ISSN: 3030-3346

PANJARAGA ASOSLANGAN KRIPTOGRAFIYA

Mustafoyev Azamat Botir o‘g‘li
‘‘UNICON.UZ” MChJ
E-mail: mustafoyevazamat01@gmail.com

K E Y W O R D S

qisqa vektor (SVP), yaqin vektor (CVP), NTRUEncrypt, Kyber, Dilithium, Falcon

A B S T R A C T

Maqolada postkvant kriptografiyaning istiqbolli yo‘nalishi - panjaraga asoslangan kriptografiya tahlil qilinadi. Uning xavfsizligi eng qisqa vektor (SVP) va eng yaqin vektor (CVP) kabi hisoblash jihatdan murakkab panjara masalalariga asoslanadi. Panjaraning matematik ta’rifi, bazis tushunchasi hamda NTRUEncrypt, Kyber, Dilithium, Falcon kabi amaliy algoritmlar qisqacha yoritiladi.

So‘nggi yillarda kvant hisoblash texnologiyalarining jadal rivojlanishi zamonaviy axborot xavfsizligi tizimlari oldida jiddiy muammolarni keltirib chiqarmoqda. An'anaviy ochiq kalitli kriptografik algoritmlar, jumladan RSA, Diffi-Xellman va elliptik egri chiziqlarga asoslangan kriptotizimlar (ECC), butun sonlarni faktorlash va diskret logarifm masalalarining hisoblash jihatdan murakkabligiga tayanadi. Klassik kompyuterlar uchun bu masalalarni yechish amalda imkonsiz hisoblansa-da, 1994-yilda P.Shor tomonidan taklif etilgan kvant algoritmi yetarlicha quvvatga ega kvant kompyuteri yordamida ushbu masalalarni polinomial vaqt ichida yechish mumkinligini isbotladi [1]. Natijada, hozirgi kunda keng qo'llanilayotgan ko'plab kriptografik protokollarning kelajakdagi xavfsizligi ostida jiddiy shubha paydo bo'ldi.

Ushbu tahdidga javob sifatida ilmiy jamoatchilik va standartlashtirish tashkilotlari (xususan, AQSh Milliy standartlar va texnologiyalar instituti - NIST) postkvant kriptografiya deb ataluvchi yangi yo'nalishni faol rivojlantirmoqda. Postkvant kriptografiya - bu xavfsizligi kvant kompyuterlari uchun ham hisoblash jihatdan murakkab bo'lgan matematik masalalarga asoslangan kriptografik algoritmlar majmuidir. Bunday yondashuvlar qatoriga panjara asosidagi (lattice-based), kod asosidagi (code-based), ko'p o'zgaruvchili (multivariate), xesh funksiyalariga asoslangan hamda izogeniya asosidagi kriptografiya kiradi.

Panjara nazariyasining kriptografik qo'llanilishi 1996-yilda M.Ajtaining tub ishidan boshlangan [2] bo'lib, keyinchalik Ajtai va Dvork [3], Goldreyx, Goldvasser va Xalevi [4], shuningdek Hoffstein, Pipher va Silverman kabi tadqiqotchilarning ishlari orqali rivojlantirildi. Natijada NTRUEncrypt, Kyber, NewHope, Dilithium va Falcon kabi amaliy algoritmlar ishlab chiqildi, ularning bir qismi NIST tomonidan postkvant standartlari sifatida tasdiqlangan [5].

Mazkur maqolaning maqsadi panjaraga asoslangan kriptografiyaning nazariy asoslarini - jumladan panjara, bazis, eng qisqa vektor muammosi (SVP) va eng yaqin vektor muammosi (CVP) kabi tushunchalarni - yoritish, ularning kriptografik tizimlar xavfsizligini ta'minlashdagi rolini tahlil qilish hamda ushbu yondashuvning IoT qurilmalari, moliyaviy tizimlar va davlat infratuzilmalarida qo'llanilish istiqbollarini ko'rib chiqishdan iborat.

Panjaraga asoslangan kriptografiya - bu postkvant kriptografiyaning istiqbolli yo‘nalishlaridan biri bo‘lib, u o‘zining xavfsizlik asosini panjara muammolarining hisobiy murakkabligiga tayanadi. Ushbu yondashuv kvant kompyuterlari tomonidan buzilishi mumkin bo‘lgan an’anaviy algoritmlarga nisbatan yuqori darajada barqarorlikni ta’minlaydi. Panjaraviy kriptotizimlar odatda eng qisqa vektor (SVP) yoki eng yaqin vektor (CVP) kabi murakkab matematik masalalarga asoslanadi, ularni yechish hatto kvant hisoblash vositalari uchun ham amaliy jihatdan mushkul hisoblanadi. Mazkur yondashuv asosida ishlab chiqilgan algoritmlar *NTRUEncrypt, Kyber, NewHope, Dilithium* va *Falcon* - shifrlash, raqamli imzo va kalit almashinuvi kabi kriptografik operatsiyalarni amalga oshirishda qo‘llaniladi.

(cc) BY

Panjaraga asoslangan kriptografiyaning afzalliklari orasida kvantga bardoshlilik, oddiy va samarali tuzilma, parallel ishlashga moslashuvchanlik, shuningdek, eng yomon holatdagi hisobiy murakkablikka asoslangan xavfsizlikni ta'minlashi alohida ajralib turadi. Bundan tashqari, bu yondashuv gomomorf shifrlash, atributga asoslangan shifrlash va kod chalkashtirish kabi ilg'or texnologiyalar bilan uyg'unlashishga mos keladi. Shu sababli, panjaraga asoslangan kriptografiya ayniqsa IoT qurilmalari, moliyaviy tizimlar va davlat infratuzilmalari kabi postkvant xavfsizlikni talab qiluvchi sohalarda dolzarb ahamiyat kasb etadi. Panjaraga asoslangan kriptografiyaning afzalliklari quyidagilardan iborat:

1. *Kvantga bardoshlilik:* Shor algoritmi kabi kvant algoritmlariga nisbatan barqaror. Ko'plab algoritmlar oddiy va parallelizatsiyalashga yaroqli.
2. *Eng yomon holatga asoslangan xavfsizlik:* Ba'zi sxemalar eng yomon holatdagi hisobiy murakkablikka tayanadi, bu esa xavfsizlikni mustahkamlaydi.
3. *Keng qo'llanilish imkoniyati:* Gomomorf shifrlash, atributga asoslangan shifrlash, va kod chalkashtirish kabi ilg'or texnologiyalar bilan uyg'unlashadi.

Ushbu yondashuv ayniqsa postkvant xavfsizlikni ta'minlash zarur bo'lgan IoT, moliyaviy tizimlar va davlat infratuzilmalari uchun dolzarb hisoblanadi.

Kvantdan keyingi kriptografiya - bu kvant kompyuterlari mavjud shifrlash algoritmlariga xavf tug'dirishi bilan bog'liq holda shakllanayotgan yangi avlod kriptografik yechimlarini anglatadi. Ushbu blog posti ushbu texnologiyaning ta'rifi, asosiy tamoyillari hamda kvant hisoblashning kriptotizimlarga bo'lgan ta'sirini tahlil qiladi. Unda postkvant kriptografiya algoritmlarining turlari o'zaro solishtiriladi va ularning amaliy qo'llanilish imkoniyatlari ko'rib chiqiladi. Bundan tashqari, ushbu texnologiyaga o'tish jarayonidagi talablar, xavf-xatarlar, yuzaga keladigan muammolar hamda mutaxassislarning baholari ko'rib chiqilib, xavfsizlikning istiqboldagi strategik yondashuvlari taklif etiladi.

Asosiy maqsad - Postkvant kriptografiyasi yordamida texnologik kelajakda axborot himoyasini ishonchli ta'minlashdir.

Kiriptografiyaning panjara asosi - Ta'rif 1. Faraz qilaylik $b_1, b_2, \dots, b_n$- bu E^n Evklid fazosidagi o'zaro chiziqli bog'liqsiz vektorlardir. Unda quyidagi ko'rinishdagi to'plam:

$$\Lambda = \{z_1 b_1 + z_2 b_2 + \cdots + z_n b_n : z_i \in Z\}$$

n o'lchamli panjara deb yuritiladi, va $\{b_1, b_2, \dots, b_n\}$ vektorlar to'plami ushbu panjaraning bazisi sifatida qabul qilinadi.

Agar $b_i = (b_{i1}, b_{i2}, \dots, b_{in})$ bo'lsa, $n \times n$ matritsaga mos keluvchi $B = (b_{ij})$ ni aniqlash va B ning determinantining absalyut qiymatini $\det(\Lambda)$ kabi belgilash mumkin. U holda, panjarani quyidagicha qayta yozish mumkin: $\Lambda = \{zB : z \in Z^n\}$.

O'z-o'zidan ma'lumki agar $n \geq 2$ bo'lsa, n o'lchamli panjara cheksiz ko'p bazislarga ega bo'ladi, ularning har qanday jufti birmodulli (determinanti ± 1 ga teng bo'lgan) matritsa U bilan bog'langan [6].

Panjara - bu matematikaning asosiy tushunchasi bo'lib, uni Gauss, Ermit va Minkovskilar tomonidan o'rganila boshlangan. Bu algebrada chekli hosil qilingan erkin guruh, sonlar nazariyasida Z va Z^n butun sonlar tizimlarini umumlashtiradi va geometriyada E^n da eng muntazam (davriy) diskret to'plamdir. Tabiiy va oddiy eshitilishga ega bo'lishiga qaramay, panjaralar murakkab ob'ektlardir, ayniqsa o'lchamlari katta bo'lsa. 1996-yilda M.Ajtai panjaraga asoslangan ochiq kalitli kriptografiya panjaralar haqidagi hisoblash murakkabligi masalalarini o'rgandi. Ikki yil ichida bunday ochiq kalitli kriptotizimlar M.Ajtay va C.Dvork, O.Goldreyx, S.Goldvasser va S.Xalevi, J.Xofestyn, J.Pifer va J.H.Silvermanlar tomonidan yaratilgan. Panjara asosidagi kriptografiyada qisqa va deyarli ortogonal vektorlardan iborat bo'lgan bazis "yaxshi bazis" deb ataladi. Bunday bazis mavjud bo'lgan holatda, ayrim hisoblash nuqtai nazaridan murakkab bo'lgan panjara muammolarini samarali algoritmlar yordamida yechish imkoni paydo bo'ladi. Shu sababli, ko'plab panjarali kriptotizimlar dizaynida maxfiy kalit sifatida yaxshi bazisdan foydalaniladi. Ochiq kalit esa unga ekvivalent bo'lgan, ammo yomon deb hisoblangan tasodifiy bazis ko'rinishida beriladi.

(cc) BY

ISSN: 3030-3346

Panjara strukturasidagi nuqtalarni aniqlash - Bazis vektorlarni n o'lchamli fazoda yozish. Masalan, 2D uchun: $b_1 = (x_1, y_1)$, $b_2 = (x_2, y_2)$, 3D uchun

$$b_1 = (x_1, y_1, z_1), b_2 = (x_2, y_2, z_2), b_3 = (x_3, y_3, z_3).$$

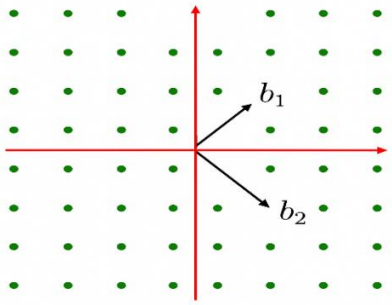
Bazis vektorlarning butun ko'paytmasini qo'shish bilan panjara nuqtalarini hosil qilish. p nuqta uchun ifoda quyidagicha: $\Lambda = z_1 b_1 + z_2 b_2 + \cdots + z_n b_n$ va bu yerda $z_i \in \mathbb{Z}$.

z_i larga butun sonlarni berib, mos panjara nuqtalari hisoblanadi.

Masalan, bazis vektorlar $b_1 = (2,1)$, $b_2 = (1,3)$ ga teng bo'lsin. U holda, $\Lambda = z_1 b_1 + z_2 b_2 = z_1(2,1) + z_2(1,3) = (2z_1 + z_2, z_1 + 3z_2)$ tenglikni qurish mumkin. z_n larning quyidagi qiymatlari orqali mos panjara nuqtalarini hisoblash mumkin:

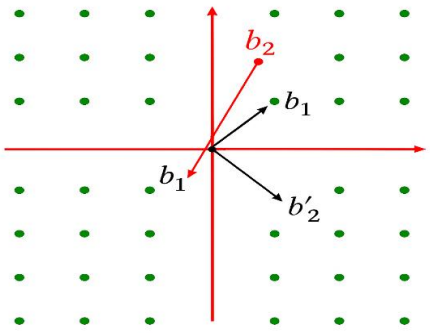
- $z_1 = 0, z_2 = 0$ uchun $\Lambda = (0,0)$;
- $z_1 = 1, z_2 = 0$ uchun $\Lambda = (2,1)$;
- $z_1 = 0, z_2 = 1$ uchun $\Lambda = (1,3)$;
- $z_1 = 1, z_2 = 1$ uchun $\Lambda = (3,4)$;
- $z_1 = -1, z_2 = 1$ uchun $\Lambda = (-1,2)$.

Quyidagi 1 - rasmda tegishli bazis vektorlarga ega panjara ko'rinishi berilgan. Panjara Λ ni ustun vektorlar sifatida bazis vektorlardan iborat B matritsa orqali hosil qilish mumkin [6].



1-rasm. Ikki o'lchamli panjaraga misol

Tavsif 2 (panjara, rang, o'lcham, to'liq-rangli panjara). Faraz qilinsin $\{b_1, b_2, \ldots, b_m\}$ -E^n ning chiziqli mustaqil vektorlari to'plami bo'lsin. Faraz qilinsin B kattalik $n \times m$ matritsa bo'lib, ustun vektorlari $b_1, b_2, \ldots, b_m$ dan iborat. U holda $\Lambda(B) = \{Bx \mid x \in Z\}$ ga B tomonidan hosil qilingan E^n dagi panjara deb ataladi. Ushbu panjara m rangli va n o'lchamli deb ataladi. m va n o'zaro teng bo'lsa, panjara to'liq-rangli panjara deb ataladi. Panjara Λ ning bazislari yagona emasligiga e'tibor berish lozim. Masalan, $\binom{0}{1}$, $\binom{1}{0}$ vektorlar orqali generatsiya qilingan panjara Z^2 ga teng. Shuningdek, Z^2 quyidagi vektorlar orqali ham generatsiya qilinishi mumkin: $\binom{2}{1}$, $\binom{1}{1}$. 8-rasmda ham ushbu fakt ko'rsatilgan. Boshqa tomondan, Z dagi n chiziqli mustaqil vektorlar Z^nning bazislari bo'lishi shart emas. Misol sifatida ko'rish mumkinki, yuqoridagi vektorlarni o'zgartirish natijasidagi $\binom{2}{0}$, $\binom{1}{1}$ vektorlar Z^2 ning bazislari emas. Ya'ni, ushbu vektorlar orqali 2 o'lchamli maydondagi barcha nuqtalarni hosil qilib bo'lmaydi.



2 - rasm. Yaxshi bazislar $\{b'_1, b'_2\}$ va yomon bazis $\{b_1, b_2\}$larga ega 2 o'lchamli panjara

Hisoblashga oid panjara muammolari Panjaralarning o'ziga xos tuzilishi ularga maxsus matematik xususiyatlarga ega bo'lish imkonini beradi. Quyidagi hisob-kitoblarni chiziqli algebra algoritmlari yordamida samarali baholash mumkin.

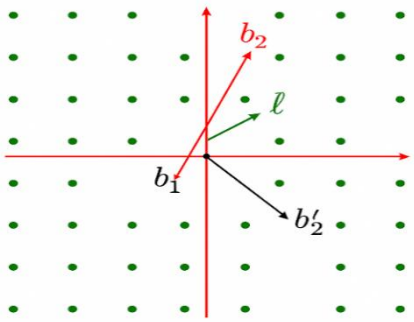
- Faraz qilinsin Λ panjarani hosil qiluvchi vektorlar to'plami $g_1, \ldots, g_k \in E^n$ bo'lsin. Λ ning bazislari $b_1, \ldots, b_m \in E^n$ ni hisoblash.
- Faraz qilinsin Λ panjara. Berilgan vektor c ni Λ panjaraning elementi ekanligini baholash.

Boshqa hisoblashga oid panjara muammolari odatda murakkab bo'lib ko'rinadi, hattoki Shor algoritmiga ham bardoshli bo'lishi mumkin. Shuning uchun ular postkvant kriptografiyada foydalanishga tavsiya etilishi mumkin bo'lgan yo'nalishdir. Ushbu muammolar quyida keltiriladi.

Eng qisqa vektor muammosi (Shortest Vector Problem, SVP)- Faraz qilinsin Λ panjara

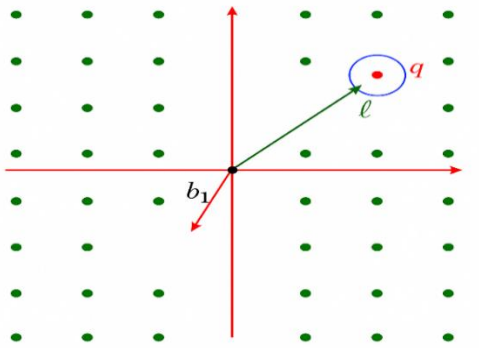
(cc) BY

bazis bazislar $B \in E^{n\times m}$ va $\|\cdot\|$ ayrim normaga (matematik funksiya, masalan, maydonda magnituda yoki uzunlikni aniqlash uchun ishlatiladi) ega bo‘lsin. Faraz qilinsin $\lambda(\Lambda)$ qiymat Λ dagi nolga teng bo‘lmagan eng qisqa vektorning uzunligi bo‘lsin. $\|l\| = \lambda(\Lambda)$ shartni qanoatlantiruvchi $l \in L$ ni topish vazifasi, ya’ni, Λ ning biror eng qisqa vektorini topish eng qisqa vektor muammosi deb ataladi. 3-rasmda panjaradagi eng qisqa vektor tasvirlangan [6].



3-rasm. $\{b_1, b_2\}$ bazisga va eng qisqa vektor l ga ega ikki o‘lchamli panjara

Eng yaqin vektor muammosi (Closest Vector Problem, CVP**)** Faraz qilaylik Λ panjara bazis bazislar $B \in E^{n\times m}$ va $\|\cdot\|$ ayrim normaga ega bo‘lsin. Berilgan $q \in E^n$ nuqta uchun $\|l - q\|$ qiymat eng minimal bo‘lishini ta’minlovchi $l \in L$ ni topish vazifasi eng yaqin vektor muammosi deb ataladi [6]. 4-rasmda panjaradagi eng yaqin vektor tasvirlangan.



4-rasm. Ikki o‘lchamli panjarada q nuqtaga eng yaqin joylashgan vektor bu l vektoridir.

Panjaraga asoslangan algoritmlarning muammolarini matematik tahlili: “LWE (Learning With Errors) muammosi - $A \cdot s + e = b$ ko‘rinishida ifodalanadi, bu yerda **A** – ochiq matritsa, **s** - maxfiy kalit, **e** - kichik tasodifiy xatolik, **b** esa hosil bo‘lgan natijadir. Masalan, asl tenglama $2x = 10$ bo‘lsa, tizim unga $e = 1$ xatolik qo‘shib $2x + 1 = 11$ ko‘rinishida uzatadi. Natijada hujumchi bir vaqtning o‘zida ham maxfiy qiymatni, ham xatoliklarni aniqlashi kerak bo‘ladi. Yuqori o‘lchamli panjaralarda ushbu jarayon eksponensial murakkablashadi va kvant kompyuterlari uchun ham qiyin hisoblanadi [7].”

Ring-LWE (Ring Learning With Errors) - bu LWE muammosining optimallashtirilgan ko‘rinishi bo‘lib, unda oddiy matritsalar o‘rniga halqa (ring) algebraik strukturalari ishlatiladi. Muammo $a \cdot s + e = b$ ko‘rinishida ifodalanadi, bu yerda **a** - ochiq polinom, **s** - maxfiy polinom, **e** - kichik tasodifiy xatolik, **b** esa hosil bo‘lgan natijadir. Masalan, asl hisob $2x = 10$ bo‘lsa, tizim xatolik qo‘shib $2x + 1 = 11$ ko‘rinishida uzatadi. Ring-LWE da ushbu hisoblar polinomlar va halqalar ustida bajariladi, bu esa xotira sarfini kamaytiradi va hisoblashni tezlashtiradi. Shu bilan birga, xatoliklar sabab yashirin kalitni aniqlash yuqori o‘lchamli panjaralarda eksponensial murakkablashadi hamda kvant kompyuterlari uchun ham qiyin hisoblanadi.”

$a(x) \cdot s(x) + e(x) = b(x)$ ko‘rinishidagi hisoblarda $a(x)$ ochiq polinom, $s(x)$ maxfiy polinom, $e(x)$ esa kichik tasodifiy xatolik hisoblanadi. Keyin ochiq polinom $a(x) = 2x + 3$, maxfiy polinom $s(x) = x + 1$ bo‘lsin.

Ularni ko‘paytirsak: $(2x + 3)(x + 1) = 2x^2 + 5x + 3$ hosil bo‘ladi. Endi tizim kichik (xatolik) sifatida $e(x) = 1$ qo‘shadi:

$$2x^2 + 5x + 3 + 1 = 2x^2 + 5x + 4$$

Natijada hujumchi faqat yakuniy $2x^2 + 5x + 4$ polinomini ko‘radi, lekin qaysi qismi asl hisob, qaysi qismi xatolik ekanini aniqlay olmaydi. Yuqori o‘lchamli panjaralarda bunday xatoliklar yashirin kalitni topishni juda murakkablashtiradi va kvant kompyuterlari uchun ham qiyin masalaga aylantiradi [7].

“Module-LWE muammosi - bu LWE va Ring-LWE muammolarining kombinatsiyalashgan ko‘rinishi bo‘lib, xavfsizlik va samaradorlik orasida muvozanat yaratadi. Unda hisoblashlar bitta polinomda emas, balki polinomlar moduli (guruh) ustida bajariladi. Muammo $\underline{A \cdot s + e = b}$ ko‘rinishida ifodalanadi, bu yerda **A** - ochiq polinomlar matritsasi, **s** - maxfiy polinomlar vektori, **e** - kichik tasodifiy xatoliklar, **b** esa hosil bo‘lgan natijadir.

(cc) BY

$$LWE\ da\ A \cdot s + e = b \quad \rightarrow \quad Ring\text{-}LWE\ da$$
$$a(x) \cdot s(x) + e(x) = b(x)$$

Module-LWE da esa - bir dona polinom emas balki polinomlar to‘plami bilan ishlaydi. $[(\mathbf{2x+1}), (\mathbf{x+3})]$ kabi bir nechta polinom ishlatiladi.

Masalan: Ochiq polinomlar $A = [2x + 1,\ x + 2]$, maxfiy polinomlar esa $\mathbf{s} = [\mathbf{x+1},\ \mathbf{1}]$ bo‘lsin.

Tizim avval polinomlarni o‘zaro ko‘paytiradi: $(2x + 1)(x + 1) = 2x^2 + 3x + 1$ va $(x + 2)(1) = x + 2$. So‘ng hosil bo‘lgan natijalar qo‘shilib $2x^2 + 4x + 3$ qiymati olinadi. Keyin tizim kichik tasodifiy (xatolik), masalan $e(x) = 1$, qo‘shib yakuniy $2x^2 + 4x + 4$ natijasini hosil qiladi. Hujumchi faqat yakuniy natijani ko‘radi, biroq qaysi qismi maxfiy polinomga, qaysi qismi xatolikka tegishli ekanini aniqlashi juda murakkab bo‘ladi. Yuqori o‘lchamli panjaralarda ushbu jarayon eksponensial murakkablashadi va kvant kompyuterlari uchun ham qiyin masala hisoblanadi [7].”

Xulosa

Maqolada panjaraga asoslangan kriptografiyaning nazariy asoslari panjara muammolari (SVP, CVP) va LWE (Ring-LWE, Module-LWE) tahlil qilindi, ularning hisobiy murakkabligi xavfsizlik bazisi sifatida o‘rganildi. Kyber, Dilithium, NewHope, NTRUEncrypt algoritmlari o‘rganilib, kvantga bardoshliligi va gomomorf shifrlash imkoniyatlari ko‘rsatildi. Panjara bazislarini generatsiya qilish yaxshi va yomon bazislar farqi matematik misollar bilan tasvirlandi.

Tadqiqot natijalari quyidagi asosiy xulosalarni shakllantirish imkonini beradi.

Panjara nazariyasi - bazis, determinant, "yaxshi" va "yomon" bazis tushunchalari - panjaraga asoslangan kriptotizimlarning matematik poydevorini tashkil etadi. Maxfiy kalit sifatida qisqa va deyarli ortogonal vektorlardan iborat "yaxshi bazis"dan, ochiq kalit sifatida esa unga ekvivalent, ammo tasodifiy "yomon bazis"dan foydalanish printsipi - bu yondashuvning asosiy kriptografik mexanizmi ekanligi ko'rsatildi.

SVP va CVP masalalari, shuningdek ulardan hosil bo'lgan LWE, Ring-LWE va Module-LWE muammolari yuqori o'lchamli panjaralarda hisoblash jihatdan amaliy yechib bo'lmaydigan darajada murakkab bo'lishi isbotlangan. Ring-LWE polinom va halqa strukturalari orqali hisoblash resurslarini optimallashtirsa, Module-LWE polinomlar vektori bilan ishlash orqali xavfsizlik va samaradorlik o'rtasida muvozanat yaratadi. Aynan Module-LWE muammosi Kyber va Dilithium algoritmlarining, Ring-LWE esa NewHope kabi kalit almashinuvi protokollarining xavfsizlik asosini tashkil etadi.

Foydalanilgan adabiyotlar ro‘yxati

1. Shor P.W. Algorithms for quantum computation: discrete logarithms and factoring Proceedings of the 35th Annual Symposium on Foundations of Computer Science. – 1994. – P. 124-134.
2. Ajtai M. Generating hard instances of lattice problems // Proceedings of the twenty-eighth annual ACM symposium on Theory of computing (STOC). – 1996. – P. 99-108.
3. Ajtai M., Dwork C. A public-key cryptosystem with worst-case/average-case equivalence Proceedings of the twenty-ninth annual ACM symposium on Theory of computing (STOC). – 1997. – P. 284-293.
4. Goldreich O., Goldwasser S., Halevi S. Public-key cryptosystems from lattice reduction problems // Advances in Cryptology - CRYPTO'97. Lecture Notes in Computer Science. – Springer, 1997. – Vol. 1294. – P. 112-131.
5. Hoffstein J., Pipher J., Silverman J.H. NTRU: A ring-based public key cryptosystem Algorithmic Number Theory Symposium (ANTS III). Lecture Notes in Computer Science. – Springer, 1998. – Vol. 1423. – P. 267-288.
6. Richter M., Bertram M., Seidensticker J., Tschache A. A mathematical perspective on post-quantum cryptography // Mathematics. – 2022. – Vol. 10, No. 15. – Article 2579.
7. Regev O. On lattices, learning with errors, random linear codes, and cryptography Journal of the ACM. – 2009. – Vol. 56, No. 6. – Article 34. – P. 1-40.

(cc) BY