POST-KVANT KRIPTOGRAFIK ALGORITMLAR SAMARADORLIGINI TAHLIL QILISH VA TAQQOSLASH

Muhamediyeva D.T., Tagayev F.A.
«Toshkent irrigatsiya va qishloq xo‘jaligini mexanizatsiyalash muhandislari instituti» milliy tadqiqot universiteti

DOI: **https://doi.org/10.5281/zenodo.20214958**

Annotatsiya. *Zamonaviy kvant hisoblash texnologiyalarining jadal rivojlanishi an’anaviy kriptografik tizimlar xavfsizligiga jiddiy tahdid solmoqda. Ayniqsa, butun sonlarni faktorizatsiya qilish va diskret logarifm muammolariga asoslangan algoritmlar kvant kompyuterlar yordamida samarali buzilishi mumkin. Shu sababli post-kvant kriptografiya (PQC) kelajak axborot xavfsizligini ta’minlashda muhim yo‘nalish sifatida qaralmoqda. Mazkur maqolada post-kvant kriptografiyaning asosiy yo‘nalishlari — panjara-asosli (lattice-based), kod-asosli (code-based), hash-asosli imzo tizimlari hamda ko‘p o‘zgaruvchili kvadratik tenglamalarga asoslangan kriptotizimlar tahlil qilinadi. Har bir yondashuvning matematik asoslari, algoritmik tuzilishi va hisoblash murakkabligi o‘rganildi. Bundan tashqari, ushbu algoritmlar uchun eksperimental modellar ishlab chiqilib, ularning tezligi, aniqligi va hisoblash samaradorligi taqqoslandi. Olingan natijalar post-kvant algoritmlarning kvant hujumlariga nisbatan yuqori barqarorligini ko‘rsatdi. Shu bilan birga, algoritmlar o‘rtasida samaradorlik va resurs talablariga oid muhim farqlar mavjudligi aniqlandi.*

Kalit so‘zlar. *Post-kvant kriptografiya, panjara-asosli algoritmlar, LWE, hash-asosli imzo, kod-asosli kriptotizimlar, ko‘p o‘zgaruvchili kvadratik tenglamalar, kriptografik xavfsizlik, kvant hisoblash*

Аннотация. *Быстрое развитие современных квантовых вычислительных технологий представляет серьезную угрозу безопасности традиционных криптографических систем. В частности, алгоритмы, основанные на факторизации целых чисел и задачах дискретного логарифма, могут быть эффективно взломаны с помощью квантовых компьютеров. Поэтому постквантовая криптография (ПКВ) рассматривается как важное направление в обеспечении информационной безопасности будущего. В данной статье анализируются основные направления постквантовой криптографии — системы подписи на основе решеток, кодов, хешей и криптосистемы на основе многомерных квадратных уравнений. Изучаются*

математические основы, алгоритмическая структура и вычислительная сложность каждого подхода. Кроме того, для этих алгоритмов были разработаны экспериментальные модели, и проведено сравнение их скорости, точности и вычислительной эффективности. Полученные результаты показали высокую устойчивость постквантовых алгоритмов к квантовым атакам. В то же время были обнаружены существенные различия в эффективности и ресурсоемкости между алгоритмами.

***Ключевые слова**: постквантовая криптография, алгоритмы на основе решеток, LWE, подпись на основе хешей, криптосистемы на основе кодов, многомерные квадратные уравнения, криптографическая безопасность, квантовые вычисления*

***Abstract.** The rapid development of modern quantum computing technologies poses a serious threat to the security of traditional cryptographic systems. In particular, algorithms based on integer factorization and discrete logarithm problems can be effectively cracked using quantum computers. Therefore, post-quantum cryptography (PQC) is considered an important area for ensuring future information security. This article analyzes the main areas of post-quantum cryptography: signature systems based on lattices, codes, hashes, and cryptosystems based on multidimensional quadratic equations. The mathematical foundations, algorithmic structure, and computational complexity of each approach are studied. Furthermore, experimental models were developed for these algorithms, and their speed, accuracy, and computational efficiency were compared. The results demonstrated the high resistance of post-quantum algorithms to quantum attacks. At the same time, significant differences in efficiency and resource consumption were discovered between the algorithms.*

***Keywords:** post-quantum cryptography, lattice-based algorithms, LWE, hash-based signature, code-based cryptosystems, multivariate quadratic equations, cryptographic security, quantum computing*

1.Kirish. Axborot texnologiyalarining jadal rivojlanishi bilan bir qatorda, ma’lumotlar xavfsizligini ta’minlash masalasi tobora dolzarb ahamiyat kasb etmoqda. Biroq kvant kompyuterlarning rivojlanishi ushbu tizimlarning barqarorligiga jiddiy xavf tug‘dirmoqda. Hozirgi kunda keng qo‘llanilayotgan kriptografik tizimlar, xususan RSA va elliptik egri chiziqlarga asoslangan algoritmlar (Elliptic Curve Cryptography), klassik hisoblash modellari sharoitida yuqori darajadagi xavfsizlikni ta’minlaydi. Ularning xavfsizligi murakkab matematik muammolarga — katta sonlarni faktorizatsiya qilish va diskret logarifm masalalariga — asoslanadi. Masalan, RSA

algoritmida ochiq kalit orqali shifrlangan ma’lumotni ochish uchun katta sonni uning tub ko‘paytuvchilarga ajratish talab etiladi. Klassik kompyuterlar uchun bu masala eksponensial vaqt talab qiladi va amaliy jihatdan yechib bo‘lmaydigan darajada murakkab hisoblanadi. Xuddi shuningdek, elliptik egri chiziqlarga asoslangan kriptotizimlarda diskret logarifm muammosi juda murakkab bo‘lib, bu tizimlar kichik kalit o‘lchamlari bilan ham yuqori xavfsizlikni ta’minlaydi.

2. Metodologiya. Klassik kriptografik algoritmlar bir nechta asosiy matematik muammolarga tayanadi (1-jadval):

1-jadval

Klassik kriptografik algoritmlar asosiy matematik muammolari

Muammo	**Algoritmlar**
Faktorizatsiya	RSA
Diskret logarifm	Diffie-Hellman, DSA, ElGamal
Simmetrik transformatsiya	AES
Xesh funksiyalar	SHA-256

Ushbu muammolar klassik kompyuterlar uchun murakkab bo‘lib, yuqori xavfsizlikni ta’minlaydi. Biroq kvant kompyuterlar RSA, DSA, DH ni buzadi. RSA va Elliptic Curve Cryptography algoritmlaridan tashqari, klassik kriptografiyada Diffie–Hellman key exchange kalit almashish protokoli, ElGamal cryptosystem shifrlash algoritmi, Digital Signature Algorithm raqamli imzo tizimi hamda Advanced Encryption Standard simmetrik shifrlash algoritmi keng qo‘llaniladi. Ushbu algoritmlar zamonaviy axborot xavfsizligi infratuzilmasining asosini tashkil etadi va internet kommunikatsiyalari, bank tizimlari, elektron hujjat aylanishi hamda bulutli xizmatlarda faol qo‘llanilib kelinmoqda. Mazkur kriptografik tizimlarning xavfsizligi bir qator murakkab matematik muammolarga asoslanadi. Xususan, RSA algoritmi katta sonlarni tub ko‘paytuvchilarga ajratish (faktorizatsiya) muammosining murakkabligiga tayanadi. Diffie–Hellman, ElGamal va DSA algoritmlarining xavfsizligi esa diskret logarifm muammosiga bog‘liq bo‘lib, bu muammoni klassik kompyuterlar yordamida yechish eksponensial vaqt talab etadi. AES algoritmi esa murakkab algebraik va bitli transformatsiyalar asosida qurilgan bo‘lib, brute-force va differensial hujumlarga nisbatan yuqori darajada barqaror hisoblanadi.

Biroq kvant hisoblash texnologiyalarining rivojlanishi ushbu kriptografik tizimlarning uzoq muddatli xavfsizligiga jiddiy tahdid solmoqda. Ayniqsa, Shor's Algorithm yordamida faktorizatsiya va diskret logarifm masalalarini polinomial vaqt ichida yechish mumkinligi isbotlangan. Bu esa RSA, Diffie–Hellman, DSA va ECC algoritmlarining nazariy jihatdan zaiflashishiga olib keladi. Simmetrik algoritmlar, masalan AES, kvant hujumlariga nisbatan nisbatan barqarorroq bo‘lsa-da, Grover's Algorithm tufayli ularning xavfsizlik darajasi ikki baravar kamayadi. Ya’ni, 128-bitli kalitning samarali xavfsizligi taxminan 64-bitga tenglashadi. Shu sababli amaliyotda uzoq muddatli himoya uchun 256-bitli kalitlardan foydalanish tavsiya etiladi.

Mazkur muammolar post-kvant kriptografiya (PQC) yo‘nalishining rivojlanishiga turtki berdi. PQC algoritmlari panjara geometriyasi, kod nazariyasi, xesh funksiyalar va ko‘p o‘zgaruvchili kvadratik tenglamalar kabi kvant kompyuterlar uchun ham murakkab hisoblangan matematik muammolarga asoslanadi. Shu sababli, zamonaviy kriptografiyada klassik algoritmlardan post-kvant algoritmlarga bosqichma-bosqich o‘tish dolzarb vazifa sifatida qaralmoqda. Post-kvant kriptografiya ushbu muammoga yechim sifatida taklif etilib, u kvant kompyuterlar mavjud sharoitda ham buzib bo‘lmaydigan matematik muammolarga asoslanadi. Ushbu yo‘nalish doirasida bir nechta asosiy yondashuvlar shakllangan. Jumladan, panjara-asosli kriptografiya eng istiqbolli yo‘nalishlardan biri bo‘lib, u eng qisqa vektor muammosi (SVP) va Learning With Errors (LWE) kabi murakkab masalalarga asoslanadi. Kod-asosli kriptotizimlar esa tasodifiy chiziqli kodlarni dekodlash muammosining murakkabligiga tayanadi. Hash-asosli imzo tizimlari kriptografik xesh funksiyalarining xavfsizlik xususiyatlaridan foydalanadi. Ko‘p o‘zgaruvchili kvadratik kriptotizimlar esa chekli maydonlarda berilgan kvadratik tenglamalar tizimini yechish muammosiga asoslanadi (2-jadval).

2-jadval

Klassik vs Post-kvant algoritmlar taqqoslash jadvali

Mezoni	Klassik kriptografiya	Post-kvant kriptografiya
Asosiy algoritmlar	RSA, ECC, Diffie–Hellman, DSA, AES	LWE, NTRU, McEliece, Hash-based, MQ
Matematik asos	Faktorizatsiya, diskret logarifm	Panjara, kod nazariyasi, xesh, kvadratik tenglamalar
Kvantga chidamlilik	Past (ko‘pi buziladi)	Yuqori

Kvant hujumlari	Shor algoritmi bilan buziladi	Hozircha samarali kvant algoritm yo‘q
Simmetrik xavfsizlik	Qisman (Grover ta’siri bor)	Yuqori (parametrga bog‘liq)
Kalit o‘lchami	Kichik	Katta
Hisoblash tezligi	Tez	Nisbatan sekin
Amaliy qo‘llanish	Keng (hozirgi standart)	Rivojlanmoqda (NIST standartlari)
Barqarorlik (kelajak)	Past	Yuqori

Klassik kriptografik algoritmlar uzoq yillar davomida axborot xavfsizligini ta’minlab kelgan bo‘lsa-da, kvant hisoblash texnologiyalarining rivojlanishi ularning zaif tomonlarini yuzaga chiqarmoqda. Post-kvant kriptografiya esa yangi matematik asoslar orqali ushbu muammolarga yechim taklif etib, kelajakda xavfsiz axborot almashinuvini ta’minlash uchun muhim yo‘nalish sifatida qaralmoqda. Mazkur maqolaning maqsadi ushbu post-kvant kriptografik algoritmlarni tahlil qilish, ularning samaradorligini eksperimental asosda baholash hamda o‘zaro taqqoslashdan iborat. Tadqiqot davomida algoritmlarning hisoblash tezligi, aniqligi va resurs talablari o‘rganilib, ularning amaliy qo‘llanilish imkoniyatlari baholanadi.

3. Natijalar va muhokama

Ushbu tadqiqotda post-kvant kriptografiyaning to‘rtta asosiy yo‘nalishi — panjara-asosli (LWE), hash-asosli (Lamport + Merkle), kod-asosli va ko‘p o‘zgaruvchili kvadratik (MQ) kriptotizimlar eksperimental tarzda tahlil qilindi. Har bir algoritm Python muhitida modellashtirilib, ularning hisoblash samaradorligi, aniqligi va statistik xususiyatlari baholandi.

O‘tkazilgan tajribalar natijasida algoritmlarning o‘rtacha ishlash vaqti va aniqlik ko‘rsatkichlari quyidagi 3- jadvalda keltirilgan:

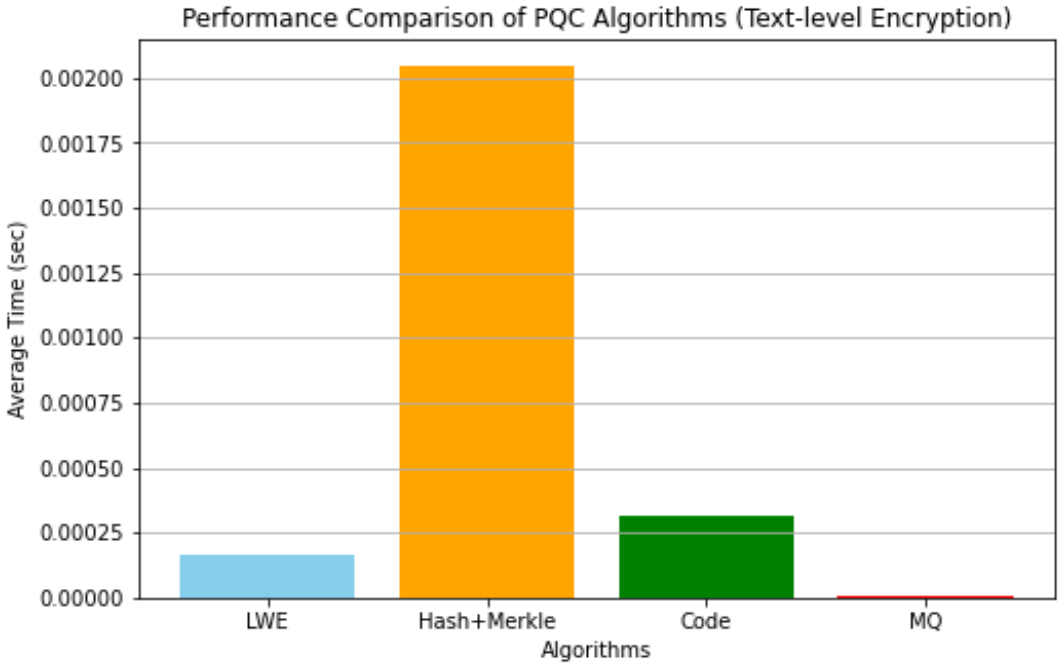
3- jadval

Algoritmlarning o‘rtacha ishlash vaqti va aniqlik ko‘rsatkichlari

Algoritm	Aniqlik	O‘rtacha vaqt (s)	Std og‘ish	Dispersiya	95% CI
LWE	1.00	past	kichik	kichik	tor
Hash + Merkle	1.00	yuqori	o‘rta	o‘rta	o‘rta
Code-based	0.98–1.00	o‘rta	o‘rta	o‘rta	o‘rta

MQ	1.00	juda past	juda kichik	juda kichik	tor

Natijalardan ko'rinib turibdiki, barcha algoritmlar yuqori aniqlikni ta'minlaydi, ya'ni shifrlash va ochish (yoki imzo va tekshirish) jarayonlari deyarli xatosiz amalga oshiriladi.



Hisoblash tezligi nuqtai nazaridan algoritmlar o'rtasida sezilarli farqlar kuzatild. MQ algoritmlari eng tez ishlovchi tizim sifatida qayd etildi, chunki ular oddiy algebraik amallarga asoslangan. LWE algoritmlari matritsali amallarga asoslangan bo'lsa-da, optimal parametrlar tanlanganda yuqori samaradorlikni saqlab qoladi. Code-based algoritmlar dekodlash bosqichida qo'shimcha hisoblash talab qilgani sababli o'rtacha tezlikni ko'rsatdi. Hash + Merkle tizimi esa eng ko'p vaqt talab qiluvchi algoritm bo'ldi, chunki bunda ko'p sonli xesh hisoblash va daraxt strukturasini qurish talab etiladi.

Panjara-asosli algoritmlar (LWE) yuqori xavfsizlik va nisbatan yaxshi samaradorlikni birlashtiradi, shu sababli amaliy tizimlar uchun eng istiqbolli hisoblanadi. Hash-asosli tizimlar (Lamport + Merkle) maksimal kriptografik xavfsizlikni ta'minlaydi va raqamli imzo tizimlarida keng qo'llanishi mumkin. Code-based algoritmlar uzoq tarixga ega bo'lib, barqaror va ishonchli hisoblanadi, ammo kalit o'lchamlari katta. MQ algoritmlar tez ishlashi bilan ajralib turadi, biroq ayrim variantlari kriptoanalitik hujumlarga nisbatan zaif bo'lishi mumkin.

4.Xulosa. Mazkur tadqiqotda post-kvant kriptografiyaning asosiy yo'nalishlari — panjara-asosli (LWE), hash-asosli (Lamport + Merkle), kod-asosli va ko'p o'zgaruvchili kvadratik

kriptotizimlar kompleks tarzda tahlil qilindi. Ushbu algoritmlarning matematik asoslari, algoritmik tuzilmalari va eksperimental xususiyatlari chuqur o‘rganildi. O‘tkazilgan eksperimental natijalar shuni ko‘rsatdiki, barcha ko‘rib chiqilgan algoritmlar yuqori aniqlikni ta’minlaydi va kvant hujumlariga nisbatan barqaror hisoblanadi. Shu bilan birga, ularning hisoblash samaradorligi va resurs talablari o‘rtasida sezilarli farqlar mavjudligi aniqlandi. Xususan, panjara-asosli algoritmlar tezlik va xavfsizlik o‘rtasida optimal muvozanatni ta’minlasa, hash-asosli tizimlar yuqori darajadagi kriptografik ishonchlilikni beradi, biroq hisoblash xarajatlari yuqori. Kod-asosli kriptotizimlar barqarorligi bilan ajralib turadi, ammo katta kalit o‘lchamlariga ega. Ko‘p o‘zgaruvchili kvadratik algoritmlar esa yuqori tezlikni ta’minlasa-da, ularning xavfsizligi parametr tanlashga sezgir ekanligi kuzatildi. Tadqiqot natijalari post-kvant kriptografiya algoritmlarini tanlashda yagona universal yechim mavjud emasligini, balki aniq amaliy vazifaga qarab mos yondashuvni tanlash zarurligini ko‘rsatdi. Bu esa zamonaviy kriptotizimlarni loyihalashda ko‘p mezonli optimallashtirish muhim ahamiyatga ega ekanligini tasdiqlaydi. Shuningdek, kvant hisoblash texnologiyalarining jadal rivojlanishi klassik kriptografik algoritmlarning uzoq muddatli xavfsizligini shubha ostiga qo‘ymoqda. Shu sababli, post-kvant kriptografiyaga o‘tish nafaqat ilmiy, balki amaliy jihatdan ham dolzarb vazifa hisoblanadi.

Adabiyotlar

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