

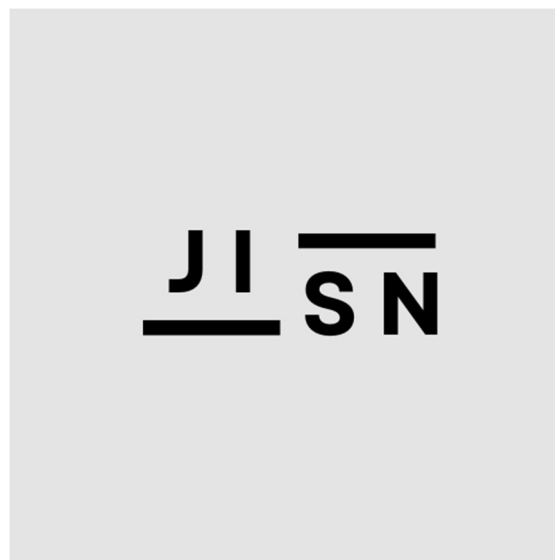
JOURNAL OF **INTERNATIONAL SCIENCE NETWORKS**



Vol. 1 No. 7 (2025)

Publisher

D-PRESS SERVICES



KVANT KOMPYUTERLARI VA AXBOROT XAVFSIZLIGINING YANGI DAVRI: ILMIY ASOSLAR VA AMALIY AHAMIYATI

¹ *Mamaraimov Abror Kamalidin o'g'li*, ² *Ziyotov Suhrobbek
Ulug'bek o'g'li*

¹ O'zbekiston Milliy universiteti Jizzax filiali katta o'qituvchisi, mamaraimovabror@gmail.com

² O'zbekiston Milliy universiteti Jizzax filiali talabasi. ziyatovsuhrob786@gmail.com



ANNOTATION:

So'nggi yillarda kvant kompyuterlari rivoji axborot texnologiyalari sohasida tub burilish yasamoqda. Ayniqsa, an'anaviy kriptografik algoritmlarning kvant hisoblashlar oldida zaiflashishi axborot xavfsizligiga yangi yondashuvlarni talab qilmoqda. Ushbu maqolada kvant kompyuterlarining ishlash prinsiplari, ularning mavjud shifrlash tizimlariga ta'siri hamda kvantga chidamli kriptografiyaning ilmiy asoslari va amaliy ahamiyati tahlil qilinadi.

KEYWORDS:

Kvant kompyuteri, kubit, kvant algoritmlari, kriptografiya, axborot xavfsizligi, Shor algoritmi, post-kvant kriptografiya, matematik model.

Accepted Date:

November 25, 2025,

Published Date:

November 30, 2025

Journal Website:

<https://d-pressa.com/index.php/jisn>
[/issue/view/jisn7](https://d-pressa.com/index.php/jisn/issue/view/jisn7)

License



This work is licensed under
a [Creative Commons
Attribution-
NonCommercial-
NoDerivatives 4.0
International License](https://creativecommons.org/licenses/by-nc-nd/4.0/).

Kirish

Axborot xavfsizligi zamonaviy raqamli jamiyatning eng muhim muammolaridan biri hisoblanadi. Internet, elektron hukumat, bank tizimlari va bulutli texnologiyalarning keng rivojlanishi ma'lumotlarni himoyalash masalasini dolzarb qilib qo'yimoqda [3]. Kvant kompyuterlarining paydo bo'lishi esa ushbu sohada yangi xavf va imkoniyatlarni yuzaga keltirdi.

An'anaviy kriptografik tizimlar matematik murakkablikka asoslangan bo'lib, klassik kompyuterlar uchun amalda yechilmas hisoblangan masalalarga tayanadi.[2] Biroq kvant kompyuterlari ushbu muammolarni juda qisqa vaqt ichida hal qila olish imkoniyatiga ega.[5]

Asosiy qism

Kvant kompyuterlarining ishlash prinsiplari: Kvant kompyuterlari klassik bitlar o'rniga kubitlar (quantum bit) dan foydalanadi. Kubitlar quyidagi xususiyatlarga ega:

- Superpozitsiya — kubit bir vaqtning o'zida 0 va 1 holatida bo'lishi mumkin;
- Entanglement (chirmashuv) — kubitlar o'zaro bog'lanib, masofadan qat'i nazar bir-biriga ta'sir qiladi;
- Interferensiya — noto'g'ri holatlar yo'qotilib, to'g'ri yechim kuchaytiriladi.

Bu xususiyatlar kvant kompyuterlarga murakkab hisoblashlarni parallel tarzda bajarish imkonini beradi.

Kvant algoritmlari va kriptografiyaga ta'siri: Kvant kompyuterlarining axborot

xavfsizligiga eng katta tahdidi — Shor algoritmi hisoblanadi.[2] Ushbu algoritm yordamida katta sonlarni tub ko'paytuvchilarga ajratish juda tez amalga oshiriladi.

RSA algoritmining xavfsizligi quyidagi matematik masalaga asoslanadi[2]:

$$N=p \cdot q$$

Bu yerda p va q — katta tub sonlar. Klassik kompyuterlar uchun bu masala juda murakkab bo'lsa, kvant kompyuterlar uchun u amaliy jihatdan tez yechiladi[5].

Shuningdek, Grover algoritmi simmetrik shifrlash tizimlarining xavfsizligini ikki barobarga kamaytiradi, bu esa kalit uzunligini oshirishni talab qiladi[2].

Post-kvant kriptografiyaning ilmiy asoslari: Kvant xavflariga qarshi post-kvant kriptografiya tushunchasi joriy etilgan. U quyidagi matematik asoslangan algoritmlarga tayangan holda ishlab chiqiladi:

- panjaraviy (lattice-based) kriptografiya;
- kodlarga asoslangan shifrlash;
- ko'p o'zgaruvchili polinomlarga asoslangan algoritmlar;
- xesh-funksiyalarga asoslangan raqamli imzolar.

Ushbu algoritmlar kvant kompyuterlar uchun ham hisoblash jihatidan murakkab hisoblanadi[1],[2].

Kvant texnologiyalarining axborot xavfsizligidagi amaliy qo'llanilishi: Kvant texnologiyalari nafaqat xavf, balki yangi imkoniyatlarni ham yaratadi. Jumladan:

- Kvant kalit almashinuvi (QKD) — fizik qonunlarga asoslangan mutlaq xavfsiz aloqa[4];

- Kvant tasodifiy sonlar generatori — kriptografik mustahkamlikni oshiradi;

- Gibrid kriptotizimlar — klassik va kvantga chidamli algoritmlarni birlashtiradi.

Bugungi kunda Google, IBM va Microsoft kompaniyalari kvant xavfsizlik yechimlarini faol ishlab chiqmoqda[5].

Iqtisodiy va xavfsizlik jihatidan tahlil

Iqtisodiy jihatlar:

- eski kriptotizimlarni almashtirish katta moliyaviy xarajat talab qiladi;

- ma'lumotlarni oldindan kvantga chidamli formatga o'tkazish iqtisodiy samaradorlikni oshiradi;

- axborot sizib chiqishi bilan bog'liq yo'qotishlar kamayadi.

Xavfsizlik jihatlar: Agar kvant tahdidlariga tayyorgarlik ko'rilmasa, bank, davlat va harbiy tizimlar jiddiy xavf ostida qoladi[1]. Shu sababli kvantga chidamli kriptografiyaga o'tish strategik ahamiyatga ega.

Xulosa

Kvant kompyuterlari axborot xavfsizligi sohasida yangi davrni boshlab bermoqda. Ular mavjud kriptografik tizimlarga jiddiy tahdid solishi bilan birga, xavfsizlikni yangi darajaga olib chiqadigan imkoniyatlarni ham yaratmoqda. Post-kvant kriptografiyaning rivoji kelajakda axborot tizimlarining barqarorligi va ishonchligini ta'minlashda muhim rol o'ynaydi.

Foydalanilgan adabiyotlar:

1. Qodirov S.S., Ismoilov D.T. *Axborot xavfsizligi va kriptografik algoritmlar*. — Toshkent: Innovatsiya, 2019.

2. Xudoyberdiyev B.A. *Kriptografiya asoslari va axborotni himoyalash usullari*. — Toshkent: O'zbekiston Milliy Universiteti nashriyoti, 2020.

3. Rashidov Sh.X. *Axborot xavfsizligining zamonaviy muammolari*. Toshkent, 2021.

4. Mirzayev N.A. *Axborot xavfsizligida kvant kalit almashinuvi texnologiyalari*. // *Axborotlashtirish muammolari ilmiy to'plami*, 2022.

5. Qodirov F.E., To'ymurodova S.E. *Kvant kompyuterlar va ularning kelajagi*. // *Ilm-fan va innovatsiya ilmiy-amaliy konferensiya materiallari*. — Toshkent, 2025.

6. Kamolov, Dostonbek. (2023). GLOBALIZATION PHENOMENON AND GLOBALISM. 1. 4-9. 10.5281/zenodo.10433143.

7. Meiirkhan, Spanov & Kamolov, Dostonbek. (2023). MODERN PROBLEMS AND SOLUTIONS OF DEMOCRACY AND MORALITY IN UZBEKISTAN СОВРЕМЕННЫЕ ПРОБЛЕМЫ И ПУТИ ИХ РЕШЕНИЯ В ОБЛАСТИ ДЕМОКРАТИИ И ПРАВСТВЕННОСТИ В УЗБЕКИСТАНЕ. 1. 168-172. 10.5281/zenodo.10113202.

8. Tirkashev U. THE NEGATIVE IMPACT OF INFLATION IN THE WORLD ON THE WELL-BEING OF THE POPULATION, THE COST OF PRODUCTS AND SERVICES // *Journal of Contemporary World Studies*. – 2024. – T. 2. – №. 1. – С. 26-30.