OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI,

MIRZO ULUG`BEK NOMIDAGI

O`ZBEKISTON MILLIY UNIVERSITETI

FIZIKA FAKULTETI

F – 2203 GURUH TALABASI

YULDASHEVA O`G`ILOYNING

ATOM FIZIKASI FANIDAN

MUSTAQIL ISHI

MAVZU:*KVANT SHIFRLASH*

BAJARDI:

QABUL QILDI:

TOSHKENT – 2024

REJA:

Kvant mexanikasi

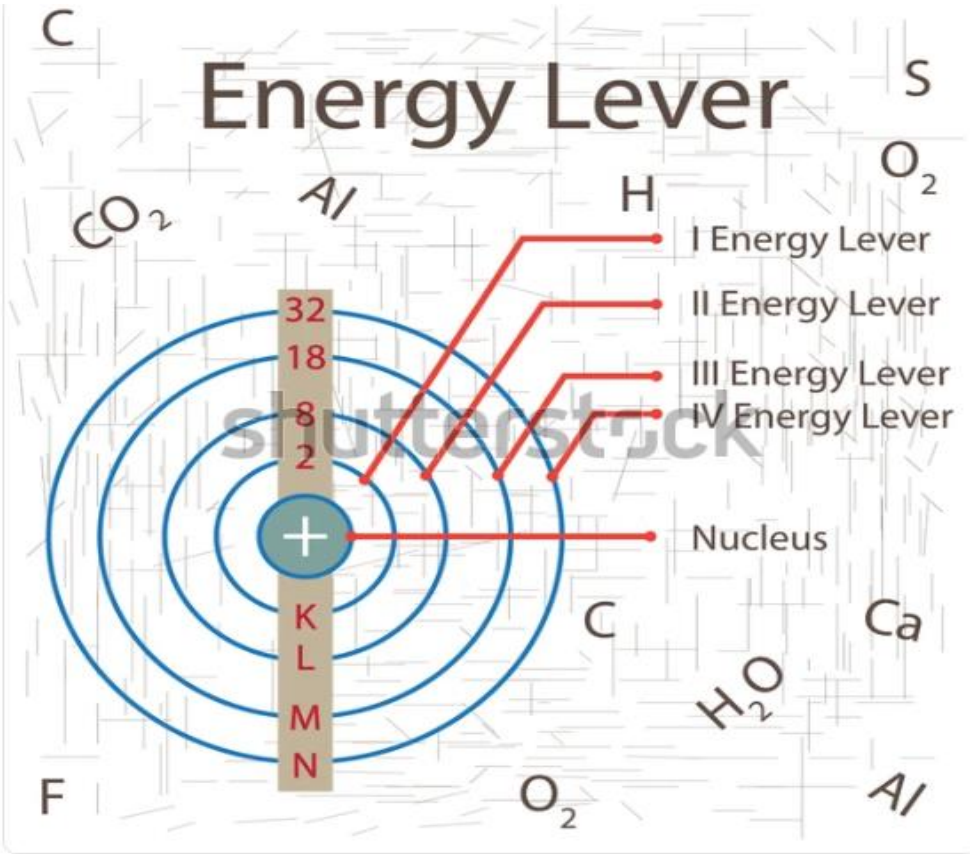
Kvant mexanikasi — bu tabiatdagi mikroskopik tizimlarni, masalan, atomlar va elementar zarralarni tushuntirish uchun yaratilgan nazariya. Klassik fizika bilan solishtirganda, kvant mexanikasi juda kichik masshtabdagi hodisalarni o'rganadi va klassik fizikaning ba'zan to'g'ri ishlamay qoladigan joylarini izohlashga yordam beradi. Ushbu nazariya 20-asrning boshida bir qator muhim olimlar, jumladan Nils Bor, Verner Geyzenberg, Ervin Shrödinger va boshqalar tomonidan ishlab chiqilgan.

Kvant mexanikasi bir necha fundamental tamoyillar asosida quriladi. Ulardan biri "to'lqin-zarra dualizmi" bo'lib, u zarralarning bir vaqtning o'zida to'lqin va zarra tabiatiga ega ekanligini ko'rsatadi. Masalan, elektronlar, fotonlar va boshqa elementar zarralar ma'lum sharoitlarda to'lqin kabi xatti-harakat qiladi, boshqa holatlarda esa zarra sifatida namoyon bo'ladi. Bu tamoyilning muhim bir tajribasi — ikki yoriqli tajriba hisoblanadi, bu yerda individual zarralar ham interferensiya naqshlarini hosil qiladi. Boshqa bir tamoyil — "noaniqlik printsipi", bu Geyzenberg tomonidan taklif qilingan. Bu printsipga ko'ra, zarraning pozitsiyasi va impulsi bir vaqtda aniq o'lchangan paytda yuzaga keladigan noaniqlik mavjuddir. Masalan, elektronning pozitsiyasini va impulsini juda aniqlik bilan o'lchash imkonsiz.

1 - rasm.

Kvant mexanikasida "kvant holati" tushunchasi ham muhimdir. Kvant holati biror tizimning barcha mumkin bo'lgan axborotini o'z ichiga oladi va odatda to'lqin funksiyasi yordamida tavsiflanadi. To'lqin funksiyasi ψ bilan belgilanadi va u kvadrat orqali zarraning ma'lum joyda topilish ehtimolini beradi.

Kvant mexanikasida ko'pincha "energiya sathlari" tushunchasi ishlatiladi. Atomlardagi elektronlar faqat diskret energiya sathlarida mavjud bo'lishi mumkin. Bular kvantlashtirilgan energiya sathlari bo'lib, elektron bir energiya sathidan boshqasiga sakrashi bilan o'zgarishi mumkin. Bu hodisa chiroqning yorug'lilik spektrida chiziqli spektrlarni hosil qiladi. Kvant mexanikasi ko'pgina matematik asboblardan foydalanadi, jumladan operatorlar va matritsalar. Operatorlar orqali fizik kattaliklarning, masalan, moment yoki energiyaning, o'lchovi kvant mexanikasida ifodalanadi.



2 - rasm.

Bu nazariya, shuningdek, bir nechta kuchli dalillarga ega. Kvant mexanikasi asosida ishlangan kvant elektrodinamikasi, kvant xromodinamikasi kabi nazariyalar

bir qator tajribiy natijalarni, jumladan elektronning anomal magnit momenti yoki koinotdagi neytron yarmshinji, aniqlik bilan ko'rsatib bergan. Kvant mexanikasining amaliy qo'llanilmalari juda keng. Masalan, yarimo'tkazgichlarning ishlash prinsipi kvant mexanikasiga asoslangan, bu esa zamonaviy elektron qurilmalarning (kompyuterlar, smartfonlar va boshqalar) yaratilishida asosiy rol o'ynaydi. Shuningdek, lazer texnologiyalari, MRI skanerlari va hatto kvant hisoblash ham kvant mexanikasi tamoyillaridan foydalanadi.

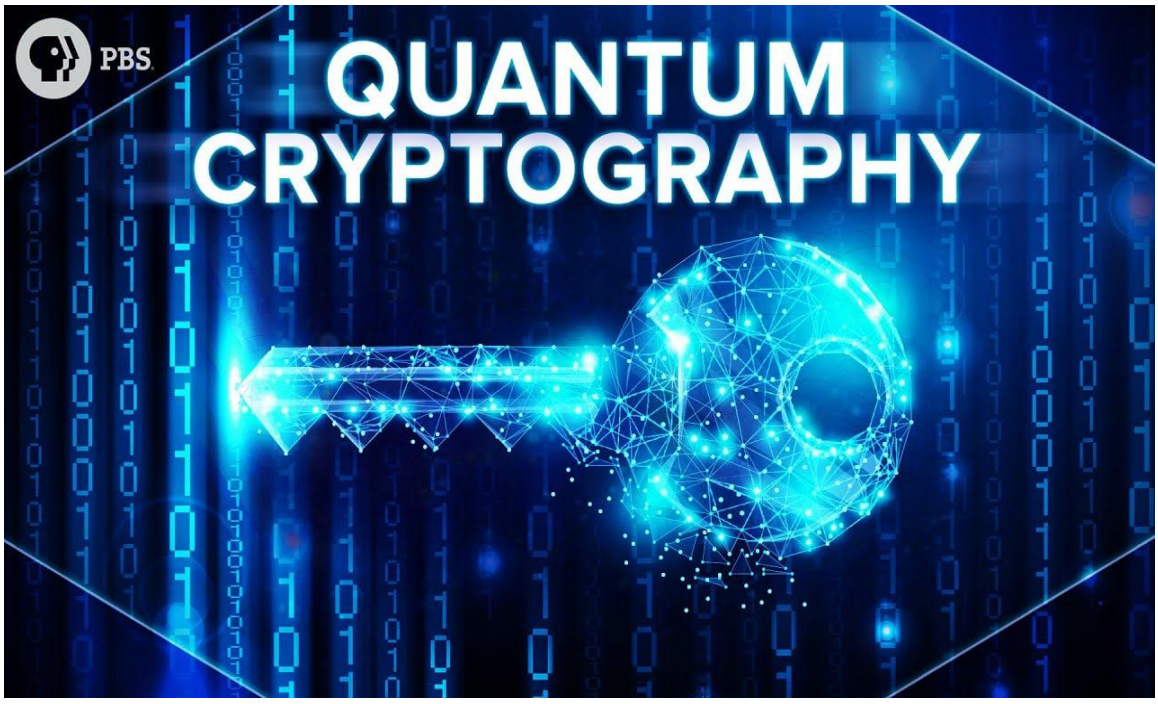
Kvant kriptografiyasi

Kvant kriptografiyasi kriptografik vazifalarni bajarish uchun kvant mexanik kvant mexanik xususiyatlardan foydalanish haqidagi fandir. Kvant kriptografiyasining eng mashhur namunasi kvant kalitlarini taqsimlash bo`lib, u kalit almashinuvi muommosiga axborot nazariy jihatidan xavfsiz yechim taklif qiladi. Kvant kriptografiyasining afzalligi shundaki, u faqat klassik (kvant bo`lmagan) aloqa yordamida isbotlangan yoki imkonsiz deb taxmin qilingan turli kriptografik vazifalarni bajarishga imkon beradi. Misol uchun, kvant holatida kodlangan ma’lumotlarni nusxalash mumkin emas. Agar kodlantgan ma’lumotni o`qishga harakat qilinsa, kvant holati to`lqin funksiyasi qulashi tufayli o`zgaradi. Bu kvant kalitlarini taqsimlashda ishlatilishi mumkin.

Kvant kriptografiyasi tarixi haqida: 1970 - yillarning boshida Nyu - Yorkdagi Kolumbiya universitetida Stiven Visner kvant konjugat kodlash tushunchasini kiritdi. Uning “Konjugat kodlash” nomli ilmiy maqolasi IEEE Axborot nazariyasi jamiyati tomonidan rad etilgan, ammo oxir oqibat 1983 - yilda SIGACT news jurnalida nashr etilgan. Ushbu maqolada ular ikkita "konjugat kuzatiladigan"da kodlash orqali ikkita xabarni qanday saqlash yoki uzatishni

ko'rsatdi, masalan, fotonlarning chiziqli va aylana qutblanishi, shuning uchun ikkala xususiyat ham qabul qilinishi va dekodlanishi mumkin.

Kvant kriptografiyasi - bu kvant mexanikasi qonunlaridan foydalanib, informatsiyani xavfsiz uzatish va himoya qilish usullarini o'rganadigan soha. An'anaviy kriptografiya matematik belgilar va algoritmlarga asoslangan bo'lsa, kvant kriptografiyasi kvant zarralarining fizik xususiyatlaridan foydalanadi. Bu texnologiya, ayniqsa, qudratli kompyuterlar bilan bozulishi mumkin bo'lgan an'anaviy kriptografiya usullarining xavfsizligini oshirish uchun muhimdir. Kvant kriptografiyasining asosiy elementi - kvant kalit taqsimoti (QKD, Quantum Key Distribution). QKD ga asoslangan tizimlar kvant mexanikasi tamoyillarini qo'llab, kalitlarni ishonchli tarzda ikki tomonlama uzatadi.



https://youtu.be/pi7YwxxZQ5A?si=bZh4tw1rlpFtHA8x **3 - rasm.**

Bu nuqtai nazardan BB84 protokoli eng keng tarqalganlardan biridir. BB84 protokoli 1984 yilda Charls Bennet va Jil Brassard tomonidan taklif qilingan. Ushbu

protokol orqali ikkita tomon (odatda "Alice" va "Bob" deb ataladi) fotonlar orqali kalitlarni uzatadi.

Kvant kriptografiyasining diqqatga sazovor xususiyati - kvant o'lchashning o'zaro bog'liqlik xususiyati. Yani, kvant zarralarning holati o'lchanganda o'zgaradi, bu esa har qanday qo'zg'alish yoki tinglash harakatlarini sezish imkonini beradi. Masalan, agar uchinchi tomon (yoki "Eve") uzatilayotgan kalitni o'qishga harakat qilsa, u kvant holatlarini o'zgartiradi va bu o'zgarish Alice va Bob tomonidan sezilishi mumkin. Shunday qilib, tinglash urinishlari aniqlanadi va Alice va Bob yangi kalit yaratish qarorini qabul qilishi mumkin.

So'nggi yillarda kvant kriptografiyasining amaliy dasturlarida sezilarli yutuqlar kuzatildi. Xitoy 2016 yilda Shijian-19 deb nomlangan birinchi kvant sun’iy yo‘ldoshini orbitaga chiqarib, kvant kriptografiyasi sohasida katta qadam tashladi. Shuningdek, turli davlatlar va tadqiqot markazlari quruqlikdagi optik tolalar orqali kvant kriptografiyani amalga oshirishda imkoniyatlarni o'rganmoqda. Shu kabi loyihalarda dastlabki sinovlarda 100 km dan oshiq masofalarda ishonchli kalittaqsimotiamalgaoshirildi.

4 - rasm.

QKD texnologiyasining yirik yutuqlari orasida Xitoyning Micius sun'iy yo'ldoshi orqali amalga oshirilgan dunyo miqyosidagi birinchi kvant kriptografiya birikmasi mavjud, bu esa ikki qit'a orasidagi masofaviy aloqalarning xavfsizligini oshirishga imkon berdi. 2017 yilda Micius sun'iy yo'ldoshi orqali Xitoy va Avstriya orasida kvant xabarlar almashinuvi ilk bor amalga oshirildi.

Kvant kriptografiyada foydalanilayotgan texnologiyalar orasida kvant to'lqinlarni qayd etish, kvant hukm chiqarish (bell inequalities) va kvant entanglement (bir-biriga bog'liq kvant holatlar) kabi murakkab temalar mavjud. Kvant hukm chiqarish orqali malum bo'lmagan harakatlar aniqlanishi va kvant kanallari orqali uzatilayotgan ma'lumotlarni diqqat bilan kuzatish mumkin. Ushbu texnologiya hali yosh bo’lsa-da, kelajakda an'anaviy kriptografiyaga kuchli muqobil bo'lishi ehtimoli yuqori.

Kvant kriptografiyasining kelajakdagi imkoniyatlari va qo'llanish doirasi katta qiziqish uyg'otmoqda, ayniqsa, kvant kompyuterlarining rivojlanishi bilan birga. Kvant kompyuterlar an'anaviy kompyuterlarga nisbatan ancha kattaroq hisoblash quvvatiga ega bo'lib, mavjud kriptografik algoritmlarni buzish imkoniyatiga ega bo'lishi mumkin. Shu sababli, kvant kriptografiyasi raqamli ma’lumotlarni himoya qilish va xavfsizlikni ta’minlashda yangi standartlarni belgilashda muhim rol o'ynaydi.

Afzalliklari: Kriptografiya ma’lumotlar xavfsizligi zanjirining eng kuchli bo`g`inidir. Biroq manfaatdor tomonlar kriptografik kalitlar abadiy xavfsiz b`lib qoladi deb taxmin qila olmaydi. Kvant kriptografiyasi klassik kriptografiyaga qaraganda ma’lumotlarni uzoqroq vaqt davomida shifrlash imkonini beradi. Klassik kriptografiyadan foydalangan holda, olimlar taxminan 30 yildan ortiq shifrlashni kafolatlay olmaydilar, ammo ba'zi manfaatdor tomonlar uzoqroq himoya davrlaridan foydalanishlari mumkin. Misol uchun, sog'liqni saqlash sohasini olaylik 2017 yilga kelib, ofisdagi shifokorlarning 85,9% bemor ma'lumotlarini saqlash va uzatish uchun elektron tibbiy yozuvlar tizimlaridan foydalanmoqda. Tibbiy sug'urta portativligi va hisobdorligi to'g'risidagi qonunga binoan tibbiy yozuvlar sir

saqlanishi kerak. Kvant kalitlarini taqsimlash elektron yozuvlarini 100 yilgacha himoya qilish mumkin. Shuningdek, kvant kriptografiyasi hukumatlar va harbiylar uchun foydali dasturlarga ega, chunki tarixiy jihatdan hukumatlar 60 yildan ortiq vaqt davomida harbiy ma'lumotlarni sir saqlashgan. Bundan tashqari, kvant kalitlarini taqsimlash shovqinli kanal orqali uzoq masofaga o'tishi va xavfsiz bo'lishi mumkinligi haqida dalillar mavjud. Uni shovqinli kvant sxemasidan klassik shovqinsiz sxemaga kamaytirish mumkin. Buni klassik ehtimollik nazariyasi bilan hal qilish mumkin. Shovqinli kanal orqali izchil himoyaga ega bo'lish jarayoni kvant takrorlagichlarini amalga oshirish orqali mumkin. Kvant takrorlagichlari kvant aloqa xatolarini samarali tarzda hal qilish qobiliyatiga ega. Kvant kompyuterlari bo'lgan kvant takrorlagichlari aloqa xavfsizligini ta'minlash uchun shovqinli kanal ustida segment sifatida joylashtirilishi mumkin. Kvant takrorlagichlari buni xavfsiz aloqa liniyasini yaratishdan oldin kanal segmentlarini tozalash orqali amalga oshiradilar. Sub-par kvant takrorlagichlari shovqinli kanal orqali uzoq masofadan samarali xavfsizlikni ta'minlashi mumkin.

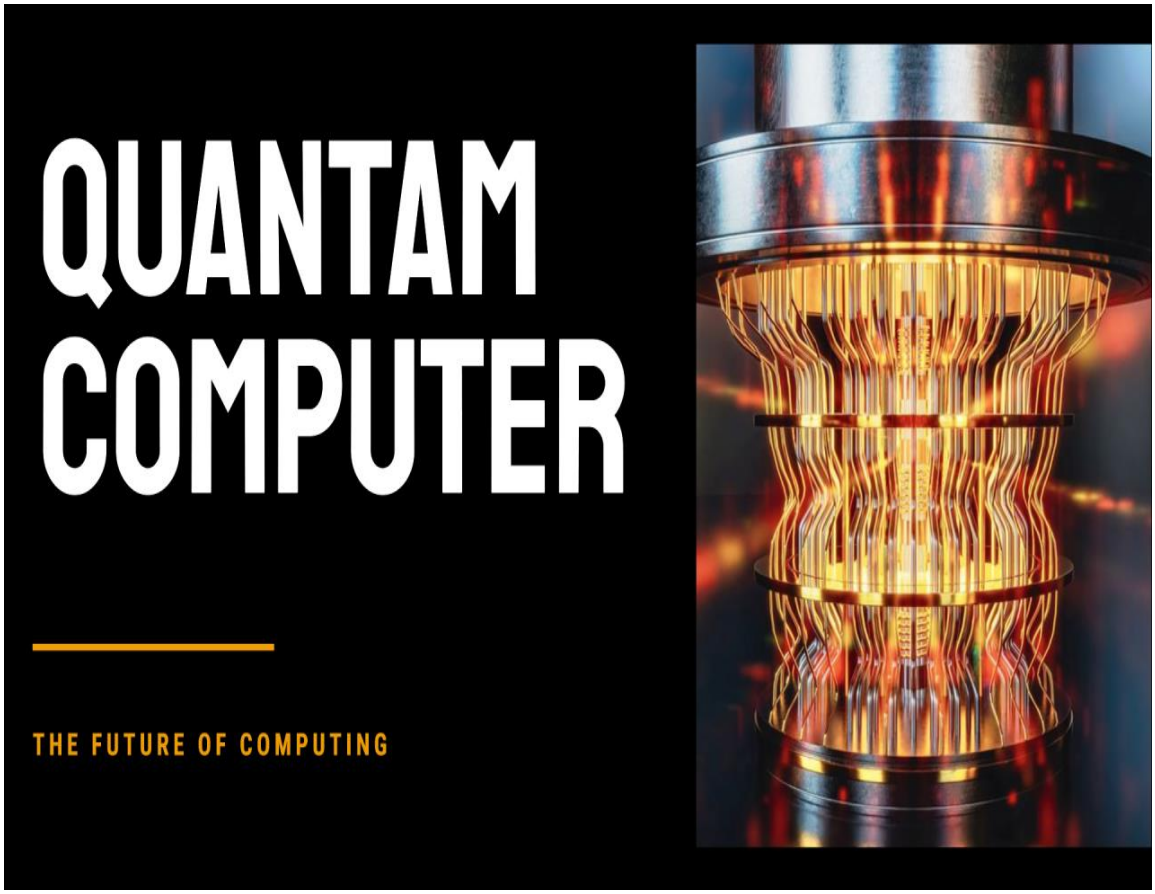
Kvant kompyuterlari.

Kvant kompyuterlari hozirgi kunda ilmiy jamoatchilik va texnologiya sohasidagi eng muhim mavzulardan biri hisoblanadi. Ushbu kompyuterlar kvant fizikasi prinsiplari asosida ishlaydi va an'anaviy hisoblash uskunalaridan farqli o'laroq, ma'lumotlarni qayta ishlashda juda katta imkoniyatlarga ega.

Kvant kompyuterlarining asosiy elementi kvant biti yoki qubit deb ataladi. Qubitlar klassik kompyuterlarning bitlaridan farqli o'laroq, kvant holatida bir vaqtning o'zida 0 va 1 holatlarda bo'la oladi. Bu xususiyat superpozitsiya deb ataladi va shu xususiyat orqali kvant kompyuterlar murakkab hisoblashlarni juda tez bajarishi mumkin.

Kvant kompyuterlarining ishlash tamoyili kvant dola jismida yotadi, bu holat qubitlar bir-biriga bog'langan va ular orasida ma'lumotlar almashinuvi sodir bo'ladigan jarayon. Entanglement yoki dola o'zaro tasirlanishlar qubitlarni ular

orasidagi masofadan qat'i nazar bog'laydi, bu esa juda katta hisoblash quvvatini ta'minlaydi.



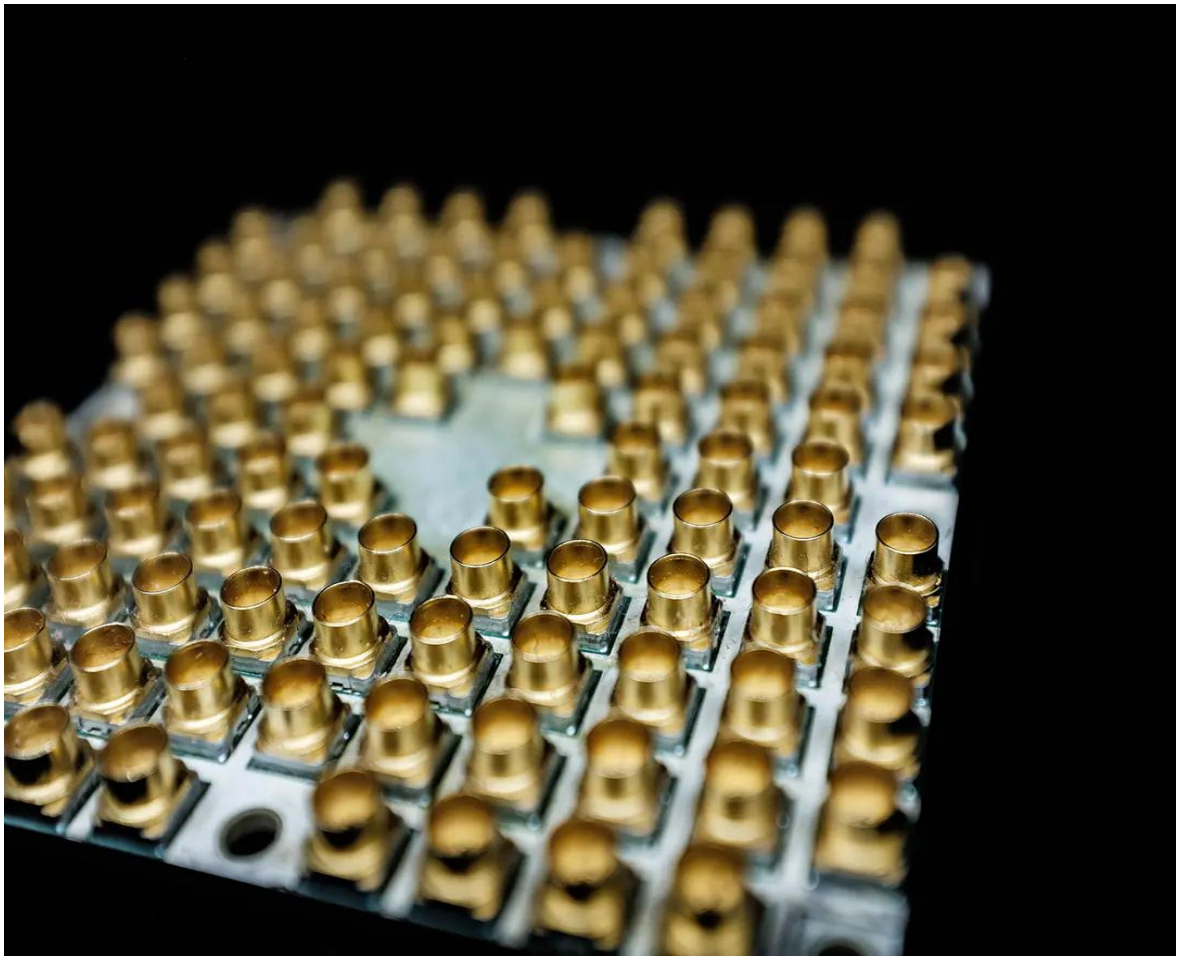
5 - rasm.

Kvant kompyuterlarining amaliy imkoniyatlari keng. Ular kriptografiya, molekulyar modelirovka, ma'lumotlarni tuzish va mashinalarni o'rganish sohalarida katta nazariy va amaliy yutuqlarga erishishi mumkin. Misol uchun, 256 bitlik kriptografik kalitni sindirish uchun hozirgi klassik kompyuter minglab yillar talab qilsa, kvant kompyuteri bu vazifani bir necha daqiqada bajarishi mumkin.

An'anaviy bitlarni turi qatorida kvant bitlari bir vaqtning o'zida bir nechta holatlarni qamrab oladi, shuning uchun kvant kompyuterlari murakkab algoritmlarni bajarishda juda samarali. Shor algoritmi va Grover qidiruv algoritmi – bu ikki misol, kvant kompyuterlari uchun mo'ljallangan maxsus algoritmlar bo'lib, ularning samaradorligi klassik algoritmlarnikidan ancha yuqori.

Google va IBM kabi kompaniyalar kvant kompyuterlar sohasida yirik tadqiqotlar o‘tkazmoqda. Google 2019 yilda Sycamore nomli 53 qubitli kvant proyektorining kvant ustunligiga erishganini e'lon qildi. Bu demakdirki, ushbu kompyuter tasdiqlangan kvant algoritmini bajarishda har qanday superkompyuterdan tez ishladi.

IBM esa o‘zining IBM Quantum Experience platformasi orqali foydalanuvchilarga kvant hisoblash imkoniyatlarini onlayn ravishda sinab ko‘rish imkoniyatini taqdim etmoqda. Ushbu platformada 5 dan 65 qubitgacha bo'lgan kvant proyektorlari mavjud. IBMning maqsadi 2023 yilga kelib 1000 dan ortiq qubitlarga ega kvant kompyuter qurishni amalga oshirishdir.



6 - rasm.

Kvant kompyuterlarining rivojlanishida yana bir muhim faktor - kvant himoyalashdir. Kvant himoyalash kvant kompyuterlarining muhitdagi shovqinlar va

kvant xatolarini tuzatish imkoniyatlarini oshiradi. Bunga erishish uchun topologik kvant bit va yuz berishi kutilmagan xatolarni aniqlash va tuzatish bo'yicha ilg'or tadqiqotlar olib borilmoqda. Kvant kompyuterlarining bozor narxi hozircha juda yuqori. D-Wave kompaniyasining tijorat kvant kompyuteri 2023 yilda taxminan 15 million AQSh dollari atrofida narxlandi. Ushbu narx kelajakda arzonlashishi kutilmoqda, chunki texnologiya rivojlanib borishi bilan ishlab chiqarish jarayoni optimallashtiriladi.

XULOSA.

Xulosa qilib aytganda, kvant mexanikasi bizning tabiat haqidagi bilimlarimizni keskin o'zgartirgan fundamental nazariyadir. U kichik zarralar dunyosida sodir bo'ladigan murakkab va noaniq hodisalarni tushuntirishda juda qimmatli. Kvant mexanikasi ham nazariy, ham amaliy aspektlarda muhim yutuqlarga olib kelgan va ilm-fan va texnologiyaning turli sohalariga kirib borgan. Shu bilan birga, kvant kriptografiyasi potensial ravishda juda muhim ahamiyatga ega, ayniqsa, yuqori darjadagi xavfsizlik talab qilinadigan sihalarda. Kvant kompyuterlari ham kelajak texnologiyasi bo'lishi kutilmoqda va ularning rivojlanishi ko'plab sohalar uchun muhim o'zgarishlar kiritishi mumkin. Shu boisdan, kvant hisoblash sohasidagi izlanishlar va sarmoyalar yil sayin oshib bormoqda.

Foydalanilgan adabiyotlar.

1. Kvant mexanikasi:Universitetlar va pedagogika institutlari uchun darslik/ M.M.Musaxanov, A.S.Rahmatov; O`zR oliy va o`tra - maxsus ta’lim vazirligi. - T.Tafakkur bo`stoni, 2011 - 352 b.

2. https://en.wikipedia.org/wiki/Quantum_cryptography

3. https://www.innovationnewsnetwork.com/cisa-how-post-quantum-cryptography-safeguards-against-quantum-threats/54045/