КВАНТ КОМПЬЮТЕРЛАРНИ АХБОРОТ ХАВФСИЗЛИГИНИ ТАЪМИНЛАШ СОҲАСИДА ҚЎЛЛАШ ИМКОНИЯТЛАРИ ХУСУСИДА

Абдуаҳатов Умиджон Абдуҳамид ўғли

Ушбу мақолада квант технологиялари асосида ишлайдиган компьютерлар яратилиш жараёнлари хамда ахборот хавфсизлиги масалаларига татбиқлари келтирилган.

В статье рассматривается процесс создания компьютеров на основе квантовых технологий и их применение во всех вопросах информационной безопасности.

The article discusses the processes of creating computers based on quantum technologies and their application in all matters of information security.

Ҳозирги замон талабига кўра, жамиятнинг барча соҳалари қатори оддий кундалик ҳаётимизга ҳам ахборот технологиялари шиддат билан кириб келмоқда. Дунё мамлакатларининг ривожланиш даражасига баҳо берганда, замонавий ахборот технологияларидан қай даражада фойдаланаётгани масаласи биринчи даражага чиқаётгани бежиз эмас. Шу билан бирга дунё бўйлаб ахборот ҳажми кундан-кунга ортиб бормоқда. Статистик маълумотларга кўра, рақамли форматдаги ахборот ҳажмининг ўзи йилига 30% га кўпайган, охирги 5 йил ичида инсоният томонидан ундан аввалги бутун тарих мобайнидаги ахборот ҳажмидан кўра кўпроқ ахборот ишлаб чиқарилган [3].

Дунёдаги етакчи IT-компанияларда ўта кучли суперкомпьютерлар мавжуд ва улар ахборотни 125,43 петафлопс тезлик билан қайта ишлай олиш қувватига эга. Маълумот учун: 1 петафлопс - сониясига 1 триллион операция бажарадиган жараёндан 1000 таси демакдир. Лекин, ахборот ҳажмининг юқорида айтилгани сингари ўсиш суръатлари сақланар экан, яқин йилларда бизга бу тезлик камлик қилиб қолиши ҳеч гап эмас қолаверса, процессорнинг амалий имкониятининг ҳам муайян физик чегараси мавжуд. Бу кетишда, яқин йилларда Мур қонуни ўз кучини йўқотади, яъни Грехем Мурнинг 1965-йилда олиб борган кузатишларига асосланган бўлиб, унга кўра, электрон қурилмаларнинг ахборотни сақлаш ва қайта ишлаш имконияти ҳар йили 2 баробардан ошиб боради, 90-йиллардан бошлаб, электрон ускуналарнинг ахборотни сақлаш ва қайта ишлаш имконияти ҳар йили эмас, балки, ҳар икки йилда 2 баробарга ошиб бормоқда.

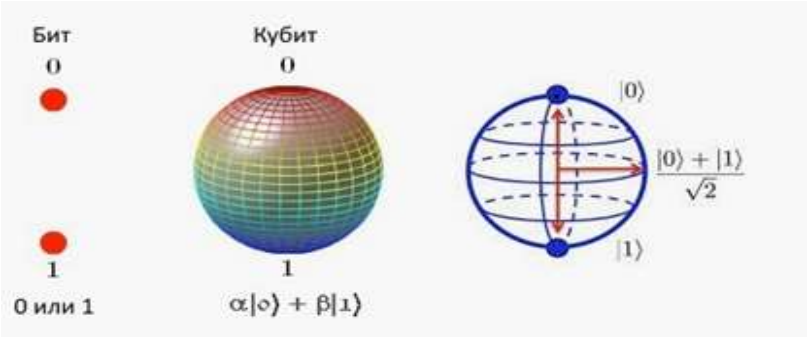
Замонавий суперкомпьютерлардан кўра кучлироқ ва тезкорроқ бўлган тамомила янги турдаги ахборотни сақлаш, узатиш ва қайта ишлаш учун янги турдаги компьютерларга эҳтиёж уйғонмоқда.

Шу боис жаҳонда нанотехнологик тадқиқотлар кўламини кенгайтириш ва бу борадаги инновацион технологиялардан тобора кенг фойдаланишга эътибор кучайиб бормоқда. Масалан, компьютер технологиялари соҳасида олиб борилаётган изланишлар натижасида, квант информатикаси фани юзага келди.

Ушбу соҳа наноўлчамли процессорларга эга бўлган квант компьютерларини яратиш ва улар учун дастурий таъминотлар ишлаб чиқишни ўз ичига олади. Квант компьютерларида бир бирлик ахборотни ёзиш учун битта ёки бир нечта атомдан фойдаланилади. Биз фойдаланаётган ҳозирги замон компьютерларида бу жараённи бажариш учун эса бир неча миллиард атом сарфланади. Демак, квант компьютерлари ҳисоблаш жараёнида, ўз-ўзидан ўта юқори тезлик ва самарадорликни оширади. Шу билан бирга, квант компьютерларининг юқори тезликда ишлай олиш қобилияти туфайли, ҳозирги криптографик алгоритмлардаги шифрлаш усулларини бузиш хавфи ҳам ошиб бормоқда [1].

Мазкур мақола ҳам айнан ушбу йўналишга бағишланган бўлиб, унда квант компьютерларини яратишда ҳозирги кунга қадар эришилган ютуқлари ва квант теҳнологиясининг ахборот хавфсизлиги масалаларига ижобий ҳамда салбий таъсирлари кўриб чиқилади.

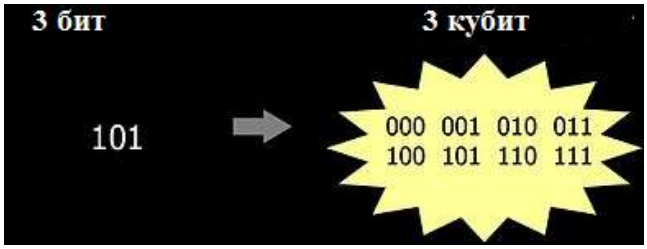
Ҳозирги классик компьютерлардаги процессорни ташкил қилувчи транзисторлар 0 ёки 1 ҳолатдан фақат биттасинигина ифодалай олса, квант компьютерларининг транзисторлари эса бир вақтнинг ўзида ҳам 0 ва ҳам 1 ҳолатини ифодалай олади. Яъни, бундай квант транзистори бир вақтнинг ўзида ҳам “ёниқ” ва ҳам “ўчиқ” бўлиши мумкин. Бу илм-фанда “суперпозиция” ҳодисаси деб аталади (1-расм).



1-расм. Бит ва кубит бирлиги.

Квант компьютер - бу маълумотни узатиш, сақлаш ва қайта ишлаш учун квант механик ҳодисалари (квант суперпозицияси ва квант чалкашлиги) асосида ишлай оладиган компьютердир.

Квант бит (кубит) квант компьютерда маълумотларни сақлашнинг энг кичик элементи хисобланади (2-расм).



2-расм. 3 бит ва 3 кубит ифодаланиши.

Бу шуни англатадики, кубитлар сони қанчалик кўп бўлса, квант компьютерларнинг ишлаши шунчалик тез амалга оширилади[4].

Бугунги кунда яратилаётган квант компьютерлари ва ҳозирда фойдаланилаётган классик компьютерлари, қуйидагича ишлаш тамойиллари бўйича фарқланади(1-жадвал).

1-жадвал. Классик ва квант компьютерлар солиштирма жадвали.

Тамойиллар	Классик компьютерлар	Квант компьютерлар
Мантиқ	0 ёки 1	a | 0> + b | 1>
Физик	Яримўтказгичли транзистор	Квант объекти
Ахборот ташувчи	Кучланиш даражаси	Поляризация, айлантириш, ...
Амалиётлар	ЙЎҚ, ВА, ЁКИ, ХОР	Гейтс: CHOT, Ҳадамард, ...
Ўзаро боғлиқлик	Яримўтказгич чипи	Ўзаро аралашиш
Алгоритмлар	Стандарт	Махсус
Ишлаш услуби	Рақамли, детерминистик	Аналог, эҳтимоллик

Ҳозирда квант транзисторларининг, яъни, кубитларнинг турли хиллари мавжуд. Масалан, “топологик кубитлар” деб ном олган кубитларни Microsoft корпорацияси ишлаб чиққан. Лекин, бу кубитлар фавқулотда нозик даражада сезувчан бўлиб, арзимаган товуш тўлқинлари ёки иссиқлик нурланиши туфайли парчаланиб кетади. Барқарор ишлаш учун, топологик кубитларга –273 °C ҳарорат зарур. Бундай ўта паст ҳароратни ҳосил қилиш жуда қийин. Бу ҳароратни барқарор сақлаб туриш эса ундан-да қийин. Лекин, топологик кубитларнинг мазкур инжиқликларига яраша ажойиб ижобий жиҳатлари ҳам мавжуд. Хусусан, бундай кубитлар асосида ишловчи квант компьютерларида, деярли хатолик бўлмайди. Microsoft корпорациясидагилар топологик кубитлар асосида ишлаб чиқилган квант компьютерлари, ишончлилик нуқтаи назаридан, ўта мукаммал бўлади деб баёнот беришмоқда.

Квант компьютерлари учта асосий турдан иборат бўлади: биринчи тур - квант компьютерининг ўзи бўлиб, у мутлақ нол –273 °C ҳароратга яқин бўлган ўта паст ҳароратлардаги кубитлардан иборат бўлади. Иккинчи тур - криоген квант компьютери бўлиб, У ҳам –268 °C ҳароратдаги кубитлардан иборат бўлади. Сўнгги, учинчи тур эса, одам ишлаши учун қулай ва мослаштирилган интерфейс компьютери бўлади. Таҳминларга кўра, бундай квант компьютерлари ҳозирда мавжуд энг илғор суперкомпьютерлардан 100-300 баробар тезкорроқ бўлади[3].

Квант компьютерлар яратиш билан бирга квант компьютерлари билан инсон ўртасида мулоқот ўрнатадиган махсус дастурий таъминот яъни квант компьютерлари учун операцион тизимлар, дастурлар ва турли бошқа иловалар ишлаб чиқиш борасида ҳам ишлар олиб борилмоқда. Шу борада Cambridge Университети олимлари квант компьютер учун операцион тизимларни ишлаб чиқмоқдалар. Янги платформани ишлаб чиқариш, улътра қудратли компьютерларнинг янги авлодини қуриш йўлидаги катта қадам бўлди.

Cambridge олимлари томонидан яратилган операцион тизимлар квант компьютерининг симулятсияси сифатида суперкомпьютерлар устида амалга оширилди.

Қуйидаги жадвалда квант компьютерларининг кубитлар сони бўйича 20 йил вақт оралиғидаги ривожланиши келтирилган (2-жадвал).

2-жадвал. Квант компьютерларининг ривожланиш жадвали.

Квант компьютер яратувчи компаниялар	Йиллар	Кубитлар сони
IBM, Oxford, Berkley, Standford, MIT	1998	2
Tehnical University of Munch	2000	5
Los Alamos National Labaoratory	2000	7
Institute for Quantum Computing. Perimeter Institute for Theoretical Phiysics, and MIT	2006	12
D-Wave Systems	2008	28
IBM, Oxford, Berkley, Standford, MIT	2017	50
Intel	2018	49
Google	2018	72
Rigetti	2019	128

Квант компьютерлари яратишлиши бугунги кунда маълумотлар яхлитлиги ва махфийлигини, ишончлилигини таъминлаётган криптографик алгоритмлар бардошлилигига ҳам ўз таъсирини ўтказади. Ҳозирги кундаги криптографик алгоритмлар математик муаммоларини ҳал қилиш учун қудратли суперкомпьютерлар ҳам юзлаб, минглаб йиллар талаб қилар эди, аммо квант компьютерининг пайдо бўлиши билан шунга ўхшаш муаммони бир неча кун ёки бир неча соат ичида ҳал қилиш мумкин бўлади.

Ҳозирда фойдаланилаётган барча ахборотни ҳимояловчи крипто тизимлар айниқса, RSA ва El-Gamal каби очиқ калитли (Ассиметрик) крипто алгоритмлардаги математик муаммоларини ҳал қилишда 1024 ёки 2048 бит узунликдаги калитни тўлиқ танлаш усули билан супер компьютерларда йиллаб вақт талаб қилган бўлса, квант компьютерлари билан бир неча соат ёки бир неча дақиқа ичида амалга ошириш мумкин бўлади.

Шунингдек, квант компьютерларининг юқори тезликда ишлай олиш қобилияти туфайли электрон рақамли имзо, ҳешлаш алгоритмлари хамда AES, Гост каби симметрик шифрлаш алгоритмларининг ҳам криптобардошлилигини камайтиради. Лекин квант компьютерлари яратилиши билан бирга квант криптографиясини яратиш бўйича ҳам кўплаб ишлар амалга оширилмоқда. Бу борада, квант алгоритмларига ҳам қўллаш мумкин бўлган учта энг машҳур криптотаҳлил алгоритмлари аллақачон мавжуд [2]:

1. Шор алгоритми (факторизация)
2. Гровер алгоритми (тартибсиз маълумотлар базасида тезкор қидирув)
3. Деутсч-Жожи алгоритми (доимий ёки мувозанатли функция)

Пост-квант (квант-хавфсиз) криптографияси, оддий классик криптография сингари, математик масалаларни ечишга асосланади. АҚШ Миллий стандартлар ва технологиялар институти (NIST) 2016 йилда квантдан кейинги очиқ калитли шифрлаш ва рақамли имзо шифрлаш стандартларини ишлаб чиқиш мақсадида очиқ танлов эълон қилди. Ушбу танлов бўйича аллақачон 1 ва 2 босқич натижаларига кўра, дастлабки алгоритмлар тўплами 69 тадан 26 гача қисқартирилганди. 2020 22-июлда 3 босқичдан натижалари ҳам эълон қилинди, унга кўра очиқ калитли шифрлаш учун 4 та номзод ва рақамли имзолар учун 3 та номзод алгоритмлар саралаб олинди[6].

Шундай қилиб, танловнинг финал босқичи учун танлаб олинган квандан кийинги очиқ калитли шифрлаш ва рақамли имзо номзод стандарт алгоритмлари ва уларнинг математик мураккабликлари ҳамда шифрлаш усуллари қуйидаги жадвалда келтирилган. (3-жадвал).

3-жадвал. Танлов финал босқичи учун номзод алгоритмлар.

Алгоритмнинг шифрлаш тури ва математик мураккаблиги	Очиқ калитли шифрлаш	Рақамли имзо
Панжара схемалар	• CRYSTALS-KYBER • NTRU • SABER	• KRISTALLAR-DILITIY • FALCON
Код асосида	• Classic McEliece	
Кўп ўзгарувчанлик		• Rainbow

Ривожланган мамлакатлар ва IT-гигант компаниялар ўзларининг квантли ахборотни қайта ишлаш лабораториялари ривожланишига ўнлаб миллиард доллар сармоя киритаётгани бежиз эмас. Ушбу мамлакатлар сарасигса АҚШ, Хитой, Япония, Россия, Европа давлатлари ва IBM, Google, D-Wave, Microsoft каби корпорацияларини киритиш мумкин. 2000 йилларга қадар Россияда ҳам квант физикаси мактаби, дунёдаги энг кучли мактаблардан бири саналарди. Ушбу мақомни, яъни Россияни квант технологиялари соҳасида дунёнинг этакчиларидан бирига қайтариш мақсадида, Россия Квант Маркази, Москва физика-техника институтида суньий квант тизимлари лабораторияси ва квант теҳнолояилари соҳасида тадқиқотлар билан шуғулланадиган нодавлат ташкилотлар лабораториялари ташкил этилди.

Бу борада қилинган ишлар натижасида, 2018 йилда Россия Фанлар академияси қошидаги "МИСИС" лабораториясида квант компьютери учун сигнал кучайтиргичи ва Россия Квант Маркази асосчиси Михаил Лукиннинг Garvard университети профессорлари билан хамкорлигида, 51 кубитлик квант процессори яратилди. Бундан ташқари Россияда квант технологиялари асосида ахборотни қайта ишлашни ривожлантириш бўйича йўл харитаси тасдиқланган бўлиб, суньий интеллект тизимлари учун квант технологияларини қўллаш афзалликларига доир ишлар хам олиб борилмоқда.

Умуман олганда, келажак квант компьютерларини яратиш билан боғлиқ ишлар аллақачон юқоридаги каби мамлакатлар ва IT компаниялар томонидан

амалга оширилиб, йил сайин уларнинг сони ҳам кенгаймоқда. Ҳозирги кунда киберхавфсизлик ва кибержиноят масалаларига бўлган эътибор олдингидан кўра ортиб бормоқда. Ўзбекистон Республикасидаги аксарият давлат ва нодавлат ташкилотларида қўлланилаётган ахборот хавфсизлигини таъминловчи дастурий ва аппарат дастурий таъминотлари, криптографик алгоритмларининг бардошлилигига таянади.

Шу каби келажак квант компьютерлари ва алгоритмларининг яратилиши билан боғлиқ бўлган таҳдидларга тайёр бўлиш учун Республикамизда ҳам хорижий мамлакатлар сингари квант технологиялари лабораторияларини ташкил этиш ҳамда квантдан кийинги ахборот хавфсизлиги масалалари йўналишига доир илмий ишларни олиб бориш долзарблигини кўрсатади.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР РЎЙҲАТИ:

1. Е.Матвеев Применение квантовомеханических эффектов в системах защиты информации.2019.
2. П.Ключарёв Алгоритмическое и программное обеспечение для моделирования квантового компьютера.2009.
3. https://orbita.uz/index.php?option=com_content&view=article&id=854:kvant-kompyuteri-u-qanday-tuzilgan&catid=49:bu-qanday-ishlaydi&Itemid=71
4. https://ru.wikipedia.org/wiki/%D0%9A%D0%B2%D0%B0%D0%BD%D1%82%D0%BE%D0%B2%D1%8B%D0%B9_%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80
5. https://www.dw.com/ru/спецслужба-сша-разрабатывает-суперкомпью-тер-для-взлома-любых-кодов/
6. https://habr.com/ru/post/512410/