Modern education and development
ISSN: 3060-4567

TARMOQLARDA KVANT KRIPTOGRAFIYASI ISTIQBOLLARI
ПЕРСПЕКТИВЫ КВАНТОВОЙ КРИПТОГРАФИИ В СЕТЯХ
PROSPECTS OF QUANTUM CRYPTOGRAPHY IN NETWORKS

Ibragimov Sh.M.[1], Ismoilova H. A.[2]

[1]*FarDU dotsenti, shavkat19702008@gmail.com*

[2]*FarDU talabasi, xulkaroyismoilova443@gmail.com*

Annotatsiya: *Ushbu maqolada tarmoqlarda kvant kriptografiyasining rivojlanish istiqbollari va uning axborot xavfsizligini ta'minlashdagi ahamiyati o'rganildi. Tadqiqot davomida kvant kalit taqsimoti (QKD) texnologiyasining ishlash prinsiplari, an'anaviy kriptografiyadan ustun jihatlari hamda ma'lumotlarni yuqori darajada himoyalash imkoniyatlari tahlil qilindi. Shuningdek, kvant kriptografiyasini amaliy tarmoqlarga joriy etishdagi texnik va iqtisodiy muammolar ham ko'rib chiqildi. Maqolada ushbu texnologiyaning bank tizimlari, davlat axborot resurslari va zamonaviy kiberxavfsizlik infratuzilmalaridagi istiqbollari yoritildi.*

Kalit so'zlar: *kvant kriptografiyasi, QKD, kvant kalit taqsimoti, axborot xavfsizligi, kompyuter tarmoqlari, kvant mexanikasi, kiberxavfsizlik, shifrlash, ma'lumotlarni himoyalash, tarmoq xavfsizligi.*

Аннотация: *В данной статье исследуются перспективы развития квантовой криптографии в сетях и её значение в обеспечении информационной безопасности. В ходе исследования проанализированы принципы работы технологии квантового распределения ключей (QKD), её преимущества по сравнению с классической криптографией, а также возможности обеспечения высокого уровня защиты данных. Также рассмотрены технические и экономические проблемы внедрения квантовой криптографии в реальные сетевые системы. В статье освещены перспективы применения данной технологии в банковских системах,*

государственных информационных ресурсах и современных инфраструктурах кибербезопасности.

Ключевые слова: *квантовая криптография, QKD, квантовое распределение ключей, информационная безопасность, компьютерные сети, квантовая механика, кибербезопасность, шифрование, защита данных, сетевая безопасность.*

Abstract: *This article explores the prospects of quantum cryptography in networks and its importance in ensuring information security. The study analyzes the principles of Quantum Key Distribution (QKD), its advantages over classical cryptography, and its capabilities for providing a high level of data protection. Technical and economic challenges of implementing quantum cryptography in real network systems are also considered. The article highlights the future applications of this technology in banking systems, government information resources, and modern cybersecurity infrastructures.*

Keywords: *quantum cryptography, QKD, quantum key distribution, information security, computer networks, quantum mechanics, cybersecurity, encryption, data protection, network security.*

KIRISH

Kvant kriptografiyasi axborot xavfsizligi sohasida nisbatan yangi, ammo juda tez rivojlanayotgan yo‘nalishlardan biri hisoblanadi. Uning ilmiy asoslari XX asrning ikkinchi yarmida kvant mexanikasi rivojlanishi bilan shakllana boshlagan. Ayniqsa, 1980–1990-yillarda kvant holatlarining o‘lchash jarayoniga ta’siri va “no-klonlash teoremasi” kabi fizik qonuniyatlar ma’lumotlarni uzatishda mutlaq xavfsizlikka erishish g‘oyasini paydo qildi. Shu asosda kvant kalit taqsimoti (QKD) konsepsiyasi ishlab chiqildi va u klassik kriptografik usullarga muqobil yondashuv sifatida shakllandi.

Bugungi kunda raqamli texnologiyalar tez sur’atlar bilan rivojlanayotgan bir paytda axborot xavfsizligi masalasi yanada dolzarb ahamiyat kasb etmoqda. An’anaviy shifrlash algoritmlari hisoblash quvvatining oshishi va kvant kompyuterlarning paydo bo‘lishi bilan zaiflashishi mumkinligi sababli, yangi

xavfsizlik mexanizmlariga ehtiyoj ortib bormoqda. Shu nuqtayi nazardan kvant kriptografiyasi ma’lumotlarni buzib bo‘lmaydigan darajada himoyalash imkonini beruvchi istiqbolli yo‘nalish sifatida qaralmoqda.

Mazkur maqolada kvant kriptografiyasining tarmoqlardagi o‘rni, uning ishlash prinsiplari, klassik kriptografiyaga nisbatan afzalliklari hamda amaliyotga joriy etish jarayonidagi mavjud muammolar tahlil qilinadi. Shuningdek, ushbu texnologiyaning kelajakdagi rivojlanish istiqbollari va turli sohalarda qo‘llanilish imkoniyatlari yoritiladi.

ADABIYOTLAR TAHLILI VA USULLAR

Kvant kriptografiyasi bo‘yicha dastlabki nazariy asoslar 1980-yillarda shakllana boshlagan. 1984-yilda C. Bennett va G. Brassard tomonidan ishlab chiqilgan BB84 protokoli kvant kalit taqsimotining birinchi amaliy modeli sifatida ilmiy jamoatchilik tomonidan keng e’tirof etildi. Ushbu yondashuvda kvant holatlar orqali kalit uzatish g‘oyasi ilgari surilib, tinglash (eavesdropping) aniqlanganda tizim avtomatik ravishda xatolikni sezishi mumkinligi isbotlangan. Bu kvant kriptografiyasining asosiy afzalliklaridan biri sifatida tarixga kirdi.

1990-yillarda Artur Ekert tomonidan E91 protokoli taklif qilindi. Ushbu model Bell tengsizliklariga asoslangan bo‘lib, kvant chigallashuv (entanglement) hodisasi orqali xavfsiz aloqa yaratish imkonini berdi. Bu yondashuv BB84 dan farqli ravishda kvant zarrachalarining o‘zaro bog‘liqligidan foydalanishi bilan yangi ilmiy bosqichni boshlab berdi. Shu davrda kvant aloqa tizimlarining nazariy chegaralari va xavfsizlik kafolatlari chuqur o‘rganildi.

2000-yillardan boshlab N. Gisin va uning hamkorlari kvant kriptografiyasining amaliy qo‘llanilishi bo‘yicha keng qamrovli tadqiqotlar olib bordi. Ularning ishlari kvant optikasi va foton uzatish texnologiyalariga asoslanib, real optik tolali tarmoqlarda QKD tizimlarini sinovdan o‘tkazishga qaratilgan edi. Bu bosqichda asosiy yangilik kvant kalit uzatishning laboratoriyadan amaliy telekommunikatsiya tizimlariga o‘tishi bo‘ldi.

2010-yillardan keyin kvant kriptografiyasi sohasida sezilarli yutuqlar kuzatildi. Xitoylik tadqiqotchilar (Jian-Wei Pan guruhi) tomonidan 2017-yilda

“Micius” sun’iy yo‘ldoshi orqali kvant aloqa tajribasi amalga oshirildi. Ushbu loyiha kvant kalitlarni kosmik masofalarda uzatish mumkinligini amalda isbotlab berdi va global kvant aloqa tarmoqlari konsepsiyasini shakllantirdi.

So‘nggi yillarda (2020-yildan hozirgacha) kvant kriptografiyasi sun’iy intellekt va klassik tarmoq infratuzilmalari bilan integratsiya qilinmoqda. Tadqiqotchilar kvant kalit taqsimotini SDN (Software Defined Networking) arxitekturasi bilan birlashtirish orqali tarmoqlarda avtomatik xavfsizlik boshqaruvini yaratish ustida ishlamoqda. Shuningdek, post-kvant kriptografiya yo‘nalishi ham rivojlanib, kvant kompyuterlarga chidamli algoritmlar ishlab chiqilmoqda.

Adabiyotlar tahlili asosida kvant kriptografiyasining rivojlanish bosqichlari, asosiy protokollari va zamonaviy yondashuvlari o‘rganildi. Usul sifatida nazariy tahlil, qiyosiy taqqoslash va ilmiy manbalarni sistematik o‘rganish metodlaridan foydalanildi. Shu orqali kvant kriptografiyasining evolyutsiyasi va uning amaliy tarmoqlardagi o‘rni kompleks tarzda baholandi.

MUHOKAMA

Kvant kriptografiyasi zamonaviy tarmoqlarda axborot xavfsizligini ta’minlashning eng istiqbolli yo‘nalishlaridan biri hisoblanadi, biroq uning amaliy joriy etilishida bir qator texnik cheklovlar mavjud. Eng asosiy muammo kvant signallarining uzoq masofaga uzatilishida yo‘qotishlar yuzaga kelishi va tashqi shovqinlar ta’sirida signal sifatining pasayishidir. Bundan tashqari, kvant uskunalarining murakkabligi hamda yuqori narxi uning keng qo‘llanishini cheklab turadi.

Ushbu muammolarni bartaraf etish uchun turli yondashuvlar ishlab chiqilgan. “Trusted Node” modeli kvant kalitlarni oraliq tugunlar orqali uzatishga asoslanadi. Bu usul mavjud optik tarmoqlarda oson qo‘llaniladi va uzatish masofasini kengaytiradi, biroq har bir tugunda xavfsizlikka ishonch talab qilinishi hamda markazlashgan xavf nuqtalarining mavjudligi uning zaif tomonidir.

Sun’iy yo‘ldosh asosidagi kvant kalit taqsimoti esa global miqyosda xavfsiz aloqa yaratish imkonini beradi va atmosferadagi yo‘qotishlarni kamaytiradi. Lekin

ushbu yondashuv juda katta iqtisodiy xarajat talab qiladi va tashqi sharoitlarga bog‘liq.

Quantum Repeater modeli kvant signallarini yo‘qotmasdan uzoq masofalarga uzatishga mo‘ljallangan bo‘lib, yuqori xavfsizlikni ta’minlaydi. Ammo bu texnologiya hali to‘liq amaliy bosqichga chiqmagan va murakkab texnik tizimlarni talab qiladi.

Gibrid kvant-klassik yondashuv esa kvant kalitlarni an’anaviy kriptografiya bilan birlashtiradi. U amaliyotga tez joriy etilishi bilan ajralib turadi, biroq to‘liq kvant xavfsizligini ta’minlamaydi.

Tadqiqot doirasida **Adaptiv kvant-gibrid kalit boshqaruv modeli (AQGKBM)** ishlab chiqildi. Ushbu model kvant kriptografiyasini klassik tarmoq tizimlari bilan moslashtirib, dinamik boshqaruv tamoyiliga asoslanadi. Tizim uch qatlamdan iborat: kvant kalit generatsiyasi, adaptiv marshrutlash va klassik shifrlash qatlami.

Kvant qatlamida kalitlar QKD orqali yaratiladi, biroq ular darhol uzatilmaydi, balki tarmoq yuklamasi va xavfsizlik holatiga qarab optimallashtiriladi. Adaptiv qatlam esa real vaqt rejimida eng samarali yo‘nalishni tanlaydi. Klassik qatlam esa ushbu kalitlar yordamida ma’lumotlarni shifrlaydi.

Ushbu modelning asosiy afzalligi uning moslashuvchanligidir. Tarmoq yuklamasi oshganda tizim avtomatik ravishda marshrutni o‘zgartiradi va xavfsizlik darajasini yangilaydi. Bu esa paket yo‘qolishini kamaytiradi va barqarorlikni oshiradi. Bundan tashqari, kvant kanal faqat zarur holatlarda ishlashi sababli resurslar samarali foydalaniladi.

Shu bilan birga, modelning ayrim kamchiliklari ham mavjud. U yuqori hisoblash quvvatini talab qiladi, chunki tarmoq holatini doimiy kuzatish zarur. Shuningdek, kvant va klassik qatlamlarni sinxronlashtirish murakkab jarayon bo‘lib, kechikishlarni yuzaga keltirishi mumkin.

Kvant kriptografiyasi tarmoqlarida xavfsizlik va samaradorlik ko‘rsatkichlarining qiyosiy tahlili.

1-jadval

Mezonlar	**Trusted Node**	**Sun’iy yo‘ldosh QKD**	**Quantum Repeater**	**Gibrid model**	**AQGKBM**
Xavfsizlik	O‘rtacha	Yuqori	Juda yuqori	O‘rtacha–yuqori	Juda yuqori
Masofa	O‘rtacha	Juda yuqori	Juda yuqori	O‘rtacha	Yuqori
Murakkablik	O‘rtacha	Juda yuqori	Juda yuqori	Past–o‘rtacha	O‘rtacha
Xarajat	O‘rtacha	Juda yuqori	Yuqori	Past	O‘rtacha
Barqarorlik	O‘rtacha	Yuqori	Yuqori	O‘rtacha	Juda yuqori
Moslashuvchanlik	Past	O‘rtacha	O‘rtacha	Yuqori	Juda yuqori

Jadval natijalari shuni ko‘rsatadiki, an’anaviy yondashuvlar ma’lum sohalarda samarali bo‘lsa-da, zamonaviy tarmoqlarning yuqori talablariga to‘liq javob bera olmaydi. Trusted Node modeli amaliy jihatdan qulay, biroq xavfsizlik jihatidan cheklangan. Sun’iy yo‘ldosh QKD global aloqa uchun juda samarali, lekin xarajatlari yuqori. Quantum Repeater kelajakda eng kuchli yechim bo‘lishi mumkin, ammo hozircha to‘liq ishlab chiqilmagan.

Taklif etilgan AQGKBM modeli esa moslashuvchanlik, xavfsizlik va resurs samaradorligini birlashtirgan holda real tarmoqlarda qo‘llash uchun qulayroq yechim sifatida ajralib turadi. Maqolada kvant kriptografiyasining rivojlanish yo‘nalishlari, mavjud muammolar va ularni hal etish usullari tahlil qilindi. Shuningdek, yangi adaptiv model ishlab chiqilib, uning an’anaviy yondashuvlarga nisbatan ustun va cheklovli jihatlari ko‘rsatib berildi. Olingan natijalar kvant kriptografiyasining kelajakda tarmoq xavfsizligida muhim o‘rin egallashini tasdiqlaydi va adaptiv yondashuvlar uning amaliy samaradorligini oshirishga xizmat qilishini ko‘rsatadi.

NATIJALAR

O‘tkazilgan tahlillar kvant kriptografiyasi tarmoq xavfsizligini ta’minlashda klassik yondashuvlardan tubdan farq qilishini ko‘rsatdi. Kvant kalit taqsimoti asosida ishlovchi tizimlar nazariy jihatdan tinglash yoki kalitni yashirin olish imkoniyatini deyarli yo‘qqa chiqaradi, bu esa axborot almashinuvining ishonchlilik darajasini sezilarli oshiradi. Shu bilan birga, mavjud yechimlar amaliy tarmoqlarda to‘liq barqaror ishlashi uchun hali bir qator texnik cheklovlarni yengib o‘tishi zarurligi aniqlandi.

Tadqiqot davomida aniqlanishicha, an’anaviy kriptografik tizimlar yuqori hisoblash quvvatiga ega hujumlarga nisbatan zaiflashib bormoqda. Ayniqsa, kvant kompyuterlar rivojlanishi fonida RSA va ECC kabi algoritmlarning kelajakdagi xavfsizlik darajasi pasayishi ehtimoli kuchaymoqda. Bu holat kvant asosidagi himoya mexanizmlariga o‘tish zaruratini yanada dolzarb qilib qo‘ymoqda.

Taklif etilgan Adaptiv kvant–gibrid kalit boshqaruv modeli (AQGKBM) natijalarini tahlil qilish shuni ko‘rsatdiki, u mavjud yondashuvlarga nisbatan bir nechta amaliy ustunliklarga ega. Birinchidan, kvant va klassik qatlamlarning birgalikda ishlashi natijasida tizim faqat zarur holatlarda kvant kanalidan foydalanadi, bu esa resurs sarfini kamaytiradi. Ikkinchidan, adaptiv marshrutlash mexanizmi tarmoq yuklamasiga qarab avtomatik moslashadi, natijada uzatishdagi kechikishlar va paket yo‘qolish holatlari kamayadi.

Shuningdek, model real tarmoq sharoitlarida xavfsizlik darajasini barqaror ushlab turish imkonini beradi. Tizimda kvant kalitlar dinamik ravishda yangilanib borishi sababli, hujumchilar uchun barqaror kalitni qo‘lga kiritish imkoniyati keskin kamayadi. Bu esa bank tizimlari, davlat ma’lumot bazalari va yuqori xavfsizlik talab qilinadigan platformalar uchun muhim afzallik hisoblanadi.

Amaliy jihatdan olib qaralganda, AQGKBM modeli joriy etilgan tarmoqlarda quyidagi ijobiy natijalar kuzatilishi mumkin: ma’lumot uzatish xavfsizligining oshishi, tarmoq yuklamasining muvozanatlashuvi, kechikishlarning kamayishi hamda resurslardan samaraliroq foydalanish. Ayniqsa, gibrid yondashuv mavjud

infratuzilmalarga to‘liq qayta qurishsiz integratsiya qilinishi mumkinligi uni iqtisodiy jihatdan ham maqbul qiladi.

Biroq, natijalar tahlili shuni ham ko‘rsatdiki, modelning samarali ishlashi yuqori darajadagi hisoblash resurslarini talab qiladi. Tarmoq holatini doimiy kuzatish va kvant–klassik sinxronizatsiya jarayonlari qo‘shimcha yuklama hosil qiladi. Bu jihat hozirgi bosqichda uning keng ko‘lamli joriy etilishiga ma’lum darajada cheklov qo‘yadi.

Qo’shimchasiga aytganda, tadqiqot natijalari kvant kriptografiyasining tarmoqlarda nafaqat nazariy, balki amaliy ahamiyati ham ortib borayotganini tasdiqlaydi. Taklif etilgan yondashuv esa kelajakda xavfsiz, moslashuvchan va resurs jihatdan optimallashtirilgan tarmoq infratuzilmalarini yaratish uchun muhim asos bo‘lib xizmat qilishi mumkin.

XULOSA

Ushbu maqola kvant kriptografiyasining zamonaviy tarmoqlarda axborot xavfsizligini ta’minlashdagi o‘rni va rivojlanish istiqbollarini kompleks tarzda yoritib berdi. Tadqiqot davomida kvant kalit taqsimoti asosidagi texnologiyalar klassik kriptografik yondashuvlardan sezilarli darajada farq qilishi, ayniqsa xavfsizlik darajasi va ma’lumot uzatishning ishonchliligi jihatidan ustun ekanligi aniqlandi. Shu bilan birga, mavjud yechimlar hali to‘liq amaliy bosqichga chiqmaganligi va bir qator texnik cheklovlarga ega ekani ham ko‘rsatib berildi.

Shu bilan bir qatorda, kvant kriptografiyasining tarixiy shakllanish jarayoni, asosiy ilmiy protokollari hamda zamonaviy tadqiqot yo‘nalishlari tahlil qilindi. Ushbu jarayonda sohaning rivojlanishi faqat nazariy emas, balki amaliy tajribalar orqali ham boyib borayotgani, xususan sun’iy yo‘ldoshlar va optik tarmoqlar orqali o‘tkazilgan tajribalar muhim bosqich bo‘lib xizmat qilgani ta’kidlandi. Natijalar kvant texnologiyalarining global tarmoq xavfsizligi uchun istiqbolli yo‘nalish ekanini yana bir bor tasdiqladi.

Shuningdek, maqolaning asosiy maqsadi sifatida kvant kriptografiyasini mavjud tarmoq infratuzilmalari bilan moslashtirish va uning samaradorligini oshirish yo‘llarini aniqlash belgilangan edi. Shu asosda taklif etilgan adaptiv gibrid model

kvant va klassik yondashuvlarni uyg‘unlashtirib, tarmoq xavfsizligi va resurs samaradorligini oshirish imkonini berishi ko‘rsatildi. Umuman olganda, ushbu tadqiqot kvant kriptografiyasining kelajakda axborot xavfsizligi sohasida muhim o‘rin egallashini va uning amaliy tatbiqi yanada kengayishini asoslab berdi.

FOYDALANILGAN ADABIYOTLAR

1. Bennett C.H., Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 1984. – P. 175–179.
2. Ekert A.K. Quantum cryptography based on Bell’s theorem. Physical Review Letters, 1991. – P. 661–663.
3. Gisin N., Ribordy G., Tittel W., Zbinden H. Quantum cryptography. Reviews of Modern Physics, 2002. – P. 145–195.
4. Nielsen M.A., Chuang I.L. Quantum Computation and Quantum Information. Cambridge University Press, 2010. – P. 250–420.
5. Scarani V., Bechmann-Pasquinucci H. et al. The security of practical quantum key distribution. Reviews of Modern Physics, 2009. – P. 1301–1350.
6. Shor P.W. Algorithms for quantum computation: discrete logarithms and factoring. Proceedings of 35th Annual Symposium on Foundations of Computer Science, 1994. – P. 124–134.
7. Kurose J.F., Ross K.W. Computer Networking: A Top-Down Approach. Pearson, 2021. – P. 300–410.
8. Tanenbaum A.S., Wetherall D.J. Computer Networks. Pearson, 2011. – P. 250–380.