POST-KVANT KRIPTOGRAFIYA ALGORITMLARINING MATEMATIK ASOSLARI VA ZAMONAVIY YONDASHUVLAR TAHLILI

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.20215170**

Annotatsiya. *Ushbu maqolada post-kvant kriptografiyaning asosiy algoritmlari va ularning matematik asoslari tahlil qilinadi. Kvant kompyuterlarning rivojlanishi natijasida an’anaviy kriptografik tizimlarning zaiflashuvi yangi, kvantga chidamli algoritmlarni ishlab chiqishni talab etmoqda. Tadqiqotda panjara asosli, kodga asoslangan, ko‘p o‘zgaruvchili va hash-funksiyaga asoslangan kriptografik yondashuvlar chuqur o‘rganiladi. Har bir algoritmning ishlash prinsipi, matematik modeli hamda xavfsizlik darajasi solishtirma tarzda baholanadi. Shuningdek, ushbu algoritmlarning afzalliklari va kamchiliklari aniqlanib, ularning amaliy qo‘llanish istiqbollari muhokama qilinadi. Olingan natijalar post-kvant kriptografiya sohasida optimal yondashuvlarni tanlashda muhim ahamiyat kasb etadi.*

Kalit so‘zlar. *Post-kvant kriptografiya, kvant kompyuterlar, panjara asosli algoritmlar, LWE, kodga asoslangan kriptografiya, multivariate tizimlar, hash-funksiyalar, kriptografik xavfsizlik*

Аннотация. *В данной статье анализируются основные алгоритмы постквантовой криптографии и их математические основы. Ослабление традиционных криптографических систем в результате развития квантовых компьютеров требует разработки новых, квантово-устойчивых алгоритмов. В исследовании подробно изучаются криптографические подходы на основе решеток, кодов, многомерных данных и хеш-функций. Проводится сравнительная оценка принципа работы, математической модели и уровня безопасности каждого алгоритма. Также определяются преимущества и недостатки этих алгоритмов и обсуждаются перспективы их практического применения. Полученные результаты имеют большое значение при выборе оптимальных подходов в области постквантовой криптографии.*

Ключевые слова: *постквантовая криптография, квантовые компьютеры, алгоритмы на основе решеток, LWE, криптография на основе кодов, многомерные системы, хеш-функции, криптографическая безопасность*

Abstract*. This article analyzes the main algorithms of post-quantum cryptography and their mathematical foundations. The weakening of traditional cryptographic systems as a result of the development of quantum computers requires the development of new, quantum-resistant algorithms. The study deeply studies lattice-based, code-based, multivariate and hash-function-based cryptographic approaches. The principle of operation, mathematical model and security level of each algorithm are comparatively evaluated. Also, the advantages and disadvantages of these algorithms are identified and their practical application prospects are discussed. The results obtained are of great importance in choosing optimal approaches in the field of post-quantum cryptography.*

Keywords. *Post-quantum cryptography, quantum computers, lattice-based algorithms, LWE, code-based cryptography, multivariate systems, hash functions, cryptographic security*

1. Kirish. Mazkur maqolada post-kvant kriptografiyaning asosiy algoritmlari, ularning matematik asoslari va ishlash prinsiplari tizimli ravishda tahlil qilinadi. Shuningdek, turli yondashuvlarning afzallik va kamchiliklari solishtirilib, ularning amaliy qo'llanish istiqbollari yoritiladi. Bu esa kelajakda xavfsiz kriptografik tizimlarni tanlash va ishlab chiqishda muhim ilmiy asos bo'lib xizmat qiladi. Post-kvant kriptografiya sohasidagi ilmiy tadqiqotlar kvant kompyuterlarning rivojlanishi bilan keskin faollashdi. Klassik kriptotizimlar xavfsizligi asosan faktorizatsiya va diskret logarifm muammolariga asoslangan bo'lib, ular kvant algoritmlari yordamida samarali yechilishi mumkin. Shu sababli, yangi kriptografik yondashuvlar murakkab matematik muammolarga asoslanmoqda. Adabiyotlar tahlili shuni ko'rsatadiki, post-kvant kriptografiya bir nechta asosiy yo'nalishlarga bo'linadi va har bir yo'nalish o'ziga xos matematik modelga ega [1-3].

2. Metodologiya. Panjara asosli kriptografiya eng ko'p o'rganilgan va amaliy jihatdan istiqbolli yo'nalishlardan biri hisoblanadi. Ushbu yondashuv panjara nazariyasiga asoslanadi va unda asosiy murakkab masala sifatida eng qisqa vektor muammosi qaraladi [4-7]:

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

Bu yerda L panjara bo‘lib, nolga teng bo‘lmagan eng kichik uzunlikdagi vektor topilishi talab etiladi. Ushbu muammo yuqori o‘lchamli fazolarda hisoblash jihatidan juda murakkab bo‘lib, kvant kompyuterlar uchun ham samarali algoritmlar mavjud emas.

Amaliy kriptografik tizimlarda panjara asosli yondashuvning keng qo‘llaniladigan varianti — Learning With Errors (LWE) muammosidir. U quyidagi matematik model orqali ifodalanadi:

$$b = As + e \pmod{q},$$

bu yerda A tasodifiy matritsa, s maxfiy vektor, e esa kichik xatolikni ifodalovchi vektordir. Tadqiqotlar shuni ko‘rsatadiki, xatolik komponentining mavjudligi tizimni kriptotahlilga nisbatan sezilarli darajada mustahkamlaydi.

Kodga asoslangan kriptografiya ham post-kvant xavfsizlikni ta'minlashda muhim o‘rin egallaydi. Ushbu yondashuv xatolarni tuzatish nazariyasiga asoslanadi va quyidagi ko‘rinishda ifodalanadi:

$$c = mG + e,$$

bu yerda G generator matritsa, m ochiq matn, e esa xatolik vektori hisoblanadi. Adabiyotlarda McEliece kriptotizimi yuqori xavfsizlik darajasi bilan ajralib turishi ta'kidlanadi, biroq uning asosiy kamchiligi sifatida kalit hajmining katta bo‘lishi ko‘rsatiladi.

Ko‘p o‘zgaruvchili kvadratik tenglamalarga asoslangan kriptografiya ham keng o‘rganilgan yo‘nalishlardan biridir. Ushbu yondashuvda shifrlash yoki imzo yaratish quyidagi umumiy ko‘rinishdagi tenglamalar tizimiga asoslanadi:

$$P_i(x_1, x_2, \ldots, x_n) = \sum_{j,k} a_{jk}^{(i)} x_j x_k + \sum_j b_j^{(i)} x_j + c_i.$$

Bu yerda asosiy muammo — ko‘p o‘zgaruvchili kvadratik tenglamalar tizimini yechish bo‘lib, bu NP-qiyin masala hisoblanadi. Tadqiqotlar shuni ko‘rsatadiki, ushbu tizimlar yuqori tezlikka ega bo‘lsa-da, ayrim parametr tanlovlarida xavfsizlik zaiflashishi mumkin.

Hash-funksiyaga asoslangan kriptografik tizimlar esa eng ishonchli yondashuvlardan biri sifatida qaraladi.

Ularning matematik asosi quyidagi ifoda bilan belgilanadi:

$$h = H(m),$$

bu yerda H — kriptografik hash funksiya, m — kiruvchi xabar. Ushbu yondashuvning xavfsizligi hash funksiyaning kolliziyaga chidamliligi va bir yo‘nalishliligiga bog‘liq.

Adabiyotlar tahlili shuni ko‘rsatadiki, har bir post-kvant kriptografik yondashuv ma’lum afzallik va kamchiliklarga ega. Panjara asosli algoritmlar yaxshi muvozanatni ta’minlasa, kodga asoslangan tizimlar yuqori ishonchlilikni beradi. Ko‘p o‘zgaruvchili tizimlar tezkorligi bilan ajralib tursa, hash asosli yondashuvlar maksimal xavfsizlikni ta’minlaydi.

Barcha tadqiqotlarda umumiy xulosa sifatida quyidagi muammolar qayd etiladi: hisoblash murakkabligi, kalit hajmining kattaligi, implementatsiya murakkabligi va uzoq muddatli xavfsizlikni isbotlashdagi cheklovlar. Aynan shu omillar post-kvant kriptografiya sohasida hali ham faol ilmiy izlanishlar olib borilayotganini ko‘rsatadi.

3.Natijalar

Mazkur tadqiqot doirasida post-kvant kriptografik algoritmlar — panjara asosli (LWE/RLWE), kodga asoslangan, ko‘p o‘zgaruvchili kvadratik (MQ) hamda hash-funksiyaga asoslangan tizimlar kompleks matematik va hisoblash mezonlari asosida baholandi. Olingan natijalar algoritmlarning samaradorligi, xavfsizlik darajasi, hisoblash va xotira murakkabligi hamda amaliy qo‘llanish imkoniyatlarini aniqlashga qaratildi.

Quyida keltirilgan jadvalda post-kvant kriptografik algoritmlar bo‘yicha olingan natijalar ilmiy mezonlar asosida umumlashtirildi (1-jadval):

1-jadval

Post-kvant kriptografik algoritmlar natijalari

Algoritm turi	Matematik asos	Hisoblash murakkabligi T(n))	Xotira murakkabligi S(n))	Xavfsizlik darajasi	Afzalliklari	Kamchiliklari
Panjara asosli (LWE)	$b = As + e \bmod q$	$O(n^2 \log q)$	$O(n^2 \log q)$	Yuqori $2^{-\lambda}$	Kvantga chidamli, barqaror	Kalit hajmi katta
Panjara asosli (RLWE)	$b(x) = a(x)s(x) + e(x)$	$O(n \log n)$	$O(n \log q)$	Yuqori	Tezkor, optimallashtirilgan	Parametr tanlash murakkab
Kodga asoslangan	$c = mG' + e$	$O(nk)$	$O(n^2)$	Juda yuqori	Sinovdan o‘tgan, ishonchli	Juda katta kalit hajmi

Multivariate (MQ)	$Pi(x1,\ldots,xn)$	$O(n^2)$	$O(n^2)$	O‘rta–yuqori	Juda tez ishlaydi	Ba’zi hujumlarga zaif
Hash asosli	$h = H(m)$	$O(n)$	$O(nlogn)$	Juda yuqori	Eng ishonchli	Imzo hajmi katta
Izogeniya asosli	$\phi: E1 \to E2$	$O(n^2)$	$O(n)$	Yuqori	Kalit kichik	Hisoblash sekin
Algoritm turi	Matematik asos	Hisoblash murakkabligi T(n))	Xotira murakkabligi S(n))	Xavfsizlik darajasi	Afzalliklari	Kamchiliklari
Panjara asosli (LWE)	$b = As + e \bmod q$	$O(n^2 logq)$	$O(n^2 logq)$	Yuqori $2^{-\lambda}$	Kvantga chidamli, barqaror	Kalit hajmi katta
Panjara asosli (RLWE)	$b(x) = a(x)s(x) + e(x)$	$O(nlogn)$	$O(nlogq)$	Yuqori	Tezkor, optimallashtirilgan	Parametr tanlash murakkab
Kodga asoslangan	$c = mG' + e$	$O(nk)$	$O(n^2)$	Juda yuqori	Sinovdan o‘tgan, ishonchli	Juda katta kalit hajmi
Multivariate (MQ)	$Pi(x1,\ldots,xn)$	$O(n^2)$	$O(n^2)$	O‘rta–yuqori	Juda tez ishlaydi	Ba’zi hujumlarga zaif
Hash asosli	$h = H(m)$	$O(n)$	$O(nlogn)$	Juda yuqori	Eng ishonchli	Imzo hajmi katta
Izogeniya asosli	$\phi: E1 \to E2$	$O(n^2)$	$O(n)$	Yuqori	Kalit kichik	Hisoblash sekin

2-jadval

Umumiy solishtirma tahlil

Mezoni	Eng yaxshi algoritm	Izoh
Tezlik	MQ, RLWE	Eng kam hisoblash vaqti
Xavfsizlik	Hash-based, Code-based	Eng yuqori kriptotahlilga chidamlilik
Xotira samaradorligi	RLWE, Izogeniya	Kamroq xotira talab qiladi
Amaliy qo‘llash	LWE / RLWE	Eng balanslangan yechim
Barqarorlik	Code-based	Yillar davomida sinovdan o‘tgan
Mezoni	Eng yaxshi algoritm	Izoh

Algoritm tanlash quyidagi ko‘p mezonli optimallashtirish masalasi bilan ifodalanadi:

$$\min(T(n), S(n)), \quad \text{sharti bilan} \quad \Pr[\text{break}] \le 2^{-\lambda}.$$

4-Xulosa

Mazkur tadqiqotda post-kvant kriptografiya sohasining asosiy yo‘nalishlari, ularning matematik asoslari hamda amaliy samaradorligi kompleks tarzda tahlil qilindi. Kvant kompyuterlarning rivojlanishi natijasida an’anaviy kriptografik algoritmlarning zaiflashuvi ehtimoli mavjudligi ilmiy jihatdan asoslandi va shu sababli kvantga chidamli yangi kriptografik yondashuvlarni ishlab chiqish zarurligi ko‘rsatib berildi. Tadqiqot davomida panjara asosli, kodga asoslangan, ko‘p o‘zgaruvchili kvadratik va hash-funksiyaga asoslangan algoritmlar chuqur matematik modellar asosida o‘rganildi hamda ularning hisoblash murakkabligi, xotira talablari va xavfsizlik darajasi o‘zaro solishtirildi. Olingan natijalar shuni ko‘rsatdiki, panjara asosli algoritmlar, ayniqsa LWE va uning halqa asosidagi modifikatsiyasi RLWE, samaradorlik va xavfsizlik o‘rtasida optimal muvozanatni ta’minlaydi. Ushbu algoritmlar polinomial vaqt murakkabligiga ega bo‘lib, yuqori o‘lchamli parametrlar uchun ham barqaror ishlaydi. Shu bilan birga, kodga asoslangan kriptotizimlar yuqori darajadagi kriptotahlilga chidamliligi bilan ajralib turadi, biroq ularning katta kalit hajmi amaliy qo‘llanishni murakkablashtiradi. Ko‘p o‘zgaruvchili tizimlar tezkor ishlashi bilan ajralib tursa-da, ularning xavfsizligi parametr tanlashga sezilarli darajada bog‘liq. Hash-funksiyaga

asoslangan algoritmlar esa konservativ yondashuv sifatida eng yuqori ishonchlilikni ta’minlaydi, ammo samaradorlik va imzo hajmi jihatidan ma’lum cheklovlarga ega.

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