KVANT KOMPYUTERLAR VA KELAJAKDAGI SHIFRLASH MUAMMOLARI

Temirxonova Zuxraxon Xomidxon qizi

O‘zbekiston Milliy universiteti Jizzax filiali

temirxonovazuxraxon18@gmail.com

Annotatsiya: Shifrlash algoritmlari elektron pochta xabarlaridan tortib tibbiy yozuvlar va moliyaviy hisobotlargacha bo'lgan maxfiy elektron ma'lumotlarni ruxsatsiz tomoshabinlardan himoya qiladi. O'nlab yillar davomida ushbu algoritmlar shifrlashni buzishga urinadigan an'anaviy kompyuterlardan foydalanadigan hujumlardan himoya qilish uchun yetarlicha kuchli ekanligini isbotladi. Biroq, kvant kompyuteri deb nomlangan yangi turdagi qurilma ushbu algoritmlarni buzishi va elektron sirlarimizni kashf etilishga moyil qilishi mumkin. Ushbu yaqinlashib kelayotgan tahdidga qarshi turish uchun bizga bugungi kunda biladigan an'anaviy kompyuterlar va ertangi kun kvant kompyuterlarining kiberhujumlarini oldini oladigan shifrlash usullari kerak. Bu yangi usullar post-kvant shifrlash algoritmlari deb ataladi.

Kalit so‘zlar: kvant hisoblash, zamonaviy kriptografiya, shifrlash tizimlari, post-kvant kriptografiya, axborot xavfsizligi, raqamli ma’lumotlar himoyasi.

Kirish

Kvant algoritmlari mavjud kriptografik tizimlarga tahdid solishi mumkin. Kvant kompyuterlar an’anaviy kompyuterlardan farqli ravishda murakkab hisoblashlarni tezroq bajarish imkoniga ega bo‘lib, kvant dunyosining o‘ziga xos xususiyatlaridan foydalanadi. Jumladan, kvant hisoblashda ma’lumotlar bir vaqtning o‘zida ham 0, ham 1 holatida mavjud bo‘lishi mumkin, bu esa klassik kompyuterlar uchun qiyin yoki imkonsiz bo‘lgan hisob-kitoblarni amalga oshirish imkonini beradi.Kriptografik algoritmlar odatda ikki asosiy vazifani bajaradi: umumiy tarmoq orqali uzatiladigan ma’lumotlarni, masalan parollarni himoya qilish hamda foydalanuvchi shaxsini tasdiqlash uchun raqamli imzolarni

ta’minlash. Biroq, kompyuter xavfsizligi bo‘yicha mutaxassislar yetarlicha kuchli kvant kompyuterlari yaratilishidan oldin post-kvant shifrlash algoritmlarini joriy etishga harakat qilayotgan bo‘lsa-da, ko‘plab shifrlangan ma’lumotlar “hozir yig‘ib ol, keyin shifrni och” turidagi hujumlar tufayli xavf ostida qolmoqda. Ushbu maqolaning asosiy maqsadi kvant kompyuterlarning zamonaviy shifrlash algoritmlariga ta’sirini tahlil qilish hamda post-kvant kriptografiya kabi istiqbolli yechimlarni ko‘rib chiqishdan iborat.

Adabiyotlar tahlili va metodlar

Shifrlash algoritmlari elektron pochta xabarlari, tibbiy yozuvlar hamda moliyaviy hisobotlar kabi maxfiy elektron ma’lumotlarni ruxsatsiz kirishdan himoya qilishda muhim ahamiyat kasb etadi. Uzoq vaqt davomida ushbu algoritmlar an’anaviy kompyuterlarga asoslangan hujumlarga nisbatan yetarli darajada ishonchli ekanligini ko‘rsatdi. Biroq, kvant kompyuterlarining paydo bo‘lishi mavjud kriptografik tizimlarning xavfsizligiga nisbatan yangi tahdidlarni yuzaga keltirmoqda.

Kvant kompyuterlar kvant mexanikasining o‘ziga xos xususiyatlaridan foydalanib, ma’lumotlarning bir vaqtning o‘zida bir nechta holatda bo‘lishiga imkon yaratadi. Bu esa klassik kompyuterlar uchun murakkab yoki uzoq vaqt talab qiladigan hisob-kitoblarni tezroq bajarish imkonini beradi. Zamonaviy kriptografik algoritmlar asosan katta sonlarni faktorlash muammosining murakkabligiga tayanadi, ammo yetarlicha rivojlangan kvant kompyuterlari ushbu matematik muammolarni samaraliroq hal qilishi mumkin.

Post-kvant shifrlash algoritmlari esa an’anaviy va kvant kompyuterlari uchun yechish qiyin bo‘lgan matematik masalalarga asoslanadi. NIST tomonidan tanlangan algoritmlarning aksariyati strukturaviy panjaralar va xesh funksiyalariga tayangan holda ishlab chiqilgan bo‘lib, ular kelajakdagi kiberxavfsizlik tahdidlariga qarshi istiqbolli yechim sifatida qaralmoqda.

Foydalanilgan metodlar:Ushbu tadqiqotda kvant kompyuterlarning zamonaviy kriptografik tizimlarga ta’sirini o‘rganish hamda post-kvant shifrlash algoritmlarining ahamiyatini aniqlash maqsadida quyidagi ilmiy metodlardan foydalanildi: Tahliliy

metod:Zamonaviy shifrlash algoritmlarining ishlash tamoyillari hamda kvant kompyuterlarning ushbu algoritmlarga potensial tahdidi ilmiy manbalar asosida tahlil qilindi. Kvant hisoblashning klassik kriptografiyaga ta’siri nazariy jihatdan o‘rganildi. Nazariy metod:Kvant hisoblashning asosiy tushunchalari, qubitlar xususiyatlari va kvant algoritmlarining matematik asoslari mavjud ilmiy manbalar orqali nazariy jihatdan ko‘rib chiqildi. Solishtirma metod:An’anaviy kriptografik algoritmlar va post-kvant kriptografiya yondashuvlari o‘zaro taqqoslanib, ularning afzalliklari va cheklovlari qiyosiy tahlil qilindi. Adabiyotlar tahlili metodi:NIST tomonidan taqdim etilgan materiallar hamda kvantdan keyingi kriptografiya bo‘yicha ilmiy maqolalar o‘rganilib, mavjud yondashuvlar umumlashtirildi.

Natijalar

Tahlil qilingan ilmiy manbalar asosida quyidagi muhim natijalarga erishildi:

Kvant kompyuterlar zamonaviy kriptografik tizimlarga tahdid solishi mumkin.Tadqiqotlar shuni ko‘rsatadiki, katta sonlarni faktorlashga asoslangan an’anaviy shifrlash algoritmlari yetarlicha kuchli kvant kompyuterlari mavjud bo‘lganda o‘zining xavfsizlik darajasini yo‘qotishi ehtimoli mavjud. Post-kvant kriptografiya zarur yo‘nalish **sifatida shakllanmoqda.** Ilmiy manbalar tahlili natijasida kvant hujumlariga chidamli bo‘lgan yangi kriptografik algoritmlarni ishlab chiqish va joriy etish muhimligi aniqlanib, bu yo‘nalish axborot xavfsizligining kelajakdagi asosiy strategiyalaridan biri sifatida baholandi. **Nazariy tahlil orqali kvant hisoblashning afzalliklari aniqlandi.** Kvant algoritmlarining bir vaqtning o‘zida ko‘plab yechimlarni tahlil qilish imkoniyati klassik hisoblash tizimlariga nisbatan sezilarli ustunlik berishi aniqlanib, bu holat kriptografik tizimlar uchun yangi xavflarni yuzaga keltirishi ko‘rsatildi.**An’anaviy va post-kvant algoritmlari o‘zaro taqqoslandi.** Solishtirma tahlil natijasida strukturaviy panjaralar va xesh funksiyalariga asoslangan algoritmlar kvant hujumlariga nisbatan barqarorroq ekanligi qayd etildi.

Muhokama

Kvant kompyuterlar katta imkoniyatlarga ega bo‘lsa-da, ularning rivojlanishida muhim texnik muammolar mavjud. Jumladan, kvant hisoblashning asosiy elementi bo‘lgan qubitlar juda mo‘rt bo‘lib, kichik tashqi ta’sirlar ham hisoblash jarayonida xatolarga olib kelishi mumkin. Shu sababli, kriptografik jihatdan yetarlicha kuchli kvant kompyuterlar hali to‘liq amaliy bosqichga yetmagan.Shunga qaramay, ilmiy hamjamiyat kvantdan keyingi shifrlash algoritmlarini hozirdanoq ishlab chiqish zarurligini ta’kidlamoqda. Sababi, kvant kompyuterlar qachon to‘liq rivojlanishi aniq bo‘lmasa ham, mavjud shifrlangan ma’lumotlar kelajakda ochilishi mumkin. Shu bois tashkilotlar va davlatlar kvantga chidamli kriptografik standartlarga bosqichma-bosqich o‘tish bo‘yicha tayyorgarlik ishlarini olib borishi lozim.

Xulosa va takliflar

Mazkur tadqiqot natijalari kvant kompyuterlarining rivojlanishi zamonaviy kriptografik tizimlar uchun yangi xavf-xatarlarni yuzaga keltirayotganini ko‘rsatdi. An’anaviy shifrlash algoritmlari murakkab matematik muammolarga asoslangan bo‘lsa-da, yetarlicha kuchli kvant kompyuterlari paydo bo‘lishi ularning xavfsizlik darajasiga salbiy ta’sir ko‘rsatishi mumkin. Shu bilan birga, kvant hisoblash texnologiyalari hali to‘liq rivojlanmagan bo‘lib, qubitlarning mo‘rtligi va texnik cheklovlar kabi muammolar mavjud.Tahlillar shuni ko‘rsatdiki, post-kvant kriptografiya kelajakda axborot xavfsizligini ta’minlashda muhim yo‘nalishlardan biri hisoblanadi. Kvant kompyuterlar qachon to‘liq amaliy bosqichga yetishi aniq bo‘lmasa-da, mavjud shifrlangan ma’lumotlarni himoya qilish uchun hozirdanoq yangi kriptografik yondashuvlarga o‘tish zarur.

Takliflar

Axborot xavfsizligini ta’minlash maqsadida post-kvant.kriptografiya algoritmlarini bosqichma-bosqich joriy etish tavsiya etiladi.Tashkilotlar va davlat idoralari mavjud shifrlash tizimlarini tahlil qilib, kvantga chidamli algoritmlarga o‘tish strategiyasini ishlab chiqishi zarur.Kiberxavfsizlik bo‘yicha mutaxassislar uchun kvant hisoblash va post-kvant

kriptografiya bo‘yicha ilmiy tadqiqotlarni kengaytirish lozimAxborot tizimlari ishlab chiquvchilari kelajakdagi kvant tahdidlarini hisobga olgan holda yangi xavfsizlik standartlarini qo‘llashi tavsiya etiladi. Xalqaro hamkorlikni kuchaytirish orqali kvantga chidamlikriptografik standartlarni joriy etish jarayonini tezlashtirish maqsadga muvofiq.

Foydalanilgan adabiyotlar ro‘yhati:

1. National Institute of Standards and Technology (NIST). What is Post-Quantum Cryptography?
https://www.nist.gov/cybersecurity/what-post-quantum-cryptography
2. Chen, L., Jordan, S., Liu, Y. va boshqalar. Report on Post-Quantum Cryptography. NISTIR 8105, 2016.https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf
3. Primov Baxtiyor Olim o‘g‘li. Kiber jinoyatchilikka qarshi immunitet hosil qilish masalalari. 2024-yil, 30-may.
IBM Quantum.What is Quantum Computing?
https://www.ibm.com/quantum/learn/what-is-quantum-computing
4. O‘zbekiston Respublikasi Prezidentining kiberxavfsizlikni rivojlantirishga oid normativ-huquqiy hujjatlari (raqamli xavfsizlik strategiyasi bo‘yicha materiallar).