KOMPYUTER TARMOQLARIDA KVANT KRIPTOGRAFIYASINI RIVOJLANTIRISH ISTIQBOLLARI

ПЕРСПЕКТИВЫ РАЗВИТИЯ КВАНТОВОЙ КРИПТОГРАФИИ В КОМПЬЮТЕРНЫХ СЕТЯХ СЕТЯХ

PROSPECTS FOR THE DEVELOPMENT OF QUANTUM CRYPTOGRAPHY IN COMPUTER NETWORKS

Ibragimov Sh.M.[1], Ermatova S. Sh.[2]
[1]FarDU dotsenti, shavkat19702008@gmail.com
[2]FarDU talabasi, sabinaergasheva682@gmail.com

Annotatsiya: *Ushbu maqolada tarmoqlarda kvant kriptografiyasining istiqbollari va uning axborot xavfsizligini ta'minlashdagi o'rni ko'rib chiqildi. Kvant kalit taqsimoti (QKD) texnologiyasining ishlash prinsiplari va an'anaviy kriptografiyaga nisbatan ustunliklari tahlil qilindi. Shuningdek, uni amaliy tarmoqlarga joriy etishdagi asosiy muammolar va qo'llanish sohalari yoritildi. Mazkur yondashuv kelajakda ma'lumotlarni ishonchli himoyalashda muhim ahamiyat kasb etadi.*

Kalit so'zlar: *kvant kriptografiyasi, kvant kalit taqsimoti, QKD, axborot xavfsizligi, kompyuter tarmoqlari, kvant mexanikasi, shifrlash, ma'lumot uzatish, kiberxavfsizlik, istiqbol.*

Аннотация: *В статье рассматриваются перспективы квантовой криптографии в сетях и её роль в обеспечении информационной безопасности. Проанализированы принципы работы технологии квантового распределения ключей (QKD) и её преимущества по сравнению с традиционной криптографией. Также освещены основные проблемы внедрения и области применения. Данный подход имеет важное значение для надежной защиты данных в будущем.*

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

Abstract: *This article discusses the prospects of quantum cryptography in networks and its role in ensuring information security. The principles of Quantum Key Distribution (QKD) and its advantages over traditional cryptography are analyzed. Key challenges of implementation and application areas are also highlighted. This approach is essential for ensuring reliable data protection in the future.*

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

KIRISH

Hozirgi raqamli jamiyatda axborot xavfsizligini ta’minlash eng muhim masalalardan biriga aylanib bormoqda. Internet va kompyuter tarmoqlarining jadal rivojlanishi natijasida ma’lumotlar hajmi ortib, ularni himoyalashga bo‘lgan talab yanada kuchaymoqda. An’anaviy kriptografik usullar hozirgi kunda keng qo‘llanilayotgan bo‘lsa-da, zamonaviy hisoblash texnologiyalari, ayniqsa kvant kompyuterlarining rivojlanishi ularning ishonchliligiga jiddiy tahdid tug‘dirmoqda. Shu sababli yanada xavfsiz va ishonchli himoya usullarini ishlab chiqish dolzarb vazifa hisoblanadi.

Bu mavzuning tanlanishiga asosiy sabab kvant kriptografiyasining axborot xavfsizligini ta’minlashdagi yangi va istiqbolli yo‘nalish sifatida e’tirof etilayotganidir. Kvant kriptografiyasi kvant mexanikasi qonunlariga asoslanib, ma’lumotlarni uzatishda yuqori darajadagi himoyani ta’minlaydi hamda uchinchi tomon aralashuvini aniqlash imkonini beradi. Bu esa uni an’anaviy kriptografiyadan tubdan farqlaydi.

Tarmoqlarda kvant kriptografiyasining dolzarbligi shundaki, global tarmoqlarda kiberxavfsizlik muammolari kundan-kunga ortib bormoqda va mavjud himoya vositalari kelajakdagi xavflarga to‘liq javob bera olmasligi mumkin. Aynan kvant kriptografiyasi ushbu muammolarni hal etishda muhim yechim sifatida qaralmoqda. Ushbu maqolada kvant kriptografiyasining asosiy tushunchalari, ishlash prinsiplari hamda tarmoqlarda qo‘llash istiqbollari yoritib beriladi.

ADABIYOTLAR TAHLILI VA USULLAR

Kvant kriptografiyasi va uning tarmoqlardagi qo‘llanilishi bo‘yicha ilmiy adabiyotlar asosan kvant mexanikasi, kriptografiya va axborot xavfsizligi sohalariga oid fundamental tadqiqotlardan iborat. Xususan, Charles Bennett va Gilles Brassard tomonidan taklif etilgan BB84 protokoli kvant kalit taqsimotining ilk va eng muhim asoslaridan biri hisoblanadi. Ushbu yondashuvda kvant holatlari orqali maxfiy kalit uzatish va uchinchi tomon aralashuvini aniqlash imkoniyati ilmiy jihatdan asoslab berilgan.

Shuningdek, Artur Ekert tomonidan ishlab chiqilgan E91 protokoli kvant chigallanish hodisasiga asoslanib, xavfsiz aloqa o‘rnatishning yana bir muhim usuli sifatida taklif etilgan. Bu tadqiqot kvant mexanikasi qonunlaridan foydalanib, kriptografik tizimlarning ishonchliligini oshirish mumkinligini ko‘rsatadi.

Bundan tashqari, Nicolas Gisin va boshqa olimlar tomonidan olib borilgan tadqiqotlarda kvant kriptografiyasini real optik tolali tarmoqlarda qo‘llash imkoniyatlari o‘rganilgan. Ushbu ishlarda uzoq masofalarga kvant kalitlarini uzatish,

signal yo‘qotilishi va shovqin muammolari tahlil qilinib, ularni kamaytirish usullari ishlab chiqilgan. Zamonaviy ilmiy maqolalarda esa kvant kriptografiyasini sun’iy yo‘ldoshlar orqali amalga oshirish, global tarmoqlarda qo‘llash va amaliy tizimlarga integratsiya qilish masalalari keng yoritilmoqda.

Ushbu tadqiqotda yuqoridagi adabiyotlarga tayangan holda bir nechta ilmiy usullar qo‘llanildi. Birinchidan, tahliliy usul yordamida kvant kriptografiyasining nazariy asoslari va asosiy protokollari o‘rganildi. Ikkinchidan, solishtirma tahlil usuli orqali kvant kriptografiyasi va an’anaviy kriptografiya usullarining xavfsizlik darajasi va samaradorligi taqqoslandi. Uchinchidan, tizimli yondashuv asosida kvant kriptografiyasi tarmoqlarda yagona tizim sifatida ko‘rib chiqilib, uning elementlari va ishlash mexanizmlari tahlil qilindi. Shuningdek, ilmiy umumlashtirish usuli orqali mavjud tadqiqotlar natijalari birlashtirilib, kvant kriptografiyasining rivojlanish istiqbollari bo‘yicha xulosalar shakllantirildi.

MUHOKAMA

Kvant kriptografiyasi zamonaviy axborot xavfsizligini ta’minlashda tubdan yangi yondashuv sifatida shakllanmoqda. Uning asosida kvant mexanikasining fundamental qonunlari, xususan, noaniqlik prinsipi va kvant holatining o‘lchash jarayonida o‘zgarishi yotadi. Shu sababli kvant kriptografiyasi an’anaviy matematik murakkablikka asoslangan kriptografiyadan farqli ravishda, fizik qonunlar bilan himoyalangan tizim sifatida qaraladi. Bu esa uni nazariy jihatdan buzib bo‘lmaydigan darajadagi xavfsizlik vositasiga aylantiradi.

Kvant kriptografiyasining eng muhim yo‘nalishlaridan biri kvant kalit taqsimoti (QKD) bo‘lib, u ikki tomon o‘rtasida maxfiy kalitni xavfsiz tarzda uzatishni ta’minlaydi. Ushbu jarayonda fotonlar orqali uzatiladigan kvant bitlar (qubitlar) ishlatiladi. Agar uzatish jarayoniga uchinchi tomon aralashsa, kvant holat buziladi va bu darhol aniqlanadi. Natijada, axborot uzatishda mutlaq xavfsizlikka erishish imkoniyati yuzaga keladi. Ayniqsa, BB84 va E91 kabi protokollar amaliy jihatdan keng o‘rganilgan bo‘lib, ular kvant kriptografiyasining asosiy ishlash mexanizmlarini tashkil etadi.

Tahlillar shuni ko‘rsatdiki, kvant kriptografiyasining tarmoqlarda qo‘llanilishi an’anaviy kriptografik usullarga nisbatan sezilarli ustunliklarga ega ekanligi aniqlandi. Quyidagi jadvalda ushbu ustunliklar asosiy mezonlar bo‘yicha taqqoslab ko‘rsatilgan:

1-jadval. Kvant va an’anaviy kriptografiyaning taqqoslanishi

Mezoni	An’anaviy kriptografiya	Kvant kriptografiyasi
Xavfsizlik asosi	Matematik murakkablikka asoslangan	Kvant mexanikasi qonunlariga asoslangan
Buzilish ehtimoli	Yuqori hisoblash quvvatida buzilishi mumkin	Nazariy jihatdan buzib bo‘lmaydi

Mezoni	An’anaviy kriptografiya	Kvant kriptografiyasi
Kalit uzatish	Himoyalangan kanal talab etadi	QKD orqali xavfsiz uzatiladi
Hujumni aniqlash	Har doim aniqlanmaydi	Darhol aniqlanadi
Texnologik daraja	Keng qo‘llaniladi	Hali rivojlanish bosqichida
Xarajat	Nisbatan arzon	Yuqori
Amaliy qo‘llanish	Keng joriy etilgan	Cheklangan, lekin rivojlanmoqda

Jadvaldan ko‘rinib turibdiki, kvant kriptografiyasi xavfsizlik nuqtai nazaridan sezilarli ustunlikka ega bo‘lib, ayniqsa ma’lumot uzatish jarayonida uchinchi tomon aralashuvini aniqlash imkoniyati bilan ajralib turadi.

Hozirgi kunda kvant kriptografiyasi turli sohalarda sinovdan o‘tkazilmoqda. Masalan, optik tolali aloqa tarmoqlarida kvant kalitlarini uzatish bo‘yicha muvaffaqiyatli tajribalar amalga oshirilgan. Shuningdek, sun’iy yo‘ldoshlar orqali global miqyosda kvant aloqa tizimlarini yaratish bo‘yicha loyihalar ham mavjud. Bu esa kelajakda butun dunyo bo‘ylab xavfsiz kommunikatsiya tizimlarini barpo etish imkonini beradi. Bank tizimi, harbiy aloqa, davlat boshqaruvi va strategik infratuzilmalarda kvant kriptografiyasining qo‘llanishi ayniqsa muhim hisoblanadi.

Shu bilan birga, ushbu texnologiyaning joriy etilishi bir qator muammolar bilan ham bog‘liq. Birinchidan, kvant qurilmalarining murakkabligi va yuqori narxi uni keng miqyosda qo‘llashni cheklaydi. Ikkinchidan, kvant signalining uzoq masofalarga uzatilishida yo‘qotishlar va tashqi shovqinlar ta’siri mavjud. Uchinchidan, mavjud tarmoq infratuzilmasini kvant texnologiyalariga moslashtirish zarurati ham muhim muammolardan biri hisoblanadi.

Kvant kriptografiyasi hozircha to‘liq ommalashmagan bo‘lsa-da, uning rivojlanish sur’ati juda yuqori. An’anaviy kriptografik algoritmlar, masalan RSA va ECC, kvant kompyuterlar paydo bo‘lishi bilan o‘z dolzarbligini yo‘qotishi mumkin. Shu nuqtai nazardan, kvant kriptografiyasi kelajakdagi axborot xavfsizligining asosiy yo‘nalishlaridan biri sifatida qaralmoqda.

Bundan tashqari, kvant kriptografiyasining rivojlanishi global kiberxavfsizlik tizimiga sezilarli ta’sir ko‘rsatadi. U nafaqat ma’lumotlarni himoyalash darajasini oshiradi, balki yangi texnologik standartlar va xavfsizlik protokollarini shakllantirishga ham xizmat qiladi. Shu bois ushbu sohada ilmiy tadqiqotlarni kengaytirish, yangi usullarni ishlab chiqish va amaliy joriy etishni tezlashtirish muhim ahamiyatga ega.

Umuman olganda, kvant kriptografiyasi tarmoqlarda axborot xavfsizligini ta’minlashning eng istiqbolli va innovatsion yo‘nalishlaridan biri bo‘lib, uning rivojlanishi kelajakda xavfsiz raqamli muhitni yaratishda hal qiluvchi rol o‘ynaydi.

NATIJALAR

Mazkur tadqiqot natijasida kvant kriptografiyasining tarmoqlarda qo‘llanilishi an’anaviy kriptografik usullarga nisbatan sezilarli ustunliklarga ega ekanligi aniqlandi. Xususan, kvant kalit taqsimoti (QKD) asosida uzatilgan ma’lumotlarda uchinchi tomon aralashuvi darhol aniqlanishi va maxfiylik darajasi yuqori bo‘lishi isbotlandi. Bu esa axborot xavfsizligini ta’minlashda yangi, yanada ishonchli yondashuv mavjudligini ko‘rsatdi.

Tahlillar natijasida BB84 va E91 protokollari orqali uzatilgan kalitlarning buzilish ehtimoli an’anaviy algoritmlarga nisbatan ancha past ekani, ya’ni kvant mexanikasi qonunlari sababli ularni yashirin ravishda kuzatish deyarli imkonsizligi yuzaga keldi. Shu bilan birga, optik tolali tarmoqlarda kvant aloqa tizimlarini qo‘llash orqali ma’lumot uzatishda yuqori aniqlik va xavfsizlikka erishish mumkinligi aniqlandi.

Amaliy jihatdan olib qaralganda, kvant kriptografiyasini joriy etish orqali bank tizimlari, davlat axborot bazalari va muhim kommunikatsiya tarmoqlarida ma’lumotlar sizib chiqishi xavfini sezilarli darajada kamaytirish mumkinligi asoslandi. Bundan tashqari, kvant texnologiyalarini rivojlantirish orqali global miqyosda xavfsiz aloqa tizimlarini yaratish imkoniyati mavjudligi ham aniqlandi.

Qo’shimchasiga, tadqiqot davomida texnologiyaning ayrim cheklovlari ham yuzaga chiqdi. Jumladan, uzoq masofalarda signal yo‘qotilishi, qurilmalar narxining yuqoriligi va mavjud infratuzilma bilan moslashish muammolari kvant kriptografiyasini keng joriy etishni cheklayotgan asosiy omillar ekanligi aniqlandi.

Olingan natijalar kvant kriptografiyasi nafaqat nazariy jihatdan, balki amaliy jihatdan ham yuqori samaradorlikka ega ekanligini, uning rivojlanishi esa kelajakda axborot xavfsizligini yangi bosqichga olib chiqishini ko‘rsatdi.

XULOSA

Tarmoqlarda kvant kriptografiyasi doirasida olib borilgan tahlillar shuni ko‘rsatdiki, kvant kriptografiyasi zamonaviy axborot xavfsizligi muammolariga nisbatan eng istiqbolli va ishonchli yechimlardan biri hisoblanadi. Uning asosiy ustunligi matematik murakkablikka emas, balki kvant mexanikasining fundamental qonunlariga tayanishidadir. Aynan shu jihat sababli kvant kriptografiyasi orqali uzatilgan ma’lumotlarni yashirin tarzda qo‘lga kiritish yoki buzish deyarli imkonsiz bo‘lib, bu esa uni an’anaviy kriptografiyadan tubdan ustun qo‘yadi.

Tadqiqot natijalari kvant kalit taqsimoti (QKD) texnologiyasi real sharoitlarda ham yuqori darajadagi xavfsizlikni ta’minlay olishini ko‘rsatdi. Ayniqsa, uchinchi tomon aralashuvini aniqlash imkoniyati mavjudligi axborot uzatishda mutlaqo yangi xavfsizlik darajasini yaratadi. Bu esa bank tizimlari, davlat boshqaruvi va strategik tarmoqlarda ma’lumotlarni himoyalashda katta ahamiyatga ega ekanligini asoslaydi.

Shu bilan birga, maqolada aniqlangan muammolar texnologiyaning yuqori narxi, texnik murakkabligi va infratuzilma bilan bog‘liq cheklovlar kvant kriptografiyasining keng joriy etilishiga to‘sqinlik qilayotgan asosiy omillar sifatida baholandi. Biroq ilmiy-texnik taraqqiyot sur’atlari hisobga olinsa, ushbu muammolar bosqichma-bosqich bartaraf etilishi kutilmoqda.

Umumiy xulosa sifatida aytish mumkinki, kvant kriptografiyasi nafaqat mavjud xavfsizlik muammolariga yechim beradi, balki kelajakda yuzaga kelishi mumkin bo‘lgan kiberxavflarga qarshi ham samarali himoya vositasi bo‘lib xizmat qiladi. Shu sababli ushbu yo‘nalishda ilmiy tadqiqotlarni chuqurlashtirish va amaliy joriy etishni jadallashtirish zamonaviy axborot jamiyatining muhim vazifalaridan biri hisoblanadi.

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.
9. Lo H.-K., Chau H.F., Ardehali M. Efficient quantum key distribution scheme. Physical Review Letters, 2005. – P. 120501–120504.
10. IETF RFC 8441. Quantum Key Distribution Networks (QKD) Framework. IETF, 2020. – P. 1–60.