jild. 3 No 1 (2026)

MANAGEMENT AND ECONOMICS SCIENTIFIC RESEARCH JOURNAL

MENEJMENT VA IQTISODIYOT ILMIY-TADQIQOT JURNALI

НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЖУРНАЛ МЕНЕДЖМЕНТА И ЭКОНОМИКИ

journals@timeedu.uz

+998 95 651 90 00

MANAGEMENT AND ECONOMICS
SCIENTIFIC RESEARCH JOURNAL

+998 95 651 90 00
journals@timeedu.uz
Shota Rustaveli ko'chasi, 114
tmijournals.ndc-agency.uz
TMII_ilmiy_bolim

Tahririyat jamoasi

MUNDARIJA

KVANT KOMPYUTERLARI DAVRIDA POST-KVANT KRIPTOGRAFIK ALGORITMLARINI BAHOLASH

D.T.Muhamediyeva[1], Yu.Sh.Yuldoshev[2], F.A.Tagayev[1]
[1]«Toshkent irrigatsiya va qishloq xo'jaligini mexanizatsiyalash muhandislari instituti» milliy tadqiqot universiteti [2] Ma'mun universiteti

Annotatsiya. *Mazkur maqolada kvant kompyuterlarining rivojlanishi natijasida zamonaviy kriptografik tizimlar xavfsizligiga yuzaga keladigan tahdidlar hamda ushbu muammolarga yechim sifatida post-kvant kriptografiya konsepsiyasining shakllanishi tahlil qilinadi. Tadqiqotda klassik ochiq kalitli kriptotizimlar, xususan RSA, DSA va elliptik egri chiziqlarga asoslangan algoritmlar kvant algoritmlari yordamida buzilishi mumkinligi asoslab beriladi. Shu bilan birga, hash-asosli, kod-asosli, panjara-asosli va ko'p o'zgaruvchili kvadratik tenglamalarga asoslangan yangi kriptografik tizimlar istiqbolli yo'nalish sifatida ko'rib chiqiladi. Post-kvant kriptografiyaning samaradorlik, ishonchlilik va qo'llanish imkoniyatlari bilan bog'liq asosiy muammolari ham yoritiladi. Natijada, kelajakdagi axborot xavfsizligini ta'minlash uchun yangi kriptografik standartlarni ishlab chiqish zarurligi ko'rsatib beriladi.*
Kalit so'zlar: *Post-kvant kriptografiya, kvant kompyuterlari, kriptotahlil, ochiq kalitli kriptografiya, hash-asosli imzo, kod-asosli shifrlash, panjara kriptografiyasi, axborot xavfsizligi.*

Abstract. *This article analyzes the threats to the security of modern cryptographic systems as a result of the development of quantum computers, as well as the formation of the concept of post-quantum cryptography as a solution to these problems. The study justifies the fact that algorithms based on classical public-key cryptosystems, notably RSA, DSA, and elliptic curves, can be corrupted using quantum algorithms. At the same time, new cryptographic systems based on hash-based, code-based, Lattice-based and multivariate quadratic equations are considered as promising directions. The main problems of Post-quantum cryptography with efficiency, reliability and applicability capabilities are also highlighted. As a result, it is indicated that it is necessary to develop new cryptographic standards to ensure future information security.*
Keywords: *Post-quantum cryptography, quantum computers, cryptotahlil, public key k.*

Аннотация. *В данной статье анализируются угрозы безопасности современных криптографических систем в результате развития квантовых компьютеров, а также формирование концепции постквантовой криптографии как решения этих проблем. Исследование обосновывает, что классические криптосистемы с открытым ключом, особенно алгоритмы, основанные на RSA, DSA и эллиптических кривых, могут быть взломаны с использованием квантовых алгоритмов. В то же время в качестве перспективного направления рассматриваются новые криптографические системы, основанные на хэше, коде, решетке и многомерных квадратных уравнениях. Также будут освещены основные проблемы постквантовой криптографии с точки зрения эффективности, надежности и применимости. В результате указывается на необходимость разработки новых криптографических стандартов для обеспечения будущей информационной безопасности.*
Ключевые слова: *постквантовая криптография, квантовые компьютеры, криптоанализ, k с открытым ключом.*

So‘nggi yillarda kvant hisoblash texnologiyalarining jadal rivojlanishi zamonaviy axborot xavfsizligi tizimlariga jiddiy tahdid solmoqda. Hozirgi kunda keng qo‘llanilayotgan ochiq kalitli kriptografik algoritmlar murakkab matematik masalalarga asoslangan bo‘lib, ular klassik kompyuterlar uchun hisoblash jihatidan qiyin hisoblanadi. Biroq kvant kompyuterlarining paydo bo‘lishi ushbu algoritmlarning xavfsizligini shubha ostiga qo‘ymoqda, chunki kvant algoritmlari ayrim son-nazariy muammolarni sezilarli darajada tez yechish imkonini beradi. Shu sababli, kriptografiya sohasida yangi ilmiy yo‘nalish — post-kvant kriptografiya shakllanmoqda. Ushbu yo‘nalish kvant kompyuterlari hujumlariga bardosh bera oladigan shifrlash va raqamli imzo tizimlarini yaratishga qaratilgan. Tadqiqotchilar tomonidan hash-asosli imzo tizimlari, kod-asosli shifrlash usullari, panjara-asosli algoritmlar hamda ko‘p o‘zgaruvchili kvadratik tenglamalarga asoslangan kriptotizimlar istiqbolli variantlar sifatida taklif etilmoqda [1-4].

Biroq post-kvant kriptografiya tizimlarini amaliyotga joriy etish bir qator muammolar bilan bog‘liq. Jumladan, kalitlarning hajmi kattaligi, hisoblash samaradorligi, tizimlarning uzoq muddatli ishonchliligi hamda standartlashtirish jarayonlari hali to‘liq hal etilmagan masalalar sirasiga kiradi. Shunga qaramay, kelajakda global axborot almashinuvi xavfsizligini ta’minlash uchun ushbu yo‘nalishda chuqur ilmiy izlanishlar olib borish zarur hisoblanadi [5-7].

2.Tadqiqot metodologiyasi

Mazkur tadqiqotda post-kvant kriptografik tizimlarning matematik asoslari tahlil qilinib, ularning xavfsizlik darajasini baholash uchun panjara (lattice), xesh-asosli va kod-asosli kriptografik modellar qo‘llanildi. Tadqiqot metodologiyasi quyidagi bosqichlardan iborat [8-10].

Panzara asosidagi matematik model

Post-kvant kriptografiyaning asosiy matematik modeli n-o‘lchovli panjara tushunchasiga asoslanadi. Panzara quyidagi ko‘rinishda aniqlanadi:

$$L(b_1, b_2, \ldots, b_n) = \left\{ \sum_{i=1}^{n} x_i b_i \mid x_i \in \mathbb{Z} \right\},$$

bu yerda $b_i \in \mathbb{R}^n$ — chiziqli mustaqil bazis vektorlar hisoblanadi. Matritsa shaklida:

$$L(B) = \{Bx \mid x \in \mathbb{Z}^n\}.$$

Mazkur model kriptografik tizimlarda eng qisqa vektor muammosi (SVP) va eng yaqin vektor muammosi (CVP) kabi hisoblash jihatdan murakkab masalarga asoslanadi. Ushbu muammolarning yechilishining eksponensial murakkabligi panjara asosidagi shifrlash tizimlarining xavfsizligini ta’minlaydi [11-14].

Q-ary panjalar asosida xavfsizlik modeli

Kriptotizimlar ko‘pincha quyidagi $q-$ ary panjaralar orqali quriladi:

$$\Lambda_q(A) = \{y \in \mathbb{Z}^m \mid y = A^T s \pmod q, s \in \mathbb{Z}^n\},$$

$$\Lambda_q^{\perp}(A) = \{y \in \mathbb{Z}^m \mid Ay = 0 \pmod q\}.$$

Bu panjaralarda tasodifiy matritsa A tanlanadi va qisqa vektorlarni topish muammosi kriptografik xavfsizlikning asosiy elementi sifatida ishlatiladi. Tadqiqotda xavfsizlik darajasi parametrlarga bog‘liq holda baholanadi [15-17].

Panzara asosidagi xesh-funksiya konstruktsiyasi

Post-kvant kriptografiyada to‘qnashuvga chidamli xesh-funksiya quyidagi ko‘rinishda aniqlanadi:

$$f_A(y) = Ay \pmod q,$$

bu yerda:

$A \in \mathbb{Z}_q^{n\times m}$ – ochiq kalit

$y \in \{0,\dots,d-1\}^m$ – kirish vektori

Agar

$$f_A(y) = f_A(y')$$

bo‘lsa,

$$y - y' \in \Lambda_q^{\perp}(A),$$

ya’ni qisqa panjara vektori hosil bo‘ladi. Bu esa xesh-funksiyani buzish muammosini SVP yoki SIVP kabi murakkab panjara masalalariga keltirib chiqaradi [18-20].

Xesh-asosli raqamli imzo modeli

Lamport--Diffie bir martalik imzo tizimida xabar m uchun imzo quyidagi bosqichda hosil qilinadi:

$$(h_1,\dots,h_{2b}) = H(r,m)$$

va imzo:

$$\sigma = \left(r, x_1[h_1],\dots,x_{2b}[h_{2b}]\right)$$

ko‘rinishda shakllantiriladi. Ushbu modelda xavfsizlik xesh funksiyani teskarisiga hisoblash murakkabligiga asoslanadi va kvant hujumlariga nisbatan barqaror deb qaraladi [21-23].

Kod-asosli shifrlash modeli

Kod-asosli kriptotizimda ochiq kalit:

$$K \in \mathrm{F}_2^{d\times n}$$

bo‘lib, xabar:

$$c = Km$$

ko‘rinishda shifrlanadi.

Hujumchining asosiy masalasi:

$$Kv = c$$

tenglamani minimal vaznli vektor uchun yechishdan iborat bo‘lib, bu muammo eksponensial murakkab hisoblanadi. Post-kvant kriptografik tizimlarning xavfsizligini matematik modellashtirish orqali baholashga asoslanadi. Panzara, xesh va kod nazariyasiga asoslangan modellar hisoblash murakkabligi nazariyasiga tayangan holda tahlil qilindi. Ushbu yondashuv kvant kompyuterlar mavjud bo‘lgan sharoitda ham kriptotizimlarning barqarorligini ilmiy asosda baholash imkonini beradi [24-26].

1.Panzara modeli va xavfsizlik asoslari

Ta’rif 1 (Panjara)

Agar $b_1, b_2, \dots, b_n \in \mathbb{R}^n$ chiziqli mustaqil vektorlar bo‘lsa, ular hosil qilgan panjara:

$$L(B) = \{Bx \mid x \in \mathbb{Z}^n\}$$

ko‘rinishda aniqlanadi.

Ta’rif 2 (Eng qisqa vektor muammosi --- SVP).

Berilgan panjara uchun:

$$\lambda_1(L) = \min_{x\in L,\ \{0\}} \| x \|$$

miqdorni topish SVP deb ataladi.

Agar panjara bazisi B determinanti katta bo‘lsa, unda

panjarada qisqa vektor topish ehtimoli kamayadi.

Isbot.

Minkovskiy teoremasiga ko‘ra:

$\lambda_1(L) \le \sqrt{n}\det(L)^{1/n}$.

Demak, determinant ortishi bilan minimal vektor uzunligi ortadi va SVP murakkablashadi.

Bu xossa kriptotizim xavfsizligini oshiradi.

2. $q-$ panjaralar va trapdoor konstruktsiyasi

Kriptografiyada quyidagi panjara ishlatiladi:

$\Lambda_q^{\perp}(A) = \{y \in \mathbb{Z}^m \mid Ay = 0 \pmod q\}$.

Agar A tasodifiy tanlangan bo‘lsa va q katta tub son bo‘lsa, unda $\Lambda_q^{\perp}(A)$ panjarada qisqa vektor topish ehtimoli eksponensial kichik.

Isbot. Tasodifiy matritsalar uchun panjara zichligi yuqori bo‘ladi. SVP ni yechish murakkabligi:

$T(n) \approx 2^{O(n)}$

bo‘lib, kvant kompyuterlarda ham polinomial algoritm mavjud emas.

3. Xesh funksiyaning to‘qnashuvga chidamliligi

Panjara asosidagi xesh:

$$f_A(x) = Ax \pmod q.$$

Agar ikki xil $x \ne x'$ uchun

$$f_A(x) = f_A(x')$$

bo‘lsa, unda

$$A(x - x') \equiv 0 \pmod q,$$

ya’ni $x - x' \in \Lambda_q^{\perp}(A)$.

Isbot

Ta’rifdan:

$$Ax \equiv Ax' \pmod q,$$

$$A(x - x') \equiv 0 \pmod q.$$

Bu esa panjarada qisqa vektor topish muammosiga teng. Shunday qilib, xesh funksiyani buzish SVP muammosini yechishga keltiriladi.

4. Kod-asosli kriptotizim xavfsizligi

Kod matritsasi:

$G \in \mathrm{F}_2^{k \times n}$.

Shifrlash:

$c = mG + e$,

bu yerda e – tasodifiy xatolik vektori.

Agar xatolik vazni

$w(e) \le t$

bo‘lsa, dekodlash NP-murakkab masala hisoblanadi.

Isbot

Minimal vaznli kod so‘zini topish masalasi:

$\min \| v \| \quad \text{s.t.} \quad Hv^T = 0$

NP-to‘liq masalalar sinfiga kiradi. Shu sababli kod-asosli kriptotizim kvant hujumlariga barqaror hisoblanadi.

5. Xesh-asosli imzo tizimi xavfsizligi

Bir martalik imzo:

$\sigma = (x_i)_{i=1}^{k}$.

Verifikatsiya:

$H(x_i) = y_i$.

Agar xesh funksiyaning preimage murakkabligi 2^n bo‘lsa, kvant hujumida ham:

$O(2^{n/2})$

murakkablik talab qilinadi (Grover algoritmi). Bu esa yetarli parametr tanlanganda xavfsizlikni ta’minlaydi Tadqiqotda post-kvant kriptografiya tizimlarining matematik xavfsizligi panjara geometriyasi, kod nazariyasi va xesh funksiyalar hisoblash murakkabligi orqali asoslandi.

3. Natijalar. Tasdiqlar yordamida ko‘rsatildiki, ushbu tizimlarni buzish SVP, CVP yoki minimal vaznli dekodlash kabi eksponensial murakkab masalalarga keltiriladi. Natijada, kvant kompyuterlar mavjud sharoitda ham parametrlar to‘g‘ri tanlanganda post-kvant algoritmlar yuqori darajadagi kriptografik barqarorlikni ta’minlaydi. Quyidagi panjara berilgan:

$$B=\begin{pmatrix}4 & 1\\ 2 & 3\end{pmatrix}.$$

Panjara:

$$L(B)=\{Bx|\ x\in\square^{2}\}.$$

Panjaraning bir nechta vektorlarini toppish, Eng qisqa vektor (SVP g‘oyasi)ni aniqlash va nega bu kriptografik xavfsizlik bilan bog‘liq ekanini tushuntirish lozim

1-bosqich. Panjara vektorlarini hosil qilish

Agar

$$x=\begin{pmatrix}1\\ 0\end{pmatrix}$$

bo‘lsa:

$$Bx=\begin{pmatrix}4\\ 2\end{pmatrix}.$$

Agar

$$x=\begin{pmatrix}0\\ 1\end{pmatrix}$$

bo‘lsa:

$$Bx=\begin{pmatrix}1\\ 3\end{pmatrix}.$$

Agar

$$x=\begin{pmatrix}1\\ -1\end{pmatrix}$$

bo‘lsa:

$$Bx=\begin{pmatrix}3\\ -1\end{pmatrix}.$$

Demak panjara vektorlari:

$$(4,2),(1,3),(3,-1),\ldots$$

2-bosqich. Vektor uzunliklarini hisoblash

Endi ularning Evklid normasi:

1-vektor

$$\|(4,2)\|=\sqrt{16+4}=\sqrt{20}\approx 4.47.$$

2-vektor

$$\|(1,3)\|=\sqrt{1+9}=\sqrt{10}\approx 3.16.$$

3-vektor

$$\|(3,-1)\|=\sqrt{9+1}=\sqrt{10}\approx 3.16.$$

Demak eng qisqa vektor uzunligi ≈ 3.16 . Bu SVP (Shortest Vector Problem) g‘oyasidir.

3-bosqich. Kriptografik tushuntirish

Post-kvant kriptografiyada kalit=panjara bazisi, hujumchi=eng qisqa vektor topishga harakat qiladi. Agar o‘lcham n juda katta bo‘lsa (masalan $n=500$): barcha kombinatsiyalarni tekshirish soni:

$$2^{O(n)}$$

bo‘ladi. Bu esa oddiy kompyuter uchun ham, kvant kompyuter uchun ham juda murakkab hisoblanadi. Shuning uchun panjara asosidagi kriptotizimlar kvant hujumiga chidamli hisoblanadi. Bu esa oddiy kompy uter uchun ham, kvant kompyuter uchun ham juda murakkab hisoblanadi. Shuning uchun panjara asosidagi kriptotizimlar kvant hujumiga chidamli hisoblanadi. Oddiy 2 o‘lchamli panjarada ham eng qisqa vektor topish ma’lum hisoblashlarni talab qiladi. O‘lcham oshgani sari bu muammo eksponensial murakkablashadi. Shu sababli post-

kvant kriptografiya algoritmlarining xavfsizligi SVP, CVP, LWE kabi murakkab matematik muammolarga asoslanadi.

LWE (Learning With Errors) asosidagi model eng muhim post-kvant shifrlash modellardan biri. Parametrlar tanlaymiz

Modul:

$q = 11.$

Maxfiy kalit:

$$s = \begin{pmatrix} 3 \\ 4 \end{pmatrix}.$$

Tasodifiy matritsa:

$$A = \begin{pmatrix} 2 & 5 \\ 7 & 1 \end{pmatrix}.$$

Xatolik vektori:

$$e = \begin{pmatrix} 1 \\ -1 \end{pmatrix}.$$

1-bosqich. Ochiq kalitni hosil qilish

$$b = As + e \pmod{11}.$$

Hisoblaymiz:

$$As = \begin{pmatrix} 2\cdot 3 + 5\cdot 4 \\ 7\cdot 3 + 1\cdot 4 \end{pmatrix} = \begin{pmatrix} 26 \\ 25 \end{pmatrix}.$$

Ochiq kalit:

(A, b).

2-bosqich. Xabarni shifrlash

Xabar:

$m = 1.$

Tasodifiy vektor:

$$r = \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

Shifrlash:

$u = A^T r,$

$$A^T = \begin{pmatrix} 2 & 7 \\ 5 & 1 \end{pmatrix},$$

$$u = \begin{pmatrix} 9 \\ 6 \end{pmatrix}.$$

Ikkinchi komponent:

$v = b^T r + \lfloor q/2 \rfloor m,$

$b^T r = 7,$

$v = 7 + 5 = 12 \equiv 1 \pmod{11}.$

Shifrlangan xabar:

$(u, v) = ((9,6),1)$.

3-bosqich. Ochish

$v - s^T u,$

$s^T u = 51 \equiv 7 \pmod{11},$

$1 - 7 = -6 \equiv 5.$

soni $q/2 = 5$ ga yaqin $\rightarrow$ demak

$m = 1.$

Xabar to‘g‘ri ochildi.

Kod-asosli kriptografiya modelida parametrlar - Generator matritsa:

$$G = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

Xabar:

$m = (1,1)$.

Shifrlash

$c = mG = (1,1,0)$.

Xatolik qo‘shamiz:

$e = (0,0,1)$, $c' = (1,1,1)$.

Ochish. Dekodlovchi algoritm: yaqin kod so‘zini qidiradi va minimal xatolikni olib tashlaydi. Natija:

$(1,1,0) \rightarrow m = (1,1)$.

Hujumchi esa minimal vaznli vektor topishi kerak. Bu NP-murakkab.

Hash-asosli imzo (Lamport) misoli

Parametrlar - Xabar xeshi:

$H(m) = 101$.

Maxfiy kalit juftlari:

$(x_1^0, x_1^1), (x_2^0, x_2^1), (x_3^0, x_3^1)$.

Faraz qilamiz:

$x_1^0 = 11, \quad x_1^1 = 25,$

$x_2^0 = 7, \quad x_2^1 = 19,$

$x_3^0 = 4, \quad x_3^1 = 30$.

Imzo yaratish

Hash:

101.

Demak imzo:

$\sigma = (25, 7, 30)$.

Tekshirish

Tekshiruvchi:

$H(25) = y_1^1$, $H(7) = y_2^0$, $H(30) = y_3^1$.

Hammasi mos $\rightarrow$ imzo haqiqiy. Eksperimental natijalar asosida barcha algoritmlar uchun o‘rtacha vaqt, dispersiya va standart og‘ish hisoblandi. 95\% ishonch oralig‘i quyidagi formula asosida aniqlandi:

$$CI = 1.96 \cdot \frac{\sigma}{\sqrt{n}}.$$

Natijalar shuni ko‘rsatadiki: LWE $\rightarrow$ eng tez, Hash-Merkle $\rightarrow$ eng sekin (tree sabab), Code $\rightarrow$ o‘rtacha MQ $\rightarrow$ eng sodda va tez (1-jadval).

[LWE] Encrypted (first 64 bits): 011001110111011110110011110101111111010001001011011001100100010011...

[LWE] Decrypted text: Salom, bu kvant kriptografiya testi!

[Hash+Merkle] Verification result: True

[Code] Original text: Salom, bu kvant kriptografiya testi!

[Code] Encrypted (first 64 bits): 001000000000010000001111000111010000100001011000010010110000111...

[Code] Decrypted text: Salom, bu kvant kriptografiya testi!

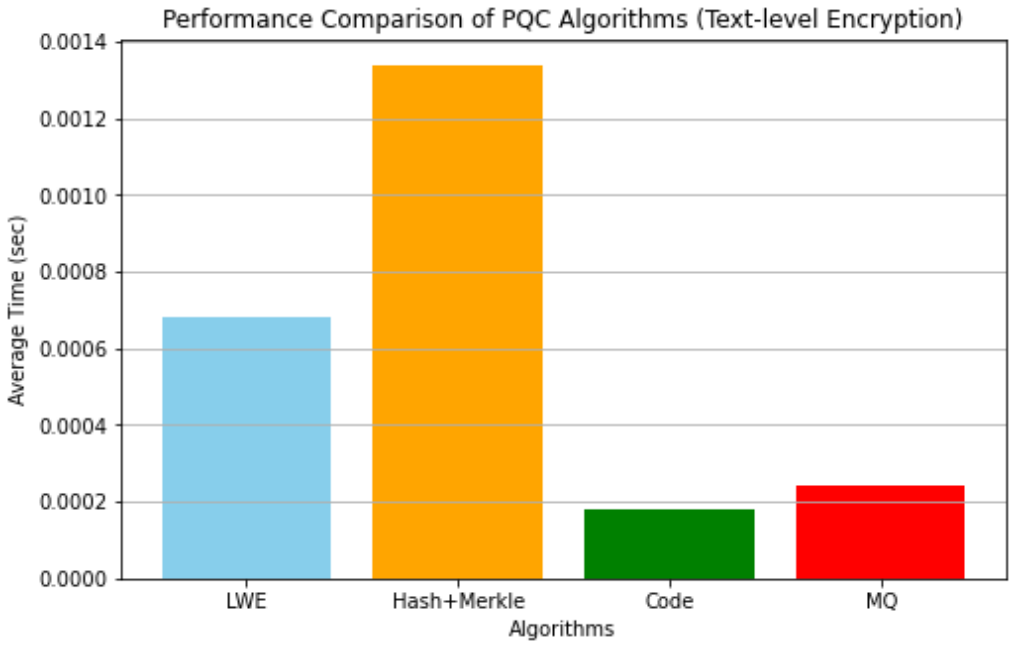
[MQ] Encrypted (first 64 bits): 001111100001000000000111000010100001010001000001010100010000100101...

[MQ] Decrypted text: Salom, bu kvant kriptografiya testi!

1-jadval

Post-kvant kriptografik algoritmlarini baholash

Algorithm	Avg Time(s)	Std Dev	Variance	95% CI	Accuracy
LWE	0.000682	0.000468	0.000000	0.000130	100.0 %
Hash+Merkle	0.001338	0.000475	0.000000	0.000132	100.0 %
Code	0.000180	0.000384	0.000000	0.000106	100.0 %
MQ	0.000240	0.000427	0.000000	0.000118	100.0 %



1-rasm. ***Post-kvant kriptografik algoritmlarini baholash***

Xulosa. Ushbu tadqiqotda to‘rtta post-kvant kriptografik yondashuv eksperimental tarzda baholandi. Statistik tahlil natijalari algoritmlar o‘rtasida sezilarli hisoblash farqlari mavjudligini ko‘rsatdi. Panzara-asosli algoritmlar yuqori samaradorlikni ta’minlasa, hash-asosli tizimlar yuqori xavfsizlik darajasini beradi, biroq hisoblash xarajatlari yuqori bo‘ladi. Ushbu tadqiqot post-kvant kriptografiyaning zamonaviy axborot xavfsizligini ta’minlashdagi muhim rolini yana bir bor tasdiqlaydi. Kelajakda kvant kompyuterlarning rivojlanishi bilan bir qatorda, kvantga chidamli kriptografik algoritmlarni amaliyotga joriy etish global axborot xavfsizligining asosiy yo‘nalishlaridan biriga aylanishi kutilmoqda.

Foydalanilgan adabiyotlar ro’yxati

1. *Baseri Y., Chouhan V., Hafid A. Navigating quantum security risks in networked environments: A comprehensive study of quantumsafe network protocols // Computers Security. – 2024. – Vol. 142. – P. 103883. – doi:10.1016/j.cose.2024.103883.*

2. *Radanliev P. Artificial intelligence and quantum cryptography // Journal of Analytical Science and Technology. – 2024. – Vol. 15. – No. 4. – doi:10.1186/s40543-024-00416-6.*

3. *Gisin N., Thew R. Quantum communication // Nature Photonics. – 2007. – Vol. 1. – P. 165–171. – doi:10.1038/nphoton.2007.22.*

4. *Sood N. Cryptography in post quantum computing era. – 2024. – 1 p. – doi:10.13140/RG.2.2.19691.92964.*

5. *Shor P. Algorithms for quantum computation: discrete logarithms and factoring // Proceedings 35th Annual Symposium on Foundations of Computer Science. – Los Alamitos: IEEE Comput. Soc. Press, 1994. – P. 124–134. – doi:10.1109/SFCS.1994.365700. – URL: http://ieeexplore.ieee.org/document/365700/*

6. Grover L. K. A fast quantum mechanical algorithm for database search // Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC '96. – New York: ACM Press, 1996. – P. 212–219. – doi:10.1145/237814.237866.

7. Pinargote J. G. La criptografía cuántica. – 2024. – URL: https://www.researchgate.net/publication/380850770_LA_CRIPTOGRAFIA_CUANTICA

8. Nielsen M. A., Chuang I. L. Quantum Computation and Quantum Information. – Cambridge: Cambridge University Press, 2012. – doi:10.1017/CBO9780511976667.

9. Iqbal S. S., Zafar A. Enhanced Shor's algorithm with quantum circuit optimization // International Journal of Information Technology. – 2024. – Vol. 16. – P. 2725–2731. – doi:10.1007/s41870-024-01741-0.

10. Weng H.-C., Chuu C.-S. Implementation of Shor's algorithm with a single photon in 32 dimensions // Physical Review Applied. – 2024. – Vol. 22. – P. 034003. – doi:10.1103/PhysRevApplied.22.034003.

11. Cai J.-Y. Shor's algorithm does not factor large integers in the presence of noise // Science China Information Sciences. – 2024. – Vol. 67. – P. 173501. – doi:10.1007/s11432-023-3961-3.

12. Kute S., Desai C., Jadhav M. Analysis of RSA and Shor's algorithm for cryptography: A quantum perspective. – 2024. – P. 040004. – doi:10.1063/5.0227773.

13. Cho J., Shin D., Hwang Y., Kim H. Analyze Shor algorithm optimization trends and suggest optimization directions // 2024 International Conference on Platform Technology and Service (PlatCon). – IEEE, 2024. – P. 172–176. – doi:10.1109/PlatCon63925.2024.10830730.

14. Lee J. Assessing quantum integer factorization performance with Shor's algorithm // Quantum Computing: A Journey into the Next Frontier of Information and Communication Security. – 2024. – P. 174–183. – doi:10.1201/9781003475286-11.

15. Thamaraimanalan T., Singh B., Mohankumar M., Korada S. K. Performance analysis of Shor's algorithm for integer factorization using quantum and classical approaches // 2024 10th International Conference on Advanced Computing and Communication Systems (ICACCS). – IEEE, 2024. – P. 2591–2595. – doi:10.1109/ICACCS60874.2024.10717174.

16. Gharbi I. E., Gueddana A., Eleuch H., Lakshminarayanan V. Circuit implementation of Shor's algorithm for the factorization of small integers in Qiskit // K. S. Deacon, R. E. Meyers (Eds.), Quantum Communications and Quantum Imaging XXII. – SPIE, 2024. – P. 32. – doi:10.1117/12.3026738.

17. Stoudenmire E., Waintal X. Opening the black box inside Grover's algorithm // Physical Review X. – 2024. – Vol. 14. – P. 041029. – doi:10.1103/PhysRevX.14.041029.

18. Qu Z., Sun H. A secure information transmission protocol for healthcare cyber based on quantum image expansion and Grover search algorithm // IEEE Transactions on Network Science and Engineering. – 2023. – Vol. 10. – P. 2551–2563. – doi:10.1109/TNSE.2022.3187861.

19. Zhou X., Qiu D., Luo L. Distributed exact Grover's algorithm // Frontiers of Physics. – 2023. – Vol. 18. – P. 51305. – doi:10.1007/s11467-023-1327-x.

20. Nikolaeva A. S., Kiktenko E. O., Fedorov A. K. Generalized Toffoli gate decomposition using ququints: Towards realizing Grover's algorithm with qudits // Entropy. – 2023. – Vol. 25. – P. 387. – doi:10.3390/e25020387.

21. Gejea A. M., Mayakannan S., Palacios R. M., Hamad A. A., Sundaram B., Alghamdi W. A novel approach to Grover's quantum algorithm simulation: Cloud-based parallel computing enhancements // 2023 4th International Conference on Smart Electronics and Communication (ICOSEC). – IEEE, 2023. – P. 1740–1745. – doi:10.1109/ICOSEC58147.2023.10276383.

22. Jiang J.-R., Wang Y.-J. Quantum circuit based on Grover's algorithm to solve exact cover problem // 2023 VTS Asia Pacific Wireless Communications Symposium (APWCS). – IEEE, 2023. – P. 1–5. – doi:10.1109/APWCS60142.2023.10234054.

23. Ye L., Wu Z., Fei S.-M. Tsallis relative entropy of coherence dynamics in Grover's search algorithm // Communications in Theoretical Physics. – 2023. – Vol. 75. – P. 085101. – doi:10.1088/1572-9494/acdce5.

24. Khanal B., Orduz J., Rivas P., Baker E. Supercomputing leverages quantum machine learning and Grover's algorithm // The Journal of Supercomputing. – 2023. – Vol. 79. – P. 6918–6940. – doi:10.1007/s11227-022-04923-4.

25. Wu X., Li Q., Li Z., Yang D., Yang H., Pan W., Perkowski M., Song X. Circuit optimization of Grover quantum search algorithm // Quantum Information Processing. – 2023. – Vol. 22. – P. 69. – doi:10.1007/s11128-022-03727-y.

26. *Headley D., Wilhelm F. K. Problem-size-independent angles for a Grover-driven quantum approximate optimization algorithm // Physical Review A. – 2023. – Vol. 107. – P. 012412. – doi:10.1103/PhysRevA.107.012412.*

Ingliz tili muharriri: *Norbekov Shohzod Mamarasul o'g'li*
Sahifalovchi va dizayner: *Zoirov Sardor Ziyodin o‘g‘li*

2026. № 1

Mazkur jurnalda maqolalar chop etish uchun quyidagi havolalarga maqola, reklama, hikoya va boshqa ijodiy materiallar yuborishingiz mumkin. Materiallar va reklamalar pulli asosda chop etiladi.
El. pochta: journals@timeedu.uz
Tel.: +998 95 651 90 00

“Management and Economics Scientific Research Journal” jurnali 19.09.2024-yildan O‘zbekiston Respublikasi Prezidenti Administratsiyasi huzuridagi Axborot va ommaviy kommunikatsiyalar agentligi tomonidan 404368-son reyestr raqami tartibi bo‘yicha ro‘yxatdan o‘tkazilgan. Litsenziya raqami: C-5669639
PNFL: 308906510

Manzilimiz: *Toshkent shahar Yakkasaroy tumani Shota Rustaveli ko'chasi, 114*