KVANT TAHDIDI VA POST-KVANT KRIPTOGRAFIYASIGA O‘TISH: MUAMMOLAR VA YECHIMLAR

Rizoqulova Marjonabonu Zokirovna
Saidov Usmon Bahron O’g’li
Buxoro Davlat Texnika Universiteti

Kirish (Introduction)

XXI asr axborot texnologiyalari rivojlanishida kvant hisoblashlar (quantum computing) yangi davrni boshlab berdi. Hozirgi kunda Internet xavfsizligining poydevori hisoblangan RSA, ECC (Elliptic Curve Cryptography) va Diffie-Hellman kabi asimmetrik shifrlash algoritmlari katta sonlarni ko‘paytuvchilarga ajratish va diskret logarifmlash kabi matematik masalalarning murakkabligiga asoslanadi.

Biroq, Shor algoritmi kabi kvant algoritmlarining paydo bo‘lishi ushbu kriptografik tizimlarning himoya funksiyalarini tubdan zaiflashtiradi. Kvant kompyuterlari klassik kompyuterlardan farqli ravishda eksponensial tezlikda hisoblashlarni amalga oshira oladi, bu esa "Kriptografik halokat" (Cryptographic Apocalypse) xavfini yuzaga keltiradi.

Muammo qo‘yilishi (Problem Statement)

Asosiy xavf nafaqat kelajakdagi tizimlarda, balki bugungi kunda uzatilayotgan va saqlanayotgan ma’lumotlarda ham mavjud. **"Store Now, Decrypt Later"** (Hozir saqlab ol, keyin shifrini och) strategiyasi kiber-hujumchilar uchun eng asosiy vositaga aylanmoqda. Hozirgi kunda shifrlangan maxfiy ma’lumotlar (davlat sirlari, bank ma’lumotlari, shaxsiy ma’lumotlar) tajovuzkorlar tomonidan saqlab qo‘yilmoqda va ular kelajakda kuchli kvant kompyuterlari yordamida shifrdan chiqarilishi kutilmoqda. Ushbu muammo quyidagi jihatlarni qamrab oladi:

Mavjud protokollarning zaifligi:

TLS, SSH va VPN kabi eng keng tarqalgan xavfsizlik protokollari kvant hujumlariga qarshi tura olmaydi.

Infratuzilmani yangilash qiymati:

Dunyo bo‘ylab millionlab serverlar, IoT qurilmalar va dasturiy ta’minotlarni yangi, kvantga chidamli algoritmlarga (Post-Quantum Cryptography - PQC) o‘tkazish ulkan resurs va vaqt talab qiladi.

Post-kvant kriptografiyasining matematik asoslari: Panjara (Lattice) tuzilmalari An’anaviy asimmetrik kriptografiya (RSA) sonlar nazariyasidagi "faktorializatsiya" (tub ko‘paytuvchilarga ajratish) murakkabligiga asoslansa, PQC asosan yuqori o‘lchamli panjaralardagi qidiruv masalalariga tayanadi.

Panjara asosidagi kriptografiyaning mohiyati

Matematik nuqtayi nazardan, n-o‘lchamli panjara L \subset \mathbb{R}^n — bu bazis vektorlarining (b_1, b_2, \dots, b_n) butun sonli chiziqli kombinatsiyasidan hosil bo‘lgan nuqtalar to‘plamidir.

PQCdagi asosiy himoya mexanizmi **"Eng yaqin vektor masalasi" (Closest Vector Problem - CVP)** va **"Eng qisqa vektor masalasi" (Shortest Vector Problem - SVP)** kabi NP-qiyin (NP-hard) masalalarga borib taqaladi. Kvant kompyuterlari uchun ham bunday ko‘p o‘lchamli fazoda eng qisqa yo‘lni topish klassik kompyuterlar kabi o‘ta murakkab hisoblanadi.

NIST standartlari va tanlangan algoritmlar

AQSH Milliy Standartlar va Texnologiyalar Instituti (NIST) kvantga chidamli algoritmlar bo‘yicha tanlov e’lon qildi. Hozirda quyidagi algoritmlar yetakchi hisoblanadi:

Algoritm nomi	Asoslangan matematik model	Asosiy maqsadi
CRYSTALS-Kyber	Module-LWE(Learning With Errors)	Kalit almashish(KEM)
CRYSTALS-Dilithium	Module-LWE	Raqamli imzo(Digital Signature)
Falcon	NTRU/Lattice-based	Yuqori tezlikdagi imzo

Ushbu algoritmlar RSA-2048 yoki ECC-256 dan sezilarli darajada kattaroq kalit o‘lchamlariga ega bo‘lsa-da, ularning hisoblash tezligi nisbatan yuqori.

Amaliy o‘tish muammolari va infratuzilma muammolari

Post-kvant kriptografiyasiga (PQC) o‘tish shunchaki algoritmni almashtirish emas, balki butun raqamli infratuzilmani qayta loyihalash jarayonidir. Quyida mazkur o‘tishning eng asosiy texnik to‘siqlari tahlil qilinadi:

Kalit va imzo o‘lchamlarining oshishi

RSA va ECC algoritmlarida kalit uzunligi nisbatan kichik (masalan, RSA-2048 uchun 256 bayt). PQC algoritmlarida esa kalit va imzo o‘lchamlari bir necha kilobaytga yetishi mumkin.

Muammo:

Protokol paketlari (masalan, TLS "ClientHello" xabari) uchun belgilangan maksimal o‘lcham chegaralari (MTU) oshib ketishi mumkin. Bu esa tarmoq fragmentatsiyasiga va kechikishlarga (latency) olib keladi.

Oqibat:

Eskirgan routerlar va tarmoq qurilmalari katta hajmdagi kalitlarni uzatishda "bottleneck" (tor bo‘g‘iz) hosil qiladi.
4.2. Resurslari cheklangan tizimlar (IoT va Embedded systems)
Aqlli shaharlar va sanoat boshqaruv tizimlaridagi (ICS) kontrollerlar ko‘pincha 8-bitli yoki 16-bitli mikrokontrollerlarda ishlaydi.

Tahlil:

Ushbu qurilmalarning tezkor xotirasi (RAM) PQC algoritmlarining murakkab matematik operatsiyalarini (matritsali ko‘paytirish, polindromik hisoblar) bajarish uchun yetarli emas.

Yechim:

"Yengil kriptografiya" (Lightweight Cryptography) standartlari va PQC ni optimallashtirilgan apparat tezlatkichlarida (FPGA/ASIC) amalga oshirish.

"Gibrid yondashuv" — Xavfsizlikning o‘tish davri strategiyasi

Mutaxassislar birdaniga to‘liq PQC ga o‘tishni tavsiya etmaydilar, chunki yangi algoritmlar hali uzoq muddatli stress-testlardan o‘tmagan.

Strategiya:

Gibrid rejim — klassik (RSA/ECC) va kvantga chidamli (Kyber/Dilithium) algoritmlarni birlashtirish.
Matematik model: K_{final} = K_{classic} \oplus K_{pqc}
Bu yondashuv shuni anglatadiki, agar kelajakda PQC algoritmi zaif deb topilsa, tizim hali ham klassik himoya bilan ta’minlangan bo‘ladi, va aksincha.

Algoritmlarning qiyosiy tahlili va amaliy cheklovlar

Post-kvant kriptografiyasiga (PQC) o‘tishdagi eng asosiy texnik muammo bu klassik algoritmlar bilan solishtirganda kalit o‘lchamlarining sezilarli darajada oshishidir. Masalan, RSA-2048 yoki ECC-256 kabi keng tarqalgan algoritmlar nisbatan kichik hajmdagi kalitlar bilan yuqori tezlikda shifrlash imkonini beradi. Biroq, CRYSTALS-Kyber yoki Dilithium kabi panjara asosidagi algoritmlar xavfsizlikni ta’minlash uchun ancha katta hajmdagi ma’lumotlar to‘plamini talab qiladi.

Bu holat tarmoq infratuzilmasida jiddiy muammolarni keltirib chiqaradi. Xususan, TLS (Transport Layer Security) protokollarining "ClientHello" kabi xabar almashinuv jarayonlarida paket o‘lchamlarining oshishi tarmoq fragmentatsiyasiga olib kelishi mumkin. Bunday fragmentatsiya eski routerlar va tarmoq qurilmalari tomonidan qayta ishlash jarayonida "tor bo‘g‘iz" (bottleneck) effektini hosil qiladi, bu esa tizimning javob berish vaqtini (latency) oshiradi.

Resurslari cheklangan qurilmalar, jumladan, IoT (Narsalar interneti) va o‘rnatilgan tizimlar uchun bu o‘zgarishlar ayniqsa sezilarli. Mazkur kontrollerlar ko‘pincha cheklangan tezkor xotira (RAM) resurslariga ega bo‘lib, PQC algoritmlarining murakkab matritsali ko‘paytirish amallarini bajarishda qiyinchiliklarga duch kelishi mumkin. Shuning uchun, bu sohada dasturiy optimizatsiya va apparat tezlatkichlaridan (FPGA/ASIC) foydalanish kelajakdagi tadqiqotlarning asosiy yo‘nalishi hisoblanadi.

Xavfsizlik siyosati va strategik o‘tish jarayoni

Kvant kompyuterlarining to‘liq quvvatga kirishi kutilayotgan davrda tashkilotlar uchun "Kriptografik egiluvchanlik" (Crypto-Agility) tushunchasi ustuvor ahamiyat kasb etadi. Bu shuni anglatadiki, dasturiy ta’minotlar va axborot tizimlari shunday arxitekturada loyihalashtirilishi kerakki, unda kriptografik algoritm tizimning boshqa qismlariga ta’sir ko‘rsatmasdan, alohida modul sifatida yangilanishi mumkin bo‘lsin.
Ayni damda mutaxassislar birdaniga to‘liq PQC ga o‘tish o‘rniga, "Gibrid yondashuv" strategiyasini qo‘llashni tavsiya etadilar. Bunda klassik RSA yoki ECC algoritmlari yangi kvantga chidamli algoritmlar bilan birgalikda ishlatiladi. Matematik jihatdan bu jarayon kalitlarni birlashtirish orqali amalga oshiriladi, bunda har ikkala algoritmning himoya mexanizmi bir vaqtda ishlaydi. Agar kelajakda PQC algoritmlaridan birida zaiflik aniqlansa,

tizim baribir klassik himoya bilan ta’minlangan bo‘ladi. Bu yondashuv xavfsizlikning uzluksizligini va o‘tish davridagi risklarning kamayishini ta’minlaydi.

"Kvant hujumlarining matematik mexanizmi"

Hozirgi matnda Shor algoritmi haqida qisqa aytib o‘tdik. Uni matematik jihatdan kengaytiramiz:

Shor algoritmining murakkabligi: O((\log N)^3).

RSA algoritmi va "Hidden Subgroup Problem" (Yashirin guruh masalasi) o‘rtasidagi bog‘liqlik.

Bu qism maqolaning "ilmiy vaznini" keskin oshiradi.

"PQC ga o‘tishning iqtisodiy va ijtimoiy jihatlari"

Global axborot tizimlarining yangilanishi uchun ketadigan xarajatlar tahlili.

"Kiber-suverenitet" va milliy kriptografik standartlarning ahamiyati (bu ayniqsa Beruniy stipendiyasi uchun qilayotgan ishingizda muhim bo'lishi mumkin).

"Case Study: Bank va Davlat sektori misolida"

Bank tizimida ma’lumotlarning "umr ko‘rish davri" (misol: kredit tarixini 50 yil saqlash).

Agar hozirgi ma’lumotlar yozib olinsa, 20 yil o‘tib kvant kompyuteri uni qanday oson ocha olishi haqida batafsil stsenariy.

"Tashkilotlar uchun amaliy tavsiyalar"

Kriptografik audit o‘tkazish tartibi.
Vendor (dasturiy ta’minot yetkazib beruvchi) tanlashda PQC talablarini belgilash.

Kvant hujumlarining matematik mexanizmi va Shor algoritmi

An’anaviy asimmetrik kriptografiya, xususan RSA, tub ko‘paytuvchilarni topish (integer factorization) va diskret logarifmlash masalalarining klassik kompyuterlar uchun o‘ta murakkabligiga asoslanadi. Klassik algoritmlar, masalan, "General Number Field Sieve" (GNFS), katta sonni ko‘paytuvchilarga ajratish uchun sub-eksponensial vaqt talab qiladi. Bu esa RSA-2048 kabi uzunlikdagi kalitlarni amalda buzib bo‘lmas holatga keltiradi.

Biroq, 1994-yilda Piter Shor tomonidan taklif etilgan kvant algoritmi ushbu paradigmani tubdan o‘zgartirdi. Shor algoritmi kvant kompyuterlarining superpozitsiya va interferensiya xususiyatlaridan foydalanib, periodni aniqlash (period finding) masalasini hal qiladi. Matematik nuqtayi nazardan, N sonini ko‘paytuvchilarga ajratish masalasi, f(x) = a^x \pmod N funksiyasining periodini topish masalasiga keltiriladi. Klassik kompyuterlar uchun bu funksiyaning davrini topish eksponensial vaqt talab qilsa, kvant kompyuterlarida "Quantum Fourier Transform" (QFT) yordamida bu jarayon polynomial vaqtda, ya'ni O((\log N)^3) murakkablikda bajariladi.

Ushbu jarayonning mohiyati shundaki, kvant kompyuteri bir vaqtning o‘zida barcha mumkin bo‘lgan x qiymatlarini qayta ishlab, ularning superpozitsiyasini yaratadi. QFT orqali esa noto‘g‘ri natijalar o‘chib ketadi va to‘g‘ri periodga mos keluvchi amplitudalar kuchayadi. Bu esa RSA algoritmining asosiy poydevori bo‘lgan "trapdoor" funksiyani shunchaki matematik tenglamaga aylantirib qo‘yadi.

Shor algoritmi shunchaki nazariy tahdid emas, u hisoblash murakkabligi nazariyasidagi inqilobdir. U shuni ko‘rsatadiki, NP-qiyin deb hisoblangan masalalar, agar kvant tizimlari yetarli darajada rivojlansa, himoya vositasi bo‘lishdan to‘xtaydi. Shuning uchun, kriptografik xavfsizlikni qayta ko‘rib chiqishda faqatgina algoritmlar tezligiga emas, balki ularning matematik asosidagi "yashirin guruh" (Hidden Subgroup Problem) tuzilmasiga e’tibor qaratishimiz zarur.

Kiber-suverenitet va milliy kriptografik standartlar

Axborot tizimlarining xavfsizligi bugungi kunda davlatlarning axborot suvereniteti bilan chambarchas bog‘liq. Post-kvant davriga o‘tishda xalqaro standartlarga (NIST tomonidan tanlangan) tayanish bilan bir qatorda, har bir davlat o‘zining milliy kriptografik algoritmlarini rivojlantirishi muhim ahamiyat kasb etadi.

Bu masalaning iqtisodiy jihati ham mavjud: dunyo bo‘ylab millionlab serverlar, davlat idoralari va bank tizimlarini yangi kriptografik standartlarga o‘tkazish milliardlab dollarlik resurs va texnik infratuzilmani yangilashni talab qiladi. "Kriptografik suverenitet" tushunchasi ostida, davlatlar o‘zlarining maxfiy ma’lumotlarini xorijiy kompaniyalar nazorat qiladigan shifrlash vositalaridan emas, balki mahalliy ekspertlar tomonidan auditi o‘tkazilgan kvantga chidamli tizimlardan foydalangan holda himoyalashlari lozim.

Kelajakda kiber-hujumlar nafaqat texnik, balki geopolitik vositaga aylanadi. Kvant kompyuterlariga ega bo‘lgan davlatlar yoki xalqaro guruhlar, ushbu texnologiyadan foydalanib, global moliyaviy va siyosiy ma’lumotlar bazasiga kirish imkoniga ega bo‘lishi mumkin. Shuning uchun, PQC ga o‘tish jarayonini "texnik yangilanish" emas, balki "milliy xavfsizlik loyihasi" deb baholash to‘g‘riroq bo‘ladi.

Case Study: Bank sektorida PQC ga o‘tish va "Ma’lumotlar umr ko‘rish davri" muammosi

Bank tizimi kiberxavfsizlikning eng nozik nuqtasi hisoblanadi. Banklar nafaqat tranzaksiyalarni himoya qilishi, balki mijozlarning moliyaviy ma’lumotlarini o‘nlab yillar davomida saqlashi shart. Bu yerda **"Store Now, Decrypt Later"** (Hozir saqlab ol, keyin shifrini och) hujum modeli eng katta xavfni yuzaga keltiradi.

Ma’lumotlarning uzoq muddatli qiymati

Bank arxivlaridagi shifrlangan ma’lumotlar (mijozlar kredit tarixi, shaxsiy ma’lumotlar, mulkiy hujjatlar) 20-30 yil davomida dolzarb bo‘lib qoladi. Kiber-hujumchi bugun ushbu ma’lumotlarni RSA-2048 yoki AES-256 shifrlash usullari bilan to‘liq qulflangan holda o‘g‘irlab olishi mumkin. Hozirgi kunda tajovuzkor bu ma’lumotlarni ocha olmaydi. Biroq, 10-15 yildan so‘ng, yetarlicha quvvatga ega kvant kompyuteri paydo bo‘lganda, ushbu o‘g‘irlangan arxivlar shifrdan chiqariladi. Natijada, mijozning o‘n yillik moliyaviy tarixi oshkor bo‘ladi.

Bank infratuzilmasini modernizatsiya qilish strategiyasi

Banklar uchun PQC ga o‘tish faqatgina dasturiy ta’minotni yangilash emas, balki murakkab logistika jarayonidir:

Kriptografik inventarizatsiya:

Bank tarmog‘idagi har bir server, har bir ATM (bankomat) va mijozlarga xizmat ko‘rsatish terminalida qaysi algoritmlar ishlatilayotganini aniqlash.

Bosqichma-bosqich o‘tish:

Banklar o‘zlarining xizmat ko‘rsatish tizimlarida (misol uchun, bank mijozining mobil ilovasi va server o‘rtasidagi aloqa) gibrid shifrlash protokollarini joriy etishlari shart. Bunda an’anaviy TLS protokoli PQC mexanizmi bilan parallel ishlaydi.

Resurslar chegarasi:

Bank xodimlari foydalanadigan maxsus dasturiy ta’minotlar va xavfsizlik tizimlari (HSM - Hardware Security Modules) yangi PQC standartlarini qo‘llab-quvvatlaydigan apparat qismlariga almashtirilishi kerak. Bu esa banklar uchun ulkan kapital qo‘yilmalarni talab qiladi.

Tadqiqotchi nuqtayi nazari: Banklar uchun PQC ga o‘tish "tavsiya" emas, balki majburiyatdir. Moliyaviy tizimda ishonchning yo‘qolishi (ma’lumotlarning sizib chiqishi) bankning qulashiga olib kelishi mumkin. Shu sababli, banklar kelgusi 5 yil ichida o‘zlarining "kriptografik agillik" (crypto-agility) strategiyasini ishlab chiqishlari va uni amalga oshirishlari maqsadga muvofiqdir.

Kriptografik audit va tizimli yondashuv

Tashkilotlar uchun PQC ga o‘tishni boshlash uchun quyidagi audit bosqichlari tavsiya etiladi:

1. **Aniqlash (Discovery):**

Tashkilotdagi barcha kriptografik aktivlarni, shu jumladan, uchinchi tomon dasturiy ta’minotlari (vendor-provided software) ichidagi shifrlash modullarini identifikatsiya qilish.

2. **Risk tahlili:**

Qaysi ma’lumotlar uzoq muddatli xavfsizlikni talab qiladi va qaysilari qisqa muddatli? (Uzoq muddatli ma’lumotlar birinchi navbatda PQC himoyasiga o‘tkazilishi kerak).

3. **Protokollarni yangilash:**

Standart aloqa protokollarini (TLS 1.3, VPN) kvantga chidamli gibrid tizimlarga o‘tkazish uchun yangi xavfsizlik kutubxonalarini (masalan, Open Quantum Safe - OQS) test muhitida sinovdan o‘tkazish.

4. **Doimiy monitoring:**

PQC algoritmlari hali yangi bo‘lganligi sababli, ularning barqarorligi va ishlash tezligi ustidan doimiy nazorat o‘rnatish.

Xulosa

Kvant hisoblash texnologiyalarining jadal rivojlanishi axborot xavfsizligi sohasida paradigmaning tubdan o‘zgarishini talab qilmoqda. Hozirgi kunda Internet xavfsizligining poydevori bo‘lib xizmat qilayotgan RSA va ECC kabi asimmetrik shifrlash algoritmlari, kvant kompyuterlari tomonidan taqdim etiladigan hisoblash quvvati oldida o‘z himoya funksiyasini yo‘qotish xavfi ostida. Shor algoritmi va kvant parallelizmi klassik kriptografiyaning "trapdoor" funksiyalarini samarali yengib o‘tishga qodir. Ushbu tadqiqotda ko‘rsatilganidek, post-kvant kriptografiyasiga (PQC) o‘tish shunchaki

algoritmni yangilash emas, balki butun raqamli infratuzilmani qayta loyihalash jarayonidir. Gibrid yondashuvlar, kriptografik agillik (crypto-agility) va milliy axborot suverenitetini ta’minlash — kelajakdagi xavfsiz axborot tizimlarining uchta ustuni hisoblanadi. Banklar, davlat idoralari va IoT tizimlari hozirdanoq o‘zlarining kriptografik aktivlarini inventarizatsiya qilishlari va uzoq muddatli ma’lumotlar xavfsizligini ta’minlash uchun kvantga chidamli algoritmlarni (masalan, Kyber, Dilithium) bosqichma-bosqich joriy etishlari zarur.

Kelajakdagi tadqiqotlar nafaqat yangi algoritmlarni yaratishga, balki ushbu algoritmlarning resurslari cheklangan qurilmalarda ishlash samaradorligini optimallashtirishga qaratilishi kerak. Axborot xavfsizligi — bu statik holat emas, balki rivojlanayotgan tahdidlarga doimiy ravishda moslashib boruvchi dinamik jarayondir.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI (REFERENCES)

1. **NIST (National Institute of Standards and Technology).** *Announcing Post-Quantum Cryptography Standards.* U.S. Department of Commerce, 2024.

2. **Shor, P. W.** (1994). *Algorithms for quantum computation: discrete logarithms and factoring.* Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE.

3. **Bernstein, D. J., & Lange, T.** (2017). *Post-quantum cryptography.* Nature News, 549(7671), 188-194.

4. **Alagic, G., et al.** (2022). *Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process.* NIST Internal Report 8413.

5. **Chen, L., et al.** (2016). *Report on Post-Quantum Cryptography.* NIST Internal Report 8105.

6. **Gentry, C.** (2009). *Fully Homomorphic Encryption Using Ideal Lattices.* Proceedings of the 41st Annual ACM Symposium on Theory of Computing.

7. **Hoffstein, J., Pipher, J., & Silverman, J. H.** (1998). *NTRU: A ring-based public key cryptosystem.* Algorithmic Number Theory, Springer.

8. **Buchmann, J. A., et al.** (2013). *Post-Quantum Cryptography.* Springer Science & Business Media.

9. **Moody, D.** (2020). *The NIST Post-Quantum Cryptography Standardization Project: A Status Update.* NIST.

10. **Stallings, W.** (2023). *Cryptography and Network Security: Principles and Practice.* Pearson Education.