OLIY TA'LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

RAQAMLI TEXNOLOGIYALAR VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI HUZURIDAGI PEDAGOG KADRLARNI QAYTA TAYYORLASH VA ULARNING MALAKASINI OSHIRISH TARMOQ MARKAZI

"POST KVANT KRIPTOGRAFIYASI"

MODULI BO'YICHA

O' Q U V –U S L U B I Y M A J M U A

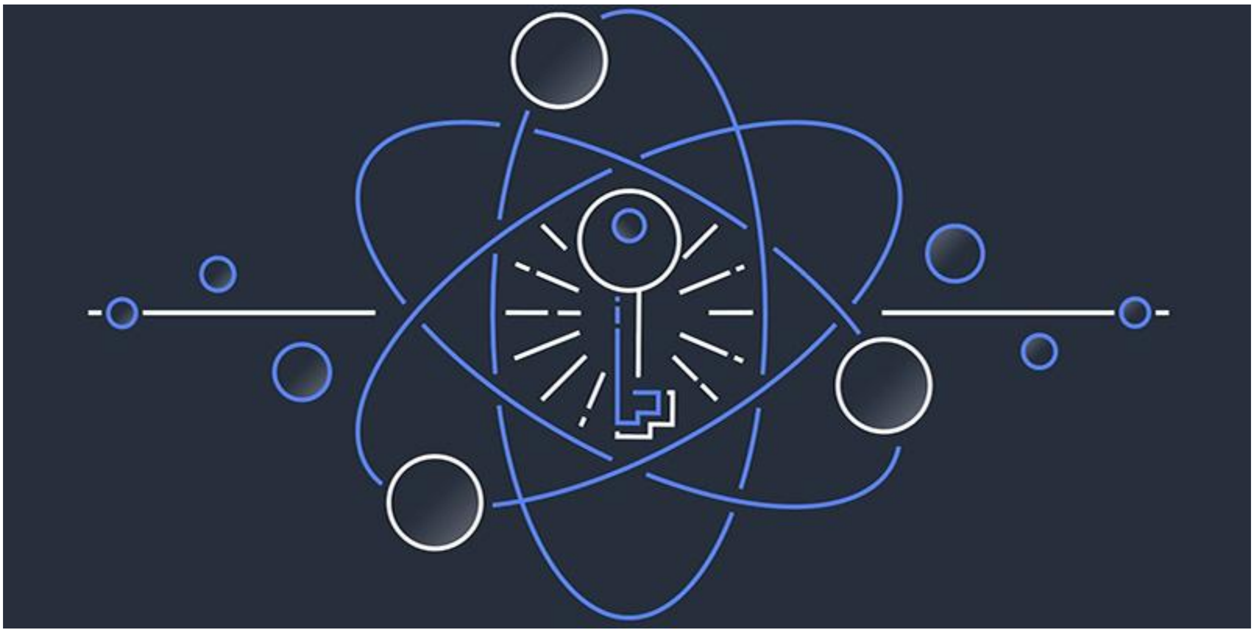
Toshkent - 2025

O‘ZBEKISTON RESPUBLIKASI OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

OLIY TA’LIM TIZIMI PEDAGOG VA RAHBAR KADRLARINI QAYTA TAYYORLASH VA ULARNING MALAKASINI OSHIRISHNI TASHKIL ETISH BOSH ILMIY - METODIK MARKAZI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI HUZURIDAGI PEDAGOG KADRLARNI QAYTA TAYYORLASH VA ULARNING MALAKASINI OSHIRISH TARMOQ MARKAZI

“Kriptologiya” yo‘nalishi



“POST KVANT KRIPTOGRAFIYASI”
MODULI BO‘YICHA

O‘ Q U V –U S L U B I Y M A J M U A

Toshkent – 2025

Modulning o‘quv-uslubiy majmuasi Oliy ta’lim, fan va innovatsiyalar vazirligining 2024 yil 27 dekabrdagi №485-sonli buyrug‘i bilan tasdiqlangan o‘quv dasturi va o‘quv rejasiga muvofiq ishlab chiqilgan.

Tuzuvchilar: **Z.T.Xudoykulov -** PhD, dotsent

Taqrizchilar: **B.F. Abdurahimov** – fizika-matematika fanlari doktori, professor.
O.P. Axmedova - texnika fanlari nomzodi, dotsent.

O‘quv-uslubiy majmua O‘quv dasturi Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Kengashining qarori bilan tasdiqqa tavsiya qilingan (2024-yil 27-noyabrdagi 3/4 (745/746)- sonli bayonnoma).

MUNDARIJA

I BO'LIM.

ISHCHI DASTUR

I. ISHCHI DASTUR

KIRISH

Ushbu dastur Oʻzbekiston Respublikasining 2020-yil 23-sentabrda tasdiqlangan “Ta’lim toʻgʻrisida” Qonuni, Oʻzbekiston Respublikasi Prezidentining 2015-yil 12-iyundagi “Oliy ta’lim muassasalarining rahbar va pedagog kadrlarini qayta tayyorlash va malakasini oshirish tizimini yanada takomillashtirish toʻgʻrisida” PF-4732-son, 2019-yil 27-avgustdagi “Oliy ta’lim muassasalari rahbar va pedagog kadrlarining uzluksiz malakasini oshirish tizimini joriy etish toʻgʻrisida” PF-5789-son, 2019-yil 8-oktabrdagi “Oʻzbekiston Respublikasi oliy ta’lim tizimini 2030-yilgacha rivojlantirish konsepsiyasini tasdiqlash toʻgʻrisida” PF-5847-son, 2020-yil 29-oktabrdagi “Ilm-fanni 2030-yilgacha rivojlantirish konsepsiyasini tasdiqlash toʻgʻrisida” PF-6097-son, 2022-yil 28-yanvardagi “2022-2026 yillarga moʻljallangan Yangi Oʻzbekistonning taraqqiyot strategiyasi toʻgʻrisida” PF-60-son, 2023-yil 25-yanvardagi “Respublika ijro etuvchi hokimiyat organlari faoliyatini samarali yoʻlga qoʻyishga doir birinchi navbatdagi tashkiliy chora-tadbirlar toʻgʻrisida” PF-14-son, Oʻzbekiston Respublikasi Prezidentining 2023-yil 11-sentabrdagi ““Oʻzbekiston — 2030” strategiyasi toʻgʻrisida” PF-158-son Farmonlari, shuningdek, 2024-yil 15-avgustdagi “Oʻzbekiston Respublikasida kriptologiya sohasida ta’lim va ilm-fanni rivojlantirish boʻyicha qoʻshimcha chora-tadbirlar toʻgʻrisida”gi PQ-293-son Qarori, shuningdek, Oʻzbekiston Respublikasi Vazirlar Mahkamasining 2019-yil 23-sentabrdagi “Oliy ta’lim muassasalari rahbar va pedagog kadrlarining malakasini oshirish tizimini yanada takomillashtirish boʻyicha qoʻshimcha chora-tadbirlar toʻgʻrisida”gi 797-son Qarori hamda Oʻzbekiston Respublikasi Vazirlar Mahkamasining “Oliy ta’lim tashkilotlari rahbar va pedagog kadrlarini qayta tayyorlash va malakasini oshirish tizimini samarali tashkil qilish chora-tadbirlari toʻgʻrisida” 2024-yil 11-iyuldagi 415-son Qarorlarida belgilangan ustuvor vazifalar mazmunidan kelib chiqqan holda tuzilgan boʻlib, u oliy ta’lim muassasalari pedagog kadrlarining kasb mahorati hamda innovatsion kompetentligini rivojlantirish, sohaga oid ilgʻor xorijiy tajribalar, yangi bilim va malakalarni oʻzlashtirish, shuningdek amaliyotga joriy etish koʻnikmalarini takomillashtirishni maqsad qiladi.

Qayta tayyorlash va malaka oshirish yoʻnalishining oʻziga xos xususiyatlari hamda dolzarb masalalaridan kelib chiqqan holda dasturda tinglovchilarning ushbu fan doirasidagi bilim, koʻnikma, malaka hamda kompetensiyalariga qoʻyiladigan talablar takomillashtirilishi mumkin.

Modulning maqsadi va vazifalari

Modulining maqsadi: kvant hisoblash qurilmalari amaliyotda qoʻllanila boshlanganda ham axborotni kriptografik himoyasini ishonchli ta’minlashni maqsad qilgan zamonaviy algoritmlar haqida oliy ta'lim muassasalari pedagog kadrlarining bilim, ko'nikma va malakalarini shakllantirishdan iborat.

Modulning vazifalari:

- Zamonaviy kriptografik algoritmlarga kvant hisoblash qurilmalarining ta'siri,
- Post kvant kriptograsiyasining matematik asoslari,
- Zamonaviy post kvant kriptografik algoritmlar,
- Post kvant algoritmlarini dasturiy amalga oshirish haqida nazariy va amaliy bilimlar, ko'nikma va malakalarni shakllantirishdan iborat.

Modul bo'yicha tinglovchilarning bilim, ko'nikma, malaka va kompetensiyalariga qo'yiladigan talablar

"Post kvant kriptografiyasi" modulini o'zlashtirish jarayonida amalga oshiriladigan masalalar doirasida:

Tinglovchi:

Kvant hisoblash qurilmalarini ananaviy kriptografik algoritmlarning xavfsizlik darajasiga ta'sirini;

Post kvant kriptografiyasining matematik asoslarini;

Zamonaviy post kvant kriptografik algoritmlarini va ularning xususiyatlarini ***biladi***.

Zamonaviy post kvant kriptografik algoritmlarni tahlil qilish, ulardan amalda foydalanish ***ko'nikmalariga*** ega bo'ladi.

Yangi post kvant kriptografik algoritmlarini yaratish, kriptografik algoritmlarni dasturiy tomonlama amalga oshirish ***malakalariga*** ega bo'ladi.

Modulni tashkil etish va o'tkazish bo'yicha tavsiyalar

"Post kvant kriptografiyasi" moduli ma'ruza va amaliy mashg'ulotlar shaklida olib boriladi.

Modulni o'qitish jarayonida ta'limning zamonaviy metodlari, pedagogik texnologiyalar va axborot-kommunikatsiya texnologiyalari qo'llanilishi nazarda tutilgan:

- ma'ruza darslarida zamonaviy kompyuter texnologiyalari yordamida prezentatsion va elektron-didaktik texnologiyalardan;
- o'tkaziladigan amaliy mashg'ulotlarda texnik vositalardan, ekspress-so'rovlar, test so'rovlari, aqliy hujum, guruhli fikrlash, kichik guruhlar bilan ishlash, kollokvium o'tkazish, va boshqa interaktiv ta'lim usullarini qo'llash nazarda tutiladi.

Modulning o'quv rejadagi boshqa modullar bilan bog'liqligi va uzviyligi

"Post kvant kriptografiyasi" moduli mazmuni o'quv rejadagi "Kriptografiyaning matematik asosi" o'quv moduli bilan uzviy bog'langan holda pedagoglarning ta'lim jarayonida kriptologiya sohasini chuqur o'rgatishga xizmat qiladi.

Modulning oliy ta’limdagi o‘rni

Modulni o‘zlashtirish orqali tinglovchilar ta’lim jarayonida kriptologiya sohasidagi eng so‘ngi, post kvant kriptografik algorimtlari, bu sohada amalga oshirilgan ishlar, erishilgan yutuqlar bo‘yicha kasbiy kompetentlikka ega bo‘ladilar.

MODUL BO‘YICHA SOATLAR TAQSIMOTI

№	Modul mavzulari	Auditoriya uquv yuklamasi				
		Jami	jumladan			
			Nazariy	Amaiy mashg‘ulot	Ko‘chma mashg‘uloti	
1.	**Post kvant kriptografiyasi (PKK):** Kriptografik algoritmlar ortiq xavfsiz emasmi? PKKdagi muammolar. Kvant hisoblash modeli, kvantli Furye almashtirishi, qidirish algoritmlari: Shor va Grover algoritmi.	2	2			
2.	**Post kvant kriptografiyasi algoritmlari:** Panjaraga asoslangan ochiq kalitli kriptografiya: panjara asosi, xatolik bilan o‘rganishga asoslangan kriptografiya: Kyber, Saber, Dilithium, NTRUga asoslangan kriptografiya: NTRU, Falcon, Kodga asoslangan kriptografiya: chiziqli kodlar, Binar Goppa kodlari, Klassik McEliece algoritmi, Ko‘p o‘zgaruvchili kriptografiya: Ko‘p o‘zgaruvchili polinom funksiyalar, MQ muammosi, IP muammosi, Rainbow, Xeshlashga asoslangan kriptografiya: SPHINCS+.	10	2	8		
3.	**Post kvant kriptografiyasi bo‘yicha NIST konkursi:** talablar, o‘tkazilish bosqichlari, ishtirokchi algoritmlar, tanlab olingan algoritmlar, kelajak	2	2			

	rejalar.					
	Jami:	**14**	**6**	**8**		

NAZARIY MASHG‘ULOTLAR MAZMUNI

1-MAVZU: POST KVANT KRIPTOGRAFIYASI (PKK) (2 SOAT)

Kriptografik algoritmlar ortiq xavfsiz emasmi? PKKdagi muammolar. Kvant hisoblash modeli, kvantli Furye almashtirishi, qidirish algoritmlari: Shor va Grover algoritmi.

2-MAVZU: POST KVANT KRIPTOGRAFIYASI ALGORITMLARI (2 SOAT).

Panjaraga asoslangan ochiq kalitli kriptografiya: panjara asosi, xatolik bilan o‘rganishga asoslangan kriptografiya, NTRUga asoslangan kriptografiya, Kodga asoslangan kriptografiya: chiziqli kodlar, Ko‘p o‘zgaruvchili kriptografiya: Ko‘p o‘zgaruvchili polinom funksiyalar, MQ muammosi, IP muammosi, Xeshlashga asoslangan kriptografiya.

3-MAVZU: POST KVANT KRIPTOGRAFIYASI BO‘YICHA NIST KONKURSI (2 SOAT).

Talablar, o‘tkazilish bosqichlari, ishtirokchi algoritmlar, tanlab olingan algoritmlar, kelajak rejalar.

AMALIY MASHG‘ULOTLAR MAZMUNI

1-MAVZU: AMALIY PKK ALGORITMLARI (4 SOAT)

Kyber, Saber, Dilithium, NTRU, Falcon, Binar Goppa kodlari, Klassik McEliece algoritmi, Rainbow, SPHINCS+ algoritmlari.

2-MAVZU: OPEN QUANTUM SAFE (OQS): LIBOQS KUTUBXONASI (4 SOAT)

Kutubxona bilan ishlash, kalitlarni hosil qilish, almashinish va ERI algoritmlardan foydalanish.

KO‘CHMA MASHG‘ULOT MAZMUNI

Ushbu modul bo‘yicha ko‘chma mashg‘ulotlar nazarda tutilmagan.

O‘QITISH SHAKLLARI

Mazkur modul bo‘yicha quyidagi o‘qitish shakllaridan foydalaniladi:

- ma’ruzalar, amaliy mashg‘ulotlar (ma’lumotlar va texnologiyalarni anglab olish, motivatsiyani rivojlantirish, nazariy bilimlarni mustahkamlash);
- davra suhbatlari (ko‘rilayotgan loyiha yechimlari bo‘yicha taklif berish qobiliyatini rivojlantirish, eshitish, idrok qilish va mantiqiy xulosalar chiqarish);

bahs va munozaralar (loyihalar yechimi bo‘yicha dalillar va asosli argumentlarni taqdim qilish, eshitish va muammolar yechimini topish qobiliyatini rivojlantirish).

II-BO‘LIM.

MODULNI O‘QITISHDA FOYDALANILADIGAN INTERFAOL TA’LIM METODLARI

II. MODULNI O‘QITISHDA FOYDALANILADIGAN INTERFAOL TA’LIM METODLARI

“Blum kubigi” metodi

Metodning maqsadi: Mazkur metod tinglovchilarda yangi axborotlar tizimini qabul qilish va bilimlarni o‘zlashtirilishini yengillashtirish maqsadida qo‘llaniladi, shuningdek, bu metod tinglovchilar uchun “Ochiq” savollar tuzish va ularga javob topish mashqi vazifasini belgilaydi.

Metodni amalga oshirish tartibi:

1. **Ushbu metodni ko‘llash uchun, oddiy kub kerak bo‘ladi. Kubning har bir tomonida ko‘yidagi so‘zlar yoziladi:**

- **Sanab bering, ta’rif bering (oddiy savol)**
- **Nima uchun (sabab-oqibatni aniqlashtiruvchi savol)**
- **Tushintirib bering (muammoni har tomonlama qarash savoli)**
- **Taklif bering (amaliyot bilan bog‘liq savol)**
- **Misol keltiring (ijodkorlikni rivojlantirovchi savol)**
- **Fikr bering (tahlil kilish va baxolash savoli)**

2. O‘qituvchi mavzuni belgilab beradi.

3. O‘qituvchi kubikni stolga tashlaydi. Qaysi so‘z chiqsa, unga tegishli savolni beradi.

“KWHL” metodi

Metodning maqsadi: Mazkur metod tinglovchilarda yangi axborot tizimini qabul qilish va bilimlarni tizimlashtirish maqsadida qo‘llaniladi, shuningdek, bu metod tinglovchilar uchun mavzu bo‘yicha quyidagi jadvalda berilgan savollarga javob topish mashqi vazifasini belgilaydi.

Izoh. *KWHL:*
Know – nimalarni bilaman?
Want – nimani bilishni xohlayman?
How - *qanday bilib olsam bo‘ladi?*
Learn - *nimani o‘rganib oldim?.*

<table>
<tr><th colspan="2">“KWHL” metodi</th></tr>
<tr><td>1. Nimalarni bilaman:
-</td><td>2. Nimalarni bilishni xohlayman, nimalarni bilishim kerak:
-</td></tr>
<tr><td>3. Qanday qilib bilib va topib olaman:
-</td><td>4. Nimalarni bilib oldim:
-</td></tr>
</table>

“5W1H” metodi

Metodning maqsadi: Mazkur metod tinglovchilarda yangi axborot tizimini qabul qilish va bilimlarni tizimlashtirish maqsadida qo‘llaniladi, shuningdek, bu metod tinglovchilar uchun mavzu bo‘yicha qo‘yidagi jadvalda berilgan oltita savollarga javob topish mashqi vazifasini belgilaydi.

What?	Nima? (ta’rifi, mazmuni, nima uchun ishlatiladi)	
Where?	Qayerda (joylashgan, qayerdan olish mukin)?	
What kind?	Qanday? (parametrlari, turlari mavjud)	
When?	Qachon? (ishlatiladi)	
Why?	Nima uchun? (ishlatiladi)	
How?	Qanday qilib? (yaratiladi, saqlanadi, to‘ldiriladi, tahrirlash mumkin)	

“SWOT-tahlil” metodi

Metodning maqsadi: mavjud nazariy bilimlar va amaliy tajribalarni tahlil qilish, taqqoslash orqali muammoni hal etish yo‘llarini topishga, bilimlarni mustahkamlash, takrorlash, baholashga, mustaqil, tanqidiy fikrlashni, nostandart tafakkurni shakllantirishga xizmat qiladi.

S – (strength)	• kuchli tomonlari
W – (weakness)	• zaif, kuchsiz tomonlari
O – (opportunity)	• imkoniyatlari
T – (threat)	• xavflari

“VEYER” metodi

Metodning maqsadi: Bu metod murakkab, ko‘ptarmoqli, mumkin qadar, muammoli xarakteridagi mavzularni o‘rganishga qaratilgan. Metodning mohiyati shundan iboratki, bunda mavzuning turli tarmoqlari bo‘yicha bir xil axborot beriladi va ayni paytda, ularning har biri alohida aspektlarda muhokama etiladi. Masalan, muammo ijobiy va salbiy tomonlari, afzallik, fazilat va kamchiliklari, foyda va zararlari bo‘yicha o‘rganiladi. Bu interfaol metod tanqidiy, tahliliy, aniq mantiqiy fikrlashni muvaffaqiyatli rivojlantirishga hamda o‘quvchilarning mustaqil g‘oyalari, fikrlarini yozma va og‘zaki shaklda tizimli bayon etish, himoya qilishga imkoniyat yaratadi. “Veyer” metodidan ma’ruza mashg‘ulotlarida individual va juftliklardagi ish shaklida, amaliy va seminar mashg‘ulotlarida kichik guruhlardagi ish shaklida mavzu yuzasidan bilimlarni mustahkamlash, tahlil qilish va taqqoslash maqsadida foydalanish mumkin.

Metodni amalga oshirish tartibi:

trener-o‘qituvchi ishtirokchilarni 5-6 kishidan iborat kichik guruhlarga ajratadi;

trening maqsadi, shartlari va tartibi bilan ishtirokchilarni tanishtirgach, har bir guruhga umumiy muammoni tahlil qilinishi zarur bo‘lgan qismlari tushirilgan tarqatma materiallarni tarqatadi;

har bir guruh o‘ziga berilgan muammoni atroflicha tahlil qilib, o‘z mulohazalarini tavsiya etilayotgan sxema bo‘yicha tarqatmaga yozma bayon qiladi;

navbatdagi bosqichda barcha guruhlar o‘z taqdimotlarini o‘tkazadilar. Shundan so‘ng, trener tomonidan tahlillar umumlashtiriladi, zaruriy axborotlr bilan to‘ldiriladi va mavzu yakunlanadi.

Muammoli savol					
1-usul		**2-usul**		**3-usul**	
afzalligi	kamchiligi	afzalligi	kamchiligi	afzalligi	kamchiligi
Xulosa:					

Muammoli savol					
1-usul		**2-usul**		**3-usul**	
afzalligi	kamchiligi	afzalligi	kamchiligi	afzalligi	kamchiligi
Xulosa:					

“Keys-stadi” metodi

«Keys-stadi» - inglizcha so‘z bo‘lib, («case» – aniq vaziyat, hodisa, «stady» – o‘rganmoq, tahlil qilmoq) aniq vaziyatlarni o‘rganish, tahlil qilish asosida o‘qitishni amalga oshirishga qaratilgan metod hisoblanadi. Mazkur metod dastlab 1921 yil Garvard universitetida amaliy vaziyatlardan iqtisodiy boshqaruv fanlarini o‘rganishda foydalanish tartibida qo‘llanilgan. Keysda ochiq axborotlardan yoki aniq voqea-hodisadan vaziyat sifatida tahlil uchun foydalanish mumkin.

“Keys metodi” ni amalga oshirish bosqichlari

Ish bosqichlari	Faoliyat shakli va mazmuni
1-bosqich: Keys va uning axborot ta’minoti bilan tanishtirish	✓ yakka tartibdagi audio-vizual ish; ✓ keys bilan tanishish(matnli, audio yoki media shaklda); ✓ axborotni umumlashtirish; ✓ axborot tahlili; ✓ muammolarni aniqlash
2-bosqich: Keysni aniqlashtirish va o‘quv topshirig‘ni belgilash	✓ individual va guruhda ishlash; ✓ muammolarni dolzarblik iyerarxiyasini aniqlash; ✓ asosiy muammoli vaziyatni belgilash
3-bosqich: Keysdagi asosiy muammoni tahlil etish orqali o‘quv topshirig‘ining yechimini izlash, hal etish yo‘llarini ishlab chiqish	✓ individual va guruhda ishlash; ✓ muqobil yechim yo‘llarini ishlab chiqish; ✓ har bir yechimning imkoniyatlari va to‘siqlarni tahlil qilish; ✓ muqobil yechimlarni tanlash
4-bosqich: Keys yechimini yechimini shakllantirish va asoslash, taqdimot.	✓ yakka va guruhda ishlash; ✓ muqobil variantlarni amalda qo‘llash imkoniyatlarini asoslash; ✓ ijodiy-loyiha taqdimotini tayyorlash; ✓ yakuniy xulosa va vaziyat yechimining amaliy aspektlarini yoritish

“Assesment” metodi

Metodning maqsadi: mazkur metod ta’lim oluvchilarning bilim darajasini baholash, nazorat qilish, o‘zlashtirish ko‘rsatkichi va amaliy ko‘nikmalarini tekshirishga yo‘naltirilgan. Mazkur texnika orqali ta’lim oluvchilarning bilish faoliyati turli yo‘nalishlar (test, amaliy ko‘nikmalar, muammoli vaziyatlar mashqi, qiyosiy tahlil, simptomlarni aniqlash) bo‘yicha tashhis qilinadi va baholanadi.

Metodni amalga oshirish tartibi:

“Assesment”lardan ma’ruza mashg‘ulotlarida talabalarning yoki qatnashchilarning mavjud bilim darajasini o‘rganishda, yangi ma’lumotlarni bayon qilishda, seminar, amaliy mashg‘ulotlarda esa mavzu yoki ma’lumotlarni o‘zlashtirish darajasini baholash, shuningdek, o‘z-o‘zini baholash maqsadida individual shaklda foydalanish tavsiya etiladi. Shuningdek, o‘qituvchining ijodiy yondashuvi hamda o‘quv maqsadlaridan kelib chiqib, assesmentga qo‘shimcha topshiriqlarni kiritish mumkin.

Har bir katakdagi to‘g‘ri javob 5 ball yoki 1-5 balgacha baholanishi mumkin.

Test

Muammoli vaziyat

Tushuncha tahlili (simptom)

Amaliy vazifa

“Insert” metodi

Metodni amalga oshirish tartibi:

- o‘qituvchi mashg‘ulotga qadar mavzuning asosiy tushunchalari mazmuni yoritilgan matnni tarqatma yoki taqdimot ko‘rinishida tayyorlaydi;
- yangi mavzu mohiyatini yorituvchi matn ta’lim oluvchilarga tarqatiladi yoki taqdimot ko‘rinishida namoyish etiladi;
- ta’lim oluvchilar individual tarzda matn bilan tanishib chiqib, o‘z shaxsiy qarashlarini maxsus belgilar orqali ifodalaydilar. Matn bilan ishlashda talabalar yoki qatnashchilarga quyidagi maxsus belgilardan foydalanish tavsiya etiladi:

Belgilar	Matn
“V” – tanish ma’lumot.	
“?” – mazkur ma’lumotni tushunmadim, izoh kerak.	
“+” bu ma’lumot men uchun yangilik.	
“– ” bu fikr yoki mazkur ma’lumotga qarshiman?	

Belgilangan vaqt yakunlangach, ta’lim oluvchilar uchun notanish va tushunarsiz bo‘lgan ma’lumotlar o‘qituvchi tomonidan tahlil qilinib, izohlanadi, ularning mohiyati to‘liq yoritiladi. Savollarga javob beriladi va mashg‘ulot yakunlanadi.

III BO‘LIM.

NAZARIY MATERIALLAR

III. NAZARIY MATERIALLAR

1-ma’ruza. POST KVANT KRIPTOGRAFIYASI (PKK) (2 soat)

Reja:

1.1. Kvant hisoblash asosi, kvant kompyuterlari.
1.2. Kvantli Furye almashtirishi.
1.3. Qidirish algoritmlari: Shor va Grover algoritmi.
1.4. Kriptografik algoritmlar ortiq xavfsiz emasmi?

Tayanch iboralar: *kvant hisoblash, kvant kompyuterlar, kubit, Superpozitsiya (Superposition), chalkashlik, “To‘lqin-zarralar ikkiligi (Wave-Particle Duality)”, Geyzenbergning noaniqlik printsipi, Shor va Grover algoritmi.*

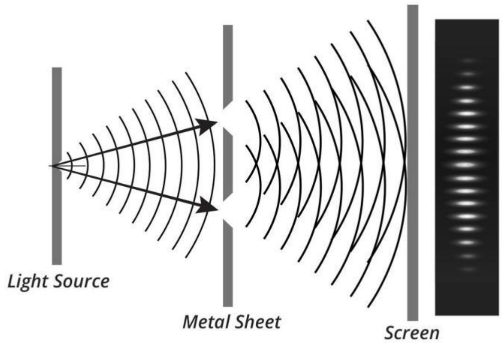
1.1. Kvant hisoblash asosi, kvant kompyuterlari

Kvant nazariyasi fizikadagi eng inqilobiy va intuitiv asoslardan biridir. U koinotning juda kichik miqyoslarda, xususan, atomlar va subatomik zarralar darajasida qanday ishlashini tasvirlash uchun bir qator printsiplar va matematik qoidalarni taqdim etadi. Quyida kvant nazariyasining ba’zi asosiy tushunchalariga batafsilroq ma’lumotlar keltirilgan.

1. “To‘lqin-zarralar ikkiligi (Wave-Particle Duality)”

Klassik fizikada zarralar va to‘lqinlar alohida hisoblanadi. To‘p zarracha, suv to‘lqinlari esa to‘lqinlardir. Ammo, kvant nazariyasida elektronlar va fotonlar (yorug‘lik zarralari) kabi zarralar ularni qanday kuzatishimizga qarab ham zarracha, ham to‘lqin sifatida harakat qilishi mumkin.

- *Misol:* Mashhur “ikki tirqishli tajribada”, agar siz ikkita tor yoriq orqali ekranga yorug‘lik (yoki elektronlarni o‘tqazsangiz) zarrachalar o‘zini faqat ikkita alohida chiziq hosil qilishi kerak bo‘lgan zarrachaga o‘xshatish o‘rniga, to‘lqinlar kabi interferentsiya naqshini hosil qiladi. Biroq, kuzatilganda, ular o‘zlarini alohida zarrachalar kabi tutib, ekranga ikkita aniq chiziq bilan uriladi.



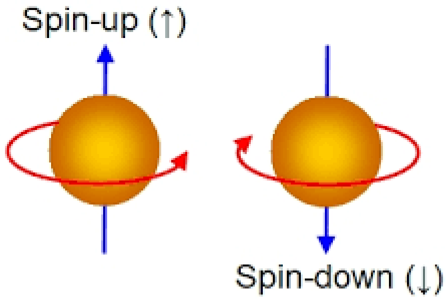
6.1-rasm. “Ikki tirqishli tajriba”

- *Ta’sir:* Bu to‘lqin-zarracha ikkiligi zarralar ham materiya, ham energiya xususiyatlariga ega ekanligini ko‘rsatadi va biz ularni kuzatish usuli ularning xatti-harakatlariga ta‘sir qiladi. Bu bizning materiya haqidagi tushunchamizni qiyinlashtiradi, fizik ob’ektlar va energiya to‘lqinlari o‘rtasidagi chegarani xiralashtiradi.

2. Superpozitsiya (Superposition)

Superpozitsiya kvant tizimlari kuzatilmaguncha yoki o‘lchanmaguncha bir vaqtning o‘zida bir nechta holatda mavjud bo‘lishi mumkinligi haqidagi konsepsiyadir.

- *Izoh:* Masalan, elektronni olaylik. Agar u “tepaga aylanish (spin-up)” va “pastga aylanish (spin-down)” holatida bo‘lsa, u bir vaqtning o‘zida ikkala holatning superpozitsiyasida mavjud. Faqat biz uni o‘lchaganimizda, biz uni yuqoriga yoki pastga aylanayotganini kuzatamiz.



6.2-rasm. “Tepaga aylanish (spin-up)” va “pastga aylanish (spin-down)” holati

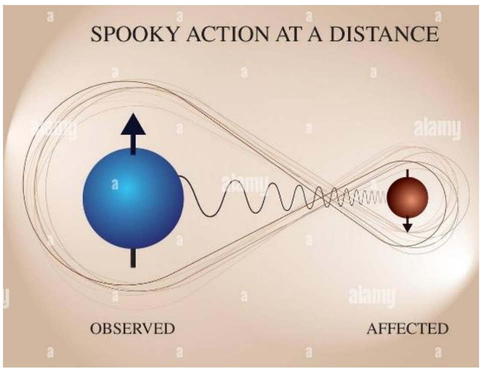
- *“Shrödingerning mushugi” fikrlash tajribasi:* Bu mashhur analogiya superpozitsiyani radioaktiv atom bilan muhrlangan qutidagi mushukni tasavvur qilish orqali tushuntiradi. Agar atom parchalansa, u mushukni o‘ldiradigan qurilmani ishga tushiradi. Kvant mexanikasiga ko‘ra, quti ochilmaguncha va kuzatilmaguncha, mushuk ham o‘lik, ham tirik bo‘lish superpozitsiyasida bo‘ladi.

Superpozitsiya kvant hisoblashlarida asosiy tushuncha bo‘lib, kvant bitlari (qubitlar) bir vaqtning o‘zida 0 va 1 ni ifodalashi mumkin, bu kvant kompyuterlariga murakkab hisob-kitoblarni klassik kompyuterlarga qaraganda eksponensial tezroq qayta ishlash imkonini beradi.

3. Chalkashlik (Entanglement)

Kvant chalkashlik - bu zarralar bir-biridan qanchalik uzoqda bo‘lishidan qat’i nazar, bir zarraning holati boshqasining holati bilan darhol bog‘langan holda bo‘lish hodisa.

- *Izoh:* Ikki, A va B chigal zarrachani tasavvur qiling. Agar A zarrachaning spini (dastagi) yuqoriga qarab o‘lchansa, B zarrasi fazoning narigi tomonida bo‘lsa ham, B zarraning spini bir zumda pastga tushadi. Bu hodisa Eynshteynni hayratda qoldirdi, u buni “uzoqdagi qo‘rqinchli harakat”(“spooky action at a distance”) deb atagan.



6.3-rasm. “Uzoqdagi qo‘rqinchli harakat”(“spooky action at a distance”)

- *Mahalliy bo'lmagan:* Chalkashlik "mahalliy bo'lmagan" ulanish shaklini taklif qiladi, bunda bir zarraning holati haqidagi ma'lumot bir zumda boshqasining holatiga ta'sir qiladi va o'zaro ta'sirlar yorug'lik tezligidan tezroq sodir bo'lmaydi degan klassik taxminlarni buzadi.

- *Ilovalar:* Chalkashlik kvant kriptografiyasi sohasidagi yutuqlarga olib keldi. Xususan, axborot xavfsizligi chigallashgan zarrachalarning xususiyatlariga asoslanadi. Bunda har qanday tinglashga urinish tizim holatini buzishi va buzg'unchi borligini aniqlash imkonini beradi.

Faraz qilinsin A va B o'zaro ta'sir qilmaydigan ikki tizim va ular mos ravishda H_A va H_B Gilbert fazosida. Kompozit tizimning Gilbert fazosi $H_A \otimes H_B$ tenzor ko'paytma. Agar birinchi tizim $|\psi\rangle_A$ holatida va ikkinchi tizim $|\psi\rangle_B$ holatida va kompozit tizim holati $|\psi\rangle_A \otimes |\psi\rangle_B$. Mazkur ko'rinishda taqdim etilgan kompozit tizimning holatlari *ajratilgan holatlar* yoki *ko'paytma holatlar* deyiladi. Barcha holatlar ham ajratilgan holatlar emas. H_A uchun $\{|i\rangle_A\}$ bazisni, H_B uchun $\{|j\rangle_B\}$ bazis belgilansa, u holda $H_A \otimes H_B$ dagi umumiy holat quyidagi ko'rinishda bo'ladi:

$$|\psi\rangle_{AB} = \sum_{i,j} C_{ij}\, |i\rangle_A \otimes |j\rangle_B.$$

Bu holat ajratilgan deyiladi agar $c_{ij} = c_i^A c_j^B$ koeffitsient $|\psi\rangle_A = \sum_i c_i^A |i\rangle_A$ va $|\psi\rangle_B = \sum_j c_j^B |j\rangle_B$ natijalarga olib kelsa. Agar $c_{ij} \neq c_i^A c_j^B$ bo'lsa, u ajratilmagan holat deyiladi. Agar holat ajratilmagan bo'lsa, u chalkashlik holati deyiladi. Masalan, berilgan H_A ning $\{|0\rangle_A, |1\rangle_A\}$ ikki bazis vektorlari va H_B ning $\{|0\rangle_B, |1\rangle_B\}$ ikki bazis vektorlari uchun quyidagi chalkashlik holati:

$$\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B).$$

Agar kompozit sistema shu holatda bo'lsa, A sistema uchun ham, B tizim uchun ham aniq sof holat tushunchasini kiritib bo'lmaydi. Buni aytishning yana bir usuli shundaki, butun holatning fon Neyman entropiyasi nolga teng bo'lsa, quyi tizimlarning entropiyasi noldan katta bo'ladi. Shu ma'noda, tizimlar "chalkash".

4. Geyzenbergning noaniqlik printsipi

Geyzenbergning noaniqlik printsipi shuni ko'rsatadiki, zarrachaning pozitsiyasi va impuls kabi ma'lum bir juft xususiyatlarni bir vaqtning o'zida aniq o'lchash mumkin emas. Biz bir xususiyatni qanchalik aniq bilsak, ikkinchisini shunchalik kam aniq bilamiz.

- *Izoh:* Masalan, elektronning aniq pozitsiyasini o'lchashga harakat qilsak, uning impulsi haqidagi aniq ma'lumotni yo'qotamiz va aksincha. Bu cheklov bizning o'lchash asboblarimizdagi kamchiliklardan kelib chiqmaydi, balki, bu kvant zarralarining asosiy xususiyatidir.

- *Noaniqlik matematikasi:* Noaniqlik printsipi matematik tarzda quyidagicha ifodalanadi:

$$\Delta x \cdot \Delta p \geq \frac{h}{4\pi}$$

Bu yerda, Δx - pozitsiyadagi noaniqlik, Δp - impulsdagi noaniqlik va h - Plank doimiysi.

- *Ta'sirlar:* Bu tamoyil bizning voqelik va determinizmni tushunishimizga chuqur ta'sir ko'rsatadi. Bu dunyo haqida bilishimiz mumkin bo'lgan narsalarning chegaralari borligini ko'rsatadi va kvant darajasida o'ziga xos tasodifiylikni kiritadi.

5. Kvant ehtimoli va o‘lchovi

Kvant mexanikasida natijalar deterministik emas, ya’ni ular klassik mexanikada bo‘lgani kabi qat’iy sabab-ta’sir qoidalariga rioya qilmaydi. Buning o‘rniga, ular ehtimollikka asoslanadi.

- *Ehtimollik to‘lqinlari:* Zarrachalar ular zarracha topilishi mumkin bo‘lgan ehtimollik taqsimotini ta’minlaydigan *to‘lqin funktsiyalari* bilan tavsiflanadi. To‘lqin funksiyasi amplitudasining har qanday joylashuvdagi kvadrati u yerda zarrachani topish ehtimolini ifodalaydi.
- *To‘lqin funktsiyasining qulashi:* Biz zarrachaning holatini o‘lchaganimizda, masalan, to‘lqin funktsiyasi “qulaydi” va zarracha aniq pozitsiyani egallaydi. O‘lchovgacha esa, zarracha aniqlik bilan emas, balki ehtimollar bilan tavsiflangan mumkin bo‘lgan holatlar oralig‘ida mavjud bo‘ladi.
- *Ta’sirlar:* Bu klassik determinizmga teskari. Kvant mexanikasi zarrachani biz o‘lchamagunimizcha aniq qayerda ekanligini aytmaydi, faqat uning qayerda bo‘lishi mumkinligini aytadi, ya’ni tasodifiylik va ehtimollik fazoning asosiy jihatlari hisoblanadi.

Kvantni klonlash mumkin emasligi to‘g‘risida teorema

Kvantni klonlash mumkin emasligi to‘g‘risida teorema 1982-yilda Wootters, Zurek va Dieks tomonidan ta’kidlangan hamda kvant hisoblash va tegishli sohalarda chuqur ta’sirga ega.

Teorema. Ixtiyoriy kvant holatini mukammal tarzda takrorlab bo‘lmaydi.

Teorema berilgan kvant holatini uning haqiqiy holatini o‘zgartirmasdan undan bir xil nusxa olish mumkin emasligini ko‘rsatadi. Bu xususiyat kvant kriptografiyasi uchun muhim bo‘lib, aloqani eshitish hujumiga bardoshlikni ta’minlashda muhim ahamiyat kasb etadi.

Kvant nazariyasining qo‘llanilishi va ahamiyati

Kvant nazariyasi shunchaki nazariy emas, balki, ko‘plab zamonaviy texnologiyalar uchun asosdir:

- *Yarimo‘tkazgichlar:* Kvant holatlaridagi elektronlarning xatti-harakatlarini tushunish bizga barcha zamonaviy elektron qurilmalarning qurilish bloklari bo‘lgan tranzistorlarni ishlab chiqishga imkon beradi.
- *Lazerlar:* Kvant mexanikasi lazerlarning ishlashi uchun asosiy bo‘lgan ogohlantirilgan emissiya jarayonini tavsiflaydi.
- *Kvant hisoblash:* Superpozitsiya va chalkashlik kabi kvant printsiplari kvant kompyuterlarini ishlab chiqishga imkon beradi, bu kriptografiya va molekulyar o‘zaro ta’sirlarni simulyatsiya qilish kabi muayyan vazifalar uchun klassik kompyuterlardan ancha ustun bo‘lishi mumkin.
- *Kvant kriptografiyasi:* nazariy jihatdan buzilmaydigan shifrlash usullarini yaratish uchun chalkashlikdan foydalanadi.
- *Magnit-rezonans tomografiya (MRI):* Kvant mexanikasi tibbiy diagnostikada MRI texnologiyasi uchun zarur bo‘lgan yadro magnit rezonansini tushuntiradi.

Kvant kompyuteri kvant mexanikasi tamoyillari asosida ishlaydigan kompyuterning ilg‘or turi bo‘lib, fizikaning asosiy nazariyasi bo‘lib, tabiatni atomlar va subatomik zarrachalarning energiya darajalarining eng kichik shkalalarida tasvirlaydi. Bitlarni axborotning eng kichik birligi sifatida ishlatadigan klassik kompyuterlardan farqli o‘laroq, kvant kompyuterlari kvant bitlari yoki kubitlardan foydalanadi. Bu kvant kompyuterlariga klassik kompyuterlar uchun bajarib bo‘lmaydigan muayyan turdagi murakkab muammolarni hal qilish imkonini beradi.

Kvant hisoblashda asosiy tushunchalar

Kubitlar:

Klassik hisoblashda bit 0 yoki 1 ga teng. Kvant hisoblashda kubit bir vaqtning o‘zida 0 va 1 ning superpozitsiyasida mavjud bo‘lishi mumkin. Bu superpozitsiyaning kvant xususiyati tufayli mumkin va bu kvant kompyuterlariga bir vaqtning o‘zida katta hajmdagi ma’lumotlarni qayta ishlash imkonini beradi.

Qubitlar odatda elektronlar yoki fotonlar kabi kvant zarralari yordamida yaratiladi. Ular turli xil fizik tizimlar, jumladan, magnit maydonlarida tutilgan ionlar, o‘ta o‘tkazuvchan zanjirlar yoki yorug‘lik zarralari bilan ifodalanishi mumkin.

Superpozitsiya:

Superpozitsiya kubitlarga bitta ikkilik holat bilan chegaralanib qolmasdan, bir vaqtning o‘zida bir nechta holatda mavjud bo‘lishga imkon beradi. Superpozitsiyadagi bitta kubit bir vaqtning o‘zida 0 va 1 ni ifodalashi mumkin. Bu ko‘proq kubitlar qo‘shilganda hisoblash quvvatini eksponent ravishda oshiradi.

Amalda, superpozitsiya kvant kompyuterining parallel ravishda ko‘plab hisob-kitoblarni bajarishi mumkinligini anglatadi, shuning uchun u klassik kompyuterlarga qaraganda ma’lum muammolarni potentsial ravishda tezroq hal qilishi mumkin.

O‘zaro bog‘liqlik:

O‘zaro bog‘liqlik - bu kvant hodisasi bo‘lib, ikki yoki undan ortiq kubitlar bir-biridan qanchalik uzoqda bo‘lishidan qat’i nazar, bir kubitning holati boshqa (lar)ning holatiga bevosita ta’sir qiladigan tarzda bog‘langandir.

O‘zaro bog‘liq kubitlar kvant kompyuterlariga juda murakkab hisob-kitoblarni amalga oshirishga va kubitlar o‘rtasidagi yuqori darajadagi o‘zaro bog‘liqlikni saqlashga imkon beradi. Bu xususiyat ko‘plab kvant algoritmlari uchun juda muhimdir, chunki u kubitlarga klassik bitlar qila olmaydigan noyob usullarda birgalikda ishlash imkonini beradi.

Interferentsiya:

Kvant aralashuvi kvant algoritmida ma’lum natijalar ehtimolini nazorat qilish uchun kvant hisoblashda qo‘llaniladi. Kvant algoritmlari ma’lum kvant holatlariga konstruktiv yoki buzg‘unchi tarzda xalaqit beradigan operatsiyalarni qo‘llash orqali to‘g‘ri javoblar ehtimolini oshirishi va noto‘g‘ri javoblarni bostirishi mumkin.

Kvant gatelar va sxemalari:

Kvant kompyuterlari kubitlarni boshqarish uchun kvant gatelaridan foydalanadi. Kvant gatelari klassik hisoblashda mantiqiy gatelarga o‘xshaydi, lekin kvant printsiplariga asoslanadi.

Kvant gatelari Hadamard gate (kubitni superpozitsiyaga qo‘yadi), Pauli-X kubiti (kubit holatini aylantiruvchi) va CNOT gate (kubitlarni o‘rab turgan ikki kubitli eshik) kabi operatsiyalarni bajaradi.

Ushbu gatelar kvant sxemalarida hisob-kitoblarni amalga oshirish uchun joylashtirilgan, algoritmlar kubitlarni kerakli chiqish holatiga o‘zgartiradigan bir qator gate operatsiyalaridan iborat.

Kvant kompyuterlari klassik kompyuterlardan qanday farq qiladi

Ma’lumotlarni qayta ishlash: Klassik kompyuterlar bitlardan ma’lumotlarning eng kichik birligi sifatida foydalanadi, bir vaqtning o‘zida bitta hisoblashni chiziqli tarzda qayta ishlaydi. Kvant kompyuterlari kubitlardan foydalanadi, bu ularga bir vaqtning o‘zida ko‘plab hisoblashlarni qayta ishlash imkonini beradi.

Muammo turlari: Kvant kompyuterlari klassik kompyuterlarni almashtirish uchun mo‘ljallanmagan; Buning o‘rniga ular katta sonlarni faktorlash, kvant fizikasini simulyatsiya qilish va optimallashtirish masalalari kabi muayyan turdagi muammolar uchun mos keladi.

Masshtablilik va xatolik darajalari: Kvant kompyuterlari masshtablilik va yuqori xato darajalari bilan bog‘liq muammolarga duch keladi. Kvant ma’lumotlari tashqi omillarga juda sezgir va kubit barqarorligini saqlash juda past harorat yoki vakuum muhitini talab qiladi.

Kvant kompyuterlarining turlari

Supero‘tkazuvchi kvant kompyuterlari:

Bular kvant effektiga erishish uchun mutlaq nolga yaqin sovutilgan o‘ta o‘tkazuvchan zanjirlardan foydalanadi. IBM, Google va Rigetti kabi kompaniyalar ushbu texnologiyadan foydalanadilar.

Supero‘tkazuvchi kubitlar nisbatan yuqori xatolik darajalariga ega, ammo ularni boshqarish va ishlab chiqarish oson, bu ularni eng ko‘p o‘rganilgan va ishlab chiqilgan kubit turiga aylantirdi.

Tuzoqlangan (trapped) ionli kvant kompyuterlari:

Ushbu yondashuvda ionlar (zaryadlangan atomlar) elektromagnit maydonlarda ushlab turiladi va lazerlar bilan boshqariladi. IonQ va Honeywell kabi kompaniyalar bu texnologiyada yetakchi hisoblanadi.

Tuzoqlangan ion tizimlari, odatda, supero‘tkazuvchan kubitlarga qaraganda kamroq xatolik va kogerentlik vaqtlariga ega, ammo ularni kengaytirish qiyinroq.

Fotonik kvant kompyuterlari:

Ular yorug‘lik zarralarini (fotonlar) kubitlar sifatida ishlatadilar va nur ajratgichlar, nometalllar va fazalarni o‘zgartirgichlar bilan boshqariladi. PsiQuantum kabi kompaniyalar ushbu yondashuvni o‘rganmoqda.

Fotonik kvant kompyuterlari xona haroratida ishlay oladi, fotonlar esa katta shovqinlarsiz uzoq masofalarni bosib o‘tadi, bu ularni kvant aloqasi uchun ham mos qiladi.

Topologik kvant kompyuterlari (eksperimental):

Microsoft tomonidan kashf qilingan ushbu yondashuv ikki o‘lchovda mavjud bo‘lgan ekzotik zarralar bo‘lgan anyonlarga asoslangan topologik kubitlardan foydalanadi. Ushbu kubitlar nazariy jihatdan barqarorroq va xatolarga kamroq moyil.

Ushbu texnologiya hali ham asosan nazariy va amaliy jihatdan amalga oshirilmagan, ammo xatolarga qarshi turuvchi barqaror kubitlarni yaratishga vada beradi.

Kvantli yumshatgichlar (Quantum annealers):

D-Wave tomonidan ishlab chiqilgan kvantli yumshatgichlar universal kvant kompyuterlari emas, balki optimallashtirish muammolarini hal qilish uchun ixtisoslashgan. Ular tizimdagi eng past energiya konfiguratsiyasini topish orqali ishlaydi.

Kvant yumshatgichlari kvant hisoblarining barcha turlari uchun mos emas, chunki ular umumiy kvant algoritmlarini bajarish qobiliyatiga ega emas. Biroq, ular optimallashtirish va mashinani o‘rganishda maxsus ilovalar uchun foydalidir.

Kvant kompyuterlarining ilovalari

Kriptografiya:

Kvant kompyuterlari Shor algoritmi kabi algoritmlar tufayli ko‘plab klassik kriptografik tizimlarni (masalan, RSA va ECC) buzishi mumkin, bu esa katta raqamlarni samarali yechishi mumkin.

Biroq, kvant kalitlarini taqsimlash (QKD) kabi kvant kriptografiyasi usullari kvant hujumlariga chidamli shifrlashning yangi, xavfsiz usullarini taklif qiladi.

Dori kashfiyoti va materialshunoslik:

Kvant kompyuterlari kvant darajasida molekulyar o‘zaro ta’sirlarni simulyatsiya qilishi mumkin, bu klassik kompyuterlar uchun qiyin. Bu olimlarga murakkab molekulalarni aniq modellashtirishga imkon berib, dori kashfiyoti, kimyo va materialshunoslikda inqilob qilishi mumkin.

Optimallashtirish muammolari:

Kvantning taxminiy optimallashtirish algoritmi (QAOA) kabi kvant algoritmlari murakkab optimallashtirish muammolarini klassik algoritmlarga qaraganda samaraliroq hal qilishi mumkin. Bu logistika, moliya, ishlab chiqarish va sun’iy intellektda ilovalarga ega.

Mashinani o‘rganish va AI:

Kvant kompyuterlari ma’lum turdagi mashinalarni o‘rganish vazifalarini tezlashtirish imkoniyatiga ega. Kvant mashinasini o‘rganish o‘sib borayotgan soha bo‘lib, shablonni aniqlash, klasterlash va tasniflash algoritmlarini yaxshilash uchun kvant hisoblashlaridan foydalanish usullarini o‘rganadi.

Iqlimni modellashtirish va atrof-muhit fanlari:

Kvant kompyuterlari ob-havo, okean oqimlari va iqlim modellari kabi murakkab tizimlarning simulyatsiyasini yaxshilashi mumkin. Ushbu simulyatsiyalar kvant kompyuterlari ta’minlay oladigan katta hisoblash quvvatini talab qiladi.

Kvant hisoblashdagi dolzarb muammolar

Dekogerentlik va xatolik darajasi:

Kubitlar atrof-muhitga sezgir va dekogerentlik tufayli kvant holatini osongina yo‘qotishi mumkin. Hisob-kitoblarni amalga oshirish uchun etarlicha uzoq vaqt barqarorlikni saqlash katta muammo hisoblanadi.

Kvant xatosini tuzatish bo‘yicha ishlar olib borilmoqda, lekin bitta “mantiqiy” kubitni yaratish uchun ko‘plab fizik kubitlarni talab qiladi, bu esa joriy kvant kompyuterlarini masshtablashni qiyinlashtiradi.

Masshtablilik:

Keng miqyosli kvant kompyuterini qurish minglab yoki hatto millionlab kubitlarni talab qiladi, ammo hozirgi texnologiya o‘nlab yoki bir necha yuz kubitlar bilan cheklangan.

Koʻp qubitlarni barqaror tarzda ulash va boshqarish muhim muhandislik muammosidir.

Kvant algoritmlari:

Kvant kompyuterlarining noyob xususiyatlaridan foydalanishi mumkin boʻlgan foydali kvant algoritmlarini ishlab chiqish doimiy tadqiqot sohasidir. Hozirgi vaqtda faqat bir nechta algoritmlar (Shor va Grover algoritmlari kabi) klassik usullardan yaqqol ustunligini koʻrsatmoqda.

Qurilma va infratuzilma:

Kvant kompyuterlari maxsus, qimmat uskunalar (masalan, oʻta oʻtkazuvchan kubitlarni mutlaq nolga yaqin sovutish kerak) va foydalanish imkoniyatini cheklaydigan murakkab infratuzilmani talab qiladi.

Texnologiya taraqqiyoti sari ba’zi kompaniyalar kvant hisoblashlarini bulut orqali foydalanish imkoniyatini yaratish ustida ishlamoqda, ammo fizik foydalanish hali ham cheklangan.

Kvant ustunligi va boshqalar

Kvant ustunligi - bu kvant kompyuteri mos vaqt ichida har qanday klassik kompyuter uchun imkonsiz boʻlgan hisoblashni amalga oshirishi mumkin boʻlgan nuqta. 2019-yilda Google oʻzining kvant kompyuteri Sycamore klassik superkompyuterlar uchun minglab yillar davom etadigan muayyan vazifani soniyalarda bajarganida kvant ustunligini da’vo qildi. Biroq, bu vazifa amaliy jihatdan foydali emas edi va amaliy, ta’sirli kvant ustunligiga erishish haqida munozaralar davom etmoqda.

Kvant hisoblashning kelajagi

Kvant hisoblash hali ham dastlabki bosqichda. IBM, Google va IonQ kabi kompaniyalar jadal taraqqiyotga erishayotgan boʻlsada, amaliy, keng koʻlamli, nosozliklarga chidamli kvant kompyuterlari hali ham yillar va hatto oʻnlab yillar uzoqda boʻlishi mumkin. Hozirgi kvant kompyuterlari shovqinli oʻrta miqyosli kvant (NISQ) qurilmalari boʻlib, ular cheklangan miqdordagi kubitlarga ega va xatolarga moyil.

Biroq, bu sohadagi tadqiqotlar va ishlanmalar oʻsishda davom etmoqda va kvant xatolarini tuzatish, qubit barqarorligi va kvant algoritmlaridagi yutuqlar bilan kvant kompyuterlari kriptografiya, materialshunoslik va sun’iy intellekt kabi murakkab hisob-kitoblarga tayanadigan sohalarni oʻzgartirishi mumkin.

Quyida mavjud kvant computerlari ularning xususiyatlari boʻyicha qiyosiy tahlil qilingan.

1.1-jadval

Mavjud kvant computerlari va ularning xususiyatlari

Tashkilot/ Kompyuter	**Kubit turi**	**Kubit soni**	**Bardoshligi**	**Foydalanish turi**	**Asosiy ilovalari**
IBM Quantum	Super-oʻtkazuvchi	127 (Eagle), 433	Yuqori kvant hajmi, past xatolik darajasi	Cloud (IBM)	Optimallashtirish, kimyo, moliya, mashinali

					o‘rganish
Google Sycamore	Super-o‘tkazuvchi	54	Kvant ustunligi, yuqori darajadagi ishonchlilik	Tadqiqot uchun faqat	Kvant algoritmlari, ustunlik tadqiqoti
D-Wave Advantage	Kvantli yumshatgich	5000	Optimallashtirish, muayyan muammolarni hal qilish	Cloud (Leap)	Rejalashtirish, logistika, mashinali o‘rganish
IonQ	Tuzoqlangan ionli	29	Yuqori aniqlik, uzoq uyg‘unlik	Cloud (AWS, Azure, Google)	Kimyo, ML, yuqori aniqlikdagi hisoblar
Rigetti Aspen	Super-o‘tkazuvchi	80	Kuchli kubit ulanishi	Cloud (QCS)	Optimallashtirish, kvant ML, kimyo
PsiQuantum	Fotonik	1 million (maqsad)	Xona haroratida ishlash, kengaytiriladigan kubitlar	Rivojlanishda	Katta miqyosdagi fizika, kriptografiya, simulyatsiyalar
Microsoft (Topological)	Topologik (tadqiqot)	Ilmiy izlanish olib borilmoqda	Yuqori barqarorlik, nazariy xatolarga chidamlilik	Cloud (Azure Quantum)	Katta miqyosli simulyatsiyalar, kriptografiya, ML

1.2. Kvantli Furye almashtirishi

Kvant Furye transformatsiyasi (QFT) klassik diskret Furye transformatsiyasining (DFT) kvant analogidir. Bu ko‘plab kvant algoritmlarining asosidir, jumladan, Shor algoritmi va kvant fazasini baholash, kvant kompyuterlariga davriylik va shovqinlarni samarali boshqarish imkonini beradi.

QFT kvant holatini hisoblash bazisidan “Furye o‘zgartirilgan” bazisiga o‘tkazadi. n qubit kvant holati $|x\rangle = \sum_{k=0}^{2^n-1} c_k |k\rangle$ uchun, QFT uni quyidagiga o‘zgartiradi: $QFT(|x\rangle) = \frac{1}{\sqrt{2n}} \sum_{y=0}^{2^n-1} (\sum_{k=0}^{2^n-1} c_k e^{2\pi iky/2^n}) |y\rangle$. Bu yerda, k va y qiymatlar hisoblash bazisini ko‘tadi, $e^{2\pi iky/2^n}$ - Furye o‘zgartirilgan bazisda kvant holatlarini ajratib turuvchi faza omilini ifodalaydi.

QFT klassik diskret Furye transformatsiyasiga qaraganda eksponent ravishda tezroq. Kvant kompyuterlarida QFT $O(n^2)$ amalni talab etadi. 2^n o‘lchamli ma’lumot uchun klassik DFT $O(2^n \log(2^n))$ murakkablikka ega.

Hadamard gate

Hadamard gate (H deb belgilangan) eng asosiy kvant gatelaridan biridir. U bitta kubitni o‘zgartirib, superpozitsiya holatini yaratadi.

Hadamard gate bir kubitli gate bo‘lib, u $|0\rangle$ va $|1\rangle$ asosiy holatlarini superpozitsiyalarga moslashtiradi:

$$H|0\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}},\ H|1\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}.$$

Matritsa shaklida Hadamard gate quyidagicha ifodalanadi:

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

1.3. Qidirish algoritmlari: Shor va Grover algoritmi

Shor algoritmi

Shor algoritmi 1994-yilda Piter Shor tomonidan ishlab chiqilgan, kriptografiyadagi quyidagi ikkita asosiy muammoni samarali hal qila oladigan innovatsion kvant algoritmidir:

1. *Butun sonni faktorlash:* Katta murakkab N sonini tub faktorlarga ajratish.
2. *Diskret logafimlash muammosi:* $a^x \equiv b\ (mod\ p)$ tenglamadagi x ni aniqlash.

Bu muammolar RSA, ECC (Elliptic Curve Cryptography) va Diffie-Hellman kabi keng qo‘llaniladigan kriptografik sxemalarning xavfsizligini ta’minlaydi. Bu vazifalar uchun klassik algoritmlar eksponensial vaqtni talab qiladi, ammo, Shor algoritmi ularni polinom vaqtida yechishi mumkin, bu esa hozirgi kriptografik tizimlar uchun katta xavf tug‘diradi.

Shor algoritmining muhim komponentlari:

Shor algoritmi funktsiya davrini topish uchun kvant hisoblash tamoyillaridan foydalanadi, bu faktorizatsiya yoki diskret logarifm masalasini hal qilishda muhim qadamdir. Bu qanday ishlashi haqida qisqacha ma’lumot quyida keltirilgan:

1. *Qo‘yilgan muammo: Butun sonni faktorlash*

Murakkab son N berilgan, uning tub ko‘paytuvchilarini topish talab etilsin.

2. *Shor algoritmidagi qadamlar:*
   - *2.1.* Klassik dastlab ishlov berish:
     - *2.1.1.* N juftligini yoki kichik tub sonlarga bo‘linishini tekshirish; agar shunday bo‘lsa, to‘xtash va tub sonlarni chiqarish.
     - *2.1.2.* Tasodifiy $1 < a < N$ bo‘ladigan butun son a ni tanlang. Agar $gcd(a, N) > 1$ bo‘lsa, $gcd(a, N)$ qiymat N ning non-trivial (xos bo‘lmagan) tub ko‘paytuvchisi bo‘ladi.
   - *2.2.* Kvant kompyuteri bilan davrni qidirish:
     - *2.2.1.* $f(x) = a^x\ mod\ N$ funksiyaning r davrini kvant kompyuterlari yordamida aniqlash, ya’ni: $a^r\ mod\ N = 1$.
   - *2.3.* Klassik so‘ngi ishlov berish:
     - *2.3.1.* r topilgandan so‘ng:

2.3.1.1. Agar r toq son yoki $a^{r/2} \equiv -1\ mod\ N$ bo‘lsa, orqaga qaytiladi va yangi a tanlanadi.

2.3.1.2. Aks holda, quyidagilar hisoblanadi: $gcd(a^{\frac{r}{2}} - 1\ , N)$ va $gcd(a^{\frac{r}{2}} + 1\ , N)$.

2.3.1.3. Ushbu qiymatlardan kamida bittasi N ning non-trivial faktorini beradi.

3. *Kvant kompyuteri bilan davrni qidirish haqida qisqacha ma’lumot*

3.1. Shor algoritmining eng muhim qismi kvant tamoyillari yordamida amalga oshiriladigan davrni aniqlashdir:

3.1.1. Superpozitsiya: x ning barcha mumkin bo‘lgan holatlarining superpozitsiyasini yaratish.

3.1.2. Funksiyani baholash: barcha x lar uchun parallel holatda $f(x) = a^x\ mod\ N$ hisoblash.

3.1.3. Kvant Furye transformatsiyasi (Quantum Fourier Transform, QFT): $f(x)$ funksiyasining davriyligi r ni chiqarish uchun QFT dan foydalanish.

3.1.4. O‘lchov: r haqida ma’lumotni ochib beradigan kvant holatini o‘lchash.

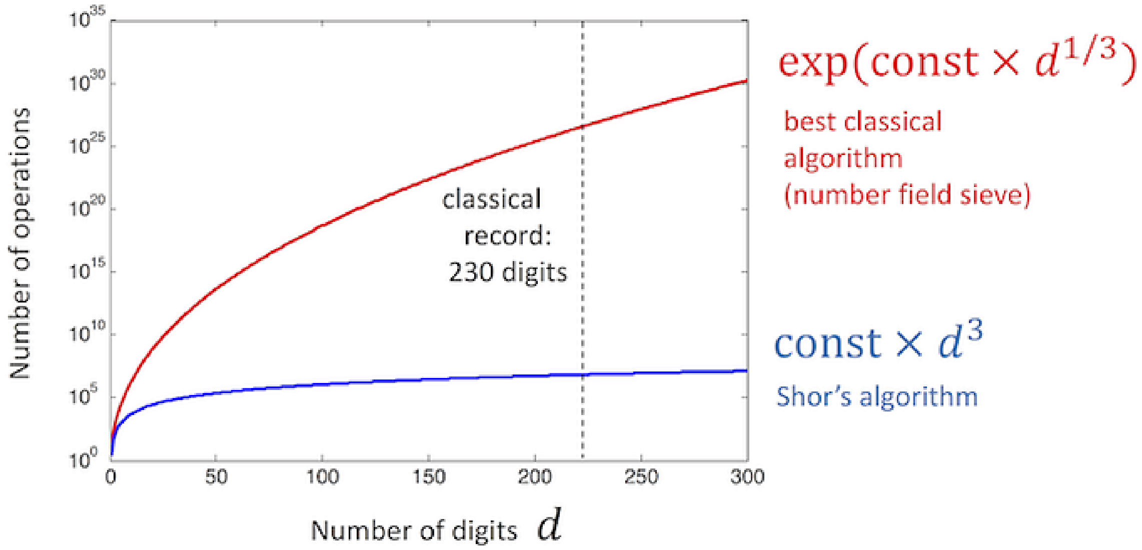
4. *Samaradorlik*

Kvant kompyuterida Shor algoritmi polinom vaqtida ishlaydi, taxminan:

$$O((\log N)^2 (\log \log N)(\log \log \log N))$$

Bu sub-eksponensial vaqtda ishlaydigan umumiy sonlar maydoni g‘alviri (General Number Field Sieve, GNFS) kabi eng mashhur klassik algoritmlarga qaraganda eksponent ravishda tezroq.

Shor algoritmining eng yaxshi klassik faktorizatsiya algoritmiga nisbatan ishlash samaradorligi 1.1-rasmda keltirilgan.



1.1-rasm. Shor algoritmining eng yaxshi klassik faktorizatsiya algoritmiga nisbatan ishlash samaradorligi

Grover algoritmi

Grover algoritmi 1996-yilda Lov Grover tomonidan ishlab chiqilgan kvant qidiruv algoritmidir. U eng mashhur kvant algoritmlaridan biri hisoblanib, u klassik algoritmlarga nisbatan strukturalashmagan qidiruv muammolari uchun kvadratik tezlikni ta'minlaydi.

Grover algoritmi strukturalashmagan ma'lumotlar bazasini qidirish muammosini hal qiladi. N elementlarning saralanmagan ma'lumotlar bazasini hisobga olgan holda, maqsad ma'lum bir elementni w ("belgilangan" element deb ataladi) topishdir. Klassik usulda qidirish eng yomon holatda $O(N)$ operatsiyani talab qiladi. Grover algoritmi buni $O(\sqrt{N})$ ga kamaytiradi. Masalan, 1 000 000 ta elementdan iborat ma'lumotlar bazasida klassik qidiruv 1 000 000 ta so'rovni talab qilishi mumkin, Grover algoritmi esa taxminan 1 000 kvant so'rovini talab qiladi.

Grover algoritmining qadamlari

1. Initsializatsiya: Hadamard gatedan foydalanib, barcha mumkin bo'lgan holatlarning teng superpozitsiyasini tayyorlash: $|\psi\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle.$

2. Oracle so'rovi: Fazali burilish orqali maqsad holati $|w\rangle$ ni belgilaydigan Oracle funksiyasi O dan foydalaniladi: $O|x\rangle = \begin{cases} -|x\rangle, agar\ x = w\ bo'lsa, \\ |x\rangle, aks\ holda \end{cases}$. Ushbu qadam belgilangan holatning amplitudasi belgisini aylantiradi.

3. Amplitudani kuchaytirish (Grover diffuziya operatori): Belgilangan holat ehtimolini o'rtacha amplituda atrofidagi holatni aks ettiruvchi Grover diffuziya operatori G yordamida kuchaytiriladi: $G = 2|\psi\rangle\langle\psi| - I$, bu yerda, I – ayniylik (identity) operatori.

4. Iteratsiyalar: Oracle va diffuziya operatorini $\approx \sqrt{N}$ marta qo'llaniladi. Har bir iteratsiya belgilangan holatning ehtimollik amplitudasini oshiradi.

5. O'lchash: Kvant holati o'lchanadi. Natijada yuqori ehtimollik bilan belgilangan holat w bo'ladi.

Grover algoritmining matematik asosi

Holatni taqdim etish: Grover algoritmining istalgan nuqtasidagi kvant holatini superpozitsiya sifatida yozish mumkin:

$|w\rangle$: - belgilangan holat;

$|r\rangle$: - qolgan $N-1$ ta belgilanmagan holat.

U holda, $|\psi\rangle = \alpha|w\rangle + \beta|r\rangle$ bo'lsin. Bu yerda, α va β lar ehtimollik amplitudalari. Dastlabki holda, $\alpha = \frac{1}{\sqrt{N}}$ va $\beta = \sqrt{\frac{N-1}{N}}$.

Amplitudani kuchaytirish: Har bir Grover iteratsiyasi holat vektorini $|w\rangle$ va $|r\rangle$ oralig'ida joylashgan ikki o'lchovli fazoda $|w\rangle$ ga yaqinroq aylantiradi. Aylanish burchagi θ taxminan $\sin\theta \approx \frac{2}{\sqrt{N}}$ ga teng. k iteratsiyadan so'ng $\alpha_k = \sin((2k+1)\theta)$, $\beta_k = \cos((2k+1)\theta)$. $|w\rangle$ o'lchash ehtimolini maksimal darajada oshirish uchun $k \approx \frac{\pi}{4}\sqrt{N}$ qiymat tanlanadi.

Grover algoritmini qo‘llanishi:

Qidiruv muammolari:

Strukturalashmagan ma’lumotlar bazasini qidirish yoki ko‘plab imkoniyatlar orasida aniq echim topish uchun.

Optimallashtirish:

Optimal kiritishni izlash orqali funksiyaning minimal yoki maksimal qiymatini topish uchun.

Kriptanaliz:

Grover algoritmi kriptografik kalitlarga qo‘pol-kuch hujumlari uchun qidiruv maydonini qisqartiradi:

Simmetrik kriptografiya: 2^{128} o‘rniga 2^{64} bosqichda 128 bitli shifrlashni buzadi.

Ochiq kalitli kriptografiyaga mos emas (masalan, RSA).

Boshqa muammolar:

NP-complete muammolarini hal qilish uchun.

1.4. Kriptografik algoritmlar ortiq xavfsiz emasmi?

Kriptografik algoritmlar kvant kompyuterlari tufayli tabiatan xavfsiz emas, lekin, kvant hisoblash kriptografik tizimlarning ayrim turlari uchun jiddiy qiyinchiliklar tug‘diradi. Bular quyidagilar:

1. Simmetrik kalitli kriptografiya (masalan, AES, SHA-2)

Ta’sir: Kvant kompyuterlari qo‘pol kuch hujumlarini tezlashtirish uchun Grover algoritmidan foydalanishi mumkin, bu esa kalit hajmining xavfsizlik darajasini samarali ravishda ikki baravar kamaytiradi. Masalan,

AES-128 kvant raqibiga qarshi 64 bitli kalitga teng xavfsizlikka ega bo‘ladi.

AES-256 128 bitli kalitga teng xavfsizlikka ega bo‘lib, u xavfsiz bo‘lib qoladi.

Qarshi choralar: Kalit hajmini oshirish (masalan, AES-256 yoki undan yuqori) kvant tahdidlarini yumshata oladi.

2. Ochiq kalitli kriptografiya (masalan, RSA, ECC, DH)

Ta’sir: Shor algoritmida ishlaydigan kvant kompyuterlari ushbu tizimlar asosida yotgan matematik muammolarni (butun sonlarni faktorizatsiya, diskret logarifmlar va elliptik egri diskret logarifmlar) samarali hal qila oladi.

RSA va ECC kvant hujumlaridan butunlay xavfsiz bo‘lmaydi.

Qarshi choralar: kvantga chidamli algoritmlarga (post-kvant kriptografiyasi) o‘tish zarur.

3. Yengil vanzli kriptografiya

PRESENT va SPECK kabi yengil algoritmlar odatda simmetrikdir. Ularning kalit o‘lchamlari Grover algoritmiga qarshi turish uchun sozlashni talab qilishi mumkin, ammo ochiq kalitli tizimlarga qaraganda kamroq ta’sir qiladi.

4. Kvant kompyuterlari qachon xavf tug‘diradi?

Hozirgi kvant kompyuterlari hali keng tarqalgan kriptografik algoritmlarni buzish uchun yetarli darajada kuchli emas. RSA yoki ECC kabi algoritmlarni buzish uchun yetarli kubitlar va xatolarni tuzatishga ega kvant kompyuterining rivojlanishi 10-30 yil davom etadi (ko‘plab mutaxassislarning fikriga ko‘ra). Biroq, hozir tayyorgarlik zarur, chunki:

“Harvest Now, Decrypt Later”: Dushmanlar kvant kompyuterlari mavjud bo‘lganda shifrlangan ma’lumotlarni ochish niyatida hozir saqlashlari mumkin.

O‘tish vaqti: Global tizimlar uchun post-kvant kriptografiyaga o‘tish yillar davom etadi.

5. Hozirgi kriptografiyadan voz kechishimiz kerakmi?

Darhol emas. Mavjud kriptografik algoritmlar klassik hujumlarga qarshi xavfsiz bo‘lib qolmoqda va bugungi kunda ko‘pgina ilovalar uchun etarli. Biroq:

Kvant hisoblashga chidamli tizimlarga o‘tish rejalarini ishlab chiqish kerak.

Yuqori xavfsizlik talab etuvchi sohalar (masalan, mudofaa, moliya) klassik va post-kvant algoritmlarini birlashtirgan holda gibrid kriptografiya bilan tajriba o‘tkazishni boshlashi mumkin.

Kvant kompyuterlari ma’lum kriptografik algoritmlarga tahdid solsada, xavf darhol yuzaga kelmaydi. Post kvant kriptografiya va proaktiv rejalashtirishni qo‘llash orqali tizimlarni hozirgi va kelajakdagi tahdidlardan himoya qilish mumkin.

Nazorat savollari:

1. Kvant nazariyasining ba’zi asosiy tushunchalarini tushuntiring?
2. Geyzenbergning noaniqlik printsipini tushuntiring?
3. Kvant nazariyasining qo‘llanilishi va ahamiyati haqida ayting?
4. Kvant kompyuterlari klassik kompyuterlardan qanday farq qiladi?
5. Kvant kompyuterlarining turlarini ayting?
6. Kvant kompyuterlarining ilovalari haqida ayting?
7. Kvantli Furye almashtirishini tushuntiring?
8. Qidirish algoritmlari: Shor va Grover algoritmini tushuntiring?
9. Kriptografik algoritmlar ortiq xavfsiz emasmi?
10. Hozirgi kriptografiyadan voz kechishimiz kerakmi?

Adabiyotlar va Internet resurslar:

1. Richter M. et al. A mathematical perspective on post-quantum cryptography //Mathematics. – 2022. – T. 10. – №. 15. – C. 2579.
2. https://en.wikipedia.org/wiki/Quantum_computing - Quantum computing
3. https://www.ibm.com/topics/quantum-computing - What is quantum computing?
4. https://www.techtarget.com/searchdatacenter/feature/Explore-the-impact-of-quantum-computing-on-cryptography#:~:text=Quantum%20attacks%20may%20pose%20a,calculations%20that%20can%20decrypt%20them. - Explore the impact of quantum computing on cryptography

2-ma’ruza. POST KVANT KRIPTOGRAFIYASI ALGORITMLARI (2 соат)

Reja:

2.1. Panjaraga asoslangan ochiq kalitli kriptografiya: panjara asosi, xatolik bilan o‘rganishga asoslangan kriptografiya, NTRUga asoslangan kriptografiya.
2.2. Kodga asoslangan kriptografiya: chiziqli kodlar.
2.3. Ko‘p o‘zgaruvchili kriptografiya: Ko‘p o‘zgaruvchili polinom funksiyalar, MQ muammosi, IP muammosi.

Tayanch iboralar: *panjara, xatolik bilan o‘rganish, eng qisqa vektor muammosi, eng yaqin vektor muammosi, qaror qabul qilishli (Decisional) LWE, Ring-LWE va Module-LWE, NTRU farazi, kodga asoslangan kriptografiya, chiziqli kodlar, Binar Goppa kodlari, ko‘p o‘zgaruvchili polinomlar, MQ muammosi.*

2.1. Panjaraga asoslangan ochiq kalitli kriptografiya: panjara asosi, xatolik bilan o‘rganishga asoslangan kriptografiya, NTRUga asoslangan kriptografiya.

Panjara asosi

Ta’rif 1. Faraz qilinsin b_1, b_2,…, b_n lar n o‘lchamli Evklid maydoni $\mathbb{E}^n$ dagi chiziqli mustaqil vektorlar. U holda $\Lambda = \{z_1b_1 + z_2b_2 + \cdots + z_nb_n : z_i \in \mathbb{Z}\}$ ifoda n o‘lchamli panjara deb ataladi va $\{b_1,\ b_2,\ldots,\ b_n\}$ lar Λ panjaraning asoslari (bazis) deb ataladi.

Agar $b_i = (b_{i1}, b_{i2}, \ldots, b_{in})$ 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 yozilish mumkin: $\Lambda = \{\mathrm{zB} : \mathrm{z} \in \mathbb{Z}^n\}$.

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.

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 $\mathbb{Z}$ va $\mathbb{Z}^n$ butun sonlar tizimlarini umumlashtiradi va geometriyada $\mathbb{E}^n$ 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 kriptografiyaga eshik ochgan 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 kriptografiyasida qisqa va deyarli ortogonal vektorlardan tashkil topgan bazis yaxshi bazis deb ataladi. Yaxshi bazisga ega bo‘lgan holda, ba‘zi qattiq panjara muammolarini samarali hal qilish mumkin. Shu sababli, odatda panjarali kriptotizimning maxfiy kaliti sifatida yaxshi bazis tanlanadi va mos keladigan ochiq kalit sifatida yomon bazis (tasodifiy bazis) olinadi.

Panjara nuqtalarini hisoblash.

1. Bazis vektorlarni taqdim etish. Bazis vektorlarni n o‘lchamli fazoda yozish. Masalan, 2D uchun: $b_1 = (x_1, y_1)$, $b_2 = (x_2, y_2)$, 3D uchun: $b_1 = (x_1, y_1, z_1)$, $b_2 = (x_2, y_2, z_2)$, $b_3 = (x_3, y_3, z_3)$.

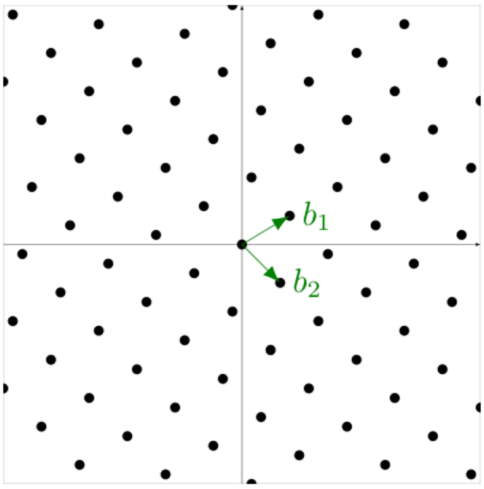
2. Bazis vektorlarning butun ko‘paytmasini qo‘shish bilan panjara nuqtalarini hosil qilish. p nuqta uchun ifoda quyidagicha: $\Lambda = z_1b_1 + z_2b_2 + \cdots + z_nb_n$ va bu yerda $z_i \in \mathbb{Z}$.

3. 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, $\Lambda = z_1b_1 + z_2b_2 = z_1(2,1) + z_2(1,3) = (2z_1 + z_2, z_1 + 3z_2)$ 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 2.1-rasmda tegishli bazis vektorlarga ega panjara ko‘rinishi berilgan. Panjara Λ ni ustun vektorlar sifatida bazis vektorlardan iborat B matritsa orqali hosil qilish mumkin.

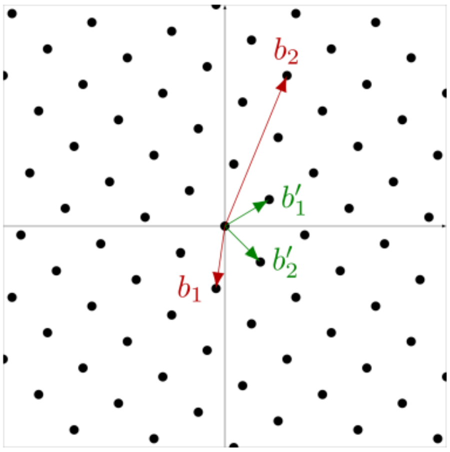


2.1-rasm. 2 o‘lchamli panjaraga misol

Ta’rif 2 (panjara, rang, o‘lcham, to‘liq-rangli panjara). Faraz qilinsin $\{b_1, b_2, \dots, b_m\}$ -$\mathbb{E}^n$ ning chiziqli mustaqil vektorlari to‘plami bo‘lsin. Faraz qilinsin B kattalik $n \times m$ matritsa bo‘lib, ustun vektorlari $b_1, b_2, \dots, b_m$ dan iborat. U holda $\Lambda(\mathrm{B}) = \{\mathrm{Bx}\ |\mathrm{x} \in \mathbb{Z}^m\}$ ga B tomonidan hosil qilingan $\mathbb{E}^n$ 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 $\mathbb{Z}^2$ ga teng, ya’ni barcha butun nuqtalar to‘plamiga. Shuningdek, $\mathbb{Z}^2$ quyidagi vektorlar orqali ham generatsiya qilinishi mumkin: $\binom{2}{1}, \binom{1}{1}$.

2.2-rasmda ham ushbu fakt ko‘rsatilgan. Boshqa tomondan, $\mathbb{Z}^n$ dagi n chiziqli mustaqil vektorlar $\mathbb{Z}^n$ning bazislari bo‘lishi shart emas. Misol sifatida ko‘rish mumkinki, yuqoridagi vektorlarni o‘zgartirish natijasidagi $\binom{2}{0}$, $\binom{1}{1}$ vektorlar $\mathbb{Z}^2$ ning bazislari emas. Ya’ni, ushbu vektorlar orqali 2 o‘lchamli maydondagi barcha nuqtalarni hosil qilib bo‘lmaydi.



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

Hisoblanarli panjara muammolari

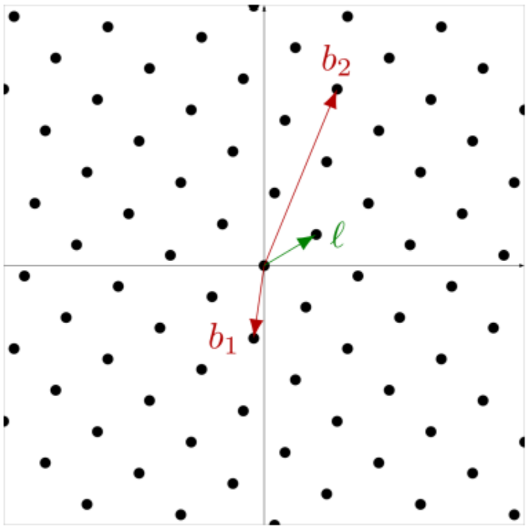
Panjaralarning o‘ziga xos tuzilishi ularga maxsus matematik xususiyatlarga ega bo‘lish imkonini beradi. Quyidagi hisob-kitoblarni chiziqli algebra algoritmlari yordamida samarali baholash mumkin:

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

Boshqa hisoblanarli panjara muammolari odatda qiyin bo‘lib ko‘rinadi, hattoki Shor algoritmiga ham chidamli bo‘lishi mumkin. Shuning uchun ular post-kvant-kriptografiyada foydalanish uchun qiziqarli matematik muammolarga nomzodlardir. Ushbu muammolar quyida keltiriladi.

Eng qisqa vektor muammosi (Shortest Vector Problem, SVP)

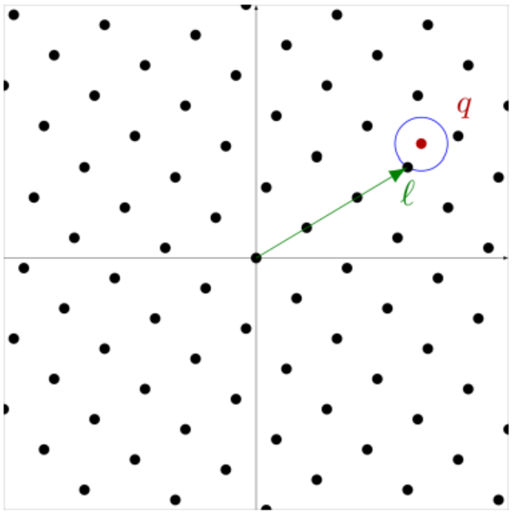
Faraz qilinsin Λ panjara bazis bazislar $B \in \mathbb{E}^{n\times m}$ va $||\cdot||$ bazi norm (matematik funksiya, masalan, maydonda magnituda yoki uzunlikni aniqlash uchun ishlatiladi) ga ega bo‘lsin. Faraz qilinsin $\lambda(\Lambda)$ qiymat Λ dagi nolga teng bo‘lmagan eng qisqa vektorning uzunligi 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. 2.3-rasmda panjaradagi eng qisqa vektor tasvirlangan.



2.3-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 qilinsin Λ panjara bazis bazislar $B \in \mathbb{E}^{n\times m}$ va $\|\cdot\|$ bazi normga ega bo‘lsin. Berilgan $q \in \mathbb{E}^n$ nuqta uchun $\|l - q\|$ qiymat eng minimal bo‘lishini ta’minlovchi $l \in L$ ni topish vazifasi *eng yaqin vektor muammosi* deb ataladi. 2.4-rasmda panjaradagi eng yaqin vektor tasvirlangan.



2.4-rasm. q nuqtaga eng yaqin bo‘lgan l vektorga ega ikki o‘lchamli panjara

Xatolik bilan o‘rganishga asoslangan kriptografiya (Learning with Errors, LWE)

LWE asoslari

Xatolik bilan o‘rganish, LWE

Faraz qilinsin $\mathbb{Z}_q$ (yoki $\mathbb{Z}/q\mathbb{Z}$ shaklida ham yoziladi) modul q bo‘yicha butun sonlar xalqasi bo‘lsin. U holda quyidagi chiziqli tenglamalar tizimni qurish mumkin:

$$A \cdot s = b,$$

bu yerda, $A \in \mathbb{Z}_q^{n\times m}$, $s \in \mathbb{Z}_q^m$ va $b \in \mathbb{Z}_q^n$. Masalan, quyidagi tenglama faraz qilinsin:

$$A = \begin{pmatrix} 10 & 3 & 5 & 1 \\ 4 & 1 & 1 & 2 \\ \vdots & \vdots & \vdots & \vdots \\ 3 & 1 & 1 & 5 \end{pmatrix}, b = \begin{pmatrix} 10 \\ 3 \\ \vdots \\ 8 \end{pmatrix}.$$

U holda, mos tenglamalar quyidagicha bo‘ladi:

$$\begin{gathered} 10 \cdot s_1 + 3 \cdot s_2 + 5 \cdot s_3 + 1 \cdot s_4 = 10 \\ 4 \cdot s_1 + 1 \cdot s_2 + 1 \cdot s_3 + 2 \cdot s_4 = 3 \\ \vdots \\ 3 \cdot s_1 + 1 \cdot s_2 + 1 \cdot s_3 + 5 \cdot s_4 = 8 \end{gathered}$$

Ushbu tenglamalar sistemasini Gaus algoritmi yordamida samarali yechish mumkin. Biroq, tenglamalar tizimiga hattoki kichik xatolik qiymati $e \in \mathbb{Z}_q^n$ ni qo‘shish $A \cdot s + e = b$ ga olib keladi. Bu yerda, tenglamalar sistemasini yechish va s yechim vektorini olish hayratlanarli darajada qiyin bo‘ladi. Bu haqiqat yuqorida tavsiflangan qattiq (hisoblanarli murakkab) panjara muammolari bilan bog‘liq bo‘lib, quyida qisqacha tavsiflanadi.

Qaror qabul qilishli (Decisional) LWE (dLWE)

LWE muammosi, odatda, dLWE deb ataladigan qaror qabul qilish muammosi sifatida ham ataladi. Yuqorida ta’riflangan LWE namunasini (A, b) hisobga olgan holda (s va e maxfiy saqlanadi), qo‘yilgan vazifa b ning qiymatlari kichik e xatolik qiymatlari bilan $A \cdot s + e$ tenglik bilan hisoblanganmi yoki b ning qiymatlari A dan mustaqil ravishda tasodifiy tanlanganligini taxmin qilishdan iborat. Ikkala variant ham bir xil darajada murakkab. LWEdan dLWE ga qisqarish Regev ([3], Lemma 4.2) tomonidan isbotlangan, dLWE dan LWE ga teskari qisqarish ahamiyatsiz.

LWE muammosi qidirish muammosi hisoblansa, dLWE esa qaror qabul qilish muammosi hisoblanadi.

LWE muammosini hisoblanarli panjara muammosiga bog‘lash

Faraz qilinsin LWE muammosi $A \cdot s + e = b$ shaklda berilgan. Bu yerda, $A \in \mathbb{Z}_q^{n \times m}$ va $b \in \mathbb{Z}_q^n$ va kichik vektorlar $s \in \mathbb{Z}_q^m$, $e \in \mathbb{Z}_q^n$.

Eng yaqin vektor muammosini hal qilish orqali aniq LWE masalasini hal qilish juda oddiy. E’tibor bering, b ga eng yaqin vektor deyarli har doim e masofadagi panjara vektori $A \cdot s$ bo‘ladi.

Xatolar bilan o‘rganish va eng qisqa vektor muammosi o‘rtasidagi bog‘liqlikni ko‘rish uchun quyidagi panjara ko‘rib chiqiladi:

$$\Lambda = \{\mathrm{x} \in \mathbb{Z}^{m+n+1} | (\mathrm{A} \| I_n \| (-\mathrm{b})) \cdot \mathrm{x} = 0 \bmod \mathrm{q}\},$$

Bu yerda, $'||'$ amali konketenatsiyani (birlashtirish) va I_n esa $n \times n$ birlik matritsani bildiradi. Quyidagi tenglik o‘rinli ekanligidan ustun vektori $(s, e, 1)$ ni Λ ning elementi ekanligini kuzatish mumkin:

$$(A \quad I_n \quad -b) \cdot \begin{pmatrix} s \\ e \\ 1 \end{pmatrix} = A \cdot s + e - b = b - b = 0 \; mod \; q$$

Bu vektor $(s, e, 1)$ aslida Λ dagi eng qisqa vektor ekanligini va shuning uchun Λ uchun SVP yechim ekanligini ko‘rsatish mumkin. Vektor $(s, e, 1)$ni olish to‘g‘ridan-to‘g‘ri s maxfiy kattalikni, shuningdek, xatolik vektori e ni ham beradi va shuning uchun LWE muammosini hal qiladi.

LWEga sodda misol

Parametrlar quyidagicha sozlangan bo‘lsin:

- Modul $q = 7$ (barcha hisoblashlar $modq$ asosida);
- O‘lcham $n = 2$ (ochiq va maxfiy vektorlar o‘lchami);
- Maxfiy vektor $s = (3,4) \in \mathbb{Z}_q^2$;
- Kichik xatolik e (tasodifiy tanlanadi).

Hosil qilish kerak:

1. Ochiq vektor $a \in \mathbb{Z}_q^n$
2. Shovqinli chiqish b, quyidagicha hisoblanadi: $b = \langle a, s\rangle + e \; mod \; q$

Misol:

1. Ochiq vektor a quyidagicha generatsiyalangan bo‘lsin: $a = (2,5) \in \mathbb{Z}_q^2$.
2. $\langle a, s\rangle$ skalyar ko‘paytma quyidagicha hisoblanadi:
   a. $\langle a, s\rangle = 2 * 3 + 5 * 4 = 6 + 20 = 26.$
3. Xatolik qiymati e ni qo‘shish.
   a. Faraz qilinsin, $e = 2$, xatolik qiymat skalyar ko‘paytmaga qo‘shiladi: $\langle a, s\rangle + e = 26 + 2 = 28$
4. $mod \; q$ bo‘yicha qisqartiriladi:
   a. $b = 28mod7 = 0$;

Shuning uchun, ushbu LWE holati uchun tenglik quyidagiga teng:

$$\langle a, s\rangle + e = b \Rightarrow \langle (2,5), (3,4)\rangle + 2 = 0mod7$$

Chiqish qiymatlari:

- Ochiq ma’lumot: $a = (2,5)$, $b = 0$.
- Maxfiy $s = (3,4)$;
- Kichik xatolik $e = 2$.

LWEga asoslangan shifrlash sxemalari

Ushbu bo‘lim LWEga asoslangan shifrlash sxemalarini tushuntirish uchun foydali dastlabki ma’lumotlarni taqdim etadi. Quyidagi soddalashtirilgan misol faqat bir bitdan iborat bo‘lgan xabarni uzatish uchun ishlatiladi. Biroq, uni istalgan uzunlikdagi bit qatorini uzatish uchun osonlik bilan kengaytirish mumkin.

Faraz qilinsin, LWE na’munasi $A \cdot s + e = b$ ko‘rinishida berilgan bo‘lsin, bu yerda, $A \in \mathbb{Z}_q^{n\times m}$ – tekis taqsimotli tasodifiy tanlanadi va $s \in \mathbb{Z}_q^m$ va $e \in \mathbb{Z}_q^n$ lar esa xatolik taqsimotidan tanlanadi, ya’ni, ularning qiymatlari juda kichik. Faraz qilinsin, A va b qiymatlari ochiq, mos keladigan s va e qiymatlari esa sir saqlanadi. Bu yerda, LWE muammosi s yoki e ni hisoblash qiyinligini bildiradi.

Haqiqatda, shifrlash sxemasini qurish uchun tasodifiy qiymatlar $r \in \mathbb{Z}_q^n$, shuningdek, xatoliklar $e_1 \in \mathbb{Z}_q^m$ va $e_2 \in \mathbb{Z}_q$ tanlanadi. Bular yordamida tenglamalar sistemasi quyidagicha quriladi:

$$u = A^T \cdot r + e_1 \in \mathbb{Z}_q^m$$

$$v = b^T \cdot r + e_2 \in \mathbb{Z}_q.$$

Ularni ekvivalent bo‘lgan quyidagicha ixcham ko‘rinishda ifodalash mumkin:

$$\binom{u}{v} = \binom{A^T}{b^T} r + \binom{e_1}{e_2}$$

Bu LWE muammosining yana bir misoli ekanligini ko‘rish oson. (A, b, u, v) ni bilish bilan boshqa qiymatlarni hisoblash qiyin. Bundan tashqari, qaror qabul qilishga asoslangan LWE muammosi shuni ko‘rsatadiki, yuqorida tavsiflangan usulda hisoblangan u, v qiymatlari va u, v' qiymatlarini ba’zi bir ixtiyoriy v' qiymati bilan farqlash hatto qiyin. Bu keltiriladigan shifrlash tizimining asosiy qismidir.

Hozircha, (u, v) qabul qiluvchiga (s bilgan) qaytariladi deb faraz qilib, $s^T \cdot u = s^T \cdot (A^T \cdot r + e_1)$ qiymati hisoblanadi. Xatolik qiymatlarini juda kichikligini inobatga olgan holda $s^T \cdot u \approx s^T \cdot A^T \cdot r$ ni va shuningdek, $v = b^T \cdot r + e_2 \approx b^T \cdot r \approx (A \cdot s)^T \cdot r = s^T \cdot A^T \cdot r$ kuzatish mumkin. Xatolik qiymatlarini e’tiborga olmagan holda, $s^T \cdot u \approx v$ ni topish mumkin.

Bu shuni anglatadiki, *taxminan* bir xil qiymatni ikki xil usulda bilvosita uzatish yo‘li topildi va bu uchinchi shaxsga sezdirmasdan qilindi: s ni bilmasdan, bu qiymatlar bir-biriga qanchalik yaqin ekanligini aniqlab bo‘lmaydi (dLWE faraz qilinadi).

Mazkur holatda ma’lumotni yashirish usuli bu qiymatlardan birida xabarni yashirishdir. Agar xabar 0 bo‘lsa, shunchaki $v' = v$ uzatiladi. Bundan tashqari, agar xabar 1 ga teng bo‘lsa, $v' = v + q/2$ (amallar $\mathbb{Z}_q$ maydonda bajariladi va shuning uchun bu 0 ga qo‘shish amali uchun teskari) uzatiladi. Qabul qiluvchi quyidagini hisoblaydi: $\mu = v' - s^T \cdot u$. Agar μ ning qiymati nolga ($mod\ q$) yaqin bo‘lsa, xabar 0 ga teng, agar $q/2$ ga teng bo‘lsa, xabar 1 ga teng.

Quyida ushbu jarayon yanada rasmiy holda ifodalanadi. Faraz qilinsin $round_n(\cdot)$ belgilanish n ning eng yaqin karralisigacha yaxlitlashni anglatsin, ya’ni, $round_n(x) = n \cdot round\left(\frac{x}{n}\right)$. Bir bit xabarni $\mu \in \{0, \lfloor q/2 \rfloor\}$ kabi shifrlash uchun, shifrmatn (u, v') juftligi quyidagiga teng:

$$u = A^T \cdot r + e_1$$
$$v' = b^T \cdot r + e_2 + \mu.$$

Qabul qiluvchi quyidagini hisoblaydi:

$round_{\lfloor q/2 \rfloor}(v' - s^T \cdot u) = round_{\lfloor q/2 \rfloor}(b^T \cdot r + e_2 + \mu - s^T(A^T \cdot r + e_1)) = round_{\lfloor q/2 \rfloor}((As + e)^T r + e_2 + \mu - s^T A^T \cdot r - s^T e_1)) = round_{\lfloor q/2 \rfloor}((As)^T r + e^T r + e_2 + \mu - (As)^T r - s^T e_1) = round_{\lfloor q/2 \rfloor}(\mu + e^T r + e_2 - s^T e_1) = \mu.$

Oxirgi tenglik to‘g‘ri bo‘lishi uchun (va shunday qilib, deshifrlash muvaffaqiyatli bo‘lishi uchun) $q/4$ dan past bo‘lishi uchun xatolikning umumiy ta’siri $(e^T r + e_2 - s^T e_1)$ ga teng bo‘lishi kerak. Amaliyotda barcha nomzod sxemalar oqilona shifrlangan matn o‘lchamlariga ega bo‘lish uchun har doim ham bunday bo‘lmaydigan xatolik taqsimoti va modul q dan foydalanadi. Barcha holatlarda muvaffaqiyatsizlik ehtimoli juda kichik, shuning uchun amaliyotda odatda ahamiyatsiz hisoblanadi. Biroq, hujumchilar maxfiy kalit haqida ma’lumot olish uchun maxsus ishlab chiqilgan shifrlangan matnlarni yaratib, deshifrlash xatoliklarini keltirib chiqarishdan ehtiyot bo‘lish kerak.

LWE variantlari: Ring-LWE va Module-LWE

Yuqorida tasvirlangan sodda kriptotizimni, xuddi shu protokolni l marta parallel ravishda ishlatish orqali, belgilangan uzunlikdagi l bitlar qatorini shifrlash uchun osonlik bilan kengaytirish mumkin. Quyida keltirilgan turli usullardan farqli o‘laroq, bu yondashuv Oddiy LWE (Plain LWE) deb ataladi (shuni ta’kidlash kerakki, $\mathbb{Z}_q$ halqa bo‘lsa ham, *Ring-LWE* termini boshqa yondashuvga tegishli, quyida keltiriladi). Oddiy LWE’dan foydalanadigan amalda foydalanishga tayyor sxema bu Frodo [1]. Uning oddiyligi tufayli u hujumlar uchun eng kam ehtimollikka ega deb hisoblanadi. Biroq, bu Ring-LWE yoki Module-LWE bilan solishtirganda 15 baravar yuqori aloqa xarajatlari evaziga amalga oshiriladi. Frodo’ning ochiq kaliti va shifrlangan matn hajmini Kyber va Saber’ning mos hajmlari bilan solishtirish ushbu faktni ko‘rsatadi. Nisbatan past samaradorligi tufayli u NIST standarti bo‘yicha finalistlar qatoriga kiritilmagan (lekin, muqobil nomzod sifatida kiritilgan). LWE ning boshqa turlari asosiy algebraik tuzilmani o‘zgartirish orqali yaratilishi mumkin. Turli xil yondashuvlar mavjud va o‘rganilgan bo‘lib, quyida tegishli turlarni batafsil bayon qilinadi.

Ring-LWE birinchi marta 2010-yilda Vadim Lyubashevskiy, Kris Peykert va Oded Regev tomonidan taklif qilingan [2]. Hisob-kitoblar $R_q = \mathbb{Z}_q[x]/f(x)$ polinom halqasida amalga oshiriladi, bu yerda $f(x)$ biror polinom. Shuning uchun, matritsalar ustida ko‘paytirish o‘rniga polinomlarni ko‘paytirish ishlatiladi.

Module-LWE esa Ring-LWE’ni yanada takomillashtirgan variant bo‘lib, u 2012-yilda Adeline Langlois va Damien Stehlé tomonidan taklif qilingan [3]. U yuqorida keltirilgan sodda tizim bilan bir xil tuzilishga ega, lekin skalyarlar avvalgi paragrafda aniqlangan R_q halqasi elementlari bilan almashtiriladi. Natijada, vektorlar halqalar ustida vektor fazolarining umumlashmasi bo‘lgan modullar deb ataladigan elementlarga aylanadi va shuning uchun ushbu nom berilgan (2.1-jadvalga qarang.

LWE asosidagi kriptografiyaning dastlabki amaliy joriy etilishlarining ko‘pchiligi, masalan, NewHope sxemasi [4], Ring-LWE’dan foydalangan. Ammo, Ring-LWE ko‘proq hujum yuzasini taqdim etishi mumkinligini ko‘rsatdi, ya’ni Ring-LWE sxemasi bir xil parametrli Module-LWE sxemasidan ko‘pi bilan bir xil darajada xavfsiz bo‘lishi mumkin [5]. Shu sababli, NIST uchinchi bosqichda Ring-LWE sxemalarini ko‘rib chiqmaslikka qaror qilgan.

2.1-jadval

LWE variantlarida foydalanilgan algebraik tuzilmalarning qiyosiy tahlili

	Oddiy LWE	**Ring-LWE**	**Module-LWE**
$\boldsymbol{A}$	$\mathbb{Z}_q^{n\times m}$	$\mathbb{Z}_q[x]/f$	$(\mathbb{Z}_q[x]/f)^{n\times m}$
$\cdot$	Matrix mult.	Polinom mult.	Matrix mult.
$\boldsymbol{s}$	$\mathbb{Z}_q^m$	$\mathbb{Z}_q[x]/f$	$(\mathbb{Z}_q[x]/f)^m$
$\boldsymbol{b}, \boldsymbol{e}$	$\mathbb{Z}_q^n$	$\mathbb{Z}_q[x]/f$	$(\mathbb{Z}_q[x]/f)^n$

Yaxlitlash bilan o‘rganish (Learning with Rounding, LWR)

Yaxlitlash bilan o‘rganish, LWR muammosi LWE muammosining varianti hisoblanadi. $As + e = b$ LWE muammosining yagona chizig‘i qaralsin. Bu yerda,

$A \in \mathbb{Z}_q^{n\times m}$ tekis taqsimotli tasodify tanlanadi va $s \in \mathbb{Z}_q^m$ va $e \in \mathbb{Z}_q^n$ lar esa xatolik taqsimotidan tanlanadi, ya’ni:

$$(As)_k + e_k = (a_{k1} \cdot s_1 + \cdots + a_{km} \cdot s_m) + e_k = b_k.$$

Tasodifiy kichik xatolik e_k ni tanlash va qo‘shish o‘rniga, shovqin oddiy yaxlitlash orqali tenglamaga qo‘shiladi. Bunda, $p < q$ bo‘lgan ba’zi bir p uchun $\mathbb{Z}_q$ ni taxminan teng o‘lchamdagi p intervalga bo‘lib $\mathbb{Z}_q$ ning elementini tegishli intervalning indeksiga o‘tkazadigan $\lfloor\cdot\rceil_p: \mathbb{Z}_q \to \mathbb{Z}_p$ yaxlitlash funksiyasini aniqlashni anglatadi. Masalan, agar p va q ikkalasi ham 2 ning darajalari bo‘lsa, yaxlitlash elementni uning $log_2(p)$ ta eng katta ahamiyatga ega bitlariga akslantirishgacha soddalashtiriladi.

Ushbu yaxlitlash funksiyasini $\mathbb{Z}_q^n$ vektorlari uchun komponentlar bo‘yicha yaxlitlash orqali kengaytirish mumkin, ya’ni har bir $(As)_k$ ni alohida yaxlitlash amalga oshiriladi. G‘ayritabiiy tarzda, garchi LWR dagi shovqin deterministik tarzda hisoblanayotgan bo‘lsa ham, uni hisoblash LWE ni yechish kabi murakkab, ya’ni A va $\lfloor A \cdot s\rceil_p$ dan s ni hosil qilish qiyin [6]. LWE holatida bo‘lgani kabi, LWR ning ham turli xil variantlari asosiy tuzilmani almashtirish orqali yaratilishi mumkin. Masalan, *Saber* sxemasi Module-LWR dan foydalanadi.

Yaxlitlash bilan o‘rganishga misol:

Faraz qilinsin, $q = 16$, $p = 4$ va $s = (3{,}2)$, $a = (5{,}7)$.

$\langle a, s\rangle$ ni hisoblash:

$\langle a, s\rangle = 5 * 3 + 7 * 2 = 29$;

Yaxlitlashni amalga oshirish:

$\langle a, s\rangle$ ni p ga bo‘lish: $\frac{29}{4} = 7.25$;

Yaqin butun songa yaxlitlash: $\lfloor 7.25\rceil = 7$;

Qayta ko‘paytirish: $7 * 4 = 28$ ($p = 4$ ni eng yaqin karralisi)

$q = 16$ modul bo‘yicha qisqartirish:

$b = 28 mod 16 = 12$.

Shuni uchun, b=12 chiqishida yaxlitlash orqali deterministik ravishda kiritilgan shovqin bor.

NTRUga asoslangan kriptografiya

NTRU asoslari

NTRU farazi

NTRU — bu panjaraga asoslangan kriptotizim bo‘lib, 1996-yilda Hoffstein, Pipher va Silverman tomonidan ishlab chiqilgan. U ikki yaxshi ma’lum sxema, ya’ni *NTRUEncrypt* va *NTRUSign*dan kelib chiqqan. “NTRU” qisqartmasi uchun bir nechta tushuntirishlar mavjud, masalan: “**n**-th degree **tru**ncated polynomial ring” yoki “**n**umber **t**heorists **r** **u**s”. Birinchisi, NTRU operatsiyalari qisqartirilgan (truncated) ko‘phadlar halqasi $\mathcal{R}_q = \mathbb{Z}_q[X]/(X^n + 1)$ da amalga oshishini anglatadi, bu yerda, n va q ikkita musbat, eng katta bo‘luvchisi 1 bo‘lgan butun sonlardir va $\mathbb{Z}_q = \mathbb{Z}_q/q\mathbb{Z}_q$ esa q modulidagi butun sonlar halqasini bildiradi. Shunday qilib, $\mathcal{R}_q$ bu darajasi n dan kichik bo‘lgan va koeffitsiyentlari $\mathbb{Z}_q$ bo‘lgan barcha ko‘phadlar halqasidir.

RSA ga o‘xshab, ya’ni RSA ni buzish butun sonni faktorlashtirish murakkabligi bilan teng ekanini isbotlash mumkin bo‘lmagan bo‘lsada, NTRU ning xavfsizligi faqat murakkablik *farazi*ga asoslanadi. Agar $\overset{\mathcal{R}}{\equiv}$ belgilanishi $\mathcal{R}$ halqasidagi kongurentlikni bildirsa, “NTRU farazi” deb ataladigan narsa quyidagi vazifani yechish murakkab ekanligini aytadi:

$f \cdot h \overset{\mathcal{R}_q}{\equiv} g$ kongurentlikdan $h \in \mathcal{R}_q$ berilganda uchlik ko‘phadlar ($\mathbb{Z}_3$ da koeffitsientlarga ega uchlik ko‘phad) $f, g \in \mathbb{Z}_3[X]/(X^n - 1)$ni topish.

Keyinchalik, ushbu holat eng qisqa vektor muammosi sifatida hal qilish mumkinligi ko‘rib o‘tiladi.

NTRUga asoslangan shifrlash sxemalari

Ushbu bo‘limda NTRU kriptotizimlarini yaratishda foydalaniladigan asosiy nazariyaga umumiy tavsif beriladi. NTRU faraziga asoslangan kriptotizimni qurish uchun ikkita tub son n va p, shuningdek, q deb ataluvchi ularga o‘zaro tub bo‘lgan butun son kerak bo‘ladi. Bundan tashqari, p kattalik q dan sezilarli darajada kichikroq bo‘lishi kerak; mazkur holatda har doim $p = 3$ bo‘ladi. Ushbu sonlar amallar bajariluvchi $\mathcal{R}_q = \mathbb{Z}_q[X]/(X^n - 1)$, $\mathcal{R}_p = \mathbb{Z}_p[X]/(X^n - 1) = \mathcal{R}_3 = \mathbb{Z}_3[X]/(X^n - 1)$ halqalarni aniqlaydi.

Birinchi qadamda, $f, g \in \mathcal{R}_3$ ikki uchlik ko‘phad olinadi, bu yerda f ko‘phad $\mathcal{R}_3$ va $\mathcal{R}_q$ maydonda invertiga ega bo‘lishi kerak. Shundan so‘ng, ushbu inverslar hisoblanadi: $f_q \coloneqq f^{-1} \in \mathcal{R}_q$, $f_3 \coloneqq f^{-1} \in \mathcal{R}_3$.

f_q esa ochiq kalitni hisoblash uchun ishlatiladi: $h \overset{\mathcal{R}_q}{\equiv} f_q \cdot g$, shaxsiy kalit sifatida esa f va f_3 xizmat qiladi. Shundan so‘ng ochiq kalitdan maxfiy kalitni chiqarib olish NTRU farazi yechimini berishini tushunish oson.

$m \in \mathcal{R}_3$ xabarni shifrlash uchun, tasodifiy uchlik ko‘phad $r \in \mathcal{R}_3$ kerak bo‘ladi. Shundan so‘ng shifrmatnni quyidagicha hisoblash mumkin:

$$c \overset{\mathcal{R}_q}{\equiv} p \cdot r \cdot h + m = 3 \cdot r \cdot h + m$$

r shifrlash jarayonining deterministik bo‘lmasligini ta’minlaydi, 3 ga ko‘paytirish esa, quyida ko‘rib o‘tiladigan, to‘g‘ri deshifrlashni amalga oshirishga imkon beradi.

Deshifrlash jarayoni ikki bosqichdan iborat. Dastlab, quyidagi hisoblanadi:

$$a = f \cdot c = f \cdot (3 \cdot r \cdot h + m) = f \cdot f_q \cdot 3 \cdot r \cdot g + f \cdot m \overset{\mathcal{R}_q}{\equiv} 3 \cdot r \cdot g + f \cdot m$$

Ikkinchi qadam $\mathcal{R}_3$ halqasida hisoblanadi, bu esa a ning birinchi hadining yo‘qolishini ta’minlaydi. Keyin f_3 ga ko‘paytirish asl xabar m ni olishga olib keladi:

$$f_3 \cdot a = f_3 \cdot (3 \cdot r \cdot g + f \cdot m) \overset{\mathcal{R}_q}{\equiv} m$$

Diqqat bilan qaralganda, nega $p \ll q$ sharti majburiy ekanligini ko‘rish mumkin, va haqiqatda, bu dastlabki holda aniq emas. Muammo $\mathcal{R}_q$ va $\mathcal{R}_p$ o‘rtasidagi o‘tishda paydo bo‘ladi. Deshifrlash jarayonining to‘g‘ri bo‘lishi uchun $a = p \cdot r \cdot g + f \cdot m$ tenglik nafaqat $\mathcal{R}_q$halqasida, balki $\mathbb{Z}[X]$ da ham bajarilishi juda muhim. Aniqlik uchun, agar $p \cdot r \cdot g + f \cdot m$ ning koeffitsiyentlari $modq$ ga nisbatan qisqartirilgan bo‘lsa, p ga nisbatan qisqartirish m ni bermaydi.

Xulosa qilib aytganda, deshifrlash to‘g‘ri bajarilishi uchun bu hisoblash n dan kichik darajaga va q dan kichik koeffitsiyentlarga ega bo‘lgan ko‘phadni keltirishi kerak. Chunki, $r, g, f, m \in \mathcal{R}_q$ kichik koeffitsiyentlarga ega, $p \ll q$ bo‘lishi yetarli.

Yana bir kuzatiladigan fakt shundaki, deshifrlash jarayoni m xabarni f ni bilmasdan olish imkonini ham beradi. Darhaqiqat (NTRU faraziga ko‘ra), hujumchining har qanday uchlik ko‘phad $\hat{f}$ ni topishi kifoya, shunda $\hat{f} \cdot h$ qiymat $mod\ q$ modul bo‘yicha yana uchlik ko‘phadga aylanadi, chunki bu hali ham $\hat{f} \cdot c$ qiymat $mod\ q$ ga nisbatan qisqarib ketmasligini va keyingi $mod\ p$ ga qisqartirish m ni berishini ta’minlaydi. Mualliflar [7]da ko‘rsatganidek, ushbu xususiyatga ega yagona ko‘phadlar, ehtimol, f ning aylanishlari (ya’ni, f ning koeffitsiyentlarini siklik ravishda aylantirish orqali olingan ko‘phadlar) bo‘ladi.

NTRU va hisoblashli panjara muammolarini bog‘lash

NTRU va halqalar o‘rtasidagi bog‘lanishni tushunish uchun, quyidagi NTRU taxminiga asoslangan har bir mumkin bo‘lgan yechimdan iborat bo‘lgan halqa, $h \in \mathcal{R}_q$ berilgan holda, quyidagi ko‘rinishda bo‘ladigan, panjara ko‘rib chiqiladi:

$$\mathcal{L} = \{(u, v) \in \mathcal{R}_q \times \mathcal{R}_q \mid u \cdot h \overset{\mathcal{R}_q}{\equiv} v\}.$$

Quyida, barcha hisoblashlar $(X^n - 1)$ ga nisbatan qisqartirilgan bo‘lib, shuning uchun $u \cdot h = v\ mod\ q$ deb yozish mumkin. $\mathcal{L}$ ning bir bazisini topish uchun, har bir $(u, v) \in \mathcal{L}$ ba’zi $k \in \mathcal{R}_q$ lar uchun quyidagicha bajarilishi kerakligi kuzatiladi:

$$u \cdot h - k \cdot q = v$$

Bu tenglik ekvivalent bo‘lgan quyidagi tenglik ko‘rinishida qayta yozilishi mumkin:

$$\binom{u}{v} = \begin{pmatrix} 1 & 0 \\ h & q \end{pmatrix} \cdot \binom{u}{-k}.$$

$u = \sum_{i=0}^{n-1} u_i x^i$, $\quad v = \sum_{i=0}^{n-1} v_i x^i$, $\quad h = \sum_{i=0}^{n-1} h_i x^i$ va $k = \sum_{i=0}^{n-1} k_i x^i$ koeffitsientlardan foydalangan holda, ushbu tenglik quyidagicha o‘zgartirilishi mumkin:

$$\begin{pmatrix} u_0 \\ u_1 \\ \vdots \\ u_{n-1} \\ \hline v_0 \\ v_1 \\ \vdots \\ v_{n-1} \end{pmatrix} = \left(\begin{array}{cccc|cccc} 1 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & 0 & \cdots & 0 \\ \hline h_0 & h_1 & \cdots & h_{n-1} & q & 0 & \cdots & 0 \\ h_{n-1} & h_0 & \cdots & h_{n-2} & 0 & q & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ h_1 & h_2 & \cdots & h_0 & 0 & 0 & \cdots & q \end{array}\right) \cdot \begin{pmatrix} u_0 \\ u_1 \\ \vdots \\ u_{n-1} \\ \hline -k_0 \\ -k_1 \\ \vdots \\ -k_{n-1} \end{pmatrix}$$

Pastki-chap kvadratni M_h ni sifatida belgilab, quyidagi matritsani panjara $\mathcal{L}$ ning bazislarini aniqlashni osonlikcha ko‘rish mumkin:

$$\begin{pmatrix} I_n & 0_n \\ M_h & q \cdot I_n \end{pmatrix}$$

Ko‘rinib turibdiki, $(f,g) \in \mathcal{L}$ va $f,g \in R_3$ bo‘lganligi sababli, bu ham nisbatan qisqa vektor. Shuningdek, ehtimoliy ravishda (f,g) haqiqatan ham $\mathcal{L}$ ning eng qisqa vektori ekanligini ko‘rish mumkin. Shunday qilib, SVP ni hal qilish, har qanday NTRU kriptotizimi uchun maxfiy kalitni topish imkonini beradi.

2.2. Kodga asoslangan kriptografiya: chiziqli kodlar.

Xatolarni tuzatuvchi kodlar — bu uzatish davomida shovqin tufayli yuzaga kelishi mumkin bo‘lgan aloqa xatolarini aniqlash va tuzatish uchun standart yondashuvdir. Ushbu texnika kriptografik tizimlarni yaratishda ham qo‘llanilishi mumkin, bunda xatolar ataylab kiritiladi va faqat mo‘ljallangan qabul qiluvchi tomonidan tuzatilishi mumkin.

Chiziqli kodlar

Ta’rif 3 (Hemming og‘irligi, hemming masofasi). Berilgan $x = (x_1, \cdots, x_n) \in \mathbb{F}_2^n$ vektor uchun x ning *hemming og‘irligi* deb $weight(x) = \sum_{i=1}^{n} x_i$ tenglik bilan hisoblanuvchi kattalikka aytiladi. Shuni ta’kidlash kerakki, bu oddiygina qiymati 1 ga teng bo‘lgan elementlarning sonini hisoblaydi.

Berilgan boshqa $y = (y_1, \cdots, y_n) \in \mathbb{F}_2^n$ uchun *hemming masofasi* deb $dist(x,y) = \sum_{i=1}^{n} |x_i - y_i|$ tenglik bilan hisoblanuvchi kattalikka aytiladi va bu x va y o‘rtasida farq qiluvchi bitlar sonini bildiradi.

Ta’rif 4 (chiziqli kod). Keling, C ni $\mathbb{F}_2^n$ vektor fazosining k o‘lchamli chiziqli qism fazosi (subspace) deb belgilaylik. Bundan tashqari, C ning ikki farqli elementi orasidagi minimum farq $d = \min\limits_{\substack{c_i, c_j \in C \\ c_i \neq c_j}} dist(c_i, c_j)$ ga teng bo‘lsin.

C – *chiziqli kod* deb ataladi yoki ekvivalent ravishda $(n,k,d) - kod$ deb ataladi. C ning elementlari *kod so‘zlar* deb ataladi.

(n,k,d)-kod C ning elementlari uzunligi n bo‘lgan ikkilik (binary) vektorlardir. Ammo, C chiziqli qism fazo sifatida k o‘lchamli bo‘lgani sababli, faqat k ta bitni ixtiyoriy tanlash mumkin, qolgan $n-k$ bitlar esa tanlangan bitlardan kelib chiqib aniqlanadi.Bu shuni anglatadiki, kodning har bir elementi uzunligi n bo‘lgan vektordir, lekin ularda faqat k ta bit o‘zgaruvchan (axborot tashuvchi) bo‘lib, qolgan $n-k$ bitlar qo‘shimcha (ortiqcha, nazorat) ma’lumot sifatida ishlaydi. Shuning uchun C ni k ta chiziqli mustaqil kodli so‘z $c_1, \cdots, c_k \in C$ larning chiziqli kombinatsiyasi sifatida ko‘rsatish mumkin, ya’ni $C = \{G \cdot x | x \in \mathbb{F}_2^k\}$, bu yerda, $G \in \mathbb{F}_2^{n\times k}$ da $c_1, \cdots, c_k$ kod so‘zlar ustun sifatida joylashgan. G - Cning *generator matritsasi* deb ataladi. G ni standart ko‘rinishga o‘tkazish mumkin (bu ta’rif standart adabiyotlardan biroz farq qilsada, Classic McEliece algoritmida ancha foydaliroq). Standart ko‘rinishdagi generator matritsa quyidagicha bo‘ladi: $G' = (T^\intercal \parallel I_k)^\intercal$, bu yerda, I_k - $k \times k$ o‘lchamli birlik matritsa va $T \in \mathbb{F}_2^{(n-k)\times k}$.

Agar generator matritsa $G' = (T^\intercal \parallel I_k)^\intercal$ standart ko‘rinishda berilgan bo‘lsa, $c \in \mathbb{F}_2^n$ so‘zining kod so‘zi ekanligini, ya’ni C ga tegishli ekanligini tekshirishning qulay usuli mavjud. Faraz qilinsin, $H = (I_{n-k} \parallel -T) \in \mathbb{F}_2^{(n-k)\times k}$ va $c \in \mathbb{F}_2^n$ joiz kod so‘z, ya’ni, ba’zi $x \in \mathbb{F}_2^k$ uchun $c = G \cdot x$ bo‘lsin. U holda quyidagi tenglik ixtiyoriy c kod so‘z uchun $\mathbb{F}_2^{n-k}$ da nol vektorga teng:

$$H \cdot c = H \cdot (G' \cdot x) = (H \cdot G') \cdot x =$$

$$\underbrace{\begin{pmatrix} 1 & 0 & \cdots & 0 & -t_{1,1} & -t_{1,2} & \cdots & -t_{1,k} \\ 0 & 1 & \cdots & 0 & -t_{2,1} & -t_{2,2} & \cdots & -t_{2,k} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & -t_{n-k,1} & -t_{n-k,2} & \cdots & -t_{n-k,k} \end{pmatrix} \cdot \underbrace{\begin{pmatrix} t_{1,1} & t_{1,2} & \cdots & t_{1,k} \\ t_{2,1} & t_{2,2} & \cdots & t_{2,k} \\ \vdots & \vdots & \ddots & \vdots \\ t_{n-k,1} & t_{n-k,2} & \cdots & t_{n-k,k} \\ \hline 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}}_{k} \cdot x}_{(n-k)+k}$$

$$= \begin{pmatrix} t_{1,1} - t_{1,1} & t_{1,2} - t_{1,2} & \cdots & t_{1,k} - t_{1,k} \\ t_{2,1} - t_{2,1} & t_{2,2} - t_{2,2} & \cdots & t_{2,k} - t_{2,k} \\ \vdots & \vdots & \ddots & \vdots \\ t_{n-k,1} - t_{n-k,1} & t_{n-k,2} - t_{n-k,2} & \cdots & t_{n-k,k} - t_{n-k,k} \end{pmatrix} \cdot x = 0 \in \mathbb{F}_2^{n-k}$$

Ushbu xususiyat tufayli H matritsasi *tenglikni nazoratlash matritsa* (parity check matrix, PCM)si deb ataladi. Darhaqiqat, $H \cdot c = 0$ sharti faqat va faqat c joiz kod so‘z bo‘lsa bajariladi.

Shunday qilib, chiziqli kod C ni tenglikni nazoratlash matritsasi H orqali ham ifodalash mumkin, chunki C aynan H aksining yadrosi (kernel) hisoblanadi. Ya’ni, $C = \{x \in \mathbb{F}_2^n | H \cdot x = 0\}$. Bu shuningdek quyidagi ta’rifni kiritishga asos yaratadi:

Ta’rif 5 (sindrom). Faraz qilinsin C tenglikni tekshirish matritsasi H bo‘lgan chiziqli kod bo‘lsin va $x \in \mathbb{F}_2^n$ vektor bo‘lsin. U holda, $H \cdot x \in \mathbb{F}_2^{n-k}$ ifoda x ning sindromi deyiladi.

Binar Goppa kodlari

An’anaviy va yaxshi o‘rganilgan chiziqli kodlar oilasidan biri ikkilik Goppa kodlaridir [8]. Ular 1978-yilda kriptografiya uchun tavsiya qilingan, chunki ularning xavfsizlik xususiyatlari kuchli va dekodlash tezligi yuqori [9]. Goppa kodlari xatolarni tuzatuvchi kuchli imkoniyatlarga ega bo‘lib, ayniqsa kodga asoslangan kriptografik tizimlar, masalan, McEliece shifrlash sxemasi kabi post-kvant kriptografiyada keng qo‘llaniladi. Shu bilan birga, ularning matematik tuzilishi kriptotahlil qilishni qiyinlashtiradi, bu esa ularni xavfsiz yechimga aylantiradi.

Ta’rif 6 (binar Goppa kod, tayanch (support), Goppa ko‘phadi). Faraz qilinsin ba’zi $m \in \mathbb{N}$ uchun $\mathbb{F}_{2^m}$ chekli maydon va $g(x) \in \mathbb{F}_{2^m}[x]$ esa $t < 2^m$ darajali keltirilmas ko‘phad. Farz qilinsin $L = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ esa $g(x)$ ning o‘zaglari (roots) bo‘lmagan $\mathbb{F}_{2^m}$ ning n turli elementlar ketma-ketligi. U holda, binar Goppa kodi $\Gamma(g, L)$ quyidagicha aniqlanadi:

$$\Gamma(g, L) = \{c \in \mathbb{F}_2^n | \textstyle\sum_{i=1}^{n} \frac{1}{x-\alpha_i} \cdot c_i \equiv 0 \; mod \; g(x)\}.$$

Bu yerda, *L tayanch* va $g(x)$ *Goppa ko‘phadi* deb ataladi.

Ikkilik Goppa kodlarining matematik tuzilishiga chuqur to‘xtalmasa ham, shuni ta’kidlash muhimki, ma’lum bir Goppa kod uning Goppa polinomi va tayanch (support) elementlariga bog‘liq. Berilgan $\Gamma(g, L)$ Goppa kodi uchun PCMni hosil qilishda quyidagini aniqlanadi: $\hat{I}_i(x, \alpha_i) \coloneqq \frac{1}{x-\alpha_i} \; mod \; g(x)$ va bu $i \in \{1, \dots, n\}$ uchun $x - \alpha_i$ ni qisqartirilgan $mod \; g(x)$ bo‘yicha teskari qiymatini bildiradi. Shuni ta'kidlash kerakki, $\alpha_1, \alpha_2, \cdots, \alpha_n$ elementlar g ning o'zagi bo'lmasligi shart. Chunki, agar $x-\alpha_i$ qiymat $g(x)$ ni bo'lsa, $x-\alpha_i$ ning teskari elementi mavjud bo'lmadi, ushbu shart tufayli $\frac{1}{x-\alpha_1}, \cdots, \frac{1}{x-\alpha_n}$ lar mavjud bo'ladi. Bu shart Goppa kodining matematik tuzilishida muhim rol o'ynaydi va uning PCMni hosil qilish uchun muhim hisoblanadi.

Chunki $\hat{I}_i(x,\alpha_i)$ allaqachon $mod\ g(x)$ bo'yicha qisqartirilgan va bir xil darajali polinomlarni qo'shish ularning darajasini oshira olmaydi, bundan $\Gamma(g,L)$ ning aniqlovchi shartini quyidagicha qayta yozish mumkin:

$$\sum_{i=1}^{n} \hat{I}_i(x,\alpha_i) \cdot c_i = 0.$$

Bundan tashqari, $\hat{I}_i(x,\alpha_i)$ - maksimum darajali $(t-1)$ bo'lgan ko'phad, ya'ni, $\hat{I}_i(x,\alpha_i) = \sum_{k=1}^{t} \hat{I}_{i,k}(\alpha_i) \cdot x^{k-1}$. Shunga qaramay, ushbu shartni quyidagicha yozish mumkin: $\sum_{i=1}^{n} c_i \sum_{k=1}^{t} \hat{I}_{i,k}(\alpha_i) \cdot x^{k-1} = 0$.

Ushbu tenglikdan, $\Gamma(g,L)$ uchun $\widehat{H}$ PCMni osonlik bilan chiqarish mumkin:

$$\widehat{H} = \begin{pmatrix} \hat{I}_{1,1}(\alpha_i) & \hat{I}_{2,1}(\alpha_i) & \cdots & \hat{I}_{n,1}(\alpha_i) \\ \hat{I}_{1,2}(\alpha_i) & \hat{I}_{2,3}(\alpha_i) & \cdots & \hat{I}_{n,2}(\alpha_i) \\ \vdots & \vdots & \ddots & \vdots \\ \hat{I}_{1,t}(\alpha_i) & \hat{I}_{2,t}(\alpha_i) & \cdots & \hat{I}_{n,t}(\alpha_i) \end{pmatrix} \in \mathbb{F}_{2^m}^{t\times n} \qquad (3)$$

$\widehat{H}$ dagi teskari elementlar hosil qilish uchun n marta kengaytirilgan Evklid algoritmini (Extended euclidean algorithm, EEA) qo'llash mumkin. EEAni to'g'ridan-to'g'ri har qanday $x-\alpha_i$ va $g(x) = \sum_{i=0}^{t} g_i \cdot x^i$ polinomiga qo'llash orqali $\widehat{H}$ ning soddalashtirilgan versiyasini hosil qilish mumkin:

$$\widehat{H} = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ g_{t-1} & 1 & 0 & \cdots & 0 \\ g_{t-2} & g_{t-1} & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ g_1 & g_2 & g_3 & \cdots & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1^1 & \alpha_2^1 & \cdots & \alpha_n^1 \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_1^{t-1} & \alpha_2^{t-1} & \cdots & \alpha_n^{t-1} \end{pmatrix} \begin{pmatrix} \frac{1}{g(\alpha_1)} & 0 & \cdots & 0 \\ 0 & \frac{1}{g(\alpha_2)} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \frac{1}{g(\alpha_n)} \end{pmatrix} \in \mathbb{F}_{2^m}^{t\times n}$$

Batafsil tafsilotlarni [10]-manbadan topish mumkin.

Classic McEliece algoritmida doimo $\widehat{H} \in \mathbb{F}_{2^m}^{t\times n}$ PCMning binar versiyasi ko'rib chiqiladi. Bu degani, $\mathbb{F}_{2^m}$ dagi barcha elementlar o'zining uzunligi m bo'lgan ikkilik ko'rinishdagi ustun vektorga aylantiriladi. Natijaviy matritsa $H \in \mathbb{F}_{2^m}^{mt\times n}$ *binar PCM* deb ataladi.

Teorema 1. Faraz qilinsin $\Gamma(g,L)$ - (n,k,d) binar Goppa kodi bo'lsin, bu yerda $g \in \mathbb{F}_{2^m}[x]$ kattalik t darajaga ega. U holda, kodning o'lchami, k, ni quyi chegarasini quyidagicha ifodalanadi: $k \geq n - mt$ va minimum masofa d quyidagiga teng: $d \geq 2t+1$.

Chunki H matritsa o'lchami $mt \times n$ ga, unga mos keluvchi generator matritsa G o'lchami $n \times k$ ga teng, bu yerda, $k \geq n - mt$. Minimal masofa uchun quyi chegarani hosil qilish jarayoni haqida batafsil ma'lumotni [11]-manbadan topish mumkin. Minimal masofaning pastki chegarasi kodning xatolarni tuzatish qobiliyatini aniqlashda muhim rol o'ynaydi va kodning ishlash samaradorligini baholashda hal qiluvchi ahamiyatga ega.

Chiziqli kodlarga oid hisoblash muammolari

Panjaralarga o‘xshash tarzda, kodlashga asoslangan turli hisoblash muammolari mavjud bo‘lib, ular hisoblash jihatidan murakkab hisoblanadi va shu sababli kriptografik algoritmlar uchun mos keladi.

Berilgan chiziqli (n, k, d) kod $C \subseteq \mathbb{F}_2^n$, tasodifiy PCM matritsa $H \in \mathbb{F}_2^{(n-k)\times n}$ va $q \in \mathbb{F}_2^n$, eng yaqin kod so‘zi $c \in C$ ni topish vazifasi, ya’ni, q va c orasidagi masofani minimallashtiruvchi kod so‘zini topish, hisoblash jihatidan murakkab bo‘lib, *sindromni dekodlash muammosi* deb ataladi.

Ammo, Goppa kodining tuzilmali PCMga ega ekanligini hisobga olib, sindromni dekodlash muammosining murakkabligi Goppa kodlariga bevosita tatbiq etilmaydi. Biroq, tadqiqotlar shuni ko‘rsatadiki, Goppa PCMni tasodifiy kodning PCMdan ajratish murakkab hisoblanadi. Tenglama (3) da keltirilgan $\widehat{H}$ PCM bu haqiqatni tasavvur qilishga yordam beradi. Har bir element tasodifiy Goppa tayanchi va tasodifiy Goppa ko‘phadiga bog‘liq bo‘lgan ko‘phadning teskari elementidir. Ushbu Goppa kodlarini ajratib bo‘lmasligi haqidagi faraz Classic McEliece kriptosistemasining asosi hisoblanadi, bu keyingi bo‘limda muhokama qilinadi.

2.3. Ko‘p o‘zgaruvchili kriptografiya: Ko‘p o‘zgaruvchili polinom funksiyalar, MQ muammosi, IP muammosi.

Ko‘p o‘zgaruvchili kriptografiya kalit juftliklarini yaratish uchun ko‘p o‘zgaruvchili polinomlardan, ya’ni, bir nechta o‘zgaruvchilarga ega polinomlardan foydalanadi. Uning xavfsizligi cheklangan maydon ustida ko‘p o‘zgaruvchili kvadratik tenglamalar sistemasini yechish hisoblash jihatdan murakkab ekanligiga asoslangan.

Ko‘p o‘zgaruvchili polinomlarning asoslari

Ko‘p o‘zgaruvchili polinom funksiyalar

Ta’rif 7 (Ko‘p o‘zgaruvchili kvadratik polinom funksiya). $\mathbb{F}$ maydon bo‘lsin. $f: \mathbb{F}^n \to \mathbb{F}$ funksiyasi ko‘p o‘zgaruvchili funksiya deb ataladi. $x_1, \dots, x_n \in \mathbb{F}$ o‘zgaruvchilarga ega p polinom berilgan bo‘lsin. Agar f funksiyani $p(x_1, \dots, x_n)$ ko‘rinishida ifodalash mumkin bo‘lsa, u ko‘p o‘zgaruvchili polinom funksiya deb ataladi (agar F cheklangan bo‘lsa, bu har qanday funksiya uchun mumkin). Agar f faqatgina ikkinchi darajali yoki undan past bo‘lgan hadlarni o‘z ichiga olsa, u *ko‘p o‘zgaruvchili kvadratik polinom funksiya (Multivariate quadratic (MQ) polynomial function)* deb ataladi.

Misol uchun, funksiya $f_1(x_1, x_2, x_3) = x_1^2 x_2 + 2x_1 x_2^2 + 3x_3 + 4$ ko‘p o‘zgaruvchili polinom funksiya (uchinchi darajali), ammo, $f_2(x_1, x_2, x_3) = x_1^2 + 2x_1 x_2 + 3x_3 + 4$ ko‘p o‘zgaruvchili kvadratik polinom funksiya hisoblanadi. $p_1, \dots, p_k$ ko‘p o‘zgaruvchili kvadratik polinom funksiyalar bo‘lsin. $\mathcal{P} = \begin{pmatrix} p_1 \\ \vdots \\ p_k \end{pmatrix}$ vektor har bir komponent uchun qo‘llanilgan funksiyalar yig‘indisi orqali $P: \mathbb{F}^n \to \mathbb{F}^k$ funksiyasi sifatida talqin qilinishi mumkin va u *polinom akslantirish* deb ataladi.

MQ muammosi

$\mathbb{F}$ cheklangan maydon bo‘lsin. $p_1, \dots, p_k: \mathbb{F}^n \to \mathbb{F}$ ko‘p o‘zgaruvchili kvadratik polinom funksiyalar bo‘lsin. Quyidagi tenglamalar tizimi uchun $s \in \mathbb{F}^n$ yechimni topish, MQ (multivariate quadratic) muammosi deb ataladi [12]:

$$p_1(s) = 0$$
$$\vdots$$
$$p_k(s) = 0$$

Ushbu muammo hisoblash jihatidan qiyin ekanligi isbotlangan.

Ko‘p o‘zgaruvchili imzo sxemalari

Ko‘p o‘zgaruvchili ochiq kalitli kriptosistemalar (Multivariate public-key cryptosystems, MPKC) polinomial akslantirishlardan ochiq va shaxsiy kalitlarni ifodalash uchun foydalaniladigan konstruksiyalardir. Ammo, MPKC konstruksiyalari asosan raqamli imzo sxemalari sifatida qo‘llaniladi va shifrlash maqsadlari uchun mos emas [13].

$\mathbb{F}$ cheklangan maydon bo‘lsin. Berilgan xabar $m \in \mathbb{F}^k$ uchun imzo $s \in \mathbb{F}^n$ yaratishning asosiy g‘oyasi P polinomial akslantirishi ostida m obraziga (image) bir yoki bir nechta asl obrazni (pre image) hisoblashdir. Bu quyidagi keltirilgan tenglamalar tizimini echimi s ni topishga teng:

$$\begin{matrix} p_1(s) = m_1 & & p_1(s) - m_1 = 0 \\ \vdots & \Leftrightarrow & \vdots \\ p_k(s) = m_k & & p_k(s) - m_k = 0 \end{matrix}$$

Bu yerda, $\mathcal{P} = (p_1, \dots, p_k)$ va $m = (m_1, \dots, m_k)$. $\mathcal{P}$ – akslantirish deb ataldi va ochiq kalitni taqdim etadi. MPKC sxemasini ochiq akslantirish ostida asl obrazlarni topishga imkon beradigan tarzda loyihalash mumkin, lekin MQ muammosini to‘g‘ridan-to‘g‘ri hal qilmasdan. Odatda, bu mexanizm $\mathcal{F}: \mathbb{F}^n \to \mathbb{F}^k$ polinomial akslantirishini o‘z ichiga oladi, u markaziy akslantirish deb ataladi. $\mathcal{F}$ akslantirishni quyidagi ikki affin akslantirishlarni qo‘llash orqali yashirish mumkin: $\mathcal{S}: \mathbb{F}^n \to \mathbb{F}^n$ va $\mathcal{T}: \mathbb{F}^k \to \mathbb{F}^k$. Hosil bo‘lgan funksiya $\mathcal{P} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{S}: \mathbb{F}^n \to \mathbb{F}^k$ tegishli shaxsiy kalit $(\mathcal{T}, \mathcal{F}, \mathcal{S})$ uchun ochiq kalit sifatida xizmat qiladi. Odatda, markaziy akslantirish F asl obrazlarni samarali hisoblash imkoniyatini talab qiladi. Affin akslantirishlar $\mathcal{S}$ va $\mathcal{T}$ teskarilanuvchi (invertible) bo‘lishi kerak; shuning uchun ular to‘liq rangga ega bo‘lishi talab etiladi.

MPKC ning asosiy komponenti markaziy akslantirish $\mathcal{F}$ ni loyihalashdir. Shaxsiy kalit $(\mathcal{T}, \mathcal{F}, \mathcal{S})$ haqida oldindan ma’lumotga ega bo‘lmasdan, hujumchi ochiq akslantirishni tasodifiy polinomial akslantirishdan farqlay olmaydi. Shu sababli, to‘g‘ridan-to‘g‘ri hujumning murakkabligi MQ muammosining qiyinligiga tenglashtiriladi. Biroq, ushbu tizimning xavfsizlik farazi markaziy akslantirish $\mathcal{F}$ ga qarshi samarali hujumlar ehtimoli tufayli MQ muammosiga qaraganda kuchliroqdir.

Ochiq akslantirishga to‘g‘ridan-to‘g‘ri hujum qilish o‘rniga, MPKCni buzishning muqobil usuli mavjud. G‘oya shundan iboratki, markaziy akslantirish $\mathcal{F}$ F ni $\mathcal{P}$ ga o‘zgartirish uchun zarur bo‘lgan ikkita muqobil affin akslantirishlarini topish kerak. Shunday qilib, kriptotizimga mos keluvchi ochiq akslantirish uchun boshqa shaxsy kalitlarni topish orqali hujum amalga oshirilishi mumkin. Bu mazmunda yangi muammo — polinomlar izomorfizmi (Isomorphism of Polynomials, IP) muammosini aniqlashtirish kerak [12].

IP muammosi

Agar $\mathcal{P}, \mathcal{F}$ - $\mathbb{F}^n$ dan $\mathbb{F}^k$ ga bo‘lgan ikkita polinomial akslantirish bo‘lsa va $\mathcal{P} = (p_1, \dots, p_k)$, $\mathcal{F} = (f_1, \dots, f_k)$ deb yozilsa, shunday shartlarda agar $\mathcal{P} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{S}$ shartni qanoatlantiruvchi ikki teskarisiga ega affin akslantirishlar $\mathcal{S}: \mathbb{F}^n \to \mathbb{F}^n$ va $\mathcal{T}: \mathbb{F}^k \to \mathbb{F}^k$ mavjud bo‘lsa, $\mathcal{S}$ va $\mathcal{T}$ ni topish IP muammosi deb atalib, u yetarlicha hisoblash murakkabligiga ega hisoblanadi [14]. IP muammosini yechish MPKCni buzishi mumkin, chunki bu usul orqali maxfiy affini funksiyalarni topish mumkin. Bu esa berilgan ochiq akslantirish va tasodifiy tanlangan markaziy akslantirishga alternativ maxfiy kalitlar topilishiga olib keladi.

Nazariy savollari:

1. Panjaraga asoslangan kriptografiyada mavjud muammolarni ayting?
2. Xatolik bilan o‘rganishga asoslangan kriptografiyada mavjud muammolatni tushuntiring?
3. LWE variantlari: Ring-LWE va Module-LWElarni tushuntiring?
4. NTRU farazini tushuntiring?
5. NTRU va hisoblashli panjara muammolari qanday bog‘langan?
6. Kodga asoslangan kriptografiya: chiziqli kodlarlar haqida ayting?
7. Binar Goppa kodlari haqida tushuntiring?
8. Ko‘p o‘zgaruvchili polinomlarning asoslari va ularda mavjud muammolar?
9. MQ va IP muammolarini tushuntiring?
10. Xeshlashga asoslangan kriptografiyaning mohiyatini tushuntiring?

Adabiyotlar va Internet resurslar:

1. Bos, J.; Costello, C.; Ducas, L.; Mironov, I.; Naehrig, M.; Nikolaenko, V.; Raghunathan, A.; Stebila, D. Frodo: Take off the Ring! Practical, Quantum-Secure Key Exchange from LWE. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 1006–1018. [CrossRef]

2. Lyubashevsky, V.; Peikert, C.; Regev, O. On Ideal Lattices and Learning with Errors over Rings. In Advances in Cryptology—EUROCRYPT 2010, Proceedings of the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Riviera, French, 30 May–3 June 2010; Gilbert, H., Ed.; Springer: Berlin/Heidelberg, Germany, 2010; pp. 1–23.

3. Langlois, A.; Stehle, D. Worst-Case to Average-Case Reductions for Module Lattices. Cryptology ePrint Archive, Report 2012/090. 2012. Available online: https://ia.cr/2012/090 (accessed on 1 July 2022).

4. Alkim, E.; Ducas, L.; Pöppelmann, T.; Schwabe, P. Post-Quantum Key Exchange—A New Hope. Cryptology ePrint Archive, Report 2015/1092. 2015. Available online: https://ia.cr/2015/1092 (accessed on 1 July 2022).

5. Peikert, C.; Pepin, Z. Algebraically Structured LWE, Revisited. Cryptology ePrint Archive, Report 2019/878. 2019. Available online: https://ia.cr/2019/878 (accessed on 1 July 2022).

6. Banerjee, A.; Peikert, C.; Rosen, A. Pseudorandom Functions and Lattices. Cryptology ePrint Archive, Report 2011/401. 2011. Available online: https://ia.cr/2011/401 (accessed on 1 July 2022).

7. Hoffstein, J.; Pipher, J.; Silverman, J. An Introduction to Mathematical Cryptography, 1st ed.; Springer Publishing Company, Incorporated: New York, NY, USA, 2008.

8. Lint, J.H.V. Introduction to Coding Theory, 3rd ed.; Number 86 in Graduate Texts in Mathematics; Springer: Berlin/Heidelberg, Germany, 1999.

9. McEliece, R.J. A Public-Key Cryptosystem Based on Algebraic Coding Theory; National Aeronautics and Space Administration: Washington, DC, USA, 1978.

10. Marcus, M. White Paper on McEliece with Binary Goppa Codes. 2019. Available online: https://www.hyperelliptic.org/tanja/students/m_marcus/whitepaper.pdf (accessed on 1 July 2022).

11. Engelbert, D.; Overbeck, R.; Schmidt, A. A Summary of McEliece-Type Cryptosystems and their Security. 2006. Available online:https://ia.cr/2006/162 (accessed on 1 July 2022).

12. Ding, J.; Yang, B.Y. Multivariate Public Key Cryptography. In Post-Quantum Cryptography; Springer: Berlin/Heidelberg, Germany,2009; pp. 193–241._6. [CrossRef]

13. Tao, C.; Diene, A.; Tang, S.; Ding, J. Simple Matrix Scheme for Encryption. In Post-Quantum Cryptography; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2013; pp. 231–242. [CrossRef]

14. Patarin, J. Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms. In Advances in Cryptology—EUROCRYPT'96, Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques, Saragossa, Spain, 12–16 May 1996; Maurer, U., Ed.; Springer: Berlin/Heidelberg, Germany, 1996; pp. 33–48.

3-ma’ruza. POST KVANT KRIPTOGRAFIYASI BO‘YICHA NIST KONKURSI (2 соат)

Reja:

3.1. Talablar, o‘tkazilish bosqichlari.
3.2. Ishtirokchi algoritmlar, tanlab olingan algoritmlar, kelajak rejalar.

Tayanch iboralar: *NIST, Post-Quantum Cryptography, Kyber, FALCON, Dilithium, SPHINCS+.*

3.1. Talablar, o‘tkazilish bosqichlari

Konkursning boshlanishi

NIST (Milliy Standartlar va Texnologiyalar Instituti) 2016-yil dekabr oyida kvant kompyuterlariga qarshi chidamli kriptografik algoritmlarni ishlab chiqish maqsadida Post-kvant kriptografiyasini (Post-Quantum Cryptography, PQC) standartlashtirish loyihasini boshladi. Ushbu tashabbus kelajakda kvant kompyuterlar imkoniyatlari rivojlangan taqdirda ham ma’lumotlarning xavfsizligini ta’minlashni maqsad qilgan.

- **2016-yil aprel:** NIST RSA kabi keng qo‘llaniladigan kriptografik tizimlarning 2030-yilga kelib kvant kompyuterlari tomonidan buzilishi xavfi haqida hisobot e’lon qildi.
- **2016-yil dekabr:** NIST kvantga chidamli yangi algoritmlar uchun takliflar konkursini e’lon qildi. Bu takliflar ochiq kalitli kriptografiya, shu jumladan raqamli imzo va kalit inkapsulyatsiya mexanizmlarini qamrab oldi.

Standartlashtirish jarayoni

NISTning standartlashtirish jarayoni bir necha bosqichda amalga oshirildi:

- **Birinchi bosqich (2017-2019):** 25 mamlakatdan 82 ta taklif qabul qilindi. Shulardan 69 tasi to‘liq va mos deb topilib, dastlabki baholash bosqichiga o‘tdi.
- **Ikkinchi bosqich (2019-2020):** 26 algoritm (ochiq kalitli shifrlash va kalit inkapsulyatsiyasiga oid 17 ta, elektron raqamli imzoga doir 9 ta ta) ikkinchi bosqichda batafsil baholash uchun tanlandi.
- **Uchinchi bosqich (2020-2022):** 7 finalchi, jumladan 3 ta raqamli imzo sxemasi ushbu bosqichga chiqdi. Shuningdek, yana 8 ta algoritm alternativ sifatida tanlandi, shulardan, 3 tasi elektron raqamli imzo algoritmlari.

3.2. Ishtirokchi algoritmlar, tanlab olingan algoritmlar, kelajak rejalar.

2022-yil 5-iyulida o‘tkazilgan 6 yillik tanlovdan so‘ng, o‘zining tanlab olgan 4 ta algoritmini e’lon qildi:

- Ochiq kalitli shifrlash/ kalit inkapsulyatsiyasi: panjaraga asoslangan CRYSTALS-Kyber;

- Elektron raqamli imzo: panjaraga asoslangan CRYSTALS-Dilithium va FALCON, xeshlashga asoslangan SPHINCS+.

- **To‘rtinchi bosqich (2022-hozirgi vaqtga qadar):** 2022-yil 5-iyulda NIST to‘rt algoritmni yakuniy bosqichga tanladi: BIKE, Classic McEliece, HQC va SIKE. Ammo, SIKE algoritmi 2022-yil 5-avgustda buzib tashlandi.

2024-yil 13-avgustda NIST uchta kvantga qarshi kriptografiya standartlarining yakuniy versiyalarini chiqardi:

1. **FIPS 203:** CRYSTALS-Kyber algoritmiga asoslangan umumiy shifrlash standarti (ML-KEM — “Module-Lattice-Based Key-Encapsulation Mechanism” deb qayta nomlangan).
2. **FIPS 204:** CRYSTALS-Dilithium algoritmiga asoslangan raqamli imzo standarti (ML-DSA — “Module-Lattice-Based Digital Signature Algorithm” deb qayta nomlangan).
3. **FIPS 205:** Sphincs+ algoritmiga asoslangan raqamli imzo standarti (SLH-DSA — “Stateless Hash-Based Digital Signature Algorithm” deb qayta nomlangan). Ushbu standart boshqa matematik yondashuvga asoslangan bo‘lib, zaxira usul sifatida belgilangan.

Xuddi shunday, FALCON atrofida qurilgan FIPS 206 standarti loyihasi chiqarilganda, algoritm FN-DSA deb nomlanadi, “FFT (fast-Fourier transform) over NTRU-Lattice-Based Digital Signature Algorithm” uchun qisqartma.

Hozirgi holat va kelajak rejalari

NIST boshqa algoritmlarni baholashni davom ettirmoqda va kelajakda yangi standartlarni chiqarishni rejalashtirgan. Tashkilotlarga kelgusida kvantga asoslangan kiber tahdidlarga qarshi ma’lumotlar tizimlarini himoya qilish uchun ushbu yangi standartlarga o‘tishni boshlash tavsiya qilinadi.

Nazariy savollari:

1. NIST (Milliy Standartlar va Texnologiyalar Instituti) tashkilotini post kvant kriptografiyasi bo‘yicha konkurs o‘tkazishini asosiy sababi?
2. Konkurs nechta bosqichda amalga oshirildi?
3. Konkursda qanday turdagi kriptografik algoritmlar ishtirok etish talabi qo‘yilgan?
4. Konkurs go‘libi sifatida qanday algoritmlar tanlandi?
5. Konkurs go‘liblari bo‘lgan algoritmlar qanday matematik muammoga asoslangan?
6. Konkurs tashkilotchilarining kelajak rejalari haqida ayting?
7. Sphincs+ algoritmi haqida ayting?
8. CRYSTALS-Dilithium algoritmi haqida ayting?
9. CRYSTALS-Kyber algoritmi haqida ayting?
10. FALCON algoritmi haqida ayting?

Adabiyotlar va Internet resurslar:

1. https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization - Post-Quantum Cryptography
2. https://en.wikipedia.org/wiki/Post-quantum_cryptography - post-quantum cryptography

IV BO‘LIM.

AMALIY MASHG‘ULOT MATERIALLARI

IV. AMALIY MASHG‘ULOT MATERIALLARI

1-amaliy ish. AMALIY PKK ALGORITMLARI (4 soat)

Amaliy ishning maqsadi – post kvant kriptografik algoritmlarining ishlash tamoyili haqida nazariy bilimlarni shakllantirishdan iborat.

Nazariy qism

Kyber

Kyber [1] — Module-LWE muammosiga asoslangan CPA (Chosen Plaintext Attack)ga xavfsiz ochiq kalitli shifrlash (PKE) sxemasidan olingan CCA (Chosen Ciphertext Attack)ga xavfsiz kalitni inkapsulyatsiyalash mexanizmi (Key Encapsulation Mechanism, KEM). $n, q \in \mathbb{N}$ uchun asos xalqa $R_q = \mathbb{Z}_q[X]/(X^n + 1)$, ya’ni, koeffitsientlari $\mathbb{Z}_q$ bo‘lgan $n-1$ darajagacha bo‘lgan polinomlar halqasi. Tegishli modul $k \in \mathbb{N}$ rangga ega R_q^k.

Quyidagi asos elementlar talab etiladi: shovqin sohasi B, bu yerda B dan qiymatni tanlab olish $\{-4, \cdots, 4\}$ diapazonda tasodifiy kichik butun qiymatni beradi. Bundan tashqari, KEM qurilishi uchun H_1, H_2 xavfsiz xesh-funksiyalar va xavfsiz kalit hosil qilish funksiyasi KDF talab qilinadi.

Ichki holatda, Kyber tomonidan shifrlangan ochiq matn $r \in R_q$ halqa elementidir. Shunday qilib, $m \in \{0,1\}^{256}$ kirish bit qatori quyidagi tarzda $r = toRing(m)$ halqa elementiga, ya’ni polinomga aylantiriladi:

$$\begin{pmatrix} 0 \\ 0 \\ 1 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \xrightarrow{toRing} \begin{pmatrix} 0 \\ 0 \\ \left\lceil \frac{q}{2} \right\rfloor \\ \vdots \\ 0 \\ \left\lceil \frac{q}{2} \right\rfloor \end{pmatrix} \Leftrightarrow 0 + 0 \cdot x + \frac{q}{2} \cdot x^2 + \cdots + 0 \cdot x^{n-2} + \frac{q}{2} \cdot x^{n-1}$$

Ko‘rinib turibdiki, hatto kichik koeffitsientli vektor qo‘shilgandan keyin ham dastlabki ko‘phadni osongina qayta tiklash mumkin. $fromRing$ dan teskari operatsiya ma’lum bir halqa elementidan bit qatorni koeffitsient bo‘yicha $\frac{q}{2}$ ga bo‘linish va keyingi yaxlitlash orqali qayta tiklaydi. Kyber spetsifikatsiyasi kodlash va siqish funksiyalarini taqdim etadi, biz ularni o‘qish va tushunishni oshirish uchun $toRing$ va $fromRing$ funksiyalariga soddalashtirdik.

Yuqorida tavsiflangan umumiy LWEga asoslangan shifrlash sxemasiga o‘xshash tarzda, Kyber kalitlarini yaratish (1-algoritm) chiziqli tenglamalar tizimi uchun A koeffitsientlarini yaratish va s yechim vektorini, shuningdek, xatolik vektori e ni tanlash orqali ma’lum bir LWE muammosini, $As + e = b$ ni keltirib chiqaradi.

1-algoritm Kyber PKE Key Generation: *keyGen.*
Kirish: Yo‘q 1. $\boldsymbol{A} \in \boldsymbol{\mathcal{R}}_{\boldsymbol{q}}^{\boldsymbol{k \times k}}$ ni hosil qilish. 2. $\boldsymbol{B}$ dan olingan koeffitsientlar bilan $\boldsymbol{s} \in \boldsymbol{\mathcal{R}}_{\boldsymbol{q}}^{\boldsymbol{k}}$ na’munalari.

3. $\boldsymbol{B}$ dan olingan koeffitsientlar bilan $\boldsymbol{e} \in \mathcal{R}_q^k$ na'munalari. 4. $\boldsymbol{b} = \boldsymbol{As} + \boldsymbol{e}$ ni hisoblash. **Chiqish:** ochiq kalit $\boldsymbol{pk} = (\boldsymbol{A}, \boldsymbol{b})$, shaxsiy kalit $\boldsymbol{s}$.

Yechim vektori s shaxsiy kalit vazifasini bajaradi, A va vektor $b = As + e$ ochiq kalit sifatida ishlatiladi. Ochiq kalitdan s ni hisoblash LWE muammosining hal qilish bilan bir xil bo'ladi.

Kyber PKE shifrlash (2-algoritm) yuqorida kiritilgan LWEga asoslangan shifrlash sxemasiga o'xshaydi, faqat Module-LWE muhitiga moslashtirilgan.

2-algoritm Kyber PKE Encryption: *enc*.
Kirish: ochiq kalit $\boldsymbol{pk} = (\boldsymbol{A}, \boldsymbol{b})$, xabar $\boldsymbol{m} \in \{\boldsymbol{0}, \boldsymbol{1}\}^{\boldsymbol{256}}$ 1. $\boldsymbol{B}$ dan olingan koeffitsientlar bilan $\boldsymbol{r} \in \mathcal{R}_q^k$ na'munalari. 2. $\boldsymbol{B}$ dan olingan koeffitsientlar bilan $\boldsymbol{e_1} \in \mathcal{R}_q^k$ na'munalari. 3. $\boldsymbol{B}$ dan olingan koeffitsientlar bilan $\boldsymbol{e_1} \in \mathcal{R}_q^k$ na'munalari. 4. $\boldsymbol{u} = \boldsymbol{A^T r} + \boldsymbol{e_1}$ ni hisoblash. 5. $\boldsymbol{v} = \boldsymbol{b^T r} + \boldsymbol{e_2} + \boldsymbol{toRing}(\boldsymbol{m})$ ni hisoblash. **Chiqish:** shifrmatn $\boldsymbol{c} = (\boldsymbol{u}, \boldsymbol{v})$.

s shaxsiy qiymatni bilgan holda, m xabarni tiklash tegishli Kyber PKE deshifrlash tartibi (3-algoritm) orqali quyidagicha amalga oshiriladi.

3-algoritm Kyber PKE Decryption: *dec*.
Kirish: shaxsiy kalit $\boldsymbol{s}$, shifrmatn $\boldsymbol{c} = (\boldsymbol{u}, \boldsymbol{v})$. 1. $\boldsymbol{m}^* = \boldsymbol{v} - \boldsymbol{s^T u}$ ni hisoblash. **Chiqish:** xabar $\boldsymbol{m} = \boldsymbol{fromRing}(\boldsymbol{m}^*)$.

$fromRing(m^*)$ operatsiyasini qo'llash haqiqiy m ni juda katta ehtimol bilan qayta tiklaydi. Haqiqatan ham, Kyber shifrlash sxemasi namunaviy vektorlar ichidagi shovqin miqdoriga qarab, original xabar m ni juda yuqori ehtimollik bilan qaytaruvchi ehtimolli algoritmdir (aniq muvaffaqqiyatsizlik ehtimoli qiymatlari uchun 2-jadvalga qarang).

Berilgan PKEdan CCA-xavfsiz KEMni qurish uchun Fujisaki-Okamoto transformatsiyasining (FO-transformatsiyasi) varianti qo'llaniladi. Fujisaki va Okamoto [2] assimetrik va simmetrik shifrlash sxemalaridan xavfsiz gibrid shifrlash sxemasiga birinchi umumiy transformatsiyani taqdim etdilar. Keyinchalik, Hofheinz, Xövelmanns va Kiltz [3] Fujisaki va Okamoto ishini kengaytirdilar va PKE sxemasini xavfsiz KEMga aylantirishni o'z ichiga olgan umumiy transformatsiya vositalar to'plamini (toolkit) taqdim etdilar. Algoritm 4 Kyber KEM kalitni hosil qilish tartibini ko'rsatadi.

4-algoritm Kyber KEM Key Generation.
Kirish: Yo'q. 1. $\boldsymbol{\sigma} \in \{\boldsymbol{0}, \boldsymbol{1}\}^{\boldsymbol{256}}$ni generatsiyalash. 2. $(\boldsymbol{pk}, \boldsymbol{s}) = \boldsymbol{PKE.keyGen}()$ ni generatsiyalash. **Chiqish:** ochiq kalit $\boldsymbol{pk}$, shaxsiy kalit $\boldsymbol{sk} = (\boldsymbol{s}, \boldsymbol{\sigma})$.

KEM (5-algorithm) inkapsulyatsiyasida r qiymati asosiy PKE (Ochiq kalitli shifrlash) algoritmida shifrlash jarayonida tasodifiy qiymatlar hosil qilish uchun seed sifatida ishlatiladi. Odatda, deterministik ochiq kalitli shifrlash algoritmi juda ham mashhur bo‘lmasada, KEM uchun qabul qiluvchi shifrlash jarayonini yuboruvchi bilan bir xil tarzda qayta takrorlashi zarur. Berilgan r bilan, shifrlash jarayonining deterministik versiyasi $PKE.enc_r(pk,m)$ bilan belgilanadi. Bundan tashqari, m xabar PKE shifrlash jarayoniga kirishdan oldin xeshlanadi.

5-algoritm Kyber KEM Encapsulation.
Kirish: ochiq kalit $\boldsymbol{pk}$. 1. Xabar $\boldsymbol{m} \in \{\boldsymbol{0},\boldsymbol{1}\}^{\boldsymbol{256}}$ni generatsiyalash. 2. $(\boldsymbol{K'},\boldsymbol{r}) = \boldsymbol{H_1}(\boldsymbol{H_2}(\boldsymbol{m})\|\|\boldsymbol{H_2}(\boldsymbol{pk}))$ ni hisoblash. 3. $\boldsymbol{c} = \boldsymbol{PKE.enc_r}(\boldsymbol{pk},\boldsymbol{H_2}(\boldsymbol{m}))$ ni hisoblash. 4. $\boldsymbol{K} = \boldsymbol{KDF}(\boldsymbol{K'}\|\|\boldsymbol{H_2}(\boldsymbol{c}))$ ni hisoblash. **Chiqish:** inkapsulyatsiya $\boldsymbol{c}$, taqsimlangan kalit $\boldsymbol{K}$.

Dekapsulyatsiya jarayoni (6-algoritm) zarur bo‘lgan qiymatlarni inkapsulyatsiya jarayoni bilan o‘xshash tarzda hisoblaydi.

6-algoritm Kyber KEM Decapsulation.
Kirish: ochiq kalit $\boldsymbol{pk}$, shaxsiy kalit $\boldsymbol{sk} = (\boldsymbol{s},\boldsymbol{\sigma})$, inkapsulyatsiya $\boldsymbol{c}$. 1. $\boldsymbol{H_m} = \boldsymbol{PKE.dec}(\boldsymbol{s},\boldsymbol{c})$ ni hisoblash. 2. $(\boldsymbol{K'},\boldsymbol{r'}) = \boldsymbol{H_1}(\boldsymbol{H_m}\|\|\boldsymbol{H_2}(\boldsymbol{pk}))$ ni hisoblash. 3. $\boldsymbol{c'} = \boldsymbol{PKE.enc_{r'}}(\boldsymbol{pk},\boldsymbol{H_m})$ ni hisoblash. 4. Agar $\boldsymbol{c} = \boldsymbol{c'}$ bo‘lsa, $\boldsymbol{K} = \boldsymbol{KDF}(\boldsymbol{K'}\|\|\boldsymbol{H_2}(\boldsymbol{c}))$ ni o‘rnatish. 5. Agar $\boldsymbol{c} \neq \boldsymbol{c'}$ bo‘lsa, $\boldsymbol{K} = \boldsymbol{KDF}(\boldsymbol{\sigma}\|\|\boldsymbol{H_2}(\boldsymbol{c}))$ ni o‘rnatish. **Chiqish:** taqsimlangan kalit $\boldsymbol{K}$.

Kyberda shifrlangan matnni tekshirish qanday ishlashini yaxshiroq tushunish uchun, yuqorida batafsil tasvirlangan shifrlash jarayoniga e’tibor berish lozim. Kyber PKE sxemasida xabar m vektorlar v va $s^T u$ orasidagi farq ichida joylashtiriladi, ya’ni

$$v - s^T \cdot u = toRing(m) + (e^T r + e_2 - s^T e_1).$$

Bu yerda, e, e_1, e_2 lar tasodifiy xatolik vektorlari. Ushbu xatoliklarning turli qiymatlari kombinatsiyalari mavjud bo‘lib, ularning barchasi bir xil m ga mos keladi. Ammo, KEMda tasodifiylik tanlangan r dan hosil qilib deterministik holga keltiriladi, shuning uchun har bir m uchun qiymatlar (e,e_1,e_2) ning yagona to‘plami mavjud bo‘ladi. Ushbu xususiyat KEMning zarur bo‘lgan CCA-xavfsizligini ta’minlaydi. Agar hujumchi dekapsulyatsiya jarayoniga tasodifiy shifrlangan matnni yuborsa, u har doim biror m xabariga ochiladi, ammo hujumchining aynan ushbu m ga mos keladigan (to‘g‘ri “tasodifiy” xatoliklar bilan hosil qilingan) shifrlangan matnni tanlash ehtimoli juda kichikdir.

Kyberning mos parametr tanlovlari bilan birga bo‘lgan misollari 1.2-jadvalda ko‘rsatilgan.

1.2-jadval

Kyber parametr to‘plamlari va ularga mos keluvchi dekodlash muvaffaqiyatsizlik ehtimoli δ.

	n	k	q	δ
Kyber512	256	2	3329	2^{-139}
Kyber768	256	3	3329	2^{-164}
Kyber1024	256	4	3329	2^{-174}

Saber

Saber [4] — bu Module-LWR asosida CPA-xavfsiz PKE dan olingan CCA-xavfsiz KEM hisoblanadi. $n, q \in \mathbb{N}$ uchun, foydalanilgan xalqa $\mathcal{R}_q = \mathbb{Z}_q[X]/(X^n + 1)$, ya'ni, darajasi $n - 1$ gacha bo'lgan va koeffitsiyentlari $\mathbb{Z}_q$ (ya'ni, q-modulli butun sonlar) to'plamidan olingan ko'phadlar halqasi. Tegishli modul $k \in \mathbb{N}$ rangga ega R_q^k.

Quyidagi asos elementlar talab etiladi: shovqin sohasi B, bu yerda B dan qiymatni tanlab olish $\{-5, \cdots, 5\}$ diapazonda tasodifiy kichik butun qiymatni beradi. Bundan tashqari, KEM qurilishi uchun H_1, H_2, H_3 xavfsiz xesh-funksiyalar va xavfsiz kalit hosil qilish funksiyasi KDF talab qilinadi.

Saberning yaxlitlash funksiyasi qat'iy ravishda pastga qarab yaxlitlamaydi, balki, yuqorida keltirilgan umumiy LWR holatida ko'rsatilganidek, har bir p intervalning o'rta nuqtasiga qarab yaxlitlaylaydi. (Bu, asosan, yaxlitlashning eng oddiy usuli hisoblanadi.) Bu jarayon $h \approx q/2p$ interval uzunligining yarmiga qo'shish va keyin pastga qarab yaxlitlash orqali amalga oshiriladi, ya'ni:

$$\lfloor x \rceil_p \coloneqq \lfloor x + h \rfloor_p.$$

Bu jarayonni samarali amalga oshirish uchun Saber parametrlar q va p uchun faqat 2 darajalaridan foydalanadi. Bu yaxlitlash jarayonini qo'shishdan keyingi bit bo'yicha siljish (bitwise shift) operatsiyasi uchun oddiylashtiradi.

Kyber kabi, Saber PKE (7–9-algoritmlar) ham yuqorida keltirilgan klassik LWE asosidagi shifrlash sxemasiga asoslangan. Biroq, xatolarni qo'shish o'rniga yaxlitlash ishlatiladi. Bu yuqorida taqdim etilgan Kyber PKE bilan yagona farqdir.

7-algoritm Saber PKE Key Generation: *keyGen.*

Kirish: Yo'q
1. $\boldsymbol{A} \in \boldsymbol{\mathcal{R}}_{\boldsymbol{q}}^{\boldsymbol{k}\times\boldsymbol{k}}$ ni hosil qilish.
2. $\boldsymbol{B}$ dan olingan koeffitsientlar bilan $\boldsymbol{s} \in \boldsymbol{\mathcal{R}}_{\boldsymbol{q}}^{\boldsymbol{k}}$ na'munalari.
3. $\boldsymbol{b} = \lfloor \boldsymbol{As} \rceil_{\boldsymbol{p}}$ni hisoblash.

Chiqish: ochiq kalit $\boldsymbol{pk} = (\boldsymbol{A}, \boldsymbol{b})$, shaxsiy kalit $\boldsymbol{s}$.

8-algoritm Saber PKE Encryption: *enc.*

Kirish: ochiq kalit $\boldsymbol{pk} = (\boldsymbol{A}, \boldsymbol{b})$, xabar $\boldsymbol{m} \in \{\boldsymbol{0}, \boldsymbol{1}\}^{\boldsymbol{256}}$
1. $\boldsymbol{B}$ dan olingan koeffitsientlar bilan $\boldsymbol{r} \in \boldsymbol{\mathcal{R}}_{\boldsymbol{q}}^{\boldsymbol{k}}$ na'munalari.
2. $\boldsymbol{u} = \lfloor \boldsymbol{A}^{\boldsymbol{T}}\boldsymbol{r} \rceil_{\boldsymbol{p}}$ ni hisoblash.
3. $\boldsymbol{v} = \lfloor \boldsymbol{b}^{\boldsymbol{T}}\boldsymbol{r} + \boldsymbol{toRing}(\boldsymbol{m}) \rceil_{\boldsymbol{p}}$ ni hisoblash.

Chiqish: shifrmatn $\boldsymbol{c} = (\boldsymbol{u}, \boldsymbol{v})$.

9-algoritm Saber PKE Decryption: *dec.*

Kirish: shaxsiy kalit $\boldsymbol{s}$, shifrmatn $\boldsymbol{c} = (\boldsymbol{u}, \boldsymbol{v})$.
1. $\boldsymbol{m}^* = \boldsymbol{v} - \boldsymbol{s}^{\boldsymbol{T}}\boldsymbol{u}$ ni hisoblash.

Chiqish: xabar $\boldsymbol{m} = \boldsymbol{fromRing}(\boldsymbol{m}^*)$.

Kyberga o'xshash tarzda, berilgan PKE asosida CCA-xavfsiz KEM qurish uchun FO-transformatsiyaning bir varianti qo‘llaniladi. Aslida, kalit yaratish algoritmi (10-algoritm) to‘liq bir xil.

10-algoritm Saber KEM Key Generation.

Kirish: Yo‘q.
1. $\boldsymbol{\sigma} \in \{\mathbf{0}, \mathbf{1}\}^{\mathbf{256}}$ni generatsiyalash.
2. $(\boldsymbol{pk}, \boldsymbol{s}) = \boldsymbol{PKE.keyGen}()$ ni generatsiyalash.

Chiqish: ochiq kalit $\boldsymbol{pk}$, shaxsiy kalit $\boldsymbol{sk} = (\boldsymbol{s}, \boldsymbol{\sigma})$.

Yana, KEM konstruktsiyasi (11 va 12-algoritmlar) Kyberga juda o‘xshash. Yagona tuzilmviy farq shundaki, xabar m ga qo‘llaniladigan qo‘shimcha xesh funksiyasi yo‘q.

11-algoritm Saber KEM Encapsulation.

Kirish: ochiq kalit $\boldsymbol{pk}$.
1. Xabar $\boldsymbol{m} \in \{\mathbf{0}, \mathbf{1}\}^{\mathbf{256}}$ni generatsiyalash.
2. $(\boldsymbol{K'}, \boldsymbol{r}) = \boldsymbol{H_2}(\boldsymbol{H_1}(\boldsymbol{pk})||\boldsymbol{m})$ ni hisoblash.
3. $\boldsymbol{c} = \boldsymbol{PKE.enc_r}(\boldsymbol{pk}, \boldsymbol{m})$ ni hisoblash.
4. $\boldsymbol{K} = \boldsymbol{H_3}(\boldsymbol{K'}||\boldsymbol{c})$ ni hisoblash.

Chiqish: inkapsulyatsiya $\boldsymbol{c}$, taqsimlangan kalit $\boldsymbol{K}$.

12-algoritm Saber KEM Decapsulation.

Kirish: ochiq kalit $\boldsymbol{pk}$, shaxsiy kalit $\boldsymbol{sk} = (\boldsymbol{s}, \boldsymbol{\sigma})$, inkapsulyatsiya $\boldsymbol{c}$.
1. $\boldsymbol{m'} = \boldsymbol{PKE.dec}(\boldsymbol{s}, \boldsymbol{c})$ ni hisoblash.
2. $(\boldsymbol{K'}, \boldsymbol{r'}) = \boldsymbol{H_2}(\boldsymbol{H_1}(\boldsymbol{pk})||\boldsymbol{m'})$ ni hisoblash.
3. $\boldsymbol{c'} = \boldsymbol{PKE.enc_{r'}}(\boldsymbol{pk}, \boldsymbol{m'})$ ni hisoblash.
4. Agar $\boldsymbol{c} = \boldsymbol{c'}$ bo‘lsa, $\boldsymbol{K} = \boldsymbol{H_3}(\boldsymbol{K'}||\boldsymbol{c})$ ni o‘rnatish.
5. Agar $\boldsymbol{c} \neq \boldsymbol{c'}$ bo‘lsa, $\boldsymbol{K} = \boldsymbol{H_3}(\boldsymbol{\sigma}||\boldsymbol{c})$ ni o‘rnatish.

Chiqish: taqsimlangan kalit $\boldsymbol{K}$.

Saber misollari va ularga mos parametr tanlovlari 1.3-jadvalda ko‘rsatilgan.

1.3-jadval

Saber parametr to‘plamlari va ularga mos keluvchi dekodlash muvaffaqiyatsizlik ehtimoli δ.

	n	k	q	p	δ
LightSaber	256	2	2^{13}	2^{10}	2^{-120}
Saber	256	3	2^{13}	2^{10}	2^{-136}
FireSaber	256	4	2^{13}	2^{10}	2^{-165}

Dilithium

Dilithium [5] — bu Module-LWE asosida qurilgan imzo sxemasi hisoblanadi. n, $q \in \mathbb{N}$ uchun, foydalanilgan xalqa $\mathcal{R}_q = \mathbb{Z}_q[X]/(X^n + 1)$, ya’ni, darajasi $n - 1$ gacha bo‘lgan va koeffitsiyentlari $\mathbb{Z}_q$ (ya’ni, q-modulli butun sonlar) to‘plamidan olingan ko‘phadlar halqasi. Tegishli modul $l \in \mathbb{N}$ rangga ega R_q^l. Bundan tashqari, Dilithium xavfsiz xesh funksiyasi H ni talab qiladi.

Kalit yaratish (13-algoritm) Kyberning kalit yaratishiga deyarli o‘xshash.

LWE holati hosil qilinadi, ya'ni, $A \in R_q^{k\times l}$ matritsasi ($k \in N$), shaxsiy vektor $s \in R_q^l$ va xatolik qiymati $e \in R_q^k$. Odatda, A va b ochiq, s esa maxfiy saqlanadi.

13-algoritm Dilithium Key Generation: *keyGen.*
Kirish: Yo‘q 1. $\boldsymbol{A} \in \boldsymbol{\mathcal{R}_q^{k\times l}}$ ni hosil qilish. 2. $\boldsymbol{B}$ dan olingan koeffitsientlar bilan $\boldsymbol{s} \in \boldsymbol{\mathcal{R}_q^l}$ na'munalari. 3. $\boldsymbol{B}$ dan olingan koeffitsientlar bilan $\boldsymbol{e} \in \boldsymbol{\mathcal{R}_q^k}$ na'munalari. 4. $\boldsymbol{b} = \boldsymbol{As} + \boldsymbol{e}$ ni hisoblash. **Chiqish:** ochiq kalit $\boldsymbol{pk} = (\boldsymbol{A}, \boldsymbol{b})$, shaxsiy kalit $\boldsymbol{s}$.

Dilithiumning imzolash jarayoni (14-algoritm) ehtimollik asosida ishlaydi. Birinchi qadamda tasodifiy vektor $y \in \boldsymbol{\mathcal{R}_q^l}$ namunalanadi. Verifikatsiya jarayonida to‘g‘rilikni ta'minlash uchun, Ay ning yaxlitlangan versiyasi $round()$ funksiyasi orqali ishlatiladi. Bu funksiya har bir ko‘phadning koeffitsientini yaxlitlaydi. Imzo (z, c) juftligini hisoblash orqali shakllantiriladi, bu yerda c xabar m va $round(Ay)$ qiymatining xesh funksiyasi orqali hosil qilinadi. Xesh funksiyasi H kirishni $\{-1, 0, 1\}$ koeffitsiyentlari bo‘lgan ko‘phadga akslantiradi.

z qiymat shaxsiy kalit s ga bog‘liq bo‘lgani uchun xavfsizlikka jiddiy muammolar keltirib chiqarishi mumkin. Shuning uchun, z bevosita chiqarilmaydi. Buning o‘rniga, z va s orasidagi statistik bog‘liqliklarni olib tashlash uchun, Dilithium "*qabul qilishdan bosh tortish*" (rejection sampling) usulini qo‘llaydi. Qabul qilishdan bosh tortishning tafsilotlari uchun [6, 7] manbalariga murojaat qilish mumkin. Agar z yaroqsiz (invalid, "qabul qilinmagan") bo‘lsa, algoritm 1-qadamdan boshlanadi.

14-algoritm Dilithium Imzoni hosil qilish.
Kirish: ochiq kalit $\boldsymbol{pk} = (\boldsymbol{A}, \boldsymbol{b})$, shaxsiy kalit $\boldsymbol{s}$, xabar $\boldsymbol{m} \in \{\boldsymbol{0}, \boldsymbol{1}\}^*$ $\boldsymbol{z}$ yaroqli (valid) bo‘lgunga qadar: 1. Kichik koeffitsientlar bilan $\boldsymbol{y} \in \boldsymbol{\mathcal{R}_q^l}$ na'munalari olinadi. 2. $\boldsymbol{w} = \boldsymbol{round}(\boldsymbol{Ay})$ hisoblanadi. 3. $\boldsymbol{c} = \boldsymbol{H}(\boldsymbol{m}\|\|\boldsymbol{w})$ hisoblanadi. 4. $\boldsymbol{z} = \boldsymbol{y} + \boldsymbol{cs}$ hisoblanadi. **Chiqish:** imzo $\boldsymbol{\sigma} = (\boldsymbol{z}, \boldsymbol{c})$.

To‘g‘ri imzo σ berilgan holda, w ni quyidagi hisoblash yordamida tiklash mumkin:

$$round(Az - bc) = round(A(y + cs) - (As + e)c)$$
$$= round(Ay + Acs - Acs - ce) = round(Ay - ce) = w$$

Haqiqatan ham w ni tiklash uchun oxirgi qadam $round(Ay - ce) = round(Ay)$ hisoblanadi. Chunki, c va e ikkala kichik koeffitsiyentlarga ega bo‘lgani uchun, ularning ko‘paytmasi ce yaxlitlash natijasiga ta'sir qilmaydi. Imzoni tekshirish uchun, tiklangan w' ni ishlatib, $c' = H(m \mid\mid w')$ ni qayta hisoblab, uni berilgan imzo qiymati c bilan taqqoslash mumkin (15-algoritm). Agar z maxfiy kalit s yordamida hisoblanmagan bo‘lsa, ya'ni, $z = y + cs$ orqali hisoblanmagan bo‘lsa, yuqoridagi tenglamada Acs atamalari bekor bo‘lmasligi sababli noto‘g‘ri $w' \neq w$ natijasiga olib keladi. Shuning uchun, c' qiymati ham noto‘g‘ri bo‘lib, berilgan imzo rad etiladi.

15-algoritm Dilithium Verifikatsiya jarayoni.
Kirish: ochiq kalit $\boldsymbol{pk} = (\boldsymbol{A}, \boldsymbol{b})$, imzo $\boldsymbol{\sigma} = (\boldsymbol{z}, \boldsymbol{c})$, xabar $\boldsymbol{m} \in \{\boldsymbol{0}, \boldsymbol{1}\}^*$ 1. $\boldsymbol{w}' = \boldsymbol{round}(\boldsymbol{Az} - \boldsymbol{bc})$ hisoblanadi.   2. $\boldsymbol{c}' = \boldsymbol{H}(\boldsymbol{m}\|\|\boldsymbol{w}')$ hisoblanadi.   **Chiqish:** agar $\boldsymbol{c} = \boldsymbol{c}'$ bo‘lsa, haqiqiy, aks holda noto‘g‘ri.

Dilithium misollari va ularga mos parametr tanlovlari 1.4-jadvalda ko‘rsatilgan.

1.4-jadval

Dilithium parametrlar to‘plamlari NIST xavfsizlik darajalari 2, 3 va 5 uchun quyidagi kutilayotgan imzo yaratish takrorlashlar soni (#reps) bilan birga

	$\boldsymbol{n}$	$(\boldsymbol{k}, \boldsymbol{l})$	$\boldsymbol{q}$	$\boldsymbol{\#reps}$
Dilithium 2	256	(4,4)	8380417	4.25
Dilithium 3	256	(6,5)	8380417	5.1
Dilithium 5	256	(8,7)	8380417	3.85

NTRU

NIST uchinchi bosqichda taqdim etilgan NTRU [8] asosan hozirgi ko‘rganimiz kabi umumiy NTRU shifrlash sxemasi asosida bo‘lsada, bir nechta muhim farqlar mavjud bo‘lib, ular qo‘shimcha tushuntirishni talab qiladi. Eng yaqqol o‘zgarish, asosiy polinom halqalari bilan bog‘liq. Avval, faqat ikkita qisqartirilgan polinom halqalari ko‘rib chiqilgan edi: $\mathcal{R}_q = \mathbb{Z}_q[X]/(X^n - 1)$ va $\mathcal{R}_p = \mathbb{Z}_p[X]/(X^n - 1)$, ikkalasi ham $(X^n - 1)$ tomonidan yaratilgan. Buning o‘rniga, uchta polinom tomonidan yaratilgan polinom halqalari ko‘rib chiqiladi:

$$\phi_1 = (X - 1),\ \phi_n = \frac{X^n - 1}{X - 1},\ \phi_1\phi_n = X^n - 1.$$

Mos halqalarni ajratish uchun, quyidagi belgilanish kiritiladi: $\mathcal{R}_k^{\phi} \coloneqq \mathbb{Z}_k[X]/\phi$.

Masalan, dastlab $\mathcal{R}_3$ sifatida foydalanilgan bo‘lsa, endi $\mathcal{R}_3^{\phi_1\phi_n}$ tarzida belgilanadi.

Kalitni generatsiyalash (Algoritm 16) asosan umumiy NTRU qurilishidagi xuddi shu qadamlarni o‘z ichiga oladi. Farq shundaki, qiymatlarni tanlash va amallar turli halqalarda va fazolarda bajariladi. Shuni ta’kidlash kerakki, g har doim ϕ_1 ning ko‘paytmasi bo‘ladi. Bundan tashqari, h_q ni hisoblash bosqichi qo‘shilgan. Ushbu o‘zgartirishlarning barchasi, deshifrlash bosqichida ko‘rib chiqilganidek, shifrlangan matnlarni soxtalashtirishga qarshi qo‘shimcha xavfsizlik qatlamini qo‘shishga qaratilgan.

16-algoritm NTRU PKE Key Generation: *keyGen*.
Kirish: Yo‘q   1. $\boldsymbol{f} \in \boldsymbol{\mathcal{R}}_3^{\boldsymbol{\phi_n}}$ tanlanadi.   2. $\boldsymbol{g} \in \{\boldsymbol{\phi_1} \cdot \boldsymbol{v} \mid \boldsymbol{v} \in \boldsymbol{\mathcal{R}}_3^{\boldsymbol{\phi_n}}\}$ tanlanadi.

3. $\boldsymbol{f_q = f^{-1} \in \mathcal{R}_q^{\phi_n}}$ hisoblanadi. 4. $\boldsymbol{h \overset{\mathcal{R}_q^{\phi_1\phi_n}}{\equiv} g \cdot f_q}$ hisoblanadi. 5. $\boldsymbol{h_q = h^{-1} \in \mathcal{R}_q^{\phi_n}}$ hisoblanadi. 6. $\boldsymbol{f_3 = f^{-1} \in \mathcal{R}_3^{\phi_n}}$ hisoblanadi. **Chiqish:** ochiq kalit $\boldsymbol{h}$, shaxsiy kalit $\boldsymbol{sk = (f, f_p, h_q)}$.

Shifrlash jarayoni (Algoritm 17) faqat shifrlashdan oldin xabar m ustida $lift$-funksiyasini qo‘llashda farq qiladi. Faraz qilinsin, $(m \cdot \phi_1^{-1})_{\mathcal{R}_3^{\phi_n}}$ belgilanish $\mathcal{R}_3^{\phi_n}$ halqada hisoblashni anglatadi, u holda:

$$Lift(m) = \phi_n \cdot (m \cdot \phi_1^{-1})_{\mathcal{R}_3^{\phi_n}}.$$

$Lift(m) \overset{\mathcal{R}_3^{\phi_n}}{\equiv} m$ tenglikni ko‘rish oson. Endi, g va $\widehat{m}$ ning ϕ_1 ning ko‘paytmalari bo‘lishi natijasida, c uchun ham shu holat amal qiladi.

17-algoritm NTRU PKE Encryption: *enc*.
Kirish: ochiq kalit $\boldsymbol{h}$, xabar $\boldsymbol{m \in \mathcal{R}_3^{\phi_n}}$ 1. $\boldsymbol{\widehat{m} = Lift(m)}$ hisoblanadi. 2. $\boldsymbol{r \in \mathcal{R}_3^{\phi_n}}$ tanlanadi. 3. $\boldsymbol{c \overset{\mathcal{R}_q^{\phi_1\phi_n}}{\equiv} 3 \cdot r \cdot h + \widehat{m}}$ hisoblanadi. **Chiqish:** shifrmatn $\boldsymbol{c}$.

Deshifrlash jarayoni umumiy NTRU qurilishiga nisbatan eng katta farqqa ega va shuning uchun qo‘shimcha tushuntirishni talab qiladi. To‘g‘ri shifrlangan xabar m holatida, deshifrlash jarayoni 2- va 3-qadamda amalga oshiriladi. 2-qadamdagi hisoblashning umumiy NTRU sxemasidagi natijaga teng bo‘lishi aniq emas, chunki f_q kattalik $\mathcal{R}_q^{\phi_n}$ dagi teskari polinom, ammo, $\mathcal{R}_q^{\phi_1\phi_n}$ dagi teskari polinom emas.

g ning ϕ_1 ning ko‘paytmasi va f_q ning $\mathcal{R}_q^{\phi_n}$ dagi teskari bo‘lishi faktiga asoslanib, quyidagini yozish mumkin:

$$g = \phi_1 \cdot v \qquad \text{ba'zi } v \in \mathcal{R}_3^{\phi_n} \text{ uchun} \qquad (1)$$

$$f \cdot f_q = 1 + k \cdot \phi_n \qquad \text{ba'zi } k \in \mathbb{Z}[X] \text{ uchun} \qquad (2)$$

Yuqoridagi tengliklarni va $\phi_1\phi_n \overset{\mathcal{R}_q^{\phi_1\phi_n}}{\equiv} 0$ inobatga olib, 2-bosqich quyidagicha yechiladi:

$$a = f \cdot c = f \cdot f_q \cdot 3 \cdot r \cdot g + f \cdot \widehat{m} = (1 + k \cdot \phi_n) \cdot 3 \cdot r \cdot g + f \cdot \widehat{m} = 3 \cdot r \cdot g + k \cdot \phi_n \cdot \phi_1 \cdot v \cdot 3 \cdot r + f \cdot \widehat{m} \overset{\mathcal{R}_q^{\phi_1\phi_n}}{\equiv} 3 \cdot r \cdot g + f \cdot \widehat{m}.$$

Eng so‘ngida, f_3 haqiqatan ham $\mathcal{R}_3^{\phi_n}$ halqasida teskari element ekanini hisobga olib, 3-qadamda m ni quyidagicha hisoblash orqali topish mumkin:

$$a \cdot f_3 = 3 \cdot r \cdot g \cdot f_3 + f \cdot f_3 \cdot \hat{m} \overset{\mathcal{R}_3^{\phi_n}}{\equiv} m.$$

Birinchi had 3 ga karrali bo‘lgani uchun yo‘q bo‘ladi va avvalroq ko‘rilganidek, $\hat{m} = Lift(m) \overset{\mathcal{R}_3^{\phi_n}}{\equiv} m$.

Deshifrlash (18-algoritm) qo‘shimcha qadamlarni asoslovchi ichki validatsiya jarayonini o‘z ichiga oladi. Keyinchalik ko‘rsatilganidek, bu qayta shifrlashdan qochadigan KEM (klassik FO-transformatsiyasidan farqli ravishda) qurishga imkon beradi.

Birinchi qadamda c ning ϕ_1 ga karrali ekanligi tekshiriladi, bu esa, avval ko‘rilganidek, to‘g‘ri generatsiya qilingan shifrlangan matnlar uchun to‘g‘ri bo‘ladi. 6 va 7-qadamda r ning $\mathcal{R}_3^{\phi_n}$ dan to‘g‘ri olinganligini tasdiqlash uchun 4 va 5-qadamlar orqali c, $Lift(m)$ va h_q yordamida r qayta tiklanadi. Agar validatsiya bosqichlarining birortasi muvaffaqiyatsiz bo‘lsa, protsedura xatolik vektori (0,0,1) ni qaytaradi; aks holda, $(r, m, 0)$ ni qaytariladi.

18-algoritm NTRU PKE Decryption: *dec.*

Kirish: shaxsiy kalit $\boldsymbol{sk} = (\boldsymbol{f}, \boldsymbol{f_p}, \boldsymbol{h_q})$, shifrmatn $\boldsymbol{c}$

1. Agar $\boldsymbol{c} \overset{\mathcal{R}_q^{\phi_1}}{\not\equiv} 0$ bo‘lsa, $(\mathbf{0}, \mathbf{0}, \mathbf{1})$ ni qaytarish.
2. $\boldsymbol{a} \overset{\mathcal{R}_q^{\phi_1 \phi_n}}{\equiv} \boldsymbol{f} \cdot \boldsymbol{c}$ hisoblanadi.
3. $\boldsymbol{m} \overset{\mathcal{R}_3^{\phi_n}}{\equiv} \boldsymbol{a} \cdot \boldsymbol{f_3}$ hisoblanadi.
4. $\hat{\boldsymbol{m}} = \boldsymbol{Lift}(\boldsymbol{m})$ hisoblanadi.
5. $\boldsymbol{r} \overset{\mathcal{R}_q^{\phi_n}}{\equiv} (\boldsymbol{c} - \hat{\boldsymbol{m}}) \cdot \frac{\boldsymbol{h_q}}{\mathbf{3}}$ hisoblanadi.
6. Agar $\boldsymbol{r} \in \mathcal{R}_3^{\phi_n}$ bo‘lsa, $(\boldsymbol{r}, \boldsymbol{m}, \mathbf{0})$ ni qaytarish.
7. Aks holda $(\mathbf{0}, \mathbf{0}, \mathbf{1})$ ni qaytarish.

Chiqish: To‘g‘ri $(\boldsymbol{r}, \boldsymbol{m}, \mathbf{0})$ yoki xato $(\mathbf{0}, \mathbf{0}, \mathbf{1})$.

NTRU KEMni qurish endi oson. Kalitni generatsiyalash jarayoni (19-algoritm) shunchaki PKE.keyGen() funksiyasini chaqiradi va keyinchalik dekapsulyatsiyalashda bilvosita rad etish uchun ishlatiladigan tasodifiy qiymat σ ni tanlaydi.

19-algoritm NTRU KEM Key Generation.

Kirish: Yo‘q

1. $\left(\boldsymbol{h}, \left(\boldsymbol{f}, \boldsymbol{f_q}, \boldsymbol{h_q}\right)\right) = \boldsymbol{PKE.keyGen}()$ ni generatsiyalash.
2. $\boldsymbol{\sigma} \in \{\mathbf{0}, \mathbf{1}\}^{\mathbf{256}}$ tanlanadi.

Chiqish: ochiq kalit $\boldsymbol{h}$, shaxsiy kalit $\boldsymbol{sk} = (\boldsymbol{f}, \boldsymbol{f_q}, \boldsymbol{h_q}, \boldsymbol{\sigma})$.

Inkapsulyatsiya (20-algoritm) uch bosqichdan iborat: r va $m \in \mathcal{R}_3^{\phi_n}$, ni tasodifiy tanlash, PKE.enc() yordamida shifrlangan matnni generatsiyalash va umumiy maxfiy kalit K ni r va m qiymatlaridan kriptografik hesh funksiyasi H_1

orqali hisoblash.

20-algoritm NTRU KEM Encapsulation.
Kirish: ochiq kalit $\boldsymbol{h}$ 1. $\boldsymbol{r}, \boldsymbol{m} \in \boldsymbol{\mathcal{R}_3^{\phi_n}}$ tanlanadi. 2. $\boldsymbol{c = PKE.enc_r(h, m)}$ hisoblanadi. 3. $\boldsymbol{K = H_1(r \parallel m)}$ **Chiqish:** enkapsulyatsiya $\boldsymbol{c}$, umumiy kalit $\boldsymbol{K}$.

Dekapsulyatsiya (21-algoritm) PKE.dec() yordamida c ni deshifrlashdan boshlanadi. Keyin ikkita xesh hisoblanadi: to‘g‘ri xesh r va m qiymatlaridan, va yolg‘on xesh esa tanlangan s va c qiymatlaridan kriptografik xesh funksiyasi H_2 yordamida aniqlanadi. Agar deshifrlash joiz bo‘lsa, birinchi (to‘g‘ri) qiymat qaytariladi; aks holda, yolg‘on qiymat qaytariladi.

21-algoritm NTRU KEM Decapsulation.
Kirish: shaxsiy kalit $\boldsymbol{sk = (f, f_q, h_q, \sigma)}$, enkapsulyatsiya $\boldsymbol{c}$. 1. $\boldsymbol{(r, m, fail) = PKE.dec((f, f_q, h_q), c)}$ hisoblanadi. 2. $\boldsymbol{k_1 = H_1(r \parallel m)}$ hisoblanadi. 3. $\boldsymbol{k_2 = H_2(\sigma \parallel c)}$ hisoblanadi. 4. $\boldsymbol{if(fail = 0)}$ u holda $\boldsymbol{K = k_1}$. 5. aks holda, $\boldsymbol{K = k_2}$. **Chiqish:** umumiy kalit $\boldsymbol{K}$.

NTRU taqdimoti ikki xil parametrlar to‘plami oilasini tavsiya qiladi, ular NTRU-HRSS va NTRU-HPS deb nomlanadi. Ushbu bo‘limdagi tushuntirishlar NTRU-HRSS ga tegishli, ammo ikkalasining ham tafsilotlari algoritm tavsifida [8] keltirilgan.

Falcon

Falcon [9] — bu NTRU tuzilmasidan foydalangan holda Gentry–Peikert–Vaikuntanathan (GPV) imzo sxemasiga asoslangan imzo sxemasidir [10]. Yuqori darajada GPV freymworkining asosiy g‘oyasi quyidagicha. Ochiq kalit — bu $A \in \mathbb{Z}_q^{n\times m}$ $(m > n)$ to‘liq rangli matritsa bo‘lib, u panjara L ni hosil qiladi, yashirin kalit esa $B \in \mathbb{Z}_q^{m\times m}$ matritsa bo‘lib, unga mos keluvchi panjara $L_q^\perp$ ni hosil qiladi. L va $L_q^\perp$ panjaralari $mod\ q$ bo‘yicha ortogonal bo‘lib, bu quyidagilarni anglatadi:

$$\forall x \in L, y \in L_q^\perp: \langle x, y\rangle = 0\ mod\ q.$$

Boshqacha aytganda, A va B matritsalarining qatorlari juft-juft ortogonaldir, ya’ni, $B \cdot A^t = 0\ mod\ q$.

Ixtiyoriy xabar m ning $H(m)$ xeshi va panjara L ga akslantiruvchi xesh-funksiyasi H berilgan holda, joiz imzo s quyidagi ikki xususiyatni qanoatlantirishi kerak:

1. $A \cdot s = H(m)\ mod\ q$;
2. Ba’zi β, ya’ni, s qisqa bo‘ladigan, uchun $\|s\| < \beta$.

Birinchi xususiyatni qanoatlantiruvchi yechim s standart chiziqli algebra yordamida osongina hisoblanishi mumkin; ammo, ikkinchi xususiyatni ham hisobga olgan holda, joiz s ni topish ancha murakkablashadi. Ushbu talablar deyarli Short

Integer Solution (SIS) muammosiga o‘xshash bo‘lib, yagona farq shundaki, SIS muammosida yechim $A \cdot s = 0\, mod\ q$ shartini bajaradi. SIS muammosi o‘rtacha holatda qiyin bo‘lib, Shortest Vector Problem (SVP) ga qisqarishi mumkin [11].

Biroq, maxfiy B matritsani bilgan holda, joiz imzo s ni samarali hisoblash mumkin. Birinchi qadam, $A \cdot s' = H(m)$ shartni qanoatlantiruvchi istalgan s' yechimni topishdir. Keyin, ortogonal panjara $L_q^{\perp}$ ga yetarlicha yaqin bo‘lgan vektor v ni topish kerak. B ni bilgan holda, buni Babai algoritmi [12] kabi samarali CVP (Closest Vector Problem) yaqinlashuv algoritmi yordamida amalga oshirish mumkin, bunda $\|s' - v\| < \beta$ sharti bajariladi.

Oxirida $A \cdot s = A \cdot s' - A \cdot v = H(m) - 0$ sababli $s = s' - v$ imzo joiz bo‘ladi, chunki, v matritsa A ning qatorlariga ortogonal.

Falconning umumiy tuzilmasi GPV sxemasiga juda o‘xshash bo‘lib, kerakli panjaralarni yaratish uchun NTRU sxemasining asosiy g‘oyasidan foydalanadi. NTRU singari, Falconning amallari ham qisqartirilgan polinomlar halqasi $\mathcal{R}_q = \mathbb{Z}_q[X]/(X^n + 1)$ da amalga oshiriladi. Bu yerda, n va q musbat va o‘zaro tub sonlar, $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ esa $mod\ q$ bo‘yicha butun sonlar halqasini anglatadi. Shunday qilib, $\mathcal{R}_q$ belgilanish $\mathbb{Z}_q$ dagi koeffitsiyentlarga ega darajasi $< n$ bo‘lgan barcha polinomlar halqasidir.

Kalit yaratish jarayoni (22-algoritm) uchun $f, g \in \mathcal{R}_q$ va $F, G \in R = \mathbb{Z}[X]/(X^n + 1)$ polinomlar to‘plami quyidagi shartni qanoatlantirishi shart:

$$fG - gF = q\ mod\ (X^n + 1)$$

Keyin, NTRU bilan o‘xshash tarzda, $h = g \cdot f^{-1} \in \mathcal{R}_q$ hisoblanadi. Ushbu polinomlardan foydalanib, ochiq kalit matritsasi $A \in \mathbb{Z}_q^{n\times 2n}$ va maxfiy kalit matritsasi $B \in \mathbb{Z}_q^{2n\times 2n}$ quyidagicha hosil qilinadi:

$$A = \begin{pmatrix} 1 & h \end{pmatrix} \qquad\qquad B = \begin{pmatrix} g & -f \\ G & -F \end{pmatrix}$$

Bu yerda har bir polinom tegishli matritsa shaklida ifodalanadi (belgilanishlar yuqorida aytib o‘tildi).

Quyidagini qanoatlantirilishini osonlik bilan tekshirilishi mumkin:

$$B \cdot A^t = \begin{pmatrix} g - hf \\ G - hF \end{pmatrix} = \begin{pmatrix} g - (gf^{-1})f \\ G - (gf^{-1})F \end{pmatrix} = \begin{pmatrix} g - g \\ ff^{-1}(G - gf^{-1}F) \end{pmatrix}$$
$$= \begin{pmatrix} 0 \\ f^{-1}(fG - gF) \end{pmatrix} = \begin{pmatrix} 0 \\ f^{-1}q \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} mod\ q$$

22-algoritm Falcon Key Generation.
Kirish: Yo‘q 1. $\boldsymbol{f, g \in \mathcal{R}_q}$ tanlanadi. 2. $\boldsymbol{f \cdot G - g \cdot F = q\ mod\ (X^n + 1)}$ shartni qanoantlantiruvchi $\boldsymbol{F, G \in \mathcal{R}}$ topiladi. 3. $\boldsymbol{h = g \cdot f^{-1}}$ hisoblanadi. **Chiqish:** ochiq kalit $\boldsymbol{h}$, shaxsiy kalit $\boldsymbol{sk = (f, g, F, G)}$.

Falcon imzosini ehtimollik ravishda amalga oshirish uchun $r \in \{0,1\}^{320}$ tasodifiy qiymat tanlanadi va u H kriptografik xesh funksiyasi yordamida $c = H(r \parallel m)$ hosil qilish uchun ishlatiladi. $A = \begin{pmatrix} 1 & h \end{pmatrix}$ tuzilishiga ko‘ra, birinchi xususiyatni qanoatlantiruvchi s'ni topish oson. $(1 \quad h) \cdot \begin{pmatrix} c \\ 0 \end{pmatrix} = c$ ekanligidan, har doim $s' = (c, 0)^\intercal$ foydalaniladi. Yuqorida aytilganidek, s' ga yaqin $v \in L_q^\perp$ vektor qidiriladi. Falcon buni Babai algoritmining modifikatsiyalangan usuli [13] yordamida amalga oshiradi. Keyin $s' - v$ farq 1 va 2-xususiyatlarni qanoatlantiradi va joiz imzo hosil qiladi (23-algoritm).

Xavfsizlikni oshirish uchun $s = (s_1, s_2)^\intercal = (c - v_1, -v_2)^\intercal$ning faqat ikkinchi komponenti uzatiladi. Bu esa s ning yaroqliligini tekshirish uchun yetarli hisoblanadi. $A \cdot s = (1 \quad h) \cdot \begin{pmatrix} s_1 \\ s_2 \end{pmatrix} = s_1 + h \cdot s_2 = c$ tufayli, s_1 faqat kichik konstanta bilan siljishni ifodalashini ko‘rish mumkin.

Bu yondashuv Falcon sxemasining samaradorligini oshiradi va imzo hajmini kamaytiradi.

23-algoritm Falcon Signature generation.
Kirish: shaxsiy kalit $\boldsymbol{sk} = (\boldsymbol{f}, \boldsymbol{g}, \boldsymbol{F}, \boldsymbol{G})$, xabar $\boldsymbol{m} \in \{\boldsymbol{0}, \boldsymbol{1}\}^*$ 1. $\boldsymbol{r} \in \{\boldsymbol{0}, \boldsymbol{1}\}^{\boldsymbol{320}}$ tanlanadi. 2. $\boldsymbol{c} = \boldsymbol{H}(\boldsymbol{r} \parallel \boldsymbol{m})$ hisoblanadi. 3. $\boldsymbol{s}' = (\boldsymbol{c}, \boldsymbol{0})^\intercal$ o‘rnatiladi. 4. $\boldsymbol{v} \in \boldsymbol{L}_{\boldsymbol{q}}^\perp$ qiymat $\Vert\boldsymbol{s}' - \boldsymbol{v}\Vert < \boldsymbol{\beta}$ shart bilan topiladi. 5. $(\boldsymbol{s_1}, \boldsymbol{s_2})^\intercal = \boldsymbol{s}' - \boldsymbol{v} = (\boldsymbol{c} - \boldsymbol{v_1}, -\boldsymbol{v_2})^\intercal$ hisoblanadi. **Chiqish:** imzo $\boldsymbol{\sigma} = (\boldsymbol{r}, \boldsymbol{s_2})$.

Xuddi imzoni hosil qilishda bo‘lgani kabi, verifikatsiya jarayonida ham (24-algoritm) xabar m va berilgan r birgalikda xesh qilinadi. Agar s_2 to‘g‘ri generatsiya qilingan deb faraz qilinsa, yetishmayotgan qiymat $s_1$ni quyidagicha hisoblash mumkin: $s_1 = A \cdot \begin{pmatrix} c \\ -s_2 \end{pmatrix} = c - s_2 \cdot h$ va u yetarli darajada kichik bo‘lsa, haqiqiy deb e’lon qilinadi, ya’ni, $\Vert(s_1, s_2)^\intercal\Vert < \beta$.

24-algoritm Falcon Verification.
Kirish: ochiq kalit $\boldsymbol{h}$, xabar $\boldsymbol{m} \in \{\boldsymbol{0}, \boldsymbol{1}\}^*$, imzo $\boldsymbol{\sigma} = (\boldsymbol{r}, \boldsymbol{s_2})$. 1. $\boldsymbol{c} = \boldsymbol{H}(\boldsymbol{r} \parallel \boldsymbol{m})$ hisoblanadi. 2. $\boldsymbol{s_1} = \boldsymbol{c} - \boldsymbol{s_2} \cdot \boldsymbol{h}$ hisoblanadi. **Chiqish:** agar $\Vert(\boldsymbol{s_1}, \boldsymbol{s_2})^\intercal\Vert < \boldsymbol{\beta}$ bo‘lsa, imzo haqiqiy, aks holda haqiqiy emas.

Falcon variantlariga mos keladigan parametr tanlovlari bilan 1.5-jadvalda keltirilgan.

1.5-jadval

Falcon parametrlar to‘plami

	n	q
Falcon-512	512	12289
Falcon-1024	1024	12289

Klassic McEliece

Classic McEliece [14] — bu Niederreiter shifrlash sxemasining bir versiyasiga asoslangan CCA-xavfsiz (Chosen Ciphertext Attack) kalitni inkapsulyatsiyalash mexanizmi. Xabar xatolik vektori e sifatida ifodalanadi, uning sindromi, ya’ni PCM (ochiq kalit) e ga qo‘llanilgani shifrlash uchun ishlatiladi. Kodning tuzilishini (shaxsiy kalitni) bilgan holda, qabul qiluvchi sindromdan sindromni dekodlash algoritmi yordamida xatolik vektori e ni qayta tiklay oladi [15].

Classic McEliece sxemasi ikkilik Goppa kodlaridan foydalanadi, ular chiziqli (n, k, d) kodlarni tashkil qiladi. Kalitni yaratish jarayonida (25-algoritm), Classic McEliece tasodifiy ikkilik Goppa kodi $\Gamma(g, L)$ ni generatsiya qiladi. Yuqorida ta'kidlanganidek, $\Gamma(g, L)$ kodi darajasi tegishli m uchun t bo'lgan $g(x) \in \mathbb{F}_{2^m}[x]$ Goppa ko'phadi va L tayanchni o'z ichiga oladi. Keyin, mos keluvchi ikkilik PCM $H \in \mathbb{F}_2^{mt\times n}$ hisoblanadi va standart shaklga o'tkaziladi. H ochiq kalit sifatida e'lon qilinadi, ammo, Goppa parametrlari g va L maxfiy saqlanadi. Classic McEliece, Goppa kodini berilgan PCM dan qayta tiklash odatda mumkin emasligidan foydalanadi.

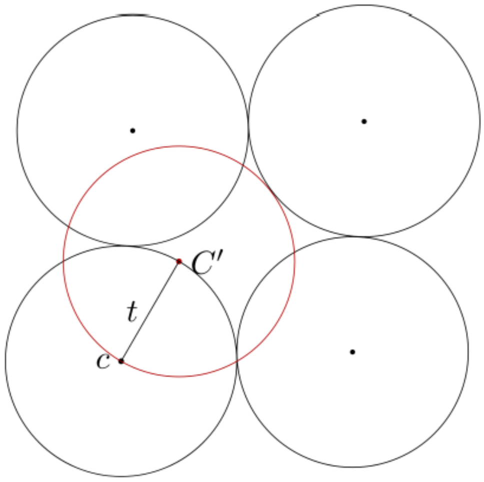
25-algoritm Classic McEliece PKE Key Generation: *keyGen.*
Kirish: Yo'q. 1. Quyidagilarga ega tasodifiy Goppa kodi $\boldsymbol{\Gamma(g, L)}$ hosil qilinadi a. $\boldsymbol{t}$ darajaga ega Goppa ko'phadi $\boldsymbol{g(x)} \in \mathbb{F}_{\boldsymbol{2^m}}[\boldsymbol{t}]$ b. $\mathbb{F}_{\boldsymbol{2^m}}$ dagi $\boldsymbol{n}$ turli elementlarning tekis taqsimlangan tasodifiy ketma-ketligi $\boldsymbol{L} = (\boldsymbol{\alpha_1}, \boldsymbol{\alpha_2}, \cdots, \boldsymbol{\alpha_n})$. 2. Tegishli binar PCM $\boldsymbol{H} \in \mathbb{F}_2^{\boldsymbol{mt\times n}}$ hisoblanadi. **Chiqish:** ochiq kalit $\boldsymbol{H}$, shaxsiy kalit $\boldsymbol{\Gamma(g, L)}$**.**

Classic McEliece shifrlashining asosiy g'oyasi (26-algoritm) — bu xato qilgan kod so'zining $H(c{+}e)$ sindromini jo'natishdir, bunda $c \in \Gamma(g, L)$ va $e \in \mathbb{F}_2^n$ xato vektoridir. Shuni kuzatish mumkinki, $H(c + e)$ aniq kod so'z c ga bog'liq emas, chunki, $H(c + e) = Hc + He = He$ barcha kod so'zlar uchun to'g'ri keladi. Shunday qilib, c ni tashlab, faqat He ni hisoblanadi. e qiymati xabar sifatida ishlatiladi, va uning og'irligi t ga teng bo'lishi talab qilinadi. Bu og'irlik t deshifrlashning to'g'ri bajarilishini ta'minlagan holda mumkin bo'lgan eng katta qiymat sifatida aniqlanadi. Shunday qilib, xabar maydonining hajmi $\binom{n}{t}$ ga teng. Berilgan PCM H yordamida tegishli sindrom He hisoblanadi va qabul qiluvchiga yuboriladi.

26-algoritm Classic McEliece PKE Encryption: *enc.*
Kirish: ochiq kalit $\boldsymbol{H} \in \mathbb{F}_2^{\boldsymbol{mt\times n}}$, $\boldsymbol{t}$ og'irlikka ega xabar $\boldsymbol{e} \in \mathbb{F}_{\boldsymbol{2}}^{\boldsymbol{n}}$. 1. $\boldsymbol{C = He} \in \mathbb{F}_{\boldsymbol{2}}^{\boldsymbol{n-k}}$ hisoblanadi. **Chiqish:** shifrmatn $\boldsymbol{C}$.

Goppa kodi tuzilishini, ya'ni maxfiy Goppa polinomi g va tayanchi $(\boldsymbol{\alpha_1}, \boldsymbol{\alpha_2}, \cdots, \boldsymbol{\alpha_n})$ ni bilgan holda, qabul qiluvchi taqdim etilgan sindrom $C = He$ dan e ni qayta tiklay oladi. Buning uchun berilgan sindrom $C \in \mathbb{F}_2^{\boldsymbol{n-k}}$ ustun vektor $C' = (C, 0, \dots, 0) \in \mathbb{F}_2^n$ shaklida k ta nolni qo'shish orqali kengaytiriladi. Birinchi navbatda quyidagi kuzatiladi: $H(C' + e) = H\big((He, 0, \dots, 0) + e\big) = H(He, 0, \dots, 0) + He = He + He = 0$.

Shuni ta'kidlash kerakki, $H(He, 0, \dots, 0) = He$ tenglik to'g'ri keladi, chunki H standart shakldа, ya'ni, $H = (I_{n-k} \parallel -T)$, bu yerda T ma'lum bir matritsadir. Yuqoridagi tenglama shuni anglatadiki, $c = C' + e$ Goppa kod $\Gamma(g, L)$ ga tegishli kod so'z. Bundan tashqari, $\Gamma(g, L)$ ichida C' ga masofa $\leq t$ bo'lgan yagona kod so'z mavjudligi ma'lum, chunki 1-teoremaga ko'ra, Goppa kod so'zlarining minimal masofasi $2t + 1$ ga teng (5-rasmga qarang). Chunki, e ning og‘irligi t ga teng, $C' + e$ ga masofa $\leq t$ bo‘lgan yagona kod so‘zdir.



5-rasm. Qora nuqtalar Goppa kod so‘zlarini ifodalaydi. Har bir qora doiraning ichki qismi xatoni tuzatish jarayonida uning markazidagi qora nuqtaga akslangan so‘zlar to‘plamini anglatadi. Ushbu rasm Classic McEliece shifrlashining intuitsiyasini ko‘rsatadi: xatolik vektori e ba’zi bir Goppa kod so‘zining atrofidagi qora doira ustida joylashgan C' nuqtasiga shifrlanadi. Qabul qiluvchi mos markazdagi qora nuqtani olish orqali xatolik vektori e ni tiklash imkoniyatiga ega bo‘ladi.

Maxfiy Goppa parametrlarini bilgan holda, qabul qiluvchi sindromni dekodlash algoritmini, masalan, Patterson algoritmini [16] ishlatib, C' ga eng yaqin kod so‘zini topadi va $c = C' + e$ ni oladi. So‘ngra, oddiy qo‘shish orqali $e = C' + c$ natijasiga erishiladi. Ushbu qadamlar 27-algoritmda umumlashtirilgan.

Shuni ta’kidlash kerakki, umumiy sindromni dekodlash qiyinligi yuqorida ko‘rsatildi. Shuning uchun, maxfiy Goppa parametrlarini bilmagan uchinchi tomon bu deshifrlash qadamini amalga oshirolmaydi.

27-algoritm Classic McEliece PKE Decryption: *dec*.

Kirish: shifrmatn $\boldsymbol{C} \in \mathbb{F}_2^{\boldsymbol{n-k}}$, Goppa kodi $\boldsymbol{\Gamma(g, L)}$.

1. $\boldsymbol{C}$ ni $\boldsymbol{k}$ ta nol qo‘shib $\boldsymbol{C}' = (\boldsymbol{C}, \boldsymbol{0}, \cdots, \boldsymbol{0}) \in \mathbb{F}_2^{\boldsymbol{n}}$ ga kengaytirish.
2. $\boldsymbol{C}'$dan $\leq \boldsymbol{t}$ masofada bo‘lgan unikal $\boldsymbol{c} \in \boldsymbol{\Gamma(g, L)}$ kod so‘zni topish. Agar bunday kod so‘z bo‘lmasa, $\perp$ qaytarish.
3. $\boldsymbol{e} = \boldsymbol{C}' + \boldsymbol{c}$ o‘rnatish
4. Agar $\boldsymbol{weight(e)} \neq \boldsymbol{t}$ yoki $\boldsymbol{C} \neq \boldsymbol{He}$ bo‘lsa, $\perp$ qaytarish.

Chiqish: xabar $\boldsymbol{e}$.

Classic McEliece KEM kalit generatsiyasi (28-algoritm) qo‘shimcha qiymat $\sigma \in \mathbb{F}_2^n$ ni tanlaydi. Shunga qaramay, kalit generatsiyasi PKE kalit generatsiyasiga o‘xshashdir.

28-algoritm Classic McEliece KEM Key Generation.

Kirish: Yo‘q.

1. $\boldsymbol{\sigma} \in \mathbb{F}_2^{\boldsymbol{n}}$ ni tasodifiy generatsiyalash.
2. $\left(\boldsymbol{H}, \boldsymbol{\Gamma(g, L)}\right) = \boldsymbol{PKE.keyGen}()$ generatsiyalash.

Chiqish: ochiq kalit $\boldsymbol{H}$, shaxsiy kalit $\boldsymbol{sk} = (\boldsymbol{\Gamma(g, L)}, \boldsymbol{\sigma})$.

Kriptografik xesh funksiyalar oilasi H_i ($i \in \{0,1,2\}$) ham enkapsulyatsiya, ham dekapsulyatsiya uchun ishlatiladi. Tasodifiy vektor $e \in \mathbb{F}_2^n$ og‘irligi t bo‘lgan holda tanlanadi va berilgan PCM H bilan shifrlanadi. Bundan tashqari, e ma’lumot e_H ga xeshlanadi. Umumiy maxfiy kalit K quyidagi tarzda hisoblanadi: $K = H_1(e, C, e_H)$ ya’ni, e va C ga bog‘liq bo‘lgan tasodifiy ko‘rinishga ega bo‘lgan qiymat (29-algoritm).

29-algoritm Classic McEliece KEM Encapsulation.
Kirish: ochiq kalit $\boldsymbol{H}$. 1. Og‘irligi $\boldsymbol{t}$ ga teng $\boldsymbol{e} \in \mathbb{F}_2^n$ tasodifiy vektorni generatsiyalash. 2. $\boldsymbol{C} = \boldsymbol{PKE.enc}(\boldsymbol{e}, \boldsymbol{H})$ hisoblash. 3. $\boldsymbol{e_H} = \boldsymbol{H_2}(\boldsymbol{e})$ hisoblash. 4. $\boldsymbol{K} = \boldsymbol{H_1}(\boldsymbol{e}, \boldsymbol{C}, \boldsymbol{e_H})$ hisoblash. **Chiqish:** inkapsulyatsiya $(\boldsymbol{C}, \boldsymbol{e_H})$, umimiy kalit $\boldsymbol{K}$.

Dekapsulyatsiya jarayoni (30-algoritm) berilgan C ni deshifrlash bilan boshlanadi, shu orqali nomzod xabar e hisoblanadi. Agar kiritish joiz bo‘lsa, asl e olinadi. Shubhasiz, $K = \boldsymbol{H_1}(\boldsymbol{e}, \boldsymbol{C}, \boldsymbol{e_H})$ orqali inkapsulyatsiyada olingan kabi bir xil umumiy maxfiy kalit hisoblanadi.

Biroq, ushbu hisoblashdan oldin, dekapsulyatsiya jarayoni o‘z kirish qiymatini tekshirish uchun ikki usuldan foydalanadi: Agar deshifrlash muvaffaqiyatsiz bo‘lsa, e'_H xesh qiymati e o‘rniga tasodifiy ko‘rinishga ega bo‘lgan σ asosida hisoblanadi. Bu keyingi taqqoslash muvaffaqiyatli bo‘lmasligini ta’minlaydi. Olingan nomzod xabar nomzod e uning og‘irligi t ga teng vektor ekanligini tekshirish orqali tasdiqlanadi (bu $PKE.dec$ jarayonida sodir bo‘ladi). Shundan so‘ng, taqdim etilgan $\boldsymbol{e_H}$ hisoblangan e'_H versiyasi bilan solishtiriladi va shu orqali encapsulyatsiya haqiqatan ham e taqdim etilgan ochiq kalit H va algoritm qoidalariga muvofiq bajarilganligi tekshiriladi.

30-algoritm Classic McEliece KEM Decapsulation.
Kirish: shaxsiy kalit $\boldsymbol{sk} = (\boldsymbol{\Gamma}(\boldsymbol{g}, \boldsymbol{L}), \boldsymbol{\sigma})$, inkapsulyatsiya $(\boldsymbol{C}, \boldsymbol{e_H})$. 1. $\boldsymbol{e} = \boldsymbol{PKE.dec}\big(\boldsymbol{C}, \boldsymbol{\Gamma}(\boldsymbol{g}, \boldsymbol{L})\big)$ hisoblanadi. 2. Agar $\boldsymbol{e} = \perp$ bo‘lsa, $\boldsymbol{e'_H} = \boldsymbol{H_2}(\boldsymbol{\sigma})$ hisoblanadi. 3. Agar $\boldsymbol{e} \neq \perp$ bo‘lsa, $\boldsymbol{e'_H} = \boldsymbol{H_2}(\boldsymbol{e})$ hisoblanadi. 4. Agar $\boldsymbol{e'_H} = \boldsymbol{e_H}$ bo‘lsa, $\boldsymbol{K} = \boldsymbol{H_1}(\boldsymbol{e}, \boldsymbol{C}, \boldsymbol{e_H})$ o‘rnatiladi. 5. Agar $\boldsymbol{e'_H} \neq \boldsymbol{e_H}$ bo‘lsa, $\boldsymbol{K} = \boldsymbol{H_0}(\boldsymbol{\sigma}, \boldsymbol{C}, \boldsymbol{e_H})$ o‘rnatiladi. **Chiqish:** umimiy kalit $\boldsymbol{K}$.

Shifrlash va deshifrlash amallari panjaraga asoslangan kriptografiyaga nisbatan sezilarli darajada tez; ammo, Classic McEliece algoritmida kalit o‘lchamlari ancha katta [17]. Masalan, eng katta parametr to‘plami ko‘rib chiqilsa (6-jadvalga qarang), siqilgan ochiq kalit H ni saqlash uchun k·(n−k)=6528·(8192−6528)=10,862,592 bit ≈ 1,3 MB xotira talab etiladi.

Classic McEliece na’munalari va ularga mos parametr variantlari 1.6-jadvalda ko‘rsatilgan.

1.6-jadval

Klassic McEliece parametrlar to‘plamlari xatolarni tuzatish qobiliyati t ga ega bo‘lgan (n, k, d) Goppa kodidan foydalanadi

	$\boldsymbol{n}$	$\boldsymbol{k}$	$\boldsymbol{d}$	$\boldsymbol{t}$
McEliece348864	3488	2720	129	64
McEliece460896	4608	3360	193	96
McEliece6688128	6688	5024	257	128
McEliece6960119	6960	5413	239	119
McEliece8192128	8192	6528	257	128

Rainbow

Rainbow imzo sxemasi [18] ehtimoliy eng keng tarqalgan ko‘p o‘zgaruvchili imzo sxemasi bo‘lgan Unbalanced Oil and Vinegar (UOV) sxemasi bilan yaqin bog‘liq. Rainbowni tushunish uchun, avvalo, UOV ni to‘g‘ri tushunish taab etiladi.

UOV ning asosiy g‘oyasi markaziy akslantirish $\mathcal{F}$ ning o‘zgaruvchilar to‘plamini ikki o‘zaro kesishmaydigan bo‘limga ajratishdan iborat bo‘lib, bular oil (neft) va vinegar (sirka) o‘zgaruvchilar deb ataladi. Eng muhim xususiyat shundaki, $\mathcal{F}$ ning kvadratik polinomlari ikki oil o‘zgaruvchisi o‘rtasida cross-term (aralash ko‘paytuvchilar) bo‘lishiga ruxsat bermaydi. UOV umumiy holda ochiq va yopiq kalitlarni tez hisoblashni taklif qiladi hamda sodda strukturasi bilan ajralib turadi. Lekin uning kamchiligi kalitlarning nisbatan katta o‘lchamida namoyon bo‘ladi.

UOV sxemasi MPKC sxemasi sifatida tavsiflanadi, yuqorida tasvirlanganidek, ochiq akslantirish $\mathcal{P} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{S}: \mathbb{F}^n \to \mathbb{F}^k$ va shaxsiy polinomial akslantirishlari $(\mathcal{T}, \mathcal{F}, \mathcal{S})$ bilan. Bu sxema oil va vinegar o‘zgaruvchilarining sonini aniqlovchi o va v butun parametrlar bilan tavsiflanadi. Ushbu parametrlar markaziy akslantirish $\mathcal{F}$ tuzilishini belgilaydi, bu yerda, $k = o$ polinomial funksiyalar va $n = o + v$ o‘zgaruvchilar mavjud. Markaziy akslantirish $\mathcal{F}: \mathbb{F}^n \to \mathbb{F}^k$ o‘z navbatida k ta polinom funksiyalar $f_1, \dots, f_k$ dan tashkil topgan. Ular bir rangli shaklga keltiriladi, ya’ni, konstanta va chiziqli hadlar tashlab yuboriladi. U holda har bir f_r quyidagi ko‘rinishga ega bo‘ladi:

$$f_r = \sum_{i=1}^{v} \sum_{j=i}^{v} \alpha_{ij}^{(r)} x_i x_j + \sum_{i=1}^{v} \sum_{j=v+1}^{n} \beta_{ij}^{(r)} x_i x_j$$

Bu yerda, $x_1, \cdots, x_v$ va $x_{v+1}, \cdots, x_n$ mos holda vinegar va oil o‘zgaruvchilari. $\mathcal{F}$ markaziy akslantirish $\mathbb{F}$ dan $\alpha_{ij}^{(r)}$, $\beta_{ij}^{(r)}$ koeffitsientlariga tasodifiy qiymatlar tayinlash orqali generatsiya qilinadi.

Affin o‘zgartirishlar $\mathcal{S}$ va $\mathcal{T}$ ham tasodifiy koeffitsientlarni tayinlash orqali tanlanadi, agar ularning o‘zgaruvchilari teskari qiymatga ega bo‘lmasa, bu jarayon takrorlanadi. Markaziy akslantirish $\mathcal{F}$ bo‘yicha asl obrazlarni hisoblash quyidagicha amalga oshiriladi:

1-qadam: Vinegar o‘zgaruvchilarga $x_1, \dots, x_k$ (qizil bilan ajratilgan) tasodifiy qiymatlar tayinlanadi. Bu jarayon vinegar o‘zgaruvchilar o‘rtasidagi ko‘paytma natijasini doimiyga qisqartiradi, shuningdek, oil va vinegar o‘zgaruvchilarning ko‘paytmasini chiziqli hadga aylantiradi:

$$f_r = \sum_{i=1}^{v}\sum_{j=i}^{v}\alpha_{ij}^{(r)}x_i x_j + \sum_{i=1}^{v}\sum_{j=v+1}^{n}\beta_{ij}^{(r)}x_i x_j.$$

2-qadam: Buning natijasida $n - v = k$ o‘zgaruvchi, ya’ni $x_{v+1}, \cdots, x_n$ uchun k ta chiziqli tenglamalar sistemasi hosil bo‘ladi. Gaus qisqartirishini qo‘llash orqali bu sistemani yechib, qolgan oil qiymatlari $x_{v+1}, \cdots, x_n$ aniqlanadi. Agar sistema yechimga ega bo‘lmasa, vinegar o‘zgaruvchilar uchun boshqa tasodifiy qiymatlar tanlash orqali jarayon takrorlanadi.

Yuqorida aytilganidek, bu MPKC konstruktsiyasi berilgan ochiq akslantirish P bo‘yicha asl obrazlarni topishni qiyinlashtiradigan tarzda ishlab chiqilgan. Ammo, shaxsiy dekompozitsiya $\mathcal{P} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{S}$ ni bilgan holda asl obrazlarni samarali hisoblash (masalan, imzo yaratish) mumkin bo‘ladi.

Rainbow imzo sxemasi UOV kontseptsiyasini umumlashtiradi. Rainbow ikki sathli Oil–Vinegar polinomlaridan tashkil topgan bo‘lib, ikkinchi sath birinchi qavatdagi barcha o‘zgaruvchilarni o‘z ichiga oladi, ya’ni ikkinchi sathdagi vinegar o‘zgaruvchilar to‘plamiga birinchi sathdagi barcha o‘zgaruvchilardan tashkil topadi.

Rainbow’ning aniq na’munasi quyidagi parametrlar orqali aniqlanadi. Birinchi sath uchun vinegar o‘zgaruvchilar soni v_1. Birinchi va ikkinchi qavatlar uchun oil o‘zgaruvchilar soni o_1 va o_2. Umumiy o‘zgaruvchilar soni $n = v_1 + o_1 + o_2$ va tenglamalar soni $k = o_1 + o_2$ formula orqali aniqlanadi. Rainbowsning markaziy akslantirish $\mathcal{F}$ ning natijaviy strukturasi quyidagi ikki sathdan iborat:

$$\text{1-sath:} \quad \underbrace{x_1, \dots, x_{v_1}}_{vinegar\ o‘zgaruvchilar}, \underbrace{x_{v_1+1}, \dots, x_{v_1+o_1}}_{oil\ o‘zgaruvchilar}$$

$$\text{2-sath:} \quad \underbrace{x_1, \dots, x_{v_1}, x_{v_1+1}, \dots, x_{v_1+o_1}}_{vinegar\ o‘zgaruvchilar}, \underbrace{x_{v_1+o_1+1}, \dots, x_{v_1+o_1+o_2}}_{oil\ o‘zgaruvchilar}$$

Bu konstruktsiya UOV holatidagi imzo o‘lchami va xabar o‘lchami o‘rtasidagi nisbati $(v + o)/o$ dan ikki sathli Rainbow holatida $(v_1 + o_1 + o_2)/(o_1 + o_2)$ ga yaxshilanadi, chunki, $v_1 < v$. Ya’ni, amalda imzolar nisbatan kichikroq bo‘ladi (bu taxminan 26% qisqarishni anglatadi [19]). Birinchi sathda kerakli koeffitsientlar sonining qisqarishi tufayli, bu xususiyat shuningdek, xususiy kalit hajmini ham kichikroq qiladi. Biroq, so‘nggi hujumlar ushbu konstruktsiyani zaif ekanligini ko‘rsatdi, bu esa mazkur samaradorlik yutuqlarining yo‘qolishiga olib keldi (quyida keltiriladi).

Aniq kalit juftligini yaratish uchun (31-algoritm), quyidagi akslantirishlar tanlab olinadi:

- Shaxsiy markaziy $\mathcal{F}$ akslantirish $k = o_1 + o_2$ ta ko‘phad $f_1, \dots, f_k$ dan tashkil topgan bo‘lib, ularning har biri quyidagi ko‘rinishga ega:

$$f_r = \begin{cases} r \in \{1, \cdots, o_1\}\ uchun \displaystyle\sum_{i \le j \in V_1} \alpha_{ij}^{(r)} x_i x_j + \sum_{i \in V_1, j \in O_1} \beta_{ij}^{(r)} x_i x_j \\ r \in \{o_1 + 1, \cdots, o_1 + o_2\}\ uchun \displaystyle\sum_{i \le j \in V_2} \gamma_{ij}^{(r)} x_i x_j + \sum_{i \in V_2, j \in O_2} \delta_{ij}^{(r)} x_i x_j \end{cases}$$

Birinchi sath, vinegar indekslari $V_1 = \{1, \cdots, v_1\}$, oil indekslari $O_1 = \{v_1 + 1, \cdots, v_1 + o_1\}$, ikkinchi qatlam, vinegar indekslari $V_2 = V_1 \cup O_1$ va oil indekslari $O_2 = \{o_1 + 1, \cdots, o_1 + o_2\}$.

Koeffitsiyent $\alpha_{ij}^{(r)}, \beta_{ij}^{(r)}, \gamma_{ij}^{(r)}$ va $\delta_{ij}^{(r)}$ lar $\mathbb{F}$ maydondan tasodifiy tanlanadi.

- Ikki maxfiy tasodifiy tanlangan teskarisiga ega affina akslantirish: $\mathcal{T}: \mathbb{F}^k \to \mathbb{F}^k$ va $\mathcal{S}: \mathbb{F}^n \to \mathbb{F}^n$. Bu akslantirishlarning koeffitsiyentlari $\mathbb{F}$ maydondan tasodifiy tanlanadi. Agar akslantirishlar teskarisiga ega bo‘lmasa, jarayon qayta amalga oshiriladi.
- Ochiq kalit: $\mathcal{P} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{S}: \mathbb{F}^n \to \mathbb{F}^k$.

31-algoritm Rainbow Key Generation.
Kirish: Yo‘q. 1. $\boldsymbol{\mathcal{S}} \in \mathbb{F}^{\boldsymbol{n}} \to \mathbb{F}^{\boldsymbol{n}}$ tanlanadi. 2. $\boldsymbol{\mathcal{F}} \in \mathbb{F}^{\boldsymbol{n}} \to \mathbb{F}^{\boldsymbol{k}}$ tanlanadi. 3. $\boldsymbol{\mathcal{T}} \in \mathbb{F}^{\boldsymbol{k}} \to \mathbb{F}^{\boldsymbol{k}}$ tanlanadi. 4. $\boldsymbol{\mathcal{P}} = \boldsymbol{\mathcal{T}} \circ \boldsymbol{\mathcal{F}} \circ \boldsymbol{\mathcal{S}} \in \mathbb{F}^{\boldsymbol{n}} \to \mathbb{F}^{\boldsymbol{k}}$ hisoblanadi. **Chiqish:** ochiq kalit $\boldsymbol{\mathcal{P}}$, shaxsiy kalit $\boldsymbol{sk} = (\boldsymbol{\mathcal{T}}, \boldsymbol{\mathcal{F}}, \boldsymbol{\mathcal{S}})$.

Yuqorida tasvirlanganidek, berilgan $m \in \{0,1\}^*$ uzunlikdagi xabar uchun haqiqiy imzo s - bu $\mathcal{P}$ ostida $H(m)$ ning asl obrazi hisoblanadi, ya’ni, $\mathcal{P}(s) = H(m)$ tenglamasi bajariladi, bunda $H: \{0,1\}^* \to \mathbb{F}^k$ mos keluvchi kriptografik xesh funksiyasi. Akslantirishlar $\mathcal{S}$ va $\mathcal{T}$ samarali tarzda teskari hisoblanganligi sababli, ularning ostida asl obrazlarni topish oson. Markaziy akslantirish $\mathcal{F}$ ostida asl obrazlarni topish esa UOV sxemasidagi kabi amalga oshiriladi:

- birinchi sath vinegar o‘zgaruvchilarini tasodifiy tanlash, ya’ni $x_1, \cdots, x_{v_1}$:
  - 1-sath: $\underbrace{x_1, \dots, x_{v_1}}_{vinegar\ o‘zgaruvchilar}, \underbrace{x_{v_1+1}, \dots, x_{v_1+o_1}}_{oil\ o‘zgaruvchilar}$
- birinchi sath oil o‘zgaruvchilarining qiymatlarini topish: hosil bo‘lgan o_1 ta tenglamalarning chiziqli sistemasi yechib, birinchi sath uchun o_1 ta oil o‘zgaruvchilarining aniq qiymatlari hisoblanadi.
- birinchi sathdan olingan qiymatlarni, ya’ni, $x_1, \dots, x_{v_1+o_1}$, ikkinchi sath tenglamalariga qo‘llash:
  - 2-sath: $\underbrace{x_1, \dots, x_{v_1}, x_{v_1+1}, \dots, x_{v_1+o_1}}_{vinegar\ o‘zgaruvchilar}, \underbrace{x_{v_1+o_1+1}, \dots, x_{v_1+o_1+o_2}}_{oil\ o‘zgaruvchilar}$
- ikkinchi sathdagi oil o‘zgaruvchilarining qiymatlarini topish: hosil bo‘lgan o_2 ta tenglamalarning chiziqli sistemasini yechib, ikkinchi sathning qolgan oil o‘zgaruvchilarining aniq qiymatlari hisoblanadi.
- tenglama yechimi yo‘q bo‘lsa: Agar chiziqli tizimlardan biri uchun yechim topilmasa, jarayon birinchi sath vinegar o‘zgaruvchilarining boshqa tasodifiy qiymatlarini tanlashdan boshlanadi.

Xabar m uchun $\mathcal{P}$ ostida haqiqiy imzoni hisoblash H funksiyasi yordamida xabarni xeshlash va keyin maxfiy akslantirishlar $\mathcal{T}$, $\mathcal{F}$ va $\mathcal{S}$ ostida asl obrazlarni topish orqali amalga oshiriladi (32-algoritm).

32-algoritm Rainbow Signature generation.
Kirish: shaxsiy kalit $\boldsymbol{sk} = (\boldsymbol{\mathcal{T}}, \boldsymbol{\mathcal{F}}, \boldsymbol{\mathcal{S}})$, xabar $\boldsymbol{m} \in \{\mathbf{0}, \mathbf{1}\}^*$. 1. $\boldsymbol{m_H} = \boldsymbol{H}(\boldsymbol{m})$ hisoblanadi. 2. $\boldsymbol{u} = \boldsymbol{\mathcal{T}}^{-\mathbf{1}}(\boldsymbol{m_H})$ hisoblanadi. 3. $\boldsymbol{\mathcal{F}}$ ostida $\boldsymbol{u}$ ning asl obrazi $\boldsymbol{u}^{-\mathbf{1}}$ topiladi. 4. $\boldsymbol{s} = \boldsymbol{\mathcal{S}}^{-\mathbf{1}}(\boldsymbol{u}^{-\mathbf{1}})$ hisoblanadi. **Chiqish:** imzo $\boldsymbol{s}$.

$m \in \{0,1\}^*$ xabar va $s \in \mathbb{F}^n$ imzo berilgan bo‘lsin. Agar $H(m) = \mathcal{P}(s)$ o‘rinli bo‘lsa, s imzo haqiqiy, aks holda imzo haqiqiy emas (33-algoritm).

33-algoritm Rainbow Verification.
Kirish: ochiq kalit $\boldsymbol{\mathcal{P}}$, xabar $\boldsymbol{m} \in \{\mathbf{0}, \mathbf{1}\}^*$, imzo $\boldsymbol{s} \in \mathbb{F}^{\boldsymbol{n}}$. 1. $\boldsymbol{m'_H} = \boldsymbol{\mathcal{P}}(\boldsymbol{s})$ hisoblanadi. 2. $\boldsymbol{m_H} = \boldsymbol{H}(\boldsymbol{m})$ hisoblanadi. **Chiqish:** agar $\boldsymbol{m'_H} = \boldsymbol{m_H}$ imzo haqiqiy, aks holda haqiqiy emas.

Rainbow parametrlarining mos keluvchi variantlari 1.7-jadvalda keltirilgan.

1.7-jadval

Rainbowning uchinchi raund parametrlari quyidagicha

	$\mathbb{F}$	$\boldsymbol{v_1}$	$\boldsymbol{o_1}$	$\boldsymbol{o_2}$
Level I	GF(16)	36	32	32
Level III	GF(256)	68	32	48
Level V	GF(256)	96	36	64

Rainbow xavfsizlik masalalari

2022-yil fevral oyida Ward Beullens tomonidan o‘tkazilgan hujum [20] Rainbow algoritmiga qarshi oldindan ma’lum bo‘lgan hujumlar samaradorligini sezilarli darajada oshirdi. Ushbu yutuq asosan oldin ishlab chiqilgan to‘rtburchakli MinRank hujumi [21] va yaxshilangan faraz qilish texnikasining kombinatsiyasidan kelib chiqadi. Ushbu hujumga qarshi turish uchun Rainbow parametrlarini standart va yaxshiroq tushunilgan UOV yondashuvi parametrlaridan ham oshirib yuborish talab etiladi. Bu esa Rainbow algoritmini UOV bilan solishtirganda afzal ko‘rishni savol ostida qoldiradi, chunki Rainbowning keltiradigan samaradorlik yutug‘i qo‘shimcha murakkablikka nisbatan juda kichik.

Hujumning mohiyati: Rainbow xavfsizlik modeliga qarshi ishlatilgan yangi hujum usuli yanada kuchliroq va samaraliroq bo‘ldi, bu esa parametrlarni kattalashtirish zaruratini yuzaga keltiradi.

UOV ustunligi: Soddalashtirilgan tuzilmasi va kamroq murakkabligi tufayli UOV usuli Rainbow bilan raqobatda sezilarli afzalliklarga ega bo‘lib qolmoqda.

Amaliy xulosa: Rainbow algoritmi murakkabligi va kattaroq parametr talablari sababli qo‘llaniladigan amaliy sohalarda o‘zining qulayligini yo‘qotishi mumkin.

Amaliy bajarish uchun vazifalar

1. Kyber algoritmini kichik sonlarda amalga oshiring?
2. Saber algoritmini kichik sonlarda amalga oshiring?
3. Dilithium algoritmini kichik sonlarda amalga oshiring?

4. Falcon algoritmini kichik sonlarda amalga oshiring?
5. Klassic McEliece algoritmini kichik sonlarda amalga oshiring?

Adabiyot va Internet saytlar:

1. Avanzi, R.; Bos, J.; Ducas, L.; Kiltz, E.; Lepoint, T.; Lyubashevsky, Schanck, J.M.; Schwabe, P.; Seiler, G.; Stehlé, D. CRYSTALS-KYBER: Algorithm Specifications and Supporting Documentation; Version 3.02. Available online: https://pq-crystals.org/kyber/data/kyber-specification-round3-20210804.pdf (accessed on 1 July 2022).
2. Fujisaki, E.; Okamoto, T. Secure Integration of Asymmetric and Symmetric Encryption Schemes. J. Cryptol. 2013, 26, 80–101 [CrossRef]
3. Hofheinz, D.; Hövelmanns, K.; Kiltz, E. A Modular Analysis of the Fujisaki-Okamoto Transformation. In Theory of Cryptography; Kalai, Y., Reyzin, L., Eds.; Lecture Notes in Computer Science; Springer International Publishing: Cham, Switzerland, 2017; Volume 10677, pp. 341–371. [CrossRef]
4. Basso, A.; Bermudo Mera, J.M.; D'Anvers, J.P.; Karmakar, A.; Roy, S.S.; Van Beirendonck, M.; Vercauteren, F. SABER: Mod-LWR Based KEM (Round 3 Submission). Available online: https://www.esat.kuleuven.be/cosic/pqcrypto/saber/files/saberspecround3.pdf (accessed on 1 July 2022).
5. Bai, S.; Ducas, L.; Kiltz, E.; Lepoint, T.; Lyubashevsky, V.; Schwabe, P.; Seiler, G.; Stehlé, D. CRYSTALS-Dilithium: Algorithm Specifications And Supporting Documentation. Version 3.1. Available online: https://pq-crystals.org/dilithium/data/dilithium-specification-round3-20210208.pdf (accessed on 1 July 2022).
6. Lyubashevsky, V. Lattice signatures without trapdoors. In Proceedings of the EUROCRYPT 2012—31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lecture Notes in Computer Science, Cambridge, UK, 15–19 April 2012; Pointcheval, D., Schaumont, P., Eds.; Springer: Cambridge, UK, 2012; Volume 7237, pp. 738–755. [CrossRef]
7. Bai, S.; Galbraith, S.D. An Improved Compression Technique for Signatures Based on Learning with Errors. In Topics in Cryptology – CT-RSA 2014, Proceedings of the Cryptographer's Track at the RSA Conference 2014, San Francisco, CA, USA, 25–28 February 2014; Benaloh, J., Ed.; Springer International Publishing: Cham, Switzerland, 2014; pp. 28–47.
8. Chen, C.; Danba, O.; Hoffstein, J.; Hülsing, A.; Rijneveld, J.; Schanck, J.M.; Schwabe, P.; Whyte, W.; Zhang, Z. NTRU: Algorithm Specifications and Supporting Documentation; Version September 2020. Available online: https://csrc.nist.gov/CSRC/media/Projects/post-quantum-cryptography/documents/round-3/submissions/NTRU-Round3.zip (accessed on 1 July 2022).
9. Fouque, P.A.; Hoffstein, J.; Kirchner, P.; Lyubashevsky, V.; Pornin, T.; Prest, T.; Ricosset, T.; Seiler, G.; Whyte, W.; Zhang, Z. Falcon: Fast-Fourier Lattice-Based Compact Signatures over NTRU. Version 1.2. Available online: https://falcon-sign.info/falcon.pdf (accessed on 1 July 2022).
10. Gentry, C.; Peikert, C.; Vaikuntanathan, V. Trapdoors for Hard Lattices

and New Cryptographic Constructions. Cryptology ePrint Archive, Report 2007/432. 2007. Available online: https://ia.cr/2007/432 (accessed on 1 July 2022).
11. Ajtai, M. Generating Hard Instances of the Short Basis Problem; Springer: Berlin/Heidelberg, Germany, 1999.
12. Babai, L. On Lovász' lattice reduction and the nearest lattice point problem. Combinatorica 1986, 6, 1–13. [CrossRef]
13. Ducas, L.; Prest, T. Fast Fourier Orthogonalization. Cryptology ePrint Archive, Report 2015/1014. 2015. Available online: https://ia.cr/2015/1014 (accessed on 1 July 2022).
14. Albrecht, M.R.; Bernstein, D.J.; Chou, T.; Cid, C.; Gilcher, J.; Lange, T.; Maram, V.; von Maurich, I.; Misoczki, R.; Niederhagen, R.; et al. Classic McEliece: Conservative Code-Based Cryptography. Version October 2020. Available online: https://classic. mceliece.org/nist/mceliece-20201010.pdf (accessed on 1 July 2022).
15. Niederhagen, R.; Waidner, M. Practical Post-Quantum Cryptography; Fraunhofer SIT: Darmstadt, Germany, 2017.
16. Sardinas, A.; Patterson, C. A necessary sufficient condition for the unique decomposition of coded messages. IRE Internat. Conv. Rec. 1953, 104–108.
17. Niederreiter, H.; Xing, C. Algebraic Geometry in Coding Theory and Cryptography; Princeton University Press: Princeton, NJ, USA, 2009.
18. Ding, J.; Chen, M.S.; Petzoldt, A.; Schmidt, D.; Yang, B.Y. Rainbow—Algorithm Specification and Documentation, The 3rd Round Proposal. Available online: https://csrc.nist.gov/CSRC/media/Projects/post-quantum-cryptography/documents/round-3/submissions/Rainbow-Round3.zip (accessed on 1 July 2022).
19. Thomae, E. About the Security of Multivariate Quadratic Public Key Schemes. Ph.D. Thesis, Universitätsbibliothek, Ruhr-Universität Bochum, Bochum, Germany, 2013; pp. 84–85.
20. Beullens, W. Breaking Rainbow Takes a Weekend on a Laptop. Cryptology ePrint Archive. 2022. Available online: https://ia.cr/2022/214 (accessed on 1 July 2022).
21. Beullens, W. Improved Cryptanalysis of UOV and Rainbow. Cryptology ePrint Archive, Report 2020/1343. 2020. Available online: https://ia.cr/2020/1343 (accessed on 1 July 2022).

2-amaliy ish. OPEN QUANTUM SAFE (OQS): LIBOQS KUTUBXONASI (2 soat)

Amaliy ishning maqsadi – post kvant kriptografiyasi algoritmlaridan amalda foydalanish boʻyicha koʻnikmalarni shakllantirishdan iborat.

Nazariy qism

Open Quantum Safe — ochiq manbali loyihadir va u kvant kompyuterlarining rivojlanishi tufayli klassik kriptografiya xavfsizligini taʼminlashga yordam berish uchun moʻljallangan. Loyiha yangi kvantbardosh (post-quantum) kriptografik algoritmlarni ishlab chiqish, sinovdan oʻtkazish va amaliyotga joriy etishga qaratilgan.

OQS loyihasi 2016-yilda tashkil etilgan boʻlib, uning asosiy maqsadi klassik internet protokollarida kvantbardosh kriptografiyani tatbiq qilishdir.

Liboqs — OQS loyihasi doirasidagi kvantbardosh algoritmlarni sinash va ishlatish uchun yaratilgan ochiq manbali kutubxona. U oʻzida NISTning kvantbardosh kriptografiya standartlashtirish jarayonida tavsiya etilgan algoritmlarni va boshqa muhim usullarni jamlagan.

Liboqs kutubxonasining asosiy xususiyatlari:

Kvantbardosh algoritmlarni qoʻllab-quvvatlash:

KEM (Key Encapsulation Mechanisms): Kalitlarni inkapsulyatsiyalash mexanizmlari.

Digital Signatures: Raqamli imzolar.

Algoritmlar roʻyxati: Liboqs NISTning 3-chi raund algoritmlarini qoʻllab-quvvatlaydi, jumladan:

Kyber (KEM)

Dilithium (raqamli imzo)

Falcon (raqamli imzo)

NTRU (KEM)

Rainbow (imzo, lekin keyinchalik NIST tomonidan chiqarib tashlangan)

TLS bilan integratsiya:

Liboqs OpenSSL bilan integratsiya qilinadi, bu esa kvantbardosh TLS protokollari orqali xavfsiz aloqa oʻrnatish imkonini beradi.

Kross-platformali:

Linux, macOS va Windows platformalarida ishlashga moslashgan.

Liboqsning asosiy funksiyalari:

Kalitlar almashinuvi:

Kvantbardosh algoritmlar yordamida xavfsiz kalitlar almashinuvini taʼminlaydi.

Raqamli imzo:

Post-quantum algoritmlar asosida xavfsiz imzo tizimlarini amalga oshiradi.

Integratsiya va sinov:

Kriptografik tizimlarni kvantbardosh kriptografiyaga moslashtirishda ishlatiladi.

Liboqsdan foydalanish sohalari:

Internet xavfsizligi:

HTTPS, VPN va boshqa protokollarni kvantbardosh holga keltirish.

IoT qurilmalari:

Kvant xavfsizligini talab qiluvchi cheklangan resurslarga ega qurilmalar.

Moliyaviy xizmatlar:

Kvant tahdidlariga qarshi mustahkam tranzaksiya tizimlari.

Liboqsni o‘rnatish va foydalanish:

Kutubxonani yuklab olish: Liboqs GitHub orqali yuklab olinadi: Open Quantum Safe GitHub

OpenSSL bilan ishlatish: Liboqs OpenSSL bilan integratsiya qilinib, kvantbardosh protokollarning sinovdan o‘tishini ta’minlaydi.

Dasturlash tilini qo‘llab-quvvatlash: Liboqs C va Python kabi tillar orqali foydalanish uchun API interfeyslarini taqdim etadi.

Amaliy qism

1. https://github.com/open-quantum-safe/liboqs manzildagi berilgan ma’lumotlar bilan tanishib chiqib, liboqs kutubxonasini o‘rnatish tartibi bilan tanishib chiqing va o‘rnatishni amalga oshiring.
2. Talab etilgan shaklda, statik yoki dinamik kutubxona shaklda amalga oshirib, C dasturlash tilida foydalanish uchun integratsiya qiling.

Amaliy bajarish uchun vazifalar.

1. Classic McEliece kalitni inkapsulyatsiyalash algoritmining turli shakllarini ishlatib ko‘ring.
2. Kyber kalitni inkapsulyatsiyalash algoritmining turli shakllarini ishlatib ko‘ring.
3. CRYSTALS-Dilithium elektron raqamli imzo sxemasini ishlatib ko‘ring.
4. SPHINCS+-SHA2 elektron raqamli imzo sxemasini ishlatib ko‘ring.

Adabiyot va Internet saytlar:

1. https://github.com/open-quantum-safe - Open Quantum Safe
2. https://openquantumsafe.org/ - Open Quantum Safe

V-BO‘LIM.

KEYSLAR BANKI

V. KEYSLAR BANKI

1-keys mavzusi: “Post kvant kriptografiyasidan foydalanish tartibini tushunish”

Vaziyat tavsifi: Axborot xavfsizligi mutaxassisi sifatida sizdan post kvant kriptografiyasini tashkilot faoliyatiga tadbiq etishni afzallik va kamchliklarini so‘rashdi.

Keys savollari:

1) Post kvant kriptografiyasi xususiyatlarini SWOT usulidan foydalanib tahlil qiling?
2) Mavjud post kvant kriptografiyasi algortmlarining xususiyatlarini quyidagi jadval bo‘yicha ajrating:

№	**Algoritm nomi**	**Algoritm turi**	**Asoslangan matematik muammo**
1			
2			
3			
4			

3) Post kvant kriptografiyasidan foydalanilmasa, kuzatiladigan oqibatlarni ularning sabablarini ko‘rsatga holda izohlang.

№	**Sabab**	**Oqibat**
1		
2		
3		
4		

2-keys mavzusi: “Post kvan kriptografiyasi haqida olingan bilimlarni aniqlash”

Vaziyat tavsifi: Dars so‘ngida post kvant kriptografiyasi haqida tinglovchilar qanday darajada bilimlarni o‘zlashtirganligini aniqlash.

Keys savollari:

1) “KWHL” metodi yordamida buni amalga oshiring:

“KWHL” metodi	
1. Nimalarni bilaman: -	***2. Nimalarni bilishni xohlayman, nimalarni bilishim kerak:*** -
3. ***Qanday qilib bilib va topib olaman:*** -	***5. Nimalarni bilib oldim:*** -

VI BO'LIM.

GLOSSARIY

VI. GLOSSARIY

Tushuncha O‘zbek tilida	Tushunchaning o‘zbek tilidagi sharhi	Tushuncha ingliz tilida
xeshga asoslangan kriptografiya	Xesh-funksiyalarning xavfsizligiga asoslangan kriptografik primitiv tuzilmalar uchun umumiy atama.	hash-based cryptography
kodlarga asoslangan kriptografiya	Post-kvant kriptografiyasining eng istiqbolli yo‘nalishlaridan biri bo‘lib, xatolikni tuzatish kodlaridan foydalanishga asoslangan kriptografik tizimlarni yaratish yondashuvini amalga oshiradi.	code-based cryptography
postkvant kriptografiyasi	Kvant kompyuterlari yordamida kriptografik tizimlarning hujumlarga dosh berish qobiliyatini baholash, shuningdek, bunday hujumlarga chidamli kriptografik tizimlarni sintez qilish bilan bog‘liq bo‘lgan kriptografiya bo‘limi.	post-quantum cryptography
kvant bit, kubit	Kvant hisoblashlar uchun qo‘llaniladigan kvant kompyuteridagi eng kichik axborot birligi (oddiy kompyuterdagi bitning analogi)	quantum bits, qubits
kvant chalkashligi	Kvant olamining noyob xususiyati, bunda zarralar (bir-biri bilan o‘zaro bog‘liq, ya’ni chalkash) bir-birlarini uzoqdan “his qilishlari” va boshqa zarrachaning holatidagi o‘zgarishlarga javoban o‘z holatlarini bir zumda o‘zgartirishlari mumkin.	quantum entanglement
kvant kalitlarini taqsimlash	Xavfsiz aloqani ta’minlash uchun kvant hodisalaridan foydalanadigan kalitni uzatish usuli.	quantum key distribution
kvant kriptografiyasi	Kvant mexanikasi tamoyillariga asoslangan axborotni kriptografik himoyalash usullarini ishlab chiqish va qo‘llash bilan bog‘liq kriptografiya bo‘limi.	quantum cryptography
kvant superpozitsiyasi	Zarra yoki kvant tizimini bir vaqtning ozida bir nechta holatda mavjud bo‘lishiga imkon beradigan	quantum superposition

	kvant mexanikasining fundamental printsipi	
kvant-bardoshli algoritmlar	Kvant hisoblashga asoslangan hujumlarga chidamli assimetrik kriptografik algoritmlar oilasi.	quantum-resistant algorithms
elektron raqamli imzo, ERI	elektron hujjatdagi mazkur elektron hujjat axborotini ERIning yopiq kalitidan foydalangan holda maxsus o‘zgarishlar natijasida hosil qilingan hamda ERIning ochiq kaliti yordamida elektron hujjatdagi axborotda xatolik mavjud emasligini aniqlash va ERI kalitining egasini identifikatsiya qilish imkonini beradigan imzo.	electronic digital signature, EDS
teskari matrisa	Matritsaga nisbatan teskari bo‘lgan kvadrat matritsa.	reverse matrix
Galua maydoni	Elementlarning chekli to‘plamidan iborat bo‘lgan maydon.	Galois field
diskret logarifm muammosi	Katta chekli maydonlarda logarifmni izlash matematik masalasi.	discrete logarithm problem
elliptik egri chiziqli diskret logarifm muammosi	mR = Q shartni qanoatlantiruvchi *m* sonini izlash, bu yerda R va Q – elliptik egri chiziqdagi *x*- va *y*-koordinata nuqtalari.	elliptic curve disc-rete logarithm problem
elliptik egri chiziq usulida tub ko‘paytuvchilarga ajratish	Murakkab butun n sonining asosiy faktori r ni aniqlash maqsadida r modulga ega bo‘lgan nuqtalar soni faqat kichik faktorga bo‘linadigan elliptik egri chiziqni topish usuli bilan tub ko‘paytuvchilarga ajratish maxsus algoritmi.	elliptic curve method
Faktorlashtirish	Butun sonni oddiy ko‘paytuvchilarga ajratish.	Factoring
eksponensial vaqt	Parametr uzunligi (masalan, kalit uzunligi)ga eksponensial bog‘liq bo‘lgan algoritm murakkabligi.	exponential time
nolinchi oshkoralik protokoli	Kriptografik protokol bo‘lib, bunda bir tomon boshqasiga biror narsaning haqiqat ekanligini oshkor etmasdan turib isbotlaydi.	zero knowledge protocol

VII BO‘LIM.

ADABIYOTLAR RO‘YXATI

VII. ADABIYOTLAR RO'YXATI

I. O'zbekiston Respublikasi Prezidentining asarlari:

1. Mirziyoyev SH.M. Buyuk kelajagimizni mard va olijanob xalqimiz bilan birga quramiz. – T.: "O'zbekiston", 2017. – 488 b.
2. Mirziyoyev SH.M. Milliy taraqqiyot yo'limizni qat'iyat bilan davom ettirib, yangi bosqichga ko'taramiz. 1-jild. – T.: "O'zbekiston", 2017. – 592 b.
3. Mirziyoyev SH.M. Xalqimizning roziligi bizning faoliyatimizga berilgan eng oliy bahodir. 2-jild. –T.: "O'zbekiston", 2018. – 507 b.
4. Mirziyoyev SH.M. Niyati ulug' xalqning ishi ham ulug', hayoti yorug' va kelajagi farovon bo'ladi. 3-jild.– T.: "O'zbekiston", 2019. – 400 b.
5. Mirziyoyev SH.M. Milliy tiklanishdan – milliy yuksalish sari. 4-jild.– T.: "O'zbekiston", 2020. – 400 b.

II. Normativ-huquqiy hujjatlar:

6. O'zbekiston Respublikasining Konstitusiyasi.–T.:O'zbekiston, 2018.
7. O'zbekiston Respublikasining 2020-yil 23-sentabrda qabul qilingan "Ta'lim to'g'risida"gi O'RQ-637-sonli Qonuni.
8. O'zbekiston Respublikasi Prezidentining 2017-yil 7-fevral "O'zbekiston Respublikasini yanada rivojlantirish bo'yicha Harakatlar strategiyasi to'g'risida"gi 4947-sonli Farmoni.
9. O'zbekiston Respublikasi Prezidentining 2018-yil 21-sentabr "2019-2021 yillarda O'zbekiston Respublikasini innovatsion rivojlantirish strategiyasini tasdiqlash to'g'risida"gi PF-5544-sonli Farmoni.
10. O'zbekiston Respublikasi Prezidentining 2019-yil 27-may "O'zbekiston Respublikasida korrupsiyaga qarshi kurashish tizimini yanada takomillashtirish chora-tadbirlari to'g'risida"gi PF-5729-son Farmoni.
11. O'zbekiston Respublikasi Prezidentining 2019-yil 27-avgust "Oliy ta'lim muassasalari rahbar va pedagog kadrlarining uzluksiz malakasini oshirish tizimini joriy etish to'g'risida"gi PF-5789-sonli Farmoni.
12. O'zbekiston Respublikasi Prezidentining 2019-yil 8-oktabr "O'zbekiston Respublikasi oliy ta'lim tizimini 2030-yilgacha rivojlantirish konsepsiyasini tasdiqlash to'g'risida"gi PF-5847-sonli Farmoni.
13. O'zbekiston Respublikasi Prezidentining 2024-yil 15-avgustdagi "O'zbekiston Respublikasida kriptologiya sohasida ta'lim va ilm-fanni rivojlantirish bo'yicha qo'shimcha chora-tadbirlar to'g'risida"gi PQ-293-son Qarori.
14. O'zbekiston Respublikasi Prezidenti Shavkat Mirziyoyevning 2020-yil 25-yanvardagi Oliy Majlisga Murojaatnomasi.
15. O'zbekiston Respublikasi Vazirlar Mahkamasining 2001-yil 16-avgustdagi "Oliy ta'limning davlat ta'lim standartlarini tasdiqlash to'g'risida"gi

343-sonli Qarori.

16. O‘zbekiston Respublikasi Vazirlar Mahkamasining 2015-yil 10-yanvardagi “Oliy ta’limning Davlat ta’lim standartlarini tasdiqlash to‘g‘risida”gi 2001-yil 16-avgustdagi “343-sonli qororiga o‘zgartirish va qo‘shimchalar kiritish haqida”gi 3-sonli qarori.

III. Maxsus adabiyotlar:

17. Richter M. et al. A mathematical perspective on post-quantum cryptography //Mathematics. – 2022. – T. 10. – №. 15. – C. 2579.

18. Akbarov D. Y. “Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qo‘llanilishi” – Toshkent, 2008 – 394 bet.

IV. Internet saytlar:

19. http://edu.uz – O‘zbekiston Respublikasi Oliy va o‘rta maxsus ta’lim vazirligi.

20. http://lex.uz – O‘zbekiston Respublikasi Qonun hujjatlari ma’lumotlari milliy bazasi.

21. http://bimm.uz – Oliy ta’lim tizimi pedagog va rahbar kadrlarini qayta tayyorlash va ularning malakasini oshirishni tashkil etish Bosh ilmiy-metodik markazi.

22. http://ziyonet.uz – Ta’lim portali ZiyonET.

23. http://natlib.uz – Alisher Navoiy nomidagi O‘zbekiston Milliy kutubxonasi.

24. https://csrc.nist.gov/projects/post-quantum-cryptography - Post-Quantum Cryptography