ISSN: 3030-3346

OQIMLI SHIFRLASH ALGORITMLARINI QIYOSIY BAHOLASH VA O‘ZBEKISTON RAQAMLI TIZIMLARI UCHUN TANLASH METODIKASI

Rahmatullayev Ilhom Raxmatullayevich

Toshkent Kimyo xalqaro universiteti Samarqand filiali, Samarqand, O‘zbekiston,
E-mail: ilhom9001@gmail.com

K E Y W O R D S

oqimli shifr; ChaCha20-Poly1305; AEAD; kriptotahlil; nonce; telemetriya; hisoblash tajribasi; O‘zbekiston

A B S T R A C T

Tadqiqotning maqsadi mavjud algoritmlar tahlilini O‘zbekiston raqamli xizmatlari va telemetriya tizimlari uchun tekshiriladigan tanlash mezonlariga aylantirishdir. Metodologiya 2024–2026-yillardagi kriptotahlilni tanqidiy ko‘rib chiqish, uchta AEAD konfiguratsiyasini bir xil muhitda o‘lchash, paket ustamasini analitik hisoblash va nonce hisoblagichini uzilishlarda tiklash simulyatsiyasini birlashtiradi. Intel Xeon Platinum 8573C serverida 16–65 536 baytli xabarlar uchun 810 ta o‘lchov seriyasi bajarildi. 32 baytda ChaCha20-Poly1305 va AES-256-GCM median vaqtlari mos ravishda 1,489 va 0,516 mikrosekundni tashkil etdi. Paket modeli 32 baytli davriy o‘lchovlarda 10 foizlik kriptografik ustama va 5 soniyalik kutish chegarasini birgalikda bajarib bo‘lmasligini, 64 baytda esa beshta o‘lchovni birlashtirish bilan bajarilishini ko‘rsatdi. Har biri 100 000 xabardan iborat 100 ta uzilish ssenariysida 256 qiymatli oraliqni oldindan saqlash nonce takrorlanishini bartaraf etdi; foydalanilgan holatni keyin saqlash siyosatida takroriy nonce medianasi 12 092 bo‘ldi. Ishning hissasi tezlik, paket va holat boshqaruvini aniq cheklovlar ostida bog‘lovchi hisoblash metodikasidir. Natijalar server tajribasi va berilgan model shartlariga tegishli; mahalliy sensorlarda energiya yoki apparat maydoni o‘lchovi sifatida talqin qilinmaydi.

Kirish

Oqimli shifrlash algoritmlarining afzalligi ko‘pincha yuqori tezlik va ixcham realizatsiya bilan izohlanadi. Biroq amaliy tizimda tezkor shifr tanlanishi axborot himoyasi to‘liq ta’minlanganini anglatmaydi. Autentifikatsiyasiz shifrlash xabarning yashirinligini saqlashi mumkin, lekin uning o‘zgartirilmaganini tasdiqlamaydi. Nonce — bir kalit ostida takrorlanmasligi kerak bo‘lgan boshlang‘ich qiymat — noto‘g‘ri boshqarilsa, matematik jihatdan kuchli konstruksiyaning amaliy xavfsizligi ham buziladi. Shu sababli algoritm, uni ishlatish rejimi va tizimning ekspluatatsiya shartlari birgalikda tadqiq etilishi lozim [1, 2].

O‘zbekistonda ushbu masalaning dolzarbligi aniq infratuzilma ko‘rsatkichlari bilan asoslanadi. Milliy statistika qo‘mitasi 2025-yil yakuniga mobil internet abonentlari soni 33,3 millionga yetganini ma’lum qilgan [3]. Suv xo‘jaligi vazirligining 2025-yil 12-dekabrdagi axborotida 13 254 ta suv olish nuqtasiga «Aqlli suv», 10 983 ta kuzatuv qudug‘iga DIVER va 1 749 ta nasos stansiyasiga monitoring qurilmalari o‘rnatilgani qayd etilgan [4]. Bu ko‘rsatkichlar ko‘p sonli masofaviy xabar manbalarining mavjudligini tasdiqlaydi. Ular qurilmalarning amaldagi shifri, protsessori yoki energiya sarfi haqida ma’lumot bermaydi; texnik talab aynan shunday ma’lumotlar bilan keyingi bosqichda aniqlashtiriladi.

Muammo shundaki, algoritmning adabiyotdagi katta bufer uchun o‘lchangan tezligi qisqa telemetriya xabarining umumiy xarajatini ifodalamaydi. Xuddi shuningdek, kalit uzunligi

(cc) BY

nonce saqlashdagi xatoni yoki qayta yuborilgan xabarni qabul qilish xavfini qoplamaydi. Mobil va bank xizmatlarida standart protokolga moslik, telemetriyada esa kichik paket va uzilishdan keyingi tiklanish tanlovni o‘zgartiradi. Bir xil nomdagi algoritm turli kutubxona va protsessorda turlicha natija berishi ham muhim.

Tadqiqotning maqsadi mavjud oqimli shifrlarni zamonaviy kriptotahlil asosida baholash va O‘zbekistonning raqamli tizimlari uchun algoritm tanlashni qayta tekshiriladigan hisoblash masalasiga aylantirishdir. Buning uchun uch savol qo‘yildi: bir xil dasturiy muhitda AEAD konstruksiyalarining xabar uzunligiga bog‘liq xarajati qanday; qisqa paketlarda ustama va kechikish cheklovlari qachon birgalikda bajariladi; uzilishlarda nonce yagonaligini saqlash qancha doimiy xotira yozuvini talab qiladi?

Ishning ilmiy-amaliy hissasi uchta bog‘langan natijadan iborat: versiya va hujum modelini hisobga oluvchi algoritmlar taqqoslovi; paket ustamasi va kutish chegarasi uchun bajariluvchanlik sharti; bir xil uzilish izlari ostida hisoblagichni saqlash siyosatlarining miqdoriy taqqoslovi. Yangi kriptografik primitiv yoki ilgari noma’lum hujum taklif qilinmaydi. Hisoblagichni oldindan saqlash g‘oyasi mavjud standartlardagi yondashuvlar bilan bog‘lanadi [2]; bu ish uning aniq parametrlar ostidagi tizim xarajatini o‘rganadi.

Adabiyotlar tahlili

Salsa20 va ChaCha modulli qo‘shish, bitli aylantirish hamda XOR amallariga tayanuvchi ARX oilasiga mansub [1, 5]. ChaCha20ning IETF varianti 256 bitli kalit va 96 bitli nonce ishlatadi. Uning Poly1305 bilan birlashtirilgan shakli shifrlangan matnga autentifikatsiya tegini qo‘shadi. TLS 1.3dagi aniq profil va tayyor kutubxonalar ushbu konstruksiyani mobil va veb xizmatlar uchun amaliy nomzod qiladi [6, 7]. Lekin ARX tuzilishining o‘zi har qanday protsessorda eng katta tezlikni kafolatlamaydi.

Rabbit va HC-128 dasturiy oqimli shifrlar bo‘lib, har ikkalasi ham 128 bitli kalitdan foydalanadi [8, 9]. Rabbitdagi 64 bitli IV va HC-128ning jami 4096 baytli ichki jadvallari ekspluatatsiya hamda xotira cheklovlarini alohida baholashni talab qiladi. Ularning xom shifrlash tezligini AEAD konstruksiyasining to‘liq tezligi bilan teng sharoitdagi natija sifatida solishtirib bo‘lmaydi: autentifikatsiya vazifasi ham bajarilishi kerak.

Triviumning 288 bitli holati va uch registrli tuzilishi ixcham apparat realizatsiyalarini o‘rganishda muhim etalondir. Klassik konfiguratsiyaning 80 bitli kaliti esa ushbu tadqiqotda tanlangan kamida 128 bitli kalit mezoniga javob bermaydi [10]. Bu — parametrga asoslangan saralash; to‘liq Trivium amalda buzilgan degan xulosa emas. Grain-128AEADv2 128 bitli kalit, 96 bitli nonce va 64 bitli teg bilan autentifikatsiyani o‘z ichiga oladi [11]. Teg uzunligi sababli uni 128 bitli tegli konstruksiyalar bilan bir xil qalbakilashtirish budjetiga ega deb qabul qilish mumkin emas.

SNOW 3G va ZUC mobil aloqa standartlaridagi maxfiylik hamda yaxlitlik profillari bilan bog‘langan [12, 13]. SNOW-V esa vektorli qayta ishlash va AES raund buyruqlaridan foydalanishga yo‘naltirilgan [14]. Bu konstruksiyalarning vazifasi operator tarmog‘i yoki yuqori tezlikdagi dasturiy platforma bo‘lib, ularni kichik sensor mikrokontrolleriga avtomatik tavsiya etish asossiz. 1-jadvalda nomzodlarning vazifasi, parametri va tanlovdagi asosiy cheklovi ajratilgan.

1-jadval.

Algoritm konfiguratsiyalari va tanlovdagi cheklovlar

Konstruksiya Construction	Kalit / nonce Key / nonce, bit	Autentifikatsiya Authentication	Vazifa va cheklov Use and constraint
Salsa20/20 [5]	128 yoki 256 / 64	Alohida talab etiladi	ARX dasturiy etaloni; AEAD emas

(cc) BY

Konstruksiya Construction	Kalit / nonce Key / nonce, bit	Autentifikatsiya Authentication	Vazifa va cheklov Use and constraint
ChaCha20 [1]	256 / 96	Alohida talab etiladi	IETF varianti; 20 raund
ChaCha20-Poly1305 [1, 6]	256 / 96	128 bitli teg	TLS profili; E1da o‘lchandi
Rabbit [8]	128 / 64	Alohida talab etiladi	Dasturiy shifr; qisqa IVni boshqarish
HC-128 [9]	128 / 128	Alohida talab etiladi	Ichki jadvallar: 4096 bayt
Trivium [10]	80 / 80	Alohida talab etiladi	Ixcham apparat etaloni; K≥128 mezoniga mos emas
Grain-128AEADv2 [11]	128 / 96	64 bitli teg	Apparat nomzodi; teg budjeti tekshiriladi
SNOW 3G va ZUC [12, 13]	Tegishli 3GPP profili	UIA2 / EIA3 alohida	Operator standartiga bog‘liq
SNOW-V [14]	256 bitli kalit	Rejimga bog‘liq	Vektorli dasturiy platforma
SNOW-Axn [15]	Kalit ≤256 bit	Rejimga bog‘liq	2026-yilgi agregatsiyalangan konstruksiya
RC4 [16]	Eski konstruksiya	Alohida talab etiladi	TLSda taqiqlangan; chiqarildi
Ascon-AEAD128 [17]	128 / 128	128 bitli teg	Permutatsiyali baza; E1da o‘lchanmadi
AES-GCM [18]	128/256 / 96[1]	128 bitli teg[1]	Blokli shifrli baza; E1da o‘lchandi

AES-GCM blokli shifrga, Ascon-AEAD128 esa permutatsiyaga asoslanadi; ular klassik oqimli shifrlar qatoriga kiritilmaydi. Ushbu ishda ular bir xil amaliy xizmatni — maxfiylik va autentifikatsiyani — bajaruvchi taqqoslash bazalaridir [17, 18]. Ascon uchun yakuniy NIST SP 800-232 standarti 2025-yilda nashr etilgan. RC4 esa TLSda qo‘llanishi taqiqlangani sababli yangi tizim nomzodlaridan chiqariladi [16].

Flórez-Gutiérrez va Todo 2025-yilda ChaCha uchun bit puncturing asosidagi kalit tiklash tahlilini rivojlantirdi [19]. Biroq qisqartirilgan variantdagi hujumni to‘liq ChaCha20ga qarshi amaliy kalit tiklash deb talqin qilish mumkin emas. Tezcan, Leander va Hadipourning GPU orqali qayta tekshirishlari ayrim oldingi ChaCha, Ascon va Serpent da’volarini qayta ko‘rib chiqish zarurligini ko‘rsatdi [20]. Shunday qilib, «eng chuqur hujum qilingan raund» jadvali keyingi tuzatishlar va tekshiruv usulini ham aks ettirishi kerak.

Beyne, Flórez-Gutiérrez va Todoning ishi puncturing asosidagi chiziqli kalit tiklashda parametrlar va ma’lumot murakkabligini aniq baholashga qaratilgan [21]. Mazkur natija xavfsizlik holatini yagona vaqt murakkabligi orqali ifodalash yetarli emasligini ko‘rsatadi. Hujum uchun kerakli kirishlar soni, mavjud ma’lumotlar fazosi va muvaffaqiyat ehtimoli birga talqin qilinishi lozim.

(cc) BY

Ghafoori va Miyaji tadqiqoti ChaCha permutatsiyasining qisqartirilgan 6 va 7 raundli variantlarini bog‘langan kalitli bumerang modeli orqali o‘rganadi [22]. Model bir-biri bilan bog‘langan kalitlardan foydalanishni talab qiladi; demak, uni mustaqil tasodifiy kalitli to‘liq ChaCha20-Poly1305 seansiga bevosita ko‘chirish mumkin emas. Mazkur ish eng yangi natijalarni kiritishda ham hujumning aynan qaysi obyektga taalluqli ekanini saqlash zarurligini ko‘rsatadi.

Grain bo‘yicha Liu va Tian dinamik kub hujumlaridagi modellashtirishni qayta ko‘rib chiqib, qisqartirilgan Grain-128AEAD uchun qisman kalit axboroti olishni tahlil qilgan [23]. Katyshev va Malovning 2025-yilgi korrelatsion tahlili esa xatolik kiritish faraziga ega [24]. Birinchisida qisqartirilgan boshlang‘ich bosqich, ikkinchisida maxsus tajovuzkor modeli mavjud. Shu sababli ikkala natija ham Grain-128AEADv2ning to‘liq amaliy buzilishi sifatida yozilmaydi.

He, Hu va Liuning 2025-yilgi preprinti 852 raundli Triviumda zaif kalitlar uchun superpolinom tiklashni ko‘rib chiqadi [25]. Bu natija 1152 boshlang‘ich taktli to‘liq konfiguratsiya va barcha kalitlar fazosini qamramaydi. Carlet va Sarkarning filtr modeli hamda Sarkarning Grain oilasini umumlashtirishga oid ishlari yangi konstruksiya yo‘nalishlarini ochadi, ammo preprintdagi taklifning mavjudligi standartlashganlik yoki mustaqil tasdiqlangan ustunlik bilan teng emas [26, 27].

Wang va hammualliflar 2026-yilda SNOW-Axnning agregatsiyalangan AEAD rejimini taklif qilgan [15]. Ushbu ish yuqori tezlikdagi oqimlarni birgalikda qayta ishlash imkoniyatini ko‘rsatadi. Biroq uning muallif o‘lchovlarini bu maqoladagi Python API orqali bitta xabarni shifrlash vaqti bilan bevosita solishtirish to‘g‘ri emas: platforma, parallelizm va o‘lchov chegarasi turlicha. 2-jadvalda yangi adabiyotlardan amaliy tanlovga o‘tishda saqlanishi zarur bo‘lgan shartlar jamlangan.

2-jadval.

Yangi adabiyotlar va natijani qo‘llash chegarasi

Ish va nashr sanasi	Tadqiqot natijasi	Saqlanadigan shart
Liu va Tian, 2024 [23]	Dinamik kub tahlilini tuzatish	Qisqartirilgan Grain-128AEAD; v2 bilan aynan bir emas
Flórez-Gutiérrez va Todo, 2025 [19]	Bit puncturing asosidagi kalit tiklash	Qisqartirilgan ChaCha; ma’lumot talabi mavjud
Tezcan va boshq., 2025 [20]	Oldingi da’volarni GPUda qayta tekshirish	Faqat sinovdan o‘tgan da’volarga tegishli
He va boshq., 2025 [25]	852 raundli Trivium superpolinomlari	Zaif kalitlar; ePrint versiyasi
Wang va boshq., 04.05.2026 [15]	SNOW-Axn agregatsiyalangan AEAD	Maxsus parallel ishlov; server API testi bilan teng emas
Beyne va boshq., 03.08.2026 [21]	Puncturing parametrlari bahosini aniqlashtirish	Vaqt bilan birga ma’lumot fazosi ham tekshiriladi
Ghafoori va Miyaji, 07.09.2026 [22]	Bog‘langan kalitli bumerang tahlili	6/7 raundli permutatsiya; to‘liq AEAD emas

(cc) BY

Ilmiy bo‘shliq shundan iboratki, bu ishlar kriptografik tuzilma va hujum imkoniyatini chuqur ochadi, lekin ulardan mahalliy xizmatning paket uzunligi, uzilish rejimi va tayyor protokolga mos tanlovi bevosita kelib chiqmaydi. Shu bois keyingi bo‘limlarda adabiyot sintezi uchta aniq hisoblash vazifasi bilan bog‘lanadi. Statistik tasodifiylik testlari kriptobardoshlik isboti o‘rnida qo‘llanmaydi; ularning bunday cheklovi NIST tavsiyalarida ham ko‘rsatilgan [28].

Metadalogiya

Tadqiqot obyekti — ishonchsiz aloqa kanali orqali autentifikatsiyalangan xabar almashadigan raqamli xizmat yoki telemetriya tuguni. Tajovuzkor paketni kuzatishi, o‘zgartirishi, yo‘qotishi va qayta yuborishi mumkin. Hisoblagichni tiklash tajribasida qurilmaning quvvati uzilishi modellashtiriladi. Kalitni jismonan o‘qib olish, apparat yon kanali va doimiy xotirani eski nusxaga ataylab qaytarish ushbu tajriba chegarasidan tashqarida.

Algoritm nomzodi a uchun K kalit uzunligini, T teg uzunligini, L foydali yukni, N uzatiladigan nonce baytlarini, k bir paketdagi o‘lchovlar sonini va Δ o‘lchov davrini belgilaymiz. Xavfsizlik saralashidan o‘tgan nomzodlar to‘plami quyidagicha aniqlanadi. Bu yerdagi mantiqiy shartlar tezlik bilan kompensatsiya qilinmaydi:

$$A_{mos} = \{a : K_a \geq 128 \wedge Auth(a) \wedge UniqueNonce(a) \wedge Moslik(a)\} \quad (1)$$

Bunda «moslik» protokol profili, kutubxona qo‘llovi, ma’lumot limiti va tashkilotning xavfsizlik talablarini o‘z ichiga oladi. 128 bitli kalit chegarasi tadqiqotning boshlang‘ich siyosati; u barcha obyektlar uchun qonunda belgilangan umumiy talab sifatida keltirilmaydi. Teg uchun yagona sonli chegarani majburan belgilash o‘rniga tegishli konstruksiya va tekshirish urinishlari budjeti hisobga olinadi.

Mos nomzodlar orasida vaqt, uzatiladigan baytlar va doimiy xotiraga yozishlar kamaytiriladi. Energiya va RAM ham amaliy tanlov mezonlaridir, ammo mazkur ishda ular o‘lchanmaganligi sababli yakuniy sonli ballga kiritilmaydi. Mezonlar bir-biriga zid bo‘lsa, qaror belgilangan xizmat cheklovlari asosida chiqariladi. Bu yondashuv tasdiqlanmagan vaznlar yordamida «eng yaxshi shifr» reytingini tuzishdan keladigan noaniqlikni kamaytiradi.

Bir o‘lchov seriyasida m ta xabarni shifrlash uchun sarflangan vaqt Δt bo‘lsin. Seriyadagi bir xabar vaqti t va foydali yuk bo‘yicha unumdorlik v quyidagicha hisoblanadi. Vaqt mikrosekundda olinsa, MB/s o‘nlik birlikda aniqlanadi:

$$t = \frac{\Delta t}{m}\ (\mu s); \quad v = \frac{L}{t}\ (MB/s) \quad (2)$$

Natija individual paket kechikishlarining medianasi emas, 30 ta seriya bo‘yicha hisoblangan o‘rtacha vaqtlar medianasidir. Farq ayniqsa tizim rejalashtiruvchisi va Python chaqiruv xarajatlarini talqin qilishda muhim. Kichik paketda doimiy API xarajati katta ulushni egallashi mumkin; katta bufer tezligini kichik xabarga ko‘chirish shu sababli xato bo‘ladi.

Bitta qurilmaning bir xil o‘lchamdagi k ta o‘lchovi bitta AEAD yozuviga birlashtiriladi. Nonce va teg har yozuv uchun bir marta uzatiladi. Qo‘shimcha xizmat maydonlari hamda transport sarlavhalari hisobga olinmagan holda kriptografik ustama O va o‘rtacha kutish vaqti W quyidagicha bo‘ladi:

$$O = \frac{N + T}{kL} \times 100\%; \quad W_{mean} = \frac{(k-1)\Delta}{2}; \quad W_{max} = (k-1)\Delta \quad (3)$$

Bu yerda kutish faqat o‘lchovlarni to‘plash jarayoniga tegishli. Shifrlash, tarmoq va server kechikishi alohida qo‘shiladi. Agar ruxsat etilgan ustama ulushi ρ va maksimal to‘plash kechikishi D bo‘lsa, k uchun pastki va yuqori chegara kelib chiqadi:

$$\left\lceil \frac{N + T}{\rho L} \right\rceil \leq k \leq \left\lfloor \frac{D}{\Delta} \right\rfloor + 1 \quad (4)$$

(cc) BY

Demak, eng kichik butun k yuqori chegaradan oshsa, berilgan talablarni agregatsiyaning o‘zi bilan bajarib bo‘lmaydi. Ushbu bajariluvchanlik mezoni maqoladagi amaliy tanlash usulining markaziy qismidir. U nonce siqilgan holda uzatiladigan yoki umuman paketga kiritilmaydigan protokollarda o‘sha profilning N qiymati bilan qayta hisoblanadi.

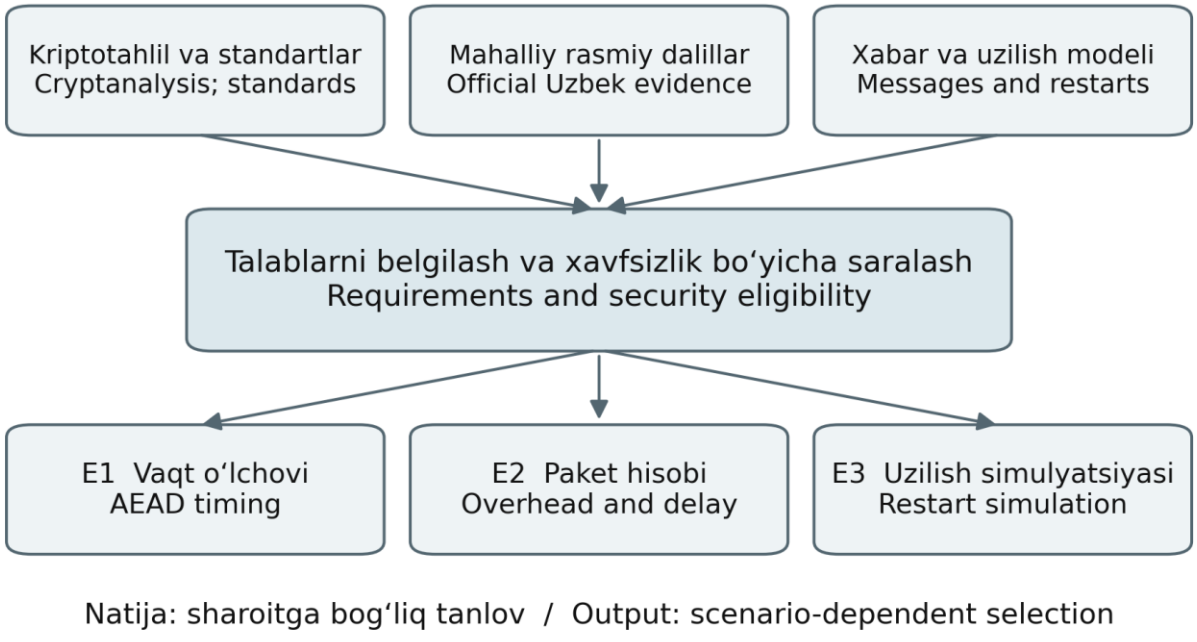
96 bitli nonce mantiqan 32 bitli kontekst identifikatori va 64 bitli monoton hisoblagichdan tuziladi. Identifikator bir kalit kontekstida manbalarni ajratishi, hisoblagich esa takrorlanmasligi kerak. Tasodifiy 32 bitli identifikatorning o‘zi ko‘p qurilmali tizim uchun yagonalik kafolati sifatida olinmaydi; qurilmaga xos kalit yoki boshqariladigan identifikator talab etiladi.

Oldindan band qilish siyosatida doimiy xotirada H chegarasi saqlanadi. Qurilma B qiymatli oraliqni ishlatishdan oldin H+B qiymatini atomar va bardavom yozadi; shundan keyingina eski H dan yangi H−1 gacha bo‘lgan hisoblagichlardan foydalanadi. Qayta ishga tushishda ishlatilmay qolgan qiymatlar tashlab yuborilib, saqlangan chegaradan yangi oraliq ajratiladi. 4-rasm bu qoidaning kichik misolini, 5-rasm esa miqdoriy natijasini beradi.

Qoidaning to‘g‘riligi oddiy invariantdan kelib chiqadi: foydalanilgan barcha hisoblagichlar doimiy xotiradagi chegaradan kichik. Yozish yakunlanmasdan xabar shifrlanmasa, uzilishdan keyingi boshlang‘ich qiymat ilgari foydalanilgan qiymatlardan katta bo‘ladi. Bu dalil atomar yozish, saqlangan holatning ortga qaytmasligi va hisoblagich toshib ketmasligi shartlariga tayanadi. RFC 8613da saqlash oralig‘i va tiklanish haqida o‘xshash tamoyil berilgan [2]; bu yerda ideal atomar yozish sharoitidagi xarajat modeli o‘rganiladi.

Tadqiqot metodologiyasi

Tadqiqot tanqidiy sharh, dasturiy o‘lchov va ssenariy modellashtirishdan tashkil topgan. 1-rasmda rasmiy dalillar, kriptotahlil va xizmat parametrlari qanday qilib bitta qaror jarayoniga ulanayotgani ko‘rsatilgan. Adabiyot qidiruvining yakuniy sanasi 2026-yil 27-sentabr. IACR, NIST, RFC Editor, ETSI, nashriyot hamda muallif sahifalari, O‘zbekiston davlat organlarining rasmiy manbalari qo‘llandi. Yangi ishlar 2024–2026-yillardan olindi; algoritmning boshlang‘ich spetsifikatsiyasi uchun eski birlamchi manbalar saqlandi.



1-rasm. Dalillar va hisoblash tajribalarini birlashtiruvchi tadqiqot dizayni. Muallif ishlanmasi.

(cc) BY

Har bir ilmiy manbada algoritm versiyasi, hujum modeli, natija turi va nashr maqomi ajratildi. Taqrizlangan maqola va preprint bir xil dalil maqomida berilmadi. Qidiruv yo‘naltirilgan tanqidiy sharhdir; to‘liq bibliometrik korpus yoki barcha ishlarni qamrab oluvchi sistematik sharh deb da’vo qilinmaydi. Rasmiy statistika esa kriptografik unumdorlikning dalili sifatida emas, qo‘llash ehtiyojini aniqlash uchun ishlatildi.

ChaCha20-Poly1305, AES-256-GCM va AES-128-GCM Python cryptography kutubxonasining bir xil yuqori darajali AEAD interfeysi orqali tekshirildi [29]. Asosiy teng kalit uzunligidagi taqqoslov ChaCha20-Poly1305 va AES-256-GCM o‘rtasida; AES-128-GCM qo‘shimcha amaliy baza sifatida kiritildi. Barcha variantlarda 96 bitli nonce va 128 bitli teg ishlatildi. Ascon, Grain va telekommunikatsiya shifrlari ushbu vaqt tajribasida o‘lchanmadi; ularning maqoladagi bahosi spetsifikatsiya va adabiyotga asoslanadi.

3-jadval.

E1–E3 tajribalarining takrorlash parametrlari

Parametr	Qiymat
Protsessor va muhit	Intel Xeon Platinum 8573C; Linux 6.18.44 x86-64; virtual muhit; bitta mantiqiy yadro
Dasturiy qatlam	Python 3.12.14; cryptography 46.0.0; OpenSSL 3.5.3
Apparat imkoniyatlari	AES, PCLMULQDQ, AVX2, VAES, VPCLMULQDQ mavjud; tabiiy tanlov yoqilgan
E1 foydali yuk, bayt	16, 32, 64, 128, 256, 1024, 4096, 16384, 65536
E1 boshqa parametrlar	AAD 17 bayt; nonce 12 bayt; teg 16 bayt; 30 sikl; 810 seriya
E1 umumlashtirish	Seriya vaqtlari medianasi; 5000 bootstrap tanlanmasi; 95% oralig‘i
E2 cheklovlar	N=12, T=16 bayt; Δ=1 s; ρ=0,10; D=5 s; k=1…16
E3 izlar va siyosatlar	100 iz × 100 000 xabar; p=0,001; 6 siyosat/parametr holati
Takrorlash seed qiymati	20260927; vaqt natijasi apparat va seansga bog‘liq

Har bir konfiguratsiya va xabar uzunligi uchun kalit obyekti o‘lchovdan oldin yaratildi. Xabar va 17 baytli AAD o‘zgarmas, nonce esa har shifrlash uchun monoton oshirildi; qizdirish va kalibrlashda ham ayni kalit ostida takrorlanmadi. Nonce baytlari seriya boshlanishidan oldin tayyorlandi. O‘lchanadigan oraliq encrypt chaqiruvlari va Python siklini qamradi; kalit yaratish, tasodifiy son generatsiyasi, faylga yozish va deshifrlash unga kiritilmadi. Bu chegara ilova interfeysi xarajatini o‘lchaydi, sof assembler yadrosining tezligini emas.

Har bir shart uchun 200 ta qizdirish va 500 ta kalibrlash chaqiruvi bajarildi. Kalibrlash asosida taxminan 8 millisekundlik seriya uchun 200–20 000 takror tanlandi. Keyin 27 ta shart 30 siklda, har siklda tasodifiy tartibda o‘lchandi. Jami 810 seriyada 7 863 030 ta vaqt hisobiga kirgan shifrlash bajarildi. Jarayon bitta mantiqiy yadroga bog‘landi; apparat tezlatkichlari tabiiy holatda qoldirildi. Virtual muhitdagi boshqa yuklamalar to‘liq nazorat qilinmagan.

Median uchun 5 000 marta almashtirib qayta tanlash asosida 95 foizlik percentile bootstrap oralig‘i hisoblandi. Bu oraliq shu seansdagi seriyalar tarqoqligini baholaydi; barcha protsessorlar yoki turli kunlardagi seanslar uchun ishonch oralig‘i emas. Tasodifiy tartib, bootstrap va

(cc) BY

simulyatsiya uchun 20260927 boshlang‘ich qiymati belgilandi. Xom vaqtlar o‘chirilmagan va chet qiymatlar chiqarilmagan.

Hisoblashdan oldin uchta ma’lum javobli namuna, jumladan RFC 8439dagi AEAD vektori tekshirildi. 30 ta shifrlash–deshifrlash sinovi va teg, shifrmatn, nonce yoki AAD o‘zgartirilgan 117 ta salbiy sinov bajarildi. To‘g‘ri matnlar qayta tiklandi, barcha salbiy sinovlar rad etildi. Bular ishlatilgan interfeysning asosiy to‘g‘riligini tekshiradi; kutubxonaning to‘liq xavfsizlik auditi hisoblanmaydi.

E2 tajribada L = 16, 32, 64, 128 va 256 bayt, k = 1 dan 16 gacha qiymatlar olindi. Nonce uchun N = 12 bayt, teg uchun T = 16 bayt, o‘lchovlar davri uchun Δ = 1 soniya belgilandi. Ushbu qiymatlar O‘zbekistondagi barcha qurilmalardan o‘lchangan parametrlar emas, ochiq ko‘rsatilgan hisoblash ssenariysidir. Amaliy cheklovlar ρ = 0,10 va D = 5 soniya deb tanlandi. Natijalar (3)–(4) formulalar bo‘yicha hisoblandi; deterministik hisobga statistik ishonch oralig‘i qo‘yilmadi.

Agregatsiya bitta manba va bir xil ishonch sohasi ichida amalga oshadi. Alohida qurilmalar yuborgan imzosiz ma’lumotni oraliq shlyuzda shunchaki birlashtirish end-to-end autentifikatsiya o‘rnini bosa olmaydi. Paket yo‘qolishining ehtimoli, radio energiyasi va qayta yuborish xarajatlari ushbu modelga kiritilmadi. Shu sababli uzatiladigan baytlar kamayishi energiya ham aynan shuncha kamayishini bildirmaydi.

E3da har biri 100 000 xabardan iborat 100 ta iz yaratildi. Har yuborishdan keyingi uzilish ehtimoli p = 0,001 bo‘lib, sessiya uzunliklari geometrik taqsimotdan olindi; yakuniy to‘xtash uzilish hisobiga qo‘shilmadi. Bir izdagi uzilish medianasi 100 tani tashkil etdi. Barcha siyosatlar aynan bir xil izlarda sinovdan o‘tkazildi. Ushbu p qiymati mahalliy elektr ta’minoti statistikasi emas, sezilarli tiklanish yuklamasini hosil qiluvchi tajriba parametri.

Uch siyosat taqqoslandi. Birinchisida qayta ishga tushganda hisoblagich nolga qaytadi. Ikkinchisida har 256 ta hisoblagich chegarasida keyingi qiymat foydalanishdan keyin saqlanadi va uzilishda oxirgi saqlangan holat tiklanadi. Uchinchisida B = 16, 64, 256 yoki 1024 qiymatli oraliq foydalanishdan oldin band qilinadi. Har siyosatda takroriy nonce soni, doimiy xotiraga yozishlar va uzilish sababli ishlatilmay tashlangan qiymatlar hisoblandi.

Ikkinchi siyosatda saqlashning o‘zi ideal bo‘lsa ham, hali saqlanmagan oraliqdagi qiymatlar qayta ishlatilishi mumkin. Uchinchi siyosatda esa yozuvning bardavomligi tasdiqlangandan keyingina shifrlashga ruxsat beriladi. Xotirani jismonan buzish, yozuv o‘rtasidagi elektr uzilishi, parallel jarayonlar va hisoblagich toshishi modelga qo‘shilmagan. Bunday sharoitlarda atomar jurnal, himoyalangan hisoblagich yoki yangi kalit kontekstini o‘rnatish kabi qo‘shimcha mexanizm kerak bo‘ladi.

Simulyatsiya natijalari 100 iz medianasi bilan berildi. Ularning 2,5–97,5 persentillari turli izlar bo‘yicha empirik tarqalish oralig‘idir; mediananing 95 foizlik ishonch oralig‘i bilan aralashtirilmaydi. Oldindan band qilishning hisoblagich qiymatlarini aniq chiqaruvchi alohida kichik modellari bilan oraliq hisobi tekshirildi. Tajribalar kodi, muhit tavsifi va xom natijalar maqolaga hamroh hisoblash materiallarida saqlandi.

Matnni tahrirlash, kod va grafiklarni tayyorlashda sun’iy intellekt yordamchisidan foydalanildi. Sonli natijalar bajarilgan Python dasturining chiqishidan olindi; ular matn yaratish modeli tomonidan taxminiy qiymat sifatida hosil qilinmadi. Shaxsga doir ma’lumotlar yoki ishlab turgan tizimlarning maxfiy kalitlari ishlatilmadi. Hisoblash tajribalari kriptotahliliy hujumning yangi murakkablik rekordini o‘rnatishga qaratilmagan.

Natijalar

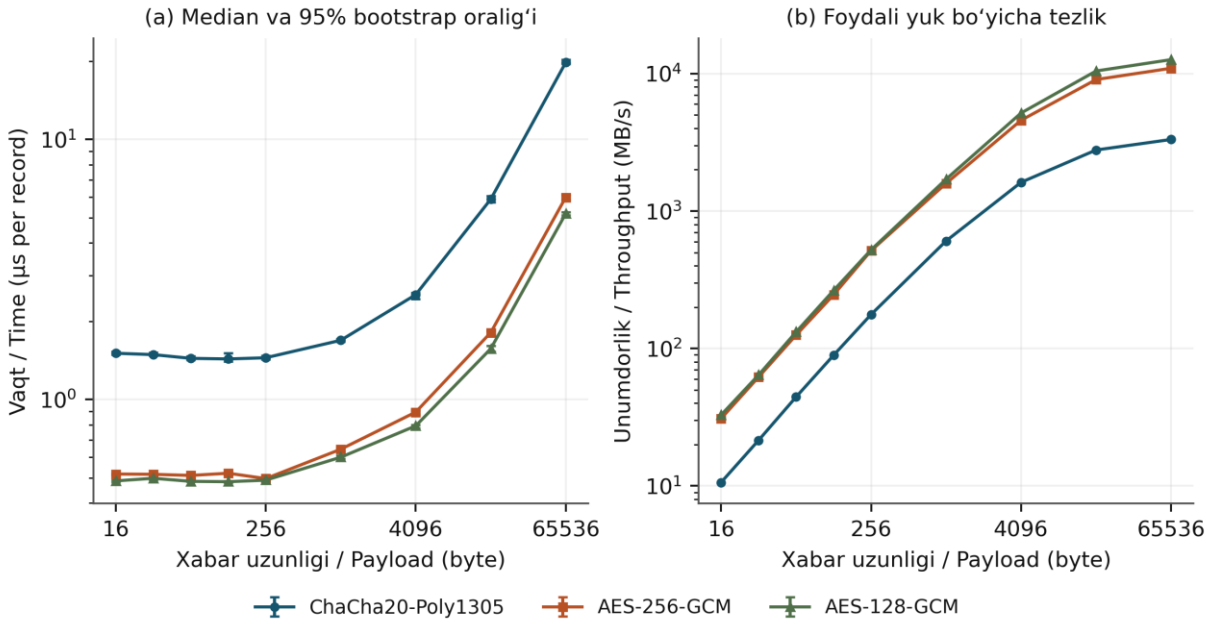
3-jadvalda ko‘rsatilgan muhitda barcha o‘lchangan uzunliklarda AES-GCM variantlari ChaCha20-Poly1305ga nisbatan kamroq vaqt sarfladi. 4-jadval medianalar va bootstrap oraliqlarini beradi. 2-rasmda shu natija xabar vaqti hamda foydali yuk unumdorligi ko‘rinishida tasvirlangan. Grafikdagi ikkita ko‘rsatkich bitta xom vaqt qatoridan kelib chiqadi; ular mustaqil tajribalar emas.

(cc) BY

4-jadval.

Bir xabarni shifrlash vaqti medianasi va 95% bootstrap oralig‘I

L, bayt	ChaCha20-Poly1305 µs	AES-256-GCM µs	AES-128-GCM µs
16	1,507 [1,486; 1,527]	0,518 [0,514; 0,518]	0,487 [0,481; 0,492]
32	1,489 [1,472; 1,520]	0,516 [0,512; 0,521]	0,498 [0,491; 0,510]
64	1,440 [1,421; 1,465]	0,511 [0,497; 0,521]	0,485 [0,483; 0,492]
128	1,433 [1,402; 1,511]	0,521 [0,515; 0,531]	0,484 [0,481; 0,487]
256	1,448 [1,430; 1,474]	0,497 [0,484; 0,506]	0,490 [0,486; 0,502]
1024	1,690 [1,669; 1,708]	0,644 [0,632; 0,654]	0,600 [0,593; 0,609]
4096	2,531 [2,433; 2,572]	0,895 [0,875; 0,911]	0,793 [0,779; 0,802]
16384	5,891 [5,748; 6,055]	1,810 [1,777; 1,840]	1,568 [1,528; 1,610]
65536	19,752 [19,514; 20,257]	5,991 [5,871; 6,106]	5,185 [5,113; 5,263]



2-rasm. E1da xabar vaqti va foydali yuk unumdorligi.

(cc) BY *dtai.uz*

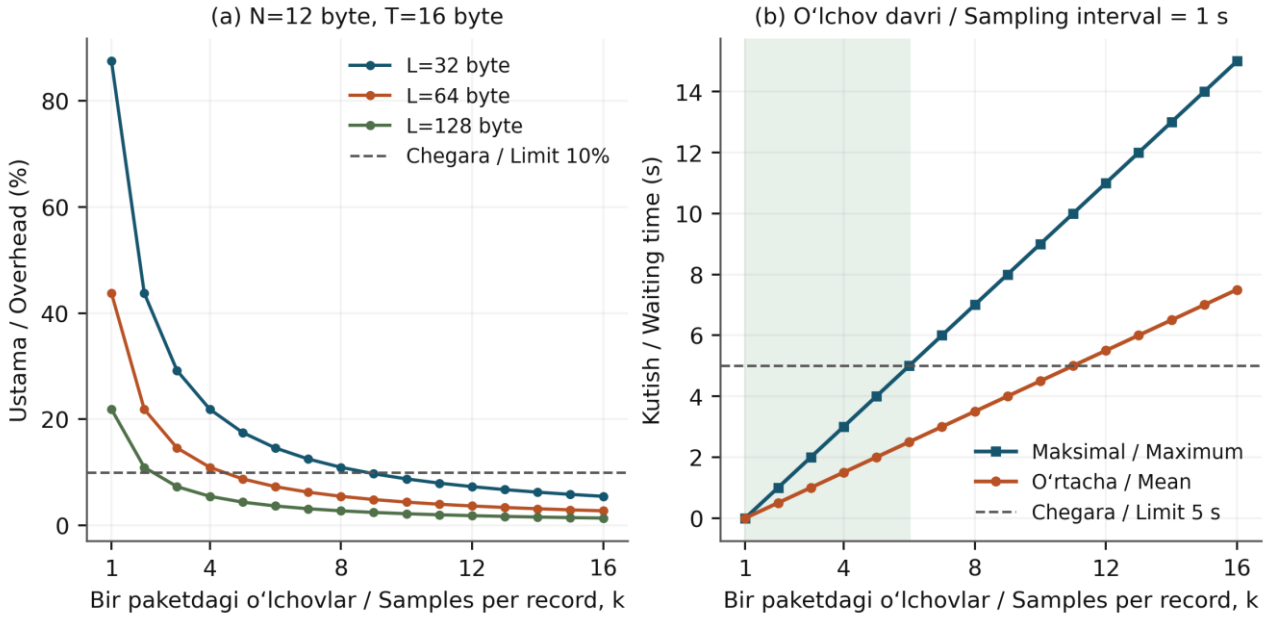
ISSN: 3030-3346

32 baytli xabarda ChaCha20-Poly1305 medianasi 1,489 µs, AES-256-GCMniki 0,516 µs bo‘ldi. Sikllar bo‘yicha juft vaqt nisbatining medianasi 2,887, bootstrap oralig‘i 2,842–2,956 ni tashkil etdi. 65 536 baytda mos vaqtlar 19,752 va 5,991 µs; juft nisbat medianasi 3,322 va oralig‘i 3,230–3,425 bo‘ldi. Nisbat bir xil sikldagi seriyalardan hisoblangani uchun u ikkita umumiy medianani bo‘lishdan biroz farqlanadi.

32 baytda foydali yuk unumdorligi ChaCha20-Poly1305 uchun 21,50 MB/s va AES-256-GCM uchun 61,99 MB/s bo‘lsa, 65 536 baytda 3 317,96 va 10 938,74 MB/s ga yetdi. Kichik paketdagi past MB/s qiymati faqat shifr yadrosining sustligini anglatmaydi: har yozuvga tushadigan interfeys va yakunlash xarajati kam baytga taqsimlanadi. Shu sababli telemetriya uchun «µs/xabar», katta trafik uchun esa «MB/s» birgalikda berilishi lozim.

Natija Xeon protsessorida AES, PCLMULQDQ, VAES va VPCLMULQDQ imkoniyatlari mavjud bo‘lgan sharoitga tegishli. Ushbu tajriba buyruqlar alohida o‘chirilib bajarilmagani sababli kuzatilgan farqning qancha qismini aynan bitta tezlatkich keltirib chiqarganini ajratmaydi. Natijadan kelib chiqadigan asosli xulosa: bu server konfiguratsiyasida ChaCha20-Poly1305ni faqat oqimli konstruksiya ekanligi sababli tezroq deb tanlash mumkin emas. ARM, mikrokontroller va tezlatkichsiz platforma uchun alohida o‘lchov talab etiladi.

Bitta 32 baytli xabarga 28 bayt nonce va teg qo‘shilganda kriptografik ustama 87,5 foiz bo‘ladi. Sakkiz o‘lchovni birlashtirish uni 10,9375 foizga tushiradi, ammo birinchi o‘lchovning kutishi 7 soniyaga yetadi. 10 foizlik chegaraga tushish uchun kamida to‘qqiz o‘lchov zarur; bu esa 8 soniyalik maksimal kutishni talab qiladi. D = 5 soniya shartida k ko‘pi bilan 6 bo‘lishi mumkin. Demak, ushbu 32 baytli ssenariyda ikki talab o‘zaro mos emas.



3-rasm. Kriptografik ustama va to‘plash kechikishi.

64 baytli o‘lchovda eng kichik k = 5 bo‘ladi. Bunda ustama 8,75 foiz, o‘rtacha kutish 2 soniya va maksimal kutish 4 soniyani tashkil qiladi. Bir o‘lchovga to‘g‘ri keladigan hisoblangan uzatish hajmi 92 baytdan 69,6 baytga tushadi; bu model doirasida 24,35 foiz kamayishdir. 5-jadval turli foydali yuklar uchun bajariluvchanlikni ko‘rsatadi. Natija «tegni qisqartirish» tavsiyasiga tayanmaydi; autentifikatsiya tegi 16 bayt holida saqlanadi.

(cc) BY

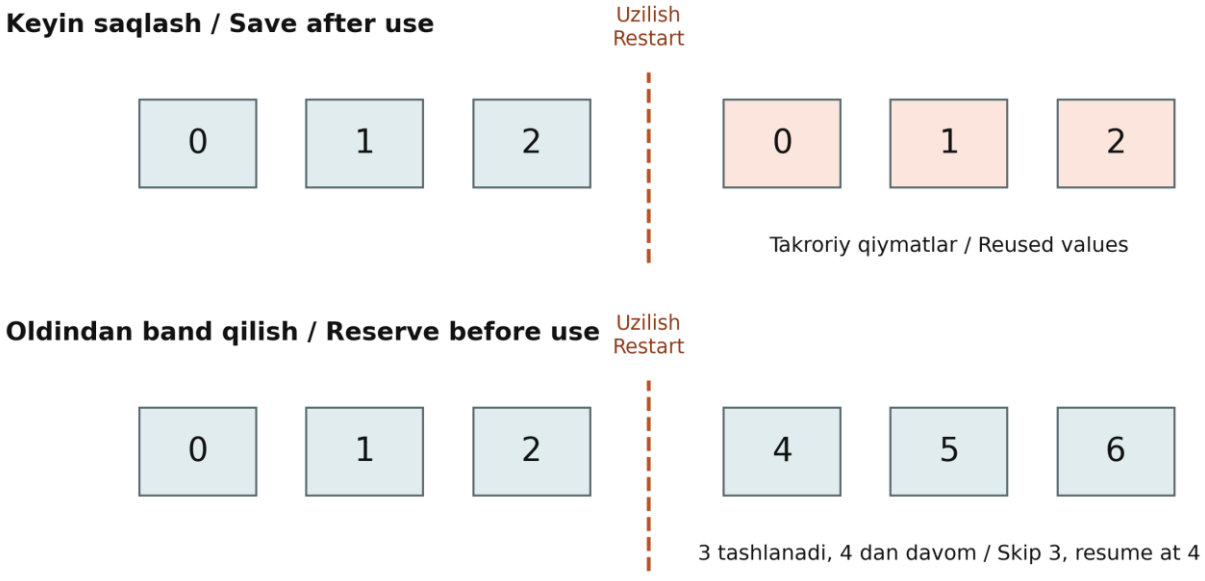
5-jadval.

Ustama va kutish cheklovlarining birgalikda bajarilishi

L, bayt	Eng kichik k	Wmax, s	O, %	D≤5 s holati
16	18	17	9,72	Bajarilmaydi / Infeasible
32	9	8	9,72	Bajarilmaydi / Infeasible
64	5	4	8,75	Bajariladi / Feasible
128	3	2	7,29	Bajariladi / Feasible
256	2	1	5,47	Bajariladi / Feasible

Ushbu hisob yangi algoritm tanlashdan oldin xizmat talablari o‘zaro muvofiqligini tekshirish mumkinligini ko‘rsatadi. Agar 32 baytli xabar uchun 5 soniya qat’iy chegara bo‘lsa, 10 foizlik ustama maqsadini qayta ko‘rish, nonce uzatish profilini o‘zgartirish yoki ma’lumot formatini qayta loyihalash kerak. Bu variantlarning har biri protokol va xavfsizlik shartlari bilan birga tekshiriladi. Favqulodda boshqaruv buyruqlariga odatiy davriy telemetriya agregatsiyasi qo‘llanmaydi.

4-rasmdagi B = 4 misolda uzilishdan oldin 0, 1 va 2 qiymatlari ishlatilgan. Foydalanishdan keyin saqlash siyosati hali yangi chegarani qayd etmagan bo‘lsa, tiklanishda ular qaytadan ishlatiladi. Oldindan band qilishda esa doimiy chegarada 4 saqlangan bo‘ladi; tiklanish 4 dan boshlanadi va foydalanilmay qolgan 3 qiymati tashlanadi. Bu misol 6-jadvaldagi katta simulyatsiya natijasini tushuntiruvchi mexanizmni beradi.



4-rasm. B=4 oraliqda uzilishdan keyingi hisoblagich: keyin saqlash va oldindan band qilish.

100 ta iz bo‘yicha hisoblagichni nolga qaytarish siyosatida takroriy nonce medianasi 94 865,5 ta, foydalanishdan keyin 256 qiymatlik checkpoint saqlashda esa 12 092 ta bo‘ldi. Birinchi siyosatdagi ulush 94,8655 foiz, ikkinchisida 12,092 foizni tashkil qiladi. Juft sonli izlar medianasi ikki

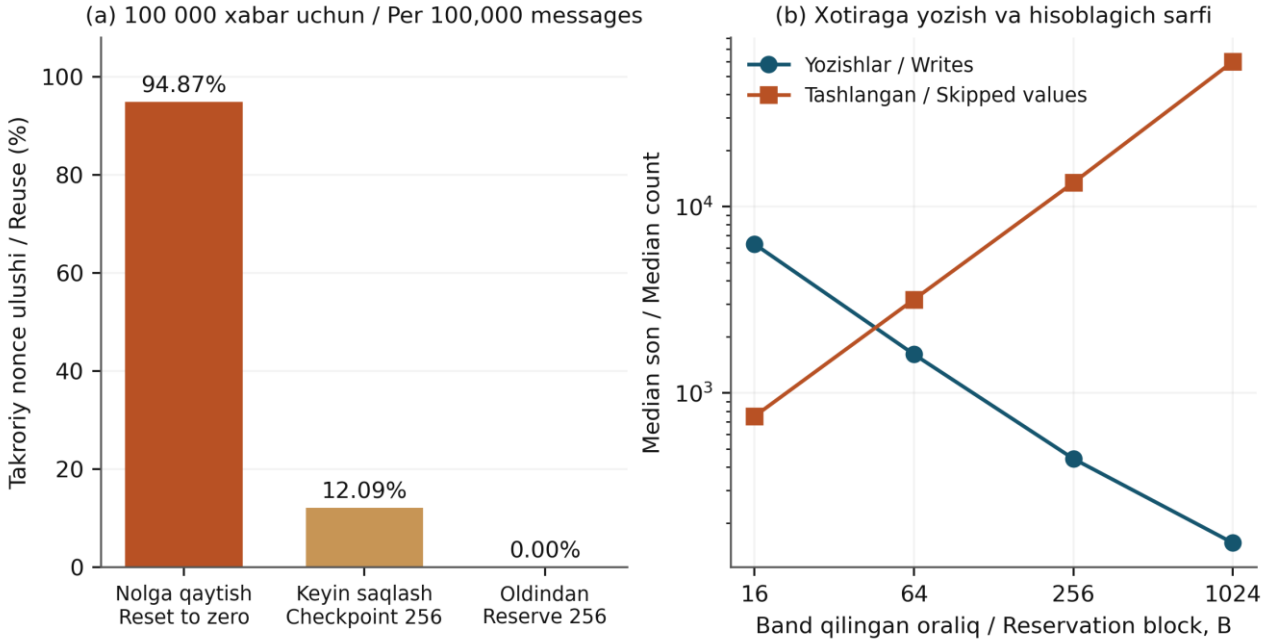
(cc) BY

markaziy qiymat o‘rtachasi bo‘lgani uchun ayrim natijalar kasr son bilan ifodalangan.

6-jadval.

Uzilishlarda nonce va xotiraga yozish natijalari

Siyosat va B Policy and B	Takroriy nonce Repeated nonces	Yozishlar Writes	Tashlangan qiymat Skipped values
Nolga qaytish / Reset	94 865,5	0	0
Keyin saqlash / Checkpoint B=256	12 092	343	0
Oldindan band / Reserve B=16	0	6 297	750,5
Oldindan band / Reserve B=64	0	1 612,5	3 176,5
Oldindan band / Reserve B=256	0	444	13 451
Oldindan band / Reserve B=1024	0	157	59 971,5



5-rasm. E3da nonce takrorlanishi va oraliq o‘lchamining ta’siri.

B = 256 qiymatli oldindan band qilishda barcha 100 izda takroriy nonce soni nol bo‘ldi. Har 100 000 xabarga yozishlar medianasi 444 ta bo‘lib, har xabardan oldin alohida bardavom yozish bajariladigan 100 000 yozuvli bazaga nisbatan 99,556 foiz kamdir. Evaziga uzilishlarda ishlatilmay tashlangan qiymatlar medianasi 13 451 tani tashkil etdi. Yozishlar sonining 2,5–97,5 persentil oralig‘i

(cc) BY

429,4–455,0 bo‘ldi; checkpoint siyosatidagi takroriy nonce uchun shu oraliq 9500,2–14 754,9 tani tashkil etdi. Bu taqqoslov kalit yoki teg uzunligini o‘zgartirmasdan holat boshqaruvi xarajatini kamaytirish imkoniyatini ko‘rsatadi.

B ni 16 dan 1024 gacha oshirish yozishlar medianasini 6297 tadan 157 tagacha kamaytirdi, tashlangan qiymatlar medianasi esa 750,5 tadan 59 971,5 tagacha ko‘paydi. Shunday qilib, kattaroq blok xotiraga murojaatni kamaytiradi, lekin hisoblagich fazosini tezroq sarflaydi. 64 bitli hisoblagich uchun bu sonlar kichik bo‘lsa ham, standartdagi bir kalit ostidagi ma’lumot limiti va qurilmaning ishlash muddati baribir tekshirilishi kerak.

Nol takrorlanishning talqini model shartlariga bog‘liq. Atomar yozish invariantidan tashqarida, masalan, saqlangan holat eski zaxiraga almashtirilsa, bu tajriba xavfsizlik kafolati bermaydi. Shuningdek, yuboruvchi nonce siyosati to‘g‘ri bo‘lishi qabul qiluvchining replay himoyasi avtomatik ishlashini anglatmaydi. Qabul qiluvchi ketma-ketlik holati alohida saqlanishi yoki yangi xavfsizlik konteksti o‘rnatilishi kerak [2].

Muhokama

Rasmiy ko‘rsatkichlar algoritm tanlashga umumiy chaqiriq bo‘lib qolmasligi uchun har bir dalil ma’lum texnik talab bilan bog‘landi.

Nazariy jihatdan (4) shart paket talablari o‘zaro mosligini kriptografik algoritmni almashtirishdan oldin tekshirish imkonini beradi. Ustama pastki chegarani, kutish esa yuqori chegarani hosil qiladi; ularning kesishmasi yo‘q bo‘lsa, tezroq shifr bu ziddiyatni bartaraf eta olmaydi. 32 va 64 baytli ssenariylar orasidagi farq aynan shu munosabatdan kelib chiqadi. Cheklovlarni ochiq ko‘rsatish yashirin taxminlarga tayangan tavsiyalarga nisbatan tekshiriladigan qaror beradi.

Amaliy jihatdan E1 katta bufer tezligi va kichik xabar xarajatini ajratdi, E3 esa xavfsizlik sharti bilan doimiy xotira xarajati o‘rtasidagi bog‘lanishni miqdoriy ifodaladi. Mazkur natijalar mavjud yechimni yaxshiroq sozlashning o‘zi ham sezilarli tizim foydasi berishi mumkinligini ko‘rsatadi. Biroq uzatiladigan bayt va yozish sonidagi kamayishni bevosita so‘mdagi iqtisodiy samara yoki batareya umrining o‘sishi deb e’lon qilish uchun radio hamda xotira energiyasi qo‘shimcha o‘lchanishi zarur.

Yangi milliy oqimli shifr yaratish zarurati ham shu dalillar zanjiri orqali asoslanishi kerak. Avval mavjud standart konstruksiyalar mahalliy qurilmada o‘lchanadi; keyin hech biri bajarmaydigan qat’iy talab aniqlanadi. Faqat shundan so‘ng yangi konstruksiya uchun aniq gipoteza qo‘yish asosli bo‘ladi. Milliy tatbiq uchun kutubxona auditi, kalit boshqaruvi, uzilishdan tiklanish va ochiq benchmark majmuasi ham mustaqil ilmiy-amaliy natijadir. Algoritmning mahalliy yaratilgani uning matematik xavfsizligiga dalil bo‘la olmaydi.

Shaxsga doir ma’lumotlar va kiberxavfsizlik bo‘yicha O‘zbekiston qonunlari texnik himoya choralarini tashkiliy talablar bilan muvofiqlashtirishni talab qiladi [33, 34]. Ushbu huquqiy asoslar aynan ChaCha yoki Grain majburiy ekanini anglatmaydi. Maqoladagi tavsiyalar muayyan obyekt uchun sertifikatlash yoki huquqiy muvofiqlik xulosasi o‘rnini bosmaydi.

Vaqt o‘lchovi bitta virtual x86-64 server, bitta kutubxona versiyasi va bitta seansga asoslangan. Protsessor chastotasi, virtual muhitdagi raqobat va API qatlamining farqi natijaga ta’sir qilishi mumkin. AES tezlatkichlarini o‘chirib takrorlash yoki turli protsessorlarda mustaqil seanslar ushbu ishga kiritilmagan. Shuning uchun natija umumjahon unumdorlik reytingi sifatida berilmaydi.

Paket modeli barcha qo‘shimcha protokol maydonlarini, yo‘qotish va qayta yuborishni hisobga olmaydi; simulyatsiya esa ideal atomar saqlashni qabul qiladi. Real qurilmada yozishning uzilish paytidagi holati, qayta ijro oynasi, kalit yangilash va xabarlarni birlashtirishning nosozlikka ta’siri tekshirilishi kerak. Kalit boshqaruvi xatosi, yon kanal va fizik buzilishlarga bardoshlik uchun alohida tajriba zarur. Ushbu chegaralar hisoblangan

(cc) BY

natijani inkor etmaydi, uning qayergacha qo‘llanishini belgilaydi.

Keyingi mahalliy pilot server, apparat AES imkoniyatiga ega mobil qurilma va cheklangan mikrokontrollerni qamrashi kerak. Bir xil xabar hamda AAD taqsimoti ostida vaqt, to‘liq uzatish sikli energiyasi, RAM/Flash sarfi va quvvat uzilishidan keyingi tiklanish qayd etiladi. Bu o‘lchovlardan keyingina ma’lum qurilma turi uchun yakuniy algoritm tavsiyasi va iqtisodiy samara bahosi berilishi mumkin.

Xulosa

Mavjud oqimli shifrlar tahlili algoritm oilasi, versiyasi va hujum modelini ajratish zarurligini ko‘rsatdi. 2024–2026-yillardagi yangi hamda qayta ko‘rib chiqilgan kriptotahlil natijalari qisqartirilgan variant, bog‘langan kalit, zaif kalit yoki fizik xatolik farazlarini saqlagan holda talqin qilindi. AES-GCM va Ascon oqimli shifr sifatida emas, bir xil himoya vazifasini bajaruvchi bazalar sifatida taqqoslandi.

Bajarilgan server tajribasida 32 baytli xabar uchun ChaCha20-Poly1305ning 1,489 µs median vaqti AES-256-GCMning 0,516 µs vaqtidan katta bo‘ldi. Bu natija apparat va realizatsiyani hisobga olmasdan oqimli shifrning tezlik ustunligini da’vo qilish mumkin emasligini tasdiqlaydi. Tajriba chegarasi va 95 foizlik bootstrap oraliqlari ochiq berildi.

Analitik model 12 baytli uzatiladigan nonce va 16 baytli teg sharoitida, sekundiga bitta 32 baytli o‘lchov uchun 10 foizlik ustama hamda 5 soniyalik maksimal kutish chegarasi birgalikda bajarilmasligini aniqladi. 64 baytli o‘lchovlarni beshtadan birlashtirish esa 8,75 foizlik ustama va 4 soniyalik maksimal kutish bilan ikkala cheklovni qanoatlantirdi. Shu tariqa algoritm tanlashdan oldin paket talablarining bajariluvchanligini tekshirish mezoni hosil qilindi.

Uzilish simulyatsiyasida B = 256 qiymatli oldindan band qilish barcha izlarda nonce takrorlanishini oldini oldi va har xabar uchun alohida yozishga nisbatan yozishlar medianasini 99,556 foiz kamaytirdi. Bu natija atomar va ortga qaytmaydigan saqlash shartiga bog‘liq. O‘zbekiston raqamli xizmatlari uchun amaliy yo‘l — standart konstruksiyani real platformada baholash, qisqa paket cheklovlarini tekshirish va tiklanishda kalit–nonce yagonaligini saqlashdir. Yangi algoritm yaratish masalasi esa mavjud yechimlar bilan bajarilmaydigan, mahalliy o‘lchovda tasdiqlangan talabdan kelib chiqishi lozim.

Foydalanilgan adabiyotlar

1. Nir Y., Langley A. ChaCha20 and Poly1305 for IETF Protocols. RFC 8439. 2018. DOI / URL
2. Selander G., Mattsson J., Palombini F., Seitz L. Object Security for Constrained RESTful Environments (OSCORE). RFC 8613. 2019. DOI / URL
3. O‘zbekiston Respublikasi Milliy statistika qo‘mitasi. O‘zbekistonda mobil internet abonentlari soni 10 yilda 4,3 barobarga oshgan. 05.08.2026. DOI / URL
4. O‘zbekiston Respublikasi Suv xo‘jaligi vazirligi. Parlamentda suv xo‘jaligi vazirining axboroti tinglandi. 12.12.2025. DOI / URL
5. Bernstein D. J. Salsa20 specification. 2005. Muallif spetsifikatsiyasining ochiq nusxasi. DOI / URL
6. Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446. 2018. DOI / URL
7. Langley A., Chang W.-T., Mavrogiannopoulos N., Strömbergson J., Josefsson S. ChaCha20-Poly1305 Cipher Suites for Transport Layer Security (TLS). RFC 7905. 2016. DOI / URL
8. Boesgaard M., Vesterager M., Zenner E. A Description of the Rabbit Stream Cipher Algorithm. RFC 4503. 2006. DOI / URL
9. Wu H. The Stream Cipher HC-128. Muallifning algoritm spetsifikatsiyasi. DOI / URL
10. De Cannière C., Preneel B. Trivium Specifications. eSTREAM algoritm spetsifikatsiyasi. DOI / URL

(cc) BY *dtai.uz*

11. Hell M., Johansson T., Maximov A., Meier W., Sönnerup J., Yoshida H. Grain-128AEADv2 — A lightweight AEAD stream cipher. NIST LWC finalist spetsifikatsiyasi. 2021. DOI / URL
12. ETSI. TS 135 216 V19.0.0. Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 2: SNOW 3G specification. 3GPP TS 35.216, Release 19. 2025-10. DOI / URL
13. ETSI. TS 135 221 V19.0.0. Specification of the 3GPP Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 1: EEA3 and EIA3 specifications. 3GPP TS 35.221, Release 19. 2025-10. DOI / URL
14. Ekdahl P., Johansson T., Maximov A., Yang J. A new SNOW stream cipher called SNOW-V. IACR Transactions on Symmetric Cryptology. 2019(3):1–42. DOI 10.13154/tosc.v2019.i3.1-42. DOI / URL
15. Wang D., Maximov A., Ekdahl P., Johansson T. Pushing to the limits: SNOW-Axn – a fast AEAD stream cipher in aggregated mode. IACR Communications in Cryptology. 2026;3(1). Nashr: 04.05.2026. DOI 10.62056/a6y7qj5vt. DOI / URL
16. Popov A. Prohibiting RC4 Cipher Suites. RFC 7465. 2015. DOI / URL
17. 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. DOI / URL
18. Dworkin M. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. NIST SP 800-38D. 2007. DOI 10.6028/NIST.SP.800-38D. DOI / URL
19. Flórez-Gutiérrez A., Todo Y. Improved Cryptanalysis of ChaCha: Beating PNBs with Bit Puncturing. EUROCRYPT 2025, Part I, LNCS 15601, 427–457. DOI 10.1007/978-3-031-91107-1_15. Ochiq versiya: ePrint 2025/437. DOI / URL
20. 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. DOI / URL
21. Beyne T., Flórez-Gutiérrez A., Todo Y. Accurate Parameter Estimates for Punctured Key Recovery Linear Attacks. IACR Communications in Cryptology. 2026;3(2). Nashr: 03.08.2026. DOI 10.62056/ava3z11w9p. DOI / URL
22. Ghafoori N., Miyaji A. The Related Key Boomerang Attack on ChaCha Permutation Function. Pragmatic Cybersecurity. 2026;1(2):16. Published 07.09.2026. DOI 10.53941/pc.2026.100016. DOI / URL
23. Liu C., Tian T. Dynamic Cube Attacks against Grain-128AEAD. IACR Transactions on Symmetric Cryptology. 2024(2):190–221. DOI 10.46586/tosc.v2024.i2.190-221. DOI / URL
24. Katyshev S. Yu., Malov M. Yu. Fast correlation attack on reduced GRAIN-128AEAD. Matematicheskie Voprosy Kriptografii. 2025;16(1):85–98. DOI 10.4213/mvk488. DOI / URL
25. 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. DOI / URL
26. Carlet C., Sarkar P. The Nonlinear Filter Model of Stream Cipher Redivivus. arXiv:2502.01110. 2025. Foydalanilgan versiya: preprint. DOI / URL
27. Sarkar P. The Grain Family of Stream Ciphers: an Abstraction, Strengthening of Components and New Concrete Instantiations. arXiv:2511.12981. 2025. Foydalanilgan versiya: preprint. DOI / URL
28. Rukhin A. va boshqalar. 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. DOI / URL

(cc) BY *dtai.uz*

29. Python Cryptographic Authority. Authenticated encryption. Cryptography 46.0.0 documentation. 2025. DOI / URL
30. O‘zbekiston Respublikasi Markaziy banki. Masofadan bank xizmatlarini ko‘rsatuvchi tizimlardan foydalanuvchilarning soni 2025-yil 1-iyul holatiga. Nashr: 25.07.2025; yangilanish: 29.07.2025. DOI / URL
31. O‘zbekiston Respublikasi Suv xo‘jaligi vazirligi, Amu-Surxon ITHB. Seminar bahona kamchiliklar oydinlashdi. 09.07.2025. DOI / URL
32. Rescorla E., Tschofenig H., Modadugu N. The Datagram Transport Layer Security (DTLS) Protocol Version 1.3. RFC 9147. 2022. DOI / URL
33. O‘zbekiston Respublikasining «Shaxsga doir ma’lumotlar to‘g‘risida»gi O‘RQ-547-son Qonuni. 02.07.2019. LexUZdagi 27.09.2026 holatiga ochilgan amaldagi tahrir. DOI / URL
34. O‘zbekiston Respublikasining «Kiberxavfsizlik to‘g‘risida»gi O‘RQ-764-son Qonuni. 15.04.2022. LexUZdagi 27.09.2026 holatiga ochilgan amaldagi tahrir. DOI / URL

(cc) BY *dtai.uz*