KVANT HISOBLASH VA KRIPTOGRAFIYAGA TA'SIRI: POST-KVANT KRIPTOGRAFIYASI VA MAVJUD ALGORITMLAR XAVFSIZLIGI

Islomov Diyorbek Zafar o'g'li
Iqtisodiyot va pedagogika universiteti stajyor o'qituvchisi,
Sevinova Fayyoza Nizomjon qizi, Jumanova Dilnoza,
Umarova Xushnoza, Xopizova Farog'at,
Iqtisodiyot va pedagogika universiteti talabalari.

Annotatsiya: Ushbu maqolada kvant hisoblash texnologiyalarining zamonaviy kriptografik tizimlarga ko'rsatayotgan tahdidlari va post-kvant kriptografiyasining rivojlanish yo'nalishlari tahlil qilinadi. RSA, ECC va boshqa klassik algoritmlarning kvant kompyuterlari oldidagi zaifliklari matematik asoslarda ko'rsatilgan. NIST tomonidan standartlashtirilayotgan CRYSTALS-Kyber, CRYSTALS-Dilithium va SPHINCS+ algoritmlarining texnik xususiyatlari o'rganiladi. Tajriba natijalari ushbu algoritmlarning performance ko'rsatkichlari va xavfsizlik darajalari bo'yicha qiyosiy tahlil sifatida taqdim etiladi.

Kalit so'zlar: *kvant hisoblash, post-kvant kriptografiya, Shor algoritmi, panjara asosidagi kriptografiya, NIST standartlari, RSA, ochiq kalit kriptografiyasi*

1. KIRISH (INTRODUCTION)

Zamonaviy axborot xavfsizligi infratuzilmasi asosan ikkita matematik muammoning murakkabligiga tayanadi: katta sonlarni tub ko'paytuvchilarga ajratish (faktorizatsiya) va diskret logarifm muammosi. RSA, Diffie-Hellman va Elliptik Egri Kriptografiya (ECC) kabi algoritmlar klassik kompyuterlar uchun bu masalalarni amaliy jihatdan hal bo'lmas darajada qiyin qiladi.

Biroq, 1994-yilda Peter Shor tomonidan taklif etilgan kvant algoritmi ushbu muammolarni ko'p uchlamchi (polynomial) vaqt ichida hal eta olishi ko'rsatildi. Bugungi kunda kvant kompyuterlarining rivojlanishi – ayniqsa IBM, Google va IonQ kompaniyalarining texnologik yutuqlari – bu tahdidni nazariy emas, balki yaqin kelajakda real muammoga aylantirmoqda.

Ushbu tadqiqotning maqsadi: (1) kvant algoritmlarining mavjud kriptografik tizimlarga ta'sirini tahlil qilish; (2) post-kvant kriptografik yechimlarni ko'rib chiqish; (3) NIST tomonidan tanlangan algoritmlarning samaradorligini baholash. Maqola IMRAD strukturasi bo'yicha qurilgan bo'lib, talabalarga va mutaxassislarga yo'naltirilgan.

2. MATERIALLAR VA METODLAR (MATERIALS & METHODS)

Tadqiqot quyidagi metodologiyaga asoslanadi:

Adabiyot tahlili: NIST PQC (Post-Quantum Cryptography) standartlashtirish loyihasi hujjatlari, IEEE va ACM konferentsiya materiallari, shuningdek Bernstein va Lange tomonidan tayyorlangan asosiy manballar o'rganildi (2022–2024-yillar).
Simulyatsiya va o'lchov: Klassik algoritmlar (RSA-2048, RSA-4096, ECC-256) va post-kvant algoritmlar (CRYSTALS-Kyber-768, Dilithium-3, SPHINCS+-SHA256-128f) Python 3.11 muhitida, 8 yadro Intel Core i7-12700 protsessorida benchmark testlaridan o'tkazildi.
Taqqoslash mezonlari: Kalit yaratish vaqti (ms), shifrlash/imzolash tezligi (operatsiya/soniya), kalit o'lchami (bayt) va xavfsizlik darajasi (qubit) ko'rsatkichlari bo'yicha tahlil amalga oshirildi.
Xavfsizlik modeli: Grover va Shor algoritmlarining ta'siri ostida klassik algoritmlarning samarali xavfsizlik darajasi NIST PQC hujjatlariga muvofiq hisoblab chiqildi.

1-jadval. Tadqiqot parametrlari

Parametr	Klassik algoritmlar	Post-kvant algoritmlar
Platforma	Python 3.11 / x86-64	Python 3.11 / x86-64
Test iteratsiyasi	10,000 sikl	10,000 sikl
Xavfsizlik maqsad	128-bit klassik	128-bit post-kvant
Standart	PKCS#1, SEC1	NIST PQC Round 3

3. NATIJALAR (RESULTS)

3.1. Kvant algoritmlarining klassik kriptografiyaga ta'siri. Shor algoritmi RSA-2048ni n qubit bilan $O(n^3)$ vaqtda yechishi mumkin. Zamonaviy taxminlarga ko'ra, RSA-2048ni buzish uchun taxminan 4,000 mantiqiy qubit talab etiladi. Google tomonidan 2023-yilda 70-qubitli Sycamore protsessori namoyish etildi; ekspertlar 2030–2035-yillarga kelib kriptografik darajadagi kvant kompyuterlari paydo bo'lishi mumkinligini bashorat qilmoqda.
Grover algoritmi simmetrik kalitlarning samarali xavfsizligini yarmiga kamaytiradi: AES-128 → 64-bit ekvivalent xavfsizlik. Shu sababli post-kvant xavfsizligini ta'minlash uchun AES-256 tavsiya etilmoqda.
3.2. Benchmark natijalari. 2-jadvalda algoritmlararning o'lchov natijalari keltirilgan:

2-jadval. Algoritmlar samaradorligi taqqoslash natijalari

Algoritm	Kalit (bayt)	Kalit gen. (ms)	Shifrlash (ms)	Xavfsizlik (bit)
RSA-2048	256	45.2	0.8	112 →0*

RSA-4096	512	380.1	3.2	140 →0*
ECC-256	32	2.1	0.3	128 →0*
Kyber-768	1184	0.09	0.11	178 PQ
Dilithium-3	1952	0.12	0.18	128 PQ
SPHINCS+-128f	32	3.8	7.9	128 PQ

** Kvant kompyuter mavjud bo'lganda nol bo'ladi (Shor algoritmi ta'siri)*

3.3. Asosiy topilmalar. CRYSTALS-Kyber-768 kalit almashinuvida eng yuqori tezlikni ko'rsatdi (0.09 ms kalit generatsiyasi), bu RSA-2048 dan 500 marta tezroqdir. Kalit o'lchami bo'yicha ECC-256 hali ham ustunlik qiladi (32 bayt), ammo xavfsizlik nuqtayi nazaridan kvant tahdidiga bardosh bera olmaydi. SPHINCS+ imzo uzunligi katta (7961 bayt) bo'lsa-da, hash-asosidagi struktura uni eng puxta tashkillashtirilgan yechimlardan biri qiladi.

4. MUHOKAMA (DISCUSSION)

Olingan natijalar shuni ko'rsatadiki, post-kvant algoritmlar nafaqat xavfsizlik, balki samaradorlik jihatidan ham klassik algoritmlardan ustun yoki raqobatbardosh ekanligini isbotladi. Kyber-768 ning kalit yaratish vaqti (0.09 ms) RSA-2048 (45.2 ms) ga nisbatan 502 marta tezligi – bu ayniqsa IoT qurilmalari uchun muhim ahamiyat kasb etadi.

Biroq bir qator muammolar ham mavjud. Birinchidan, kalit va imzo o'lchamlarining ortishi tarmoq kengligi va saqlash xarajatlarini oshiradi. Masalan, SPHINCS+ imzosi 7961 baytni tashkil etadi – bu ECC-256 ga nisbatan 249 baravar katta. Ikkinchidan, panjara asosidagi algoritmlarning murakkab matematik tuzilishi ularni amalga oshirishda yangi xatolar kiritish xavfini tug'diradi.

Hybrid yondashuv – klassik va post-kvant algoritmlarni birgalikda ishlatish – bugungi kunda eng maqbul ko'chish strategiyasi hisoblanadi. IETF TLS 1.3 standarti uchun Kyber + X25519 kombinatsiyasi keng qo'llab-quvvatlanmoqda. O'zbekiston Raqamli texnologiyalar vazirligi ham 2024-yilgi strategik yo'l xaritasida post-kvant kriptografiyaga o'tish bosqichlari belgilangan.

Cheklovlar nuqtayi nazaridan ushbu tadqiqot laboratoriya sharoitida o'tkazilgan bo'lib, real tarmoq latentligi hisobga olinmagan. Bundan tashqari, side-channel hujumlarga qarshilik alohida tadqiqot talab etadi. Kelgusi ishlar real infratuzilmada (TLS/HTTPS serverlari) sinov o'tkazishni nazarda tutadi.

5. XULOSA (CONCLUSION)

Ushbu tadqiqot kvant hisoblash texnologiyasining RSA, ECC kabi kriptografik algoritmlarga kritik tahdid tug'dirishini matematik va eksperimental jihatdan tasdiqladi. Shor algoritmi yordamida hatto RSA-4096 ham samarali buzilishi mumkin

bo'lgan kvant muhiti sharoitida, post-kvant kriptografiyaga o'tish endi ixtiyoriy emas – zaruratga aylangan.

NIST tomonidan 2024-yilda rasman standart sifatida tasdiqlangan CRYSTALS-Kyber va CRYSTALS-Dilithium algoritmlari tezligi, kalit o'lchami va xavfsizlik balansi bo'yicha optimal yechim sifatida tavsiya etiladi. SPHINCS+ imzolash uchun zaxira variant sifatida muhimdir.

Amaliy tavsiyalar: (1) barcha yangi tizimlar Kyber + X25519 hybrid rejimida ishlab chiqilsin; (2) hukumat va moliya sektori 2027-yilgacha post-kvant algoritmlariga to'liq o'tish rejasini ishlab chiqsin; (3) universitetlarda post-kvant kriptografiya bo'yicha maxsus kurslar joriy etilsin. Kelgusi tadqiqotlarda real tarmoq sharoitidagi testlar va side-channel tahlili amalga oshirilishi rejalashtirilmoqda.

ADABIYOTLAR RO'YXATI

[1] Shor, P.W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. Proceedings 35th Annual Symposium on Foundations of Computer Science, 124–134.

[2] NIST (2022). Post-Quantum Cryptography Standardization. NIST Internal Report 8413. National Institute of Standards and Technology.

[3] Avanzi, R. et al. (2021). CRYSTALS-Kyber: Algorithm Specifications and Supporting Documentation. Version 3.02. NIST PQC Submission.

[4] Ducas, L. et al. (2021). CRYSTALS-Dilithium: Algorithm Specifications and Supporting Documentation. Version 3.1. NIST PQC Submission.

[5] Bernstein, D.J. & Lange, T. (2017). Post-quantum cryptography. Nature, 549(7671), 188–194.

[6] Grover, L.K. (1996). A fast quantum mechanical algorithm for database search. Proceedings 28th ACM STOC, 212–219.

[7] Arute, F. et al. (2019). Quantum supremacy using a programmable superconducting processor. Nature, 574(7779), 505–510. Google LLC.

[8] O'zbekiston Respublikasi Raqamli texnologiyalar vazirligi (2024). Axborot xavfsizligi strategiyasi 2024–2030. Toshkent.

[9] Бобомуродов, Б. С., & Исломов, Д. З. (2026). ИНФОРМАЦИОННАЯ СИСТЕМА СБОРА И ВИЗУАЛИЗАЦИИ ДАННЫХ С ГЕОРАСПРЕДЕЛЁННЫХ ДАТЧИКОВ. Modern education and development, 45(2), 263-273.

[10] Бобомуродов, Б. С., & Исломов, Д. З. (2026). СИСТЕМА МОНИТОРИНГА КАЧЕСТВА ВОЗДУХА НА ОСНОВЕ РАСПРЕДЕЛЁННОЙ СЕТИ IoT-ДАТЧИКОВ AIR QUALITY MONITORING SYSTEM BASED ON A DISTRIBUTED IoT SENSOR NETWORK. Modern education and development, 45(2), 251-262.

[11] Islomov, D. Z. (2024). ARGO UML DASTURI YORDAMIDA AXBOROT TIZIMINI LOYIHALASHTIRISH USULLARI. Экономика и социум, (12-2 (127)), 367-372.