MUHANDISLIK & IQTISODIYOT

ijtimoiy-iqtisodiy, innovatsion texnik,
fan va ta'limga oid ilmiy-amaliy jurnal

№2
MAXSUS SON

2026
MART

Milliy nashrlar
OAK: https://oak.uz/pages/4802

05.00.00 - Texnika fanlari
08.00.00 - Iqtisodiyot fanlar

Google Scholar · OPEN ACCESS · ULRICHSWEB GLOBAL SERIALS DIRECTORY · Academic Resource Index ResearchBib · ISSN INTERNATIONAL STANDARD SERIAL NUMBER INTERNATIONAL CENTRE · CYBERLENINKA · OpenAIRE · ROAD · INDEX COPERNICUS INTERNATIONAL · BASE · Crossref · НАУЧНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА eLIBRARY.RU

BAKALAVR TALABALARINIG MAQOLALARI TO'PLAMI

РЭУ.РФ РОССИЙСКИЙ ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ Г.В. ПЛЕХАНОВА ТАШКЕНТСКИЙ ФИЛИАЛ · TDIU · TDTU · TOSHKENT DAVLAT TRANSPORT UNIVERSITETI · TOSHKENT ARXITEKTURA-QURILISH UNIVERSITETI · TOSHKENT KIMYO-TEXNOLOGIYA INSTITUTI · JIZPI

Elektron nashr, 45 sahifa,
mart, 2026-yil.

muhandislik & iqtisodiyot

ijtimoiy-iqtisodiy, innovatsion texnik,
fan va ta'limga oid ilmiy-amaliy jurnal

muhandislik & iqtisodiyot

ijtimoiy-iqtisodiy, innovatsion texnik,
fan va ta’limga oid ilmiy-amaliy jurnal

MUNDARIJA • СОДЕРЖАНИЕ • CONTENTS

Ma’lumot uchun, OAK Rayosatining 2024-yil 28-avgustdagi 360/5-son qarori bilan “Dissertatsiyalar asosiy ilmiy natijalarini chop etishga tavsiya etilgan milliy ilmiy nashrlar ro‘yxati”ga texnika va iqtisodiyot fanlari bo‘yicha “Muhandislik va iqtisodiyot” jurnali ro‘yxatga kiritilgan.

Muassis: “Tadbirkor va ishbilarmon” MChJ
Hamkorlarimiz:
1. Toshkent shahridagi G.V.Plexanov nomidagi Rossiya iqtisodiyot universiteti
2. Toshkent davlat iqtisodiyot universiteti
3. Toshkent irrigatsiya va qishloq xo‘jaligini mexanizatsiyalash muhandislari instituti” milliy tadqiqot universiteti
4. Islom Karimov nomidagi Toshkent davlat texnika universiteti
5. Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
6. Toshkent davlat transport universiteti
7. Toshkent arxitektura-qurilish universiteti
8. Toshkent kimyo-texnologiya universiteti
9. Jizzax politexnika instituti

MUNDARIJA • СОДЕРЖАНИЕ • CONTENTS

MUNDARIJA

TASHKILOT AXBOROT TIZIMLARINI KVANT TAHDIDLARIDAN HIMOYALASHDA POST-KVANT KRIPTOGRAFIK ALGORITMLARNI QO‘LLASH

G‘ofurova Muxlisa G‘ulom qizi
Toshkent ijtimoiy innovatsiya universiteti
Iqtisodiyot va pedagogika fakulteti 2-bosqich talabasi
muxlisagofurova18@gmail.com

Ilmiy rahbar :
Tursunova Sadoqat Abdusalom qizi
Toshkent ijtimoiy innovatsiya universiteti
Iqtisodiyot va raqamli texnologiyalar kafedrasi katta o‘qituvchisi

Annotatsiya: Zamonaviy tashkilotlarning axborot tizimlari kriptografik himoyaning yangi avlodiga – post-kvant kriptografiyaga (Post-Quantum Cryptography, PQC) o‘tishni talab qilmoqda. Ushbu maqolada kvant kompyuterlarining an’anaviy kriptografik algoritmlar – RSA, ECC va Diffie–Hellman tizimlariga bo‘lgan tahdidi IMRAD metodologiyasi asosida tahlil qilingan. Shuningdek, 2024-yilda NIST tomonidan standartlashtirilgan CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON va SPHINCS+ algoritmlarining nazariy asoslari hamda amaliy qo‘llanish imkoniyatlari o‘rganilgan. Tadqiqot natijalari asosida tashkilotlar uchun post-kvant kriptografiyaga o‘tishning bosqichma-bosqich migratsiya strategiyasi ishlab chiqilgan hamda xarajat-foyda (cost-benefit) tahlili amalga oshirilgan. Shuningdek, O‘zbekiston Respublikasining 2024-yildagi PQ-293-son qarorida kriptologiya sohasini rivojlantirish bo‘yicha belgilangan vazifalar doirasida milliy axborot xavfsizligi tizimini mustahkamlashga qaratilgan amaliy tavsiyalar taqdim etilgan.

Kalit so‘zlar: post-kvant kriptografiya, kvant kompyuterlar, CRYSTALS-Kyber, NIST standartlari, axborot xavfsizligi, panjara asosidagi kriptografiya, gibrid kriptografiya, “hozir yig‘ib keyinroq ochish” (harvest-now-decrypt-later) hujumi.

Abstract: Modern organizational information systems require a transition to a new generation of cryptographic protection known as Post-Quantum Cryptography (PQC). This article analyzes the potential threat posed by quantum computers to traditional cryptographic algorithms such as RSA, ECC, and Diffie–Hellman using the IMRAD framework. Particular attention is given to the algorithms CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, and SPHINCS+, which were standardized by the National Institute of Standards and Technology (NIST) in 2024. These algorithms are examined from both theoretical and practical perspectives. Based on the research findings, a step-by-step migration strategy toward post-quantum cryptography for organizations is proposed, accompanied by a cost-benefit analysis. Furthermore, practical recommendations are provided to strengthen the national information security system in the context of Uzbekistan’s Presidential Decree PQ-293 (2024) on the development of cryptology.

Keywords: post-quantum cryptography, quantum computers, CRYSTALS-Kyber, NIST standards, information security, lattice-based cryptography, hybrid cryptography, harvest-now-decrypt-later attack.

Аннотация: Современные информационные системы организаций требуют перехода к новому поколению криптографической защиты – постквантовой криптографии (Post-Quantum Cryptography, PQC). В данной статье в соответствии со структурой IMRAD проводится анализ угрозы квантовых компьютеров для традиционных криптографических алгоритмов RSA, ECC и Diffie–Hellman. Особое внимание уделяется алгоритмам CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON и SPHINCS+, стандартизированным Национальным институтом стандартов и технологий США (NIST) в 2024 году, которые рассматриваются с теоретической и практической точек зрения. На основе полученных результатов разработана поэтапная стратегия миграции организаций к постквантовой криптографии, а также проведён анализ затрат и ожидаемых преимуществ. В контексте Постановления Президента Республики Узбекистан № ПҚ-293 (2024 г.), направленного на развитие криптологии, предложены практические рекомендации по укреплению национальной системы информационной безопасности.

Ключевые слова: постквантовая криптография, квантовый компьютер, CRYSTALS-Kyber, стандарты NIST, информационная безопасность, криптография на решётках, гибридная криптография, атака «harvest-now-decrypt-later».

KIRISH

Raqamli iqtisodiyot va axborot texnologiyalarining tez rivojlanishi bilan bir qatorda tashkilotlarning axborot tizimlariga bo‘lgan tahdidlar ham sezilarli darajada o‘zgarib bormoqda. Bugungi kunda RSA, ECC (Elliptic Curve Cryptography) va Diffie–Hellman kabi klassik kriptografik algoritmlar korporativ ma’lumotlarni himoyalashda asosiy vositalardan biri bo‘lib xizmat qilmoqda. Biroq kvant hisoblash texnologiyalarining rivojlanishi ushbu algoritmlarning uzoq muddatli barqarorligiga nisbatan yangi xavfsizlik masalalarini yuzaga keltirishi mumkin [1, 2].

O‘zbekiston Respublikasi Prezidentining 2024-yil 15-avgustdagi PQ-293-son qarorida kriptologiya sohasida ta’lim va ilm-fanni rivojlantirish bo‘yicha qator muhim chora-tadbirlar belgilangan. Qarorning so‘z boshisida shunday ta’kidlanadi: “Axborot va kiberxavfsizlik sohasidagi zamonaviy tahdidlarning ortib borishi, kvant texnologiyalariga asoslangan yuqori tezlikdagi kompyuterlarning yaratilishi axborotni himoyalashda qo‘llaniladigan kriptografik algoritmlarni doimiy ravishda takomillashtirib borishni taqozo etadi” [3]. Mazkur holat O‘zbekiston Respublikasida post-kvant kriptografiyasiga o‘tish masalasi davlat siyosatining muhim yo‘nalishlaridan biri sifatida e’tirof etilayotganini ko‘rsatadi.

Xalqaro miqyosda esa AQSh Milliy standartlar va texnologiyalar instituti (NIST) tomonidan 2016-yilda boshlangan tanlov jarayoni 2024-yilda yakunlandi. 25 ta mamlakatdan taqdim etilgan 82 ta algoritm orasidan to‘rttasi rasmiy standart sifatida tasdiqlandi [4]. Shu bilan birga, ayrim yirik texnologik kompaniyalar ham post-kvant kriptografiyasini amaliyotga bosqichma-bosqich joriy etishni boshladi. Jumladan, Apple kompaniyasi iMessage tizimi uchun PQ3 protokolini, Signal messenjeri esa PQXDH (Post-Quantum Extended Diffie–Hellman) protokolini joriy etdi [5]. Bu holat post-kvant kriptografiyasining amaliy ahamiyati ortib borayotganini ko‘rsatadi.

Mazkur maqolaning maqsadi – tashkilotlarning axborot tizimlarida kvant texnologiyalari bilan bog‘liq ehtimoliy tahdidlarni baholash, NIST tomonidan standartlashtirilgan post-kvant kriptografiya algoritmlarini qiyosiy tahlil qilish hamda O‘zbekiston tashkilotlari uchun amaliy migratsiya strategiyasini ishlab chiqishdan iborat.

MAVZUGA OID ADABIYOTLAR SHARHI

Kvant hisoblash va uning kriptografiyaga ta’siri bo‘yicha olib borilgan adabiyotlar tahlili shuni ko‘rsatadiki, so‘nggi yillarda ushbu ilmiy yo‘nalish jadal rivojlanmoqda. Xudoykulov Z. va hamkasblari tomonidan 2023-yilda Toshkent axborot texnologiyalari universitetida (TATU) yaratilgan “Kriptografik usullar” o‘quv qo‘llanmasi o‘zbek tilidagi fundamental manbalardan biri sifatida e’tirof etilib, unda kriptografiyaning matematik asoslari batafsil yoritilgan [6]. Mazkur qo‘llanmada, shuningdek, asimmetrik kriptografiyaning zamonaviy holati hamda unga ta’sir ko‘rsatishi mumkin bo‘lgan ehtimoliy tahdidlar tahlil qilingan.

Abduraximov B.F., Boyquziyev I.M. va Arabboyev A.A. tomonidan 2025-yilda “Al-Farg‘oniy avlodlari” jurnalida e’lon qilingan maqolada post-kvant kriptografiyasining beshta asosiy yo‘nalishi tahlil qilingan. Ular qatoriga panjara asosidagi, kod asosidagi, xesh asosidagi, ko‘p o‘zgaruvchili hamda izogeniya asosidagi kriptografiya kiradi. Mazkur tadqiqotda NIST tomonidan olib borilgan standartlashtirish jarayonining bosqichlari hamda tanlab olingan algoritmlarning asosiy xususiyatlari batafsil ko‘rib chiqilgan [7].

Rus tadqiqotchilaridan Fedorov A.K. 2023-yilda RusCrypto konferensiyasida tashkilotlar uchun kvant kalitlarni taqsimlash qurilmalari bilan post-kvant kriptografiya algoritmlarini kombinatsiyalash orqali axborot tizimlarini himoyalash usulini taklif etgan [8]. Ushbu yondashuv gibrid kriptografiyaning amaliy imkoniyatlarini yanada chuqurroq asoslashga xizmat qiladi. Shuningdek, Grebnyov S.V. Rossiya Federatsiyasida kvantga bardoshli raqamli imzo tizimi bo‘yicha olib borilgan Gipericum loyihasini ishlab chiqishda ishtirok etgan.

Xalqaro miqyosda Bernstein D.J. va Lange T. 2017-yilda Nature jurnalida post-kvant kriptografiyasining umumiy holati va istiqbollarini tahlil qilgan. Saidova M.R. va Karimov A.A. (TATU) tomonidan bulutli hisoblash tizimlarida autentifikatsiya jarayonlarining ayrim muammolari o‘rganilgan [9]. Alagic G. va hamkasblari 2022-yilda NIST tomonidan olib borilgan post-kvant kriptografiya standartlashtirish jarayonining uchinchi bosqichi bo‘yicha batafsil hisobotni e’lon qilgan [10].

Yaponova E. va hamkasblari 2024-yilda MDPI Technologies jurnalida post-kvant kriptografiyasining amaliy qo‘llanish yo‘nalishlari bo‘yicha keng qamrovli tahlil o‘tkazib, panjara asosidagi, kod asosidagi hamda xesh asosidagi algoritmlarning bank tranzaksiyalari, aloqa kanallari va IoT qurilmalarida qo‘llash imkoniyatlarini ko‘rib chiqqan [11].

TADQIQOT METODOLOGIYASI

Ushbu tadqiqotda quyidagi metodlar qo‘llanildi: (1) tizimli adabiyotlar tahlili – 2019-2025 yillar orasida e’lon qilingan o‘zbek, rus va ingliz tilidagi ilmiy manbalar; (2) NIST mezonlari asosida algoritmlarni qiyosiy baholash; (3) tashkilotlarga amaliy qo‘llash bo‘yicha sintetik tahlil.

Algoritmlarni baholashda NIST belgilagan beshta xavfsizlik darajasi asosida taqqoslash o‘tkazildi. Samaradorlik ko‘rsatkichlari uchun kalit hajmi, imzo hajmi va hisoblash xarajati inobatga olindi. Migratsiya strategiyasi AQSh OMB M-23-02 yo‘riqnomasi va CISA tavsiyalariga asoslanib ishlab chiqildi [12, 13].

TAHLIL VA NATIJALAR

Kvant kompyuterlarining klassik kriptografiyaga ta’siri

Kvant kompyuterlarining kriptografiyaga nisbatan asosiy tahdidi ikki muhim algoritm bilan bog‘liq. Birinchisi – 1994-yilda Piter Shor tomonidan taklif etilgan Shor algoritmi bo‘lib, u RSA va ECC asosidagi asimmetrik kriptotizimlarni polinomial vaqt murakkabligida, ya’ni $O(n^3)$ vaqt ichida yechish imkonini beradi. Mazkur kriptotizimlarning xavfsizligi asosan katta tub sonlarni faktorizatsiya qilish hamda diskret logarifm masalalarining murakkabligiga asoslanadi. Klassik kompyuterlar uchun ushbu masalalar eksponensial vaqt talab qilsa, kvant kompyuterlari ularni nazariy jihatdan polinomial vaqt ichida hal qilishi mumkin [1].

Ikkinchi muhim algoritm – 1996-yilda Lov Grover tomonidan ishlab chiqilgan Grover algoritmi bo‘lib, u simmetrik kriptografiya tizimlariga nisbatan qidiruv jarayonini tezlashtirish orqali xavfsizlik darajasini taxminan ikki baravar kamaytiradi. Masalan, AES-128 algoritmini buzish uchun nazariy jihatdan $O(\sqrt{2^{128}}) = O(2^{64})$ murakkablikdagi qidiruv yetarli bo‘lishi mumkin. Shu sababli ko‘plab tadqiqotchilar kvant hisoblash sharoitida AES-256 algoritmidan foydalanishni tavsiya etadilar, chunki u kvant hujumlari sharoitida ham taxminan 128-bit xavfsizlik darajasini saqlab qolishi mumkin [7].

Shuningdek, “Hozir yig‘ib, keyinroq ochish” (Harvest Now, Decrypt Later – HNdL) deb ataladigan tahdid ham muhim muammolardan biri sifatida ko‘rib chiqilmoqda. Grebnyov S.V. ta’kidlaganidek, hujumchi bugungi kunda shifrlangan trafikni yig‘ib borib, kelajakda yetarlicha qudratli kvant kompyuterlar paydo bo‘lganda ushbu ma’lumotlarni ochishga harakat qilishi mumkin. Bunday holat, ayniqsa, uzoq muddatli maxfiylikni talab qiladigan ma’lumotlar – davlat sirlari, tibbiy yozuvlar va moliyaviy ma’lumotlar uchun sezilarli xavf tug‘dirishi mumkin.[8].

1-jadval. Kvant algoritmlarining kriptografik tizimlarga ta’siri [1, 7, 10]

Algoritm	**Turi**	**Kvant hujumi**	**Holat**
AES-128	Simmetrik	Grover: 64-bit ga tushadi	AES-256 ga o‘tish zarur
AES-256	Simmetrik	Grover: 128-bit saqlanadi	Nisbatan xavfsiz
RSA-2048	Asimmetrik	Shor: polinomial buziladi	Ishonchsiz
ECC-256	Asimmetrik	Shor: polinomial buziladi	Ishonchsiz
DH/ECDH	Kalit almashinuv	Shor: buziladi	Ishonchsiz
SHA-256	Xesh	Grover: qisman zaiflanadi	SHA-384/512 tavsiya etiladi

NIST tomonidan 2016-yilda boshlangan tanlov jarayoniga 25 ta mamlakatdan 69 ta kriptografik algoritm taqdim etilgan. Uch bosqichli baholash jarayoni natijasida 2024-yil avgust oyida uchta rasmiy standart – FIPS 203, FIPS 204 va FIPS 205 e’lon qilindi. To‘rtinchi standart – FIPS 206 (FALCON) esa 2024-yil oxirida e’lon qilinishi kutilayotgan edi [4].

NIST baholash jarayonida bir nechta asosiy mezonlarga e’tibor qaratgan. Birinchi mezon – xavfsizlik darajasi bo‘lib, bunda algoritmning IND-CCA2 (chosen-ciphertext attack) modeliga nisbatan bardoshliligi asosiy talab sifatida ko‘rib chiqilgan. Ikkinchi mezon – xarajat va samaradorlik bo‘lib, bu hisoblash tezligi, xotira resurslari talabi hamda kalit hajmi kabi ko‘rsatkichlarni o‘z ichiga oladi. Uchinchi mezon esa algoritm va implementatsiya xususiyatlari bilan bog‘liq bo‘lib, bunda moslashuvchanlik, implementatsiyaning soddaligi hamda turli platformalarda samarali ishlash imkoniyati muhim omillar sifatida baholangan [7, 10].

2-jadva. NIST 2024-yil rasmiy PQC standartlari [4, 10]

№	Algoritm	Oila	Qo‘llanishi	Standart	Xavfsizlik
1	CRYSTALS-Kyber (ML-KEM)	Panjara	Kalit inkapsulatsiya	FIPS 203	1, 3, 5-daraja
2	CRYSTALS-Dilithium (ML-DSA)	Panjara	Raqamli imzo	FIPS 204	2, 3, 5-daraja
3	SPHINCS+ (SLH-DSA)	Xesh	Raqamli imzo	FIPS 205	1, 3, 5-daraja
4	FALCON (FN-DSA)	Panjara	Raqamli imzo	FIPS 206	1, 5-daraja

CRYSTALS-Kyber (FIPS 203): Kalit kapsulatsiya mexanizmi (KEM) sifatida standartlashtirilgan Kyber algoritmi Module-LWE (MLWE) matematik muammosiga asoslanadi. Kyber-512, Kyber-768 va Kyber-1024 versiyalari mos ravishda 1-, 3- va 5-darajali xavfsizlikni ta’minlaydi. Intel AVX2 ko‘rsatmalari yordamida amalga oshirilgan hisoblashlarda ishlash tezligi RSA-2048 algoritmiga nisbatan taxminan 5–10 baravar yuqori ekanligi Kannwischer va boshq. (2021) tadqiqotida ko‘rsatib o‘tilgan [11]. Kalit hajmi 800–1568 baytni tashkil etadi. Bu ko‘rsatkich RSA-2048 ning 256 baytlik kalit hajmiga nisbatan kattaroq bo‘lsa-da, amaliy tajribalar shuni ko‘rsatadiki, u tizim samaradorligiga sezilarli ta’sir ko‘rsatmaydi hamda ECC-256 ning 64 baytli kalitiga nisbatan kattaroq bo‘lishi muhim muammo sifatida baholanmaydi.

CRYSTALS-Dilithium (FIPS 204): Ushbu algoritm raqamli imzo sxemasi bo‘lib, MLWE va Module-SIS matematik muammolariga asoslanadi. NIST Dilithium algoritmini asosiy post-kvant raqamli imzo algoritmi sifatida tavsiya etadi, chunki u xavfsizlik darajasi, hisoblash samaradorligi va implementatsiya murakkabligi o‘rtasida muvozanatli natijalarni ta’minlaydi. Masalan, Dilithium3 (3-darajali xavfsizlik) uchun imzo hajmi 3293 baytni tashkil etadi. Bu ko‘rsatkich RSA-2048 ning 256 baytli imzosiga nisbatan kattaroq bo‘lsa-da, amaliy tarmoq sinovlarida uning tarmoq o‘tkazuvchanligiga ta’siri minimal darajada ekanligi qayd etilgan [10].

FALCON (FIPS 206): Mazkur algoritm NTRU panjara muammosiga asoslangan bo‘lib, raqamli imzo sxemalari orasida tarmoq kengligi (bandwidth) jihatidan eng kichik talablarni qo‘yadigan algoritmlardan biri hisoblanadi. FALCON-512 algoritmi uchun imzo hajmi 690 bayt bo‘lib, bu Dilithium2 algoritmidagi 2420 baytga nisbatan taxminan 3,5 baravar kichikdir. Imzoni tekshirish jarayoni juda tez amalga oshiriladi. Biroq kalit yaratish jarayonida floating-point operatsiyalar qo‘llanilishi sababli implementatsiya jarayoni nisbatan murakkabroq bo‘lishi mumkin [7].

SPHINCS+ (FIPS 205): SPHINCS+ xesh funksiyalariga asoslangan raqamli imzo sxemasi bo‘lib, u faqat bitta kriptografik primitiv – bir yo‘nalishli hash funksiyasiga tayanadi. Shu sababli u nazariy jihatdan eng yuqori darajadagi ishonchlilikka ega post-kvant algoritmlardan biri sifatida qaraladi. Post-kvant kriptografiya algoritmlari orasida kvantdan keyingi sharoitda kriptoanalitik usullar bilan buzilish ehtimoli eng past bo‘lgan sxemalardan biri sifatida baholanadi. Biroq uning asosiy cheklovlaridan biri – imzo hajmining kattaligi (taxminan 7856–29792 bayt) hamda imzo yaratish jarayonining nisbatan sekinligidir. Tadqiqotlarga ko‘ra, imzo yaratish uchun zarur hisoblash resurslari Dilithium algoritmiga nisbatan ancha ko‘proq bo‘lishi mumkin [7, 11].

3-jadval. PQC algoritmlarining qiyosiy ko‘rsatkichlari [7, 10, 11]

Algoritm	Ochiq kalit	Imzo/Shifrmatn	**Tezlik (ms)**	**Xavfsizlik**
RSA-2048	256 b	256 b	0.3 / 2.5	Kvantga zaif
ECC-256	64 b	64 b	0.06 / 0.07	Kvantga zaif
Kyber-768	1184 b	1088 b	0.02 / 0.03	3-daraja (192-bit)
Dilithium3	1952 b	3293 b	0.08 / 0.05	3-daraja (192-bit)
FALCON-512	897 b	690 b	10.1 / 0.03	1-daraja (128-bit)
SPHINCS+-128s	32 b	7856 b	67.1 / 0.7	1-daraja (128-bit)

Tadqiqot natijalari shuni ko‘rsatadiki, tashkilotlar uchun yagona “to‘g‘ri” algoritm mavjud emas. Eng maqbul tanlov, avvalo, tashkilotning o‘ziga xos ehtiyojlari va texnologik infratuzilmasiga bog‘liq bo‘ladi. Xudoykulov Z. va hamkasblari (2023) ta’kidlaganidek, yengil vaznli kriptografik algoritmlar resurslari cheklangan muhitlar uchun alohida tahlil va moslashtirilgan yondashuvni talab qiladi [6].

Kalit almashinuvi jarayonlari uchun CRYSTALS-Kyber algoritmi hozirgi vaqtda asosiy tanlovlardan biri sifatida qaraladi. U ishlash tezligi, xavfsizlik darajasi hamda implementatsiya soddaligi jihatidan muvozanatli natijalarni ta’minlaydi. Raqamli imzo tizimlari uchun esa CRYSTALS-Dilithium algoritmi asosiy standart sifatida tavsiya etiladi. Shu bilan birga, tarmoq o‘tkazuvchanligi cheklangan muhitlarda FALCON algoritmidan foydalanish maqsadga muvofiq bo‘lishi mumkin. Agar tizimda maksimal darajadagi kriptografik ishonchlilik talab etilsa, SPHINCS+ algoritmini tanlash ham asosli variantlardan biri sifatida ko‘rib chiqiladi.

4-jadval. Tashkilot turiga qarab algoritmni tanlash tavsiyalari

Tashkilot turi / holat	**Tavsiya etilgan algoritm**	**Sabab**
Bank / moliya tizimlari	Kyber + Dilithium	Muvozanatli xavfsizlik va tezlik
Davlat axborot tizimlari	Kyber + SPHINCS+	Maksimal ishonchlilik
IoT / mobil qurilmalar	Kyber + FALCON	Kichik kalit va imzo hajmi
Arxiv / uzoq muddatli saqlash	SPHINCS+	Eng konservativ matematik asos
TLS/HTTPS protokollari	Kyber (gibrid rejim)	Orqaga moslik ta’minlanadi

Fedorov A.K. (2023) hamda xalqaro tadqiqotchilar tavsiya etganidek, gibrid kriptografiya, ya’ni klassik va post-kvant kriptografiya (PQC) algoritmlarini parallel qo‘llash, hozirgi sharoitda eng maqbul yondashuvlardan biri sifatida qaralmoqda [8]. Masalan, Google kompaniyasi 2016-yildan boshlab ushbu yondashuvni qo‘llab kelmoqda. SIKE algoritmi 2022-yilda kriptoanalitik jihatdan zaif deb topilganida ham, X25519 qatlamining mavjudligi tizim himoyasini saqlab qolishga yordam berdi [5]. Shuningdek, Signal messenjeridagi PQXDH hamda Apple kompaniyasining PQ3 protokollari ham gibrid kriptografiya yondashuviga asoslanadi.

Gibrid yondashuvning asosiy afzalliklari quyidagilardan iborat:

- mavjud infratuzilma bilan **orqaga moslik (backward compatibility)**ni saqlab qolish;
- agar algoritmlardan biri zaiflashsa yoki buzilsa, ikkinchisi himoya darajasini saqlab turish imkonini berishi;
- kriptografik tizimlarni bosqichma-bosqich modernizatsiya qilish imkoniyatini yaratishi.

Shu bilan birga, ayrim texnik jihatlar ham e’tiborga olinadi. Masalan, kalit va shifrmatn hajmining ortishi hamda qo‘shimcha hisoblash resurslari talabi tizim samaradorligiga ma’lum darajada ta’sir ko‘rsatishi mumkin.

Tashkilotlar uchun migratsiya strategiyasi va xarajat tahlili

CISA (2022) hamda AQSh Boshqaruv va byudjet boshqarmasining M-23-02 yo‘riqnomasi (2022) tavsiyalariga asoslanib, tashkilotlar uchun to‘rt bosqichli migratsiya strategiyasi taklif etiladi [12, 13].

1-bosqich (0–6 oy) – Inventarizatsiya.

Bu bosqichda tashkilotdagi barcha kriptografik protokollar, kalitlar va sertifikatlar ro‘yxatga olinadi. Shuningdek, kvant texnologiyalari nuqtai nazaridan potensial zaif nuqtalar aniqlanadi hamda ma’lumotlarning maxfiylik muddatlari baholanadi.

2-bosqich (6–18 oy) – Sinov.

Bu bosqichda liboqs va OpenSSL 3.x kabi ochiq kodli kriptografik kutubxonalar yordamida test muhitida tajribalar o‘tkaziladi. Tarmoq kechikishlari o‘lchanadi hamda mutaxassislar uchun malaka oshirish va tayyorlov ishlari amalga oshiriladi.

3-bosqich (18–36 oy) – Gibrid joriy etish.

Muhim axborot tizimlari gibrid kriptografiya rejimiga o‘tkaziladi. Masalan, TLS 1.3 + ML-KEM kombinatsiyasi qo‘llanishi mumkin. Shu bilan birga, mavjud PKI infratuzilmasi bosqichma-bosqich yangilanadi.

4-bosqich (36 oy va undan keyin) – To‘liq migratsiya.

Ushbu bosqichda barcha tizimlar post-kvant kriptografiya algoritmlariga to‘liq o‘tkaziladi. Klassik kriptografik algoritmlar bosqichma-bosqich foydalanishdan chiqariladi hamda NIST tomonidan 2035-yilgacha belgilangan tavsiyalarga muvofiqlik ta’minlanadi.

Xarajat–foyda tahlili shuni ko‘rsatadiki, PQC texnologiyalariga o‘tish ko‘plab tashkilotlar uchun iqtisodiy jihatdan asoslangan investitsiya sifatida baholanadi. IBM Security (2024) ma’lumotlariga ko‘ra, ma’lumotlar buzilishining o‘rtacha global qiymati 4,88 million AQSh dollarini tashkil etadi, bu esa o‘tgan yilga nisbatan taxminan 10 % ga oshganini ko‘rsatadi. Shu bilan birga, o‘rta hajmdagi tashkilot uchun PQC texnologiyalarini joriy etish xarajati odatda 50 000–300 000 AQSh dollari atrofida baholanadi. Bu potensial zarar miqdorining taxminan 1–6 % ini tashkil etadi va mazkur investitsiyaning iqtisodiy jihatdan maqsadga muvofiqligini ko‘rsatadi.

5-jadval. Tashkilot hajmiga qarab PQC joriy etish xarajatlari (taxminiy) [12, 13]

Tashkilot turi	**Xodim soni**	**Taxminiy xarajat ($)**	**Asosiy element**
Kichik	< 50	10 000 – 30 000	VPN, email, sertifikat yangilash
O‘rta	50 – 500	50 000 – 300 000	PKI, HSM, kadrlash, audit
Yirik / davlat	> 500	500 000 – 5 000 000+	To‘liq infratuzilma migratsiyasi

O‘zbekiston Respublikasi Prezidentining 2024-yildagi PQ-293-son qarori axborotni kriptografik himoyalash milliy tizimini rivojlantirish hamda kriptologiya sohasida milliy standartlar ishlab chiqish zarurligini belgilab berdi [3]. Mazkur kontekstda mahalliy tashkilotlar uchun ikki asosiy ustuvor yo‘nalish ajralib turadi.

Birinchidan, O‘zDst (O‘zbekiston davlat standartlari) tizimiga post-kvant kriptografiya (PQC) algoritmlarini kiritish masalasi muhim ahamiyat kasb etadi. Bu yo‘nalishda Toshkent axborot texnologiyalari universitetining “Kriptologiya” kafedrasi hamda tegishli ilmiy muassasalar tomonidan qator ilmiy tadqiqotlar olib borilmoqda. Masalan, Xudoykulov Z., Karimov A. va Abdurakhmanov R. (2023) tomonidan bulutli hisoblash tizimlarida autentifikatsiya jarayonlari bilan bog‘liq muammolar o‘rganilgan [9]. Bu esa ushbu sohada mahalliy ilmiy izlanishlar ham muhim natijalar berayotganini ko‘rsatadi.

Ikkinchidan, amaliy jihatdan muhim bo‘lgan “Hozir yig‘ib, keyinroq ochish” (Harvest Now, Decrypt Later – HNdL) tahdidi mavjud. Davlat axborot tizimlari orqali uzatilayotgan ayrim maxfiy ma’lumotlar bugungi kunda shifrlangan holda saqlanib, kelajakda yanada rivojlangan hisoblash texnologiyalari yordamida tahlil qilinishi ehtimoli ham mavjud. Shu sababli, ayniqsa davlat siri yoki shaxsiy ma’lumotlarni qayta ishlovchi tashkilotlar uchun post-kvant kriptografiyaga o‘tish jarayonini rejalashtirish muhim ahamiyat kasb etadi.

XULOSA VA TAKLIFLAR

Ushbu tadqiqot natijalari quyidagi asosiy xulosalarga kelish imkonini beradi:

1. Kvant kompyuterlarining RSA, ECC va Diffie–Hellman algoritmlariga nisbatan potensial ta’siri ilmiy jihatdan keng muhokama qilinmoqda. Shor algoritmi ushbu tizimlarni polinomial vaqt ichida tahlil qilish imkonini berishi nazariy jihatdan asoslab berilgan. Shuningdek, “Hozir yig‘ib, keyinroq ochish” hujum strategiyasi ham kelajakdagi xavfsizlik masalalari nuqtai nazaridan muhim omil sifatida ko‘rib chiqilmoqda.
2. NIST tomonidan 2024-yilda tasdiqlangan post-kvant kriptografiya standartlari – CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON va SPHINCS+ – tashkilotlar uchun istiqbolli kriptografik yechimlar sifatida qaralmoqda. Ular orasida kalit almashinuvi uchun Kyber, raqamli imzo uchun esa Dilithium ko‘plab tizimlarda asosiy tanlov sifatida tavsiya etilmoqda.
3. Gibrid kriptografiya yondashuvi, ya’ni klassik va post-kvant algoritmlarini parallel qo‘llash, mavjud infratuzilma bilan moslikni saqlash hamda migratsiya jarayonidagi xavflarni kamaytirish uchun samarali boshlang‘ich strategiya sifatida baholanadi.
4. Xarajat–foyda tahlili post-kvant kriptografiyaga o‘tish ko‘plab tashkilotlar uchun iqtisodiy jihatdan maqsadga muvofiq ekanini ko‘rsatadi. Baholashlarga ko‘ra, migratsiya xarajatlari potensial zarar miqdorining taxminan 1–6 % ini tashkil etadi.
5. O‘zbekiston Respublikasi Prezidentining 2024-yildagi PQ-293-son qarori post-kvant kriptografiya texnologiyalarini joriy etish masalasiga davlat siyosati darajasida e’tibor qaratilayotganini ko‘rsatadi. Shu bois mahalliy tashkilotlar uchun to‘rt bosqichli migratsiya strategiyasini bosqichma-bosqich amalga oshirish maqsadga muvofiq hisoblanadi.

Kelgusidagi tadqiqot yo‘nalishlari sifatida quyidagilar tavsiya etiladi:

- O‘zbekiston tashkilotlarining real tarmoq muhitida PQC algoritmlarining samaradorligini eksperimental baholash;
- O‘zDst milliy standartlariga PQC algoritmlarini kiritish bo‘yicha ilmiy-amaliy takliflar ishlab chiqish;
- ayniqsa IoT va mobil qurilmalar uchun mos keladigan yengil vaznli PQC implementatsiyalarini o‘rganish.

Foydalanilgan adabiyotlar ro‘yxati

1. Shor P.W. Algorithms for quantum computation: discrete logarithms and factoring // Proceedings 35th Annual Symposium on Foundations of Computer Science. – IEEE, 1994. – B. 124–134.
2. Bernstein D.J., Lange T. Post-quantum cryptography // Nature. – 2017. – Vol. 549, №7671. – B. 188–194.
3. NIST. Post-Quantum Cryptography Standardization. Federal Information Processing Standards (FIPS) 203, 204, 205, 206. – Gaithersburg: NIST, 2024. [Online]. URL: https://csrc.nist.gov/projects/post-quantum-cryptography
4. Wikipedia. Post-quantum cryptography. [Online]. URL: https://en.wikipedia.org/wiki/Post-quantum_cryptography (murojaat: 2025-yil fevral).
5. Xudoykulov T., Boyquziyev I.M., Allanov O.M., Mardiyev U.R., Jabbarov N.A. Kriptografik usullar: O‘quv qo‘llanma. – Toshkent: Lesson-Press, 2023. – 255 b.
6. Abduraximov B.F., Boyquziyev I.M., Arabboyev A.A. Zamonaviy postkvant kriptografik algoritmlar va ularning samaradorligi // Al-Farg‘oniy avlodlari elektron ilmiy jurnali. – 2025. – Tom 1, Son 3. – B. 29–36.
7. Fedorov A.K. Zashchita informatsionnykh sistem na osnove kombinatsii ustroystv kvantovogo raspredeleniya klyuchey i postkvantovykh algoritmov. Doklad na konferentsii RusCrypto. – Moskva, 2023.
8. Khudoykulov Z., Karimov A., Abdurakhmanov R., Mirzabekov M. Authentication in Cloud Computing: Open Problems // 2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC). – IEEE, 2023. – DOI: 10.1109/ICESC57686.2023.10193438.
9. Alagic G. et al. Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. NIST IR 8413. – Gaithersburg: NIST, 2022.
10. Yaponova E. et al. Applications of Post-quantum Cryptography // MDPI Technologies. – 2024. – Vol. 12, №12. – DOI: 10.3390/technologies12120241.
11. CISA. Post-Quantum Cryptography Initiative. – Washington, 2022. [Online]. URL: https://www.cisa.gov/quantum
12. U.S. Office of Management and Budget. M-23-02 Memorandum on Migration to Post-Quantum Cryptography. – Washington: OMB, 2022.
13. IBM Security. Cost of a Data Breach Report 2024. – New York: IBM Corporation, 2024.
14. Qodirov F., Abduxalilova M. Kriptografiya va shifrlash usullari // Прикладные nauki v sovremennom mire: problemy i resheniya. – 2024. – №11. [Online]. URL: https://inlibrary.uz

muhandislik & iqtisodiyot

ijtimoiy-iqtisodiy, innovatsion texnik,
fan va ta'limga oid ilmiy-amaliy jurnal

Ingliz tili muharriri: Feruz Hakimov

Musahhih: Zokir Alibekov

Sahifalovchi va dizayner: Iskandar Islomov

2-Maxsus son.
Bakalavr talabalarining maqolalari to‘plami

“Muhandislik va iqtisodiyot” jurnali 26.06.2023-yildan
O‘zbekiston Respublikasi Prezidenti Adminstratsiyasi huzuridagi
Axborot va ommaviy kommunikatsiyalar agentligi tomonidan
№S–5669245 reyestr raqami tartibi bo‘yicha ro‘yxatdan o‘tkazilgan.
Litsenziya raqami: №095310.

**Manzilimiz: Toshkent shahri Yunusobod
tumani 15-mavze 19-uy**

+998 93 718 40 07 https://muhandislik-iqtisodiyot.uz/index.php/journal t.me/yait_2100