ZAMONAVIY KVANT TEXNOLOGIYALARI: KVANT KOMPYUTERLAR VA KRIPTOGRAFIYA

Begmuradov Shohzod Dilmurod o'g'li
Jizzax davlat pedagogika universiteti

Annotatsiya: Ushbu maqolada zamonaviy kvant texnologiyalari — xususan, kvant kompyuterlar va kvant kriptografiyasi — keng ko‘lamda tahlil qilinadi. Avvalo, kvant hisoblashning ilmiy asoslari, uning an’anaviy raqamli hisoblashga nisbatan afzalliklari va hozirgi holati tushuntiriladi. Keyin, kriptografiyaga kvant texnologiyalarining ta’siri — ya’ni klassik shifrlash usullariga tahdidlar va kvant asosidagi himoyalash yondashuvlari — ko‘rib chiqiladi. Asosiy e’tibor: kvant kompyuterlar yordamida RSA, ECC singari algoritmlarning buzilishi ehtimoli, shuningdek, Quantum Key Distribution (QKD) va Post-Quantum Cryptography (PQC) kabi himoya mexanizmlariga qaratilgandir. Maqolaning xulosasida kvant texnologiyalarining kelajakdagi istiqbollari va raqamli xavfsizlik uchun muhim bo‘lgan strategik qarorlar muhokama qilinadi.
Kalit so‘zlar: kvant kompyuterlar, kvant kriptografiya, kvant hisoblash, superpozitsiya, entanglement, QKD, post-kvant kriptografiya, raqamli xavfsizlik, shifrlash algoritmlari.

KIRISH

So‘nggi yillarda ilm-fan va axborot texnologiyalari sohasida eng katta e’tibor tortayotgan yo‘nalishlardan biri — kvant texnologiyalari. An’anaviy kompyuter arxitekturasi asosida qurilgan tizimlar, ya’ni bitlar orqali ishlovchi klassik kompyuterlar, ma’lum chegara va chegaralanishlarga ega. Ammo kvant mexanikasi tamoyillariga tayangan holda ishlovchi kvant kompyuterlar, ya’ni qubitlar (quantum bits) asosida qurilgan tizimlar, masalalarni butunlay yangi darajada hal etish imkonini bermoqda. NIST+1 Shuningdek, ma’lumotni uzatish, shifrlash va xavfsizlikni ta’minlash sohalarida kvant mexanikasining o‘ziga xos xususiyatlari — masalan, superpozitsiya, o‘lchash effektlari, no-cloning teoremasi — yangi, ilg‘or himoya mexanizmlarini yaratishga imkon beradi. NIST+1

Ammo, kvant texnologiyalarining bu afzalliklari bilan birga, xavfsizlik sohasida katta tahdidlarni ham yuzaga keltiradi. An’anaviy shifrlash algoritmlari, ushbu kelajakdagi kvant kompyuterlar tomonidan buzilishi mumkin bo‘lgan asosiy himoya ustunliklariga tayangan. Masalan, shifrlashning asosi sifatida ishlatiladigan katta sonlarning faktorizatsiyasi yoki diskret logarifm topilishi kabi masalalar kvant algoritmlar orqali an’anaviy kompyuterlarga nisbatan arzimagan vaqt ichida yechilishi mumkin. Identity+1 Shunday ekan, kvant texnologiyalari — xavfsizlik va kriptografiya olamiga kirib borayotgan muhim omilga aylangan.

Ushbu maqolada quyidagi masalalar ko‘rib chiqiladi: birinchidan, kvant kompyuterlarning tadqiqiy holati va ishlash printsiplari; ikkinchidan, kvant kriptografiyasi tushunchasi, imkoniyatlari va cheklovlari; uchinchidan, an’anaviy kriptografiyaga kvant tahdidlarining ta’siri va himoya strategiyalari; va nihoyat, kelajak istiqbollari hamda ularni joriy qilish bilan bog‘liq muammolar. Maqolaning maqsadi — zamonaviy kvant texnologiyalarining raqamli xavfsizlikdagi rolini tushunish va bular bilan yuzaga keladigan muammolar hamda yechimlar haqida muvozanatli fikr yuritishdir.

ASOSIY QISM

1. Kvant kompyuterlar: printsiplari va taraqqiyoti

Kvant kompyuterlar — bu klassik “bit” o‘rniga “qubit” (quantum bit) deb nomlanadigan kvant holatidagi birliklar orqali ma’lumotni kodlash imkoniga ega bo‘lgan hisoblash tizimlari. Qubitlar 0 yoki 1 holatlaridan birida bo‘lishi mumkin, lekin kvant holatlarida ular bir vaqtning o‘zida 0 va 1 holatlarining superpozitsiyasida bo‘lishlari mumkin. NIST+1 Shu bilan birga, bir nechta qubitlar entanglement (kavsharlanish) holatiga kirib, bir-biriga bog‘lanadi, bu esa parallel ravishda ko‘plab holatlarni birlashtirish imkonini beradi. NIST

Masalan, agar 2 ta klassik bit bo‘lsa — bu faqat 00, 01, 10, 11 kombinatsiyalari orqali 4 holatni ifodalaydi. Ammo 2 ta qubit superpozitsiyasi ostida bir vaqtning o‘zida 00, 01, 10 va 11 holatlarini aks ettirishi mumkin, ya’ni imkoniyatlar soni eksponentsial tarzda o‘sadi. NIST Bu omil kvant kompyuterlarni muayyan hisoblash masalalarda klassik kompyuterlarga nisbatan nazariy jihatdan ustunlashtiradi.

Hozirgi paytda kvant hisoblash sohasida ilg‘or sohalar “Noisy Intermediate-Scale Quantum” (NISQ) deb atalmoqda — ya’ni qubitlar soni nisbatan ko‘p bo‘lsa ham, xatoliklar (noise) va kvant o‘zgaruvchanligi tufayli to‘liq ishonchli xatolarni to‘liq to‘liq boshqaradigan darajada emas. Википедия+1

Taraqqiyot tez sur’atda — turli kompaniyalar, ilmiy markazlar yangi qubitar, kvant chiplar, kvant algoritmlar ishlab chiqmoqda. Shu bilan birga, hali milliardlab (millionlab) qubitlarga ega bo‘lgan, barcha xatolarni to‘liq nazorat qiluvchi kvant kompyuter — ya’ni «fault-tolerant» kvant kompyuter — hali keng amaliy foydalanishga tayyor emas. NIST+1

2. Kvant kriptografiyasi: himoya mexanizmlari va imkoniyatlari

Kvant kriptografiyasi — bu ma’lumotni shifrlash, uzatish va qabul qilish jarayonida kvant mexanikasining xususiyatlaridan foydalanadigan texnologiyalar majmuasidir. NIST+1 Asosan ilmiy jihatdan ikki yo‘nalishga e’tibor beriladi:

- Quantum Key Distribution (QKD): Ikki tomon orasida xavfsiz shifrlash kalitini almashish uchun kvant holatlarida uzatiladigan fotonlar kabi zarrachalardan foydalaniladi. Agar uchinchi tomon (haker) bu zarrachalarga aralashsa, kvant mexanikasining qonunlari bo‘yicha tasir bo‘ladi va bu holat aniqlanadi. IBM+1

- Post-Quantum Cryptography (PQC): Kvant kompyuterlar kelganda ham an’anaviy (klassik) kompyuterlar ustida ishlashi mumkin bo‘lgan va kvant tahdidlarga chidamli bo‘lgan yangi shifrlash algoritmlarini ishlab chiqish va standarlashtirishga qaratilgan. Википедия+1

QKD ning ishlash printsipi: masalan, yuboruvchi fotonlarni polarisatsiya yo‘nalishida uzatadi, qabul qiluvchi esa fotonlarning holatini o‘lchaydi. Agar haker fotonlarni kuzatishga urinib, holatni o‘zgartirsa, yuboruvchi va qabul qiluvchi buni aniqlay oladi va keyingi qadamda kalitni bekor qiladi. IBM+1

Kvant kriptografiyaning afzalliklari quyidagilardan iborat:

- Bilim nuqtai nazaridan ma’lumot uzatilganda haker tomonidan “tengsiz” ko‘rinmasdan ko‘chirilishi yoki isbotlanmasdan almashilishi deyarli imkonsiz — kvant mexanikasi “o‘lchash” tamoyili orqali holatlar o‘zgarsa, bu darhol aniqlanadi. NIST
- Shuningdek, to‘liq kvant holati himoyalashga asoslanadi, ya’ni fizika qonunlari matematik taxminlarga emas, balki haqiqatga asoslanadi. IBM

Biroq, kvant kriptografiyaning ham cheklovlari mavjud. Masalan: QKD uchun maxsus foton uzatuvchi va detektor qurilmalar talab etiladi, ular yuqori aniqlik va ishonchlilik bilan ishlashi lozim. Shuningdek, uzoq masofagulamishda kvant holatlarini uzatishdagi yo‘qotishlar, kvant repeaterlar kerakligi kabi muammolar mavjud. NIST

3. Kriptografiya va kvant tahdid: an’anaviy algoritmlar oldidagi xavf

Kriptografiya sifatida keng qo‘llanilayotgan algoritmlar (masalan, RSA, Elliptic Curve Cryptography (ECC), Diffie–Hellman) matematik jihatdan murakkab masalalarga (katta sonlarni faktorizatsiya qilish, diskret logarifmani topish) asoslanadi. Ushbu masalalar klassik kompyuterlar uchun juda ko‘p vaqt talab etadi va shuning uchun shu algoritmlar hozirgacha xavfsiz deb hisoblanadi. Identity

Ammo kvant algoritmlari, xususan Shor’s algorithm va Grover’s algorithm, bu masalalarni an’anaviy usullarga nisbatan ancha tezroq yechish imkonini beradi. Masalan, Shor’s algoritmi faktorizatsiya va diskret logarifm topishni polinomial vaqt ichida qilishi mumkin, bu esa RSA va ECC kabi algoritmlarni zaiflashtiradi. F5, Inc. Grover’s algoritmi esa simmetrik shifrlash usullarini (“brute force” usuli bilan) yarmigacha tezlashtirishi mumkin, bu esa barcha simmetrik algoritmlar xavfsizligini yarmiga kamaytiradi. F5, Inc.

Shunday qilib, kelajakda kuchli kvant kompyuterlar paydo bo‘lsa, hozirgi ko‘plab himoya tizimlari zaiflashishi mumkin. Bu esa “post-kryptografik” davrni chaqiradi: ya’ni kvant kompyuterlar duch kelsa ham xavfsiz bo‘lgan yangi shifrlash usullari zarur bo‘ladi. NIST+1

4. Himoya strategiyalari va kvantga tayyorgarlik

Kvant tahdidlariga qarshi ikki asosiy yo‘l mavjud: birinchisi — kvant qonunlari asosida qurilgan himoya (masalan QKD), ikkinchisi — klassik kompyuterlar bo‘yicha ishlovchi, ammo kvantga chidamli kriptografik algoritmlar (PQC).

QKD — yuqorida ta’kidlangan — fizik jihatdan kuzatuvchan va haker aralashuvi aniqlanishi mumkin bo‘lgan kalit almashish mexanizmi. Bu ayniqsa yuqori darajadagi maxfiylik va uzoq muddatli xavfsizlik talab qilinadigan sohalarda (masalan, mudofaa, davlat sirlarini uzatish) muhim. Lekin QKD jihozlari va infratuzilmasi ko‘p mablag‘ talab qiladi hamda keng ko‘lamda tarqatilishi hali boshlang‘ich bosqichda. NIST+1

PQC esa kengroq amaliy yo‘l bo‘lib, hozirda standartlashtirilmoqda. National Institute of Standards and Technology (NIST) tomonidan post-kvant algoritmlari tanlangan va standart sifatida bosqichma-bosqich joriy etilmoqda. Википедия Bunday algoritmlar: modul-lattice asosidagi, kod-asosidagi (code-based) shifrlash usullari va boshqalar. Ular kvant kompyuterlar paydo bo‘lgan taqdirda ham himoya kafolatini berishi ko‘zlanmoqda. qtanalytics.in+1

Shuningdek, tashkilotlar uchun tayyorgarlik rejalari muhim: ma’lumotni saqlash muddati, retroaktiv buzilishi ehtimoli, “hozirgi shifrlangan ma’lumotni saqlab, kelajakda kvant kompyuter bilan ochish” xatarini hisobga olish lozim. Identity+1

5. Amaliy sohalar va muammolar

Kvant texnologiyalari himoya va tahdid jihatidan turli sohalarga ta’sir ko‘rsatmoqda. Masalan, moliya, bank, telekom, hukumat xizmatlari — bular ma’lumot xavfsizligi bo‘yicha juda sezgir bo‘lgan tarmoqlar. Kvant kompyuterlar yordamida ma’lumotlarni buzish yoki shifrlash kalitlarini olish imkoniyati paydo bo‘lsa, bu tizimlar jiddiy xavf ostida bo‘ladi. Boshqa tomondan, QKD va PQC kabi himoya texnologiyalari bu tahdidlarga javob bo‘lishi mumkin.

Biroq, amaliyotda bir qator muammolar mavjud:

- Qubitlar hali ham noz, ya’ni atrof-muhitning aralashuvi natijasida oson buziladi, bu esa xatoliklarni (decoherence) keltirib chiqaradi. Википедия+1
- QKD tizimlari uchun maxsus optik tolalar, foton detektorlari, kvant repeaterlar kerak, bu esa kosmik va masofaviy tarmoqlarda qo‘llanishni murakkablashtiradi. NIST+1
- PQC algoritmlari biroz ko‘proq manbalar (masalan kalit uzunligi, protsessor resurslari) talab qilishi mumkin, bu esa eski tizimlarga moslashtirishda muammo tug‘diradi. qtanalytics.in
- Shuningdek, sohani tartibga solish, standartlashtirish, xodimlar tayyorlash, infratuzilma modernizatsiyasi kabi strategik jihatlar ham dolzarb.

6. Kelajak istiqbollari

Kvant kompyuterlar va kvant kriptografiya istiqbollari juda keng. Kvant hisoblash muhandisligi rivojlanishi bilan birdaniga butun ilmiy-texnik masalalarni hal etish imkoniyati paydo bo‘lishi mumkin: masalan, yangi materiallar yaratish, dori dizayni, murakkab simulyatsiyalar va boshqalar. arXiv+1

Shifrlash sohasida esa, kelajakda butun axborot-kommunikatsiya tarmoqlari, IoT, bulutli xizmatlar, blokcheyn va kripto valyutalar ham kvant tahdidlariga qarshi moslashishining muhimligi ortadi. Ichki himoya mexanizmlarining kvant xavfsiz (quantum-safe) bo‘lishi ya’ni standartlashtirilgan PQC algoritmlar bilan ta’minlanishi muhim bo‘ladi.

Xulosa qilib aytganda, kvant texnologiyalari nafaqat hisoblash jihatidan inqilobni, balki butun raqamli xavfsizlik paradigmalarini qayta shakllantirish imkoniyatini beradi.

XULOSA

Ushbu maqolada biz zamonaviy kvant texnologiyalarining – xususan, kvant kompyuterlar va kvant kriptografiyasining – asosiy tushunchalari, imkoniyatlari, xavflari va himoya yo‘llari bilan tanishdik. Kvant kompyuterlar superpozitsiya va entanglement tamoyillari orqali eksponentsial hisoblash quvvatiga ega bo‘lishi mumkin. Shu bilan birga, ular an’anaviy kriptografiya uchun tahdid yaratmoqda, chunki RSA, ECC kabi algoritmlarni buzish ehtimoli mavjud. Boshqa tomondan, kvant kriptografiyasi — QKD kabi kvant mexanikasiga asoslangan usullar va PQC kabi kvant tahdidlarga tayyorlangan algoritmlar — yangi himoya istiqbollarini ochmoqda.

Amalga tatbiq qilish tarafida — infratuzilma, standartlashtirish, xavfsizlik siyosati, ilm-fanni texnologiyaga aylantirish bo‘yicha qator masalalar mavjud. Kelajakda raqamli xavfsizlikni ta’minlash uchun har bir tashkilot, davlat va kompaniya kvantga tayyorgarlik ko‘rishi muhimdir. Ayniqsa, uzoq muddatli saqlanishi lozim bo‘lgan ma’lumotlar, yuqori himoya talab qiladigan tizimlar kvant tahdidlarini inobatga olgan holda strategiyalarni ishlab chiqishlari zarur.

Shunday ekan, kvant texnologiyalari faqat ilmiy meros bo‘lib qolmay, balki yaqin kelajakda xavfsizlik, kommunikatsiya, axborot texnologiyalari sohalarini tubdan o‘zgartirishi mumkin. Biz bu o‘zgarishga bugundan tayyor bo‘lishimiz muhim.

FOYDALANILGAN ADABIYOTLAR RO’YXATI

1. Nielsen, M. A., & Chuang, I. L. (2010). *Quantum Computation and Quantum Information.* 10th Anniversary Edition. Cambridge University Press.
2. Preskill, J. (2018). “Quantum Computing in the NISQ era and beyond.” *Quantum*, 2(79), 1–20. DOI: 10.22331/q-2018-08-06-79.
3. National Institute of Standards and Technology (NIST). (2023). *Post-Quantum Cryptography Standardization Project.* https://csrc.nist.gov/projects/post-quantum-cryptography
4. IBM Quantum. (2024). *What is Quantum Cryptography?* IBM Knowledge Center. https://www.ibm.com/topics/quantum-cryptography
5. NIST Quantum Information Science. (2024). *Quantum Computing Explained.* https://www.nist.gov/quantum-information-science/quantum-computing-explained
6. F5 Labs. (2023). *Quantum Computing and the Future of Encryption.* https://www.f5.com/labs/articles/what-is-quantum-computing