ISSN: 3030-3346

KVANT KOMPYUTERLARI VA ULARNING IMKONIYATLARI

Mustafoyev Azamat Botir o‘g‘li

‘‘UNICON.UZ” MChJ

K E Y W O R D S

Kvant kompyuterlari, Shor va Grover algoritmlari, postkvant kriptografiya

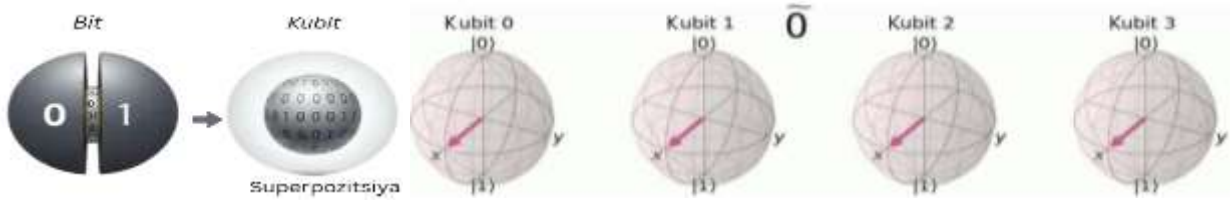
A B S T R A C T

Ushbu maqolada kvant hisoblashning asosiy tushunchalari va ishlash tamoyillari bayon etilgan. Kvant kompyuterlarning klassik kompyuterlardan farqi hamda Shor va Grover algoritmlarining kriptografiyaga ta’siri tahlil qilingan. Shuningdek, kvant xatoliklarni tuzatish usullari va postkvant kriptografiyaning dolzarbligi yoritilgan.

Kirish. Kvant texnalogiyasi axborot texnologiyalarining jadal rivojlanishi, hisoblash tizimlarining imkoniyatlariga bo‘lgan talabni keskin oshirmoqda. Klassik kompyuterlar uzoq yillar davomida ilm-fan va sanoatning turli sohalarida muhim o‘rin egallab kelgan bo‘lsa-da, murakkab matematik masalalar, katta hajmdagi ma’lumotlarni tahlil qilish va yuqori darajadagi axborot xavfsizligini ta’minlash kabi vazifalarda ularning imkoniyatlari tobora cheklanib bormoqda [1]. Shu sharoitda kvant mexanikasi qonunlariga asoslangan kvant hisoblash texnologiyalari istiqbolli yechim sifatida ommaga keng tarqalmoqda.

Kvant kompyuterlar klassik hisoblash modellaridan tubdan farq qilib, axborotni kubitlar orqali qayta ishlaydi hamda superpozitsiya va chigallik kabi kvant hodisalaridan foydalanadi. Bu esa ayrim hisoblash masalalarini, xususan, katta sonlarni faktorizatsiya qilish, optimallashtirish va murakkab tizimlarni modellashtirish jarayonlarini ancha samarali bajarish imkonini beradi [2]. Ayniqsa, Shor va Grover algoritmlarining ishlab chiqilishi kvant kompyuterlarning nazariy ustunligini amalda namoyon etib, zamonaviy kriptografik tizimlarning barqarorligiga jiddiy ta’sir ko‘rsatdi. Bugungi kunda kvant kompyuterlarining rivojlanishi axborot xavfsizligi sohasida muhim muammolarni yuzaga keltirmoqda. Mavjud ochiq kalitli kriptografik algoritmlar kvant hisoblashlar qarshisida zaif bo‘lib qolishi mumkin. Shu sababli, kvant kompyuterlarining ishlash prinsiplarini chuqur o‘rganish, ularning imkoniyatlari va cheklovlarini tahlil qilish hamda postkvant kriptografik yechimlarni ishlab chiqish dolzarb ilmiy masalalardan biri hisoblanadi. Ushbu maqola aynan shu masalalarni yoritishga bag‘ishlangan.

Kvant kompyuterlarining asosiy tushunchalari: Klassik kompyuterlar ma’lumotlarni ikkilik tizimda, ya’ni 0 va 1 bitlari shaklida qayta ishlaydi. Kvant kompyuterlari esa kvant bitlari yoki “kubitlar” asosida ishlaydi, ular kvant mexanikasining superpozitsiya va chigallik (entanglement) xususiyatlaridan foydalanadi [10].

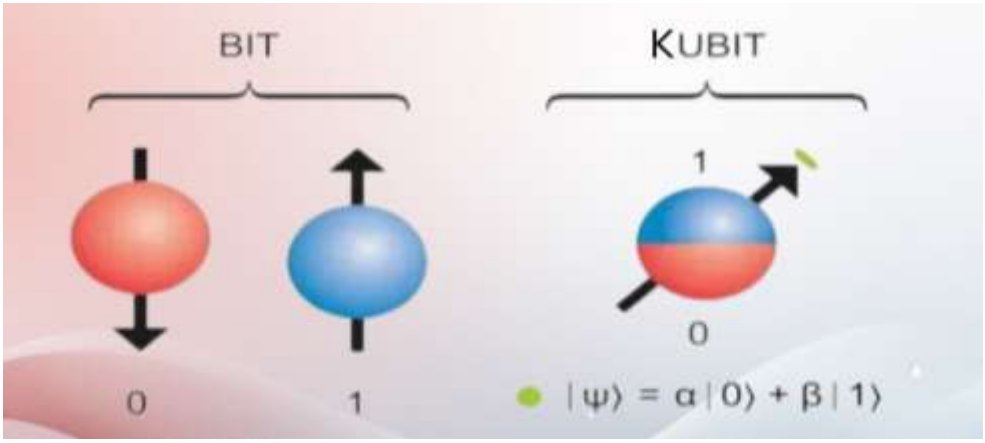


1-rasm Kubitlarning holatlari va superpozitsiya tasviri

Kubit klassik bitdan farqli o‘laroq, nafaqat 0 yoki 1 holatida, balki ularning superpozitsiyasida, ya’ni ($|\gamma\rangle=\alpha|0\rangle+\beta|1\rangle$) shaklida bo‘lishi mumkin [3], bu yerda (alpha) va (beta) kompleks sonlar bo‘lib, ularning kvadratlari yig‘indisi 1 ga teng (($|\alpha|^2 + |\beta|^2 = 1$)) [1]. Superpozitsiya kubitning bir vaqtning o‘zida bir nechta holatlarni ifodalash imkonini beradi, bu esa kvant kompyuterlarining parallel hisoblash qobiliyatini oshiradi. Chigallik esa ikki yoki undan ortiq kubitlarning o‘zaro

© *Mustafoyev Azamat Botir o‘g‘li*

bog'langan holati bo'lib, bir kubitning holati boshqasining holatiga bevosita ta'sir qiladi, hatto ular jismoniy jihatdan bir-biridan uzoqda bo'lsa ham.



2-rasm Kubit holatining matematik ifodasi bilan taqqoslanishi

Bu nima degani *?* Aytaylik, oddiy kompyuter - bu 100 ta kalitdan iborat bog'lamda kerakli kalitni qidirayotgan odam sifatida qaraylik. U bir kalitni olib sinab ko'radi, mos kelmaydi - keyingisini oladi va hokazo, to keraklisini topmaguncha bu jarayon davom etadi. Ushbu xususiyat kvant kompyuterlariga murakkab hisob-kitoblarni samaraliroq amalga oshirish imkonini beradi. Bundan tashqari, kvant kompyuterlari kvant darvozalari (quantum gates) yordamida ma'lumotlarni qayta ishlaydi, bu klassik kompyuterlardagi mantiqiy darvozalarga o'xshash, lekin kvant mexanikasining qonunlariga asoslanadi .

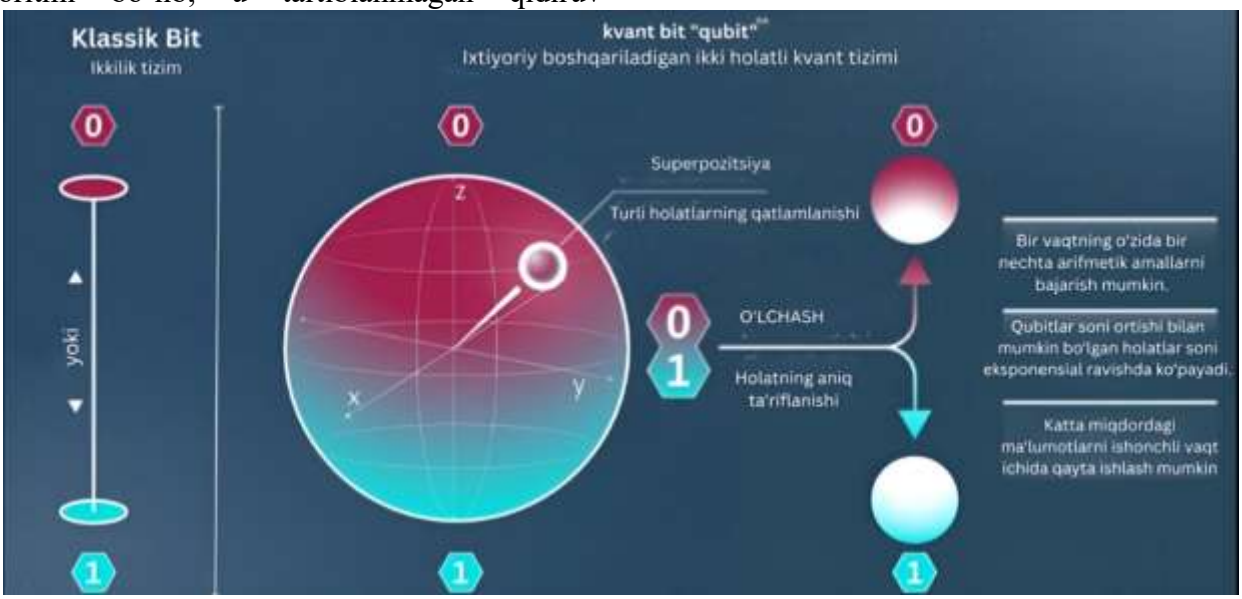
- ***Kvant kompyuterlarining rivojlanish tarixi va hozirgi holati:*** Kvant kompyuterlari nazariyasining shakllanishi XX asr boshlaridagi bir nechta fundamental ilmiy kashfiyotlarga tayanadi. Ushbu yutuqlarni yaratgan olimlar keyinchalik Nobel mukofoti bilan taqdirlangan. Ulardan biri - nemis nazariyotchi olimi Maks Plank bo'lib, u kvant fizikasi asoschisi sifatida tan olingan. U 1918-yilda "kvant" - elementar zarracha tushunchasini ilmiy muomalaga kiritgan. Kvant kompyuterlari g'oyasi dastlab 1980-yillarda Richard Feynman va David Deutsch kabi fiziklar tomonidan taklif qilingan. Feynman kvant tizimlarini simulyatsiya qilish uchun kvant hisoblash mashinalarining zarurligini ta'kidlagan bo'lsa, Deutsch kvant kompyuterlarining klassik kompyuterlarga nisbatan afzalliklarini ko'rsatuvchi nazariy asoslar ishlab chiqqan. 1994-yilda Peter Shor tomonidan ishlab chiqilgan Shor algoritmi kvant kompyuterlarining katta sonlarni faktorizatsiya qilish va diskret logarifm muammolarini polinomial vaqt ichida yechish qobiliyatini ko'rsatdi [3], bu esa kriptografiya sohasida inqilobiy o'zgarishlarga olib keldi. Hozirgi kunda kvant kompyuterlari sohasida sezilarli yutuqlarga erishilmoqda. IBM, Google, Microsoft va D-Wave kabi kompaniyalar kvant kompyuterlarini ishlab chiqishda faol ishtirok etmoqda. Masalan, 2019-yilda Google o'zining "Sycamore" kvant protsessori yordamida "kvant ustunligi" (quantum supremacy) ga erishganini e'lon qildi, ya'ni kvant kompyuteri klassik superkompyuterlar yecholmaydigan muammoni qisqa vaqt ichida yechdi. Biroq, bu yutuqlar hali ham sinov bosqichida bo'lib, keng ko'lamli, barqaror va xatolarga chidamli kvant kompyuterlarni yaratish yo'lida ko'plab muammolar mavjud, masalan, kubitlarning barqarorligini ta'minlash va kvant xatolarini tuzatish.

- ***Kvant kompyuterlarining ishlash prinsiplari***. Kvant kompyuterlarining ishlash prinsipi kvant mexanikasining asosiy qonunlariga, xususan, superpozitsiya, chigallik va kvant o'lchovi (measurement) tamoyillariga asoslanadi. Kvant hisoblash jarayonida dastlab kubitlar ma'lum bir boshlang'ich holatga keltiriladi, so'ngra kvant darvozalar yordamida kerakli hisoblash operatsiyalari amalga oshiriladi. Nihoyat, natija o'lchov orqali aniqlanadi, bu jarayonda kvant holati klassik holatga "yemiriladi" (collapses). Kvant kompyuterlarining asosiy afzalligi ularning parallel hisoblash qobiliyatidadir. Masalan, (n) kubitli tizim bir vaqtning o'zida ($2^{\square}$) holatni ifodalay oladi, bu esa

© Mustafoyev Azamat Botir o'g'li

kvant kompyuterlariga muayyan muammolarni eksponensial darajada tez yechish imkonini beradi [1]. Biroq, bu afzallik faqat ma’lum turdagi muammolar uchun amal qiladi, masalan, Shor algoritmi yoki Grover algoritmi kabi kvant algoritmlari uchun.

- ***Kvant algoritmlari.*** Kvant algoritmlari kvant mexanikasining asosiy tamoyillariga tayangan holda ishlaydi va ayrim masalalarni oddiy (klassik) algoritmlarga qaraganda ancha tez yecha oladi. Eng mashhur kvant algoritmlaridan biri Shor algoritmi bo‘lib, u katta sonlarni omillarga ajratishda juda yuqori tezlikni ta’minlaydi. Yana bir muhim algoritm - Grover algoritmi bo‘lib, u tartiblanmagan qidiruv masalalarini yechishda klassik usullarga nisbatan tezroq natija beradi. Kvant kompyuterlar ma’lumotni kubitlar yordamida qayta ishlaydi. Kubitlar bir vaqtning o‘zida bir nechta holatda bo‘la olgani sababli, hisoblashlar parallel tarzda bajariladi. Kvant algoritmlarining samaradorligi asosan kubitlar soni va ularning barqaror ishlash vaqtiga bog‘liq. Kvant algoritmlar kriptografiya, optimallashtirish va murakkab tizimlarni modellashtirish kabi sohalarda katta imkoniyatlarga ega. Shu bilan birga, kvant xatoliklarni tuzatish va tashqi shovqinlarni kamaytirish ustida olib borilayotgan tadqiqotlar kvant kompyuterlarning amaliy qo‘llanilishi uchun juda muhimdir.



1-rasm Klassik bit va kvant bit (qubit) taqqoslanishi

- ***Kvant xatoliklarni tuzatish (QEC) Quantum Error Correction*** kvant kompyuterlarning ishonchli ishlashi uchun juda muhim hisoblanadi. Kvant ma’lumotlar tashqi shovqinlar va atrof-muhit ta’siri sababli tez buzilishi mumkin. Shu bois kvant axborotni himoyalash uchun samarali xatoliklarni tuzatish usullaridan foydalanish zarur. QEC usullarida kvant axborot bir nechta harakatlanuvchi kubitlar yordamida himoyalanadi va bitta asosiy kubit hosil qilinadi. Kvant xatoliklarni tuzatishda keng qo‘llaniladigan usullarga **Shor kodi** va **surface code (yuzaki kod)** kiradi [4]. *Shor* kodi to‘qqizta jismoniy kubit yordamida bitta mantiqiy kubitni bitta kubitda yuzaga keladigan xatolardan himoya qiladi. *Surface code* esa kubitlarni panjara shaklida joylashtirishga asoslangan bo‘lib, ko‘p sonli kubitlar bilan ishlash uchun qulay va istiqbolli usul hisoblanadi. Samarali QEC usullari xatoliklar sonini sezilarli darajada kamaytiradi. Amaliy kvant hisoblashlarni amalga oshirish uchun xatolik darajasi 1 foizdan past bo‘lgan, xatolarga chidamli (fault-tolerant) tizimga erishish asosiy maqsad hisoblanadi. Kvant kriptografiyasi axborotni uzatishda yuqori darajadagi xavfsizlikni ta’minlash uchun kvant mexanikasi qonunlaridan foydalanadi. Bu sohadagi eng mashhur usul kvant kalitlarini taqsimlash bo‘lib, u orqali ikki tomon o‘rtasida maxfiy kalit yaratiladi. Kvant kalitlarini taqsimlashning eng mashhur usullaridan biri - BB84 protokoli bo‘lib, u 1984-yilda yaratilgan [8]. Bu usul orqali uzatilgan kalitni uchinchi tomon yashirincha kuzatmoqchi bo‘lsa, kvant xususiyatlari sababli bu darhol aniqlanadi. Chunki kvant ma’lumotlarni o‘lchash ularning holatini o‘zgartiradi. Kvant kriptografiyasi fotonlar yordamida ishlaydi va ularning holati axborotni himoyalashga xizmat qiladi. Shu sababli, bu usul nazariy jihatdan buzib kirishlardan himoyalangan hisoblanadi. Kvant kompyuterlar rivojlanib

(cc) BY © Mustafoyev Azamat Botir o‘g‘li

borayotgan bir paytda, oddiy kriptografik tizimlar zaiflashishi mumkin. Kvant kriptografiyasi esa kelajakda yanada kuchli himoya vositasi bo‘lishi kutilmoqda. Hozirgi kunda kvant kalitlarini uzatish texnologiyalari optik tolalar va sun’iy yo‘ldoshlar orqali yuzlab kilometr masofalarda muvaffaqiyatli qo‘llanilmoqda, bu esa uning amaliy ahamiyatini ko‘rsatadi.

- ***Superpozitsiya nima***. Kvant mexanikasida superpozitsiya - bu kvant sistemasining bir vaqtning o‘zida bir nechta holatda bo‘lishi mumkinligini anglatadi. Klassik fizikada obyekt bir vaqtda faqat bitta holatda bo‘lishi mumkin, ammo kvant sistemasi bir vaqtda bir nechta holatlarning kombinatsiyasida bo‘lishi mumkin.

Misollar: 1) Tanga havoga aylantirib otildi. U havoda aylanib turganida, u na “gerb”, na “raqam”, balki ikkalasining ham kombinatsiyasi holatida bo‘ladi. Bu superpozitsiya. Ammo, agar siz tangani ushlab, unga qarasangiz, u yoki “gerb” bo‘ladi, yoki “raqam”. Siz uni kuzatganingizda, u o‘zining superpozitsiya holatini yo‘qotadi va aniq bir holatga yerga tushadi. ***2) Yorug’lik.*** Yorug'lik bir vaqtning o‘zida ham to‘lqin, ham zarracha kabi harakat qilishi mumkin. ***3) Elektron.*** Elektron bir vaqtning o‘zida bir nechta joyda bo‘lishi mumkin[1].

- ***Kvant sensorlari*** yuqori aniqlik va sezgirlikka ega bo‘lib, fizik nazarda turli xil ko‘rish imkoniyatlarini oshirishga yordam beradi. Masalan, geofizika, tibbiyot va havo haqidagi ma’lumotlarni yaxshiroq qabul qilish uchun kvant sensorlaridan foydalanish mumkin [9]. Shuningdek, kvant sensorlari GPS tizimlarini to‘liq almashtirish imkonini berishi mumkin, chunki ular signallarni yuqori aniqlik bilan qabul qilishga qodir.

- ***Tibbiyot va biotexnologiyalar***. Kvant texnologiyalari to‘g‘ridan to‘g‘ri tibbiyotda ham qo‘llaniladi. Kvant tashxisi, molekular tahlil va aniq diagnostika usullari orqali bemorlarning holatini tez va aniq baholash mumkin bo‘ladi. Shuningdek, kvant simulyatorlari genetik kodning aniqlik bilan ishlashini tahlil qilishga yordam beradi. Bu yangi dori vositalarini ishlab chiqish va tibbiyotni rivojlantirishga yo‘naltirilgan. Bundan tashqari, kvant texnologiyalari raqamli marketing, moliyaviy modellashtirish, talab va ta’minotni optimallashtirish va ishlab chiqarish jarayonlarini avtomatlashtirish kabi ko‘plab sohalarda ishlatilishi mumkin. Kvant texnologiyalarining, xususan kvant kompterlarining ko‘pgina sohalarda kriptografik tizimlar uchun katta tahdid tug‘diradi, chunki ularning hisoblash qobiliyatlari klassik kompyuterlarga qaraganda juda yuqori. Kvant kompyuterlarining rivojlanishi, ayniqsa, kriptografik sistemalarning xavfsizligini boshqa darajaga olib chiqishi mumkin. Bu tahdidlarni tushunish uchun, birinchi navbatda, kvant kompyuterlarining ishlash prinsiplarini va ularning kriptografiyaga ta’sirini ko‘rib chiqish lozim. Kvant kompyuterlari va klassik kompyuterlar orasida bir necha muhim farqlar bor. Bu farqlar asosan ularning ishlash prinsiplariga, ma’lumotni ishlash va saqlash usullariga bog‘liq. Kvant kompyuterlarining asosiy afzalligi - ularning kvant mexanikasini qo‘llashida, ya’ni kubitlarning xosliklarini (superpozitsiya va pleting) foydalanishida. Klassik kompyuterlar esa bunga qarama-qarshi, bitlar orqali ma’lumotni ishlaydi. Nosimmetrik kriptografiyada ikkita kalit mavjud: ochiq va maxfiy. Birinchisi ma’lumotlarni shifrlash uchun kerak bo‘lsa, ikkinchisi shifrini ochish uchun kerak. Ikkala kalit ham matematik funksiya bilan o‘zaro bog‘langan bo‘lishiga qaramay, shaxsiy kalitsiz ma’lumotlarga kirish mumkin emas: na shaxsiy kompyuterlar, na superkompyuterlar hisoblash quvvati yetishmasligi tufayli bu vazifani bajara olmaydi. Shu bilan birga, assimetrik shifrni buzish mumkin: bu vazifani bajara oladigan algoritm olim Piter Shor tomonidan 1994 yilda ishlab chiqilgan. Yetti yil o‘tgach, 2001 yilda uning funksionalligi bir guruh IBM mutaxassislari tomonidan namoyish etildi. 7 kubitli kvant kompyuter yordamida 15 raqami 3 va 5 tub ko‘paytuvchilarga ajratildi [3]. Agar yetarli quvvatga ega kvant kompyuteri yaratilsa, Shor algoritmi hozirda qo‘llanilayotgan assimetrik kriptografik sxemalarning aksariyatini (RSA, DSA, EdDSA, GOST R 34.10-2012 va boshqalar) samarali (shifrlash uchun zarur bo‘lgan vaqtdan bir oz ko‘proq vaqt ichida) sindirish imkonini beradi.

- ***Kvant kompyuterlarining imkoniyatlari*** kvant kompyuterlari bir qator sohalarda inqilobiy imkoniyatlar taqdim etadi. Quyida ularning asosiy qo‘llanilishi va imkoniyatlari keltiriladi:

- *kriptografik tahlil:* Kvant kompyuterlari Shor algoritmi yordamida katta sonlarni faktorizatsiya qilish va diskret logarifm muammolarini yechish orqali ochiq kalitli shifrlash tizimlarini, masalan, RSA va Diffi-Hellman algoritmlarini osonlikcha buzishi

(cc) BY © Mustafoyev Azamat Botir o‘g‘li

mumkin. Bu klassik kriptografik tizimlarning xavfsizligiga jiddiy tahdid soladi.

- *ma’lumotlarni qidirish va optimallashtirish:* Grover algoritmi kvant kompyuterlariga nustrukturlashtirilmagan ma’lumotlar bazasida qidirishni kvadrat darajada tezlashtirish imkonini beradi. Bu, masalan, ma’lumotlar tahlili va mashinaviy o‘qitishda muhim ahamiyatga ega, qolaversa kvant kompyuterlari molekulalarning kvant xususiyatlarini simulyatsiya qilishda katta imkoniyatlarga ega. Bu yangi dori-darmonlar ishlab chiqish va materialshunoslik sohasida inqilobiy o‘zgarishlarga olib kelishi mumkin .

- ***Kvant kompyuterlarining kriptografiyaga ta’siri*** kvant kompyuterlarining eng muhim ta’sirlaridan biri axborot xavfsizligi, xususan, kriptografiya sohasiga qaratilgan. Shor algoritmi ushbu muammolarni polinomial vaqt ichida yechish imkonini beradi, bu esa mazkur algoritmlarni deyarli himoyasiz holatga keltiradi. Masalan, 2048 bitli RSA kalitini faktorizatsiya qilish klassik kompyuterlarda milliardlab yillar talab qilsa, yetarlicha quvvatli kvant kompyuteri buni bir necha soat yoki hatto daqiqalar ichida amalga oshirishi mumkin. Bundan tashqari, Grover algoritmi simmetrik shifrlash tizimlariga, masalan, AES va SHA-256 kabi algoritmlarga ta’sir qiladi. Grover algoritmi kalit uzunligini kvadrat darajada qisqartiradi, ya’ni 128 bitli kalit xavfsizligi taxminan 64 bitli kalit darajasiga tushadi. Bu simmetrik shifrlash tizimlarining xavfsizligini ta’minlash uchun kalit uzunligini ikki baravar oshirish zarurligini keltirib chiqaradi [5].

- ***Kvant kompyuterlarining cheklovlari va kelajakdagi istiqbollari*** kvant kompyuterlari katta imkoniyatlarga ega bo‘lsa-da, ularning hozirgi holatda bir qator cheklovlari mavjud. Birinchi navbatda, kvant kompyuterlari hali keng ko‘lamli va barqaror emas. Kubitlarning barqarorligini ta’minlash (decoherence muammosi) va kvant xatolarini tuzatish texnologiyalari hali to‘liq rivojlanmagan. Ikkinchidan, kvant kompyuterlari faqat ma’lum turdagi muammolarni tez yechishda samarali bo‘lib, umumiy hisoblash vazifalari uchun klassik kompyuterlardan ustunlikka ega emas.Biroq, kelajakda kvant kompyuterlarining rivojlanishi bilan ular axborot xavfsizligi sohasida jiddiy o‘zgarishlarga olib kelishi kutilmoqda. Shu sababli, kvantga chidamli (post-quantum) kriptografik algoritmlarni ishlab chiqish bugungi kunda eng dolzarb vazifalardan biri hisoblanadi [5]. Postkvant kriptografiya kvant kompyuterlarining tahdidlariga qarshi turishga qodir bo‘lgan yangi matematik muammolarga asoslanadi, bu haqda keyingi bo‘limlarda batafsil muhokama qilinadi. Kvant kompyuterlari kvant mexanikasining superpozitsiya, chigallik va o‘lchov prinsiplariga asoslangan holda klassik kompyuterlarga nisbatan sezilarli hisoblash afzalliklarini taqdim etadi. Ularning imkoniyatlari, xususan, Shor va Grover algoritmlari orqali ochiq kalitli va simmetrik shifrlash tizimlariga jiddiy tahdid soladi. Hozirgi kunda kvant kompyuterlari hali sinov bosqichida bo‘lsa-da, ularning kelajakdagi rivojlanishi axborot xavfsizligi sohasida yangi yondashuvlarni talab qiladi. Kelajakda kvant kompyuterlarning rivojlanishi axborot xavfsizligi sohasida tub o‘zgarishlarga olib kelishi kutilmoqda. Shor va Grover algoritmlari kabi kvant algoritmlari mavjud ochiq kalitli (RSA, Diffie-Hellman) va simmetrik (AES, SHA) shifrlash tizimlarini samarali sindirish imkoniyatini beradi. Shu sababli, kvantga chidamli (post-quantum) kriptografiya bugungi kunda eng dolzarb ilmiy va amaliy vazifa sifatida qaraladi. Postkvant kriptografiya masalalari klassik kompyuterlar tomonidan hal qilinadigan matematik muammolarga asoslanib, kvant tahdidlariga qarshi turishga mo‘ljallangan algoritmlarni ishlab chiqishga qaratilgan. Ular orasida lattice-based, code-based, multivariate polynomial va hash-based algoritmlar eng istiqbolli yo‘nalishlar hisoblanadi.

Xulosa

Kvant hisoblash texnologiyalari axborotni qayta ishlashda mutlaqo yangi yondashuvni taklif etib, klassik kompyuterlar imkoniyatlaridan tubdan farq qiladi. Ushbu maqolada kvant kompyuterlarining ishlash asoslari, jumladan kubitlar, superpozitsiya va chigallik kabi kvant mexanikasiga xos hodisalar tahlil qilindi. Shor va Grover algoritmlari misolida kvant hisoblashning kriptografiya va hisoblash murakkabligi masalalariga ko‘rsatadigan kuchli ta’siri asoslab berildi.

Tahlillar shuni ko‘rsatadiki, kvant kompyuterlarining rivojlanishi mavjud kriptografik tizimlar uchun jiddiy tahdid tug‘diradi va axborot xavfsizligini ta’minlashda yangi yondashuvlarni talab etadi. Shu bilan birga, kvant

© Mustafoyev Azamat Botir o‘g‘li

xatoliklarni tuzatish texnologiyalarining rivoji kvant kompyuterlarning amaliy qo‘llanilishi uchun hal qiluvchi ahamiyatga ega hisoblanadi. Natijada, postkvant kriptografiyani ishlab chiqish va joriy etish bugungi kunda dolzarb ilmiy va amaliy vazifa sifatida namoyon bo‘lmoqda.

Foydalanilgan adabiyotlar

1. Nielsen M., Chuang I. *Quantum Computation and Quantum Information*. Cambridge University Press, 2010.
2. IBM Quantum Computing Research. https://www.ibm.com/quantum
3. Rieffel E., Polak W. *Quantum Computing: A Gentle Introduction*. MIT Press.
4. Bennett C., Brassard G. *Quantum Cryptography: Public Key Distribution and Coin Tossing*. 1984.
5. NIST. *Post-Quantum Cryptography Standardization Project*. https://csrc.nist.gov
6. Nielsen, MA, Chuang, IL Kvant hisoblash va kvant ma'lumotlari . Cambridge University Press, 2000.
7. Grover, L. K. (1996). "A fast quantum mechanical algorithm for database search". Proceedings of the twenty-eighth annual ACM symposium on Theory of computing (STOC), 212–219.
8. Hayashi, M. (2015). Introduction to Quantum Information Science. Graduate Texts in Physics. Springer.
9. Bernstein, D. J., & Lange, T. (2017). "Post-quantum cryptography". Nature, 549(7671), 188–194.
10. Shor, P. W. (1997). "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". SIAM Journal on Computing, 26(5), 1484–1509.

© *Mustafoyev Azamat Botir o‘g‘li*