KVANT KRIPTOGRAFIYASINING KOMPYUTER TARMOQLARIDA QO'LLANILISHI ISTIQBOLLARI

IBRAGIMOV SH.M., SOLIJONOVA G.S.

FarDU dotsenti, shavkat70@bk.ru,

FarDU talabasi gulsanamsolijonova18@gmail.com

Annotatsiya. Ushbu tadqiqotning maqsadi kvant kriptografiyasining zamonaviy kompyuter tarmoqlarida qo'llanilishi istiqbollarini tahlil qilishdir. Tadqiqot metodlari sifatida adabiyotlar tahlili, qiyosiy tahlil va amaliy tatbiq misollarini o'rganish usullari qo'llanildi. Tadqiqot natijalari shuni ko'rsatadiki, BB84 protokoli va kvant kalitlarini taqsimlash (QKD) texnologiyalari klassik kriptografiyadan mutlaq xavfsizlik, tinglashni darhol aniqlash va kvant kompyuterlariga chidamlilik jihatidan ustun turadi. Xulosa sifatida kvant kriptografiyasi kelajakdagi axborot xavfsizligining asosiy poydevori bo'lib, bank tizimlari, davlat axborot tarmoqlari va korporativ infratuzilmalarda keng joriy etilishi zarur ekanligi aniqlandi.

Kalit so'zlar: kvant kriptografiyasi, QKD, BB84 protokoli, qubit, kvant mexanikasi, post-kvant kriptografiya, shifrlash, kompyuter tarmoqlari, axborot xavfsizligi, kriptografik protokollar.

KIRISH. Zamonaviy axborot texnologiyalari jadal rivojlanishi bilan birga, axborot xavfsizligi masalasi tobora dolzarb bo'lib bormoqda. Klassik kriptografik algoritmlar - RSA, AES va ECC - bugungi kunda kompyuter tarmoqlarida keng qo'llaniladi. Biroq kvant kompyuterlari rivojlanishi bilan ushbu algoritmlar jiddiy tahdid ostida qolmoqda: Shor algoritmi yordamida kvant kompyuterlari RSA ni eksponensial tezlikda buzishi mumkin.

Muammo shundaki, internet trafikning 90% dan ortig'i RSA va elliptik egri kriptografiyasiga tayanuvchi TLS/SSL protokoli orqali himoyalanadi. Kvant kompyuterlarining amaliy tadbiqqa tayyor bo'lishi bu tizimlarni butunlay eskirtirib qo'yishi mumkin. Shu bois kvant mexanikasi qonunlariga asoslangan yangi avlod shifrlash tizimlarini o'rganish va joriy etish zarurati yuzaga kelmoqda.

O'rganilmagan muammo sifatida O'zbekistonda kvant kriptografiyasining milliy tarmoqlarga integratsiyasi va amaliy tatbiq yo'nalishlari yetarlicha tadqiq etilmagan. 2025-yilgi ma'lumotlarga ko'ra, Xitoy, AQSh, Yaponiya, Germaniya va Janubiy Koreya QKD tizimlarini milliy tarmoqlarga joriy etishni boshlagan bo'lsa-da, O'zbekistonda bu borada ilmiy tadqiqotlar boshlang'ich bosqichda.

Ushbu maqolaning maqsadi - kvant kriptografiyasining zamonaviy kompyuter tarmoqlaridagi qo'llanilish istiqbollarini tahlil qilish, uning afzalliklari va cheklovlarini o'rganish hamda O'zbekiston axborot xavfsizligi tizimidagi o'rni va rivojlanish yo'nalishlarini aniqlashdan iborat.

Kvant kriptografiyasining ahamiyatini to‘liq anglash uchun uning tarixiy rivojlanishini ko‘rib chiqish zarur. 1970-yillarda Stephen Wiesner kvant mexanikasiga asoslangan pul o‘tkazmalari kontseptsiyasini taklif qildi, ammo bu g‘oya o‘sha davrda amalga oshirib bo‘lmaydigandek tuyuldi. 1984-yilda Charles Bennett va Gilles Brassard BB84 protokolini ishlab chiqib, kvant kriptografiyasi fanining amaliy poydevorini yaratdilar. Keyinchalik 1991-yilda Artur Ekert kvant chalkashligiga (quantum entanglement) asoslangan E91 protokolini taklif qildi, bu esa kvant aloqa kanallarini yanada xavfsizroq va samaraliroq qilish imkoniyatlarini ochib berdi.

Bugungi kunda global kiberhavfsizlik bozori jadal o‘sib bormoqda. Cybersecurity Ventures hisobotiga ko‘ra, 2025-yilga kelib kiberxurujlardan yillik zarar 10,5 trillion dollarga yetishi kutilmoqda. Ayniqsa, ma’lumotlarni hozirgi vaqtda to‘plab, kelajakda kvant kompyuterlari yordamida shifrlashni buzish - “Harvest Now, Decrypt Later” deb ataluvchi hujum strategiyasi - davlat sirlari va bank ma’lumotlari uchun jiddiy xavf tug’dirmoqda. Shu sababli kvant-xavfsiz kriptografiyaga o‘tishni kechiktirish qo‘shimcha xavf-xatarlarni keltirib chiqaradi.

O‘zbekistonda raqamli iqtisodiyotni rivojlantirish bo‘yicha 2030-yilgacha mo‘ljallangan strategiya axborot xavfsizligini ustuvor yo‘nalish sifatida belgilaydi. Mamlakatimizda elektron hukumat xizmatlari, raqamli to‘lov tizimlari va onlayn banking keng qo‘llanilayotgan bir sharoitda bu tizimlarning ishonchli kriptografik himoyasi davlat ahamiyatiga ega masalaga aylangan. Bundan tashqari, O‘zbekiston Respublikasining “Kiberhavfsizlik to‘g’risida” qonuni (2022) va Prezidentning tegishli farmonlari axborot infratuzilmasini zamonaviy texnologiyalar asosida himoyalash zarurligini qonuniy jihatdan mustahkamlagan.

Kvant kriptografiyasining ilmiy asosi 1984-yilda Bennett va Brassard tomonidan yaratilgan BB84 protokoliga borib taqaladi [1]. Gisin va boshqalar [2] kvant

kriptografiyasining nazariy asoslarini to'liq tahlil qilib, uning klassik kriptografiyadan tub farqlarini ko'rsatib bergan. Lo, Curty va Tamaki [3] xavfsiz QKD tizimlarining amaliy muammolarini - shu jumladan real qurilmalarning cheklovlarini - tadqiq etgan.

Liao va boshqalar [4] Xitoyning Micius yo'ldoshi orqali 1200 km masofada kvant bog'lanishni (entanglement) muvaffaqiyatli amalga oshirganligini isbotlagan. Pirandola va boshqalar [6] kvant kriptografiyasidagi so'nggi yutuqlarni, jumladan ko'p tugunli kvant tarmoqlari va kvant takrorlagichlar (repeater) muammolarini batafsil ko'rib chiqqan. Stucki va boshqalar [7] real tarmoq sharoitida SwissQuantum tizimining uzoq muddatli ishlashini tahlil qilib, amaliy QKD tizimlarining ishonchliligini isbotlagan.

NIST [5] 2022-yilda post-kvant kriptografiyani standartlashtirish uchun CRYSTALS-Kyber va CRYSTALS-Dilithium algoritmlarini tavsiya qilgan. Wehner, Elkouss va Hanson [8] kvant internetining kelajakdagi arxitekturasi va rivojlanish yo'lini ko'rsatib bergan.

Ushbu tadqiqotda quyidagi metodlardan foydalanildi:

– Ilmiy adabiyotlar tahlili - 2002–2024-yillar oralig'ida chop etilgan 10 ta asosiy manba tahlil qilindi;

– Qiyosiy tahlil - kvant va klassik kriptografiya tizimlari parametrlari bo'yicha solishtirma o'rganish o'tkazildi;

– Amaliy tatbiq misollarini o'rganish - Xitoy, AQSh, Yevropa va Shveytsariya QKD loyihalari tahlil qilindi;

– Texnik tavsif metodi - BB84 protokolining ishlash mexanizmi va QKD tizimlarining texnik xususiyatlari bayon etildi.

Tadqiqot natijasida aniqlangan BB84 protokolining ishlash tamoyili quyidagicha: jo'natuvchi (Alice) tasodifiy bitlar ketma-ketligini turli kvant qutblanish holatlari orqali yuboradi. Qabul qiluvchi (Bob) tasodifiy o'lchov bazasini tanlab, natijalarni ochiq kanal orqali solishtiradi - mos kelgan o'lchovlar umumiy kalitni tashkil etadi. Kvant mexanikasining nusxa ko'chirish mumkin emasligi teoremasi

(No-Cloning Theorem) tufayli tinglashga urinish kvant holatini o'zgartiradi va darhol aniqlanadi.

Kvant kriptografiyasi va klassik kriptografiyaning qiyosiy tahlili quyidagi natijalarni ko'rsatdi:

– Xavfsizlik asosi: klassik kriptografiya hisoblash murakkabligiga, kvant kriptografiyasi esa fizika qonunlariga tayanadi;

– Kvant kompyuterlariga chidamlilik: RSA va ECC Shor algoritmi oldida zaif, kvant kriptografiyasi esa mutlaq himoyalangan;

– Tinglashni aniqlash: klassik tizimlar tinglashni aniqlolmaydi, kvant tizimi esa har qanday hujumni darhol fosh etadi;

– Uzun muddatli himoya: klassik kalitlar vaqt o'tishi bilan zaiflanadi, kvant kalitlari esa muddatsiz xavfsiz qoladi.

Tadqiqot davomida aniqlangan amaliy natijalar shuni ko'rsatadiki, QKD texnologiyasi haqiqiy tarmoq sharoitida muvaffaqiyatli ishlaydi. Xitoy 2016-yilda Micius kvant yo'ldoshini ishga tushirib, 2017-yilda Beijing–Shanxay orasida 2000 km uzunlikdagi kvant kriptografik magistral qurildi. Toshiba Research Europe laboratoriyasi 2021-yilda 600 km optik tola bo'ylab kvant kaliti taqsimlashni muvaffaqiyatli sinab ko'rdi. ID Quantique (Shveytsariya) kompaniyasi tijorat QKD qurilmalarini ishlab chiqarib, hukumat va bank tarmoqlarida qo'llanilmoqda.

Yevropa Ittifoqida 2020-yildan EuroQCI (European Quantum Communication Infrastructure) loyihasi amalga oshirilmoqda. O'zbekistonda esa UZINFOCOM va bir qator universitetlar axborot xavfsizligi tizimlarini zamonaviylashtirish doirasida kvant texnologiyalarini o'rganishni boshlagan.

Tadqiqot davomida mavjud cheklovlar ham aniqlandi:

- Masofa cheklovi: hozirgi QKD tizimlari 400-600 km gacha samarali ishlaydi; kvant takrorlagichlar (quantum repeaters) texnologiyasi hali tajriba bosqichida;

- Tezlik cheklovi: kvant kalitlarini taqsimlash tezligi hali 10-100 kbit/s darajasida bo'lib, klassik kanallar bilan raqobatlasha olmaydi;

- Infratuzilma xarajatlari: maxsus optik kabellar va kriogen qurilmalar yuqori kapital xarajatlarni talab qiladi.

Bu cheklovlarga qaramay, NIST tomonidan standartlashtirilgan CRYSTALS-Kyber va CRYSTALS-Dilithium algoritmlari kvant va klassik tizimlarning gibrid qo'llanilishini ta'minlaydi. NASA va DARPA 2030-yilgacha kvant internetining prototipini yaratishni rejalashtirayapti.

Ushbu tadqiqot natijasida quyidagi xulosalar chiqarildi:

- Kvant kriptografiyasi fizika qonunlariga asoslanib, klassik kriptografiyadan tubdan farq qiladigan, matematikaga emas balki kvant mexanikasiga asoslangan mutlaq xavfsizlikni ta'minlaydi.

- BB84 protokoli va QKD tizimlari dunyoning yetakchi mamlakatlarida hukumat va moliya sohalarida amaliy tatbiq etilmoqda, bu esa texnologiyaning ishonchliligini isbotlaydi.

- Post-kvant kriptografiya standartlari (CRYSTALS-Kyber, CRYSTALS-Dilithium) kvant va klassik tizimlarni birga qo'llash imkonini berib, o'tish davrini osonlashtiradi.

- O'zbekiston uchun raqamli iqtisodiyot va kiberhavfsizlik strategiyalari doirasida kvant kriptografiyasini o'rganish va milliy tarmoqlarga bosqichma-bosqich joriy etish istiqbolli va zaruriy yo'nalish hisoblanadi.

- Kvant kriptografiyasi kelajakdagi axborot xavfsizligining asosiy poydevori bo'lib xizmat qilishi shubhasizdir; masofa va xarajat cheklovlari esa texnologiyaning tez rivojlanishi natijasida bartaraf etilishi kutilmoqda.

ADABIYOTLAR RO'YXATI

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. Gisin N., Ribordy G., Tittel W., Zbinden H. Quantum cryptography // Reviews of Modern Physics. - 2002. - Vol. 74. - P. 145-195.
3. Lo H.K., Curty M., Tamaki K. Secure quantum key distribution // Nature Photonics. - 2014. - Vol. 8. - P. 595-604.
4. Liao S.K. et al. Satellite-based entanglement distribution over 1200 kilometers // Science. - 2017. - Vol. 356. - P. 1140-1144.

5. NIST. Post-Quantum Cryptography Standardization. National Institute of Standards and Technology. - 2022.
6. Pirandola S. et al. Advances in quantum cryptography // Advances in Optics and Photonics. - 2020. - Vol. 12. - P. 1012-1236.
7. Stucki D. et al. Long-term performance of the SwissQuantum quantum key distribution network in a field environment // New Journal of Physics. - 2011. - Vol. 13. - No. 123001.
8. Wehner S., Elkouss D., Hanson R. Quantum internet: A vision for the road ahead // Science. - 2018. - Vol. 362. - No. eaam9288.
9. Xu F. et al. Secure quantum key distribution with realistic devices // Reviews of Modern Physics. - 2020. - Vol. 92. - No. 025002.
10. ID Quantique. Quantum-Safe Security Solutions. - Geneva: ID Quantique, 2023. - https://www.idquantique.com