105. С. 188–204.

9. Gonçalves G. M., Vaz Pato M. A three-phase procedure for designing an irrigation system's water distribution network // Annals of Operations Research. 2000. Т. 94, № 1–4. С. 163–179.

10. N. A. Akhand, D. L. Larson, D. C. Slack. Canal Irrigation Allocation Planning Model // Transactions of the ASAE. 1995. Т. 38, № 2. С. 545–550.

11. Marques G. F., Lund J. R., Howitt R. E. Modeling irrigated agricultural production and water use decisions under water supply uncertainty // Water Resources Research. 2005. Т. 41, № 8. С. 2005WR004048.

12. Luss H., Smith D. R. Resource allocation among competing activities: a lexicographic minimax approach // Operations Research Letters. 1986. Т. 5, № 5. С. 227–231.

ELLIPTIK EGRI CHIZIQ KRIPTOGRAFIYASI ASOSIDA KVANT KALIT ALMASHINUVI SXEMASINI MODELLASHTIRISH

[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 Elliptik egri chiziq kriptografiyasi (ECC) asosida kalit almashinuvi jarayoni va uning kvant simulyatsiyasi Qiskit muhiti yordamida amalga oshiriladi. Elliptik egri chiziq ustida nuqta qo'shish va ko'paytirish amallari orqali Alice va Bob o'zlarining maxfiy va ochiq kalitlarini generatsiya qiladi. Shundan so'ng, ular o'zaro umumiy kalitni hisoblaydilar va ushbu kalit bir xil natijaga ega bo'lishi tekshiriladi. Maqolada kvant simulyatsiya bosqichi sifatida Hadamard va CNOT kvant darvozalari ishlatilgan bo'lib, ular orqali kvant holatlaridagi superpozitsiya va bog'liqlik (entanglement) jarayoni modellashtirilgan. Natijalar kvant hisoblashning ECC asosidagi xavfsiz kalit almashinuvi tizimlarini yanada takomillashtirish imkonini berishini ko'rsatadi.

Kalit so'zlar: Elliptik egri chiziq kriptografiyasi; kvant kalit almashinuvi; superpozitsiya; kvant simulyatsiyasi.

МОДЕЛИРОВАНИЕ СХЕМЫ КВАНТОВОГО ОБМЕНА КЛЮЧАМИ НА ОСНОВЕ КРИПТОГРАФИИ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

[1]Д.Т. Мухамедиева, [1]Тагаев Фархад Абдувахабович

Национальный исследовательский университет «Ташкентский институт инженеров ирригации и механизации сельского хозяйства»

dilnoz134@rambler.ru

Аннотация: В данной статье реализован процесс обмена ключами на основе криптографии на эллиптических кривых (ECC) и его квантовое моделирование с использованием среды Qiskit. Алиса и Боб генерируют свои секретный и открытый ключи, добавляя и умножая точки на эллиптической кривой. После этого они вычисляют общий ключ и проверяют, даёт ли этот ключ одинаковый результат. В статье квантовые вентили Адамара и CNOT используются в качестве этапов квантового моделирования, посредством которых моделируются процессы суперпозиции и запутывания в квантовых состояниях. Результаты показывают, что квантовые вычисления могут дополнительно улучшить безопасные системы обмена ключами на основе ECC.

Ключевые слова: эллиптическая кривая криптографии; квантовый обмен ключами; суперпозиция; квантовое моделирование.

MODELING OF A QUANTUM KEY EXCHANGE SCHEME BASED ON ELLIPTIC CURVE CRYPTOGRAPHY

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

Annotation: In this article, the key exchange process based on elliptic curve cryptography (ECC) and its quantum simulation are implemented using the Qiskit environment. Alice and Bob generate their secret and public keys by adding and multiplying points on the elliptic curve. After that, they calculate a common key and check whether this key has the same result. In the article, Hadamard and CNOT quantum gates are used as quantum simulation stages, through which the superposition and entanglement processes in quantum states are modeled. The results show that quantum computing can further improve secure key exchange systems based on ECC.

Keywords: Elliptic curve cryptography; quantum key exchange; superposition; quantum simulation.

Kirish. So‘nggi yillarda kvant hisoblash texnologiyalarining rivojlanishi mavjud kriptotizimlarning xavfsizligiga sezilarli ta’sir ko‘rsatmoqda. Ayniqsa, Shor algoritmi kabi kvant algoritmlari klassik Elliptik egri chiziq va RSA asosidagi tizimlarning zaiflashishiga sabab bo‘lishi mumkin. Shu sababli, post–kvant kriptografiya yo‘nalishidagi izlanishlar muhim ilmiy masalaga aylangan. Elliptik egri chiziq kriptografiyasi (ECC) – klassik tizimlarda yuqori darajadagi xavfsizlikni ta’minlaydigan, ammo kalit uzunligi kichik bo‘lgan samarali usullardan biridir. ECC asosidagi Diffie–Hellman (ECDH) protokoli yordamida ikki tomon (Alice va Bob) o‘zaro umumiy maxfiy kalitni almashish imkoniyatiga ega bo‘ladi [1–3].

Ushbu ishda ECC asosidagi kalit almashinuvi algoritmi Python dasturlash tili va Qiskit kvant hisoblash kutubxonasi yordamida modellashtirildi. Elliptik egri chiziq ustida arifmetik amallar (nuqta qo‘shish va ko‘paytirish) orqali ochiq va maxfiy kalitlar hisoblandi, so‘ngra kvant simulyatsiya orqali kvant darvozalari yordamida superpozitsiya holati va entanglement jarayoni ko‘rsatildi. Bu yondashuv ECC asosidagi kriptotizimlarning kvant muhitidagi barqarorligini tahlil qilish hamda ularni kvant kalit almashinuvi sxemalariga moslashtirish imkonini beradi [4–8].

Ushbu tadqiqotning asosiy maqsadi — elliptik egri chiziq kriptografiyasi asosida kalit almashinuvi jarayonini kvant hisoblash muhiti bilan uyg‘unlashtirish hamda Qiskit dasturiy platformasi yordamida ushbu jarayonni modellashtirishdir. Tadqiqot orqali klassik ECC mexanizmlarining kvant muhitidagi ishlash imkoniyatlarini aniqlash, superpozitsiya va entanglement kabi kvant xususiyatlaridan foydalangan holda xavfsiz va samarali kalit almashinuvi modelini yaratish ko‘zda tutiladi. Shuningdek, Elliptik egri chiziq ustida nuqta amallarining kvant algoritmlar bilan o‘zaro integratsiyasi orqali post–kvant kriptografik tizimlarga o‘tish uchun nazariy asos shakllantirish maqsad qilingan [9–11].

Tadqiqot maqsadiga erishish uchun bir qator aniq ilmiy vazifalar belgilangan. Birinchidan, Elliptik egri chiziq ustida nuqta qo‘shish va ko‘paytirish amallarini modulyar arifmetika asosida Python dasturida amalga oshirish. Ikkinchidan, ECC asosida Alice va Bob o‘rtasida maxfiy hamda ochiq kalitlarni hisoblash va ularni o‘zaro tekshirish mexanizmini yaratish. Uchinchidan, Qiskit kutubxonasi yordamida kvant registrlar, Hadamard va CNOT darvozalari asosida superpozitsiya hamda isogeniya xaritasini modellashtirish. To‘rtinchidan, kvant simulyatsiya natijalarini tahlil qilib, ularning ECC xavfsizlik darajasiga ta’sirini baholash. Shuningdek, olingan natijalar asosida post–kvant kriptotizimlar uchun yangi modellashtirish yondashuvini taklif etish [12–13].

Tadqiqotning ilmiy yangiligi shundaki, unda klassik elliptik egri chiziq kriptografiyasi jarayoni kvant simulyatsiya muhiti bilan birlashtirilib, Qiskit platformasida yangi turdagi kvant–Elliptik egri chiziq

kalit almashinuvi modeli ishlab chiqildi. Mazkur modelda isogeniya xaritasi kvant CNOT darvozasi orqali ifodalanib, kalit almashish jarayonining kvant darajasida bog‘lanish (entanglement) xususiyati namoyon etildi. Shuningdek, elliptik egri chiziq arifmetikasi va kvant superpozitsiyasi o‘rtasida matematik moslik yaratilgani ECC algoritmlarining post–kvant himoya mexanizmlarini tadqiq etish uchun yangi konseptual yo‘nalish ochadi. Bu yondashuv ECC xavfsizligini kvant sharoitida tahlil qilish uchun innovatsion asos yaratadi [14–15].

Ushbu tadqiqotning amaliy ahamiyati shundaki, u kvant texnologiyalari rivojlanayotgan bir davrda klassik kriptografik tizimlarning barqarorligini saqlash va yangi post–kvant algoritmlar yaratishda foydalanish imkonini beradi. Ishlab chiqilgan Qiskit asosidagi kvant–ECC modellashtirish usuli kelajakda kvant xavfsiz aloqa tarmoqlarini yaratish, raqamli imzo tizimlarini himoyalash va kvant internet infratuzilmasida xavfsiz kalit taqsimlash mexanizmlarini sinovdan o‘tkazishda qo‘llanilishi mumkin. Bundan tashqari, taklif etilgan model ta’lim va ilmiy tadqiqot sohalarida kvant kriptografiya va ECC integratsiyasini o‘rganish uchun o‘quv–uslubiy platforma sifatida ham xizmat qilishi mumkin [16–17].

Metodologiya Elliptik

egri asoslari.

Elliptik egri chiziq kriptografiyasi quyidagi umumiy ko‘rinishdagi algebraik egri asosida quriladi:

$$E: y^2 \equiv x^3 + ax + b \pmod{p},$$

b

u yerda:

p – tub son - modulyar maydonning asosiy moduli,

$a, b \in \mathrm{F}_p$ – egri chiziq parametrlaridir.

Egri chiziq diskriminanti $\Delta = 4a^3 + 27b^2 \neq 0 \pmod{p}$ bo‘lishi kerak, ya’ni egri chiziq silliq singular bo‘lmagan bo‘lishi talab etiladi. ya’ni

Elliptik egri chiziq ustidagi nuqtalar to‘plami:

$$E(\mathrm{F}_p) = \{(x, y) \in \mathrm{F}_p^2 : y^2 = x^3 + ax + b\} \cup \{O\},$$

bu yerda O – “cheksizlikdagi nuqta” yoki neytral element.

2.2. Nuqta qo‘shish amali.

Agar ikkita nuqta $P = (x_1, y_1)$ va $Q = (x_2, y_2)$ elliptik egri chiziq ustida yotsa, ularning yig‘indisi $R = P + Q = (x_3, y_3)$ quyidagi formulalar bilan hisoblanadi:

$$\lambda = \begin{cases} y_2 - y_1 \pmod{p}, & P \neq Q \\ x - x \\ 2 \quad 1 \\ 3x^2 + a \\ [10pt] \frac{1}{\quad} \pmod{p}, & P = Q \\ 2y_1 \end{cases}$$

$$x_3 = \lambda^2 - x_1 - x_2 \pmod{p},$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \pmod{p}.$$

Bu amal modulyar teskari elementlar orqali hisoblanadi:

$$\lambda_{\text{den}}^{-1} = (x_2 - x_1)^{-1} \pmod p.$$

2.3. Kalit almashinuvi (Elliptic Curve Diffie–Hellman).

Har bir foydalanuvchi elliptik egri ustida bir asosiy nuqtani tanlaydi:

$$P \in E(\mathrm{F}_p).$$

Keyin foydalanuvchilar quyidagicha harakat qiladilar: Alice uchun maxfiy kalit: $d_A \in [1, n-1]$.

Ochiq kalit: $Q_A = d_A P$. Bob uchun maxfiy kalit:

Ochiq kalit: $Q_B = d_B P$.

Umumiy (yashirin) kalit ikki tomonda bir xil qiymatga ega bo‘ladi:

$$S_A = d_A Q_B = d_A d_B P,$$
$$S_B = d_B Q_A = d_B d_A P,$$
$$\Rightarrow S_A = S_B.$$

Natijada ishlatiladi. $S = (x_S, y_S)$ koordinatalaridan hasil bo‘lgan qiymat – umumiy maxfiy kalit sifatida

2.4. Kvant simulyatsiya modeli.

Ushbu tadqiqotda Qiskit muhtida kvant simulyatsiya jarayoni ECC mexanizmining kvant analogini modellashtiradi. Kvant sxema quyidagi bosqichlarni o‘z ichiga oladi:

1. Superpozitsiya yaratish:

$$|0\rangle \xrightarrow{H} \frac{|0\rangle + |1\rangle}{\sqrt{2}}.$$

Bu jarayon Alice va Bob o‘rtasidagi kalit tanlash ehtimolligini ifodalaydi.

2. Isogeniya xaritasi (CNOT darvozasi orqali):

$$|a,b\rangle \xrightarrow{CNOT} |a, a \oplus b\rangle.$$

Bu amal elliptik egri chiziq ustidagi nuqtalar o‘zaro bog‘lanishi jarayoniga mos keladi.

3. O‘lchov (measurement):

Kvant holat o‘lchanadi va $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ natijalar ehtimollik taqsimoti shaklida olinadi:

$$P(ij) = |\langle ij | \psi \rangle|^2.$$

Bu bosqich kvant tarmog‘idagi kalitlarni taqsimlash (Quantum Key Distribution, QKD) jarayonining abstrakt modelini beradi.

2.5. Algoritmik sxema.

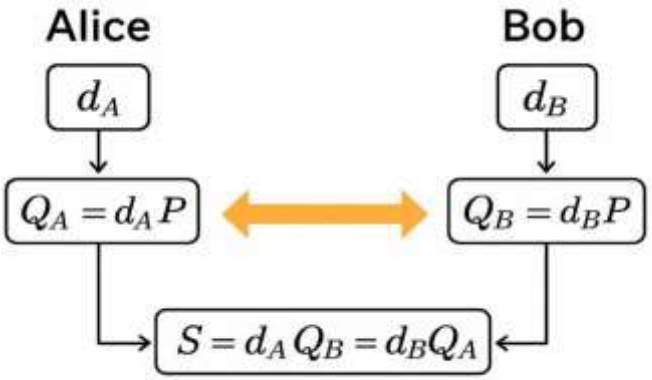
Umumiy kvant–elliptik egri kalit almashinuvi algoritmi quyidagicha tavsiflanadi:

Bosqich 1: Tanlang $E: y^2 = x^3 + ax + b \pmod p, P \in E(\mathrm{F}_p)$.

Bosqich 2: $\text{Alice}: Q_A = d_A P, \quad \text{Bob}: Q_B = d_B P$.

Bosqich 3: $\text{Alice}: S_A = d_A Q_B, \quad \text{Bob}: S_B = d_B Q_A$.

Bosqich 4: $S_A = S_B = d_A d_B P$ (1-rasm).



1-rasm Elliptik egri chiziq (ECC) qismi — matematik kalit hosil qilish bosqichi.

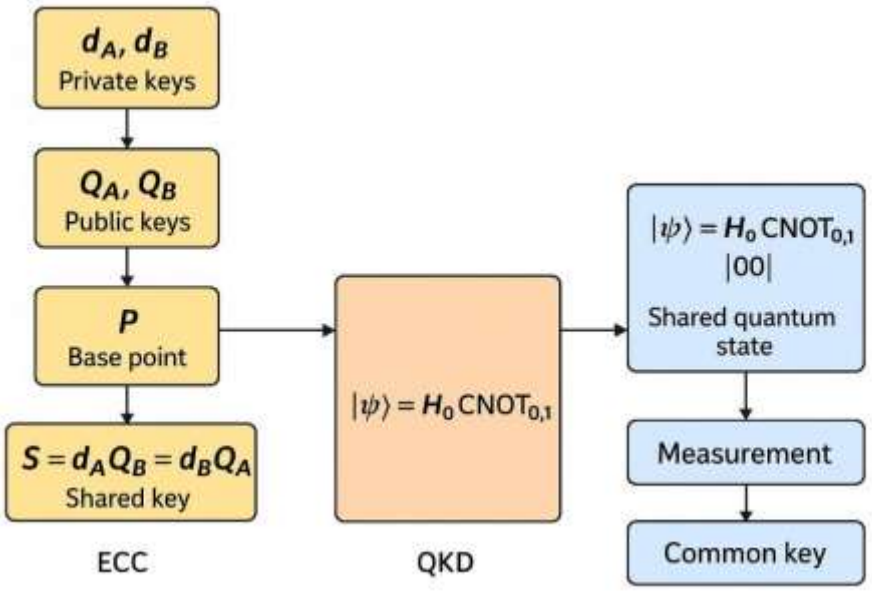
Bosqich 5: Kvant sxemada : $H(0) \rightarrow CNOT(0,1) \rightarrow$ Measure .

Modelning umumiy tuzilmasi.

Metodologiyani quyidagi blok–sxema tarzida ifodalash mumkin:

Klassik ECC hisoblash $\Rightarrow$ Qiskit Kvant ModeliUmumiy $\Rightarrow$ Kalit Tekshiruvi .

Shunday qilib, klassik elliptik egri mekanizmlari kvant sxemadagi superpozitsiya va entanglement jarayonlari bilan uyg‘unlashadi. Bu esa post–kvant davrida ECC algoritmlarining xavfsizlik xususiyatlarini tahlil qilish uchun nazariy asos yaratadi (2-rasm).



2-rasm, Kvant qismi — fizik (kvant) asosda umumiy bitni hosil qilish bosqichi

Ikkalasi bir–birini to‘ldiradi: ECC matematik xavfsizlikni beradi, QKD esa fizik xavfsizlikni ta’minlaydi.

Natijalar

Elliptik egri tanlash.

Biz quyidagi elliptik egri chiziqni olamiz:

$$E : y^2 = x^3 + 2x + 2 \pmod{17}$$

Bu egrichiziq modulyar maydonda, ya’ni barcha hisob–kitoblar 17 ga bo‘linma qoldig‘ida bajariladi. Egri ustidagi boshlang‘ich nuqta (generator) sifatida

Alice va Bob'ning maxfiy kalitlari

Har bir

foydalanuvchi o‘z maxfiy kalitini tanlaydi: Alice $P = (5,1)$ tanlanadi. uchun: $d_A = 5$

Bob uchun: $d_B = 7$

Bu sonlar tasodifiy tanlanadi va sir tutiladi.

Ochiq kalitlarni hisoblash

Har ikkala foydalanuvchi o‘zining ochiq kalitini elliptik egri chiziq ustida hisoblaydi:

$$Q_A = d_A \cdot P, \quad Q_B = d_B \cdot P .$$

Bu degani – nuqta P o‘z–o‘ziga bir necha marta qo‘shiladi.

Masalan:

$$Q_A = 5P = P + P + P + P + P$$

$$Q_B = 7P = P + P + P + P + P + P + P$$

Dasturda bu amallar elliptic_curve_addition() funktsiyasi orqali modulyar arifmetik yordamida hisoblanadi.

Hisoblash natijasida:

$$Q_A = (0,6) .$$

$$Q_B = (13,7) .$$

Bob uchun hisoblash

Bob maxfiy kalit: $d_B = 7 .$

Ochiq kalit:

$Q_B = 7P$.

Bu P ni 7 marta o‘z–o‘ziga qo‘shish degani.

Dasturda hisoblash natijasi:

$Q_B = (13,7)$.

Bu nuqta ham egri $y^2 = x^3 + 2x + 2 \pmod{17}$ ustida yotadi, chunki tekshiramiz:

Chap tomoni: $y^2 = 7^2 = 49 \equiv 49 \pmod{17} = 49 - 34 = 15$.

O‘ng tomoni: $x^3 + 2x + 2 = 13^3 + 2(13) + 2 = 2197 + 26 + 2 = 2225 \equiv 2225 - 17 \times 130 = 2225 - 2210 = 15$.

Tenglik to‘g‘ri: $y^2 \equiv x^3 + 2x + 2 \pmod{17}$.

Demak, $Q_B = (13,7)$ haqiqatan ham egri ustida yotadi.

$Q_A =$

$Q_B = (0,6)$ – bu Alice'ning ochiq kaliti, ya’ni u P ni 5 marta o‘z–o‘ziga qo‘shib olgan.

$(13,7)$ – bu Bob'ning ochiq kaliti, ya’ni u P ni 7 marta o‘z–o‘ziga qo‘shib olgan.

Har biri bu qiymatni ochiq kanalda yuboradi, lekin o‘z maxfiy sonini hech kimga bermaydi.

Keyin ular bu nuqtalar yordamida umumiy kalitni topadilar tomon bir xil kalitga ega bo‘ladi.

Umumiy kalitni hisoblash

Endi ular o‘zaro umumiy kalitni topadilar: $S = d_A Q_B = d_B Q_A$va natijada ikkala

Alice hisoblaydi:

$S_A = d_A \cdot Q_B$,

Bob hisoblaydi: , $S_B = d_B \cdot Q_A$.

Matematik jihatdan ikkisi ham bir xil qiymatga ega: $S_A = S_B = d_A d_B P$.

Dasturda bu ham ketma–ket qo‘shish orqali amalga oshiriladi.

Natija:

$S_A = S_B = (10,6)$.

Demak, ikkala foydalanuvchi bir xil umumiy kalitga ega bo‘ldi.

Natijani tahlil qilish

Alice va Bob klassik qismda umumiy kalitni topdi:

$S = (10,6)$

Kvant qismda ular superpozitsiya va entanglement orqali isogeniya munosabatini kvant simulyatsiyada modellashtirishdi.

Bu degani:

Klassik qism $\rightarrow$ Kalitni hisoblaydi.

Kvant qism $\rightarrow$ Kalit almashinuvi jarayonini xavfsiz kanal orqali tasvirlaydi.

Elliptik egri chiziq qismi orqali matematik umumiy nuqta hasil bo‘ladi: $S = (x_S, y_S)$. Bu raqamli (klassik) umumiy kalit.

Kvant qismi esa bu kalitning fizik parallelini yaratadi ya’ni:

Alice va Bob entanglement orqali bir xil kvant bit (0 yoki 1) hasil qiladilar. O‘lchovdan so‘ng, ular bu bitlardan umumiy shifrlash kalitini shakllantirradilar (masalan, 1010110).

Shunday qilib:

Klassik ECC kalit $(S) \Rightarrow$ Kvant kalit bitlari (entangled pair) .

Xulosa. Ushbu ishda klassik Elliptik egri chiziq kriptografiyasi va kvant kalit almashinuvi mexanizmlarining gibrid birikmasi asosida xavfsiz aloqa tizimini yaratish yondashuvi taklif qilindi. Taklif etilgan modelda avvalo elliptik egri ustida d_A, d_B maxfiy kalitlar yordamida ochiq kalitlar Q_A, Q_B hosil qilindi hamda ular orqali umumiy maxfiy kalit $S = d_A Q_B = d_B Q_A$ aniqlanadi. Ushbu kalit klassik matematik xavfsizlikni ta'minlasa, keyingi bosqichda kvant sxemasi orqali (Hadamard va CNOT eshiklari yordamida) kvant entanglement holati $|\psi\rangle = H_0 CNOT_{0,1} |00\rangle$ hasil qilinib, o'lchov natijasida ikkala tomon ham bir xil kvant bitga ega bo'ladi.

Natijada, gibrid kriptotizim ikkita mustahkam xavfsizlik mexanizmini – klassik hisoblash murakkabligi va kvant fizik qonunlariga asoslangan noaniqlikni — birlashtiradi. Bunday yondashuvning afzalligi shundaki, u kelajakda kvant kompyuterlar tomonidan klassik ECC tizimlarining buzilish xavfini kamaytiradi va ma'lumot almashishning mutlaq xavfsizligini ta'minlaydi. Tadqiqot natijalari ushbu modelni kvant xavfsiz tarmoqlar, blokcheyn tizimlari va post–kvant kriptografiya sohalarida qo'llash imkoniyatlarini ochib beradi.

Foydalanilgan adabiyotlar

1. **Swan M.** *Blockchain: Blueprint for a New Economy*. — Sebastopol, CA, USA: O'Reilly Media, 2015. — 352 p.
2. **Bennett C. H., Brassard G.** Quantum cryptography: Public key distribution and coin tossing // *Proc. IEEE Int. Conf. Comput. Syst. Signal Process.* — 1984. — P. 175–179.
3. **Lenstra A. K., Verheul E. R.** Selecting cryptographic key sizes // *Journal of Cryptology*. — 2001. — Vol. 14, № 4. — P. 255–293.
4. **Shor P. W.** Polynomial–time algorithms for prime factorization and discrete logarithms on a quantum computer // *SIAM Review*. — 1997. — Vol. 41, № 2. — P. 303–332.
5. **Diffie W., Hellman M. E.** New directions in cryptography // *IEEE Transactions on Information Theory*. — 1976. — Vol. 22, № 6. — P. 644–654.
6. **Rivest R. L., Shamir A., Adleman L.** A method for obtaining digital signatures and public–key cryptosystems // *Communications of the ACM*. — 1978. — Vol. 21, № 2. — P. 120–126.
7. **Koblitz N.** Elliptic curve cryptosystems // *Mathematics of Computation*. — 1987. — Vol. 48, № 177. — P. 203–209.
8. **Miller V. S.** Use of elliptic curves in cryptography // *Advances in Cryptology — CRYPTO '85*. — 1986. — P. 417–426.
9. **Menezes A. J., van Oorschot P. C., Vanstone S. A.** *Handbook of Applied Cryptography*. — Boca Raton: CRC Press, 1996. — 780 p.
10. **Gentry C.** Fully homomorphic encryption using ideal lattices // *Proceedings of the 41st Annual ACM Symposium on Theory of Computing (STOC '09)*. — 2009. — P. 169–178.
11. **Joye M., Yen S.–M.** The Montgomery power ladder in elliptic curve cryptography // *Cryptology ePrint Archive*, Report 2002/088. — 2002. — URL: https://eprint.iacr.org/2002/088.
12. **Galbraith S. D., Lin X.** Implementing cryptographic pairings // *Post–Quantum Cryptography*. — 2011. — P. 265–289.
13. **Hoffstein J., Pipher J., Silverman J. H.** *An Introduction to Mathematical Cryptography*. — New York: Springer Science & Business Media, 2008. — 512 p.
14. **Menezes A., Vanstone S.** Practical Cryptography in the Global Computing Environment // *Proceedings of the 1st Workshop on Cryptography and Network Security*. — 1994. — P. 1–16.
15. **Wang W.** A blockchain–based quality acceptance system for construction projects with human–computer interaction // *Proc. Int. Conf. Eng. Constr. Manage. Innov.* — 2024. — P. 300–305.

16. **Zhang G.** et al. A blockchain–based method and system for the quality acceptance of concealed engineering // *Proc. Int. Symp. Cybersecurity Inf. Secur.* — 2024. — P. 20–25.

17.Zubayda Jumayeva, Nurbek Khushvaktov, Rustam Nizomov. BIO Web Conf., 173 (2025) 01030. DOI:https://doi.org/10.1051/bioconf/202517301030

АЛГОРИТМИЗАЦИЯ И ПРИМЕНЕНИЕ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ В РЕШЕНИИ ЗАДАЧ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Дариев Хайрулла
Старший преподаватель филиала Казанского федерального университета (Приволжский регион) в г. Джизаке.

KDariev@kpfu.ru
Ибрагимов Зойиржон Зиятович
и.о. доцент кафедры «К и ПИ» Джизакского политехнического института. zoyirjon.ibragimov@gmail.com

Аннотация: В данной статье рассматриваются вопросы алгоритмизации и применения математических моделей при решении задач искусственного интеллекта. Особое внимание уделяется роли математических методов в построении эффективных алгоритмов, обеспечивающих обработку и анализ данных. Рассматриваются основные подходы к формализации задач, методы оптимизации и моделирования, а также их применение в интеллектуальных системах. Показано, что интеграция алгоритмических и математических подходов позволяет повысить точность, скорость и надежность решений в системах искусственного интеллекта.

Ключевые слова: искусственный интеллект, алгоритмизация, математические модели, оптимизация, анализ данных, интеллектуальные системы, моделирование, алгоритмы.

ALGORITHMIZATION AND THE APPLICATION OF MATHEMATICAL MODELS IN SOLVING ARTIFICIAL INTELLIGENCE PROBLEMS

Dariyev Khayrulla
Senior Lecturer at the Branch of Kazan Federal University (Volga Region) in Jizzakh KDariev@kpfu.ru
Ibragimov Zoyirjon Ziyatovich
Acting Associate Professor of the Department "Computer and Software Engineering"
Jizzakh Polytechnic Institute
zoyirjon.ibragimov@gmail.com

Abstract: This article examines the issues of algorithmization and the application of mathematical models in solving artificial intelligence problems. Particular attention is paid to the role of mathematical methods in the development of efficient algorithms for data processing and analysis. The main approaches to problem formalization, optimization methods, and modeling techniques are considered, as well as their application in intelligent systems. It is shown that the integration of algorithmic and mathematical approaches improves the accuracy, speed, and reliability of solutions in artificial intelligence systems.

Keywords: artificial intelligence, algorithmization, mathematical models, optimization, data analysis, intelligent systems, modeling, algorithms.

SUN’IY INTELLEKT MASALALARINI YECHISHDA ALGORITMLASHTIRISH VA MATEMATIK MODELLARNI QO‘LLASH