

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/360005762>

# QUANTUM COMPUTER

Article in International Journal of Innovative Research in Science Engineering and Technology · April 2022

DOI: 10.15680/IJIRSET.2022.1104029

CITATIONS

0

READS

323

2 authors, including:



**A. Ospanova**

Al-Farabi Kazakh National University

251 PUBLICATIONS 610 CITATIONS

SEE PROFILE

Some of the authors of this publication are also working on these related projects:



IJIRSET APRIL [View project](#)



MAY XOSIYAT [View project](#)

# QUANTUM COMPUTER

Manoj Lakhani

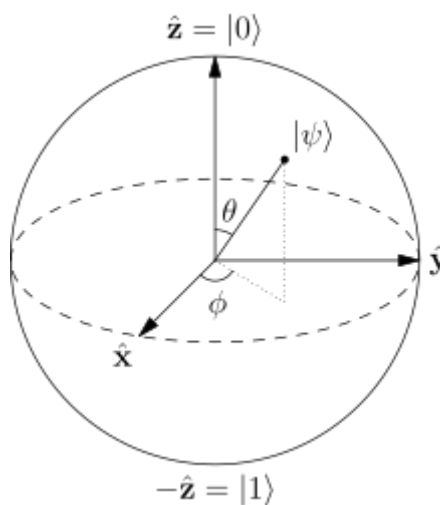
Assistant Professor, Department of Physics, M.L.V. Government College, Bhilwara, Rajasthan, India

**ABSTRACT:** Quantum computing is a type of computation that harnesses the collective properties of quantum states, such as superposition, interference, and entanglement, to perform calculations. The devices that perform quantum computations are known as quantum computers. Though current quantum computers are too small to outperform usual (classical) computers for practical applications, they are believed to be capable of solving certain computational problems, such as integer factorization (which underlies RSA encryption), substantially faster than classical computers. The study of quantum computing is a subfield of quantum information science. There are several types of quantum computers (also known as quantum computing systems), including the quantum circuit model, quantum Turing machine, adiabatic quantum computer, one-way quantum computer, and various quantum cellular automata. The most widely used model is the quantum circuit, based on the quantum bit, or "qubit", which is somewhat analogous to the bit in classical computation. A qubit can be in a 1 or 0 quantum state, or in a superposition of the 1 and 0 states. When it is measured, however, it is always 0 or 1; the probability of either outcome depends on the qubit's quantum state immediately prior to measurement. Efforts towards building a physical quantum computer focus on technologies such as transmons, ion traps and topological quantum computers, which aim to create high-quality qubits. These qubits may be designed differently, depending on the full quantum computer's computing model, as to whether quantum logic gates, quantum annealing, or adiabatic quantum computation are employed. There are currently a number of significant obstacles to constructing useful quantum computers. It is particularly difficult to maintain qubits' quantum states, as they suffer from quantum decoherence and state fidelity. Quantum computers therefore require error correction.

**KEYWORDS:** quantum, computer, calculations, machine, state, qubits, adiabatic, logic, gates

## I. INTRODUCTION

Any computational problem that can be solved by a classical computer can also be solved by a quantum computer. Conversely, any problem that can be solved by a quantum computer can also be solved by a classical computer, at least in principle given enough time. In other words, quantum computers obey the Church–Turing thesis. This means that while quantum computers provide no additional advantages over classical computers in terms of computability, quantum algorithms for certain problems have significantly lower time complexities than corresponding known classical algorithms. [1,2] Notably, quantum computers are believed to be able to quickly solve certain problems that no classical computer could solve in any feasible amount of time—a feat known as "quantum supremacy." The study of the computational complexity of problems with respect to quantum computers is known as quantum complexity theory. The prevailing model of quantum computation describes the computation in terms of a network of quantum logic gates. This model is a complex linear-algebraic generalization of boolean circuits. In quantum mechanics, probability vectors can be generalized to density operators. The quantum state vector formalism is usually introduced first because it is conceptually simpler, and because it can be used instead of the density matrix formalism for pure states, where the whole quantum system is known.[3,4]



**The Bloch sphere is a representation of a qubit, the fundamental building block of quantum computers.**

Progress in finding quantum algorithms typically focuses on this quantum circuit model, though exceptions like the quantum adiabatic algorithm exist. Quantum algorithms can be roughly categorized by the type of speedup achieved over corresponding classical algorithms. Quantum algorithms that offer more than a polynomial speedup over the best known classical algorithm include Shor's algorithm for factoring and the related quantum algorithms for computing discrete logarithms, solving Pell's equation, and more generally solving the hidden subgroup problem for abelian finite groups. These algorithms depend on the primitive of the quantum Fourier transform. No mathematical proof has been found that shows that an equally fast classical algorithm cannot be discovered, although this is considered unlikely. Certain oracle problems like Simon's problem and the Bernstein–Vazirani problem do give provable speedups, though this is in the quantum query model, [5] which is a restricted model where lower bounds are much easier to prove and doesn't necessarily translate to speedups for practical problems. Other problems, including the simulation of quantum physical processes from chemistry and solid-state physics, the approximation of certain Jones polynomials, and the quantum algorithm for linear systems of equations have quantum algorithms appearing to give super-polynomial speedups and are BQP-complete. Because these problems are BQP-complete, an equally fast classical algorithm for them would imply that no quantum algorithm gives a super-polynomial speedup, which is believed to be unlikely. [6] Some quantum algorithms, like Grover's algorithm and amplitude amplification, give polynomial speedups over corresponding classical algorithms. Though these algorithms give comparably modest quadratic speedup, they are widely applicable and thus give speedups for a wide range of problems. Many examples of provable quantum speedups for query problems are related to Grover's algorithm, including Brassard, Høyer, and Tapp's algorithm for finding collisions in two-to-one functions, which uses Grover's algorithm, and Farhi, Goldstone, and Gutmann's algorithm for evaluating NAND trees, which is a variant of the search problem. [7,8]

## II. DISCUSSION

A notable application of quantum computation is for attacks on cryptographic systems that are currently in use. Integer factorization, which underpins the security of public key cryptographic systems, is believed to be computationally infeasible with an ordinary computer for large integers if they are the product of few prime numbers (e.g., products of two 300-digit primes). [29] By comparison, a quantum computer could efficiently solve this problem using Shor's algorithm to find its factors. This ability would allow a quantum computer to break many of the cryptographic systems in use today, in the sense that there would be a polynomial time (in the number of digits of the integer) algorithm for solving the problem. In particular, most of the popular public key ciphers are based on the difficulty of factoring integers or the discrete logarithm problem, both of which can be solved by Shor's algorithm. In particular, the RSA, Diffie–Hellman, and elliptic curve Diffie–Hellman algorithms could be broken. These are used to protect secure Web pages, encrypted email, and many other types of data. Breaking these would have significant ramifications for electronic privacy and security. [9]

Identifying cryptographic systems that may be secure against quantum algorithms is an actively researched topic under the field of post-quantum cryptography. Some public-key algorithms are based on problems other than the integer factorization and discrete logarithm problems to which Shor's algorithm applies, like the McEliece cryptosystem based

on a problem in coding theory. Lattice-based cryptosystems are also not known to be broken by quantum computers, and finding a polynomial time algorithm for solving the dihedral hidden subgroup problem, which would break many lattice based cryptosystems, is a well-studied open problem. It has been proven that applying Grover's algorithm to break a symmetric (secret key) algorithm by brute force requires time equal to roughly  $2^{n/2}$  invocations of the underlying cryptographic algorithm, compared with roughly  $2^n$  in the classical case, meaning that symmetric key lengths are effectively halved: AES-256 would have the same security against an attack using Grover's algorithm that AES-128 has against classical brute-force search.

Since chemistry and nanotechnology rely on understanding quantum systems, and such systems are impossible to simulate in an efficient manner classically, many believe quantum simulation will be one of the most important applications of quantum computing. Quantum simulation could also be used to simulate the behavior of atoms and particles at unusual conditions such as the reactions inside a collider. Quantum simulations might be used to predict future paths of particles and protons under superposition in the double-slit experiment. About 2% of the annual global energy output is used for nitrogen fixation to produce ammonia for the Haber process in the agricultural fertilizer industry while naturally occurring organisms also produce ammonia. Quantum simulations might be used to understand this process increasing production. Quantum cryptography could potentially fulfill some of the functions of public key cryptography. Quantum-based cryptographic systems could, therefore, be more secure than traditional systems against quantum hacking.[10,11]

### III. RESULTS

Since quantum computers can produce outputs that classical computers cannot produce efficiently, and since quantum computation is fundamentally linear algebraic, some express hope in developing quantum algorithms that can speed up machine learning tasks. For example, the quantum algorithm for linear systems of equations, or "HHL Algorithm", named after its discoverers Harrow, Hassidim, and Lloyd, is believed to provide speedup over classical counterparts. Some research groups have recently explored the use of quantum annealing hardware for training Boltzmann machines and deep neural networks. In the field of computational biology, quantum computing has played a big role in solving many biological problems. One of the well-known examples would be in computational genomics and how computing has drastically reduced the time to sequence a human genome. Given how computational biology is using generic data modeling and storage, its applications to computational biology are expected to arise as well. Deep generative chemistry models emerge as powerful tools to expedite drug discovery. However, the immense size and complexity of the structural space of all possible drug-like molecules pose significant obstacles, which could be overcome in the future by quantum computers. Quantum computers are naturally good for solving complex quantum many-body problems and thus may be instrumental in applications involving quantum chemistry. Therefore, one can expect that quantum-enhanced generative models including quantum GANs may eventually be developed into ultimate generative chemistry algorithms. Hybrid architectures combining quantum computers with deep classical networks, such as Quantum Variational Autoencoders, can already be trained on commercially available annealers and used to generate novel drug-like molecular structures.[12,13]

One of the greatest challenges involved with constructing quantum computers is controlling or removing quantum decoherence. This usually means isolating the system from its environment as interactions with the external world cause the system to decohere. However, other sources of decoherence also exist. Examples include the quantum gates, and the lattice vibrations and background thermonuclear spin of the physical system used to implement the qubits. Decoherence is irreversible, as it is effectively non-unitary, and is usually something that should be highly controlled, if not avoided. Decoherence times for candidate systems in particular, the transverse relaxation time  $T_2$  (for NMR and MRI technology, also called the dephasing time), typically range between nanoseconds and seconds at low temperature. Currently, some quantum computers require their qubits to be cooled to 20 millikelvin (usually using a dilution refrigerator in order to prevent significant decoherence). A 2020 study argues that ionizing radiation such as cosmic rays can nevertheless cause certain systems to decohere within milliseconds.

As a result, time-consuming tasks may render some quantum algorithms inoperable, as maintaining the state of qubits for a long enough duration will eventually corrupt the superpositions.[14,15]

These issues are more difficult for optical approaches as the timescales are orders of magnitude shorter and an often-cited approach to overcoming them is optical pulse shaping. Error rates are typically proportional to the ratio of operating time to decoherence time, hence any operation must be completed much more quickly than the decoherence time.

## REFERENCES:

1. Кобилов, А. У., & Джурабоев, А. М. (2020). Технологии компьютерного дистанционного обучения. *Academic Research in Educational Sciences*, 1 (3), 287-293.
2. Махкамбаев, А., Джурабоев, А. (2022). Использование адаптивной физической культуры при обучении студентов с инвалидностью и особыми физическими потребностями. Проблемы і перспективи розвитку спортивних ігор і єдиноборств у вищих навчальних закладах, 1(2), 133-137.
3. Джўрабаев, А. М., Казоков, Р. Т. (2021). Биомеханик тахлиллар асосида енгил атлетикачиларнинг функционал тайёргарлигидаги корреляция алоқаларининг тахлили. *Yoshlarni qo'llab-quvvatlash va aholi salomatligini mustahkamlash yili*ga bag'ishlangan, 4(4), 198-208.
4. Kazonov, R. T., Djuraboev, A. M. (2021). Kredit modul tizimi nima. Ta'limni raqamlashtirish sharoitida pedagog kadrlarni qayta tayyorlash va malakasini oshirish, 4(4), 198-206.
5. Djuraboev, A. M., Bozorova, S. X., Aminova, A. A. (2021). Jamiyatimizda jismonan sog'lom avlod tarbiyasi. Бешта муҳим ташаббус буюк келажак пойдевори, 3(3), 205-209.
6. Ibodov, A. I., Beknazarov, Sh. Q., Djuraboev, A. M. (2021). Yuridik bilim berish v amalaka oshirish tizimini takomillashtirishning yangi uflari. Ta'limni raqamlashtirish sharoitida pedagog kadrlarni qayta tayyorlash va malakasini oshirish, 2(3), 195-201.
7. Djuraboev, A. M., Akbarov, A. (2021). Ilmiy tadqiqot materiallari bilan ishlashda zamonaviy AT foydalanish. Zamonaviy sharoitda JT va sportni ommaviy rivojlantirishning innovatsion yo'nalishlari, 1(2), 188-197.
8. Эшназарова, М. Ю., Катаева, М. М., Мадаминжанов, А. Д. (2021). Теоретические основы использования возможностей мобильного обучения в образовательном процессе. Экономика и социум, 4(83), 1239-1243.
9. Eshnazarova, M. Y., Katayeva, M. M. (2021). Theoretical basis of mobile learning and use of mobile platforms. *International Journal on Integrated Education*, 4(1), 184-187.
10. Eshnazarova, M., Toshboyev, S. (2020). Pedagogical Basis and Organization of Distance Learning in Modern Educational. *The American Journal of Social Science and Educational Innovations*, 2(2), 614-619.
11. Эшназарова, М. Ю., Тошбоев, С. М. (2020). Замонавий таълимда масофавий ўқитишнинг педагогик асослари ва ташкил этилиши. Современное образование (Узбекистан), 10(95), 18-24.
12. Эшназарова, М. Ю., & Настинов, С. Т. (2020). Мобил таълим ва мобил платформалардан фойдаланишнинг назарий асослари. *Academic Research in Educational Sciences*, 1 (4), 513-518.
13. Имомов, А., Эшназарова, М. Ю., Тошбоев, С. М. (2020). Чизикли алгебраик тенгламалар системаси мавзусини Муаммоли технология асосида ўқитиш. Modern informatics and its teaching methods, 1(1), 197-202.
14. Эшназарова, М. Ю., Ҳасанов, С. С., & Жамалов, О. О. (2020). Мобил иловалар яратиш технологиялари ва уларнинг имкониятлари. *Academic Research in Educational Sciences*, 1(4), 548-556
15. Eshnazarova, M., Nurmatov, B. (2019). The current state and content of the course Methods of calculations. *International Journal of Research Culture Society*, 3(3), 79-83.
16. Eshnazarova, M. Y. (2019). Mobility as a principle of modernization of higher pedagogical education. *Scientific Bulletin of Namangan State University*, 1(12), 327-332.
17. Eshnazarova, M. (2019). Some requirements and principles of mobile learning. *Scientific Bulletin of Namangan State University*, 1(2), 266-270.
18. Mambetaliev, KA (2022). Integration of Sciences in the Scientific and Professional and Educational Process. *International Journal of Innovative Research in Science Engineering and Technology*. 2(2), 1662-1663.
19. Ерғешова, Ф. А., Мамбеталиев, Қ. (2022). Оқитуды ұйымдастыру формалар. *Central Asian Academic Journal of Scientific Research*, 2(1), 158-168.
20. Ғанибаева, Б. Ш., Мамбеталиев, Қ. А. (2021). Бастауыш сынып өзбек және қазақ тіліндегі ана тілі оқулықтарының салыстырмалы сипаты. МУҒАЛЛИМ ҲӘМ ҮЗЛИКСИЗ БИЛИМЛЕНДИРИҰ, 5(5), 143-148.
21. Мамбеталиев, Қ. А. (2021). Бастауыш сыныпта ана тілі пәнін тиімді оқытып үйретудің сапасын арттыруда мәтінмен жұмысты ұтымды ұйымдастыру. МУҒАЛЛИМ ҲӘМ ҮЗЛИКСИЗ БИЛИМЛЕНДИРИҰ, 6(6), 151-155.
22. Мамбеталиев, Қ. (2021). XX ғасыр басындағы өзбек-қазақ халықтарының әдеби байланыстары. *Academic Research in Educational Sciences*, 2(12), 959-964.
23. Buriyev, B. U., Qodirov, R. R., Kazonov, R. T. (2021). Jismoniy tarbiya va sportda axborot kommunikatsiya texnologiyasining tuzilishi va tamoyillari. Ta'limda zamonaviy axborot texnologiyalaridan foydalanishning innovatsion usullari, 5(5), 555-559.
24. Казоков, Р. Т., Бекназаров, Ш. Қ., Ибодов, А. И. (2021). Футболчиларнинг антропометрик ўлчамлари ва тезлик сифатлари орасидаги корреляциясини ўрганишда ақт дан фойдаланиш. Тиббиёт ва спорт, 1(10), 27-30.
25. Казоков, Р. Т. (2019). Талабаларга ахборот хавфсизлигини таъминлаш компонентлигини ривожлантиришнинг ҳукукий асослари. Ўзбекистон давлат санат ва маданият институти хабарлари, 4(12), 61-68.
26. Жуманова, Ф. У., Мирзарахмонова, Ш. М. (2021). Дуал таълим ва унинг имкониятлари. Бошқарув ва Этика Қоидалари онлайн илмий журналы, 1(6), 122-124.
27. Mirzaahmadovna, M. S. (2021). Didactic System of Vocational Guidance of Students on the Basis of Dual Education. *European Journal of Life Safety and Stability*, 11, 5-8.
28. Mirzarakhmonova, S. M. (2021). Talabalar kasbiy shakllanishida shaxs yo'nalganlik motivlarini ahamiyati. Муғаллим ҳәм узликсиз билимлендириў, 5(5), 43-45.
29. Қораев, С. Б.; Мирзарахмонова, Ш. М. (2021). Таълим тизимида ижтимоий-гуманитар фанлар. Илмий методологик ва илмий услубий журнал, 1(188), 16-20.
30. Mirzarakhmonova, S. M. (2021). Advantages of a dual-based learning system in vocational education. *Results of Modern Scientific Research and Development*, 1(1), 222-225.
31. Мирзарахмонова, Ш. М. (2021). Таълимнинг инновацион кластерида дуал таълимни ташкил этиш асослари. *Academic research in educational sciences*, 2(4), 154-158.
32. Абдухаликова, Н. Р., Рустамов, У. Р., Тилолов, И.И. (2022). Исследование влияния магнитных полей на суперионную проводимость. Современная наука и образование, 3(94), 66-69.
33. Суяров, К. Т., Абдухаликова, Н. Р., Суяров, А. А. (2022). Физика в офтальмологических исследованиях. Экономика и социум, 3(94), 1211-1216.
34. Абдухаликова, Н. Р., Азимова, Д. Д. (2021). Особенности проектной деятельности в образовании физики в школах. Экономика и социум, 10(89), 1340-1346.