KVANT KOMPUTERLARNING ZAMONAVIY KRIPTOGRAFIYAGA TAHDIDLARI

Mustafoyev Azamat Botir o'g'li
''UNICON.UZ'' MChJ
E-mail: mustafoyevazamat01gmail.com

K E Y W O R D S

kvant kompyuter, kriptografiya, Shor algoritmi, Grover algoritmi, post-kvant kriptografiya, RSA, AES, axborot xavfsizligi, shifrlash, kvant ustunligi

A B S T R A C T

Ushbu maqolada kvant komputerlarning zamonaviy kriptografik tizimlariga yetkazishi mumkin bo'lgan tahdidlar masalasi o'rganilgan. Tadqiqot davomida kvant hisoblash texnologiyalarining rivojlanish tendensiyalari, ularning klassik shifrlash algoritmlariga ta'siri hamda post-kvant kriptografiya sohasidagi ilmiy izlanishlar tahlil qilingan. Maqolada Shor va Grover algoritmlari asosida RSA, ECC va AES kabi keng tarqalgan kriptografik standartlarning zaifliklari ochib berilgan. Tadqiqot natijalariga ko'ra, kvant komputerlarning amaliy qo'llanilishi kriptografik infratuzilmani tubdan o'zgartirish zaruratini keltirib chiqaradi va post-kvant kriptografiya algoritmlariga o'tish strategiyasini ishlab chiqish dolzarb ahamiyat kasb etadi.

KIRISH

Zamonaviy raqamli kommunikatsiyalar tizimi kriptografik himoya mexanizmlariga asoslangan bo'lib, ushbu mexanizmlar axborotning maxfiyligi, yaxlitligi va autentifikatsiyasini ta'minlaydi. Bugungi kunda internet-banking, elektron tijorat, davlat boshqaruvi tizimlari va shaxsiy ma'lumotlarni himoyalash kabi muhim sohalarda RSA, elliptik egri chiziqlar kriptografiyasi (ECC) hamda simmetrik shifrlash algoritmlari keng qo'llanilmoqda [1]. Biroq, kvant hisoblash texnologiyalarining jadal rivojlanishi bu kriptografik tizimlarning barqarorligiga jiddiy tahdid solmoqda. Kvant komputerlar klassik kompyuterlardan tubdan farq qiluvchi fizik tamoyillarga asoslangan bo'lib, ular ma'lum matematik masalalarni eksponensial tezroq yechish qobiliyatiga ega [2].

Kvant mexanikasining superpozitsiya va chalkashlik (entanglement) hodisalari kvant bitlari (kubitlar) yordamida bir vaqtning o'zida ko'plab hisoblashlarni amalga oshirish imkonini beradi. Bu xususiyat klassik kompyuterlar uchun amaliy jihatdan yechib bo'lmaydigan murakkab matematik muammolarni hal qilishda kvant kompyuterlariga ustunlik beradi [3]. Xususan, katta sonlarni tub ko'paytuvchilarga ajratish va diskret logarifm masalalari, ya'ni zamonaviy assimetrik kriptografiyaning matematik asosi, kvant kompyuterlar uchun samarali yechilishi mumkin. Shu sababli, kvant hisoblash texnologiyalarining takomillashuvi global axborot xavfsizligi infratuzilmasiga strategik tahdid sifatida baholanmoqda va ilmiy hamjamiyat tomonidan post-kvant kriptografiya sohasida faol izlanishlar olib borilmoqda [4].

Ushbu tadqiqotning maqsadi kvant komputerlarning zamonaviy kriptografik algoritmlariga tahdidlarini nazariy jihatdan tahlil qilish, mavjud ilmiy adabiyotlar asosida kvant hujumlariga qarshi himoya strategiyalarini o'rganish hamda post-kvant kriptografiya sohasidagi istiqbolli yo'nalishlarni aniqlashdan iborat.

METODOLOGIYA VA ADABIYOTLAR TAHLILI

Tadqiqot metodologiyasi sifatida tizimli adabiyotlar tahlili va qiyosiy tahlil usullari qo'llanildi. Ilmiy izlanish davomida xalqaro va mahalliy ilmiy manbalar, jumladan, IEEE, ACM, Springer ma'lumotlar bazalaridagi maqolalar, monografiyalar hamda NIST (Amerika Milliy Standartlar va Texnologiyalar Instituti) rasmiy hujjatlari tahlil qilindi. Tadqiqot ob'ekti sifatida

(cc) BY

RSA, ECC va AES kriptografik algoritmlari, Shor va Grover kvant algoritmlari hamda post-kvant kriptografiya standartlari tanlandi. Kvant hisoblash nazariyasining kriptografiyaga ta'siri birinchi marta 1994-yilda amerikalik matematik Piter Shor tomonidan ilmiy asoslab berildi. Shor o'z tadqiqotida kvant kompyuterda katta butun sonlarni tub ko'paytuvchilarga polinom vaqtda ajratish algoritmini taqdim etdi [5]. Ushbu kashfiyot RSA kriptotizimining xavfsizligiga bevosita tahdid soldi, chunki RSA ning xavfsizligi aynan katta sonlarni faktorizatsiya qilishning klassik kompyuterlar uchun amaliy jihatdan imkonsizligiga asoslangan. Shor algoritmining murakkabligi $O((\log N)^3)$ tartibida bo'lib, bu klassik algoritmlarning subeksponensial murakkabligidan sezilarli darajada past [2].

Grover algoritmi esa 1996-yilda Lov Grover tomonidan ishlab chiqilgan bo'lib, u tartiblanmagan ma'lumotlar bazasida qidiruvni kvadratik tezlashtirish imkonini beradi [6]. Simmetrik shifrlash algoritmlariga nisbatan Grover algoritmi samarali hujum vositasi hisoblanadi. Masalan, 128-bitli AES kalitini klassik kompyuterda topish uchun 2^{128} operatsiya talab etilsa, kvant kompyuterda Grover algoritmi yordamida bu ko'rsatkich 2^{64} ga tushadi. Shu sababli, kvant tahdidlariga qarshi simmetrik algoritmlar uchun kalit uzunligini ikki baravar oshirish tavsiya etiladi [7].

Rossiyalik olimlar S.Ya. Kilin va D.B. Xorujan'ning tadqiqotlarida kvant kriptografiya va kvant kalitlarni taqsimlash protokollari (QKD) batafsil tahlil qilingan [8]. Ularning ta'kidlashicha, BB84 va E91 kabi kvant protokollari nazariy jihatdan mutlaq xavfsizlikni ta'minlaydi, biroq amaliy tatbiqda qurilmalarning texnik cheklovlari va yangi turdagi hujumlar (side-channel attacks) muammolari mavjud. O'zbekistonlik olimlar ham axborot xavfsizligi sohasida tadqiqotlar olib bormoqda, xususan, N.Xalikova va boshqalarning ishlarida milliy kriptografik standartlarni kvant tahdidlariga moslash masalalari ko'tarilgan [9].

NIST 2016-yildan boshlab post-kvant kriptografiya standartlashtirish jarayonini boshlagan bo'lib, 2024-yilga kelib CRYSTALS-Kyber (kalit almashish), CRYSTALS-Dilithium va FALCON (raqamli imzo) algoritmlari asosiy standartlar sifatida tasdiqlandi [4]. Bu algoritmlar panjarali kriptografiya (lattice-based cryptography), kod nazariyasiga asoslangan kriptografiya va ko'p o'lchovli kvadratik tenglamalar tizimlariga asoslangan.

NATIJALAR VA MUHOKAMA

Olib borilgan adabiyotlar tahlili va qiyosiy tadqiqot natijalari shuni ko'rsatadiki, kvant komputerlarning kriptografiyaga tahdidi real va yaqin kelajakda amaliy ahamiyat kasb etadi. Hozirgi kunda IBM, Google, IonQ va boshqa yetakchi texnologiya kompaniyalari 1000 dan ortiq kubitli kvant kompyuterlarni yaratish ustida ish olib bormoqda [3]. 2019-yilda Google o'zining 53-kubitli Sycamore protsessori yordamida "kvant ustunligi"ga erishganini e'lon qildi, ya'ni klassik superkompyuterlar uchun 10000 yil talab etiladigan hisoblashni 200 sekundda amalga oshirdi. Garchi bu natija kriptografik algoritmlarni buzish uchun hali yetarli bo'lmasa-da, texnologik rivojlanish tezligini hisobga olsak, 2030-2040-yillarga kelib kriptografik jihatdan muhim kvant kompyuterlarning paydo bo'lishi kutilmoqda [10].

Tahlil natijalari assimetrik kriptografiya tizimlarining kvant hujumlariga nisbatan eng zaif ekanligini ko'rsatadi. RSA-2048 algoritmini buzish uchun taxminan 4000 xatosiz kubit talab etiladi, ECC-256 uchun esa taxminan 2500 kubit yetarli [5]. Hozirgi kvant kompyuterlari shovqin darajasi yuqori bo'lgani uchun bu ko'rsatkichlarga hali yetishmagan, biroq xatolarni tuzatish texnologiyalari jadal takomillashmoqda. Simmetrik algoritmlar nisbatan barqarorroq hisoblanadi, chunki Grover algoritmi faqat kvadratik tezlanish beradi, shu sababli AES-256 kvant davrida ham yetarli xavfsizlik darajasini saqlab qoladi [7].

Post-kvant kriptografiya algoritmlari tahlili shuni ko'rsatadiki, panjarali kriptografiyaga asoslangan sxemalar eng istiqbolli hisoblanadi. CRYSTALS-Kyber algoritmi samaradorlik va xavfsizlik nisbati bo'yicha optimal natijalarni namoyish etadi, kalit va shifrlangan matn hajmlari RSA ga nisbatan kichikroq, shu bilan birga kvant hujumlariga qarshi matematik asosi mustahkam [4]. Biroq, post-kvant algoritmlarning amaliy tatbiqi bir qator muammolarni keltirib chiqaradi: yangi algoritmlar klassik tizimlarga nisbatan ko'proq hisoblash resurslari talab etadi, mavjud infratuzilmani yangilash katta moliyaviy xarajatlarni talab qiladi va o'tish davrida gibrid kriptografik sxemalardan foydalanish zarurati tug'iladi.

(cc) BY

"Hozir yig'ib, keyinroq shifrini ochish" (harvest now, decrypt later) tahdidi alohida e'tiborga loyiq. Hujumchilar hozirda shifrlangan ma'lumotlarni yig'ib, kelajakda kvant kompyuterlar yordamida ularning shifrini ochish imkoniyatiga ega bo'ladi [10]. Bu tahdid davlat sirlari, strategik biznes ma'lumotlari va uzoq muddatli maxfiylikni talab etuvchi shaxsiy ma'lumotlar uchun ayniqsa jiddiy. Shu sababli, ko'plab davlatlar va yirik korporatsiyalar post-kvant kriptografiyaga o'tish jarayonini allaqachon boshlagan.

XULOSA

Kvant komputerlarning zamonaviy kriptografiyaga tahdidlari real va dolzarb muammo hisoblanadi. Tadqiqot natijalari shuni ko'rsatadiki, Shor algoritmi RSA va ECC kabi assimetrik kriptografik tizimlarni to'liq buzish imkoniyatini beradi, Grover algoritmi esa simmetrik algoritmlarning samarali xavfsizlik darajasini ikki baravar kamaytiradi. Kvant komputerlarning hozirgi texnik imkoniyatlari hali kriptografik jihatdan muhim darajaga yetmagan bo'lsa-da, texnologik rivojlanish tendensiyalari 10-15 yil ichida vaziyatning tubdan o'zgarishini bashorat qiladi.

Post-kvant kriptografiya sohasida sezilarli yutuqlar qo'lga kiritilgan, NIST tomonidan standartlashtirish jarayoni yakunlangan va amaliy tatbiq bosqichi boshlangan. Panjarali kriptografiyaga asoslangan algoritmlar, xususan CRYSTALS-Kyber va CRYSTALS-Dilithium, kvant davrida axborot xavfsizligini ta'minlash uchun ishonchli asos yaratadi. O'zbekiston uchun milliy kriptografik standartlarni kvant tahdidlariga moslash, kadrlar tayyorlash va ilmiy-tadqiqot ishlarini kuchaytirish ustuvor vazifalar qatoriga kiradi. Kvant xavfsiz kriptografiyaga o'tish strategik zarurat bo'lib, bu jarayonni bugundan boshlash kelajakda axborot xavfsizligini ta'minlashning kafolati hisoblanadi.

ADABIYOTLAR RO'YXATI

1. Каримов, И.А. Замонавий ахборот хавфсизлиги муаммолари ва ечимлари / И.А. Каримов, Н.Р. Юсупов // Ахборот технологиялари. – 2021. – № 3. – Б. 45-52.
2. Shor, P.W. Algorithms for quantum computation: discrete logarithms and factoring / P.W. Shor // Proceedings of 35th Annual Symposium on Foundations of Computer Science. – IEEE, 1994. – P. 124-134.
3. Arute, F. Quantum supremacy using a programmable superconducting processor / F. Arute [et al.] // Nature. – 2019. – Vol. 574. – P. 505-510.
4. National Institute of Standards and Technology. Post-Quantum Cryptography Standardization. – NIST, 2024. – 156 p.
5. Proos, J. Shor's discrete logarithm quantum algorithm for elliptic curves / J. Proos, C. Zalka // Quantum Information & Computation. – 2003. – Vol. 3, № 4. – P. 317-344.
6. Grover, L.K. A fast quantum mechanical algorithm for database search / L.K. Grover // Proceedings of 28th Annual ACM Symposium on Theory of Computing. – 1996. – P. 212-219.
7. Bernstein, D.J. Post-quantum cryptography / D.J. Bernstein, J. Buchmann, E. Dahmen. – Berlin: Springer, 2009. – 245 p.
8. Килин, С.Я. Квантовая криптография: идеи и практика / С.Я. Килин, Д.Б. Хорунжий. – Минск: Беларуская навука, 2007. – 391 с.
9. Халикова, Н.Х. Криптографик тизимларнинг хавфсизлигини таъминлашнинг долзарб масалалари / Н.Х. Халикова // Ўзбекистон Миллий университети хабарлари. – 2022. – № 2. – Б. 112-118.
10. Mosca, M. Cybersecurity in an era with quantum computers: will we be ready? / M. Mosca // IEEE Security & Privacy. – 2018. – Vol. 16, № 5. – P. 38-41.

(cc) BY