ISSN: 3030-3346

POST KVANT KRIPTOGRAFIYASIGA OID KUTUBXONALAR TAHLILI

Mustafoyev Azamat Botir o‘g‘li

‘‘UNICON.UZ” MChJ
Email: mustafoyevazamat01@gmail.com

K E Y W O R D S

postkvant kriptografiya, kriptografik kutubxonalar, liboqs, Microsoft PQCrypto, CIRCL, PQClean, ML-DSA, Dilithium, Falcon, Kyber

A B S T R A C T

Ushbu maqolada to‘rtta mashhur (PQC) Post-Kvant Kriptografiyasi kutubxonasi tahlil qilinadi - liboqs, Microsoft PQCrypto, CIRCL va PQClean haqida batafsil ma'lumot beriladi, ularning xususiyatlari, afzalliklari, kamchiliklari va qo‘llanilish sohalari tahlil qilinadi.

Post-kvant kriptografiyasi (PQC) zamonaviy xavfsizlik sohasida inqilobiy o‘zgarishlarni keltirib chiqarmoqda, chunki kvant kompyuterlari an'anaviy shifrlash usullarini, xususan, RSA, ECC va DSA kabi algoritmlarni osongina buzish imkoniyatiga ega. Kvant kompyuterlarining Shor algoritmi yordamida katta sonlarni faktorizatsiya qilish va diskret logarifm muammolarini yechish qobiliyati tufayli yangi, kvantga bardoshli algoritmlarga ehtiyoj ortib bormoqda. Bu ehtiyojni qondirish uchun maxsus kutubxonalar ishlab chiqilmoqda, ular dasturchilarga (PQC) Post-Kvant Kriptografiyasi algoritmlarini tizimlarga integratsiya qilish imkonini beradi

liboqs (Open Quantum Safe) liboqs ochiq kodli (open-source) C va C++ kutubxonasi (library) bo‘lib, Open Quantum Safe loyihasi doirasida ishlab chiqilgan. U kvantga bardoshli algoritmlarni (quantum-resistant algorithms) sinovdan o‘tkazish (testing) va real dunyo ilovalariga (real-world applications) integratsiya qilish (integration) uchun mo‘ljallangan. liboqs panjara asosidagi algoritmlar (lattice-based algorithms) - Kyber, Saber, NTRU, kodga asoslangan algoritmlar (code-based algorithms) - McEliece, BIKE va xeshga asoslangan algoritmlar (xesh-based algorithms) - SPHINCS+ kabi keng doiradagi algoritmlarni qo‘llab-quvvatlaydi (supports). Ochiq manbalarga ko‘ra, liboqs NISTning post-kvant kriptografiya standartlashtirish jarayoniga (NIST Post-Quantum Cryptography Standardization) to‘liq mos keladi. Kutubxona faol jamoa (active community) tomonidan qo‘llab-quvvatlanadi, bu uning doimiy rivojlanishini (continuous development) ta’minlaydi. Ba’zi algoritmlar optimallashtirish darajasi (optimization level) past bo‘lib, ishlash tezligiga (performance speed) ta’sir qiladi. liboqs xavfsiz aloqa protokollari (secure communication protocols) - TLS (Transport Layer Security, transport qatlami xavfsizligi), SSH (Secure Shell, xavfsiz qobiq) va raqamli imzo tizimlarida qo‘llaniladi.

Kyber algoritmi formulasi Kyber qisqa vektorli panjara muammosiga (short vector lattice problem) asoslanadi va Learning With Errors (LWE, xatolar bilan o‘rganish) muammosiga tayanadi: $b = A * s + e$ bu yerda A-tasodifiy matritsa, (random matrix) , s - maxfiy kalit vektori (secret key vector), e - kichik xato vektori (small error vector), b - ochiq kalit (public key). Kyberning xavfsizligi (security) **s** ni A va b dan aniqlashning qiyinligiga asoslanadi.

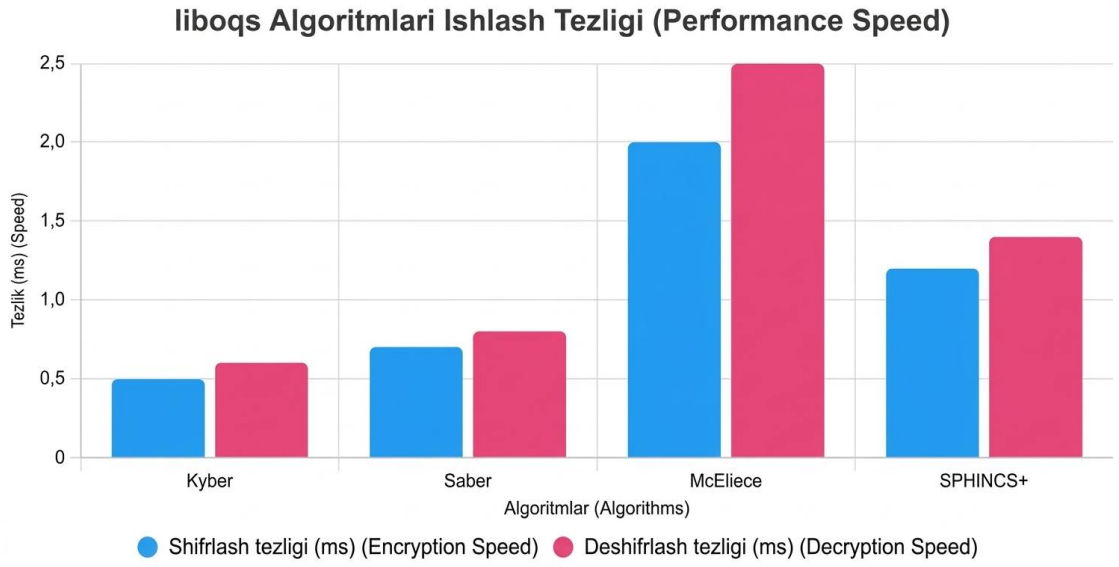
(cc) BY *dtai.uz*

ISSN: 3030-3346

1-jadval

liboqs algoritmlari xususiyatlari

Algoritm	*Turi*	*Kalit uzunligi (bit)*	*Xavfsizlik darajasi (NIST)*	*Ishlash tezligi*
Kyber	Panjara asosli (Lattice-based)	512-1024	1-5	Yuqori (High)
Saber	Panjara asosli (Lattice-based)	(Lattice-based)512-1024	1-5	O‘rtacha (Medium)
McEliece	Kodga asosli (Code-based)	3488-8192	1-5	Past (Low)
SPHINCS+	Xeshga asosli (Xesh-based)	256	1-5	O‘rtacha (Medium)



1-rasm. liboqs algoritmlari ishlash tezligi

Microsoft PQCrypto Microsoft Research tomonidan ishlab chiqilgan kutubxona bo‘lib, ilmiy tadqiqotlar (scientific research) va eksperimental loyihalar (experimental projects) uchun mo‘ljallangan. U FrodoKEM, SIDH (Supersingular Isogeny Diffie-Hellman, supero‘zgaruvchan izogeniya Diffi-Hellman) va Classic McEliece algoritmlarini qo‘llab-quvvatlaydi [39].

Kutubxona yuqori darajada optimallashtirilgan (highly optimized) va Microsoftning SymCrypt dvigateli (SymCrypt engine) bilan ishlaydi. U bulutli xizmatlar (cloud services), masalan, Azure platformasida xavfsiz aloqa tizimlarini (secure communication systems) sinovdan o‘tkazish uchun ishlatiladi. Microsoft ML-DSA (Module-Lattice-based Digital Signature Algorithm, modul-panjara asosli raqamli imzo algoritmi) va LMS (Leighton-Micali Signature, Leighton-Micali imzo) algoritmlarini Windows va Linux tizimlarida sinovdan o‘tkazmoqda. Kutubxona cheklangan algoritmlar sonini qo‘llab-quvvatlaydi va liboqs kabi keng jamoa qo‘llab-quvvatlashiga (community support) ega emas, ammo optimallashtirish darajasi yuqori samaradorlik (high performance) talab qilinadigan loyihalarda afzallik beradi.

FrodoKEM algoritmi formulasi: FrodoKEM LWE muammosiga asoslanadi va oddiyroq matritsa tuzilishidan (simpler matrix structure) foydalanadi:

$b = A * s + e \bmod q$ bu yerda q – katta modul (large modulus), xavfsizlikni (security) oshiradi, lekin kalit hajmi (key size) katta bo‘ladi.

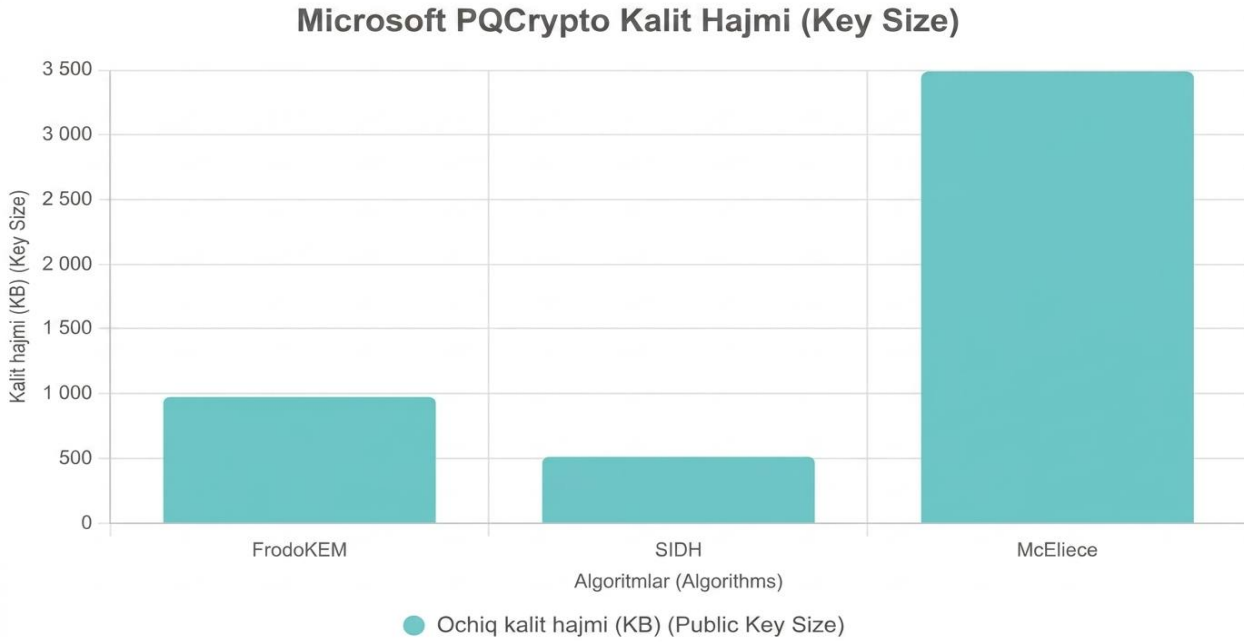
(cc) BY

ISSN: 3030-3346

2-jadval

Microsoft PQCrypto algoritmlari xusiyatlari

Algoritm	*Turi*	*Kalit uzunligi (bit)*	*Xavfsizlik darajasi*	*Ishlash tezligi*
FrodoKEM	Panjara asosli (Lattice-based)	976-1344	1-5	O‘rtacha (Medium)
SIDH	Super o‘zgaruvchan	512	1-3	Past (Low)
McEliece	Kodga asosli (Code-based)	3488-8192	1-5	Past (Low)



2-rasm. Microsoft PQCrypto kalit hajmi

CIRCL (Cloudflare Interoperable, Reusable Cryptographic Library) CIRCL Cloudflare tomonidan ishlab chiqilgan ochiq kodli kutubxona bo‘lib, Go dasturlash tilida (Go programming language) yozilgan va veb-ilovalar (web applications) uchun optimallashtirilgan. U Kyber, Dilithium va SPHINCS+ algoritmlarini qo‘llab-quvvatlaydi. CIRCL HTTPS (Hypertext Transfer Protocol Secure, xavfsiz gipermatn uzatish protokoli) va TLS protokollarida post-kvant algoritmlarni sinovdan o‘tkazish uchun ishlatiladi. Go tilida yozilganligi zamonaviy veb-xizmatlar (web services) va bulutli tizimlarda (cloud systems) qulay integratsiyani ta’minlaydi. CIRCL yangi loyiha bo‘lib, cheklangan algoritm tanloviga ega va keng sinovdan (extensive testing) o‘tmagan.

Dilithium algoritmi formulasi Dilithium raqamli imzo algoritmi (digital signature algorithm) bo‘lib, panjara asosidagi qisqa butun sonlar muammosiga (short integer lattice problem) tayanadi: $sig = s + H(m, pk) \bmod q$ bu yerda **s**ig – raqamli imzo , $\boldsymbol{s}$ – maxfiy kalit, H – xesh funksiya, m – xabar, pk - ochiq kalit.

(cc) BY

ISSN: 3030-3346

3-jadval

CIRCL algoritmlari xususiyatlari

Algoritm	*Turi*	*Imzo uzunligi (bit)*	*Xavfsizlik darajasi(NIST)*	*Ishlash tezligi*
Kyber	Panjara asosli (Lattice-based)	512-1024	1-5	Yuqori (High)
Dilithium	Panjara asosli (Lattice-based)	2420-4595	1-5	O‘rtacha (Medium
PHINCS+	Xeshga asosli (Xesh-based	17088	1-5	Past (Low)

PQClean kutubxonasi PQClean ochiq kodli loyiha bo‘lib, toza (clean) va portativ (portable) C kodida yozilgan PQC algoritmlarini taqdim etadi. U Kyber, NTRU, Saber va McEliece algoritmlarini qo‘llab-quvvatlaydi. PQClean turli platformalarda, ayniqsa resurslari cheklangan IoT qurilmalarda (Internet of Things devices) ishlashga moslashtirilgan. NISTning post-kvant standartlashtirish jarayoniga qat’iy rioya qiladi, lekin optimallashtirish darajasi (optimization level) past bo‘lib, yuqori samaradorlik (high performance) talab qilinadigan loyihalarda cheklovlar yaratadi.

McEliece algoritmi formulasi McEliece kodga asoslangan shifrlash algoritmi (code-based encryption algorithm) bo‘lib, Goppa kodlariga (Goppa codes) asoslanadi: $c = m * G + e$ bu yerda c – shifrlangan xabar, m – ochiq kalit, G – generatsiya matritsasi, **e** – tasodifiy xato vektori.

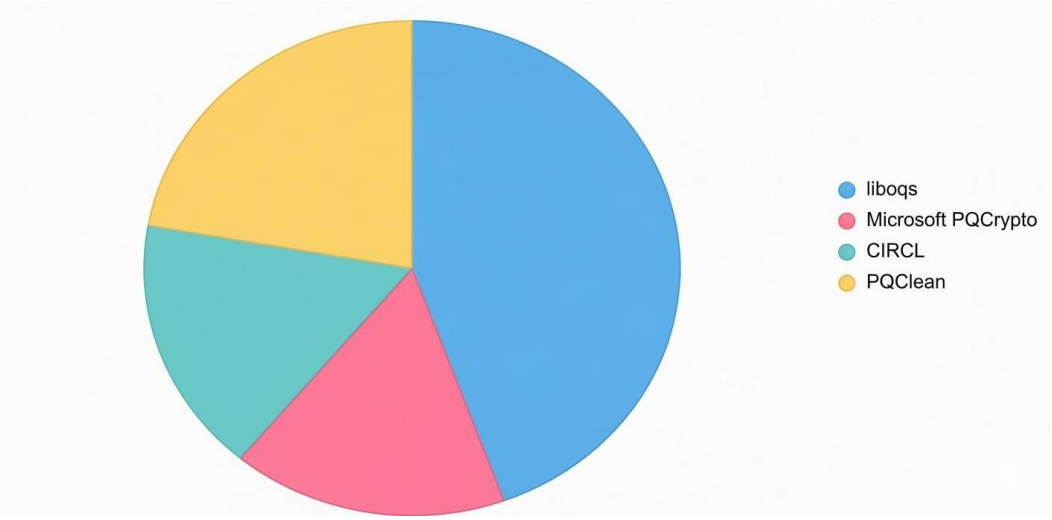
4-jadval

PQClean algoritmlari xususiyatlari

Algoritm	*Turi*	*Kalit uzunligi (bit)*	*Xavfsizlik darajasi(NIST)*	*Ishlash tezligi*
Kyber	Panjara asosli (Lattice-based)	512-1024	1-5	Yuqori (High)
NTRU	Panjara asosli (Lattice-based)	512-1024	1-5	O‘rtacha (Medium)
Sayber	Panjara asosli (Lattice-based)	512-1024	1-5	O‘rtacha (Medium)
McEliece	Kodga asosli (Code-based)	3488-8192	1-5	Past (Low)

(cc) BY

ISSN: 3030-3346



3-rasm. Kutubxonalar bo‘yicha algoritmlar taqsimoti

5- jadval

Kutubxonalarni taqqoslash jadvali

Kutub-xona	*Dastur-lash tili*	*Algoritmlar soni*	*Asosiy afzallik*	*Asosiy kamchilik*	*Qo‘llanilish sohasi*
liboqs	C, C++	8	Keng algoritm tanlovi, jamoa qo‘llab-quvvatlashi	Optimallashtirish muammolari	TLS, SSH, raqamli imzo
Microsoft PQCrypto	C, C++	3	Yuqori optimallashtirish	Cheklangan algoritmlar	Bulutli xizmatlar
CIRCL	Go	3	Veb-ilovalar uchun qulay	Yangi loyiha, sinovlar kam	HTTPS, TLS
PQClean	C	4	Portativlik	Optimallashtirish	IoT, cheklangan resurslar

liboqs keng algoritm tanlovi va faol jamoa qo‘llab-quvvatlashi bilan ajralib turadi. Ushbu kutubxona ko‘plab post-kvant algoritmlarni, jumladan, panjara asosidagi (Kyber, Saber, NTRU), kodga asoslangan (McEliece, BIKE) va xeshga asoslangan (SPHINCS+) algoritmlarni qamrab oladi. Jamoaning faol ishtiroki tufayli kutubxona doimiy yangilanib, NIST standartlariga mos keladi. Biroq, ayrim algoritmlarning optimallashtirish darajasi pastligi ishlash tezligiga ta’sir qiladi. liboqs xavfsiz aloqa protokollari (TLS, SSH) va raqamli imzo tizimlarida keng qo‘llaniladi, bu uning amaliy ahamiyatini ko‘rsatadi.

Microsoft PQCrypto yuqori optimallashtirish darajasi va ilmiy tadqiqot loyihalari uchun mosligi bilan e’tiborga sazovor. U FrodoKEM, SIDH va Classic McEliece kabi algoritmlarni qo‘llab-quvvatlaydi, Microsoftning SymCrypt dvigateli bilan integratsiyalashgan holda ishlaydi. Bulutli xizmatlar, xususan Azure platformasida xavfsiz aloqa tizimlarini sinovdan o‘tkazishda foydalaniladi. ML-DSA va LMS algoritmlari Windows va Linux tizimlarida sinovdan o‘tkazilmoqda. Shu bilan birga, cheklangan algoritm tanlovi va jamoa qo‘llab-quvvatlashining kamligi keng qo‘llanilishini cheklaydi.

CIRCL veb-ilovalar uchun optimallashtirilgan Go tilida yozilgan kutubxona bo‘lib, Kyber, Dilithium va SPHINCS+ algoritmlarini qo‘llab-quvvatlaydi. HTTPS va TLS protokollarida post-kvant algoritmlarni sinovdan o‘tkazishda qo‘llaniladi. Go tilining afzalliklari tufayli zamonaviy veb-xizmatlar va bulutli tizimlarda qulay integratsiyani ta’minlaydi.

(cc) BY

Yangi loyiha sifatida algoritm tanlovi cheklangan va keng sinovlardan o‘tmagan, ammo veb-xavfsizlik sohasida yuqori potentsialga ega.

PQClean toza va portativ C kodida yozilgan bo‘lib, Kyber, NTRU, Saber va McEliece algoritmlarini qamrab oladi. Resurslari cheklangan IoT qurilmalarida ishlashga moslashtirilgan. NIST standartlariga qat’iy rioya qiladi, lekin optimallashtirish darajasi pastligi yuqori samaradorlik talab qilinadigan loyihalarda cheklovlar yaratadi. Ilmiy tahlillarda PQClean’ning IoT va cheklangan resursli muhitlarda samaradorligi ta’kidlanadi.

Xulosa

O‘tkazilgan tahlil natijasida to‘rtta yetakchi post-kvant kriptografiya kutubxonasi - liboqs, Microsoft PQCrypto, CIRCL va PQClean - turli mezonlar bo‘yicha qiyoslandi: dasturlash tili, qo‘llab-quvvatlanadigan algoritmlar soni, ishlash tezligi, optimallashtirish darajasi va qo‘llanilish sohasi.

Tahlil shuni ko‘rsatdiki, har bir kutubxona o‘ziga xos ustunlik va cheklovlarga ega bo‘lib, ular turli maqsadlar uchun mo‘ljallangan:

–**liboqs** eng keng algoritm tanlovi va faol jamoa qo'llab-quvvatlashi tufayli TLS, SSH va raqamli imzo tizimlarini rivojlantirish uchun eng universal tanlov hisoblanadi, ammo ayrim algoritmlarning optimallashtirilmaganligi ishlash tezligiga salbiy ta'sir ko'rsatadi.

–**Microsoft PQCrypto** yuqori darajada optimallashtirilganligi bois ilmiy-tadqiqot loyihalari va Azure kabi bulutli platformalarda sinov o'tkazish uchun qulay, biroq cheklangan algoritm to'plami uning qo'llanilish doirasini toraytiradi.

–**CIRCL** Go tilida yozilganligi sababli zamonaviy veb-ilovalar va bulutli xizmatlarda qulay integratsiyani ta'minlaydi, lekin nisbatan yangi loyiha bo'lgani uchun keng sinovlardan o'tmagan.

–**PQClean** o'zining portativligi va toza kod tuzilishi tufayli resurslari cheklangan IoT qurilmalarida qo'llash uchun eng maqbul yechim hisoblanadi.

Kvant kompyuterlarining rivojlanishi an'anaviy kriptografik tizimlar uchun jiddiy xavf tug‘dirmoqda, shu sababli tashkilotlar va dasturchilar o'z ehtiyojlariga -xavfsizlik darajasi, ishlash tezligi, platforma turi va resurs cheklovlariga - mos keluvchi PQC kutubxonasini tanlashlari zarur.

FOYDALANILINGAN ADABIYOTLAR RO‘YXATI

1. National Institute of Standards and Technology (NIST). *Post-Quantum Cryptography Standardization Project*. https://csrc.nist.gov/projects/post-quantum-cryptography
2. Open Quantum Safe Project. *liboqs: C library for quantum-resistant cryptographic algorithms*. — https://openquantumsafe.org/liboqs/
3. Microsoft Research. *PQCrypto-VPN va Microsoft PQCrypto loyihalari*. — https://github.com/microsoft/PQCrypto-SIDH
4. Cloudflare. *CIRCL: Cloudflare Interoperable, Reusable Cryptographic Library*.
5. PQClean Project. *Clean implementations of post-quantum cryptography*. — https://github.com/PQClean/PQClean
6. Bos J., Ducas L., Kiltz E. va boshq. *CRYSTALS-Kyber: Algorithm Specifications and Supporting Documentation*. NIST PQC Round 3 Submission.
7. Ducas L., Lepoint T., Lyubashevsky V. va boshq. *CRYSTALS-Dilithium: Digital Signature Scheme*. NIST PQC Round 3 Submission.
8. Bernstein D.J., Hülsing A., Kölbl S. va boshq. *SPHINCS+: Stateless Hash-Based Signatures*. NIST PQC Submission.
9. Shor P.W. *Algorithms for Quantum Computation: Discrete Logarithms and Factoring*. Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 1994.
10. Alagic G., Alperin-Sheriff J., Apon D. va boshq. *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*. NIST IR 8413, 2022.

(cc) BY