DOI: 10.65322/j.srd.05192026.24

AXBOROT XAVFSIZLIGI TIZIMLARIDA KRIPTOGRAFIK ALGORITMLARNING AMALIY SAMARADORLIGI TAHLILI

Xaydarov K.S., *PhD,*
Shokirov D.A., *PhD,*
E-mail:kamoliddin1506@gmail.com
Namangan davlat texnika universiteti

Annotatsiya: *Maqolada axborot xavfsizligi tizimlarida qo‘llanadigan kriptografik algoritmlarning amaliy samaradorligi (throughput, latency, CPU/RAM, energiya va xavfsizlik darajasi) ko‘p mezonli yondashuvda baholanadi. Tahlil simmetrik AEAD (AES-GCM, ChaCha20-Poly1305), klassik assimetrik (RSA-2048/4096, ECC P-256) va post-kvant standartlari (Kyber → ML-KEM; Dilithium → ML-DSA) bo‘yicha rasmiy standartlar hamda reproduksiyalanadigan benchmark manbalariga tayangan holda tuzildi. Natijalar apparat tezlatgichlar (AES-NI) va platforma sinfi (server/ARM/embedded) algoritm tanloviga bevosita ta'sir qilishini ko‘rsatadi.*

Abstract: *This paper analyzes the practical efficiency of cryptographic algorithms used in information security systems using a multi-metric methodology (throughput, latency, CPU/RAM footprint, energy, and security level). The study covers symmetric AEAD schemes (AES-GCM, ChaCha20-Poly1305), classical public-key algorithms (RSA-2048/4096, ECC P-256), and post-quantum standards currently standardized by NIST (Kyber → ML-KEM; Dilithium → ML-DSA). Findings emphasize that hardware acceleration (e.g., AES-NI) and platform class (server vs. ARM/embedded) dominate real-world performance, while PQC adoption introduces bandwidth and key/signature size trade-offs requiring crypto-agile deployment strategies.*

Kalit so‘zlar: *axborot xavfsizligi, kriptografik algoritmlar, AEAD, AES-GCM, ChaCha20-Poly1305, RSA, ECC P-256, post-kvant kriptografiya, ML-KEM, ML-DSA, benchmark, crypto agility.*

Keywords: *information security, cryptographic algorithms, AEAD, AES-GCM, ChaCha20-Poly1305, RSA, ECC P-256, post-quantum cryptography, ML-KEM, ML-DSA, benchmarking, crypto agility.*

Kirish. Axborot xavfsizligida shifrlash va autentifikatsiya amaliyoti odatda "kriptografik mustahkamlik" (formal xavfsizlik) bilan cheklanmaydi: real tizimlar uchun kechikish (latency), o‘tkazuvchanlik (throughput), resurs iste'moli (CPU/RAM/energiya), implementatsiya xatarlari (nonce reuse, side-channel), moslik va standartlarga muvofiqlik ham bir xil darajada muhimdir. Ayniqsa, TLS/DTLS, VPN, ma'lumotlar bazasi shifrlashi, IoT telemetriyasi kabi ish yuklarida algoritm tanlovi tizimning umumiy SLA/UX ko‘rsatkichlariga bevosita ta'sir qiladi [1].

Muammo shundaki, algoritmlar "tez/sek" bo‘yicha oddiy taqqoslashga yomon bo‘ysunadi: masalan, AES-GCM server CPUlarida apparat tezlatgich bilan juda tez ishlashi mumkin, lekin AES tezlatgichi yo‘q ARM/embedded muhitda ChaCha20-Poly1305 ustun bo‘lishi kuzatiladi [2].

Bundan tashqari, post-kvant davrga tayyorgarlik kontekstida RSA/ECC kabi klassik ochiq-kalit mexanizmlari Shor algoritmi tufayli konseptual risk ostida [3]; simmetrik algoritmlar esa Grover algoritmi sabab xavfsizlik zaxirasini oshirish (masalan, AES-256) kabi strategiyalarni talab qiladi [4]. Natijada, tizimlar "crypto-agility" tamoyiliga tayangan holda ML-KEM/ML-DSA kabi post-kvant standartlariga bosqichma-bosqich o‘tishni rejalashtirishi lozim.

Maqolaning maqsadlari quyidagicha shakllantirildi: (i) AES-GCM va ChaCha20-Poly1305'ni turli platforma sinflarida amaliy samaradorlik mezonlari asosida taqqoslash; (ii) RSA-2048/4096 va ECC P-256'ning operatsion xarajatini (imzo, verifikatsiya, key exchange) real tizim kontekstida baholash; (iii) ML-KEM va ML-DSA'ning (Kyber/Dilithium) o‘lcham/performance

DOI: 10.65322/j.srd.05192026.24

ko‘rsatkichlari va resurs profilini klassik algoritmlar bilan bir jadvalda ko‘rsatish; (iv) arxitektura darajasida amaliy tavsiyalar, qo‘llash ssenariylari va cheklovlarni berish.

Simmetrik shifrlash bo‘yicha zamonaviy de-fakto standart sifatida AES blok shifri FIPS 197'da tasdiqlangan bo‘lib, 128-bit blok va 128/192/256-bit kalitli variantlar (AES-128/192/256) belgilangan [5]. AEAD (Authenticated Encryption with Associated Data) ehtiyojlari uchun AES ustida qurilgan GCM rejimi (SP 800-38D) keng tarqalgan: u confidentiality va integrity'ni bir operatsiyada beradi va autentifikatsiya tegi bilan ishlaydi; ammo GCM xavfsizligi uchun IV/nonce takrorlanmasligi kritiklikka ega, standart esa bir xil kalit bilan IV takrorlanish ehtimolini qat'iy cheklash zarurligini ochiq aytadi [6].

IETF ekotizimida ChaCha20 va Poly1305 asosidagi AEAD (ChaCha20-Poly1305) RFC 8439 bilan normativ aniqlangan; bu konstruktsiya apparat AES tezlatgichi bo‘lmagan platformalarda barqaror va tez ishlashi uchun amaliy protokollarda (jumladan TLS) keng joriy etilgan [7]. TLS 1.3 (RFC 8446) amaliy profil sifatida muhim: u mandatory-to-implement sifatida AES-128-GCM'ni majburiy qiladi va ChaCha20-Poly1305'ni implementatsiya qilishni tavsiya etadi. Bu holat ishlab chiquvchi uchun "kamida ikki AEAD" konsepsiyasini amaliy defaultga aylantiradi [1].

Klassik ochiq-kalit kriptografiyada RSA spetsifikatsiyasi PKCS#1 (RFC 8017) orqali keng qo‘llanadi [8]; NIST SP 800-56B Rev.2 esa RSA asosidagi key establishment'ni standartlashtiradi va RSA modulus uzunligi bo‘yicha taxminiy xavfsizlik kuchini beradi (masalan, 2048 → 112 bit, 4096 → 152 bit) [9]. ECC yo‘nalishida NIST SP 800-186 AQSh hukumatida tavsiya etilgan elliptik egri chiziqlar to‘plamini belgilaydi va klassik Weierstrass egri chiziqlar bilan bir qatorda yangi Edwards egri chiziqlarni ham ko‘rsatadi; amaliyotda P-256 (secp256r1) eng keng tarqalgan NIST egrilaridan biri bo‘lib qolmoqda (ayniqsa TLS va PKI'da) [10].

Post-kvant yo‘nalishida NIST IR 8105 quantum xavfini va crypto-agility zaruratini urg‘ulaydi; Shor (faktorizatsiya va diskret log) va Grover (qidiruv) algoritmlari nazariy bazani tashkil etadi [11]. NIST tomonidan yakuniy standart sifatida chiqarilgan FIPS 203 (ML-KEM) va FIPS 204 (ML-DSA) amaliy migratsiya uchun "rasmiy tayanch" hujjatlar bo‘lib, ular parametr to‘plamlari, kalit/kripto-matn/imzo o‘lchamlari, implementatsiya talablarini normativ belgilaydi va xavfsizlik ↔ performance trade-off'larini parametr darajasida eksplisit qiladi [12, 13]. Samaradorlikni baholashda akademik hamjamiyat va ochiq benchmark tashabbuslari (masalan, eBACS/eBATS) "turli arxitektura, turli implementatsiya" kontekstida o‘lchovlarni tizimlashtirishga harakat qiladi; bu esa "bir jadval – hamma holat" yondashuvining noto‘g‘riligini yana bir bor tasdiqlaydi [14].

Materiallar va metodlar. Maqola "meta-benchmark" yondashuviga tayandi: yagona laboratoriya stendi bilan cheklanmasdan, rasmiy standartlar (parametrlar, xavfsizlik kategoriyalari, foydalanish cheklovlari) va reproduksiyalanadigan o‘lchov natijalari (turli platformalarda benchmark) kombinatsiya qilindi. Bu yondashuv real dunyo tizimlarida uchraydigan "server ↔ mobil ↔ embedded" heterogenligini qamrab oladi [2]. Ma'lumotlarning asosiy bloklari quyidagilardan iborat:

– *AEAD throughput:* IETF konferensiya slaydlarida Intel Xeon E5-2690 (AES-NI yoqilgan/yoqilmagan) va ARM Cortex-A9 uchun AES-128-GCM hamda ChaCha20-Poly1305 o‘tkazuvchanligi (MB/s) keltirilgan [2];

– *Public-key "ops/s" profili:* Cloudflare ishlab chiqarish profilingi asosida bitta yadro uchun RSA/ECDSA/ECDHE tezliklarini (signatures/s va operations/s) e'lon qilgan (BoringSSL speed) [15];

– *PQC cycles/RAM:* Kyber Round 3 spetsifikatsiyasi Intel Haswell (Core i7-4770K) uchun cycle counts va Cortex-M4 uchun cycle+RAM o‘lchovlarini, shuningdek KAT (Known Answer Tests) joylashuvini beradi [16];

DOI: 10.65322/j.srd.05192026.24

– *PQC imzo cycles:* Dilithium rasmiy sahifasi Skylake (Core i7-6600U) uchun reference va AVX2 optimizatsiyalangan cycle ko‘rsatkichlarini beradi [17];

– *PQC energiya/vaqt:* resurs-cheklangan qurilmalarda (Raspberry Pi sinfi) KEM'lar bo‘yicha "execution time, power consumption, memory usage" o‘lchovlarini bergan ishlar tahlilga kiritildi [18].

Metrikalar va baholash mezonlari. Ushbu maqolada metrikalar quyidagicha operatsionlashtirildi:

– *Throughput (MB/s):* katta hajmli oqimlarda AEAD'ning "bulk data" ishlash tezligi [2];

– *Latency:* (a) public-key operatsiyalarda ops/s orqali; (b) PQC'da cycles (va imkon qadar platforma chastotasi ma'lum bo‘lsa – taxminiy vaqt) [15];

– *CPU/RAM:* Cortex-M4 uchun Kyber spetsifikatsiyasidagi RAM usage; ishlab chiqarish profilingida TLS kriptografiya stack'ining CPU ulushi [15, 16];

– *Energy:* Raspberry Pi asosidagi tajribadan Watt qiymatlari (low-load/high-load) va execution time [18];

– *Xavfsizlik darajasi:* (a) NIST SP 800-57 jadvali bo‘yicha klassik ekvivalent; (b) ML-KEM/ML-DSA parametr setlari uchun FIPS'larda berilgan security category va o‘lchamlar; (c) RSA modulus uzunligi bo‘yicha SP 800-56B Rev.2 estimatsiyasi [9, 19].

Test vektorlar va validatsiya. Amaliy implementatsiya sifatini tekshirish (correctness + konformatsiya) uchun quyidagi "test vector" va validatsiya yo‘llari normativ hisoblanadi. NIST CAVP (Cryptographic Algorithm Validation Program) tasdiqlangan algoritmlar implementatsiyasini validatsiyalash uchun asos bo‘lib, kriptomodul validatsiyasi (CMVP) uchun ham pre-rekvizit sifatida ko‘rsatiladi [20]. GCM uchun NIST SP 800-38D algoritmik tavsifi (IV konstruksiyasi, tag verifikatsiyasi) va IV uniqueness talabi test va audit tekshiruvlarida muhim nazorat nuqtalaridir [6]. ChaCha20-Poly1305 uchun RFC 8439 test vektorlari amaliy implementatsiyalarda moslikni tekshirishga xizmat qiladi [7]. Kyber Round 3 spetsifikatsiyasida KAT fayllari kataloglari va NIST PQCgenKAT_kem yordamida generatsiya qilinganligi ko‘rsatiladi (bu, amalda, regressiya test pipeline'iga mos keladi) [16].

Chegaralar va farazlar/ Bu ishning eng muhim farazi: turli manbalardagi benchmarklar bir xil kutubxona, bir xil kompilyator flagi, bir xil mikroarxitektura va bir xil workload profiliga ega emas; demak, absolut raqamlarni "adolatli universal reyting" sifatida talqin qilish mumkin emas. Shu bois natijalar ko‘proq trend va qaror qoidalari (decision rules)ni chiqarishga yo‘naltirildi [14].

Natijalar va muhokama. Tahlil natijalari to‘rt yo‘nalish bo‘yicha – simmetrik AEAD, klassik ochiq-kalit kriptografiya, post-kvant standartlari hamda energiya va resurs sarfi bo‘yicha – keltiriladi.

Simmetrik AEAD: throughput va platformaga bog‘liqlik. 1-jadvalda bir xil manbada keltirilgan o‘lchovlar (MB/s) asosida AES-128-GCM va ChaCha20-Poly1305'ning platformaga sezgirligi ko‘rsatilgan [2].

1-jadval

Simmetrik AEAD algoritmlarining o‘tkazuvchanligi (MB/s) turli platformalarda

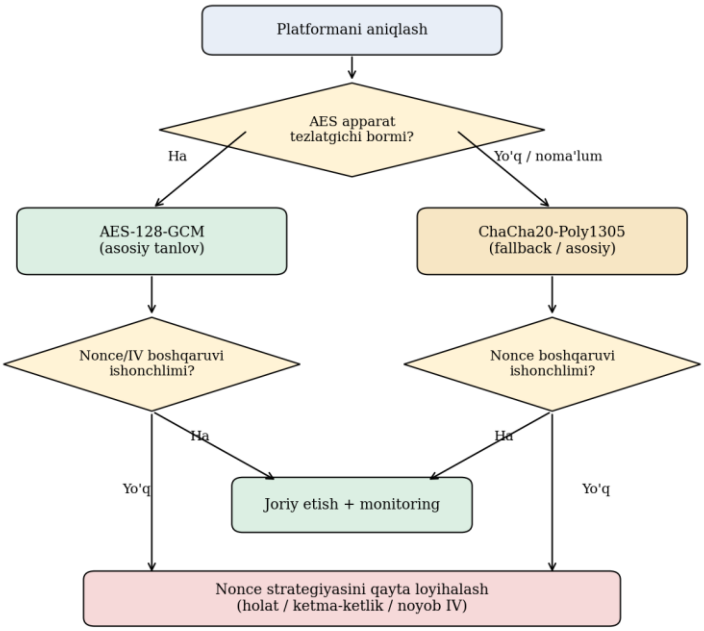
Platforma / sharoit	AES-128-GCM, MB/s	ChaCha20-Poly1305, MB/s	Izoh
Intel Xeon E5-2690, AES-NI o‘chiq	131	427	AES-NI yo‘q holatda ChaCha ustun
Intel Xeon E5-2690, AES-NI yoqiq	892	427–560	AES-NI bilan AES-GCM ustun; ChaCha kompilyatsiya optimizatsiyasi bilan oshadi
ARM Cortex-A9 @1.2 GHz	25	92	AES tezlatgichsiz ARM'da ChaCha ustun

DOI: 10.65322/j.srd.05192026.24

Manba: [2].

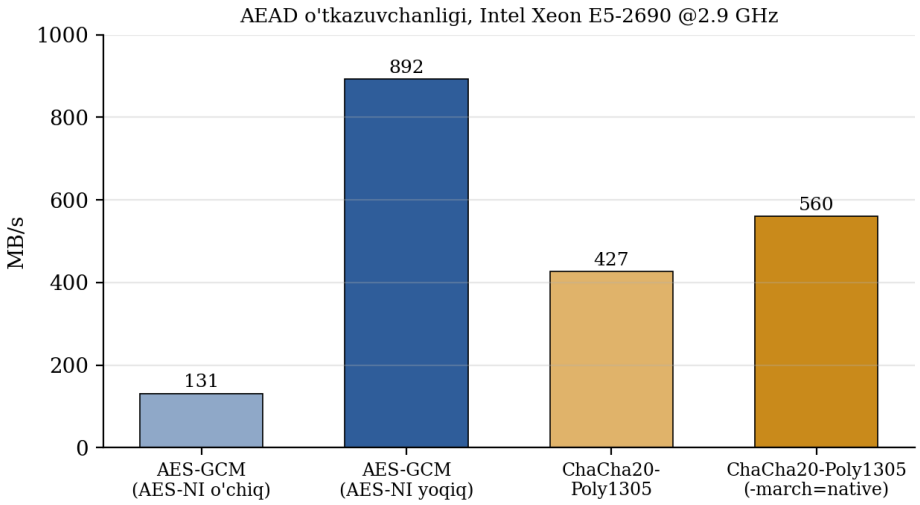
Ushbu ma'lumotlar asosida amaliy xulosa shuki: server tomonida AES-NI/ARMv8 Crypto Extensions kabi tezlatgichlar mavjud bo‘lsa, AES-GCM default bo‘lishi iqtisodiy; aks holda (mobil/embedded/ba'zi VM instanslar) ChaCha20-Poly1305 ko‘pincha yaxshiroq yoki barqarorroq ishlaydi [2].

GCM'da nonce/IV reuse xavfi juda kritik: SP 800-38D bitta kalit ostida IV takrorlanish ehtimoli bo‘yicha qat'iy talab qo‘yadi hamda bu talabga rioya qilish GCM xavfsizligi uchun "kalit maxfiyligi"ga yaqin ahamiyatga ega ekanini urg‘ulaydi [6]. 1-rasmda AEAD tanlovining "qaror oqimi" soddalashtirib berilgan.



1-rasm. AEAD algoritmini tanlash bo‘yicha qaror oqimi

2-rasmda Intel Xeon E5-2690 misolida throughput'ning vizual taqqoslanishi keltirilgan; qiymatlar IETF o‘lchovlaridan olingan [2].



2-rasm. AEAD o‘tkazuvchanligi (MB/s), Intel Xeon E5-2690 @2.9 GHz

DOI: 10.65322/j.srd.05192026.24

Ochiq-kalit kriptografiya: RSA va ECC amaliy "qimmatligi"

Real tizimlarda (xususan TLS) ochiq-kalit operatsiyalar ko‘pincha sessiyaning boshida bajariladi, ammo ular "spike" yuklanish (handshake storm) ssenariylarida CPU bottleneck bo‘lishi mumkin. Cloudflare profilingi buni raqam bilan ko‘rsatadi: RSA imzolari ECDSA'ga nisbatan keskin sekin (RSA-4096 ayniqsa) [15]. 2-jadval Cloudflare e'lon qilgan bitta yadro tezliklari asosida tuzildi.

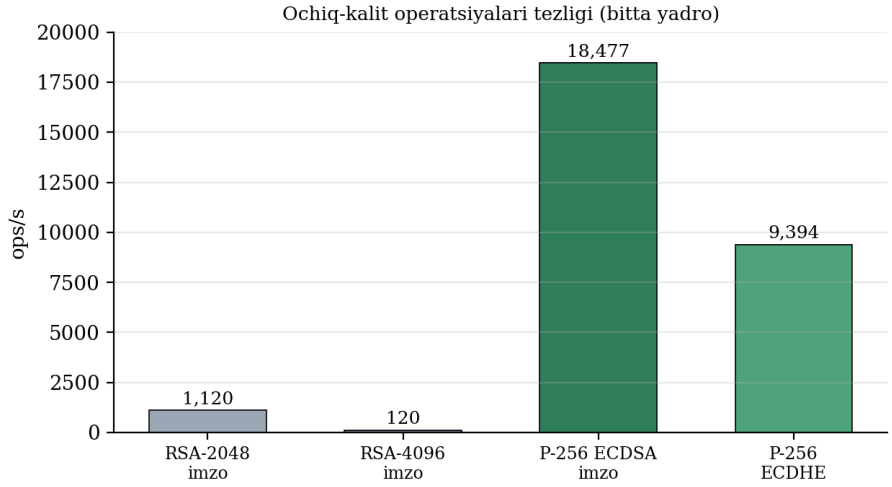
2-jadval

Ochiq-kalit operatsiyalarining bitta yadrodagi tezligi

Operatsiya (bitta yadro)	Tezlik, ops/s	Amaliy talqin
RSA-2048 signature	1,120	PKI'da CPU qimmat
RSA-4096 signature	120	"High assurance" oshishi katta performance narxiga ega
P-256 ECDSA signature	18,477	RSA'dan o‘nlab marta tez
P-256 ECDHE	9,394	Key exchange xarajati

Manba: [15].

RSA kalit uzunligining kriptografik kuchi ham to‘g‘ridan-to‘g‘ri "2048/4096" raqamiga teng emas: NIST SP 800-56B Rev.2 jadvalida RSA-2048 ≈ 112-bit, RSA-4096 ≈ 152-bit maksimal xavfsizlik kuchi sifatida baholanadi [9]. ECC P-256 ekvivalenti klassik NIST jadvaliga ko‘ra 128-bit xavfsizlik diapazoniga mos keladi (ECC order "f" 256...383 oralig‘i 128-bit strength qatorida) [19]. 3-rasmda RSA va ECC farqi (ops/s) ko‘rsatilgan; qiymatlar Cloudflare profilingidagi BoringSSL speed natijalaridan olingan [15].



3-rasm. Ochiq-kalit operatsiyalarining bitta yadrodagi tezligi (ops/s)

Post-kvant standartlari: ML-KEM va ML-DSA'ning "o‘lcham – ishlash – resurs" profili. Post-kvant migratsiyada asosiy amaliy muammo – xavfsizlikdan tashqari bandwidth va hisoblash xarajati. FIPS 203 ML-KEM uchun 3 ta parametr setni belgilaydi va kalit/ciphertext o‘lchamlarini aniq beradi (3-jadval) [12].

3-jadval

ML-KEM parametr to‘plamlari va o‘lchamlari (bayt)

ML-KEM parametr seti	Inkapsulyatsiya kaliti, B	Dekapsulyatsiya kaliti, B	Shifrmatn, B	Xavfsizlik kategoriyasi
ML-KEM-512	800	1632	768	1
ML-KEM-768	1184	2400	1088	3

DOI: 10.65322/j.srd.05192026.24

ML-KEM parametr seti	Inkapsulyatsiya kaliti, B	Dekapsulyatsiya kaliti, B	Shifrmatn, B	Xavfsizlik kategoriyasi
ML-KEM-1024	1568	3168	1568	5

Manba: [12].

ML-DSA (FIPS 204) ham shunga o‘xshash tarzda kalit va imzo o‘lchamlarini beradi (4-jadval): imzolar ECDSA'dan kattaroq, ammo standartlashtirilgan parametrlar bilan boshqariladi [13].

4-jadval

ML-DSA parametr to‘plamlari va o‘lchamlari (bayt)

ML-DSA parametr seti	Maxfiy kalit, B	Ochiq kalit, B	Imzo, B	Xavfsizlik kategoriyasi
ML-DSA-44	2560	1312	2420	2
ML-DSA-65	4032	1952	3309	3
ML-DSA-87	4896	2592	4627	5

Manba: [13].

Ishlash (latency) nuqtayi nazaridan Kyber (ML-KEM'ning ildizi) Round 3 spetsifikatsiyasida Haswell uchun cycle counts keltirilgan; AVX2 optimizatsiyasi sezilarli tezlik beradi. Masalan, Kyber768 (ML-KEM-768 bilan o‘lcham jihatdan mos) uchun AVX2'da keygen ~52 732 cycles, encaps ~67 624 cycles, decaps ~53 156 cycles [16]. Embedded kontekstda ham Kyber spetsifikatsiyasi Cortex-M4 uchun cycle va RAM usage ko‘rsatadi; bu IoT uchun juda muhim, chunki RAM ko‘pincha "hard cap" hisoblanadi [16].

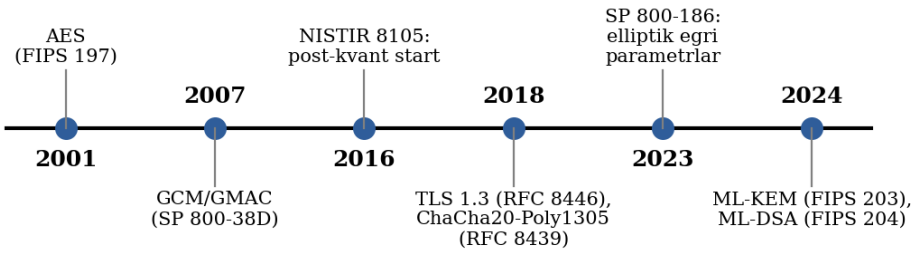
Dilithium (ML-DSA ildizi) bo‘yicha rasmiy sahifada Skylake uchun cycle ko‘rsatkichlari keltirilgan: Dilithium3 (ML-DSA-65 o‘lchamlariga yaqin) AVX2'da keygen ~256 403 cycles, sign ~529 106 cycles, verify ~179 424 cycles [17]. Bu raqamlar "klassik" ECDSA bilan bevosita bir xil sharoitda o‘lchanmagan bo‘lsa-da, amaliy xulosa shuki: PQC KEM'lar (ML-KEM) ko‘pincha juda tez, ammo imzo sxemalari (ML-DSA) bandwidth va o‘lcham hisobiga keladi (2,4–4,6 KB signature) [16].

Energiya va resurs-cheklangan qurilmalar

Resurs-cheklangan muhitlarda PQC'ni baholagan tajribiy ishlar Kyber oilasining energiya nuqtayi nazaridan ham ma'qul ko‘rinishini ko‘rsatadi: masalan, Raspberry Pi asosidagi testbed'da Kyber-512/768/1024 "high-load" sharoitida taxminan 3,5 W (client) va 3,9 W (server) atrofida qayd etiladi; execution time esa ~0,041–0,042 s darajasida berilgan [18]. Bu natijalar shuni anglatadiki, PQC'ni "faqat sekin va og‘ir" deb qabul qilish noto‘g‘ri: KEM darajasida Kyber/ML-KEM ko‘pincha juda raqobatbardosh; asosiy muammo ko‘proq bandwidth va PKI artefaktlari (sertifikat, imzo, handshake hajmi)da paydo bo‘ladi [18].

Standartlashuv va migratsiya vaqt chizig‘i

4-rasmda amaliyotda ko‘p uchraydigan standartlarning "qachon paydo bo‘lganini" va post-kvant standartlarning qayerda turganini ko‘rsatuvchi vaqt chizig‘i keltirilgan [1, 5, 6, 7, 10–13].



4-rasm. Kriptografik standartlar evolyutsiyasi (tanlab)

DOI: 10.65322/j.srd.05192026.24

Amaliy tavsiyalar. TLS / API gateway / microservice. TLS 1.3 profili uchun AES-128-GCM'ni majburiy, ChaCha20-Poly1305'ni tavsiya qilingan cipher suite sifatida implementatsiya qilish amaliy minimum. Serverlarda AES-NI mavjudligi ko‘pincha AES-GCM'ni ustun qiladi; mobil/embedded uchun ChaCha20-Poly1305 muhim "fallback" hisoblanadi [1].

Nonce boshqaruvi. AES-GCM'da IV takrorlanish xavfi eng yirik implementatsion xatarlardan. SP 800-38D IV uniqueness talabini normativ darajada belgilaydi; ishlab chiqarishda IV strategiyasi (sequence number, per-key counter, device/context fixed field) audit qilinishi shart [6].

PKI va sertifikatlar. RSA-4096 "kuchliroq" bo‘lsa ham, performance narxi juda yuqori; RSA-2048 ham ECDSA'ga nisbatan qimmat. Shuning uchun amaliyotda P-256 ECDSA sertifikatlari ko‘pincha "tejamkor + yetarli" yechim (klassik xavfsizlik nuqtayi nazaridan) bo‘lib, RSA faqat moslik talablarida qoladi [15].

PQC migratsiya. Uzoq muddatli maxfiylik ("harvest now, decrypt later") riskli segmentlarda key establishment uchun ML-KEM'ni pilot qilish (ko‘pincha gibrid shaklda) pragmatik; FIPS 203 ML-KEM o‘lchamlari tarmoq overheadini oldindan hisoblash imkonini beradi [12].

Imzo migratsiyasi. ML-DSA imzolari (2,4–4,6 KB) sertifikat/handshake hajmini oshiradi, ammo standartlashgan parametrlarga ega; bu PKI'da chain hajmi, MTU/fragmentatsiya, handshake memory va rate-limit siyosatiga ta'sir qiladi. Shuning uchun ML-DSA joriy etish "traffic engineering" va "certificate lifecycle" bilan birga rejalashtirilishi kerak [13].

IoT/edge. Energiya va resurs cheklovlari uchun KEM darajasida Kyber/ML-KEM ko‘pincha maqbul, ammo RAM/flash cheklovi qat'iy bo‘lgan MCUlarda implementatsiya tanlovi (optimallashtirilgan vs "clean") va stack/heap profili alohida sinovdan o‘tishi shart [16].

Cheklovlar

Birinchi cheklov – benchmark heterogenligi: keltirilgan throughput/ops/cycles turli platforma, turli implementatsiya va turli kompilyatsiya flaglari bilan o‘lchangan; shuning uchun ular "universal reyting" emas, "trend va qaror qoidalari" sifatida talqin qilinadi [14].

Ikkinchi cheklov – side-channel va constant-time: yuqori tezlikka erishgan optimizatsiyalar (SIMD/AVX2) doim ham bir xil threat modelga mos emas; real tizimlarda constant-time talablari va validatsiya (CAVP/CMVP) yo‘nalishiga mos kelish talab etiladi [20].

Uchinchi cheklov – post-kvant ekotizim: FIPS 203/204 standartlari mavjud bo‘lsa-da, protokol integratsiyasi (TLS, PKI, HSM, smart-card) "operatsion tayyorgarlik" (agility, monitoring, fallback, roll-back) bilan birga kechadi; NISTIR 8105 bu muammoni strategik darajada ko‘taradi [11].

Xulosa. Keltirilgan tahlil shuni ko‘rsatadiki, kriptografik algoritm tanlovi "mustahkamlik" va "tezlik"dan ko‘ra kengroq masala: real tizimlar uchun apparat tezlatgichlar, nonce boshqaruvi, ochiq-kalit operatsiyalar xarajati, energiya va bandwidth cheklovlari, hamda post-kvant migratsiya strategiyasi bir butun sifatida ko‘rilishi zarur.

AES-GCM serverlarda (AES-NI bilan) eng yaxshi throughput'ni beradi, ChaCha20-Poly1305 esa tezlatgichsiz ARM/embedded muhitlarda ko‘pincha ustun. RSA (ayniqsa 4096) amaliy jihatdan qimmat, ECC P-256 esa juda samarali.

Post-kvant standartlari sifatida ML-KEM/ML-DSA "parametrli trade-off" modelini beradi: KEM darajasida Kyber/ML-KEM juda raqobatbardosh bo‘lsa-da, imzo artefaktlari hajmi PKI va transport qatlamiga sezilarli ta'sir qiladi.

Bugungi tizimlar uchun amaliy jihatdan eng maqbul ssenariy: AES-GCM + ChaCha20-Poly1305 "dual-stack", P-256/ECDHE (yoki zamonaviy profillarda X25519) asosidagi key exchange va sertifikatlarda ECDSA yo‘nalishini saqlagan holda, "uzoq muddatli maxfiylik" talab

DOI: 10.65322/j.srd.05192026.24

qilinadigan segmentlarda gibrid (klassik + ML-KEM) kelishuvga bosqichma-bosqich o‘tish hamda PKI qatlamida ML-DSA'ni pilot joriy etish (crypto-agility bilan).

Adabiyotlar ro‘yxati

1. Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3: RFC 8446. – IETF, 2018. – doi:10.17487/RFC8446. – URL: https://datatracker.ietf.org/doc/html/rfc8446

2. IETF 88, TLS ishchi guruhi taqdimot slaydlari (AES-GCM va ChaCha20-Poly1305 o‘tkazuvchanligi). – URL: https://www.ietf.org/proceedings/88/slides/slides-88-tls-1.pdf

3. O‘zbekiston Respublikasi. “Kiberxavfsizlik to‘g‘risida”gi Qonun. Toshkent shahri, 2022-yil 15-aprel, O‘RQ-764-son.

4. Grover L.K. A fast quantum mechanical algorithm for database search. – 1996. – URL: https://arxiv.org/abs/quant-ph/9605043

5. Sayfullayevich, X. K., & Qizi, A. H. R. (2024). CISCO MARSHRUTIZATORINI SOZLASH VA ISHLASH JARAYONINI TEKSHIRISH. Механика и технология, 4(17), 260-263. 6. International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information Security Management Systems (ISMS). Geneva, Switzerland. 7. Xaydarov, K. S. (2025). ZAMONAVIY TARMOQ XAVFSIZLIGINI TA'MINLASHDA CISCO PACKET TRACER DASTURINI IMKONIYATLARI. Экономика и социум, (1-2 (128)), 509-512.

7. Nir Y., Langley A. ChaCha20 and Poly1305 for IETF Protocols: RFC 8439. – IETF, 2018. – doi:10.17487/RFC8439. – URL: https://datatracker.ietf.org/doc/html/rfc8439

8. PKCS #1: RSA Cryptography Specifications Version 2.2: RFC 8017. – IETF, 2016. – doi:10.17487/RFC8017.

9. NIST SP 800-56B Rev.2: Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography. – 2019. – doi:10.6028/NIST.SP.800-56Br2. – URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Br2.pdf

10. NIST SP 800-186: Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters. – 2023. – doi:10.6028/NIST.SP.800-186. – URL: https://csrc.nist.gov/pubs/sp/800/186/final