

**KVANT KOMPYUTERLARI RIVOJLANISHINING RSA
SHIFRLASH ALGORITMIGA TA'SIRI****Asatullayeva Hosila Sobir qizi**

Termiz davlat universiteti

60610300-Kompyuter injiniringi

yo'nalishi talabasi

Annotatsiya: Mazkur maqolada kvant kompyuterlarining rivojlanishi va ularning zamonaviy kriptografiya tizimlariga, xususan RSA shifrlash algoritmiga ta'siri tahlil qilinadi. RSA algoritmining ishlash tamoyillari, uning xavfsizligi asoslangan matematik muammolar hamda kvant kompyuterlarida qo'llaniladigan Shor algoritmining imkoniyatlari yoritilgan. Shuningdek, kvant texnologiyalarining rivojlanishi natijasida yuzaga keladigan xavflar va ularga qarshi ishlab chiqilayotgan kvantga chidamli kriptografik usullar haqida ma'lumot berilgan

Kalit so'zlar: kvant kompyuteri, RSA algoritmi, kriptografiya, axborot xavfsizligi, Shor algoritmi, kubit, kvant hisoblash, post-kvant kriptografiya.

Аннотация : В данной статье исследуется влияние развития квантовых компьютеров на безопасность алгоритма шифрования RSA, который является одним из наиболее распространённых методов криптографической защиты информации. Рассмотрены принципы работы алгоритма RSA, его математические основы и механизмы обеспечения безопасности. Особое внимание уделено возможностям квантовых вычислений и их потенциальному воздействию на современные криптографические системы.

В ходе исследования проанализированы особенности квантовых компьютеров, включая использование кубитов, принципов суперпозиции и квантовой запутанности. Также рассмотрен алгоритм Шора, позволяющий эффективно решать задачу факторизации больших чисел, лежащую в основе криптостойкости RSA. Показано, что создание масштабируемых и отказоустойчивых квантовых компьютеров может существенно снизить уровень безопасности существующих систем открытого ключа.

На основе анализа научной литературы и современных исследований сделан вывод о том, что, несмотря на сохранение практической надёжности RSA в настоящее время, дальнейшее развитие квантовых технологий представляет

серьезную долгосрочную угрозу для данного алгоритма. В связи с этим обоснована необходимость перехода к постквантовой криптографии и внедрения новых криптографических стандартов, устойчивых к атакам со стороны квантовых компьютеров.

Ключевые слова: квантовый компьютер, алгоритм RSA, криптография, алгоритм Шора, постквантовая криптография, информационная безопасность, кубит, факторизация, шифрование.

Abstract : This article examines the impact of quantum computer development on the security of the RSA encryption algorithm, one of the most widely used methods for protecting digital information. The study discusses the working principles of RSA, its mathematical foundations, and the mechanisms that ensure its cryptographic security. Particular attention is given to the capabilities of quantum computing and their potential influence on modern cryptographic systems.

The research analyzes the fundamental concepts of quantum computing, including qubits, superposition, and quantum entanglement. Furthermore, Shor's algorithm, which enables the efficient factorization of large integers, is examined as a major threat to the security assumptions underlying RSA encryption. The findings indicate that the emergence of large-scale, fault-tolerant quantum computers could significantly weaken the security of current public-key cryptographic systems.

Based on a review of scientific literature and recent technological developments, the study concludes that although RSA remains practically secure under current computational conditions, continued advances in quantum technologies pose a serious long-term challenge to its reliability. Therefore, the transition to post-quantum cryptography and the adoption of quantum-resistant cryptographic standards are essential to ensure future information security.

Keywords: Quantum Computing, RSA Algorithm, Cryptography, Shor's Algorithm, Post-Quantum Cryptography, Information Security, Qubit, Factorization, Encryption.

KIRISH

Bugungi kunda axborot texnologiyalari jamiyatning barcha sohalariga chuqur kirib bormoqda. Davlat boshqaruvi, bank tizimlari, elektron tijorat, sog'liqni saqlash va ta'lim kabi muhim sohalarda katta hajmdagi ma'lumotlar elektron shaklda saqlanadi va uzatiladi. Ushbu ma'lumotlarning maxfiyligi, yaxlitligi va xavfsizligini ta'minlash uchun turli kriptografik algoritmlar qo'llaniladi. Eng keng tarqalgan ochiq kalitli kriptografik tizimlardan biri RSA algoritmi hisoblanadi. RSA ko'plab internet xizmatlari, elektron imzo tizimlari va xavfsiz aloqa

protokollarining asosini tashkil etadi. Biroq, kvant kompyuterlarining rivojlanishi RSA algoritmining xavfsizligiga jiddiy tahdid tug'dirmoqda. Kvant texnologiyalarining rivojlanishi natijasida ilgari yechish qiyin bo'lgan matematik masalalarni qisqa vaqt ichida hal qilish imkoniyati paydo bo'lmoqda.

RSA shifrlash algoritmining ishlash prinsipi

RSA algoritmi 1977-yilda Ronald Rivest, Adi Shamir va Leonard Adleman tomonidan ishlab chiqilgan. Ushbu algoritmi ochiq kalitli kriptografiya tamoyiliga asoslanadi. RSA tizimida foydalanuvchi ikkita kalitga ega bo'ladi:

Ochiq kalit (Public Key);

Yopiq kalit (Private Key).

Ochiq kalit ma'lumotlarni shifrlash uchun, yopiq kalit esa ularni deshifrlash uchun ishlatiladi. RSA algoritmining asosiy afzalligi shundaki, ochiq kalit hammaga ma'lum bo'lsa ham, yopiq kalitni aniqlash amaliy jihatdan juda murakkab hisoblanadi.

Algoritmining xavfsizligi katta tub sonlardan tashkil topgan sonlarni faktorlashning murakkabligiga bog'liq. Hozirgi klassik kompyuterlar uchun 2048 bitli RSA kalitlarini buzish juda katta vaqt va hisoblash resurslarini talab qiladi.

Kvant kompyuterlarining asosiy afzalliklari:

Parallel hisoblash imkoniyati;

Katta hajmdagi ma'lumotlarni tez qayta ishlash;

Murakkab matematik masalalarni samarali yechish.

Kvant kompyuterlarining RSA algoritmiga ta'siri

1994-yilda Peter Shor kvant kompyuterlari uchun maxsus algoritmi – Shor algoritmini taklif qildi. Ushbu algoritmi katta sonlarni tub ko'paytuvchilarga juda tez ajratish imkonini beradi.

Agar yetarlicha quvvatli kvant kompyuterlari yaratilsa, RSA algoritmining asosiy himoya mexanizmi zaiflashadi. Chunki Shor algoritmi yordamida RSA kalitlarini hosil qiluvchi katta sonlarni qisqa vaqt ichida faktorlash mumkin bo'ladi.

Natijada:

1. RSA bilan himoyalangan ma'lumotlarni buzish osonlashadi.
2. Elektron tijorat tizimlari xavf ostida qoladi.
3. Bank va moliyaviy operatsiyalar xavfsizligi pasayadi.
4. Davlat va harbiy axborot tizimlariga tahdid kuchayadi.
5. Internetdagi ko'plab xavfsizlik protokollarini yangilash zarurati tug'iladi.

Kvantga chidamli kriptografiya

RSA algoritmgiga bo'lgan tahdid sababli olimlar kvantga chidamli kriptografik algoritmlarni ishlab chiqmoqdalar. Ushbu algoritmlar kvant kompyuterlari hujumlariga bardosh bera oladigan matematik muammolarga asoslanadi.

Kvantga chidamli kriptografiyaning asosiy yo'nalishlari:

Panjaralarga asoslangan kriptografiya (Lattice-based cryptography);

Kodlarga asoslangan kriptografiya;

Hash-funksiyalarga asoslangan imzo tizimlari;

Ko'p o'zgaruvchili kriptografik tizimlar.

Bu algoritmlar kelajakda RSA va boshqa an'anaviy shifrlash usullarining o'rnini bosishi mumkin.

METODOLOGIYA VA ADABIYOTLAR TAHLILI

Metodologiya: Ushbu tadqiqotda kvant kompyuterlarining rivojlanishi va ularning RSA shifrlash algoritmi xavfsizligiga ta'siri nazariy hamda tahliliy yondashuvlar asosida o'rganildi. Tadqiqot jarayonida ilmiy adabiyotlarni tahlil qilish, qiyosiy tahlil, mantiqiy umumlashtirish va sistemali yondashuv usullaridan foydalanildi.

Birinchi bosqichda RSA shifrlash algoritmining matematik asoslari, kalitlarni generatsiya qilish, shifrlash va deshifrlash jarayonlari o'rganildi. RSA algoritmi xavfsizligining asosi bo'lgan katta sonlarni faktorlash muammosining hisoblash murakkabligi tahlil qilindi.

Ikkinchi bosqichda kvant hisoblash texnologiyalarining nazariy asoslari, kubitlar, superpozitsiya va kvant chigallanishi kabi tushunchalar ko'rib chiqildi. Kvant kompyuterlarining klassik kompyuterlardan farqli jihatlari va hisoblash samaradorligi o'rganildi.

Uchinchi bosqichda Shor algoritmining RSA algoritmgiga ta'siri tahlil qilindi. Mazkur algoritmi yordamida katta sonlarni faktorlashning nazariy murakkabligi va uning amaliy oqibatlari baholandi. Shuningdek, RSA algoritmining kvant hisoblash muhitidagi zaif tomonlari aniqlanib, mavjud himoya mexanizmlarining samaradorligi ko'rib chiqildi.

Tadqiqotning yakuniy bosqichida post-kvant kriptografiya algoritmlarining imkoniyatlari va istiqbollari o'rganildi hamda ularning RSA algoritmgiga muqobil yechim sifatidagi afzalliklari baholandi.

Adabiyotlar tahlili : Kvant kompyuterlari va RSA algoritmi o'rtasidagi bog'liqlik so'nggi yillarda kriptografiya sohasidagi eng muhim tadqiqot

yo'nalishlaridan biriga aylandi. Mazkur yo'nalishdagi dastlabki fundamental ishlardan biri Rivest, Shamir va Adleman tomonidan yaratilgan RSA algoritmidir. Mualliflar ochiq kalitli kriptografiya konsepsiyasini taklif etib, katta sonlarni faktorlash muammosiga asoslangan yangi xavfsizlik mexanizmini ishlab chiqqanlar.

1994-yilda Peter Shor tomonidan taklif etilgan Shor algoritmi kriptografiya sohasida tub burilish yasadi. Muallif kvant kompyuterlari yordamida katta sonlarni polinomial vaqt ichida faktorlash mumkinligini matematik jihatdan isbotladi. Ushbu natija RSA algoritmining uzoq muddatli xavfsizligiga jiddiy tahdid sifatida baholandi.

Michael Nielsen va Isaac Chuangning kvant hisoblash bo'yicha ilmiy ishlarida kvant kompyuterlarining nazariy asoslari, kvant algoritmlari va ularning kriptografik tizimlarga ta'siri batafsil yoritilgan. Mualliflar kvant hisoblashning amaliy rivojlanishi RSA kabi an'anaviy algoritmlarni qayta ko'rib chiqishni talab qilishini ta'kidlaydilar.

William Stallings tomonidan yozilgan kriptografiya va tarmoq xavfsizligi bo'yicha adabiyotlarda RSA algoritmining ishlash prinsiplari, matematik asoslari hamda amaliy qo'llanilish sohalari keng tahlil qilingan. Ushbu manba RSA algoritmining afzalliklari va cheklovlarini tushunishda muhim nazariy asos bo'lib xizmat qiladi.

So'nggi yillarda olib borilgan tadqiqotlar post-kvant kriptografiya yo'nalishiga qaratilgan. Tadqiqotchilar panjara (lattice) asosidagi kriptotizimlar, kodlarga asoslangan algoritmlar va xesh-funksiyalarga asoslangan imzo sxemalarini kvant kompyuterlariga bardoshli yechim sifatida ko'rsatmoqdalar. Bu tadqiqotlar kelajakda RSA algoritmini bosqichma-bosqich almashtirish zarurligini ko'rsatadi.

Tahlil qilingan adabiyotlar shuni ko'rsatadiki, hozirgi vaqtda RSA algoritmi amaliy jihatdan xavfsiz bo'lib qolayotgan bo'lsa-da, kvant kompyuterlarining rivojlanishi uning uzoq muddatli istiqboliga salbiy ta'sir ko'rsatishi mumkin. Shu sababli ilmiy hamjamiyat tomonidan post-kvant kriptografiya algoritmlarini ishlab chiqish va joriy etish bo'yicha keng ko'lamli tadqiqotlar olib borilmoqda. Maqolangizning ***"Natijalar va muhokama"*** bo'limi uchun quyidagi ilmiy uslubdagi matndan foydalanishingiz mumkin.

NATIJALAR VA MUHOKAMA

Tadqiqot davomida RSA shifrlash algoritmining ishlash prinsiplari, uning matematik asoslari hamda kvant kompyuterlarining ushbu algoritm xavfsizligiga ta'siri o'rganildi. Olingan natijalar RSA algoritmining xavfsizligi katta sonlarni faktorlash muammosining murakkabligiga bevosita bog'liqligini tasdiqladi.

Tahlillar shuni ko'rsatdiki, klassik kompyuterlar yordamida 2048 bitli RSA kalitlarini buzish juda katta hisoblash quvvatini va uzoq vaqtni talab qiladi. Shu sababli

RSA algoritmi hozirgi kunda elektron tijorat, bank tizimlari, raqamli imzo va internet xavfsizligi sohalarida keng qo'llanilmoqda.

Biroq kvant hisoblash texnologiyalarining rivojlanishi RSA algoritmi uchun yangi xavflarni yuzaga keltirmoqda. Ayniqsa, Shor algoritmi nazariy jihatdan katta sonlarni polinomial vaqt ichida faktorlash imkonini berishi RSA xavfsizligining asosiy tamoyiliga tahdid soladi. Tadqiqot natijalari shuni ko'rsatadiki, yetarli miqdordagi barqaror va xatolarga bardoshli kubitlarga ega kvant kompyuterlari yaratilganda RSA algoritmining amaldagi kalit uzunliklari o'z himoya darajasini yo'qotishi mumkin.

Tahlil davomida RSA algoritmi va kvant hisoblash texnologiyalari o'rtasidagi munosabatlar qiyosiy ravishda baholandi. Natijalar quyidagilarni ko'rsatdi:

- * Klassik hisoblash muhitida RSA algoritmi yuqori darajadagi xavfsizlikni ta'minlaydi.

- * Kvant kompyuterlari rivojlanishi bilan RSA algoritmining matematik himoya mexanizmi zaiflashadi.

- * Kalit uzunligini oshirish klassik hujumlarga qarshi samarali bo'lsa-da, kvant hujumlariga nisbatan yetarli himoya bera olmaydi.

- * Kelajakda post-kvant kriptografik algoritmlar RSA algoritmining o'rnini bosishi ehtimoli yuqori.

Shuningdek, tadqiqot davomida "Harvest Now, Decrypt Later" konsepsiyasi ham muhokama qilindi. Ushbu yondashuvga ko'ra, hujumchilar bugungi kunda shifrlangan ma'lumotlarni yig'ib borishi va kelajakda kvant kompyuterlari yordamida ularni deshifrlashi mumkin. Bu esa uzoq muddat saqlanishi zarur bo'lgan maxfiy ma'lumotlar uchun jiddiy xavf tug'diradi.

Muhokama natijalari shuni ko'rsatadiki, kvant kompyuterlarining hozirgi rivojlanish darajasi RSA-2048 yoki undan katta kalitlarni amaliy tarzda buzish imkonini bermaydi. Biroq dunyoning yetakchi ilmiy markazlari va texnologik kompaniyalari tomonidan olib borilayotgan tadqiqotlar kelajakda bu imkoniyatning yuzaga kelishi ehtimolini oshirmoqda.

Shu sababli axborot xavfsizligi sohasida faoliyat yurituvchi tashkilotlar va mutaxassislar kvant davriga tayyorgarlik ko'rishlari zarur. Xususan, post-kvant kriptografiya standartlarini joriy etish, mavjud axborot tizimlarini modernizatsiya qilish hamda yangi xavfsizlik protokollarini ishlab chiqish muhim vazifa hisoblanadi.

Umuman olganda, tadqiqot natijalari kvant kompyuterlarining rivojlanishi RSA shifrlash algoritmi uchun uzoq muddatli strategik tahdid ekanligini ko'rsatdi. Mazkur holat zamonaviy kriptografik tizimlarni takomillashtirish va kvant hujumlariga bardoshli yangi algoritmlarni ishlab chiqish zaruratini yuzaga keltirmoqda.

Ushbu bo‘limdan keyin ilmiy maqolada odatda ***“Xulosa va takliflar”*** qismi beriladi. Bu qismda tadqiqot natijalari qisqacha umumlashtiriladi va amaliy tavsiyalar keltiriladi.

XULOSA

Ushbu tadqiqotda kvant kompyuterlarining rivojlanishi va ularning RSA shifrlash algoritmiga ko‘rsatadigan ta’siri nazariy hamda amaliy jihatdan tahlil qilindi. Tadqiqot natijalari RSA algoritmining zamonaviy axborot xavfsizligi tizimlarida muhim o‘rin egallashini va uning xavfsizligi katta sonlarni faktorlash masalasining hisoblash murakkabligiga asoslanishini ko‘rsatdi.

O‘rganishlar natijasida RSA algoritmi klassik kompyuterlar sharoitida yuqori darajadagi himoya ta’minlashi aniqlandi. Hozirgi kunda elektron tijorat tizimlari, internet-banking, elektron hukumat platformalari, VPN texnologiyalari, SSL/TLS protokollari va raqamli imzo tizimlarida RSA algoritmidan keng foydalanilmoqda. Katta uzunlikdagi kalitlardan foydalanish klassik hisoblash muhitida algoritmning ishonchliligini ta’minlaydi.

Biroq kvant kompyuterlarining jadal rivojlanishi mavjud kriptografik tizimlar uchun yangi tahdidlarni yuzaga keltirmoqda. Tadqiqot davomida Shor algoritmining ishlash tamoyili tahlil qilinib, u katta sonlarni faktorlash masalasini klassik algoritmlarga nisbatan ancha samarali yechishi mumkinligi aniqlandi. Natijada RSA algoritmining xavfsizlik asosi bo‘lgan matematik muammo kvant kompyuterlari uchun murakkab hisoblanmasligi mumkin.

Tadqiqot natijalari shuni ko‘rsatadiki, hozirgi vaqtda mavjud kvant kompyuterlari RSA-2048 kabi amaliy kriptografik kalitlarni buzish imkoniyatiga ega emas. Biroq ilmiy markazlar va texnologik kompaniyalar tomonidan kvant texnologiyalari sohasida olib borilayotgan izlanishlar kelajakda bunday imkoniyatlarning paydo bo‘lish ehtimolini oshirmoqda. Shu sababli bugungi kunda himoyalangan deb hisoblanayotgan ma’lumotlar ham uzoq muddatli istiqbolda xavf ostida qolishi mumkin.

Tahlillar natijasida “Harvest Now, Decrypt Later” strategiyasi alohida ahamiyatga ega ekanligi aniqlandi. Mazkur yondashuvda hujumchilar hozirgi vaqtda shifrlangan ma’lumotlarni yig‘ib borib, kelajakda qudratli kvant kompyuterlari paydo bo‘lganda ularni deshifrlashga urinadilar. Bu esa davlat boshqaruvi, moliyaviy sektor, sog‘liqni saqlash tizimlari va ilmiy tadqiqotlar bilan bog‘liq maxfiy ma’lumotlar uchun jiddiy xavf tug‘diradi.

Tadqiqot davomida post-kvant kriptografiya yo‘nalishining ahamiyati ham o‘rganildi. Kvant kompyuterlariga bardoshli yangi algoritmlarni ishlab chiqish va joriy

etish kelajakdagi axborot xavfsizligini ta'minlashning asosiy yo'nalishlaridan biri ekanligi aniqlandi. Panjara asosidagi, kodlarga asoslangan va xesh-funksiyalarga asoslangan kriptografik algoritmlar istiqbolli yechimlar sifatida baholanmoqda.

Shunday qilib, kvant kompyuterlarining rivojlanishi RSA shifrlash algoritmi uchun uzoq muddatli strategik tahdid hisoblanadi. Hozirgi davrda RSA algoritmi o'z ahamiyatini saqlab qolayotgan bo'lsa-da, kelajakda axborot xavfsizligini ta'minlash uchun post-kvant kriptografik standartlarga bosqichma-bosqich o'tish zarur. Davlat tashkilotlari, ilmiy markazlar va xususiy sektor vakillari kvant davriga tayyorgarlik ko'rishlari, mavjud kriptografik infratuzilmalarni modernizatsiya qilishlari hamda yangi xavfsizlik mexanizmlarini joriy etishlari lozim.

Natijada, kvant kompyuterlari va kriptografiya o'rtasidagi munosabatlar kelajakdagi axborot xavfsizligi tizimlarining rivojlanishida hal qiluvchi omillardan biri bo'lib qoladi. RSA algoritmi uzoq yillar davomida ishonchli himoya vositasi sifatida xizmat qilgan bo'lsa-da, kvant texnologiyalarining rivojlanishi yangi avlod kriptografik yechimlarini yaratish zaruratini yuzaga keltirmoqda.

Bu xulosa ilmiy maqola uchun taxminan **1–1,5 sahifa** hajmida bo'lib, mavzuning dolzarbligi, tadqiqot natijalari, amaliy ahamiyati va kelajakdagi istiqbollarni to'liq qamrab oladi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI

1. Rivest R. L., Shamir A., Adleman L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems // Communications of the ACM. – 1978. – Vol. 21, No. 2. – P. 120–126.
2. Shor P. W. Algorithms for Quantum Computation: Discrete Logarithms and Factoring // Proceedings of the 35th Annual Symposium on Foundations of Computer Science. – IEEE, 1994. – P. 124–134.
3. Nielsen M. A., Chuang I. L. Quantum Computation and Quantum Information. – Cambridge: Cambridge University Press, 2010. – 702 p.
4. Stallings W. Cryptography and Network Security: Principles and Practice. – 8th Edition. – London: Pearson Education, 2023. – 850 p.
5. Bernhardt C. Quantum Computing for Everyone. – Cambridge: MIT Press, 2019. – 216 p.
6. Yanofsky N. S., Mannucci M. A. Quantum Computing for Computer Scientists. – Cambridge University Press, 2008. – 372 p.
7. Paar C., Pelzl J. Understanding Cryptography: A Textbook for Students and Practitioners. – Berlin: Springer, 2010. – 390 p.

8. Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C. – 20th Anniversary Edition. – Wiley, 2015. – 784 p.
 9. Kaye P., Laflamme R., Mosca M. An Introduction to Quantum Computing. – Oxford University Press, 2007. – 274 p.
 10. Preskill J. Quantum Computing in the NISQ Era and Beyond // Quantum. – 2018. – Vol. 2. – Article 79.
 11. Chen L., Jordan S., Liu Y.-K., Moody D., Peralta R., Perlner R., Smith-Tone D. Report on Post-Quantum Cryptography. – Gaithersburg: National Institute of Standards and Technology (NIST), 2016.
 12. Bernstein D. J., Buchmann J., Dahmen E. Post-Quantum Cryptography. – Berlin: Springer, 2009. – 245 p.
 13. Katz J., Lindell Y. Introduction to Modern Cryptography. – 3rd Edition. – CRC Press, 2020. – 603 p.
 14. Menezes A., van Oorschot P., Vanstone S. Handbook of Applied Cryptography. – CRC Press, 1996. – 816 p.
 15. Alimov R., Tursunov B. Axborot xavfsizligi va kriptografiya asoslari. – Toshkent: O‘zbekiston Respublikasi Oliy ta’lim muassasalari uchun o‘quv qo‘llanma, 2021. – 320 b.
 16. Abdullayev A. Zamonaviy axborot xavfsizligi texnologiyalari. – Toshkent: Fan va texnologiyalar nashriyoti, 2022. – 285 b.
 17. NIST. Post-Quantum Cryptography Standardization Project. – AQSH Milliy Standartlar va Texnologiyalar Instituti materiallari.
 18. Quantum Computing Report. Global Developments in Quantum Technologies and Cybersecurity. – 2024.
 19. Arute F. va boshqalar. Quantum Supremacy Using a Programmable Superconducting Processor // Nature. – 2019. – Vol. 574. – P. 505–510.
 20. Mosca M. Cybersecurity in an Era with Quantum Computers: Will We Be Ready? // IEEE Security & Privacy. – 2018. – Vol. 16, No. 5. – P. 38–41.
- Agar universitetingiz **GOST, OAK (O‘zbekiston OAK talabi), APA 7 yoki IEEE** formatida adabiyotlar talab qilsa, ushbu ro‘yxatni aynan o‘sha standart bo‘yicha qayta rasmiylashtirib berishim mumkin.