

KVANT HISOBLASH DAVRIGA TAYYORGARLIK: MILLIY AXBOROT TIZIMLARINI POSTKVANT KRIPTOGRAFIYAGA BOSQICHMA- BOSQICH O'TKAZISH MODELI

Yuldashev Ramozon Shokir o'g'li

Termiz iqtisodiyot va servis universiteti

Annotatsiya. Maqolada kvant kompyuterlarining rivojlanishi natijasida zamonaviy ochiq kalitli kriptografik algoritmlarga yuzaga kelayotgan tahdid tahlil qilingan. 2024-yilda AQSh Standartlar va texnologiyalar milliy instituti (NIST) tomonidan qabul qilingan postkvant kriptografiya standartlari ko'rib chiqilgan. Elektron hukumat, bank va elektron raqamli imzo tizimlarini postkvant algoritmlarga bosqichma-bosqich o'tkazish modeli taklif etilgan hamda o'tish davridagi texnik muammolar yoritilgan.

Kalit so'zlar: kvant hisoblash, postkvant kriptografiya, Shor algoritmi, ML-KEM, ML-DSA, kripto-moslashuvchanlik, elektron raqamli imzo.

Аннотация. В статье анализируется угроза, которую развитие квантовых компьютеров создаёт для современных криптографических алгоритмов с открытым ключом. Рассмотрены стандарты постквантовой криптографии, принятые Национальным институтом стандартов и технологий США (NIST) в 2024 году. Предложена модель поэтапного перевода систем электронного правительства, банковских систем и систем электронной цифровой подписи на постквантовые алгоритмы, освещены технические проблемы переходного периода.

Ключевые слова: квантовые вычисления, постквантовая криптография, алгоритм Шора, ML-KEM, ML-DSA, криптогибкость, электронная цифровая подпись.

Abstract. The article analyzes the threat that the development of quantum computers poses to modern public-key cryptographic algorithms. The post-quantum cryptography standards adopted by the US National Institute of Standards and Technology (NIST) in 2024 are reviewed. A model for the phased migration of e-government, banking and electronic digital signature systems to post-quantum algorithms is proposed, and the technical challenges of the transition period are discussed.

Keywords: quantum computing, post-quantum cryptography, Shor's algorithm, ML-KEM, ML-DSA, crypto-agility, electronic digital signature.

KIRISH

Bugungi kunda internet orqali uzatiladigan ma'lumotlar, elektron raqamli imzo va bank tranzaksiyalarining xavfsizligi asosan RSA, Diffi–Xellman va elliptik egri chiziqlarga asoslangan (ECC) algoritmlarga tayanadi. Bu algoritmlarning bardoshlilikiga katta sonlarni tub ko'paytuvchilarga ajratish va diskret logarifmlash masalalarini klassik kompyuterlarda amalda yechib bo'lmasiligiga asoslangan.

Biroq 1994-yilda P.Shor kvant kompyuterida ushbu masalalarni polinomial vaqtda yechuvchi algoritmi taklif etgan [1]. Yetarli quvvatga ega kvant kompyuteri hali yaratilmagan bo'lsa-da, xavf allaqachon real: tajovuzkorlar hozir shifrlangan ma'lumotlarni to'plab, kelajakda ularni ochish strategiyasini ("harvest now, decrypt later") qo'llashi mumkin. Shu bois uzoq muddat maxfiy saqlanishi lozim bo'lgan ma'lumotlar bugunning o'zida himoyaga muhtoj.

O'zbekistonda elektron hukumat, soliq, bank va elektron raqamli imzo tizimlari jadal rivojlanmoqda, "Kiberxavfsizlik to'g'risida"gi Qonun [7] esa muhim axborot infratuzilmasi obyektlarini himoya qilish tartibini belgilab bergan. Ammo milliy axborot tizimlarini postkvant kriptografiyaga o'tkazish masalasi hali tizimli o'rganilmagan. Maqolaning maqsadi kvant tahdidining mohiyatini tahlil qilish va ushbu o'tishning bosqichma-bosqich modelini taklif etishdan iborat.

ASOSIY QISM

Kvant tahdidining mohiyati. Kvant algoritmlari kriptografik algoritmlarga turlicha ta'sir qiladi. Shor algoritmi ochiq kalitli (asimmetrik) algoritmlarni to'liq zaiflashtiradi, L.Grover algoritmi [2] esa simmetrik shifrlash va xesh-funksiyalarga qarshi hujumni faqat kvadratik darajada tezlashtiradi. Demak, simmetrik algoritmlar uchun kalit uzunligini oshirish yetarli bo'lsa, asimmetrik algoritmlarni butunlay almashtirishga to'g'ri keladi (1-jadval).

1-jadval. Kriptografik algoritmlarga kvant tahdidi darajasi [3–5; 8]

Algoritm	Vazifasi	Tahdid darajasi	Tavsiya etilgan yechim
RSA, ECDSA	Raqamli imzo	Yuqori (Shor algoritmi)	ML-DSA, SLH-DSA
RSA, DH, ECDH	Kalit almashish	Yuqori (Shor algoritmi)	ML-KEM
AES-128	Simmetrik shifrlash	O'rtacha (Grover algoritmi)	AES-256

Algoritm	Vazifasi	Tahdid darajasi	Tavsiya etilgan yechim
SHA-256	Xeshlash	Past	SHA-256 yoki SHA-384

Postkvant standartlar. NIST 2016-yilda boshlagan ko‘p bosqichli tanlovdan so‘ng 2024-yil avgust oyida uchta standartni e‘lon qildi: panjaralarga (lattice) asoslangan ML-KEM kalit inkapsulyatsiya mexanizmi (FIPS 203) [3], ML-DSA raqamli imzo algoritmi (FIPS 204) [4] va xesh-funksiyalarga asoslangan SLH-DSA raqamli imzo algoritmi (FIPS 205) [5]. Ushbu algoritmlarning xavfsizligi kvant kompyuterlari uchun ham samarali yechimi ma‘lum bo‘lmagan matematik masalalarga asoslangan [8]. NIST e‘lon qilgan o‘tish rejasi loyihasida kvant hujumlariga zaif algoritmlarni 2030-yildan keyin eskirgan deb hisoblash, 2035-yildan so‘ng esa ulardan foydalanishni to‘xtatish ko‘zda tutilgan [9].

Xavfni baholash mezoni. Tashkilot qachon harakat boshlashi kerakligini aniqlashda M.Moska taklif etgan mezondan foydalanish qulay [6]: agar $x + y > z$ bo‘lsa, tashkilot xavf ostida hisoblanadi. Bu yerda x – ma‘lumotlarning maxfiy saqlanishi zarur bo‘lgan muddat, y – tizimni yangi algoritmlarga to‘liq o‘tkazish uchun zarur vaqt, z – kriptografik jihatdan xavfli kvant kompyuteri paydo bo‘lishigacha qolgan vaqt. Masalan, soliq yoki tibbiy ma‘lumotlar 20 yil maxfiy saqlanishi, o‘tish esa 7 yil davom etishi kerak bo‘lsa, kvant kompyuteri 27 yildan oldin paydo bo‘lishi ehtimoli bor ekan, bu ma‘lumotlar bugunoq xavf ostida bo‘ladi.

Bosqichma-bosqich o‘tish modeli. Postkvant kriptografiyaga o‘tish bir martalik almashtirish emas, balki bir necha yil davom etadigan jarayondir. Milliy axborot tizimlari uchun quyidagi besh bosqichli model taklif etiladi:

- 1) *kriptografik inventarizatsiya* – qaysi tizimda qanday algoritmlar, kalitlar va sertifikatlar ishlatilayotganini aniqlash;
- 2) *risklar bo‘yicha ustuvorlashtirish* – Moska mezoni asosida uzoq muddat maxfiy saqlanadigan ma‘lumotlarni qayta ishlovchi tizimlarni (soliq, tibbiyot, davlat arxivi, bank) birinchi navbatga qo‘yish;
- 3) *gibrid rejim* – klassik va postkvant algoritmlarni birgalikda qo‘llash, bunda ulardan biri buzilgan taqdirda ham himoya saqlanib qoladi;
- 4) *kripto-moslashuvchanlik* – algoritmni dastur kodini qayta yozmasdan, sozlamalar orqali almashtirish imkonini beruvchi arxitekturaga o‘tish;
- 5) *to‘liq o‘tish va monitoring* – zaif algoritmlarni bosqichma-bosqich o‘chirish va jarayonni doimiy nazorat qilish.

Gibrid yondashuv amalda o'zini oqlamoqda: yetakchi veb-brauzerlar TLS protokolida klassik X25519 va ML-KEM algoritmlarini birlashtiruvchi gibrid kalit almashish usulini qo'llab-quvvatlay boshladi.

O'tish davridagi muammolar. Postkvant algoritmlarning kalit va imzo o'lchamlari klassik algoritmlarnikidan ancha katta. Masalan, ML-DSA-44 imzosining hajmi 2420 baytni tashkil etadi [4], bu ECDSA P-256 imzosidan (64 bayt) qariyb 38 marta katta. Bu esa tarmoq trafigi, smart-kartalar va USB-tokenlar xotirasiga qo'shimcha yuk tushiradi. Bundan tashqari, elektron raqamli imzo kalitlarini saqlovchi qurilmalarni yangilash, milliy kriptografik standartlarni qayta ko'rib chiqish hamda sohada malakali mutaxassislar tayyorlash zarurati yuzaga keladi.

XULOSA

Kvant hisoblashning rivojlanishi ochiq kalitli kriptografiyaga asoslangan barcha axborot tizimlari uchun strategik tahdid hisoblanadi va unga tayyorgarlikni hozirdan boshlash zarur. Tahlil natijalariga ko'ra quyidagilar taklif etiladi:

- 1) milliy darajada postkvant kriptografiyaga o'tish bo'yicha "yo'l xaritasi"ni ishlab chiqish;
- 2) muhim axborot infratuzilmasi obyektlarida kriptografik inventarizatsiya o'tkazishni majburiy talab sifatida belgilash;
- 3) elektron hukumat va bank tizimlarida gibrid rejimni tajriba-sinov loyihasi sifatida joriy etish;
- 4) milliy kriptografik standartlarga postkvant algoritmlarni kiritish masalasini o'rganish;
- 5) oliy ta'lim muassasalarining kiberxavfsizlik yo'nalishlari o'quv dasturlariga postkvant kriptografiya mavzularini kiritish.

Ushbu choralar milliy axborot tizimlarining uzoq muddatli xavfsizligini ta'minlashga xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR

1. Shor P.W. Algorithms for quantum computation: discrete logarithms and factoring // Proceedings 35th Annual Symposium on Foundations of Computer Science. – IEEE, 1994. – P. 124–134.
2. Grover L.K. A fast quantum mechanical algorithm for database search // Proceedings of the 28th Annual ACM Symposium on Theory of Computing. – 1996. – P. 212–219.
3. NIST FIPS 203. Module-Lattice-Based Key-Encapsulation Mechanism Standard. – Gaithersburg: NIST, 2024.
4. NIST FIPS 204. Module-Lattice-Based Digital Signature Standard. – Gaithersburg: NIST, 2024.

5. NIST FIPS 205. Stateless Hash-Based Digital Signature Standard. – Gaithersburg: NIST, 2024.
6. Mosca M. Cybersecurity in an Era with Quantum Computers: Will We Be Ready? // IEEE Security & Privacy. – 2018. – Vol. 16, No. 5. – P. 38–41.
7. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni. 2022-yil 15-aprel, O‘RQ-764-son.
8. Bernstein D.J., Lange T. Post-quantum cryptography // Nature. – 2017. – Vol. 549. – P. 188–194.
9. NIST IR 8547 (Initial Public Draft). Transition to Post-Quantum Cryptography Standards. – Gaithersburg: NIST, 2024.