KVANT KALITLARINI TAQSIMLASH BILAN OPTIK TOLALI ALOQA LINIYALARINING KIBERHIMOYASINI TA'MINLASH

Axmadxonov Afzaliddin Abduvosi o'g'li

O'zbekiston Respublikasi Jamoat xavfsizligi universiteti "Axborot texnologiyalari" kafedrasi o'qituvchisi

Annotatsiya: *Mazkur ilmiy maqola zamonaviy telekommunikatsiya infratuzilmasining muhim yo'nalishlaridan biri bo'lgan kvant kriptografiyasi, xususan, kvant kalitlarini taqsimlash (Quantum Key Distribution — QKD) texnologiyasi asosida optik tolali aloqa liniyalarining kiberhimoyasini ta'minlash masalalariga bag'ishlangan. Axborot xavfsizligi global miqyosda dolzarb muammoga aylangan bir sharoitda, klassik kriptografik algoritmlarning hisoblash quvvatining ortib borishi va kvant kompyuterlar rivoji sababli zaiflashib borayotgani ilmiy jamoatchilik tomonidan keng muhokama qilinmoqda. Shu nuqtai nazardan, kvant mexanikasi qonunlariga asoslangan xavfsiz aloqa texnologiyalarini ishlab chiqish va amaliyotga joriy etish muhim ahamiyat kasb etadi. Maqolada QKD texnologiyasining nazariy asoslari, xususan, kvant holatlarining superpozitsiyasi, noaniqlik printsipi va kvant o'lchov jarayonining axborotga ta'siri kabi fundamental tushunchalar tahlil qilinadi. Shuningdek, BB84 va E91 kabi asosiy QKD protokollarining ishlash prinsiplari ilmiy asoslangan holda bayon etiladi. Ushbu protokollar yordamida kalitlarni uzatishda uchinchi tomon aralashuvini aniqlash imkoniyati mavjudligi ko'rsatib beriladi, bu esa klassik kriptografiyaga nisbatan tubdan yangi xavfsizlik paradigmasini shakllantiradi. Optik tolali aloqa liniyalarida QKD texnologiyasini joriy etishning texnik jihatlari ham maqolada batafsil yoritilgan. Jumladan, fotonlarning susayishi, dispersiya, shovqinlar va detektorlarning samaradorligi kabi muammolar ko'rib chiqiladi. Shu bilan birga, real telekommunikatsiya tizimlarida QKD integratsiyasining arxitektura yechimlari va mavjud cheklovlar tahlil qilinadi. Maqolada zamonaviy tajribalar va amaliy*

loyihalar, jumladan, Yevropa, Xitoy va AQShda amalga oshirilgan kvant aloqa tarmoqlari haqida qisqacha ilmiy sharh beriladi.

KIRISH

XXI asrda axborot texnologiyalarining jadal rivojlanishi, raqamli iqtisodiyotning shakllanishi va global tarmoqlarning kengayishi natijasida axborot xavfsizligi masalasi strategik ahamiyat kasb etuvchi yo‘nalishga aylandi. Zamonaviy jamiyatda davlat boshqaruvi, moliya tizimi, harbiy infratuzilma va sanoat tarmoqlarining aksariyati raqamli platformalar asosida faoliyat yuritmoqda. Shu sababli uzatilayotgan ma’lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta’minlash kiberxavfsizlikning asosiy vazifalaridan biri sifatida qaraladi. Biroq klassik kriptografik tizimlar, jumladan RSA va ECC kabi algoritmlar, hozirgi kunda hisoblash quvvatining oshishi va ayniqsa kvant kompyuterlarining paydo bo‘lishi fonida o‘zining nisbiy barqarorligini yo‘qotib bormoqda.

Kvant hisoblash texnologiyalarining rivojlanishi Shor algoritmi kabi samarali usullar yordamida katta sonlarni tez faktorizatsiya qilish imkonini bermoqda, bu esa ochiq kalitli kriptografiya tizimlarining xavfsizligini jiddiy xavf ostiga qo‘yadi. Shu nuqtai nazardan, yangi avlod kriptografik yondashuvlar, xususan kvant mexanikasi qonunlariga asoslangan usullarni ishlab chiqish zarurati yuzaga kelmoqda. Kvant kalitlarini taqsimlash (QKD) texnologiyasi aynan shunday yondashuvlardan biri bo‘lib, u fundamental fizik qonunlarga tayangan holda mutlaq xavfsizlikni ta’minlash imkonini beradi.

QKD texnologiyasining asosiy afzalligi shundaki, u axborot uzatish jarayonida uchinchi tomon aralashuvini aniqlash imkonini beradi. Bu kvant mexanikasining asosiy prinsiplari — superpozitsiya va o‘lchash jarayonining tizim holatiga ta’siri bilan bog‘liq. Ya’ni, agar tajovuzkor kvant kanal orqali uzatilayotgan fotonlarni kuzatishga harakat qilsa, bu holat tizim parametrlarida o‘zgarish keltirib chiqaradi va qonuniy foydalanuvchilar tomonidan aniqlanadi. Shu sababli QKD texnologiyasi nazariy jihatdan “mutlaq xavfsiz” aloqa vositasi sifatida qaraladi.

Optik tolali aloqa liniyalari bugungi kunda global telekommunikatsiya infratuzilmasining asosini tashkil etadi. Ular yuqori tezlikda katta hajmdagi

ma’lumotlarni uzatish imkonini beradi va elektromagnit shovqinlarga nisbatan yuqori chidamlilikka ega. Shu bilan birga, optik tolali tarmoqlarda axborot xavfsizligini ta’minlash masalasi dolzarbligicha qolmoqda. Ayniqsa, tolali kanallar orqali uzatilayotgan ma’lumotlarga noqonuniy kirish, signallarni tahlil qilish va yashirin tinglash kabi tahdidlar mavjud. Shu sababli optik aloqa tizimlariga kvant kriptografiyasini integratsiya qilish ilmiy va amaliy jihatdan muhim vazifa hisoblanadi.

Kvant kalitlarini taqsimlash texnologiyasining nazariy asoslari va fizik prinsiplari.

Kvant kalitlarini taqsimlash (QKD) texnologiyasi zamonaviy kiberxavfsizlik tizimlarida tub burilish yasagan yo‘nalishlardan biri bo‘lib, uning nazariy asoslari kvant mexanikasining fundamental qonunlariga tayanadi. Klassik kriptografiya matematik murakkablikka asoslangan bo‘lsa, QKD tizimlari fizik qonunlar bilan himoyalanganligi sababli mutlaqo yangi xavfsizlik paradigmasini taqdim etadi. Ushbu texnologiyaning ishonchliligi kvant tizimlarining o‘ziga xos xususiyatlari, jumladan superpozitsiya holati, kvant o‘lchovining buzuvchi ta’siri va noaniqlik prinsipi bilan bevosita bog‘liqdir.

Kvant mexanikasida har qanday zarra, xususan foton, bir vaqtning o‘zida bir nechta holatda mavjud bo‘lishi mumkin. Bu hodisa superpozitsiya deb ataladi va QKD tizimlarida axborotni kodlash uchun asosiy mexanizm sifatida ishlatiladi. Masalan, fotonning qutblanish holati orqali ikkilik (0 va 1) qiymatlar ifodalanadi. Shu bilan birga, kvant tizimining o‘lchanishi uning dastlabki holatini o‘zgartirib yuboradi. Bu esa aloqa kanalida yashirin tinglash (eavesdropping) holatlarini aniqlash imkonini beradi.

QKD texnologiyasining eng muhim fizik asoslaridan biri bu Hezenberg noaniqlik prinsipi hisoblanadi. Ushbu prinsipga ko‘ra, kvant tizimining ayrim juft parametrlarini bir vaqtning o‘zida aniq o‘lchash mumkin emas. Bu esa axborotni uzatishda uchinchi tomonning aralashuvini muqarrar ravishda aniqlashga olib keladi. Mazkur prinsip matematik jihatdan quyidagicha ifodalanadi:

$$\Delta x \cdot \Delta p \geq \frac{\hbar}{2}$$

Bu yerda Δx — zarra koordinatasining noaniqligi, Δp — impulsning noaniqligi, $\hbar$ esa Plank doimiysining kamaytirilgan qiymatini anglatadi. Ushbu tengsizlik kvant tizimlarining fundamental chegarasini belgilaydi va QKD tizimlarida xavfsizlikning fizik asosini tashkil etadi.

QKD tizimlarida odatda ikki asosiy tomon ishtirok etadi: uzatuvchi (an'anaviy ravishda "Alice") va qabul qiluvchi ("Bob"). Ular o'rtasida kvant kanal (odatda optik tolali aloqa liniyasi) va klassik aloqa kanali mavjud bo'ladi. Kvant kanal orqali fotonlar uzatiladi, klassik kanal esa ochiq bo'lib, kalitlarni moslashtirish va xatoliklarni tuzatish uchun xizmat qiladi. Agar uchinchi tomon ("Eve") kvant kanalga aralashsa, u holda tizimda xatoliklar darajasi ortadi va bu holat qonuniy foydalanuvchilar tomonidan aniqlanadi.

Eng keng tarqalgan QKD protokollaridan biri BB84 protokoli bo'lib, u 1984-yilda Charles Bennett va Gilles Brassard tomonidan taklif qilingan. Ushbu protokol fotonlarning turli bazislar (masalan, to'g'ri va diagonal qutblanish) yordamida kodlanishiga asoslanadi. Alice tasodifiy bitlar ketma-ketligini generatsiya qiladi va har bir bitni tasodifiy tanlangan bazisda kodlaydi. Bob esa kelayotgan fotonlarni o'zining tasodifiy tanlangan bazisida o'lchaydi. Keyinchalik ular klassik kanal orqali o'z bazislarini taqqoslaydi va mos kelgan holatlarda kalitni shakllantiradi.

QKD tizimlarining yana bir muhim xususiyati bu kvant xatolik darajasi (QBER) orqali kanalning xavfsizligini baholash imkoniyatidir. Agar QBER ma'lum bir chegaradan oshsa, bu tizimda tashqi aralashuv mavjudligini bildiradi. Shu sababli QKD tizimlari nafaqat kalitlarni taqsimlaydi, balki ularning xavfsizligini real vaqt rejimida nazorat qiladi.

Nazariy jihatdan QKD tizimlari mutlaq xavfsizlikni ta'minlaydi, biroq amaliyotda turli texnik cheklovlar mavjud. Jumladan, fotonlarning yo'qolishi, detektorlarning samaradorligi, shovqinlar va kvant kanallarining uzunligi kabi omillar tizim samaradorligiga ta'sir ko'rsatadi. Shu sababli zamonaviy tadqiqotlar

ushbu muammolarni minimallashtirish va QKD tizimlarini real telekommunikatsiya infratuzilmasiga moslashtirishga qaratilgan.

QKD protokollari va ularning ishlash mexanizmlari.

Kvant kalitlarini taqsimlash texnologiyasining amaliy qo‘llanilishi, avvalo, uning asosini tashkil etuvchi protokollar orqali amalga oshiriladi. Ushbu protokollar kvant mexanikasining fundamental qonunlariga asoslanib, ikki tomon o‘rtasida mutlaqo xavfsiz kalit almashish imkonini beradi. QKD protokollari ichida eng keng tarqalganlari BB84 va E91 protokollari bo‘lib, ular turli fizik prinsiplarga asoslangan holda yuqori darajadagi xavfsizlikni ta’minlaydi. Mazkur qismda ushbu protokollarning ishlash mexanizmlari, afzalliklari va cheklovlari ilmiy jihatdan tahlil qilinadi.

BB84 protokoli kvant kriptografiyasining ilk va eng muhim protokollaridan biri hisoblanadi. U fotonlarning qutblanish holatlari yordamida axborotni kodlashga asoslangan. Ushbu protokolda Alice tomonidan generatsiya qilingan tasodifiy bitlar ketma-ketligi ikki xil bazis — to‘g‘ri (rektilinear) va diagonal bazislar orqali kodlanadi. Har bir bit uchun bazis ham tasodifiy tanlanadi. Bob esa kelayotgan fotonlarni o‘zining mustaqil tanlangan bazisida o‘lchaydi. Natijada, faqat Alice va Bob tomonidan bir xil bazis tanlangan hollardagina to‘g‘ri bitlar olinadi.

Protokolning keyingi bosqichida Alice va Bob klassik kanal orqali o‘z bazislarini taqqoslaydi va mos kelmagan o‘lchov natijalarini chiqarib tashlaydi. Bu jarayon “sifting” deb ataladi. Natijada qolgan bitlar xom kalitni tashkil etadi. Shundan so‘ng xatoliklarni aniqlash va tuzatish (error correction) hamda maxfiylikni kuchaytirish (privacy amplification) bosqichlari amalga oshiriladi. Agar tizimda uchinchi tomon aralashuvi mavjud bo‘lsa, bu holat xatoliklar darajasining ortishi orqali aniqlanadi.

E91 protokoli esa kvant chigalashuv (entanglement) hodisasiga asoslanadi va 1991-yilda Artur Ekert tomonidan taklif qilingan. Ushbu protokolda ikkita chigalashgan zarra (odatda fotonlar) jufti hosil qilinadi va ular Alice hamda Bobga yuboriladi. Chigalashgan zarrachalar orasidagi korrelyatsiya shunday kuchliki, ular orasidagi o‘lchov natijalari klassik fizikadan farqli ravishda Bell tengsizliklarini

buzadi. Bu holat tizimda tashqi aralashuv yo‘qligini tasdiqlovchi mezon sifatida xizmat qiladi.

E91 protokolining asosiy ustunligi shundaki, u xavfsizlikni kvant chigalashuvning fundamental xususiyatlariga asoslab beradi. Agar uchinchi tomon tizimga aralashsa, u holda zarrachalar orasidagi kvant korrelyatsiya buziladi va bu Bell tengsizliklari orqali aniqlanadi. Shu sababli ushbu protokol nazariy jihatdan yanada kuchliroq xavfsizlik kafolatlarini taqdim etadi.

QKD protokollarining samaradorligini baholashda muhim ko‘rsatkichlardan biri bu maxfiy kalit generatsiya tezligi hisoblanadi. Ushbu ko‘rsatkich tizimning real sharoitda qanchalik samarali ishlashini ifodalaydi va u kanal xatoliklari hamda tashqi aralashuv ehtimoli bilan chambarchas bog‘liqdir. Maxfiy kalit tezligi quyidagi umumiy ko‘rinishdagi formula orqali ifodalanadi:

$$R = Q[1 - 2H(e)]$$

Bu yerda R — maxfiy kalit tezligi, Q — qabul qilingan signal ulushi (gain), e — kvant bit xatolik darajasi (QBER), H(e) esa binar entropiya funksiyasini anglatadi. Ushbu formula shuni ko‘rsatadiki, tizimdagi xatoliklar darajasi oshgan sari foydali kalit tezligi kamayadi. Agar xatolik darajasi ma’lum chegaradan oshib ketsa, tizim umuman xavfsiz kalit generatsiya qila olmaydi.

Amaliy jihatdan QKD protokollarini joriy etishda bir qator muammolar mavjud. Jumladan, real qurilmalarda ideal kvant holatlarni hosil qilish va aniqlash qiyin, detektorlar cheklangan samaradorlikka ega va shovqinlar mavjud. Bundan tashqari, optik tolali kanallarda signalning susayishi uzoq masofalarda kalit almashuv tezligini keskin kamaytiradi. Shu sababli zamonaviy tadqiqotlar kvant takrorlagichlar (quantum repeaters) va yangi turdagi detektorlarni ishlab chiqishga qaratilgan.

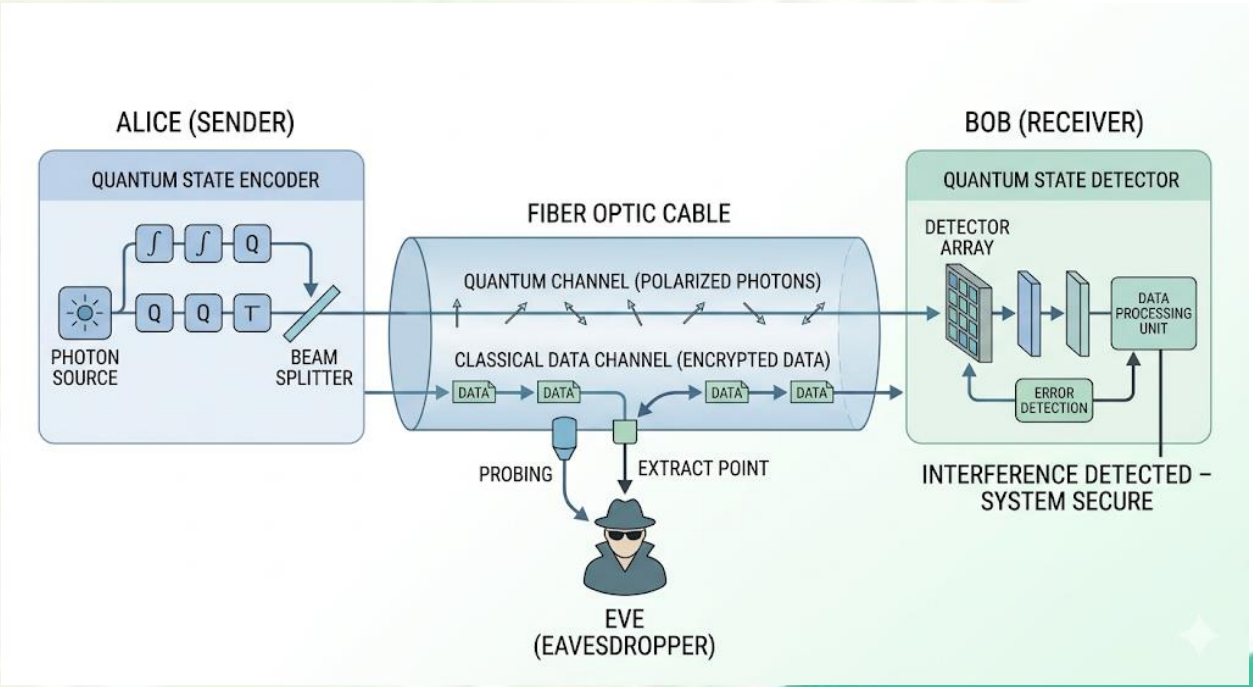
Shuningdek, QKD tizimlarining xavfsizligi faqat nazariy model bilan cheklanib qolmaydi, balki amaliy hujumlarga ham bardosh bera olishi kerak. Masalan, “photon number splitting” (PNS) hujumi yoki detektorlarni aldashga qaratilgan hujumlar real tizimlarda xavf tug‘dirishi mumkin. Shu sababli zamonaviy

QKD protokollari ushbu tahdidlarga qarshi qo‘shimcha himoya mexanizmlarini ham o‘z ichiga oladi.

QKD texnologiyasini optik tolali aloqa liniyalariga integratsiya qilish va texnik muammolar.

Kvant kalitlarini taqsimlash texnologiyasini real telekommunikatsiya infratuzilmasiga joriy etish masalasi, ayniqsa optik tolali aloqa liniyalari kontekstida, zamonaviy ilmiy tadqiqotlarning eng muhim yo‘nalishlaridan biri hisoblanadi. Optik tolali aloqa tizimlari bugungi kunda global ma’lumot uzatish tarmoqlarining asosini tashkil etadi va yuqori tezlik, katta o‘tkazuvchanlik hamda past yo‘qotish kabi afzalliklarga ega. Shu sababli QKD texnologiyasini aynan shu infratuzilma bilan integratsiya qilish kiberxavfsizlikni yangi bosqichga olib chiqish imkonini beradi.

QKD tizimlarini optik tolali liniyalarga integratsiya qilishda asosiy element sifatida kvant kanal va klassik kanalning birgalikda ishlashi ko‘zda tutiladi. Kvant kanal orqali alohida fotonlar uzatiladi, ular orqali maxfiy kalit shakllantiriladi. Klassik kanal esa ochiq bo‘lib, u orqali bazislarni taqqoslash, xatoliklarni tuzatish va maxfiylikni kuchaytirish jarayonlari amalga oshiriladi. Bunday ikki kanalli arxitektura tizimning barqaror ishlashini ta’minlaydi, biroq uni amaliyotga joriy etishda bir qator muhim texnik muammolar yuzaga keladi (1-rasm).



1-rasm. Optik tolali aloqa liniyasida QKD texnologiyasini joriy etishning funksional sxemasi: Alice (uzatuvchi) va Bob (qabul qiluvchi) o‘rtasidagi kvant va klassik kanallarning integratsiyasi hamda uchinchi tomon (Eve) aralashuvini real vaqt rejimida aniqlash mexanizmi.

Eng asosiy muammolardan biri bu optik tolada signalning susayishidir. Optik tolalar orqali uzatilayotgan fotonlar masofa ortishi bilan energiyasini yo‘qotadi, bu esa qabul qilinayotgan signalning kuchsizlanishiga olib keladi. Natijada, uzoq masofalarda kvant kalitlarini samarali taqsimlash qiyinlashadi. Ushbu jarayon matematik jihatdan quyidagi eksponensial qonun bilan ifodalanadi:

$$P(L) = P_0 e^{-\alpha L}$$

Bu yerda $P(L)$ — L masofadan keyingi signal quvvati, P_0 — boshlang‘ich signal quvvati, α — optik tolaga xos susayish koeffitsienti, L sa uzatish masofasini anglatadi. Ushbu formula shuni ko‘rsatadiki, masofa ortishi bilan signal eksponensial ravishda kamayadi, bu esa QKD tizimlarining maksimal ishlash masofasini cheklaydi.

Yana bir muhim muammo — bu shovqinlar va tashqi ta’sirlar hisoblanadi. Optik tolali kanallarda termik shovqinlar, fon nurlanishi va detektorlarning noto‘g‘ri ishlashi kvant bit xatolik darajasini (QBER) oshiradi. Bu esa tizimning xavfsizligiga bevosita ta’sir qiladi. Agar xatolik darajasi kritik chegaradan oshsa, QKD tizimi xavfsiz kalit generatsiya qila olmaydi. Shu sababli yuqori aniqlikka ega foton detektorlari va shovqinlarni minimallashtiruvchi texnologiyalarni ishlab chiqish muhim ahamiyatga ega.

QKD tizimlarini optik tarmoqlarga integratsiya qilishda dispersiya hodisasi ham muhim rol o‘ynaydi. Dispersiya tufayli turli chastotadagi signal komponentlari turli tezlikda tarqaladi, bu esa signal impulslarining kengayishiga olib keladi. Natijada, ketma-ket uzatilayotgan fotonlar bir-biriga aralashib ketishi mumkin, bu esa o‘lchov natijalarining aniqligini pasaytiradi. Ayniqsa yuqori tezlikda ishlovchi tizimlarda bu muammo yanada dolzarb hisoblanadi.

Amaliy jihatdan yana bir murakkablik — bu mavjud optik tarmoqlar bilan moslashuv masalasidir. Hozirgi telekommunikatsiya infratuzilmasi asosan klassik

signal uzatishga mo‘ljallangan bo‘lib, kvant signallar juda past quvvatda uzatiladi. Shu sababli ularni bir xil tolada uzatish jarayonida klassik signallardan kelib chiqadigan shovqinlar kvant signallarni buzishi mumkin. Buni hal qilish uchun spektral ajratish (wavelength division multiplexing — WDM) texnologiyalaridan foydalaniladi, ya’ni kvant va klassik signallar turli to‘lqin uzunliklarida uzatiladi.

QKD tizimlarining yana bir muhim cheklovi bu kvant takrorlagichlarning yetarlicha rivojlanmaganligidir. Klassik aloqa tizimlarida signal kuchaytirgichlar yordamida uzoq masofalarga uzatiladi, biroq kvant signallarni oddiy kuchaytirish mumkin emas, chunki bu kvant holatini buzadi. Shu sababli kvant takrorlagichlar ishlab chiqilmoqda, ular kvant chigalashuv va kvant xotira texnologiyalariga asoslanadi. Ammo hozirgi kunda bu texnologiyalar hali to‘liq amaliy bosqichga yetmagan.

Shu bilan birga, optik tolali QKD tizimlari bo‘yicha dunyo miqyosida qator muvaffaqiyatli loyihalar amalga oshirilgan. Masalan, Xitoyda Pekin va Shanxay shaharlarini bog‘lovchi kvant aloqa liniyasi ishga tushirilgan bo‘lib, u minglab kilometr masofada xavfsiz kalit almashuvini ta’minlaydi. Yevropa va AQShda ham kvant tarmoqlarini yaratish bo‘yicha keng ko‘lamli ilmiy tadqiqotlar olib borilmoqda.

QKD asosida kiberxavfsizlikni baholash va matematik modellashtirish

Kvant kalitlarini taqsimlash texnologiyasining samaradorligini chuqur tahlil qilish va uning real sharoitdagi kiberxavfsizlik darajasini aniqlash matematik modellashtirish usullarini qo‘llashni talab etadi. QKD tizimlari nazariy jihatdan mutlaq xavfsizlikni ta’minlasa-da, amaliyotda turli fizik va texnik omillar ularning ishlashiga ta’sir ko‘rsatadi. Shu sababli tizimning barqarorligi, xavfsizlik darajasi va samaradorligini baholash uchun ehtimollik nazariyasi, axborot nazariyasi va statistik tahlil metodlaridan keng foydalaniladi.

QKD tizimlarida kiberxavfsizlikni baholashning asosiy mezonlaridan biri bu kvant bit xatolik darajasi (Quantum Bit Error Rate — QBER) hisoblanadi. Ushbu ko‘rsatkich uzatilgan va qabul qilingan bitlar orasidagi nomuvofiqlik darajasini ifodalaydi. Agar tizimda uchinchi tomon aralashuvi mavjud bo‘lsa yoki shovqin

darajasi yuqori bo‘lsa, QBER qiymati ortadi. Shu sababli QBER ni real vaqt rejimida kuzatish QKD tizimlarining xavfsizligini nazorat qilishda muhim vosita hisoblanadi.

Matematik jihatdan QBER quyidagi ifoda orqali aniqlanadi:

$$QBER = \frac{N_{error}}{N_{total}}$$

Bu yerda N_{error} — noto‘g‘ri qabul qilingan bitlar soni, N_{total} esa umumiy uzatilgan bitlar sonini anglatadi. Ushbu formula yordamida tizimdagi xatolik darajasi aniqlanadi va u xavfsizlik chegaralari bilan taqqoslanadi. Odatda, agar QBER ma’lum kritik qiymatdan (masalan, 11% atrofida) oshsa, tizim xavfsiz deb hisoblanmaydi va kalitlar rad etiladi.

QKD tizimlarida xavfsizlikni baholash faqat xatolik darajasi bilan cheklanmaydi, balki axborot nazariyasiga asoslangan yondashuvlar ham muhim ahamiyatga ega. Xususan, entropiya tushunchasi tizimdagi axborotning noaniqlik darajasini ifodalaydi. Agar tajovuzkor tizim haqida ma’lumot olishga harakat qilsa, u holda qonuniy foydalanuvchilar va tajovuzkor o‘rtasidagi axborot miqdori farqi kamayadi. Shu sababli maxfiy kalitni shakllantirish jarayonida ushbu farqni maksimal darajada oshirish muhim hisoblanadi.

Matematik modellashtirish jarayonida yana bir muhim tushuncha bu o‘zaro axborot (mutual information) hisoblanadi. Bu ko‘rsatkich Alice va Bob o‘rtasidagi axborot miqdori bilan Alice va ehtimoliy tajovuzkor (Eve) o‘rtasidagi axborot miqdorini solishtirish imkonini beradi. Agar Alice va Bob o‘rtasidagi axborot ustun bo‘lsa, tizim xavfsiz kalit generatsiya qila oladi.

QKD tizimlarida xavfsizlikni ta’minlashning muhim bosqichlaridan biri bu maxfiylikni kuchaytirish (privacy amplification) jarayonidir. Bu bosqichda xom kalitdan ehtimoliy tajovuzkor ega bo‘lishi mumkin bo‘lgan axborot qismlari matematik transformatsiyalar yordamida chiqarib tashlanadi. Natijada qisqaroq, ammo yuqori darajada xavfsiz kalit hosil bo‘ladi. Ushbu jarayon odatda xesh funksiyalar va tasodifiy matritsalar yordamida amalga oshiriladi.

Amaliy tizimlarda matematik modellashtirish nafaqat xavfsizlikni baholash, balki tizim parametrlarini optimallashtirish uchun ham qo‘llaniladi. Masalan,

fotonlar intensivligini tanlash, detektorlarning sezgirligini sozlash va signal uzatish tezligini optimallashtirish kabi masalalar matematik modellarga asoslanadi. Bu esa tizimning maksimal samaradorlik bilan ishlashini ta’minlaydi.

Shuningdek, QKD tizimlarining xavfsizligini baholashda turli hujum modellari ham hisobga olinadi. Jumladan, individual hujumlar, kollektiv hujumlar va koherent hujumlar kabi turli ssenariylar matematik jihatdan modellashtiriladi. Har bir hujum turiga qarshi tizimning barqarorligi alohida tahlil qilinadi va tegishli himoya mexanizmlari ishlab chiqiladi.

Zamonaviy ilmiy tadqiqotlarda QKD tizimlarini baholash uchun Monte-Karlo simulyatsiyalari, statistik testlar va kompyuter modellashtirish usullaridan keng foydalanilmoqda. Bu usullar yordamida turli sharoitlarda tizimning ishlashi oldindan prognoz qilinadi va optimal konfiguratsiyalar aniqlanadi.

XULOSA

Mazkur tadqiqot natijalari shuni ko‘rsatadiki, kvant kalitlarini taqsimlash (QKD) texnologiyasi optik tolali aloqa liniyalarida kiberxavfsizlikni ta’minlashning istiqbolli va fundamental jihatdan ishonchli yechimidir. QKD tizimlari klassik kriptografiyadan farqli ravishda matematik murakkablikka emas, balki kvant mexanikasining buzilmas qonunlariga asoslanadi, bu esa ularni nazariy jihatdan mutlaq xavfsiz qiladi. Tadqiqot davomida kvant superpozitsiyasi, noaniqlik prinsipi va kvant o‘lchovining buzuvchi xususiyati kabi fizik asoslar QKD xavfsizligining poydevorini tashkil etishi ilmiy jihatdan asoslab berildi.

Asosiy qismda ko‘rib chiqilgan BB84 va E91 protokollari QKD texnologiyasining amaliy mexanizmlarini namoyon qilib, ularning turli fizik yondashuvlarga asoslangan holda yuqori darajadagi xavfsizlikni ta’minlashi ko‘rsatildi. Shu bilan birga, optik tolali aloqa liniyalarida QKD ni joriy etishda signalning susayishi, shovqinlar va texnik cheklovlar kabi muammolar mavjudligi aniqlandi. Matematik modellashtirish orqali esa QBER va maxfiy kalit tezligi kabi parametrlar asosida tizim xavfsizligini baholash mumkinligi isbotlandi.

Umuman olganda, QKD texnologiyasini optik telekommunikatsiya infratuzilmasiga integratsiya qilish zamonaviy kiberxavfsizlik talablariga javob

beruvchi innovatsion yondashuv hisoblanadi. Ushbu texnologiyani yanada takomillashtirish va amaliyotga keng joriy etish kelajakda global miqyosda ishonchli va himoyalangan aloqa tizimlarini yaratishda muhim ilmiy-amaliy asos bo‘lib xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI:

1. Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 175–179.
2. Ekert, A. K. (1991). Quantum cryptography based on Bell’s theorem. Physical Review Letters, 67(6), 661–663.
3. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M. (2009). The security of practical quantum key distribution. Reviews of Modern Physics, 81(3), 1301–1350.
4. Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. Reviews of Modern Physics, 74(1), 145–195.
5. Lo, H.-K., Curty, M., & Tamaki, K. (2014). Secure quantum key distribution. Nature Photonics, 8(8), 595–604.
6. Pirandola, S., Andersen, U. L., Banchi, L., et al. (2020). Advances in quantum cryptography. Advances in Optics and Photonics, 12(4), 1012–1236.
7. Xu, F., Ma, X., Zhang, Q., Lo, H.-K., & Pan, J.-W. (2020). Secure quantum key distribution with realistic devices. Reviews of Modern Physics, 92(2), 025002.
8. Townsend, P. D. (1997). Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing. Electronics Letters, 33(3), 188–190.
9. Elliott, C. (2002). Building the quantum network. New Journal of Physics, 4, 46.
10. Sasaki, M., Fujiwara, M., Ishizuka, H., et al. (2011). Field test of quantum key distribution in the Tokyo QKD Network. Optics Express, 19(11), 10387–10409.
11. Peev, M., Pacher, C., Alléaume, R., et al. (2009). The SECOQC quantum key distribution network in Vienna. New Journal of Physics, 11, 075001.

12. Takesue, H., Sasaki, M., Tamaki, K., & Sakai, Y. (2007). Experimental quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors. Nature Photonics, 1(6), 343–348.

13. Agrawal, G. P. (2012). Fiber-Optic Communication Systems (4th ed.). Wiley.

14. Nielsen, M. A., & Chuang, I. L. (2010). Quantum Computation and Quantum Information. Cambridge University Press.

15. Diamanti, E., Lo, H.-K., Qi, B., & Yuan, Z. (2016). Practical challenges in quantum key distribution. npj Quantum Information, 2, 16025.

Internet manbaalar:

1. Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. IBM Research. https://research.ibm.com/publications/quantum-cryptography-public-key-distribution-and-coin-tossing

2. European Telecommunications Standards Institute (ETSI). (2023). Quantum Key Distribution (QKD); Overview. https://www.etsi.org/technologies/quantum-key-distribution

3. National Institute of Standards and Technology (NIST). (2022). Quantum Information Science (QIS). https://www.nist.gov/quantum-information-science

4. ID Quantique. (2024). Quantum Key Distribution – Technology and Applications. https://www.idquantique.com/quantum-safe-security/quantum-key-distribution

5. Toshiba Quantum Technology Division. (2023). Quantum Key Distribution (QKD) solutions. https://www.global.toshiba/ww/products-solutions/security-ict/qkd.html

6. Centre for Quantum Technologies (National University of Singapore). (2023). Quantum Cryptography. https://www.quantumlah.org/research/quantum-cryptography

7. SECOQC Project (Secure Communication based on Quantum Cryptography). (2008). Final Report. https://cordis.europa.eu/project/id/506813

8. Nature Photonics Journal. (2020). Secure quantum key distribution with realistic devices. https://www.nature.com/articles/s41566-020-0610-y

9. Optica Publishing Group. (2011). Tokyo QKD Network field test. https://opg.optica.org/oe/fulltext.cfm?uri=oe-19-11-10387

10. arXiv.org. (2020). Advances in quantum cryptography. https://arxiv.org/abs/1906.01645

11. Quantum Flagship (European Union). (2024). Quantum Communication Infrastructure (QCI). https://digital-strategy.ec.europa.eu/en/policies/quantum-communication-infrastructure