интеллектуального анализа данных. В дальнейшем планируется расширить экспериментальные исследования за счёт использования других наборов данных и проведения сравнительного анализа с существующими методами селекции объектов.

Список литературы

1. Игнатьев Н.А., Акбаров Б.Х. Оценка близости структур отношений объектов обучающей выборки на многообразиях наборов латентных признаков // Вестник Томского государственного университета. Управление, вычислительная техника и информатика. 2023. № 65. С. 69–78.

2. *https://archive.ics.uci.edu/dataset/144/statlog+german+credit+data*

3. Н. А. Игнатьев Выбор целевых признаков для классификации и кластерного анализа структур отношений объектов// InternationalJournalof Open Information Technologies ISSN: 2307-8162 vol. 14, no. 3, 2026

4. Hart P. The condensed nearest neighbor rule // IEEE Transactions on Information Theory. 1968. Vol. 14, No. 3. P. 515–516. https://doi.org/10.1109/TIT.1968.1054155

5. Wilson D. Asymptotic properties of nearest neighbor rules using edited data // IEEE Transactions on Systems, Man, and Cybernetics. 1972. Vol. 2, No. 3. P. 408–421. https://doi.org/10.1109/TSMC.1972.4309137

6. Tomek I. Two modifications of CNN // IEEE Transactions on Systems, Man, and Cybernetics. 1976. Vol. 6. P. 769–772.

7. Aha D., Kibler D., Albert M. Instance-based learning algorithms // Machine Learning. 1991. Vol. 6. P. 37–66. https://doi.org/10.1023/A:1022689900470

8. Wilson D., Martinez T. Reduction techniques for instance-based learning algorithms // Machine Learning. 2000. Vol. 38. P. 257–286. https://doi.org/10.1023/A:1007626913721

9. García S., Derrac J., Cano J., Herrera F. Prototype selection for nearest neighbor classification: taxonomy and empirical study // IEEE Transactions on Pattern Analysis and Machine Intelligence. 2012. Vol. 34. No. 3. P. 417–435. https://doi.org/10.1109/TPAMI.2011.142

KVANT KALITLARINI TA’MINLASH USULI ORQALI XAVFSIZ AXBOROT ALMASHINUVI

[1] D.T. Muhamediyeva, [1] Tagaev Farxad Abduvaxabovich
«Toshkent irrigatsiya va qishloq xo’jaligini mexanizatsiyalash muhandislari instituti» milliy tadqiqot universiteti
dilnoz134@rambler.ru

Annotatsiya: Ushbu maqolada kvant kriptografiyasining BB84 protokoli asosida xavfsiz kalit almashinuvi modeli ishlab chiqildi va simulyatsiya qilindi. Tadqiqotda Alice va Bob orasidagi kvant kanal orqali uzatilgan fotonlar kvant holatlarida kodlanib, ularni o‘qishda bazalarning tasodifiy tanlanishi orqali xavfsizlik ta’minlandi. Eavesdropping (Eve) aralashuvi aniqlanishi uchun xatolik ko‘rsatkichi hisoblandi. Kalitni generatsiya qilgandan so‘ng, ma’lumotlarni himoyalangan tarzda uzatish uchun XOR asosidagi sodda ECC shifrlash algoritmi qo‘llandi. Natijalar BB84 protokoli orqali shakllangan kalit yordamida axborot maxfiyligini samarali saqlash mumkinligini ko‘rsatdi.

Kalit so‘zlar. BB84 protokoli, kvant kalit taqsimoti (QKD), kvant kriptografiyasi, XOR shifrlash, Aer simulyatori.

ЗАЩИЩЕННЫЙ ОБМЕН ИНФОРМАЦИЕЙ С ИСПОЛЬЗОВАНИЕМ КВАНТОВОГО МЕТОДА ПРЕДОСТАВЛЕНИЯ КЛЮЧА

[1]Д.Т. Мухамедиева, [1]Тагаев Фархад Абдувахабович
Национальный исследовательский университет «Ташкентский институт инженеров »

dilnoz134@rambler.ru

Аннотация: В данной статье разработана и промоделирована модель безопасного обмена ключами на основе протокола квантовой криптографии BB84. В исследовании фотоны, передаваемые по квантовому каналу между Алисой и Бобом, кодировались в квантовых состояниях, а безопасность обеспечивалась случайным выбором базисов при их чтении. Был рассчитан индикатор ошибки для обнаружения помехи Eavesping (Eve). После генерации ключа для защищенной передачи данных использовался простой алгоритм шифрования ECC на основе XOR. Результаты показали, что можно эффективно сохранять конфиденциальность информации, используя ключ, сформированный по протоколу BB84.

Ключевые слова: Протокол BB84, квантовое распределение ключей (QKD), квантовая криптография, шифрование XOR, симулятор Aer.

SECURE INFORMATION EXCHANGE THROUGH QUANTUM KEY PROVISION METHOD

[1]D.T. Muhamediyeva, [1]Tagaev Farkhad Abduvakhabovich
National Research University “Tashkent Institute of Irrigation and
Agricultural Mechanization Engineers”
dilnoz134@rambler.ru

Abstract: In this article, a model of secure key exchange based on the BB84 protocol of quantum cryptography was developed and simulated. In the study, photons transmitted through a quantum channel between Alice and Bob were encoded in quantum states, and security was ensured by random selection of bases when reading them. An error indicator was calculated to detect Eavesdropping (Eve) interference. After generating the key, a simple ECC encryption algorithm based on XOR was used to transmit data in a protected manner. The results showed that it is possible to effectively maintain information confidentiality using a key formed through the BB84 protocol.

Keywords: BB84 protocol, quantum key distribution (QKD), quantum cryptography, XOR encryption, Aer simulator.

Kirish. Raqamli axborot xavfsizligini ta’minlash zamonaviy kriptotizimlarning eng muhim vazifalaridan biridir. Klassik kriptografiya algoritmlarining mustahkamligi, asosan, katta hisoblash murakkabligiga asoslangan bo‘lib, kvant hisoblash texnologiyalarining rivoji ushbu tizimlarning zaiflashishiga olib kelishi mumkin. Shu sababli, yangi avlod xavfsizlik protokollarini ishlab chiqish dolzarb masalalardan sanaladi. Kvant kriptografiyasi – kvant mexanikasi qonuniyatlariga tayangan holda ishlaydigan mutlaqo yangi yondashuv bo‘lib, u axborotning uzatilish jarayonida uni yashirincha o‘zgartirish yoki tinglashning iloji yo‘qligini kafolatlaydi. Xususan, BB84 protokoli kvant holatlarining o‘zgarmasligi va superpozitsiya prinsipiga asoslangan holda, abonentlar o‘rtasida xavfsiz maxfiy kalitni yaratadi [1-4].

Ushbu tadqiqotda BB84 protokoli Qiskit platformasi yordamida modellashtirildi. Alice tomonidan yaratilgan bitlar va bazalar yordamida foton holatlari shakllantirildi hamda Bob tomonidan o‘lchandi. Tinglovchining aralashuvi xatolik darajasi orqali monitoring qilindi. Formirovka qilingan kalit yordamida oddiy XOR shifrlash usulida matnli xabar himoyalandi. Tadqiqot natijalari BB84 protokolining axborot

xavfsizligini samarali ta’minlashdagi ustunliklarini tasdiqladi [5-7].

Ushbu tadqiqotning asosiy maqsadi — kvant mexanikasi tamoyillariga asoslangan BB84 protokoli yordamida xavfsiz kalit almashinuvi tizimini yaratish va uni XOR shifrlash usuli bilan birgalikda qo‘llab, axborotni uzatish jarayonida tinglovchi mavjudligini aniqlash hamda ma’lumot maxfiyligini ta’minlashdir. Shu orqali klassik kriptografiya usullaridan farqli o‘laroq, kvant kanallar yordamida axborot uzatish xavfsizligini yuqori darajada kafolatlovchi model ishlab chiqish ko‘zda tutilgan [8-11].

Tadqiqot maqsadiga erishish uchun quyidagi asosiy vazifalar belgilandi [12-14]:Qiskit platformasida BB84 kvant kalit taqsimoti (QKD) protokolini modellashtirish;

Alice va Bob o‘rtasidagi kvant kanal orqali qubitlar yuborilishi va o‘lchanish jarayonini simulyatsiya qilish;

Tinglovchi (Eve) aralashgan holatda xatolik darajasini aniqlash va kanal xavfsizligini baholash;

BB84 orqali yaratilgan kalitdan foydalanib, XOR shifrlash yordamida matnli ma’lumotni shifrlash va qayta tiklash;

Olingan natijalar asosida kvant kalit almashinuvi va klassik shifrlash algoritmlarini birlashtirish samaradorligini tahlil qilish.

Tadqiqotning ilmiy yangiligi shundaki, unda kvant kalit taqsimoti tizimi (BB84) bilan klassik ECC-ga o‘xshash XOR shifrlash mexanizmi birgalikda qo‘llanilib, axborot xavfsizligini ta’minlashning gibrid modeli taklif etildi. Ushbu yondashuv nafaqat kvant kanal orqali kalit almashishning nazariy asoslarini, balki uni amaliy shifrlash algoritmlariga integratsiya qilish imkoniyatlarini ham ko‘rsatadi. Shuningdek, tinglovchi mavjudligi holatida xatolik ko‘rsatkichini aniqlash orqali kanal xavfsizligini baholashning avtomatlashtirilgan usuli ishlab chiqildi [15-17].

Tadqiqot natijalari kvant kriptografiya tizimlarini dasturiy modellashtirish, xavfsiz axborot almashinuvi platformalarini ishlab chiqish, va kelajakdagi kvant tarmoqlarini yaratishda amaliy asos bo‘la oladi. Taklif etilgan BB84 + XOR integratsiyalangan model real kvant aloqa tarmoqlarida kalit almashinuvi xavfsizligini oshirish, ma’lumotni himoyalash va cyberxavfsizlik tizimlarini mustahkamlashda qo‘llanishi mumkin. Bundan tashqari, Qiskit asosida yaratilgan simulyatsiya o‘quv jarayonlarida kvant kriptografiya prinsiplari va ularning amaliy qo‘llanilishi uchun samarali laboratoriya vositasi sifatida ham xizmat qiladi [18-20].

2. METODOLOGIYA

Ushbu ishning metodologiyasi BB84 kvant kalit tarqatish protokoli va elliptik egri chiziqli kriptografiya (ECC) algoritmini integratsiyalashga asoslangan bo‘lib, quyidagi bosqichlarni o‘z ichiga oladi.

BB84 kvant kalit tarqatish.

Alice n bitli tasodifiy ketma-ketlik hosil qiladi:

$$\mathbf{a} = (a_1, a_2, \ldots, a_n), \qquad a_i \in \{0,1\}.$$

Har bir qubit uchun Alice tasodifiy bazani tanlaydi:

$$\mathbf{B_A} = (B_{A1}, B_{A2}, \ldots, B_{An}), \qquad B_{Ai} \in \{Z, X\}.$$

Bob ham n ta tasodifiy bazani tanlaydi:

$$\mathbf{B_B} = (B_{B1}, B_{B2}, \ldots, B_{Bn}), \qquad B_{Bi} \in \{Z, X\}.$$

Alice tomonidan tayyorlangan har bir qubitning holati:

$$b_i = \begin{cases} 0, & \text{agar o'lchov natijasi } |0\rangle \text{ yoki } |+\rangle \\ 1, & \text{agar o'lchov natijasi } |1\rangle \text{ yoki } |-\rangle \end{cases}$$

Bob o‘lchovi natijasi:

Mos kelgan bazalar bo‘yicha xavfsiz kalit hosil qilinadi:

$$\mathbf{K_{BB84}} = \{a_i \mid B_{Ai} = B_{Bi}\}.$$

Kvant kanal xatolik darajasi:

$$e = \frac{\sum_{i=1}^{n} \delta(a_i \neq b_i) \cdot 1_{\{B_{Ai}=B_{Bi}\}}}{|\mathbf{K_{BB84}}|} \cdot 100\%$$

2. ECC orqali xabar shifrlash Alice va Bob elliptik egri chiziqli kalitlarni hosil qiladi:

$$Q_A = d_A G,$$

$$Q_B = d_B G.$$

Alice tasodifiy ephemeralik kalit k hosil qiladi va umumiy sirni hisoblaydi:

$$S = kQ_B.$$

BB84 orqali hosil qilingan kalit bilan birlashtirish:

$$K_{\text{combined}} = \text{SHA256}(S \,||\, \mathbf{K_{BB84}}).$$

m xabar shifrlanishi:

$$c = m \oplus K_{\text{combined}}[:|m|].$$

Deshifrlash:

$$m = c \oplus K_{\text{combined}}[:|c|].$$

3. Kanal xavfsizligi va aralashuvni aniqlash

Eve (tinglovchi) aralashuvi natijasida xatolik darajasi oshadi. Kanal xavfsizligi shunday baholanadi:

$$\text{Agar } e > e_{\text{threshold}}, \text{ kanal ishonchsiz.}$$

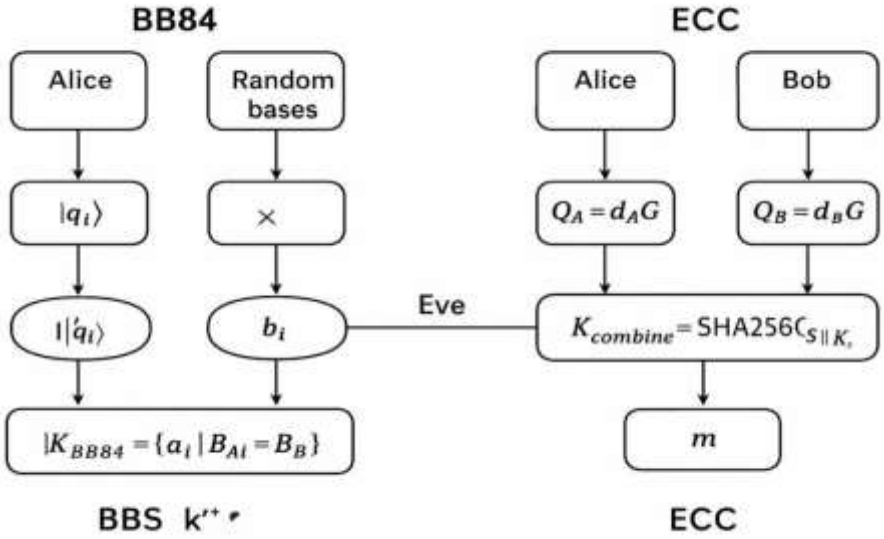
Shuningdek, BB84 + ECC kombinatsiyasi orqali xabarlar muvaffaqiyatli shifrlanadi va deshifrlanadi, ya’ni:

$$\text{Decrypt}(\text{Encrypt}(m, K_{\text{combined}}), K_{\text{combined}}) = m.$$

BB84 kanal orqali xavfsiz, tasodifiy kalit hosil qiladi, lekin u hali xabar shifrlashga tayyor emas. ECC hosil qilingan kalitni kuchaytiradi va xabar shifrlashga tayyor qiladi. BB84 kaliti ECC orqali hosil qilingan umumiy sirga qo‘shilib, final xavfsiz kalitni yaratadi:

$$K_{\text{final}} = \text{SHA256}(S \,||\, \mathbf{K_{BB84}}).$$

Shu yo‘l bilan, xabarlar ECC yordamida shifrlanishi va deshifrlanishi mumkin bo‘ladi, va BB84



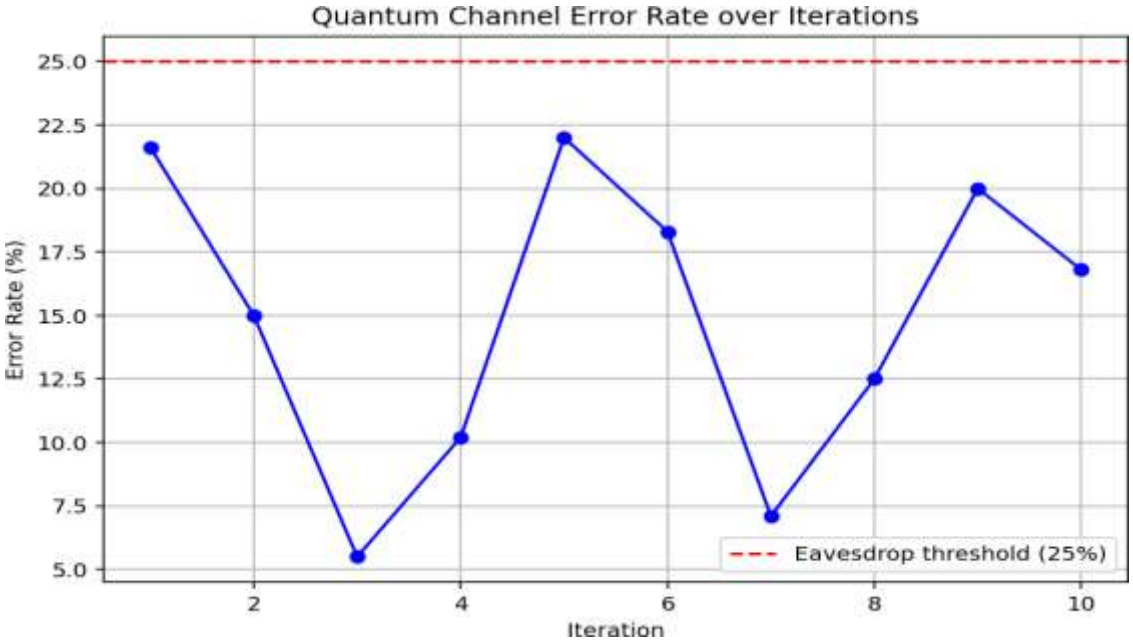
rqali hosil qilingan kvant kalit hech qanday klassik kanal orqali uzatilmasdan xavfsiz bo‘ladi.

Natijalar

BB84 protokoli orqali 37 ta qubit bazalari mos kelgan holda o‘lchandi. Kanaldagi xatolik darajasi quyidagicha hisoblandi:

$$E = \frac{\text{mos kelgan qubitlar orasidagi xatolar soni}}{\text{mos kelgan qubitlar soni}} \times 100\% = \frac{8}{37} \times 100\% \approx 21.62\%$$

Xatolik darajasi 25% dan past bo‘lgani sababli kanal xavfsiz deb baholandi va maxfiy kalit hosil qilindi. Kvant kanalning xatolik darajasi 21.62% bo‘lib, BB84 protokoli orqali maxfiy kalitni muvaffaqiyatli generatsiya qilish mumkinligi tasdiqlandi.



1-rasm. Qizil chiziq – xatolik chegarasi (Eve mavjud bo‘lishi ehtimoli).

Kanaldan olingan mos kelgan qubitlar asosida BB84 protokoli yordamida yakuniy simmetrik kalit hosil qilindi. Hosil qilingan kalit 16-bitli shaklda quyidagicha ifodalanadi:

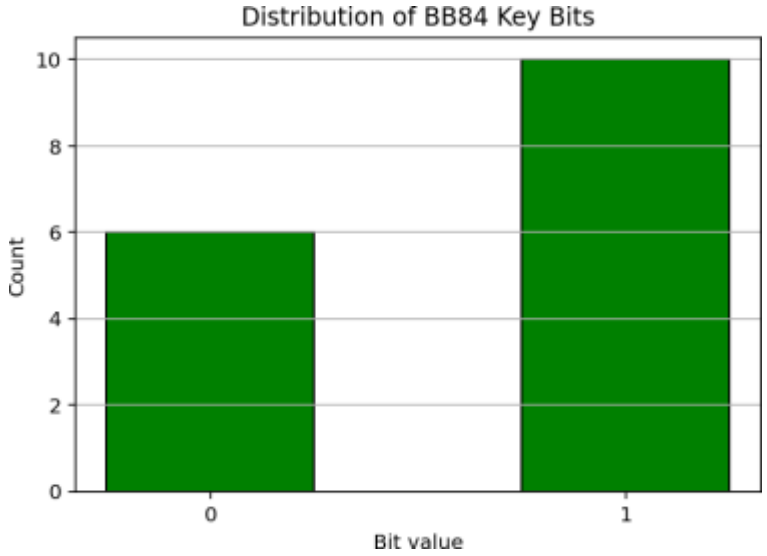
Hosil qilingan kalit yordamida xabar XOR + ECC integratsiyalangan algoritm orqali shifrlanadi. Shifrlangan xabar quyidagicha ko‘rinadi:

Shifrlangan ma'lumot:

1050fa7b597069fbacb8c3bde1801230121a90039ae0a71c0db1097c814f2f01

Keyinchalik kalitni ishlatib deshifrlash amalga oshirildi, natija esa dastlabki xabar bilan to‘liq mos kelmoqda:

Deshifrlangan xabar: Bu BB84 + ECC integratsiyalangan.



2-rasm. Kalit bitlar 0 va 1 ga qanday taqsimlanganini ko‘rsatadi (key randomness).

Hosil qilingan kalit ECC bilan birlashtirilgan XOR shifrlash uchun ishlatilgan va xabar muvaffaqiyatli shifrlanib, deshifrlash jarayonida asl holatga tiklandi.

Xulosa. Ushbu ishning maqsadi BB84 kvant kalit taqsimoti protokolini klassik ECC (Elliptic Curve Cryptography) bilan birlashtirib, xavfsiz ma’lumot uzatish mexanizmini yaratishdir. Simulyatsiya natijalari shuni ko‘rsatdiki, kanaldagi xatolik darajasi 21.62% bo‘lib, maxsus xatolik chegarasidan pastligi sababli kalit hosil qilish muvaffaqiyatli amalga oshirilgan. Hosil qilingan BB84 kaliti ECC bilan integratsiyalashgan XOR shifrlash uchun ishlatilgan va xabar shifrlash-desfiyrlash jarayonida to‘liq moslik ta’minlangan.Natijalar shuni tasdiqladiki, kvant kanali orqali uzatilgan qubitlar yordamida simmetrik kalit xavfsiz ravishda hosil qilinadi va ECC bilan birgalikda ishlatilganda, ma’lumotlarning sir saqlanishi yanada mustahkamlanadi. Shu bilan birga, realistik simulyatsiya muhiti va Qiskit kutubxonasi yordamida olingan natijalar protokolning amaliy qo‘llanilishi va xavfsizlikni baholash imkonini beradi.Kelajakda ishni yanada rivojlantirish uchun information reconciliation (Cascade parity block) va privacy amplification jarayonlarini integratsiyalash orqali kalitning yakuniy entropiyasi va xavfsizlik darajasini oshirish mumkin. Shu yo‘l bilan BB84 + ECC protokoli real dunyo sharoitida xavfsiz ma’lumot uzatish uchun mukammal yechim sifatida ishlatilishi mumkin.

Foydalanilgan adabiyotlar

1. Shor P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer // SIAM J. Comput. – 1997. – Vol. 26, №5. – P. 1484–1509.

2. Grover L.K. Quantum mechanics helps in searching for a needle in a haystack // Phys. Rev. Lett. – 1997. – Vol. 79. – P. 325–328.

3. Milanov E. The RSA algorithm // RSA Lab. – 2009. – P. 1–11.

4. Hankerson D., Menezes A. Elliptic curve cryptography // Encyclopedia of Cryptography, Security and Privacy. – Springer, 2021. – P. 1–2.

5. Alléaume R., Branciard C., Bouda J., Debuisschert T., Dianati M., Gisin N., Godfrey M., Grangier P., Länger T., Lütkenhaus N., et al. Using quantum key distribution for cryptographic purposes: a survey // Theoret. Comput. Sci. – 2014. – Vol. 560. – P. 62–81.

6. Ekert A.K. Quantum cryptography based on Bell’s theorem // Phys. Rev. Lett. – 1991. – Vol. 67. – P. 661–663.

7. Gisin N., Bechmann-Pasquinucci H. Bell inequality, Bell states and maximally entangled states

for n qubits // Phys. Lett. A. – 1998. – Vol. 246, №1–2. – P. 1–6.

8. Cheddad A., Condell J., Curran K., Mc Kevitt P. Digital image steganography: Survey and analysis of current methods // Signal Process. – 2010. – Vol. 90, №3. – P. 727–752.

9. Özkaynak F. Brief review on application of nonlinear dynamics in image encryption // Nonlinear Dynam. – 2018. – Vol. 92, №2. – P. 305–313.

10. Sharma M., Choudhary V., Bhatia R., Malik S., Raina A., Khandelwal H. Leveraging the power of quantum computing for breaking RSA encryption // Cyber-Phys. Syst. – 2021. -Vol. 7, №2. – P. 73–92.

11. Zhang Y. Test and verification of AES used for image encryption // 3D Res. – 2018. – Vol. 9. – P. 1–27.

12. Pawar H.R., Harkut D.G. Classical and quantum cryptography for image encryption & decryption // Proc. 2018 International Conference on Research in Intelligent and Computing in Engineering (RICE). – IEEE, 2018. – P. 1–4.

13. Dworkin M.J. Advanced Encryption Standard (AES) // Federal Information Processing Standards (FIPS)-197. – 2001.

14. Data Encryption Standard (DES) // Fed. Inf. Process. Stand. Publ. 112. – 1999. – P. 3.

15. Preneel B. Cryptographic hash functions // Eur. Trans. Telecommun. – 1994. – Vol. 5, №4. – P. 431–448.

16. Ullah S., Zheng J., Din N., Hussain M.T., Ullah F., Yousaf M. Elliptic curve cryptography; applications, challenges, recent advances, and future trends: A comprehensive survey // Comput. Sci. Rev. – 2023. – Vol. 47. – P. 100530.

17. Sharma P.L.G., Nayyar S., Harish A., Gupta M., Sharma K., Kumar A. ECC based novel color image encryption methodology using primitive polynomial // Multimedia Tools Appl. – 2024.

18. Shivaramakrishna D., Nagaratna M. A novel hybrid cryptographic framework for secure data storage in cloud computing: Integrating AES-OTP and RSA with adaptive key management and time-limited access control // Alex. Eng. J. – 2023. – Vol. 84. – P. 275–284.

19. Kumar S.S., Deepmala. A chaotic based image encryption scheme using elliptic curve cryptography and genetic algorithm // Artif. Intell. Rev. – 2024.

20. Rahman R., Azad M.S., Hasan M.R., Emad S., Shubha U., Mahdy M. Enhancing the security of image transmission in quantum era: A chaos-assisted QKD approach using entanglement – 2023. – ArXiv:2311.18471.

GIDROMODULLI RAYONLASHTIRISH VA GRAF MODEL ASOSIDA SUV RESURSLARINI ADOLATLI LIMITLASH ALGORITMI

Qudaybergenov A.A.[1]
[1]*PhD, dotsent, Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universiteti doktoranti*
adilbaygm@gmail.com
Qazimbetova M.M.[2]
[2]*PhD, Berdax nomidagi Qoraqalpoq davlat universiteti doktoranti, Nukus, O‘zbekiston*
qazimbetovamuxabbad@gmail.com
Ispanova J.P.[3]
[3]*Berdax nomidagi Qoraqalpoq davlat universiteti tayanch doktoranti, Nukus, O‘zbekiston*
paraxatovna1996@gmail.com

Annotatsiya: Ushbu ishda gidromodulli rayonlashtirish, kanal tarmog‘ini graf ko‘rinishida ifodalash va chiziqli dasturlash usulini birlashtirgan holda suv resurslarini adolatli limitlash algoritmi ishlab chiqildi. Taklif etilgan yondashuv fermerlar kesimida netto va brutto suv talabini hisoblash, tarmoqdagi o‘tkazuvchanlik va taqsimot cheklovlarini inobatga olish hamda cheklangan suv sharoitida suvni maqbul taqsimlash imkonini beradi. Olingan natijalar qondirilmagan talabni kamaytirish, nisbiy defitsitni