КВАНТ КРИПТОГРАФИЯСИНИНГ АСОСИЙ ПАРАМЕТРЛАРИ ВА КВАНТ ТЕХНОЛОГИЯСИ АСОСИДА КРИПТОГРАФИК КАЛИТЛАРНИ АЛМАШИШ ПРОТОКОЛИ

Илхом Марданокулович БОЙҚУЗИЕВ
катта ўқитувчи
физика-математика фанлари бўйича (PhD) фалсафа доктори
Тошкент ахборот технологиялари университети
Тошкент, Ўзбекистон
salyut2017@gmail.com
Ориф Менглимуратович АЛЛАНОВ
доцент
техника фанлари бўйича (PhD) фалсафа доктори
Тошкент ахборот технологиялари университети
Тошкент, Ўзбекистон
orif_allanov@mail.ru
Маъмур Маърупович МУРОДОВ
ассистент
Тошкент ахборот технологиялари университети
Тошкент, Ўзбекистон
ma'mur2136@mail.ru

Аннотация

Мақолада квант технологиясининг асосий тушунчалари, квант элементлари ҳақида тушунчалар келтирилган. Квант технологиясининг қўлланилиш соҳалари таҳлил қилинган.

Таянч сўзлар: симметрик криптография, асимметрик криптография, Гейзенберг ноаниқлик принципи, квант телепортацияси, квант схемалари.

ОСНОВНЫЕ ПАРАМЕТРЫ КВАНТОВОЙ КРИПТОГРАФИИ И ПРОТОКОЛА ОБМЕНА КРИПТОГРАФИЧЕСКИМИ КЛЮЧАМИ НА ОСНОВЕ КВАНТОВОЙ ТЕХНОЛОГИИ

Ильхом Марданокулович БОЙКУЗИЕВ
старший преподаватель
доктор философии (PhD) по физико-математическим наукам
Ташкентский университет информационных технологий
Ташкент, Узбекистан
salyut2017@gmail.com
Ориф Менглимуратович АЛЛАНОВ
доцент
доктор философии (PhD) по техническим наукам
Ташкентский университет информационных технологий
Ташкент, Узбекистан
orif_allanov@mail.ru
Маъмур Маърупович МУРОДОВ
ассистент

Ташкентский университет информационных технологий
Ташкент, Узбекистан
ma’mur2136@mail.ru

Аннотация

В статье представлены основные понятия квантовой технологии, понятие квантовых элементов. Проанализированы области применения квантовых технологий.

Ключевые слова: симметричная криптография, асимметричная криптография, принцип неопределенности Гейзенберга, квантовая телепортация, квантовые схемы.

Криптография – бу бизга юборувчи ва қабул қилувчи ўртасида учинчи томон аралашувисиз хавфсиз алоқа ўрнатишга ёрдам берадиган фан соҳаси. Маълумотлар яхлитлиги, аутентификация, муаллифликдан бош тортиш ва маълумотларнинг махфийлиги замонавий криптографиянинг асосий воситаларидир. Замонавий криптография ёки классик криптографиядан электрон тижорат, автоматлаштирилган касса машиналари, банкоматлар, компьютер пароллари ва бошқа кўплаб муҳим иловаларда фойдаланилади.

Классик криптография асосан турли хил алгоритмлардан фойдаланган ҳолда оддий матнни кодлар матнига айлантиради. Маълумотларни шифрлаш учун ишлатиладиган калитлар жўнатувчи ва қабул қилувчи ўртасида бўлинади, шунда улар хабарни шифрлаши ёки шифрини очиши мумкин.

Классик криптография икки турга бўлинади:

1. Симметрик криптография – бу шифрлаш ва шифрни очиш учун ишлатиладиган калитлар бир хил бўлган энг мураккаб криптография усули [1].

2. Асимметрик криптография – шифрлаш ва шифрни очиш учун турли калитлардан фойдаланадиган криптографиянинг бироз мураккаб усули. Асимметрик криптография модели ҳеч қачон жўнатувчи ва қабул қилувчи ўртасида шахсий калитларни алмаштирмаган ва у фақат очиқ калитлардан фойдаланади. Шундай қилиб, у кибер-ҳужумларга камроқ мойил бўлади ва фойдаланувчига маълумотлар билан хавфсиз мулоқот қилиш имконини беради.

Ушбу криптография усулларидан кейин ҳам маълумотларнинг бузилиши сони кескин ўсиб бормоқда. Шунингдек, бу усуллардан фойдаланиш маълумотларни чекланган ҳисоблаш имкониятига эга. Рақамли даврда эса маълумотлар ҳажми ва хилма-хиллиги мазкур ҳисоблаш чегараларидан каттароқ имкониятларни талаб қилади.

Криптографик алгоритмларнинг асосий ишлаш принципи математик моделлар атрофида ишлаб чиқилган ва шунинг учун ушбу моделлар кўплаб хавфсизлик камчиликларига эга, масалан: қўпол куч ҳужуми, факторизация муаммоси ва бошқалар. Шундай қилиб, технологиянинг ривожланиши туфайли классик криптография маълумотлар махфийлиги ва хавфсизлиги учун хавфсиз вариант эмас. Айнан шунинг учун Квант криптографияси деб аталадиган янги технологияга ўтиш муаммоси долзарб ҳисобланади [1].

Квант криптографияси квант физикаси ҳодисаларига асосланади, бу жўнатувчи ва қабул қилувчи ўртасида хавфсиз маълумотларни узатиш имконини беради. Квант криптографияси тармоқ хавфсизлиги соҳасида инқилобни ташкил этади [2].

Квант криптографияси криптографиянинг энг сўнгги ва илғор соҳаси бўлиб, унинг асоси квант техникасининг иккита принципига асосланади: Гейзенбергнинг ноаниқлик принципи ва фотон қутбланиш принципи [2].

Гейзенбергнинг ноаниқлик принципи шуни кўрсатадики, баъзи жисмоний хусусиятлар жуфтлиги бир хусусиятни ўлчашда одамнинг бир вақтнинг ўзида бошқасини билишига тўсқинлик қилиши мумкин. Хусусан, қайси йўналишни ўлчашни танлаш барча кетма-кет ўлчовларга таъсир қилади. Поляризацияланмаган ёруғлик вертикал текисланган фильтрга кирганда, у ёруғликнинг бир қисмини ўзлаштиради ва қолган қисмини вертикал йўналишда қутблайди. Қайсидир бурчак остида $к$ эгилган кейинги фильтр қутбланган ёруғликнинг бир қисмини ўзига сингдиради ва қолган қисмига янги қутбланиш беради ҳамда узатади. Горизонтал/вертикал каби фотонларнинг қутбланишини ифодалаш учун фойдаланиладиган бир жуфт ортогонал қутбланиш ҳолатлари базис деб аталади [3].

1984 йилда BB84 деб номланган квант калитларини тақсимлаш протоколи ишлаб чиқилди. BB84 протоколи қуйидаги босқичлардан ўтади:

1. Юборувчи поляризацияланган фотонларни қабул қилувчига тўғри чизиқли ёки диагонал йўналишда юборади;

2. Қабул қилувчи базисни (тўғри чизиқли/диагонал) тасодифий танлаб, фотонларнинг йўналишини текширади ва натижаларни сақлайди. Юборувчи ва қабул қилувчи томонидан ўлчаш учун танланган базис бир хил бўлиши шарт эмас;

3. Очиқ канал орқали қабул қилувчи жўнатувчига ўзининг ўлчов базислари ҳақида хабар беради;

4. Сўнгра жўнатувчи қабул қилинган базис билан ҳақиқий базисни солиштиргандан сўнг тўғри битларни (асослари бир хил бўлган битларни) умумий канал орқали юборади;

5)Нотўғри битлар жўнатувчи ва қабул қилувчи томонидан ўчирилади ва тўғрилари калит сифатида қабул қилинади. Агар тажовузкор жўнатувчи билан бир хил базисдан фойдаланса, у асл маълумотни башорат қила олади, агар бўлмаса, тажовузкорнинг бу фаолияти юборилган маълумотларга таъсир қилади ва бунинг натижасида қабул қилувчи тўсқинлик қилинган маълумотларни олади ёки маълумотлар мавжуд бўлмайди йўқ, иккала ҳолатда ҳам тажовузкор мавжудлиги аниқланади [3].

Калитларни тақсимлаш – бу шифрланган калитларни икки томон ўртасида тарқатиш усули. Калитларни тарқатишнинг оддий усули хавфсиз муҳитда шахсан учрашиш ва калитларни алмашишдир. Аммо энди биз ҳар қандай калитларни алмаштириш учун RSA, Diffie-Hellman, ECC каби алгоритмлар ёрдамида масофада очиқ калитлардан фойдаланиб алмашишимиз мумкин [4].

Анъанавий калитларни тақсимлаш билан боғлиқ муаммолар шундан иборатки, улар маълумотларни узатиш учун оддий математик ҳисоб-китоблардан фойдаланади, уларни ҳисоблаш осон ва уларга учинчи шахслар осонгина киришлари мумкин [4].

Ушбу классик калит тарқатиш ёндашуви кўплаб қийинчиликларга эга.

Улар классик калитга ўхшайди, фақат учинчи шахслар томонидан осонгина олиниши мумкин бўлган заиф тасодифий рақамларни яратиши мумкин. Бундан ташқари, процессор қуввати ва бу калитлар янги ҳужум стратегияларига нисбатан заифдир, чунки агар бирон-бир янги ҳужум стратегиясидан фойдаланилган бўлса, уларни қайта дастурлаш керак. Квант компьютерлари ушбу классик шифрлаш стратегияларини хавф остида қолдириши мумкин, чунки квант компьютерлари ҳақиқатга айланса, улар ёрдамида классик калитлардаги маълумотларни осонгина декодлаши мумкин. Бу эса симметрик калитларни хавфсиз сақлаш ва тарқатиш учун катта ассиметрик калитлардан фойдаланиш заруриятини юзага келтиради. Буларнинг барчаси криптографик калитларнинг хавфсизлигини қайта кўриб чиқишга мажбур қилади [4].

QKD маълумот ёки маълумотни бир нуқтадан иккинчи нуқтага ўтказиш учун барча квант механикасидан фойдаланган ҳолда криптографик калитлар дуч келадиган ушбу муаммоларни ҳал қилади. QKD маълумотларни узатувчидан қабул қилувчига ўтказиш учун ўзига хос квант каналидан фойдаланади. Бундан ташқари, у пост қайта ишлашга кириши учун оммавий алоқа ҳаволасига муҳтож. Шунингдек, у ушлаш орқали йўқолган маълумотлар миқдорини ҳисоблайдиган порталга эга [4].

Квант саноатига қарши турадиган энг катта қийинчилик квант компютерларини ёки унинг турли иловаларини унинг чекловларига қарамай тижорат ва кенг фойдаланишга олиб чиқишдир. Квант компьютерларини олиб келишнинг асосий мақсади инсоният ҳал қила олмаган муаммоларни ҳал қилишдир.

Квант криптотаҳлили шифрланган маълумотларнинг маъносини асл маълумотларга кирмасдан тушунишдир. Бунда асосий ҳаракат махфий калитни топишга қаратилади [5]. Шифрланган маълумотни олиш учун ҳужумларнинг турлари ҳам ўрганилади. Ушбу ҳужумларни ўрганиш хавфсизликни амалий жиҳатдан текшириш орқали амалга оширилиши

мумкин. Умуман олганда, QKD тизимидаги амалий муаммо – бу бўшлиқларни криптоанализ ёрдамида ўрганиш ва ҳалқа тешикларини аниқлаш [5].

Електронлар ёки кубитлар, агар улар исталган нуқтада ўзаро таъсир қилсалар, бу зарралар ўртасида боғланиш бўлади. Агар электронлар ёки кубитлар бу хусусиятларни кўрсатса, улар корреляцияда жойлашган ёки улар бир-бирига боғланган деб аталади. Бир электроннинг спинини билгандан сўнг, бошқа ўралган электрон бошқа электронга тескари йўналишда спинга эга бўлади. Квант суперпозитсиясидан фойдаланилганлиги сабабли, зарралар ҳисоб-китоблар бошланишидан олдин спин ёки йўналишга эга эмас, лекин заррача юқорига ва пастга ёки 0 с ва 1 с ҳолатларида муқобил равишда мавжуд. Заррачанинг спини ўлчаш вақтида ўлчанади ва у бир вақтнинг ўзида ўзининг чигаллашган зарраси билан боғланади, у ўлчанган заррачанинг дастлабки спинига тескари айланиш йўналишига эга. Ушбу хусусият билан кубитлар ўзаро таъсир қилиши мумкин, ўзаро боғлиқ зарралар орасидаги масофа қанчалик катта бўлмасин, улар изоляция қилинганлиги сабабли боғлиқ ҳолда қолади [6].

Квант телепортацияси. Квант ҳолатлари жуда беқарор, агар улар бошқа тизимлар билан ўзаро таъсир қилса ёки тўқнашса, бу уларнинг суперпозиция хусусиятларининг бузилишига ёки ҳатто йўқ қилинишига олиб келади. Классик битлар билан ҳар қандай хатолик юзага келса, квант битлари билан солиштирганда осонликча ҳал қилиш мумкин. Квант телепортацияси номаълум квант ҳолатлари ва ҳимояланган муҳит орқали маълумотларни узатишга қаратилган. Агар келажакда ушбу илова ҳақиқатга айланса, компютер томонидан ишлаб чиқарилган натижаларни телепортация қилиш орқали кириш сифатида фойдаланиш мумкин [7]. Телепортация квант боғланиш хусусиятидан фойдаланади. Бу маълумотни бир нуқтадан иккинчи нуқтага ўтказишда ёрдам беради. Эркин космик квант алоқаси ҳақиқатдир,

чунки алоқа деярли 200 км масофада уланишлар орқали амалга оширилиши мумкин. Бу амалда исботланган [7].

Киберхавфсизликда квант криптографиясининг қўлланилиши:

Квант компьютерларида мавжуд бўлган афзалликлар туфайли RSA, ElGamal ва бошқа очиқ калитлар квант компьютерларида хавфсизроқ бўлмайди. Чунки дискрет логарифм муаммоси ёки бутун сонларни факторизация қилиш каби муаммоларни квант компьютерлари ёрдамида осонгина ечиш мумкин. Шундай қилиб, ушбу тизимларни ҳимоя қилиш учун юқоридаги муаммоларга асосланмаган турли хил криптотизимлар керак [8].

Тармоқ хавфсизлиги ҳам, криптография ҳам ахборот тизимларининг хавфсизлигини таъминлашда муҳим аҳамиятга эга. Киберхавфсизликнинг асосий шартларидан бири квант криптографик протоколларини ўрганишдир [8].

Квант маълумотлари классик маълумотлар эга бўлмаган ўзига хос хусусиятларга эга. Асосан боғланган ҳолатда мавжуд бўлган квант кодлари ҳақидаги маълумотларни олиш қийин [8].

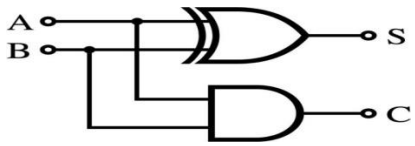
1. Ноаниқлик принципи: Бу тамойил микро дунёда заррачанинг ҳолатини аниқлаш қийинлигини ва шунингдек, заррачаларнинг жойлашуви турли жойларда ҳар хил эканлигини билдиради.

2. Квантсиз клонлаш: Клонлаш – бу бутунлай бошқа ҳолатда бир хил квант заррачасини ишлаб чиқариш. Квант машиналари бу хусусиятни акс эттириши олимлар томонидан исботланган. Квант ҳолатларида тиклаш хусусияти деб аталадиган хусусият ҳам мавжуд. Бу шуни англатадики, заррачани квант ҳолатларида йўқ қилиш ёки шикастлаш алоқа тизимларида из қолдиради. Квант ҳолатининг нусхасини ўчириш квант механикасининг чизиқлилиги сабабли рухсат этилмайди [8].

Квант схемалари – бу квант маълумотлари бўйича изчил квант операцияларини ўз ичига олган ҳисоблаш амалиёти, одатда кубитлар деб номланувчи ва биргаликда мавжуд бўлган реал вақтда классик ҳисоблаш. Бу

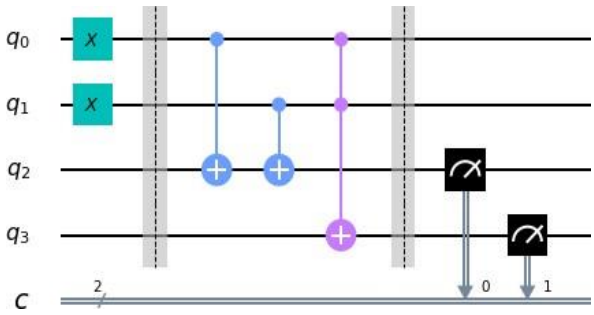
квант эшиклари, ўлчовлари ва қайта ўрнатишларнинг кетма-кет жойлашувидир [8].

Ҳаммаси асосий тасвирдан бошланади, қуйидаги 1-расмда мантиқий ВА, ОР элементлари қўлланиладиган классик схема диаграммаси келтирилган, бу ерда киришлар чап томонида, чиқиш эса схеманинг ўнг томонида жойлашган:



1-расм. Мантиқий AND, OR элементлари қўлланиладиган классик схема диаграммаси.

Худди шу мантиқий схеманинг квант схемаси қуйидагича ифодаланиши мумкин [10]:



2-расм. Мантиқий AND, OR элементларининг квант схемаси.

Квант занжирини қуриш учун қуйидаги учта босқични бажариш керак [9]: 1)киришларни кодлаш; 2) мантиқий ҳисоблашни қўллаш; 3) чиқиш маълумотларини ажратиб олиш.

Ҳар қандай миқдордаги кубитлар билан квант занжирини яратиш мумкин, қуйидаги 3-расмда квант занжирини тасвирлаш учун 5 кубитдан фойдаланилган.

Кубит элементлари. Кубит элементлари матрицаси асосий чизиқли алгебра тамойилларига асосланади. У жуда кенг тарқалган квант элементларини ифодалаш учун ишлатилади.

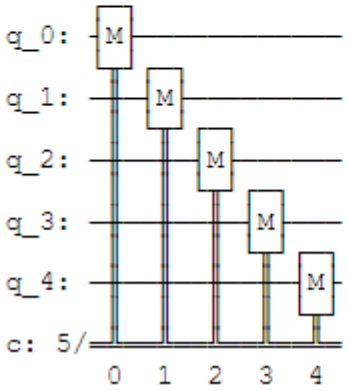
X элементларининг Паули-X матрицаси қуйида кўрсатилган:

$$q = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0|$$

Биз шунчаки кубитнинг ҳолат векторини элементга кўпайтириш орқали элементнинг таъсирини баҳолашимиз мумкин. X-ешик $|0\rangle$ ва $|1\rangle$ ҳолатларнинг амплитудаларини ўзгартириши аниқ кўрсатилган:

$$X|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$$

```
import qiskit as qk
n=5
n_q=n
n_b=n
qc_chiqish=qk.QuantumCircuit(n_q,n_b)
for j in range(n):
    qc_chiqish.measure(j,j)
qc_chiqish.draw()
```



3-расм. 5 кубитли квант занжир схемаси.

plot_bloch_multivector() функсияси ёрдамида кубит ҳолат векторининг ҳақиқий ҳолатини тасаввур қилиш мумкин.

```
from qiskit import*
from math import pi
from qiskit.visualization import plot_bloch_multivector
qc=QuantumCircuit(1)
qc.x(0)
qc.draw()
```

4-расм. Квант элементининг тасвирланиши

Иккита фойдаланувчи мамлакатлар орасидаги масофа нуқтаи назаридан ва юборилаётган маълумотлар қийматидан қатъи назар, маълумотларни нотўғри ишлатиши мумкин бўлган рухсатсиз

фойдаланувчидан ҳимоя қилиш асосий мақсад ҳисобланади. Муаммо бу иккиси ўртасидаги маълумотларни бузмасдан хавфсиз тарзда етказишдир.

Ушбу муаммони жўнатувчи ва қабул қилувчи ўртасида узатиладиган маълумотлар ҳар доим хавфсиз эканлигига ишонч ҳосил қилиш ва рухсатсиз фойдаланувчи маълумотларга кира олмаслигига ишонч ҳосил қилиш орқали ҳал қилиш мумкин. Буни Quantum Key Distribution (QKD) ёрдамида амалга ошириш мумкин.

Натижа. Квант калитларини тақсимлаш квант криптографиясининг бўлими бўлиб, у икки томон, жўнатувчи ва қабул қилувчи ўртасида хавфсиз маълумотларни узатишни таъминлайди. Классик криптография усуллари исботланмаган ҳисоблаш фаразларига таянадиган калит тақсимотига асосланади, Quantum Key Distribution (QKD) эса квант механикаси ҳодисаларини кузатиб боради. Классик криптографияда шунчаки тингловчининг ҳисоблаш қобилияти ишончли. Ушбу усулларда улар фақат рухсатсиз фойдаланувчининг транзит пайтида маълумотларга кириш учун жуда юқори ҳисоблаш ресурсларига эга эмаслигига умид қилишлари мумкин [11].

Квант калитларини тақсимлаш – бу оддий математик муаммоларни ҳисоблаш мураккаблигига асосланган классик криптография ўрнига квант физикаси ҳодисаларига асосланган усул бўлиб, у ҳар қандай одам ҳужум қилиши ва кириши мумкин бўлган хавфсиз бўлмаган алоқа каналида мураккаб шифрлаш калитларини ишлаб чиқади ва тарқатади. Квант калитларини тақсимлаш квант каналининг квант бит хатолик тизими орқали маълумотларга ҳар қандай потенциал рухсатсиз киришни аниқлай оладиган ягона фотон технологиясидан фойдаланишга асосланган.

Quantum Key Distribution (QKD) тизими асосан классик канал ва квант канали бўлган икки турдаги каналларни ўз ичига олади. Классик канал анъанавий IP-канал сифатида кўриб чиқилиши мумкин (оптик канал бўлиши ҳам мумкин). Бу бутунлай тизим дизайнига боғлиқ ва у вақт талабларида фойдаланадиган квант каналига чамбарчас боғлиқ бўлиши мумкин. Квант

канали йўқолган ва эҳтимолли канал бўлиб, у асосан кубитларни (битта фотонларни) узатиш учун ишлатилади ва шаффоф бўлиши керак бўлган оптик йўлдан иборат [12].

Квант калитларини тақсимлаш протоколлари алоқа каналида жўнатувчи ва қабул қилувчи ўртасида ноёб калитларни алмашишни таъминлаш учун ишлатилади. Хавфсиз алоқани ҳатто хавфсиз бўлмаган умумий тармоқда ҳам ушбу ноёб калитлардан фойдаланиш мумкин. Кўпинча нотўғри ишлаб чиқилган калитларни тарқатиш протоколлари хавфсизлик муаммоларидан азият чекади. Шундай қилиб, калитларни тарқатиш протоколини лойиҳалаш алоқа тизимидаги энг устувор вазифадир. Баъзи асосий тарқатиш протоколларида калитларни жўнатувчи ва қабул қилувчига узатувчи Ишончли марказ ((Trusted Centre-TC)) мавжуд. Жўнатувчи, қабул қилувчи ва TCни ўз ичига олган ушбу протоколлар уч томонли тарқатиш протоколлари деб аталади. Бу асосий алмашишлар фақат икки томон ўртасида бўладиган одатий икки томонли протоколга қараганда яхшироқ протокол ҳисобланади [13].

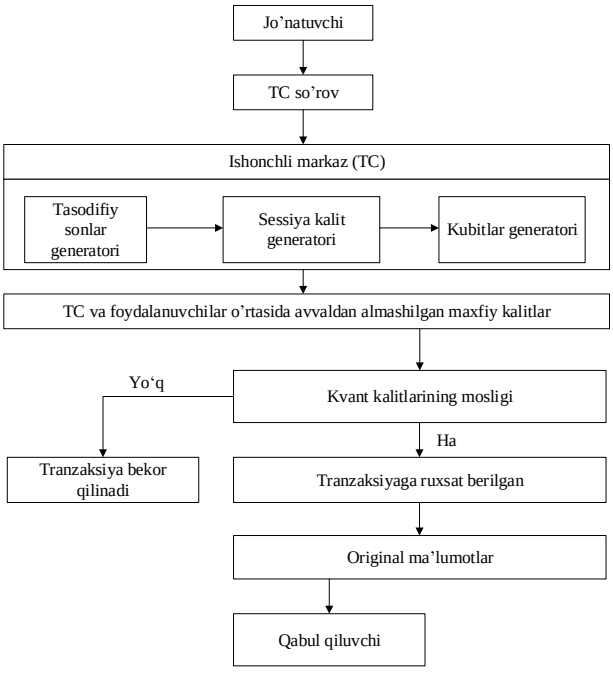
Классик криптографияда такрорий ҳужумларнинг олдини олишда такрорий ҳужумларни аниқлаш учун вақт тамғасидан самарали фойдаланадиган уч томонли калит тарқатиш протоколлари қўлланилади. Бироқ, бу ёндашув ишончли эмас, у ғаразли томон ҳужумлари ва тармоқ кечикишларининг олдиндан айтиб бўлмайдиган табиати туфайли тақсимланган тизимларда деярли имконсиз бўлган соат синхронизацияси тахминига асосланади. Классик криптография одатда, тинглаш деб номланувчи пассив ҳужумларни аниқлай олмаслигининг сабаби ҳам шу ҳисобланади[14].

Квант криптографияси ва классик криптография ўртасидаги асосий фарқ шундан иборатки, квант калитларини тақсимлаш протоколлари (QKDP) тингловчиларни текшириш ва сессия калитининг тўғрилигини текшириш учун сессия калитларини ва оммавий алмашишларни тарқатишда квант механикасидан фойдаланади. Оммавий алмашишларда жўнатувчи ва қабул

қилувчи ўртасида қўшимча алоқа босқичлари талаб қилинади, классик криптографик ёндашувда калитларни текшириш ва фойдаланувчи аутентификацияси учун самаралироқ усуллар мавжуд [15]

Иккита уч томонлама квант калитини тарқатиш протоколлари мавжуд бўлиб, улардан бирида фойдаланувчилар текширилиши мумкин, иккинчиси аниқ умумий аутентификацияга эга, эски услуб ва квант криптографиясини умумлаштиришнинг афзалликларини кўрсатиш учун бирлаштирилган. Классик уч томонли асосий тарқатиш конвенциялари асосида таклиф қилинган QKDP лар такрорий ҳужумларга самарали қаршилик кўрсатади. Ушбу иш Классик протоколларнинг афзалликларини квант криптографияси билан бирлаштириш орқали QKDP ларни ишлаб чиқиш бўйича алоҳида тадқиқот ҳисобланади [16].

Қуйидаги 5-расмда таклиф қилинган уч томонлама QKDP тизими архитектураси тасвирланган:



5-Расм: Уч томонлама QKDP тизими архитектураси.

Архитектурада кўриниб турибдики, таклиф қилинган QKDP ларда ТС ва фойдаланувчи ўзларининг қутбланиш асосларини олдиндан улашилган сирли калитга мувофиқ синхронлаштиради. Шифрлаш калитини яратиш

жараёнида олдиндан улашилган сирли калит ва тасодифий қатор шифрлаш калитини етказиб бериш учун ишлатиладиган бошқа бир калитни ишлаб чиқишда фойдаланилади. Рухсатга эга бўлмаган фойдаланувчи шифрлаш калити қайта узатилишидан қатъи назар, худди шундай қутбланиш кубитига эга бўлмайди.

Хулоса қиладиган бўлсак, квант ҳисоблашда квант криптографияси, маълумотни телепортация қилиш каби кўплаб иловалар мавжуд. Бундан ташқари, молекуляр хатти-ҳаракатларни ўрганиш орқали дори воситаларини ишлаб чиқишда фойдаланиш, шунингдек, сунъий йўлдош алоқаларида ҳам қўлланилиши мумкин. Айтиш жоизки, мазкур назариялар бир кун келиб амалий аҳамиятга молик бўлади. Унинг афзалликларидан фаннинг бошқа кўплаб соҳаларида фойдаланиш мумкин. Мазкур ишда квант технологияларининг криптографияда қўлланилишининг классик криптографиядан афзалликлари очиб берилди. Квант технологияси асосида таклиф қилинган уч томонлама калитларни алмашиш протоколи келтирилди.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР:

1. Gruska, J. (1999). Quantum computing, Citeseer.
2. Gisin, N., et al. (2002). "Quantum cryptography." Reviews of modern physics 74(1): 145.
3. Häffner, H., et al. (2008). "Quantum computing with trapped ions." Physics reports 469(4): 155-203.
4. GUANCO, F. (2015). "What is Quantum Key Distribution." Cloud Security Alliance.
5. Ma, X. (2008). "Quantum cryptography: theory and practice." arXiv preprint arXiv:0808.1385.
6. Jennewein, T., et al. (2000). "Quantum cryptography with entangled photons." Physical review letters 84(20): 4729.
7. Spiller, T. P. (1996). "Quantum information processing: cryptography, computation, and teleportation." Proceedings of the IEEE 84(12): 1719-1746.

8. Zhou, T., et al. (2018). "Quantum cryptography for the future internet and the security analysis." Security and Communication Networks 2018.

9. Politi, A., et al. (2008). "Silica-on-silicon waveguide quantum circuits." Science 320(5876): 646-649.

10. Gu, X., et al. (2017). "Microwave photonics with superconducting quantum circuits." Physics reports 718: 1-102.

11. Lo, H.-K., et al. (2005). "Decoy state quantum key distribution." Physical review letters 94(23): 230504.

12. Gottesman, D., et al. (2004). Security of quantum key distribution with imperfect devices. International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings., IEEE.

13. Shor, P. W. and J. Preskill (2000). "Simple proof of security of the BB84 quantum key distribution protocol." Physical review letters 85(2): 441.

14. Scarani, V., et al. (2009). "The security of practical quantum key distribution." Reviews of modern physics 81(3): 1301.

15. Goyal, A., et al. (2011). Quantum Cryptography & its Comparison with Classical Cryptography: A Review Paper. 5th IEEE International Conference on Advanced Computing & Communication Technologies [ICACCT-2011].

16. Wasankar, M. P. P. and P. Soni (2013). "An invention of quantum cryptography over the classical cryptography for enhancing security." International Journal of Application or Innovation in Engineering & Management (IJAIEM), vol 2.