POSTKVANT KRIPTOGRAFIYASINING ASOSIY TAMOYILLARI VA VAZIFALARI

https://doi.org/10.70728/conf.v2.i02.030

Abduraximov Baxtiyor Fayziyevich[1], Boyquziyev Ilxom Mardanoqulovich[2], Arabboyev Alisher Avazbek o'g'li[3]
[1]Mirzo Ulug'bek nomidagi O'zbekiston milliy universiteti,
[2]Muhammad Al-Xorazmiy nomidagi TATU,
[3]Farg'ona davlat texnika univeristeti,
[1]a_baxtiyor@mail.ru
[2]salyut2017@gmail.com
[3]alisher_arabboev@mail.ru

Annotatsiya: Ushbu tezis postkvant kriptografiyasining asosiy tamoyillari va vazifalariga bag'ishlangan. Tezis kvant hisoblashning rivojlanishi bilan bog'liq bo'lgan tahdidlar va zamonaviy kriptografik tizimlarning zaif tomonlari hamda kvant kompyuterlariga nisbatan qiyin bo'lgan matematik muammolar asosida yaratilgan postkvant kriptografik usullarga qaratilgan.

Аннотация: Статья посвящена основным принципам и задачам постквантовой криптографии. В статье рассматриваются угрозы, связанные с развитием квантовых вычислений, и слабые стороны современных криптографических систем, а также постквантовые криптографические методы, созданные на основе математических задач, сложных для квантовых компьютеров.

Abstract: This article is devoted to the basic principles and tasks of post-quantum cryptography. The article focuses on the threats associated with the development of quantum computing and the weaknesses of modern cryptographic systems, as well as post-quantum cryptographic methods created based on mathematical problems that are difficult for quantum computers.

Kalit so'zlar: kvant tahdidlari, postkvant kriptografiyasi, kriptografik algoritmlar, NIST standartlari.

Ключевые слова: квантовые угрозы, постквантовая криптография, криптографические алгоритмы, стандарты NIST.

Key words: quantum threats, post-quantum cryptography, cryptographic algorithms, NIST standards.

Kirish

Postkvant kriptografiya kvant kompyuterlari tomonidan amalga oshirilishi mumkin bo'lgan hisoblash qudratiga qarshi bardosh bera oladigan kriptografik algoritmlarni ishlab chiqishga qaratilgan kriptografiyaning yangi yo'nalishidir. An'anaviy kriptografik

tizimlar, jumladan RSA, DSA, Diffie-Hellman va elliptik egri chiziqlar asosidagi kriptotizimlar bugungi kompyuterlar uchun xavfsiz hisoblansada, kvant kompyuterlari ushbu tizimlarni tezda buzishga qodir. Aynan shuning uchun postkvant kriptografiya hozirgi va kelajak axborot xavfsizligini ta’minlashda muhim ahamiyat kasb etadi.

Postkvant kriptografiyaning asosiy tamoyili bu - kvantga chidamli, ya’ni kvant kompyuterlari uchun ham yechimi amalda imkonsiz bo‘lgan matematik muammolarga asoslangan algoritmlarni ishlab chiqishdir. Bunda shifrlash, kalit almashish va raqamli imzo kabi asosiy kriptografik funksiyalarni yangilash zarur bo‘ladi [1]. Bu algoritmlar turli matematik asoslarga tayanadi, masalan panjara (lattice), kod nazariyasi (code-based), ko‘p o‘zgaruvchili polinomlar (multivariate polynomial), hash-funksiyalarga asoslangan tizimlar va izogeniyalar asosidagi yondashuvlar. Har biri kvant hisoblashga qarshi o‘ziga xos ustunlik va murakkablik darajasiga ega.

Postkvant kriptografiyaning muhim tamoyillaridan yana biri mavjud infratuzilmaga mos bo‘lishiligi. Ya’ni yangi algoritmlar amaldagi protokollar va tizimlar bilan integratsiyalashuvga yaroqli bo‘lishi, amaliy jihatdan samarali va resurslar jihatidan tejamkor bo‘lishi lozim. Chunki xavfsizlikdan tashqari, ish tezligi, xotira sarfi, tarmoqli kengligi kabi omillar ham muhim ahamiyatga ega [2].

Tadqiqot usuli

Postkvant kriptografiyaning asosiy vazifalaridan biri - ma’lumotlarni shifrlash va ularni saqlashda kvant hujumlariga qarshi mustahkam himoyani ta’minlashdir. Bu ayniqsa maxfiy ma’lumotlar, moliyaviy tranzaksiyalar, davlat sirlarini uzatish yoki shaxsiy sog‘liq ma’lumotlarini himoyalashda dolzarbdir [3].

Shuningdek, raqamli imzolarni yangilash orqali ma’lumotlarning haqiqiyligi va ishonchliligi ta’minlanadi. Kalit almashish mexanizmlari ham kvant tahdidiga bardosh beruvchi tarzda qayta ko‘rib chiqilishi zarur. Bularning barchasi mavjud tizimlarni bosqichma-bosqich yangilashni, ya’ni migratsiya jarayonini talab etadi. Bu jarayonda “gibrid” yondashuv qo‘llanilishi mumkin, bunda eski va yangi algoritmlar birgalikda ishlaydi.

Amaliy jihatdan postkvant kriptografiyaning joriy etilishi banklar, elektron hukumat, sog‘liqni saqlash tizimi, sanoat tarmoqlari, IoT qurilmalari va bulutli xizmatlarda xavfsizlikni ta’minlashga xizmat qiladi. Ayniqsa, uzoq muddatli xavfsizlik muhim bo‘lgan sohalarda bu texnologiya muhim ahamiyatga ega. Hozirda NIST (National Institute of Standards and Technology) tomonidan postkvant kriptografik algoritmlarni standartlashtirish ishlari olib borilmoqda va ayrim algoritmlar allaqachon tanlab olingan.

Natijalar

So‘nggi o‘n yilliklarda keng qo‘llanilayotgan kriptografik tizimlar (RSA, ECC va boshqalar) matematik qiyin muammolar - butun sonni faktorizatsiya qilish va diskret

logarifm muammosiga asoslangan. Biroq, kvant hisoblash texnologiyalarining rivojlanishi bu tizimlarning xavfsizligiga jiddiy tahdid solmoqda. Xususan, kvant kompyuterlarining rivojlanishi bilan an'anaviy kriptografik tizimlar, masalan, RSA va elliptik egri egri (ECC), xavfsizlik nuqtai nazaridan zaiflashmoqda. Shor algoritmi kabi kvant algoritmlari bu tizimlarning asosiy matematik muammolarini samarali ravishda yechishi mumkin. Bunday tahdidlarga qarshi turish uchun postkvat kriptografiyasi (PQC) ishlab chiqilgan bo'lib, u kvant kompyuterlariga chidamli bo'lgan kriptografik algoritmlarni yaratishga qaratilgan.

PQC xavfsizligi kvant kompyuterlari yordamida yechish qiyin bo'lgan matematik muammolarga asoslanadi. Bu muammolar quyidagi toifalarga bo'linadi:

- Lattice-based (panjara asosli) bu toifadagi algoritmlar xavfsizligi panjara asosidagi muammolarining qiyinligiga asoslanadi [4]. Panjara - bu n-o'lchovli fazodagi vektorlarning diskret guruhi. Eng mashhur muammolar quyidagilar [5]:

- Qisqa Vektor Muammosi (SVP) - berilgan panjarada eng qisqa nolga teng bo'lmagan vektorni toping;
- Eng Yaqin Vektor Muammosi (CVP) - berilgan nuqtaga eng yaqin panjara vektorini toping;
- Learning With Errors (LWE) Muammosi - bu muamma ko'p panjara muammolaridan amaliyroq hisoblanadi.

CRYSTALS-Kyber va CRYSTALS-Dilithium algoritmlari yuqorida keltirilgan panjara asosidagi muammolar qiyinligiga asoslangan [6].

- Code-based (kod asosli) bu toifadagi algoritmlar kod nazariyasiga asoslanadi. Masalan, Classic McEliece;

- Hash-based (xesh asosli) bu toifadagi algoritmlar xesh funksiyalariga asoslanadi. Masalan, SPHINCS+;

- Multivariate (ko'p o'zgaruvchili) bu toifadagi algoritmlar chekli maydonlardagi ko'p o'zgaruvchili polinom tenglamalar sistemasini yechish qiyinligiga asoslanadi. Masalan, Rainbow.

PQC quyidagi asosiy kriptovazifalarni bajaradi:

- Kalit almashish - bu vazifa ikki tomon o'rtasida xavfsiz kalit almashishni ta'minlaydi;
- Shifrlash - bu vazifa ma'lumotlarni shifrlash orqali ularning maxfiyligini ta'minlaydi;
- Imzolash - bu vazifa ma'lumotlarning butunligini va manbaini tasdiqlashni ta'minlaydi.

Muhokama

Postkvant kriptografiyaning rivojlanishi va joriy etilishi bir qator muhim amaliy va nazariy masalalarni keltirib chiqarmoqda. Tadqiqot natijalari shuni ko‘rsatadiki, turli matematik asoslarga ega bo‘lgan postkvant algoritmlar o‘rtasida sezilarli farqlar mavjud.

Panjara asosidagi algoritmlar, xususan NIST tomonidan tanlangan Kyber, kichik kalit hajmi va yuqori tezlik bilan ajralib turishi bilan amaliy qo‘llanish uchun juda mos keladi. Biroq, ularning xavfsizligi hali to‘liq isbotlanmagan matematik gipotezalarga asoslanganligi muammo sifatida qolmoqda. Kod asosidagi algoritmlar, masalan McEliece, uzoq vaqt davomida o‘rganilgan va matematik jihatdan ishonchli hisoblanadi, ammo katta kalit hajmlari ularni cheklangan resurslarga ega bo‘lgan qurilmalarda qo‘llashni qiyinlashtiradi [7].

Ko‘p o‘zgaruvchili va xesh asosidagi algoritmlar nisbatan soddaroq matematik tuzilishga ega bo‘lishiga qaramay, ularning ko‘pchiligi kalit hajmi yoki hisoblash murakkabligi jihatidan samaradorlik muammolariga duch kelmoqda.

Muhim muammolardan biri - bu turli postkvant algoritmlarining bir-biri bilan muvofiqligi va mavjud infratuzilma bilan integratsiyasi. Ko‘pgina an’anaviy tizimlar postkvant algoritmlarining katta kalit hajmlari va qo‘shimcha hisoblash talablarini qo‘llab-quvvatlash uchun moslashtirilishi kerak.

Xulosa

Xulosa qilib aytganda, postkvant kriptografiya bu nafaqat kelajak uchun xavfsizlik kafolati, balki hozirdanoq ko‘rilishi lozim bo‘lgan strategik ehtiyojdir. Texnologik taraqqiyot tahdidlarni keltirib chiqarishi mumkin bo‘lsada, unga qarshi ilg‘or ilmiy va matematik yondashuvlar bilan javob berish mumkin. Postkvant kriptografiya shu jihatdan axborot xavfsizligining yangi poydevorini yaratadi.

FOYDALANILGAN ADABIYOTLAR

[1] Dam,D.-T.; Tran, T.-H.; Hoang, V.-P.; Pham, C.-K.; Hoang, T.-T. A Survey of Post-Quantum Cryptography: Start of a New Race. Cryptography 2023, 7, 40.

[2] Miklós Ajtai and Cynthia Dwork. A public-key cryptosystem with worst-case/average-case equivalence. pages 284–293, 1997.

[3] L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone. Report on post-quantum cryptography. NISTIR 8105, 2016. http://dx.doi.org/10.6028/NIST.IR.8105.

[4] ShiBai, Adeline Langlois, Tancrède Lepoint, Damien Stehlé, and Ron Steinfeld. Improved security proofs in lattice-based cryptography: Using the Rényi divergence rather than the statistical distance. pages 3–24, 2015.

[5] NIST. Module-Lattice-Based Key-Encapsulation Mechanism Standard; National Institute of Standards and Technology: Gaithersburg, MD,USA,2024.

[6] Roberto Avanzi, Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lep oint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé. CRYSTALS-Kyber– algorithm specifica tions and supporting documentation. Submission to the NIST post quantum project, 2017.

[7] Singh, H. Code-Based Cryptography: Classic McEliece, 2019. Available online: https://www.semanticscholar.org/paper/Code based-Cryptog-raphy:-Classic-McEliece-Singh/09a4bdf55d0ca5046a2cb868ef74dfb1a021a28d