Ilmiy tadqiqotlar va ularning yechimlari jurnali
Aoka guvohnoma № 323759 ISSN: 3060-4818

POST-KVANT KRIPTOGRAFIYASI

Zavqiyev Suxrob Sunnatulayevich
https://doi.org/10.5281/zenodo.21993193

ANNOTATSIYA.

Mazkur maqolada post-kvant kriptografiyasining shakllanish sabablari, kvant kompyuterlarining klassik kriptografik algoritmlarga ta’siri hamda kvantga chidamli kriptografik yondashuvlar tahlil qilinadi. Ishda panjaraga asoslangan, kodga asoslangan, ko‘p o‘zgaruvchili va xeshga asoslangan algoritmlar sinfi nazariy va amaliy jihatdan ko‘rib chiqiladi. Shuningdek, post-kvant kriptografiyada xavfsizlik modellari, standartlashtirish jarayonlari va real axborot tizimlariga joriy etish bilan bog‘liq muammolar yoritiladi. Tadqiqot natijalari post-kvant kriptografiyaning kvant kompyuterlar davrida axborot xavfsizligini ta’minlashdagi muhim rolini ko‘rsatadi.

KALIT SO‘ZLAR: post-kvant kriptografiya, kvant kompyuterlar, kriptografik algoritmlar, axborot xavfsizligi, lattice-based kriptografiya, kodga asoslangan kriptografiya, raqamli imzo, standartlashtirish

KIRISH

So‘nggi o‘n yilliklarda raqamli texnologiyalarning jadal rivojlanishi axborot almashinuvi hajmini keskin oshirdi. Internet tarmoqlari, elektron hukumat tizimlari, onlayn bank xizmatlari hamda bulutli hisoblash platformalari kundalik hayotning ajralmas qismiga aylandi. Ushbu tizimlarning barchasi axborotning maxfiyligi, yaxlitligi va autentifikatsiyasini ta’minlash uchun kriptografik mexanizmlarga tayanadi. Hozirgi kunda keng qo‘llanilayotgan RSA, DSA va elliptik egri chiziqlarga asoslangan algoritmlar klassik hisoblash modellari sharoitida yetarli darajada xavfsiz deb hisoblanib kelindi.

Biroq kvant hisoblash texnologiyalarining rivojlanishi ushbu yondashuvlarga nisbatan jiddiy xavotirlarni yuzaga chiqardi. Ilmiy tadqiqotlarda ko‘rsatib o‘tilishicha, yetarlicha quvvatga ega kvant kompyuterlar paydo bo‘lsa, mavjud ochiq kalitli kriptografiya algoritmlarining asosini tashkil etuvchi matematik muammolar qisqa vaqt ichida yechilishi mumkin. Bu holat nafaqat kelajakdagi, balki hozir saqlanayotgan shifrlangan ma’lumotlar uchun ham real tahdid hisoblanadi. Shu sababli kriptografiya sohasida uzoq muddatli xavfsizlikni ta’minlash masalasi dolzarb ilmiy muammoga aylandi.

Aynan shu nuqtada post-kvant kriptografiyasi tushunchasi paydo bo‘ldi. Post-kvant kriptografiyasi kvant kompyuterlar imkoniyatlarini hisobga olgan holda ishlab chiqilgan va ularga chidamli bo‘lishi kutilayotgan kriptografik algoritmlar majmuasini anglatadi. Muhim jihati shundaki, bu algoritmlar kvant kompyuterlarda emas, balki mavjud klassik hisoblash muhitida ishlashga mo‘ljallangan. Bu esa ularni amaldagi axborot tizimlariga nisbatan osonroq joriy etish imkonini beradi.

So‘nggi yillarda post-kvant kriptografiyasi bo‘yicha olib borilgan tadqiqotlar ko‘lami sezilarli darajada kengaydi. Lattice-based, code-based, multivariate hamda hash-based algoritmlar kabi bir nechta asosiy yo‘nalishlar shakllandi.

Post-kvant kriptografiyaning ahamiyati faqat nazariy tadqiqotlar bilan cheklanib qolmaydi. Bugungi kunda xalqaro tashkilotlar va standartlashtirish institutlari ushbu algoritmlarni tanlash va baholash jarayonlarini faol olib bormoqda. Xususan, ochiq kalitli kriptografiyaning kelajak avlodini

belgilash masalasi global miqyosda muhokama qilinmoqda. Bu jarayon axborot xavfsizligi strategiyalarini qayta ko‘rib chiqishni va uzoq muddatli himoya yondashuvlarini ishlab chiqishni talab etadi.

Mazkur maqolaning asosiy maqsadi post-kvant kriptografiyasining nazariy va amaliy jihatlarini tahlil qilish, kvant kompyuterlarining mavjud kriptografik tizimlarga ta’sirini ko‘rsatish hamda kvantga chidamli algoritmlarning afzallik va cheklovlarini yoritishdan iborat. Maqolada zamonaviy ilmiy manbalarga tayangan holda post-kvant kriptografiyaning hozirgi holati, rivojlanish tendensiyalari va amaliy joriy etish istiqbollari muhokama qilinadi.

KVANT KOMPYUTERLARINING KLASSIK KRIPTOGRAFIYAGA TAHDIDI

Klassik kriptografik tizimlarning aksariyati hisoblash nuqtayi nazaridan murakkab bo‘lgan matematik masalalarga asoslanadi. Ushbu masalalar an’anaviy kompyuterlar uchun amaliy jihatdan yechilmas deb qaraladi, chunki ularni hisoblash uchun juda katta vaqt yoki resurs talab etiladi. Masalan, RSA algoritmi katta butun sonlarni faktorizatsiya qilish muammosiga, elliptik egri chiziqlarga asoslangan kriptografiya esa diskret logarifm masalasiga tayangan holda ishlaydi. Hozirgi kungacha bu muammolar klassik hisoblash modelida yetarli darajada ishonchli himoya mexanizmi sifatida xizmat qilib kelmoqda.

Biroq kvant kompyuterlar ushbu yondashuvni tubdan o‘zgartirishi mumkin. Kvant hisoblash kvant mexanikasining superpozitsiya va chigallik (entanglement) kabi xususiyatlariga asoslanadi. Natijada kvant kompyuterlar ayrim turdagi hisoblash masalalarini klassik kompyuterlarga nisbatan ancha tez bajarish imkoniyatiga ega bo‘ladi. Ayniqsa, kriptografiya sohasida mashhur bo‘lgan Shor algoritmi katta sonlarni faktorizatsiya qilish va diskret logarifm masalalarini polinomial vaqt ichida yechishga qodir ekani bilan e’tiborni tortadi.

Shor algoritmining mavjudligi ochiq kalitli kriptografiya uchun fundamental tahdid hisoblanadi. Agar yetarli miqdordagi kvant bitlarga ega bo‘lgan barqaror kvant kompyuter yaratilsa, RSA va ECC kabi algoritmlarning maxfiy kalitlarini ochish amaliy jihatdan mumkin bo‘lib qoladi. Bu esa nafaqat yangi shifrlangan ma’lumotlar, balki ilgari shifrlanib saqlangan arxivlar uchun ham xavf tug‘diradi. Amaliyotda bu holat “hozir yig‘ib, keyin yechish” (harvest now, decrypt later) strategiyasi orqali izohlanadi, ya’ni hujumchi bugun shifrlangan ma’lumotni saqlab, kelajakda kvant kompyuter yordamida uni ochishi mumkin.

Simmetrik kriptografiya kvant hujumlariga nisbatan nisbatan barqarorroq hisoblanadi. Grover algoritmi simmetrik kalitli shifrlash tizimlarida kalitni topish jarayonini tezlashtirishi mumkin bo‘lsa-da, bu tahdid kalit uzunligini oshirish orqali qisman bartaraf etiladi. Masalan, 256 bitli simmetrik kalitlar kvant hujumlari sharoitida ham amaliy jihatdan xavfsiz deb qaraladi. Shunga qaramay, ochiq kalitli kriptografiya tizimlari kvant hisoblash ta’sirida jiddiy qayta ko‘rib chiqilishini talab qiladi.

Ilmiy tadqiqotlarda qayd etilishicha, kvant kompyuterlarning ommaviy amaliyotga joriy etilishi hali vaqt talab qilsa-da, tayyorgarlik jarayonlarini kechiktirish xavfli bo‘lishi mumkin. Kriptografik infratuzilmalarni to‘liq almashtirish uzoq vaqt va katta resurs talab etadi. Shu sababli ko‘plab mutaxassislar kvant kompyuterlar yetarli darajada rivojlanishidan oldinroq muqobil, kvantga chidamli kriptografik yechimlarga o‘tishni tavsiya etmoqda.

Natijada, kvant kompyuterlarning klassik kriptografiyaga bo‘lgan tahdidi post-kvant kriptografiyasining shakllanishiga asosiy turtki bo‘ldi. Ushbu tahdidni inkor etish yoki kechiktirish

o‘rniga, unga moslashgan yangi kriptografik yondashuvlarni ishlab chiqish axborot xavfsizligini uzoq muddatli ta’minlashning muhim sharti hisoblanadi.

POST-KVANT KRIPTOGRAFIYASI TUSHUNCHASI VA UMUMIY YONDASHUVLAR

Post-kvant kriptografiyasi kvant kompyuterlar sabab yuzaga keladigan xavfsizlik muammolariga javob sifatida shakllangan zamonaviy kriptografiya yo‘nalishidir. Ushbu yondashuvning asosiy g‘oyasi shundan iboratki, kriptografik algoritmlar kvant hisoblash imkoniyatlariga ega bo‘lgan hujumchilarga qarshi ham barqaror bo‘lishi lozim. Shu bilan birga, post-kvant algoritmlar amaldagi klassik kompyuterlarda samarali ishlashi va mavjud axborot infratuzilmasiga mos kelishi talab etiladi. An’anaviy kriptografiyada xavfsizlik ko‘pincha aniq matematik muammolarning murakkabligiga tayanadi. Post-kvant kriptografiyasida esa bu yondashuv qayta ko‘rib chiqiladi va kvant algoritmlar yordamida tez yechilmaydigan muammolar tanlanadi.

Post-kvant kriptografiyasining muhim afzalliklaridan biri — uning texnologik jihatdan nisbatan moslashuvchanligidir. Kvant kriptografiyasi bilan solishtirilganda, post-kvant algoritmlar maxsus kvant aloqa kanallari yoki fizik qurilmalarni talab qilmaydi. Bu esa ularni dasturiy ta’minot darajasida joriy etish imkonini beradi. Natijada bank tizimlari, davlat axborot resurslari va internet protokollarida bosqichma-bosqich yangilanishlar amalga oshirilishi mumkin.

Shu bilan birga, post-kvant kriptografiyasi yagona algoritm yoki yagona yondashuv bilan cheklanmaydi. Aksincha, bu soha bir nechta mustaqil, ammo o‘zaro raqobatlashuvchi algoritmik oilalardan tashkil topgan. Har bir algoritm sinfi o‘zining xavfsizlik modeli, hisoblash murakkabligi va amaliy samaradorligi bilan farqlanadi. Masalan, ayrim algoritmlar yuqori darajadagi nazariy xavfsizlikni taklif etsa, boshqalari amaliy tezlik va resurs tejamkorligi bilan ajralib turadi. Post-kvant kriptografiyani joriy etishda muhim masalalardan biri — xavfsizlik baholash jarayonidir. Klassik kriptografiyada ko‘p yillar davomida sinovdan o‘tgan ishonch modellari mavjud bo‘lsa, post-kvant algoritmlar nisbatan yangi bo‘lgani sababli ularni uzoq muddatli tahlil qilish zarur. Shu sababli ilmiy hamjamiyatda ushbu algoritmlarni ochiq muhokama qilish, kriptotahlil qilish va turli hujum modellarida sinovdan o‘tkazish muhim ahamiyat kasb etadi. Natijada, post-kvant kriptografiyasi bugungi kunda faqat nazariy muammo emas, balki amaliy ehtiyoj sifatida qaralmoqda. Kvant kompyuterlarning to‘liq yetuk bosqichga yetib kelishini kutmasdan, ularga chidamli kriptografik mexanizmlarni ishlab chiqish va joriy etish axborot xavfsizligini uzoq muddat davomida ta’minlash uchun muhim strategik qaror hisoblanadi.

POST-KVANT KRIPTOGRAFIYADA XAVFSIZLIK MODELLARI VA MATEMATIK ASOSLAR

Post-kvant kriptografiyaning ishonchliligi bevosita uning matematik asoslari va xavfsizlik modellari bilan bog‘liq. Har qanday kriptografik tizim singari, post-kvant algoritmlar ham aniq taxminlarga asoslanadi. Ushbu taxminlar kvant hisoblash imkoniyatlariga ega bo‘lgan hujumchilar uchun ham murakkab bo‘lishi lozim. Shu sababli xavfsizlikni baholashda nafaqat klassik, balki kvant hujum modellari ham hisobga olinadi. Post-kvant kriptografiyada xavfsizlik modellari odatda “kvantga chidamlilik” tushunchasi bilan ifodalanadi. Bu tushuncha algoritmning kvant kompyuter yordamida ham samarali buzilmasligini anglatadi. Amaliy jihatdan bu holat algoritm asosidagi matematik muammoning kvant algoritmlar yordamida tez yechilmasligi bilan bog‘liq. Masalan, panjaralarga asoslangan kriptografiyada ishlatiladigan ayrim masalalar uchun hozirgi kungacha Shor algoritmiga o‘xshash

samarali kvant yechimlar topilmagan. Matematik asoslar nuqtayi nazaridan post-kvant kriptografiya bir nechta mustaqil nazariy yo‘nalishlarga tayangan holda rivojlanmoqda. Panjara nazariyasida vektorlarning ma’lum fazoda eng qisqa yoki eng yaqin nuqtalarini topish kabi masalalar ko‘rib chiqiladi. Ushbu masalalar yuqori o‘lchamli fazolarda nihoyatda murakkab bo‘lib, klassik va kvant algoritmlar uchun ham katta hisoblash resurslarini talab qiladi. Shu sababli ular kriptografik konstruktsiyalar uchun mustahkam asos sifatida qaraladi.

Xavfsizlikni baholash jarayonida yana bir muhim jihat — formal isbotlardir. Ko‘plab post-kvant algoritmlar xavfsizligi yaxshi o‘rganilgan matematik muammolarga qisqartiriladi. Bu shuni anglatadiki, agar asosiy muammo yechilmasa, unga asoslangan kriptografik sxema ham buzilmaydi. Bunday qisqartirishlar kriptografik tizimlarning nazariy ishonchliligini oshiradi va ularni ilmiy jihatdan asoslash imkonini beradi. Kvant hujum modellarida hujumchi klassik va kvant resurslarining turli kombinatsiyalariga ega bo‘lishi mumkin. Masalan, ayrim modellar hujumchining faqat kvant hisoblash imkoniyatlariga ega ekanini nazarda tutsa, boshqalari kvant xotira yoki kvant tarmoqlar mavjudligini ham hisobga oladi. Shu sababli post-kvant kriptografiyada xavfsizlik tushunchasi bir xil emas, balki bir nechta darajalarda baholanadi. Bu holat algoritmlarni solishtirish va tanlash jarayonini murakkablashtiradi. Natijada, post-kvant kriptografiyaning matematik asoslari va xavfsizlik modellari ushbu sohaning eng muhim va murakkab qismi hisoblanadi. Algoritmlarning amaliy samaradorligi qanchalik yuqori bo‘lmasin, agar ularning xavfsizlik asoslari yetarlicha isbotlanmagan bo‘lsa, uzoq muddatli foydalanish uchun mos deb hisoblanmaydi. Shu bois, nazariy tadqiqotlar post-kvant kriptografiyaning barqaror rivojlanishida hal qiluvchi rol o‘ynaydi.

PANJARAGA ASOSLANGAN (LATTICE-BASED) KRIPTOGRAFIYA

Panjaraga asoslangan kriptografiya post-kvant kriptografiyasi yo‘nalishlari orasida eng ko‘p o‘rganilgan va amaliy jihatdan istiqbolli hisoblanadi. Ushbu yondashuvning asosi yuqori o‘lchamli panjaralarda uchraydigan murakkab matematik masalalarga tayanadi. Panjara deganda, ko‘p o‘lchamli fazoda ma’lum qoidalar asosida joylashgan nuqtalar to‘plami tushuniladi. Bunday fazolarda ayrim muammolarni yechish klassik va kvant kompyuterlar uchun ham nihoyatda murakkab bo‘lib qolmoqda.

Lattice-based kriptografiyada eng ko‘p qo‘llaniladigan masalalar qatoriga Shortest Vector Problem (SVP) va Learning With Errors (LWE) kiradi. SVP masalasi panjaradagi eng qisqa nol bo‘lmagan vektorni topish bilan bog‘liq bo‘lsa, LWE masalasi shovqin qo‘shilgan chiziqli tenglamalar tizimini yechishni talab qiladi. Tadqiqotlar shuni ko‘rsatadiki, ushbu masalalar uchun hozirgi kungacha samarali kvant algoritmlar mavjud emas, bu esa ularni post-kvant kriptografiya uchun mustahkam asosga aylantiradi.

Panjaraga asoslangan yondashuvning muhim afzalliklaridan biri — uning ko‘p funksiyali ekanligidir. Lattice-based usullar yordamida shifrlash, raqamli imzo, kalit almashish va hatto gomomorf shifrlash sxemalarini qurish mumkin. Bu esa yagona matematik asosda turli kriptografik vazifalarni bajarish imkonini beradi. Aynan shu xususiyat panjara asosidagi algoritmlarning keng qo‘llanilishiga sabab bo‘lmoqda. Amaliy jihatdan panjaraga asoslangan post-kvant algoritmlar orasida CRYSTALS-Kyber va CRYSTALS-Dilithium alohida o‘rin tutadi. Ushbu algoritmlar xavfsizlik, tezlik va kalit hajmi o‘rtasidagi muvozanatni nisbatan yaxshi ta’minlaydi. Shu sababli ular xalqaro standartlashtirish jarayonlarida yetakchi nomzodlar sifatida qaralmoqda. Biroq, bu algoritmlarning murakkab matematik tuzilishi ularni to‘liq tushunish va to‘g‘ri joriy etishni qiyinlashtirishi mumkin.

Shu bilan birga, lattice-based kriptografiyaning ayrim cheklovlari ham mavjud. Eng asosiy muammolardan biri kalit va imzo hajmining klassik kriptografiyaga nisbatan kattaroq bo‘lishidir. Bu holat resurslari cheklangan qurilmalar, masalan, IoT tizimlarida qo‘llashni murakkablashtiradi. Bundan tashqari, noto‘g‘ri parametr tanlash yoki implementatsiya xatolari xavfsizlikka jiddiy ta’sir ko‘rsatishi mumkin. Umuman olganda, panjaraga asoslangan kriptografiya post-kvant kriptografiyasining markaziy yo‘nalishlaridan biri sifatida shakllanib bo‘ldi. Nazariy jihatdan mustahkamligi va amaliy imkoniyatlari uni kvant kompyuterlar davrida ochiq kalitli kriptografiyaning asosiy nomzodiga aylantirmoqda. Shu sababli ushbu yo‘nalish bo‘yicha tadqiqotlar va tajribaviy joriy etish ishlari jadal davom etmoqda.

KODGA ASOSLANGAN (CODE-BASED) POST-KVANT KRIPTOGRAFIYA

Kodga asoslangan kriptografiya post-kvant kriptografiyasining eng qadimgi va eng barqaror yo‘nalishlaridan biri hisoblanadi. Ushbu yondashuvning asosi xatolarni tuzatish kodlari nazariyasiga borib taqaladi. Dastlab bu g‘oya aloqa kanallarida xatolarni aniqlash va tuzatish maqsadida ishlab chiqilgan bo‘lsa-da, keyinchalik uning kriptografik jihatdan ham yuqori darajada ishonchli ekani aniqlandi. Kodga asoslangan kriptografiya uzoq yillar davomida kriptotahlilga bardosh berib kelgani sababli, post-kvant davrida muhim nomzod sifatida qaralmoqda.

Mazkur yo‘nalishdagi eng mashhur kriptotizim McEliece sxemasi hisoblanadi. Ushbu tizim umumiy holda chiziqli kodlarning dekodlash masalasiga asoslanadi. Dekodlash masalasi tasodifiy xatolar mavjud bo‘lgan kod so‘zidan asl xabarni tiklashni talab qiladi va bu masala yuqori o‘lchamli fazolarda juda murakkab hisoblanadi. Muhimi shundaki, bu muammo uchun hozirgi kungacha samarali kvant algoritmlar aniqlanmagan, bu esa McEliece sxemasini kvant hujumlariga nisbatan barqaror qiladi. Kodga asoslangan kriptografiyaning muhim afzalligi — uning xavfsizlik tarixidir. Ushbu yo‘nalish qariyb yarim asr davomida faol o‘rganilgan bo‘lib, ko‘plab kriptotahlil urinishlariga qaramay, asosiy g‘oyalar saqlanib qolgan. Bu holat kodga asoslangan tizimlarga nisbatan ishonchni oshiradi. Ayniqsa, uzoq muddatli maxfiylik talab etiladigan tizimlarda bunday ishonchlilik muhim ahamiyat kasb etadi.

Shu bilan birga, kodga asoslangan post-kvant algoritmlar jiddiy amaliy cheklovlarga ham ega. Eng katta muammolardan biri ochiq kalit hajmining juda katta bo‘lishidir. Ayrim sxemalarda ochiq kalitlar bir necha yuz kilobayt yoki undan ham katta bo‘lishi mumkin. Bu esa tarmoq orqali uzatish, saqlash va resurslari cheklangan qurilmalarda qo‘llashni murakkablashtiradi. Natijada, bunday algoritmlar barcha tizimlar uchun universal yechim sifatida qaralmasligi mumkin. Kodga asoslangan kriptografiyada ham turli optimallashtirish va takomillashtirish ishlari olib borilmoqda. Kalit hajmini kamaytirish, hisoblash tezligini oshirish va implementatsiya murakkabligini pasaytirish bo‘yicha ko‘plab takliflar mavjud. Biroq bu jarayonda xavfsizlikdan voz kechmaslik muhim hisoblanadi, chunki har qanday soddalashtirish yangi zaifliklarga olib kelishi mumkin.

KO‘P O‘ZGARUVCHILI (MULTIVARIATE) KRIPTOGRAFIK TIZIMLAR

Ko‘p o‘zgaruvchili kriptografik tizimlar post-kvant kriptografiyasining nisbatan murakkab, ammo qiziqarli yo‘nalishlaridan biri hisoblanadi. Ushbu yondashuv ko‘p o‘zgaruvchili kvadrat polinomlar tizimini yechish masalasiga asoslanadi. Umumiy holda, bunday tenglamalar tizimini yechish matematik jihatdan juda murakkab bo‘lib, hatto kichik o‘lchamlar uchun ham katta hisoblash resurslarini talab etadi. Shu sababli bu masala kriptografik maqsadlar uchun mos deb qaraladi. Multivariate kriptografiyada xavfsizlik asosi sifatida NP-murakkab masalalar qaraladi. Polinom tenglamalar tizimini yechish klassik

hisoblashda ham, kvant hisoblashda ham samarali bajarilishi hozircha noma'lum. Aynan shu jihat ushbu yo'nalishni post-kvant sharoitida istiqbolli variantlardan biriga aylantiradi. Ko'p o'zgaruvchili tizimlar asosan raqamli imzo sxemalarida qo'llaniladi, chunki ular tezkor imzolash va tekshirish jarayonlarini ta'minlay oladi.

Ushbu yo'nalishning muhim afzalliklaridan biri — imzo yaratish jarayonining tezligidir. Ayrim multivariate sxemalar resurslari cheklangan qurilmalarda ham nisbatan samarali ishlashi mumkin. Shu bilan birga, imzo uzunligi ko'pincha maqbul darajada bo'lib, tarmoq orqali uzatishda katta muammo tug'dirmaydi. Bu holat ularni real vaqt tizimlari yoki katta miqdordagi imzolar talab etiladigan muhitlar uchun qiziqarli variantga aylantiradi. Biroq ko'p o'zgaruvchili kriptografik tizimlar bilan bog'liq jiddiy muammolar ham mavjud. Tarixan, ushbu yo'nalishdagi ko'plab taklif etilgan algoritmlar keyinchalik kriptotahlil natijasida buzilgan yoki zaif tomonlari aniqlangan. Bu holat multivariate kriptografiyaga nisbatan ehtiyotkorlik bilan yondashishni talab qiladi. Ayniqsa, parametrlarni noto'g'ri tanlash yoki matematik tuzilmani yetarlicha chuqur tahlil qilmaslik xavfsizlikni keskin pasaytirishi mumkin. Shu sababli zamonaviy tadqiqotlarda multivariate algoritmlarni baholashda konservativ yondashuv qo'llanilmoqda. Yangi sxemalar keng jamoatchilik tomonidan uzoq muddat sinovdan o'tkazilmasdan turib, amaliy tizimlarga joriy etilmaydi. Bu esa ilmiy hamjamiyatda ochiq muhokama va mustaqil tahlilning ahamiyatini yana bir bor ko'rsatadi. Umuman olganda, ko'p o'zgaruvchili kriptografik tizimlar post-kvant kriptografiyasining muhim, ammo ehtiyotkorlikni talab qiladigan yo'nalishidir. Ular yuqori tezlik va samaradorlikni taklif qilishi mumkin, biroq xavfsizlik nuqtayi nazaridan chuqur va uzoq muddatli tadqiqotlar zarur. Shu sababli bu yo'nalish hozircha asosiy yechimdan ko'ra, muqobil variant sifatida ko'proq qaralmoqda.

XESHGA ASOSLANGAN (HASH-BASED) RAQAMLI IMZOLAR

Xeshga asoslangan raqamli imzolar post-kvant kriptografiyasining eng sodda va nazariy jihatdan eng ishonchli yo'nalishlaridan biri hisoblanadi. Ushbu yondashuv kriptografik xesh-funksiyalarning bir tomonlama xossalariga tayanadi. Xesh-funksiyalar uchun hozirgi kungacha samarali kvant algoritmlar topilmaganligi sababli, ular kvant hujumlariga nisbatan barqaror deb qaraladi. Shu jihatdan, hash-based imzolar post-kvant davrida ishonchli muqobil sifatida e'tirof etiladi. Xeshga asoslangan imzo sxemalarining asosiy g'oyasi oddiy: xabar qisqa xesh qiymatga o'tkaziladi va ushbu qiymat maxfiy kalit yordamida imzolanadi. Xavfsizlik to'liq holda xesh-funksiyaning kolliziya va preimage hujumlariga chidamliligiga bog'liq bo'ladi. Kvant hisoblash sharoitida ham xesh-funksiyalar nisbatan barqaror bo'lib qoladi, chunki Grover algoritmi ta'siri kalit uzunligini oshirish orqali qisman kompensatsiya qilinishi mumkin. Tarixan, xeshga asoslangan imzo sxemalari bir martalik yoki cheklangan miqdorda imzo qo'yish uchun mo'ljallangan edi. Bunday yondashuvlar amaliy jihatdan noqulay bo'lsa-da, ular yuqori darajadagi nazariy xavfsizlikni ta'minlagan. Keyinchalik Merkle daraxtlari kabi konstruksiyalar yordamida ushbu cheklov qisman bartaraf etildi va ko'p martalik imzo qo'yish imkoniyati yaratildi. Bu esa hash-based imzolarni real tizimlarda qo'llash imkoniyatini kengaytirdi.

Zamonaviy post-kvant kriptografiyada SPHINCS+ kabi sxemalar xeshga asoslangan imzolarni yangi bosqichga olib chiqdi. Ushbu algoritmlar holatga bog'liq bo'lmagan (stateless) tuzilishga ega bo'lib, implementatsiya jarayonini ancha soddalashtiradi. Shu bilan birga, ular yuqori darajadagi xavfsizlikni ta'minlash bilan birga, foydalanish jarayonida kamroq xatolik ehtimolini keltirib chiqaradi. Biroq xeshga asoslangan imzolar ham ayrim amaliy cheklovlarga ega. Eng asosiy kamchiliklardan biri

imzo hajmining nisbatan katta bo‘lishidir. Bu holat tarmoq orqali tez-tez imzo uzatiladigan tizimlarda ma’lum noqulayliklar tug‘dirishi mumkin. Shuningdek, imzo yaratish va tekshirish jarayonlari ayrim hollarda boshqa post-kvant sxemalarga nisbatan sekinroq bo‘lishi mumkin.

GOMOMORF SHIFRLASH VA POST-KVANT KRIPTOGRAFIYA

Gomomorf shifrlash kriptografiyaning eng murakkab va shu bilan birga eng istiqbolli yo‘nalishlaridan biri hisoblanadi. Ushbu yondashuv shifrlangan ma’lumotlar ustida ularni ochmasdan turib hisob-kitoblar bajarish imkonini beradi. Natijada, hisoblash jarayonida ma’lumotlarning maxfiyligi saqlanib qoladi. So‘nggi yillarda gomomorf shifrlash texnologiyalari, ayniqsa, bulutli hisoblash va tashqi serverlarda ma’lumotlarni qayta ishlash jarayonlarida muhim ahamiyat kasb etmoqda.

Post-kvant kriptografiya doirasida gomomorf shifrlash asosan panjaraga asoslangan matematik modellarga tayanadi. Buning asosiy sababi shundaki, lattice-based muammolar kvant hujumlariga nisbatan barqaror deb qaraladi va ular yordamida murakkab kriptografik konstruktsiyalarni qurish mumkin. Learning With Errors kabi masalalar gomomorf shifrlash sxemalarining xavfsizlik poydevorini tashkil etadi. Shu jihatdan, post-kvant gomomorf shifrlash klassik gomomorf yondashuvlarga nisbatan uzoq muddatli xavfsizlikni ta’minlashga qaratilgan. Gomomorf shifrlashning post-kvant muhitdagi ahamiyati ayniqsa ma’lumotlarni tashqi muhitda qayta ishlash bilan bog‘liq tizimlarda yaqqol namoyon bo‘ladi. Masalan, foydalanuvchi o‘z ma’lumotlarini shifrlangan holda bulutli serverga yuborishi va server ushbu ma’lumotlar ustida hisob-kitoblar bajarishi mumkin. Natijaviy shifrlangan ma’lumot foydalanuvchiga qaytariladi va faqat u tomonidan ochiladi. Bu yondashuv ma’lumotlar maxfiyligini ta’minlash bilan birga, xizmat ko‘rsatuvchi tomonga ishonchni minimal darajaga tushiradi.

Shu bilan birga, gomomorf shifrlashning amaliy joriy etilishi jiddiy texnik muammolar bilan bog‘liq. Hisoblash murakkabligi juda yuqori bo‘lib, oddiy shifrlash sxemalariga nisbatan ancha ko‘p resurs talab etiladi. Ayniqsa, to‘liq gomomorf shifrlash sxemalari katta hisoblash quvvati va xotira talab qiladi. Bu holat hozircha ushbu texnologiyaning keng miqyosda qo‘llanilishini cheklab kelmoqda. Post-kvant gomomorf shifrlashda yana bir muhim masala — parametrlarni to‘g‘ri tanlashdir. Xavfsizlik va samaradorlik o‘rtasidagi muvozanatni ta’minlash oson emas. Parametrlar juda kichik bo‘lsa, xavfsizlik zaiflashadi, juda katta bo‘lsa, tizim amaliy jihatdan samarasiz bo‘lib qoladi. Shu sababli zamonaviy tadqiqotlar ushbu muvozanatni optimallashtirishga qaratilgan.

Umuman olganda, gomomorf shifrlash post-kvant kriptografiyaning eng murakkab, ammo istiqbolli yo‘nalishlaridan biridir. U hozircha cheklangan sohalarda qo‘llanilayotgan bo‘lsa-da, kelajakda maxfiy hisoblash va ma’lumotlarni himoyalash texnologiyalarining asosiy tarkibiy qismiga aylanishi mumkin. Shu sababli ushbu yo‘nalish bo‘yicha tadqiqotlar post-kvant kriptografiyaning uzoq muddatli rivojlanishida muhim rol o‘ynaydi.

POST-KVANT KRIPTOGRAFIYADA STANDARTLASHTIRISH JARAYONLARI

Post-kvant kriptografiyaning amaliyotga joriy etilishida standartlashtirish jarayonlari muhim o‘rin tutadi. Kriptografik algoritmlarning keng miqyosda qo‘llanilishi uchun ularning xavfsizligi, barqarorligi va amaliy samaradorligi mustaqil tashkilotlar tomonidan baholanishi lozim. Aks holda, turli tizimlarda mos kelmaydigan, bir-biriga zid yechimlar paydo bo‘lishi mumkin. Shu sababli post-kvant kriptografiyada standartlashtirish masalasi nazariy tadqiqotlar bilan bir qatorda muhim strategik yo‘nalish sifatida qaraladi.

So‘nggi yillarda post-kvant kriptografiyani standartlashtirish bo‘yicha eng yirik tashabbuslardan biri AQSh Milliy Standartlar va Texnologiyalar Instituti tomonidan olib borilgan ochiq tanlov jarayonidir. Ushbu jarayonning asosiy maqsadi kvant hujumlariga chidamli ochiq kalitli kriptografik algoritmlarni aniqlash va ularni kelajakdagi standartlar sifatida tavsiya etishdan iborat bo‘ldi. Tanlov bir necha bosqichda o‘tkazilib, unda turli mamlakatlardan yuzlab tadqiqotchilar taklif etgan algoritmlar ishtirok etdi. Standartlashtirish jarayonida algoritmlar bir nechta mezonlar asosida baholanadi. Ular orasida xavfsizlik darajasi, hisoblash samaradorligi, kalit va imzo hajmi, implementatsiya qulayligi hamda mavjud tizimlarga moslashuv imkoniyatlari muhim hisoblanadi. Shu bilan birga, algoritmlarning kriptotahlilga ochiqligi va mustaqil tadqiqotchilar tomonidan tekshirilishi jarayonning asosiy talablaridan biri bo‘lib qolmoqda. Bu yondashuv tanlangan algoritmlarga bo‘lgan ishonchni oshiradi.

Post-kvant kriptografiyada standartlashtirish faqat bitta tashkilot bilan cheklanib qolmaydi. Yevropa Ittifoqi va boshqa xalqaro tuzilmalar ham ushbu yo‘nalishda o‘z strategiyalarini ishlab chiqmoqda. Xususan, davlat axborot tizimlari va muhim infratuzilmalar uchun kvantga chidamli kriptografik mexanizmlarni joriy etish bo‘yicha tavsiyalar berilmoqda. Bu holat post-kvant kriptografiyaning global miqyosda muhokama qilinayotganini ko‘rsatadi. Biroq standartlashtirish jarayoni murakkab va uzoq vaqt talab etadigan jarayondir. Ayrim algoritmlar dastlab istiqbolli deb baholangan bo‘lsa-da, keyinchalik kriptotahlil natijasida zaif tomonlari aniqlanishi mumkin. Shu sababli standartlashtirish bosqichma-bosqich amalga oshiriladi va tanlangan algoritmlar ham doimiy ravishda qayta baholanadi. Bu ehtiyotkor yondashuv uzoq muddatli xavfsizlikni ta’minlashga xizmat qiladi. Natijada, post-kvant kriptografiyada standartlashtirish jarayonlari ushbu sohaning amaliy rivojlanishida hal qiluvchi ahamiyatga ega. Ular ilmiy tadqiqotlar natijalarini real tizimlarga tatbiq etish, muvofiqlikni ta’minlash va kelajakdagi axborot xavfsizligi strategiyalarini shakllantirish uchun mustahkam asos yaratadi.

POST-KVANT KRIPTOGRAFIYANING AMALIY JORIY ETILISHI VA MUAMMOLARI

Post-kvant kriptografiyasini real axborot tizimlariga joriy etish nazariy tadqiqotlardan ko‘ra ancha murakkab jarayon hisoblanadi. Amaliy muhitda kriptografik algoritmlar nafaqat xavfsiz, balki samarali, moslashuvchan va barqaror bo‘lishi ham talab etiladi. Shu sababli post-kvant algoritmlarini joriy etishda texnik, tashkiliy va iqtisodiy omillar birgalikda hisobga olinadi. Amaliy joriy etishdagi asosiy muammolardan biri — mavjud kriptografik infratuzilma bilan moslik masalasidir. Ko‘plab axborot tizimlari yillar davomida klassik kriptografiya asosida qurilgan bo‘lib, ularni to‘liq almashtirish katta vaqt va resurs talab etadi. Shu sababli post-kvant kriptografiyasiga o‘tish ko‘pincha bosqichma-bosqich amalga oshiriladi. Bu jarayonda gibrid yondashuvlar, ya’ni klassik va post-kvant algoritmlarini birgalikda qo‘llash keng tarqalmoqda. Yana bir muhim muammo — hisoblash va xotira resurslariga bo‘lgan talabdir. Ko‘plab post-kvant algoritmlar klassik analoglariga nisbatan kattaroq kalit va imzo hajmlariga ega. Bu holat tarmoq yuklamasini oshiradi hamda resurslari cheklangan qurilmalarda, masalan, mobil qurilmalar yoki IoT tizimlarida qo‘llashni qiyinlashtiradi. Natijada, har bir amaliy muhit uchun mos algoritmni tanlash muhim ahamiyat kasb etadi.

Post-kvant kriptografiyani joriy etishda inson omili ham e’tibordan chetda qolmaydi. Kriptografik tizimlarning noto‘g‘ri sozlanishi yoki xatoli implementatsiyasi hatto eng kuchli algoritmlarni ham zaiflashtirishi mumkin. Shu sababli dasturchilar va tizim administratorlari uchun maxsus tayyorgarlik,

hujjatlashtirish va tavsiyalar zarur bo‘ladi. Amaliy tajriba shuni ko‘rsatadiki, xavfsizlik muammolarining katta qismi algoritm tanlashdan ko‘ra, uni noto‘g‘ri qo‘llash bilan bog‘liq bo‘ladi. Bundan tashqari, post-kvant kriptografiyaning iqtisodiy jihatlari ham muhim hisoblanadi. Yangi algoritmlarga o‘tish dasturiy ta’minotni yangilash, apparat resurslarini kengaytirish va xodimlarni qayta tayyorlash kabi qo‘shimcha xarajatlarni talab etadi. Ayrim tashkilotlar uchun bu jarayon qisqa muddatda amalga oshirilishi qiyin bo‘lishi mumkin. Shu sababli joriy etish strategiyalari uzoq muddatli rejalashtirish asosida ishlab chiqiladi.

Umuman olganda, post-kvant kriptografiyaning amaliy joriy etilishi texnik imkoniyatlar bilan bir qatorda tashkiliy va strategik yondashuvni ham talab qiladi. Ushbu muammolarni bosqichma-bosqich hal etish orqali kvant kompyuterlar davrida ham axborot xavfsizligini ta’minlash mumkin bo‘ladi.

POST-KVANT KRIPTOGRAFIYA SOHASIDAGI GLOBAL TADQIQOT TENDENSIYALARI VA BIBLIOMETRIK TAHLIL

Post-kvant kriptografiyasi so‘nggi yillarda kriptografiya va axborot xavfsizligi sohalaridagi eng faol ilmiy yo‘nalishlardan biriga aylandi. Kvant kompyuterlar rivojlanishining tezlashuvi ushbu sohada olib borilayotgan tadqiqotlar soni va sifatiga bevosita ta’sir ko‘rsatmoqda. Bibliometrik tahlillar shuni ko‘rsatadiki, post-kvant kriptografiya bo‘yicha ilmiy maqolalar soni yil sayin ortib bormoqda va bu yo‘nalish xalqaro miqyosda keng e’tirof etilmoqda. Ilmiy nashrlar tahlili natijalariga ko‘ra, post-kvant kriptografiya bo‘yicha yetakchi tadqiqotlar asosan AQSh, Yevropa Ittifoqi mamlakatlari va Sharqiy Osiyo davlatlarida olib borilmoqda. Universitetlar, ilmiy tadqiqot markazlari hamda sanoat vakillari o‘rtasidagi hamkorlik ushbu yo‘nalishning tez rivojlanishiga xizmat qilmoqda. Ayniqsa, ochiq kriptografik tanlovlar va xalqaro konferensiyalar ilmiy fikr almashinuvi uchun muhim maydon bo‘lib xizmat qilmoqda.

Bibliometrik tahlil shuni ham ko‘rsatadiki, post-kvant kriptografiya bo‘yicha tadqiqotlar mavzu jihatidan tobora ixtisoslashib bormoqda. Dastlab umumiy tushunchalar va nazariy asoslar ustuvor bo‘lgan bo‘lsa, hozirgi bosqichda alohida algoritmik oilalar, implementatsiya muammolari va real tizimlarga moslashuv masalalari ko‘proq o‘rganilmoqda. Bu holat sohaning yetuklik darajasi oshib borayotganidan dalolat beradi. Shuningdek, so‘nggi yillarda amaliy yo‘naltirilgan tadqiqotlar ulushi sezilarli darajada oshdi. Ilmiy maqolalarda nafaqat algoritmlarning nazariy xavfsizligi, balki ularning real tizimlarda ishlash samaradorligi, resurslarga ta’siri va muhandislik nuqtayi nazaridan qulayligi ham tahlil qilinmoqda. Bu tendensiya post-kvant kriptografiyaning faqat akademik muammo emas, balki amaliy ehtiyojga aylanganini ko‘rsatadi.

Bibliometrik ko‘rsatkichlar orasida hamkorlik darajasi ham muhim ahamiyatga ega. Ko‘plab ilmiy ishlar bir nechta mualliflar va turli tashkilotlar ishtirokida yozilmoqda. Bu esa post-kvant kriptografiya murakkab va ko‘p fanli yondashuvni talab qilishini ko‘rsatadi. Matematika, informatika, muhandislik va xavfsizlik sohalarining kesishgan nuqtasida olib borilayotgan tadqiqotlar ushbu yo‘nalishning asosiy harakatlantiruvchi kuchiga aylanmoqda. Umuman olganda, bibliometrik tahlil post-kvant kriptografiya sohasining jadal rivojlanayotganini va global miqyosda dolzarb ekanini yaqqol ko‘rsatadi. Ilmiy faollikning ortishi, mavzularning chuqurlashuvi va amaliy yo‘nalishlarning kuchayishi ushbu sohaning yaqin kelajakda axborot xavfsizligi tizimlarida muhim o‘rin egallashidan dalolat beradi.

MUHOKAMA: POST-KVANT KRIPTOGRAFIYANING AFZALLIKLARI VA CHEKLOVLARI

Post-kvant kriptografiyasi zamonaviy axborot xavfsizligi muammolariga javob sifatida shakllangan bo‘lsa-da, uni baholashda faqat ijobiy jihatlar bilangina cheklanib qolish to‘g‘ri bo‘lmaydi. Ushbu yo‘nalishning afzalliklari va cheklovlarini birgalikda ko‘rib chiqish post-kvant kriptografiyaning real imkoniyatlarini to‘g‘ri anglashga yordam beradi. Ayniqsa, kvant kompyuterlar hali to‘liq amaliy bosqichga yetib kelmagan bir paytda bunday muhokama muhim ahamiyat kasb etadi. Post-kvant kriptografiyaning asosiy afzalligi — uning uzoq muddatli xavfsizlikka yo‘naltirilganligidir. Kvant kompyuterlar paydo bo‘lishi ehtimoli hisobga olingan holda ishlab chiqilgan algoritmlar hozirgi va kelajakdagi tahdidlarga nisbatan barqarorroq hisoblanadi. Bu holat ayniqsa uzoq vaqt saqlanishi kerak bo‘lgan maxfiy ma’lumotlar uchun muhimdir. Post-kvant yondashuvlar hozirgi shifrlangan ma’lumotlarning kelajakda ochilib ketish xavfini kamaytirishga xizmat qiladi.

Yana bir muhim afzallik — post-kvant algoritmlarning klassik hisoblash muhitida ishlashi mumkinligidir. Bu ularni kvant kriptografiyasidan farqlaydi, chunki kvant kriptografiya maxsus apparat va fizik aloqa kanallarini talab etadi. Post-kvant kriptografiya esa mavjud dasturiy va apparat infratuzilmaga moslashish imkonini beradi. Natijada joriy etish jarayoni nisbatan soddaroq va iqtisodiy jihatdan maqbulroq bo‘lishi mumkin.

Biroq post-kvant kriptografiyaning cheklovlari ham mavjud. Eng ko‘p uchraydigan muammolardan biri — samaradorlik masalasidir. Ko‘plab post-kvant algoritmlar klassik algoritmlarga nisbatan kattaroq kalit va imzo hajmlariga ega. Bu holat tarmoq trafigining ortishiga, hisoblash vaqtining ko‘payishiga va resurslar iste’molining oshishiga olib keladi. Ayniqsa, resurslari cheklangan qurilmalarda bu cheklovlar sezilarli bo‘lishi mumkin. Shuningdek, post-kvant kriptografiyaning nisbatan yangi yo‘nalish ekanligi ham ehtiyotkorlikni talab etadi. Ko‘plab algoritmlar hali uzoq muddatli amaliy sinovlardan to‘liq o‘tmagan. Tarix shuni ko‘rsatadiki, ayrim kriptografik sxemalar dastlab xavfsiz deb baholangan bo‘lsa-da, vaqt o‘tishi bilan yangi hujum usullari orqali buzilgan. Shu sababli post-kvant algoritmlarga nisbatan doimiy tahlil va ochiq muhokama zarur.

Muhokama jarayonida yana bir muhim jihat — moslashuv strategiyalaridir. Hozirgi sharoitda ko‘plab mutaxassislar klassik va post-kvant kriptografiyani birgalikda qo‘llashni eng maqbul yechim deb hisoblamoqda. Bunday gibrid yondashuvlar qisqa muddatda xavfsizlikni ta’minlash bilan birga, uzoq muddatli o‘tish jarayonini silliq amalga oshirish imkonini beradi.

XULOSA

Mazkur maqolada post-kvant kriptografiyasining shakllanish sabablari, nazariy asoslari va amaliy ahamiyati tizimli ravishda tahlil qilindi. Kvant kompyuterlarning rivojlanishi klassik ochiq kalitli kriptografiya algoritmlariga jiddiy tahdid solayotgani, xususan, faktorizatsiya va diskret logarifmga asoslangan tizimlarning uzoq muddatli xavfsizligi shubha ostida qolayotgani ko‘rsatib berildi. Ushbu holat post-kvant kriptografiyasini kelajak uchun muqobil emas, balki zarur yo‘nalishga aylantirmoqda. Tahlil jarayonida post-kvant kriptografiyaning asosiy algoritmik oilalari — panjaraga asoslangan, kodga asoslangan, ko‘p o‘zgaruvchili va xeshga asoslangan yondashuvlar alohida ko‘rib chiqildi. Har bir yo‘nalish o‘ziga xos matematik asos, xavfsizlik darajasi va amaliy cheklovlarga ega ekani aniqlandi. Ayniqsa, panjaraga asoslangan algoritmlar nazariy mustahkamlik va funksional imkoniyatlar nuqtayi

nazaridan yetakchi o‘rinni egallayotgani, shu bilan birga kodga asoslangan tizimlar uzoq yillik barqarorlik tajribasi bilan ajralib turishi qayd etildi.

Shuningdek, maqolada post-kvant kriptografiyaning amaliy jihatlari, jumladan, standartlashtirish jarayonlari, real tizimlarga joriy etish muammolari va global tadqiqot tendensiyalari yoritildi. Bibliometrik tahlil natijalari ushbu soha jadal rivojlanayotganini, ilmiy faollik va amaliy qiziqish yil sayin ortib borayotganini ko‘rsatdi. Bu esa post-kvant kriptografiyaning faqat nazariy yo‘nalish emas, balki real ehtiyoj sifatida qaralayotganini tasdiqlaydi.Shu bilan birga, post-kvant kriptografiya mutlaq yechim emasligi ham muhokama qilindi. Katta kalit hajmlari, hisoblash resurslariga bo‘lgan talab va yangi algoritmlarning yetarlicha uzoq muddat sinovdan o‘tmaganligi kabi omillar ehtiyotkor yondashuvni talab qiladi. Shu sababli hozirgi bosqichda klassik va post-kvant kriptografiyani birgalikda qo‘llashga asoslangan gibrid strategiyalar eng maqbul yo‘l sifatida qaralmoqda. Umuman olganda, post-kvant kriptografiyasi kvant kompyuterlar davrida axborot xavfsizligini ta’minlash uchun muhim ilmiy va amaliy asos yaratadi. Ushbu yo‘nalish bo‘yicha tadqiqotlarni chuqurlashtirish, algoritmlarni real sharoitlarda sinovdan o‘tkazish va bosqichma-bosqich joriy etish kelajakda barqaror va ishonchli kriptografik infratuzilmani shakllantirishga xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR

1. Post-Quantum Cryptography: Challenges and Advances. IACR ePrint Archive, 2024. URL: https://eprint.iacr.org/2024/1940
2. A Survey on Post-Quantum Cryptography: State-of-the-Art and Challenges. arXiv preprint, 2023. URL: https://arxiv.org/abs/2312.10430
3. Homomorphic Encryption Based on Lattice Post-Quantum Cryptography. arXiv preprint, 2025. URL: https://arxiv.org/abs/2501.03249
4. A Note on Quantum Security for Post-Quantum Cryptography. arXiv preprint, 2014. URL: https://arxiv.org/abs/1409.2187
5. The Impact of Quantum Computing on Present Cryptography. arXiv preprint, 2018. URL: https://arxiv.org/abs/1804.00200
6. Exploring the Landscape of Post-Quantum Cryptography: A Bibliometric Analysis. Journal of Big Data, 2025. URL: https://journalofbigdata.springeropen.com/articles/10.1186/s40537-025-01269-5
7. Post-Quantum Cryptography. European Union Technical Report, 2022. URL: https://op.europa.eu/en/publication-detail/-/publication/a716a504-618f-11ed-92ed-01aa75ed71a1
8. Post-Quantum Cryptography: From Theory to Practice. Theses Journal, 2023. URL: https://thesesjournal.com/index.php/1/article/view/428
9. Post-Quantum Cryptography. ARIS Open Access Journal, 2022. URL: https://aris-journal.com/aris/index.php/journal/article/view/17
10. Post-Quantum Cryptography for Engineers. IETF Internet-Draft, 2024. URL: https://www.ietf.org/archive/id/draft-ietf-pquip-pqc-engineers-14.html