bo‘yicha asosiy natijalar va ularning maqomi

Oila va natija	Yil	Obyekt (raund/takt)	Hujum turi	Murakkablik	Maqom
RC4, Vanhoef–Piessens [8]	2015	To‘liq, WPA-TKIP va TLS	Ochiq matnni tiklash	≈75 soat (cookie)	Amaliy, taqrizli
RC4, AlFardan va boshq. [7]	2013	To‘liq, TLS	Ochiq matnni tiklash	2^{26}–2^{32} shifrmatn	Amaliy, taqrizli
RC4, Mantin–Shamir [6]	2001	To‘liq, 2-bayt	Farqlovchi	$\approx 2^{8}$ chiqish	Amaliy, isbotlangan
Trivium, Aumasson va boshq. [13]	2009	885 / 1152 takt	Notasodifiylik (kub testeri)	2^{27}	Amaliy, taqrizli
Trivium, Li va boshq. [19]	2025	855 / 1152 takt	Kalitni tiklash	2^{74} zaif kalit	Nazariy, zaif kalit
Trivium, He–Hu–Liu [20]	2025	852 / 1152 takt	Superpolinom	Zaif kalitlar	Preprint
Trivium, He va boshq. [17]	2024	851 / 1152 takt	Kalitni tiklash (superpolinom)	Nazariy	Taqrizli
Trivium, Li va boshq. [19]	2025	840 / 1152 takt	Kalitni tiklash	$< 2^{55}$	Amaliy, taqrizli
Trivium, Zhang–Sun [18]	2024	832 / 1152 takt	Kalitni tiklash	$\leq 2^{50}$	Amaliy, taqrizli

(cc) BY

Oila va natija	Yil	Obyekt (raund/takt)	Hujum turi	Murakkablik	Maqom
ChaCha, Bellini va boshq. [24]	2023	7,5 / 20 raund	Farqlovchi	$2^{251,4}$	Nazariy, taqrizli
ChaCha, Xu va boshq. [25]	2024	7,25 / 20 raund	Kalitni tiklash	$2^{223,9}$	Nazariy, taqrizli
ChaCha, Xu va boshq. [25]	2024	7 / 20 raund	Kalitni tiklash	$2^{189,7}$	Nazariy, taqrizli
ChaCha, Coutinho–Souza Neto [23]	2021	6 / 20 raund	Farqlovchi	$< 2^{51}$	Amaliy, taqrizli

2-jadvalda bir xil murakkablik sonlarini solishtirishda saqlanishi zarur bo‘lgan shartlar jamlangan.

2-jadval.

Natijani amaliy tanlovga ko‘chirish chegarasi

Shart	RC4	Trivium	ChaCha20
Hujum obyekti	To‘liq algoritm	Qisqartirilgan initsializatsiya	Qisqartirilgan raundli shifr yoki permutatsiya
Tajovuzkor modeli	Bir matnning ko‘p shifrlanishi	Tanlangan IV, ba’zan zaif kalit	Tanlangan nonce/hisoblagich, ba’zan bog‘langan kalit
Kalitni tiklash bo‘yicha zaxira M_key	0	0,26 (851/1152)	0,64 (7,25/20)
Farqlovchi bo‘yicha zaxira M_dist	0	0,23 (885/1152)	0,625 (7,5/20)
Kalit uzunligi	40–2048 bit	80 bit	256 bit
Standart holati	TLSda taqiqlangan [4]	ISO/IEC 29192-3 [11]	RFC 8439, TLS 1.3 [1, 3]

Ilmiy bo‘shliq shundan iboratki, adabiyot hujum chegarasini juda chuqur ochib bergan, lekin turli maqomdagi natijalar yagona, takrorlanadigan ko‘rsatkich bilan bog‘lanmagan. Xususan, oddiy statistik testlar qayerda to‘xtashi va kriptotahlil undan qancha uzoqqa borishi bir xil sharoitda o‘lchanmagan. Statistik testlar kriptobardoshlik isboti o‘rnini bosmaydi [32]; aynan shuning uchun ularning chegarasi zaxira bahosi uchun pastki tayanch nuqta sifatida qiziq. Oqimli shifrlarning statistik xususiyatlarini marginal, juft va shartli mezonlar bilan baholash hamda kriptobardoshlikni statistik va kriptotahliliy usullar majmuasi asosida baholash metodikasi muallifning avvalgi ishlarida taklif qilingan [39, 40]; ushbu maqola bu yondashuvni adabiyotdagi hujum chegaralari bilan bog‘laydi.

Metodologiya

Tadqiqot ikki qismdan iborat: tanqidiy adabiyot sharhi va uchta hisoblash tajribasi (E1–E3). Sharhda IACR ePrint, IACR Transactions on

Symmetric Cryptology, LNCS (CRYPTO, EUROCRYPT, ASIACRYPT, FSE), USENIX Security, RFC Editor va ISO manbalari ko‘rib chiqildi; qidiruvning yakuniy sanasi 2026-yil 31-oktabr. Har bir manbada algoritm versiyasi, hujum modeli, natija turi va nashr maqomi alohida qayd etildi. Preprint va texnik hisobot taqrizli maqola bilan bir xil dalil maqomida berilmadi. Sharh yo‘naltirilgan bo‘lib, to‘liq sistematik sharh deb da’vo qilinmaydi.

Xavfsizlik zaxirasi hujum qilingan raund yoki takt soni R_att va to‘liq algoritmdagi R_full orqali aniqlanadi:

$$M = 1 - \frac{R_{att}}{R_{full}} \qquad (1)$$

To‘liq algoritmga qarshi amaliy hujum mavjud bo‘lsa (RC4), M = 0 deb olinadi. M faqat raund o‘lchovini ifodalaydi; murakkablik, ma’lumot hajmi va hujum modeli alohida saqlanadi (1- va 2-jadvallar).

Statistik tajribalarda bir xil qoidalar qo‘llandi. Bitli farq yoki bayt qiymati uchun og‘ish quyidagicha baholandi:

$$\varepsilon = 2Pr[\Delta = 0] - 1, \qquad z = \hat{\varepsilon}\sqrt{N} \qquad (2)$$

Bu yerda N — mustaqil namunalar soni. Ko‘p sonli kombinatsiyalar orasidan eng kuchli og‘ishni tanlash tasodifiy shovqinni ham kuchaytiradi. Shu sababli E2 va E3 da ikki bosqichli sxema ishlatildi: birinchi tanlanmada eng yaxshi kombinatsiya tanlanadi, ikkinchi, mustaqil tanlanmada uning og‘ishi qayta o‘lchanadi. Natija |z| > 5 bo‘lganda statistik ahamiyatli deb hisoblandi.

E1 — RC4 kalit oqimidagi og‘ishlar. N = 2^{24} ta tasodifiy 16 baytli kalit uchun dastlabki 256 bayt hisoblandi. Har bir r pozitsiya va v qiymat uchun nisbiy ehtimol 256·Pr[Z_r = v] baholandi; teng taqsimotda u 1 ga teng. Har bir pozitsiyada teng taqsimotga moslik χ^2 mezoni bilan, Bonferroni tuzatmasi (α = 0,001/256) bilan tekshirildi.

E2 — ChaCha permutatsiyasidagi bir bitli differensial. Kirish farqi (ID) nonce va hisoblagich so‘zlaridagi 128 bitning biriga, chiqish farqi (OD) esa r raunddan keyingi 512 bitli holatning bir bitiga qo‘yildi; yakuniy qo‘shish (feed-forward) qo‘llanmadi. r = 1…8 uchun tanlov $N_1 = 2^{16}$, 3,5 va 4 raund uchun $N_1 = 2^{20}$ namunada, tasdiqlash $N_2 = 2^{24}$ mustaqil namunada bajarildi. 3,5 raund uchun budjet ta’sirini tekshirish maqsadida tanlov $N_1 = 2^{22}$ bilan takrorlandi va eng kuchli juftlik mustaqil realizatsiya hamda boshqa seed (20261101) bilan $N_2 = 2^{30}$ namunada tasdiqlandi. Qo‘shimcha ravishda bir bitli kirish farqidan keyingi o‘rtacha Hamming og‘irligi (ko‘chki effekti) o‘lchandi.

E3 — Trivium qisqartirilgan initsializatsiyasidagi kub testeri. d o‘lchamli kub uchun IV bitlarining d tasini barcha 2^d qiymat bo‘yicha o‘zgartirib, birinchi kalit oqimi bitining XOR yig‘indisi (superpolinom qiymati) olindi. d = 1 bir bitli differensialga teng. d ∈ {1, 4, 8, 12} uchun 8 tadan tasodifiy kub tanlandi. Bitli-parallel realizatsiya bitta o‘tishda R = 0…1152 takt uchun natijani beradi. d = 1 alohida, ko‘proq namunada (har yarmida 2^{19}) ham hisoblandi.

3-jadval.

E1–E3 tajribalarining takrorlash parametrlari

Parametr	Qiymat
Protsessor va muhit	Intel Xeon 2,10 GHz, 2 vCPU, 7 GB RAM; Linux 6.18 x86-64, virtual muhit
Dasturiy qatlam	Python 3.13.18; NumPy 2.5.3; cryptography 50.0.1 (faqat tekshiruv uchun)
Realizatsiya	Vektorlashtirilgan RC4 va ChaCha; bitli-parallel Trivium (64 nusxa/so‘z)

(cc) BY

Parametr	Qiymat
To‘g‘rilik tekshiruvi	RC4: 3 ma’lum vektor; ChaCha20: RFC 8439 vektori + 200 tasodifiy taqqoslov; Trivium: 4 eSTREAM vektori
E1	$N = 2^{24}$ kalit, kalit 16 bayt, Z_1…Z_256
E2	ID: 128 bit (x12–x15), OD: 512 bit; $N_1 = 2^{16} / 2^{20}$ (3,5 raund uchun qo‘shimcha 2^{22}); $N_2 = 2^{24}$ (3,5 raund uchun qo‘shimcha 2^{30})
E3	d = 1, 4, 8, 12; har d uchun 8 kub; R = 0…1152; N = 4096 har yarmida (d = 1 da 2^{19})
Ahamiyatlilik mezoni	Mustaqil tasdiqlash tanlanmasida $\|z\| > 5$
Seed	20261031 (3,5 raundli tasdiqlash uchun 20261101)

Amalga oshirishlar test vektorlari bilan tekshirildi: RC4 uchta ma’lum vektorni, ChaCha20 RFC 8439 vektorini va cryptography kutubxonasi bilan 200 ta tasodifiy taqqoslovni, Trivium esa to‘rtta eSTREAM vektorini to‘liq qaytardi. Bitli-parallel Trivium mos yozuvli realizatsiya bilan 0 dan 1190 gacha bo‘lgan taktlarda solishtirildi. Sonli natijalar faqat bajarilgan dastur chiqishidan olindi; matn, kod va grafiklarni tayyorlashda sun’iy intellekt yordamchisidan foydalanildi. Real kalitlar yoki shaxsga doir ma’lumotlar ishlatilmadi.

Natijalar

Uchala tajriba bir xil xulosaga olib keldi: arzon, umumiy statistik testlar RC4 ni to‘liq ko‘rinishida, Trivium ni 651 taktgacha va ChaCha ni 3 raundgacha ($N = 2^{30}$ budjetda 3,5 raundgacha) ajratadi. Bu chegaralar adabiyotdagi eng chuqur natijalardan ancha past, lekin ular takrorlanadigan va bir xil protokol bilan olingan.

RC4 (E1). $N = 2^{24}$ ta 16 baytli kalitda ikkinchi baytning nolga teng bo‘lish ehtimoli nazariy 2/256 ga deyarli aynan mos keldi. 16-pozitsiyada kalit uzunligiga bog‘liq og‘ish ham aniq ko‘rindi. Boshqa tanlangan qiymatlar uchun og‘ish shu namuna hajmida ahamiyatli bo‘lmadi; nisbiy og‘ishning standart xatosi $\sigma = 0{,}0039$ ni tashkil etdi. Hisob 1151 soniya davom etdi.

4-jadval.

RC4 kalit oqimidagi pozitsion og‘ishlar ($N = 2^{24}$ kalit, $\ell = 16$ bayt)

Hodisa	256·Pr (o‘lchangan)	Kutilgan	z
$Z_2 = 0$	1,9988	≈ 2 [6]	256,2
$Z_{16} = 240$ $(256 - \ell)$	1,0409	> 1 [9]	10,5
$Z_1 = 0$	0,9962	≈ 1	−1,0
$Z_{10} = 10$	1,0097	> 1 [9]	2,5
$Z_{100} = 100$	1,0014	> 1 [9]	0,3

Pozitsiyalar bo‘yicha χ^2 testi (255 erkinlik darajasi, kritik qiymat 368,9) 256 pozitsiyadan faqat bittasida — r = 2 da ($\chi^2 = 65\,962{,}7$) — teng taqsimot gipotezasini rad etdi. 16-pozitsiyada $\chi^2 = 351{,}6$ bo‘lib, kritik qiymatdan past qoldi, garchi aniq $Z_{16} = 240$ hodisasi z = 10,5 bilan ajralsa ham. Demak, 256 qiymatga «yoyilgan» umumiy test bitta qiymatga

(cc) BY

to‘plangan og‘ishni sezmaydi; maqsadli gipoteza testi bir xil ma’lumotda kuchliroq.

ChaCha (E2). Bir bitli kirish farqidan keyin o‘zgargan chiqish bitlari ulushi 1 raundda 0,041, 2 raundda 0,315, 3 raundda 0,4995 bo‘ldi va 4 raunddan boshlab 0,5000 ga yetdi. Bir bitli differensial og‘ish 3 raundda ham kuchli saqlandi. 3,5 raundda $N_1 = 2^{20}$ tanlov va $N_2 = 2^{24}$ tasdiqlash ahamiyatli og‘ish bermadi. Tanlov $N_1 = 2^{22}$ bilan takrorlanganda topilgan x12[22] → x1[16] juftligi esa mustaqil $N_2 = 2^{30}$ namunada $\varepsilon = 2{,}39 \cdot 10^{-4}$ ($z = 7{,}8$) og‘ishni ko‘rsatdi (5-jadval). Bunday og‘ishni $z = 5$ darajada ajratish uchun taxminan $2^{28{,}6}$ namuna kerak; shu sababli ChaCha uchun R_det namuna hajmiga bog‘liq: $N = 2^{24}$ da 3, $N = 2^{30}$ da 3,5 raund. 4 raund va undan keyin hech bir budjetda og‘ish topilmadi. Tanlov bosqichidagi shovqin chegarasi $N_1 = 2^{16}$ da ≈ 0,018, $N_1 = 2^{20}$ da ≈ 0,0045 ni tashkil etdi.

5-jadval.

ChaCha permutatsiyasida ko‘chki effekti va eng kuchli bir bitli differensial

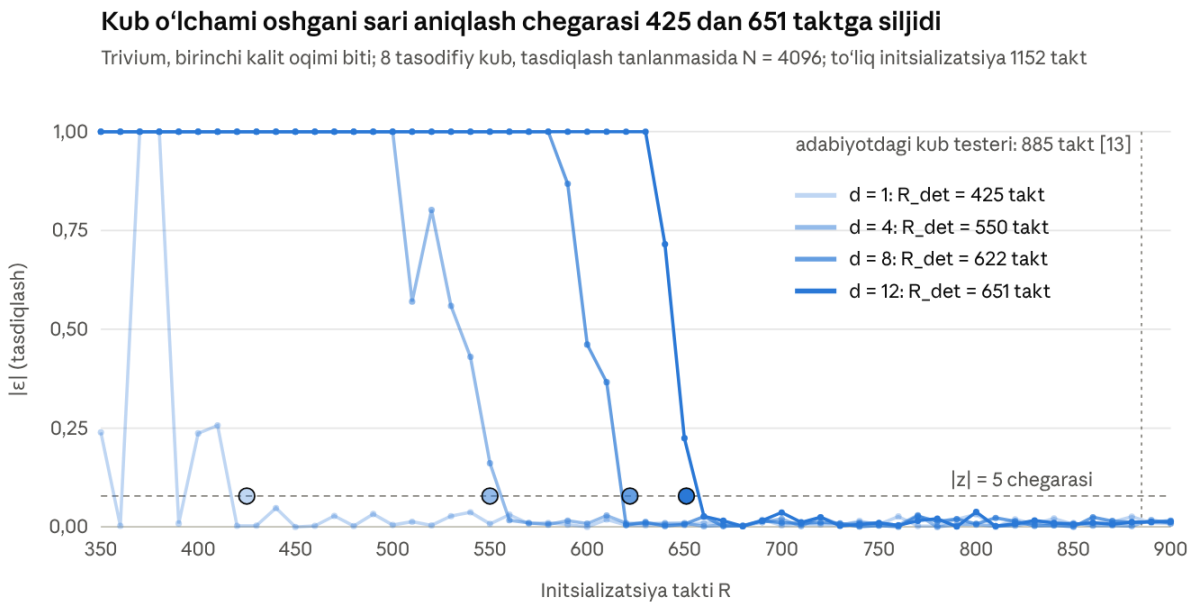
Raund	Ko‘chki: o‘rtacha / minimal	ID → OD	ε (tasdiq)	N_2	z
1	0,0411 / 0,0329	x12[0] → x0[14]	0,99996	2^{24}	4 095,8
2	0,3152 / 0,2861	x12[0] → x0[15]	0,99996	2^{24}	4 095,8
3	0,4995 / 0,4987	x15[21] → x1[0]	0,1976	2^{24}	809,3
3,5	—	x15[14] → x10[11] (tanlov 2^{20})	−0,00009	2^{24}	−0,4
3,5	—	x12[22] → x1[16] (tanlov 2^{22})	0,00024	2^{30}	7,8
4	0,5000 / 0,4997	x13[3] → x9[5]	−0,00009	2^{24}	−0,4
5–8	0,5000 / 0,4998	tanlovda topilgan juftlar	$\lvert\varepsilon\rvert \le 0{,}0003$	2^{24}	$\lvert z\rvert \le 1{,}1$

3 raundda ko‘chki effekti deyarli ideal bo‘lsa ham, alohida bitlar orasidagi bog‘lanish kuchli saqlanadi. Bu o‘rtacha ko‘chki ko‘rsatkichi diffuziya sifatini baholash uchun yetarli emasligini ko‘rsatadi.

Trivium (E3). Barcha 80 ta IV biti tekshirilgan bir bitli differensialda (har yarmida $N = 2^{19}$) og‘ish 420 taktgacha juda kuchli bo‘ldi: R = 400 da $\varepsilon = -0{,}249$ ($z = -180$), R = 420 da $\varepsilon = -0{,}252$ ($z = -183$). Keyin u keskin kamaydi: R = 440 da $\varepsilon = 0{,}046$ ($z = 33$), R = 460 da $\varepsilon = 0{,}016$ ($z = 11$), R = 480 da $\varepsilon = 0{,}0015$ ($z = 1{,}1$). $|z| > 5$ shartini qanoatlantirgan oxirgi takt R = 497 bo‘ldi.

Kub o‘lchami oshgan sari aniqlash chegarasi ham oshdi: 8 ta tasodifiy kub va har yarmida N = 4096 bilan d = 1, 4, 8 va 12 uchun R_det mos ravishda 425, 550, 622 va 651 taktni tashkil etdi (1-rasm). d = 1 dan 12 gacha o‘tishda chegara 226 taktga siljidi, lekin har bosqichdagi qo‘shimcha o‘sish 125, 72 va 29 taktgacha kamaydi. d = 1 dagi 425 va to‘liq skanerdagi 497 orasidagi farq test budjetining ta’siri: birinchisida 8 ta IV biti va kichikroq N ishlatilgan.

(cc) BY



1-rasm. Trivium kub testerida aniqlash chegarasining kub o‘lchami d ga bog‘liqligi (E3).

d = 1 egri chizig‘idagi keskin sakrashlar har bir R uchun eng yaxshi bitning alohida tanlanishidan kelib chiqadi.

6-jadvalda uchala oila bo‘yicha zaxiralar jamlangan. R_att uchun adabiyotdagi eng chuqur kalit tiklash va farqlovchi natijalari alohida olingan (1-jadval).

6-jadval.

Xavfsizlik zaxirasi va statistik aniqlash chegarasi

Oila	R_full	R_att: kalit tiklash	R_att: farqlovchi	R_det (bu ish)	M_key	M_dist	M_det
RC4	to‘liq	to‘liq [7, 8]	to‘liq [6]	to‘liq (Z_2, Z_{16})	0	0	0
Trivium	1152 takt	851 [17] (855 zaif kalit [19])	885 [13]	651 (d = 12)	0,26	0,23	0,43
ChaCha20	20 raund	7,25 [25]	7,5 [24]	3 ($N = 2^{24}$); 3,5 ($N = 2^{30}$)	0,64	0,625	0,85; 0,825

Farqlovchi va bizning testlarimiz orasidagi masofa nisbiy o‘lchovda ikki oilada yaqin chiqdi: Trivium uchun (885 − 651)/1152 = 0,20, ChaCha20 uchun $N = 2^{30}$ budjetda (7,5 − 3,5)/20 = 0,20 ($N = 2^{24}$ da 0,225). Ya’ni ixtisoslashgan kriptotahlil umumiy, arzon testlardan to‘liq algoritm uzunligining taxminan beshdan bir qismi chuqurroq boradi.

Muhokama

Olingan natijalar uchta oilada xavfsizlik holati turli tabiatga ega ekanini ko‘rsatadi. RC4 da muammo algoritmning o‘zida: og‘ishlar to‘liq algoritmda, oddiy hisoblash resursida va kichik namunalarda ham ko‘rinadi. Trivium va ChaCha20 da esa barcha ma’lum hujumlar qisqartirilgan variantlarga tegishli; ular orasidagi farq zaxira hajmida va hujum modelida.

(cc) BY

Zaxirani o‘lchash usuli. Bitta «hujum qilingan raund» soni yetarli emas. ChaCha20 da 7,5 raundli farqlovchi $2^{251,4}$ murakkablikka ega va amaliy ma’lumot chegarasidan ancha uzoq; 6 raundli 2^{51} farqlovchi esa amalda bajariladigan eng chuqur natija bo‘lib qolmoqda [23, 24, 31]. Trivium da 885 taktli notasodifiylik 2^{27} murakkablikda kuzatiladi, lekin u kalitni tiklash emas [13]. Shu sababli 6-jadvalda M_key va M_dist alohida berildi; ular orasidagi farq Trivium da 0,03, ChaCha20 da 0,015 ni tashkil etadi.

Statistik chegara ham parametr. E1–E3 natijalari aniqlash chegarasi testning o‘ziga ham bog‘liqligini ko‘rsatdi. RC4 da umumiy χ^2 testi faqat ikkinchi baytni rad etdi, maqsadli test esa 16-baytdagi og‘ishni ham aniqladi. Trivium da kub o‘lchamini 1 dan 12 gacha oshirish R_det ni 226 taktga surdi, kub testerlari adabiyotda 885 taktgacha yetgan [13]. ChaCha da 3 raunddagi o‘rtacha ko‘chki deyarli ideal bo‘lsa-da, bitli differensial og‘ish $\varepsilon = 0{,}198$ saqlanib qoldi; 3,5 raunddagi og‘ish esa $N = 2^{24}$ da ko‘rinmadi va faqat $N = 2^{30}$ da $z = 7{,}8$ bilan aniqlandi. Demak, R_det ni hisobot qilishda test turi, namuna hajmi va ko‘p testlash tuzatmasi albatta ko‘rsatilishi kerak.

Ilmiy bo‘shliq. Tahlil asosida quyidagi aniq bo‘shliqlar ajratildi. Ular «Oqimli shifrlash algoritmlarining ichki parametrlarini tanlash va takomillashtirish usullari hamda ularning kriptografik va hisoblash xususiyatlarini baholash» mavzusidagi tadqiqotning keyingi bosqichlari vazifalarini belgilaydi:

1. Ichki parametrlarni (raund yoki takt soni, registr uzunligi va taplar, aylantirish konstantalari, almashtirish o‘lchami N, tashlab yuboriladigan baytlar soni) bir vaqtda kriptografik ko‘rsatkichlar (M_key, M_dist, M_det) va hisoblash ko‘rsatkichlari (sikl/bayt, ishga tushirish xarajati, xotira, apparat maydoni) bilan bog‘laydigan yagona, takrorlanadigan baholash protokoli mavjud emas.

2. Trivium variantlar fazosi (Bivium, Kreyvium, qisqartirilgan initsializatsiya, 128 bitli kalit varianti) bir xil test va bir xil budjet bilan solishtirilmagan; 1152 takt va tap pozitsiyalari tanlovi tasodifiy konfiguratsiyalar fonida miqdoriy baholanmagan.

3. RC4 variantlari (drop-n, RC4A, VMPC, RC4+, Spritz) uchun pozitsion og‘ishlar va realizatsiya darajasidagi oqish (maxfiy holatga bog‘liq xotira murojaati) bir xil protokolda o‘lchanmagan; eski tizimlardan chiqish uchun asoslangan mezon yo‘q.

4. ChaCha da aylantirish konstantalari va raund soni tanlovining dalil bazasi asosan muallif dizayni va hujum natijalariga tayanadi; umumiy testlar (3–3,5 raund) va ixtisoslashgan hujumlar (7–7,5 raund) orasidagi 4–4,5 raundlik oraliqni neyron va rotatsion usullar qanchalik qoplashi baholanmagan.

5. NIST SP 800-22 kabi bitta uzun oqimga mo‘ljallangan testlar ko‘p kalitli pozitsion og‘ishlarni qay darajada ko‘rishi va bunday og‘ishlar uchun zarur namuna hajmi tizimli o‘rganilmagan [32].

Amaliy ma’no. O‘zbekiston raqamli tizimlari uchun xulosa uchta qismdan iborat. Yangi tizimlarda RC4 ishlatilmasligi kerak; mavjud bo‘lsa, protokol darajasida almashtirish rejasi tuziladi [4]. Trivium faqat apparat cheklangan profilda va 80 bitli kalit cheklovi hisobga olingan holda ko‘rib chiqiladi; 128 bitli talab bo‘lsa, Ascon kabi standartlashgan yengil AEAD muqobil sifatida baholanadi [35]. Dasturiy xizmatlarda ChaCha20-Poly1305 standart profil sifatida qoladi [1, 3]. Bu tavsiyalar qonunchilikdagi umumiy talablarni texnik jihatdan to‘ldiradi, lekin muayyan obyekt uchun sertifikatlash yoki huquqiy muvofiqlik xulosasi o‘rnini bosmaydi [33, 34].

Cheklovlar. Statistik tajribalar bitta virtual muhitda, bitta seed bilan bajarildi. R_det qiymatlari tanlangan test va namuna hajmiga bog‘liq: Trivium da faqat birinchi kalit oqimi biti va tasodifiy kublar, ChaCha da yakuniy qo‘shimchasiz permutatsiya, RC4 da faqat 16 baytli kalitlar tekshirildi. Adabiyot qidiruvi yo‘naltirilgan bo‘lib, sistematik sharh emas; adabiyotdagi murakkablik qiymatlari mualliflar e’lon qilgan shaklda olindi va bu ishda qayta tekshirilmadi. Shu sababli 6-jadvaldagi

zaxiralar taqqoslash vositasi bo‘lib, xavfsizlik isboti emas.

Xulosa

RC4, Trivium va ChaCha oilalari bo‘yicha natijalar hujum turi, obyekt, murakkablik va nashr maqomi bo‘yicha ajratilganda xavfsizlik holati aniq farqlanadi. RC4 to‘liq algoritmda amaliy hujumlarga ega va TLSda taqiqlangan. Trivium uchun kalitni tiklash 851 taktgacha (zaif kalitlar uchun 855 taktgacha), notasodifiylik 885 taktgacha yetgan; zaxira M_key = 0,26 va M_dist = 0,23. ChaCha20 uchun kalitni tiklash 7,25 raundgacha, farqlovchi 7,5 raundgacha ma’lum; zaxira M_key = 0,64 va M_dist = 0,625.

Bir xil seed va tekshirilgan realizatsiyalarda bajarilgan tajribalar statistik aniqlash chegarasini o‘lchadi. RC4 da $N = 2^{24}$ kalit ikkinchi baytdagi og‘ishni $256 \cdot \Pr[Z_2 = 0] = 1{,}9988$ ($z = 256{,}2$) va 16-baytdagi og‘ishni $z = 10{,}5$ bilan aniqladi. ChaCha da bir bitli differensial 3 raundda $\varepsilon = 0{,}198$ bilan saqlandi; 3,5 raunddagi $\varepsilon = 2{,}4 \cdot 10^{-4}$ og‘ish faqat $N = 2^{30}$ tanlanmada aniqlandi, 4 raunddan keyin esa topilmadi. Trivium da kub testerining chegarasi d = 1 dan 12 gacha 425 dan 651 taktga oshdi.

Umumiy testlar va eng yaxshi ixtisoslashgan natijalar orasidagi nisbiy masofa Trivium da 0,20, ChaCha20 da $N = 2^{30}$ budjetda 0,20 ($N = 2^{24}$ da 0,225) ni tashkil etdi. Bu masofa ichki parametrlarni, avvalo raund soni va initsializatsiya taktini, faqat umumiy statistik testlar asosida tanlash xavfli ekanini ko‘rsatadi. Shu bilan birga, tajriba chegarasi test turi va namuna hajmiga bog‘liq bo‘lgani uchun u hisobotda doim ko‘rsatilishi kerak.

Ajratilgan beshta ilmiy bo‘shliq oqimli shifrlarning ichki parametrlarini tanlash va takomillashtirish bo‘yicha keyingi tadqiqot vazifalarini belgilaydi: yagona baholash protokoli, Trivium va RC4 variantlar fazosini bir xil sharoitda solishtirish, ChaCha parametrlari tanlovining dalil bazasini kengaytirish hamda ko‘p kalitli pozitsion testlarning o‘rnini aniqlash. Bu vazifalar kriptografik va hisoblash ko‘rsatkichlarini bitta tanlash qoidasida birlashtirishga xizmat qiladi.

Foydalanilgan adabiyotlar

1. Nir Y., Langley A. ChaCha20 and Poly1305 for IETF Protocols. RFC 8439. 2018. https://www.rfc-editor.org/rfc/rfc8439
2. Bernstein D. J. ChaCha, a variant of Salsa20. Workshop Record of SASC 2008. https://cr.yp.to/chacha/chacha-20080128.pdf
3. Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446. 2018. https://www.rfc-editor.org/rfc/rfc8446
4. [4] Popov A. Prohibiting RC4 Cipher Suites. RFC 7465. 2015. https://datatracker.ietf.org/doc/html/rfc7465
5. Fluhrer S., Mantin I., Shamir A. Weaknesses in the Key Scheduling Algorithm of RC4. SAC 2001, LNCS 2259. 2001:1–24. DOI 10.1007/3-540-45537-X_1. https://doi.org/10.1007/3-540-45537-X_1
6. Mantin I., Shamir A. A Practical Attack on Broadcast RC4. FSE 2001, LNCS 2355. 2002:152–164. DOI 10.1007/3-540-45473-X_13. https://doi.org/10.1007/3-540-45473-X_13
7. AlFardan N., Bernstein D. J., Paterson K. G., Poettering B., Schuldt J. C. N. On the Security of RC4 in TLS. 22nd USENIX Security Symposium. 2013. https://usenix.org/conference/usenixsecurity13/security-rc4-tls
8. Vanhoef M., Piessens F. All Your Biases Belong to Us: Breaking RC4 in WPA-TKIP and TLS. 24th USENIX Security Symposium. 2015:97–112. https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/vanhoef
9. Sen Gupta S., Maitra S., Paul G., Sarkar S. (Non-)Random Sequences from (Non-)Random Permutations — Analysis of RC4 Stream Cipher. Journal of Cryptology. 2014;27(1):67–108. DOI 10.1007/s00145-012-9138-1. https://eprint.iacr.org/2011/448
10. De Cannière C., Preneel B. Trivium Specifications. eSTREAM, ECRYPT Stream Cipher Project. 2005. https://web.archive.org/web/20161020205326/http://www.ecrypt.eu.org/stream/ciphers/trivium/trivium.pdf

(cc) BY *dtai.uz*

11. ISO/IEC 29192-3:2012. Information technology — Security techniques — Lightweight cryptography — Part 3: Stream ciphers. 2012. https://www.iso.org/standard/56426.html
12. Dinur I., Shamir A. Cube Attacks on Tweakable Black Box Polynomials. EUROCRYPT 2009, LNCS 5479. 2009:278–299. DOI 10.1007/978-3-642-01001-9_16. https://eprint.iacr.org/2008/385
13. Aumasson J.-P., Dinur I., Meier W., Shamir A. Cube Testers and Key Recovery Attacks on Reduced-Round MD6 and Trivium. FSE 2009, LNCS 5665. 2009:1–22. DOI 10.1007/978-3-642-03317-9_1. https://drops.dagstuhl.de/entities/document/10.4230/DagSemProc.09031.6
14. Fouque P.-A., Vannet T. Improving Key Recovery to 784 and 799 Rounds of Trivium Using Optimized Cube Attacks. FSE 2013, LNCS 8424. 2014:502–517. DOI 10.1007/978-3-662-43933-3_26. https://doi.org/10.1007/978-3-662-43933-3_26
15. Hao Y., Leander G., Meier W., Todo Y., Wang Q. Modeling for Three-Subset Division Property without Unknown Subset: Improved Cube Attacks against Trivium and Grain-128AEAD. EUROCRYPT 2020. Kengaytirilgan versiya: Cryptology ePrint Archive 2020/441. https://eprint.iacr.org/2020/441
16. He J., Hu K., Preneel B., Wang M. Stretching Cube Attacks: Improved Methods to Recover Massive Superpolies. ASIACRYPT 2022. Cryptology ePrint Archive 2022/1218. https://eprint.iacr.org/2022/1218
17. He J., Hu K., Lei H., Wang M. Massive Superpoly Recovery with a Meet-in-the-Middle Framework — Improved Cube Attacks on Trivium and Kreyvium. EUROCRYPT 2024. DOI 10.1007/978-3-031-58716-0_13. https://eprint.iacr.org/2024/342
18. Zhang M., Sun Y. A New Practical Cube Attack via Recovering Numerous Superpolys. IACR Transactions on Symmetric Cryptology. 2024(4):38–63. DOI 10.46586/tosc.v2024.i4.38-63. https://doi.org/10.46586/tosc.v2024.i4.38-63
19. Li H., Wang S., Liu M. va boshq. Cube Attacks with Elimination Strategy: Key Recovery Attacks on Trivium. IACR Transactions on Symmetric Cryptology. 2025(4):308–356. DOI 10.46586/tosc.v2025.i4.308-356. https://doi.org/10.46586/tosc.v2025.i4.308-356
20. He J., Hu K., Liu G. Exploring Core Monomial Prediction Further: Weak-Key Superpoly Recovery for 852-Round Trivium. Cryptology ePrint Archive, Paper 2025/1330. 2025. Foydalanilgan versiya: preprint. https://eprint.iacr.org/2025/1330
21. Aumasson J.-P., Fischer S., Khazaei S., Meier W., Rechberger C. New Features of Latin Dances: Analysis of Salsa, ChaCha, and Rumba. FSE 2008, LNCS 5086. 2008:470–488. Kengaytirilgan versiya: ePrint 2007/472. https://eprint.iacr.org/2007/472
22. Beierle C., Leander G., Todo Y. Improved Differential-Linear Attacks with Applications to ARX Ciphers. CRYPTO 2020. Kengaytirilgan versiya: ePrint 2020/775. https://eprint.iacr.org/2020/775
23. Coutinho M., Souza Neto T. C. Improved Linear Approximations to ARX Ciphers and Attacks Against ChaCha. EUROCRYPT 2021. Cryptology ePrint Archive 2021/224. https://eprint.iacr.org/2021/224
24. Bellini E., Gerault D., Grados J., Makarim R. H., Peyrin T. Boosting Differential-Linear Cryptanalysis of ChaCha7 with MILP. IACR Transactions on Symmetric Cryptology. 2023(2):189–223. DOI 10.46586/tosc.v2023.i2.189-223. https://tosc.iacr.org/index.php/ToSC/article/view/10983

(cc) BY *dtai.uz*

25. Xu Z., Xu H., Tan L., Qi W. Differential-Linear Cryptanalysis of Reduced Round ChaCha. IACR Transactions on Symmetric Cryptology. 2024(2):166–189. DOI 10.46586/tosc.v2024.i2.166-189. https://tosc.iacr.org/index.php/ToSC/article/view/11626
26. Dey C., Sarkar S. A New Distinguishing Attack on Reduced Round ChaCha Permutation. Scientific Reports. 2023;13. DOI 10.1038/s41598-023-39849-1. https://doi.org/10.1038/s41598-023-39849-1
27. Flórez-Gutiérrez A., Todo Y. Improved Cryptanalysis of ChaCha: Beating PNBs with Bit Puncturing. EUROCRYPT 2025, Part I, LNCS 15601. 2025:427–457. DOI 10.1007/978-3-031-91107-1_15. https://eprint.iacr.org/2025/437
28. Tezcan C., Leander G., Hadipour H. Cryptanalysis: Theory Versus Practice — Correcting Cryptanalysis Results on Ascon, ChaCha, and Serpent Using GPUs. IACR Transactions on Symmetric Cryptology. 2025(3):729–754. DOI 10.46586/tosc.v2025.i3.729-754. https://doi.org/10.46586/tosc.v2025.i3.729-754
29. Beyne T., Flórez-Gutiérrez A., Todo Y. Accurate Parameter Estimates for Punctured Key Recovery Linear Attacks. IACR Communications in Cryptology. 2026;3(2). DOI 10.62056/ava3z11w9p. https://doi.org/10.62056/ava3z11w9p
30. Ghafoori N., Miyaji A. The Related Key Boomerang Attack on ChaCha Permutation Function. Pragmatic Cybersecurity. 2026;1(2):16. DOI 10.53941/pc.2026.100016. https://doi.org/10.53941/pc.2026.100016
31. Okada Y., Miyaji A. Revisitied Distinguishers for Stream Cipher ChaCha. IEICE Technical Report, ISEC2025-132. 2026;125(405):290–297. Foydalanilgan versiya: texnik hisobot. https://ken.ieice.org/ken/paper/202603176ctX/
32. Rukhin A. va boshq. 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. https://doi.org/10.6028/NIST.SP.800-22r1a
33. O‘zbekiston Respublikasining «Shaxsga doir ma’lumotlar to‘g‘risida»gi O‘RQ-547-son Qonuni. 02.07.2019. https://lex.uz/docs/4396419
34. O‘zbekiston Respublikasining «Kiberxavfsizlik to‘g‘risida»gi O‘RQ-764-son Qonuni. 15.04.2022. https://lex.uz/uz/docs/5960604
35. Sönmez Turan M., 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. https://doi.org/10.6028/NIST.SP.800-232
36. Xudoyqulov Z. T., Rahmatullayev I. R. Mavjud oqimli shifrlash algoritmlarining qiyosiy tahlili. Al-Farg‘oniy avlodlari. 2024;1(1):129–134.
37. Rahmatullayev I. R. Mavjud sinxron oqimli shifrlash algoritmlarining qiyosiy tahlili. Mexanika va texnologiya. 2024;5(2):236–243.
38. Rakhmatullaev I. R., Boykuziev I. M. Analysis of cryptanalysis methods applied to stream encryption algorithms. In: Artificial Intelligence, Blockchain, Computing and Security, Vol. 1. CRC Press; 2023:393–401.
39. Rahmatullayev I., Abduraximov B. Oqimli shifrlash algoritmlarining kriptobardoshligini kompleks baholash metodologiyasi. Al-Fargoniy avlodlari. 2026;(3):607–615. https://al-fargoniy.uz/index.php/journal/article/view/514
40. Rahmatullayev I. Oqimli shifrlarning statistik xususiyatlarini kompleks baholash: marginal, juft va shartli mezonlarning qiyosiy tahlili. Al-Fargoniy avlodlari. 2026;(3):616–628. https://al-fargoniy.uz/index.php/journal/article/view/1344

(cc) BY *dtai.uz*