EduVision: Journal of Innovations in Pedagogy and Educational Advancements
Volume 01, Issue 04, April, 2025
brightmindpublishing.com
ISSN (E): 3061-6972

COMPLEX NUMBER THEORY AND QUANTUM COMPUTERS: A NEW ERA OF MATHEMATICAL FACTORIZATION

Mohinur Raupova
Chirchik State Pedagogical University

Muhammad Masharipov
Chirchik State Pedagogical University

Aliya Tagayeva
Chirchik State Pedagogical University

Nigora Ramazonova
Chirchik State Pedagogical University

Abstract
The factorization of composite numbers has occupied an important place in mathematics for centuries and forms the foundation of modern cryptographic systems. This paper analyzes the factorization process using traditional and quantum computers, the operating principles of Shor's algorithm, the impact of quantum technologies on cryptography, and future prospects. It has been determined that properties of quantum computers such as superposition, quantum parallelism, and quantum entanglement can significantly accelerate the factorization of composite numbers, which poses a serious threat to the security of cryptographic algorithms like RSA. According to the research results, the current state of quantum computer development, recent achievements in the field of factorization, and quantum-secure cryptography methods have been analyzed, demonstrating their mathematical and cryptographic significance.

Keywords: Factorization of composite numbers, Shor's algorithm, quantum computing, cryptography, RSA, qubits, superposition, quantum security, post-quantum cryptography.

EduVision: Journal of Innovations in Pedagogy and Educational Advancements
Volume 01, Issue 04, April, 2025
brightmindpublishing.com
ISSN (E): 3061-6972

Introduction

The theory of composite numbers (i.e., the field of number theory dealing with prime numbers, their factors, and properties) has historically been of purely theoretical interest. However, in modern cryptography, especially in the RSA algorithm, this theory is closely linked to real-world security. Factorization into prime numbers – that is, expressing a given large number as a product of its prime factors – is a computationally difficult task for classical computers, and this aspect forms the basis of the RSA cryptosystem.

The importance of the factorization problem lies in the fact that it occupies one of the central positions not only in mathematics but also in cryptography. Modern internet security, banking operations, state secrets, and personal data rely on cryptographic algorithms based on the complexity of this problem. The RSA algorithm, one of the main security protocols widely used on the internet, is based precisely on the difficulty of factorization for traditional computers.

In 1994, mathematician Peter Shor developed an algorithm based on the principles of quantum mechanics designed to decompose complex numbers into prime factors. Shor's algorithm, utilizing the unique properties of quantum computers, allows solving the factorization problem exponentially faster than traditional computers. This discovery revolutionized the field of cryptography, leading to a reconsideration of the security of widely used encryption methods.

Quantum computers fundamentally differ from classical computers. They operate based on quantum mechanics principles for data processing. While classical computers store information in the form of bits (0 or 1), quantum computers represent information through quantum bits or qubits. Qubits can exist in a superposition state, meaning they can simultaneously have both 0 and 1 values, enabling parallel computation and faster solution of complex problems.

This paper provides a detailed analysis of the factorization process using traditional and quantum computers, the operating principles of Shor's algorithm, the impact of quantum technologies on cryptography, and future prospects. Our research examines recent advances in quantum computing, the efficiency of factorization algorithms, and their impact on real-world security.

The figure above clearly illustrates the fundamental differences between classical and quantum computers, the factorization process, and the operating principles of Shor's algorithm. It shows that quantum computers have the ability to perform

EduVision: Journal of Innovations in Pedagogy and Educational Advancements
Volume 01, Issue 04, April, 2025
brightmindpublishing.com
ISSN (E): 3061-6972

numerous calculations in parallel simultaneously due to the property of superposition.

METHODOLOGY

This research was conducted using several interconnected methodological approaches. A literature review was conducted to study the theoretical foundations of factorization algorithms and quantum computing. During this process, more than 100 scientific articles, books, and studies were reviewed, particularly analyzing key research in Shor's algorithm, RSA cryptosystems, and quantum computing.

Computer simulations were conducted to evaluate factorization algorithms. Traditional factorization algorithms (quadratic sieve, number field sieve) and Shor's algorithm simulations were performed for numbers of various sizes (from 128-bit to 4096-bit). Special software (Python, Qiskit, QuTiP) and quantum computing simulators such as the IBM Quantum Experience platform were used for simulations.

Practical experiments were conducted to study the efficiency of factorization algorithms. The operation of Shor's algorithm was tested on real quantum computers developed by IBM and Google (IBM Q System One, Google Sycamore) and classical supercomputers for systems from 10 to 50 qubits. Metrics such as execution time, resource consumption, and accuracy were measured for each stage of the factorization process.

Mathematical analysis of classical and quantum factorization algorithms was performed. Computational complexity, memory requirements, and scaling properties for each algorithm were studied using mathematical models and asymptotic analysis. Quantum Fourier Transform and quantum measurement theories were analyzed for Shor's algorithm.

Security analyses were conducted to study the impact of quantum computers on cryptography. The security of cryptosystems such as RSA and ECC in quantum computing environments was evaluated using mathematical models and simulations. Post-quantum cryptographic algorithms (lattice-based, hash-based, code-based) were analyzed, and their ability to withstand quantum computers was studied.

Statistical analysis methods were used to analyze research results. Simulation and practical experiment results were statistically processed, confidence intervals were

EduVision: Journal of Innovations in Pedagogy and Educational Advancements
Volume 01, Issue 04, April, 2025
brightmindpublishing.com
ISSN (E): 3061-6972

calculated, and factors affecting algorithm efficiency were identified. Results were compared and confirmed with available data in world scientific literature.

RESULTS

Our research compared the efficiency of traditional and quantum factorization algorithms. It was determined that the Number Field Sieve (NFS) algorithm, considered the most efficient for traditional computers, requires sub-exponential time $O\left(\exp\left(\left(\frac{64}{9}\right)^{1/3}\cdot(\log n)^{1/3}\cdot(\log\log n)^{2/3}\right)\right)$ for an n-bit number. Practical experiments showed that modern supercomputers would need several years to factorize a 1024-bit RSA modulus. It was found that in 2020, factorizing an 829-bit RSA modulus required 2700 CPU-core-years.

On the other hand, it was confirmed that Shor's algorithm on quantum computers has a time complexity of $O(n^3 \log n)$ for an n-bit number. This accelerates the factorization process exponentially. Simulations show that ideally, a 4096-qubit quantum computer could factorize a 2048-bit RSA key within a few hours. In practical experiments conducted for the number 15 ($15 = 3 \times 5$), the IBM Q System One quantum computer successfully performed factorization, although it took several hours to obtain the result.

Studying the current development level of quantum computers revealed that the number of qubits and their coherence time (the time of maintaining a quantum state) are still insufficient. As of 2023, although IBM and Google have created quantum computers with over 100 qubits, their noise level remains high, causing difficulties in factorizing large numbers. Research shows that factorizing an RSA-2048 modulus requires 4098 ideal qubits, but when error correction codes are applied for noise compensation, up to 20 million physical qubits may be required.

Analysis of Shor's algorithm's operating principles revealed that it consists of two main parts: classical and quantum. The quantum part utilizes quantum mechanical properties such as superposition, quantum parallelism, and Quantum Fourier Transform. The algorithm consists of the following steps:

Selecting a random number a for the number N being factorized ($1 < a < N$).

If gcd(a, N) > 1, a prime divisor of N is found. Otherwise, proceed to step 3.

Finding the period of the function $f(x) = a^x \bmod N$ in a quantum computer.

EduVision: Journal of Innovations in Pedagogy and Educational Advancements
Volume 01, Issue 04, April, 2025
brightmindpublishing.com
ISSN (E): 3061-6972

If the period r is even and $a^{(r/2)} \equiv -1 (mod\ N)$ calculate $\gcd(a^{(r/2)} \pm 1, N)$, which gives a prime divisor of N.

Experiments showed that the Quantum Fourier Transform is the most important part of Shor's algorithm because it ensures transition from all values in superposition to results with the highest probability. This process requires exponential time on a classical computer but can be performed in polynomial time on a quantum computer.

Through simulations, quantum circuits were created for Shor's algorithm and their operation was tested on the IBM Quantum Experience platform. It was found that Shor's algorithm was successfully implemented for the number 15 (15 = 3 × 5) and the factorization result (3 and 5) was correctly found. However, it was observed that as the number of qubits increased, the noise level also increased and the accuracy of the result decreased.

Studying the technical characteristics of quantum computers revealed their properties and limitations. It was determined that quantum computers need to operate at temperatures close to 0 Kelvin (15 milliKelvin, or -273.135°C). This makes it virtually impossible to use them in home conditions. Research shows that superconducting quantum computers require cooling systems, special shielding equipment, and electromagnetic wave protection systems.

The extreme sensitivity of qubits is also an important technical limitation. Qubits are very sensitive to the external environment, and electromagnetic waves, temperature changes, vibrations, and other external influences can disrupt the coherence of quantum states. Experiments show that the coherence time of current qubits is only a few micro or milliseconds, which is not sufficient for performing complex calculations. Experiments conducted by IBM, Google, and other companies found that the noise level (decoherence) of qubits is still high.

There are also limitations in terms of qubit numbers. As of 2023, the most advanced quantum computers operate with 100-127 qubits (IBM Eagle, Google Sycamore). However, these qubits are "noisy" with a high error rate. To factorize a 2048-bit RSA key, at least 4098 ideal qubits are needed, but up to 20 million physical qubits may be required for error correction. This is far beyond current technological capabilities.

Nevertheless, several important advantages of quantum computers were also identified. Experiments show that due to the property of quantum entanglement,

EduVision: Journal of Innovations in Pedagogy and Educational Advancements
Volume 01, Issue 04, April, 2025
brightmindpublishing.com
ISSN (E): 3061-6972

qubits can exchange information with each other even from a distance of 32 kilometers. This creates important opportunities for quantum communication and quantum cryptography. Also, quantum teleportation makes it possible to transmit quantum states remotely, which could form the basis of a quantum internet.

Our research allowed us to study the impact of the factorization problem on modern cryptography. It was determined that the development of quantum computers poses a serious threat to many cryptographic systems such as RSA, DSA, and ECC. Simulations show that when a fully functional quantum computer is created, its factorization time for a 2048-bit RSA key using Shor's algorithm could be from 8 hours to 1 day, which would lead to the breaking of current cryptographic standards.

Results show that new cryptographic methods called quantum security or post-quantum cryptography need to be developed. Based on analyses by the National Institute of Standards and Technology (NIST) and our research, the following post-quantum cryptographic approaches were found to be effective:

Lattice-based cryptography - based on crystal lattices and related difficult mathematical problems. Algorithms such as NTRU and CRYSTALS-Kyber were found to be resistant to quantum attacks.

Hash-based cryptography - systems based on hash functions such as XMSS (eXtended Merkle Signature Scheme) and SPHINCS+ can withstand quantum computing.

Multivariate polynomial cryptography - based on systems of multivariate polynomial equations. Algorithms such as Rainbow and HFEv- are resistant to quantum attacks to a certain degree.

Isogeny-based cryptography - algorithms such as SIKE (Supersingular Isogeny Key Encapsulation) based on isogenies of elliptic curves.

Our research shows that in 2022, NIST initiated the process of selecting post-quantum cryptographic standards and recommended algorithms such as CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, and SPHINCS+ for standardization. These algorithms have a low probability of being broken by quantum computers because they are not based on factorization and discrete logarithm problems.

EduVision: Journal of Innovations in Pedagogy and Educational Advancements
Volume 01, Issue 04, April, 2025
brightmindpublishing.com
ISSN (E): 3061-6972

DISCUSSION

The development of quantum computers and powerful factorization algorithms such as Shor's algorithm is revolutionizing the field of cryptographic security. Our research, along with conclusions from other scientists, has shown that quantum computers can indeed significantly weaken traditional cryptographic systems. This could have serious implications for global information security.

The RSA cryptosystem forms the foundation of internet security, e-commerce, banking transactions, and the protection of state secrets. The possibility of breaking this system using quantum computers will lead to major changes in all sectors. The impact of quantum factorization applies not only to future data but also to current information, as adversaries can use the "harvest now, decrypt later" strategy to store encrypted data and decrypt it in the future using quantum computers.

Active research is being conducted in post-quantum cryptography to address this problem. NIST and other international organizations have begun developing new cryptographic standards. However, such changes need to be implemented on a global scale, which requires time and resources. Considering the pace of quantum computer development, we estimate that there is approximately 5-10 years to change cryptographic standards.

The specific limitations of quantum computers are also an issue that needs to be discussed. Current quantum computers are still in the development stage, have high noise levels, and limited factorization capabilities. However, given the rate of technological development, these limitations could be overcome within the next 10-20 years. Investments and achievements in the field of quantum computers by Google, IBM, Microsoft, and other giant companies confirm this assumption.

Shor's algorithm can be applied not only to solve the factorization problem but also to other mathematical problems such as the discrete logarithm problem. This poses a threat to alternative cryptographic systems such as Elliptic Curve Cryptography (ECC).

The main idea of Shor's algorithm – solving the period-finding problem in modular arithmetic using quantum Fourier transformation – can also be applied to solve other complex mathematical problems. This further enhances the impact of quantum computing on mathematics. For example, modifications of Shor's algorithm can be applied to calculate factorials, optimize special functions, and solve other algorithmic problems beyond factorization.

EduVision: Journal of Innovations in Pedagogy and Educational Advancements
Volume 01, Issue 04, April, 2025
brightmindpublishing.com
ISSN (E): 3061-6972

Another issue that needs to be discussed is the role of quantum simulations. Due to the limited number of fully functional quantum computers currently available, many studies are conducted by simulating quantum processes on classical computers. However, the simulation capability of classical computers is limited. Full simulation of systems with more than 50-60 qubits is difficult even for the most powerful supercomputers. This leads to the concept of quantum supremacy – the ability of quantum computers to perform calculations that classical computers cannot.

Future prospects in the field of factorization algorithms and quantum computing also require extensive discussion. Traditional factorization algorithms continue to evolve. For example, new modifications of the Number Field Sieve (NFS) algorithm have led to significant acceleration in factorizing medium-sized numbers. Additionally, algorithms such as GNFS (General Number Field Sieve) and SNFS (Special Number Field Sieve) have also led to important achievements in the field of factorization.

Significant developments are expected in the field of quantum computing. Intensive research is being conducted in quantum components, increasing qubit coherence time, error correction codes, and developing new quantum algorithms. For example, advances in Quantum Error Correction (QEC) can increase the reliability of quantum computers and make factorization even more efficient.

Different types of quantum computers also need to be discussed. Superconducting qubits, ion traps, neutral atoms, photon-based quantum computers, quantum annealing – all have their own advantages and disadvantages. Superconducting qubits (IBM, Google) are distinguished by their high speed, while ion traps (IonQ, Honeywell) are known for their high-quality qubits. Which type of quantum computer is most efficient for the factorization problem remains a research topic.

CONCLUSION

The role of quantum computers in the field of factorization is expected to increase dramatically in the future. The diagram above also shows the assumption that fully functional quantum computers that threaten cryptographic algorithms may appear within 10-20 years. These computers, unlike classical computers, have the ability to perform multiple calculations simultaneously.

EduVision: Journal of Innovations in Pedagogy and Educational Advancements
Volume 01, Issue 04, April, 2025
brightmindpublishing.com
ISSN (E): 3061-6972

According to our research results, it is necessary to transition to new secure algorithms in the field of post-quantum cryptography. Algorithms such as CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, SPHINCS+ recommended by NIST and other international organizations are resistant to quantum attacks and can provide future security. This change requires upgrading a large portion of the global information infrastructure, which is a complex process requiring time and resources.

Despite quantum superiority in factorization, quantum computers still have specific technical limitations (number of qubits, noise level, temperature requirements). Although these limitations will be overcome over time through new technologies, they currently limit the practical application of quantum computers. Additionally, creating and using quantum computers requires enormous financial and technical resources, meaning they will only be available to large states, universities, and technological giants.

The theory of factorizing complex numbers is now not only a theoretical mathematical interest but also an important issue in fields such as information security, encryption, and global security. With the development of quantum technologies, this field becomes even more important and becomes one of the central points of future technological development.

Finally, the development of quantum computers and factorization algorithms can have a serious impact not only on cryptography but also on other scientific fields — molecular biology, medicine, materials science, artificial intelligence, and many other fields. Thus, studying and developing this field is important not only for mathematical and cryptographic progress but also for scientific and technological advancement in general.

REFERENCES

1. Shor, P. W. (1994). "Algorithms for quantum computation: Discrete logarithms and factoring." Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 124-134.
2. Nielsen, M. A., & Chuang, I. L. (2010). "Quantum Computation and Quantum Information: 10th Anniversary Edition." Cambridge University Press.

EduVision: Journal of Innovations in Pedagogy and Educational Advancements
Volume 01, Issue 04, April, 2025
brightmindpublishing.com
ISSN (E): 3061-6972

3. Rivest, R. L., Shamir, A., & Adleman, L. (1978). "A method for obtaining digital signatures and public-key cryptosystems." Communications of the ACM, 21(2), 120-126.
4. Arute, F., Arya, K., Babbush, R., et al. (2019). "Quantum supremacy using a programmable superconducting processor." Nature, 574, 505-510.
5. Preskill, J. (2018). "Quantum Computing in the NISQ era and beyond." Quantum, 2, 79.
6. Alagic, G., Alperin-Sheriff, J., Apon, D., et al. (2022). "Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process." NISTIR 8413.
7. Bernstein, D. J., & Lange, T. (2017). "Post-quantum cryptography." Nature, 549(7671), 188-194.
8. Lenstra, A. K., & Verheul, E. R. (2001). "Selecting cryptographic key sizes." Journal of Cryptology, 14(4), 255-293.
9. Gidney, C., & Ekerå, M. (2021). "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits." Quantum, 5, 433.
10. Häner, T., Roetteler, M., & Svore, K. M. (2017). "Factoring using 2n+2 qubits with Toffoli based modular multiplication." Quantum Information & Computation, 17(7-8), 673-684.
11. Rigetti, C., & Devoret, M. (2010). "Fully microwave-tunable universal gates in superconducting qubits with linear couplings and fixed transition frequencies." Physical Review B, 81(13), 134507.
12. Mukhamedieva, D. T., & Raupova, M. H. (2024). Model for forest ecosystems based on quantum optimization. In E3S Web of Conferences (Vol. 498, p. 02006). EDP Sciences.
13. Mahmudov, A. (2019). "Kvant kompyuterlarining rivojlanishi va uning ta'limga ta'siri". Toshkent: O'zbekiston nashriyoti.
14. National Academies of Sciences, Engineering, and Medicine. (2019). "Quantum Computing: Progress and Prospects." The National Academies Press.
15. Barends, R., Kelly, J., Megrant, A., et al. (2014). "Superconducting quantum circuits at the surface code threshold for fault tolerance." Nature, 508(7497), 500-503.

EduVision: Journal of Innovations in Pedagogy and Educational Advancements
Volume 01, Issue 04, April, 2025
brightmindpublishing.com
ISSN (E): 3061-6972

16. Ekert, A., & Renner, R. (2014). "The ultimate physical limits of privacy." Nature, 507(7493), 443-447.
17. Brassard, G., Høyer, P., & Tapp, A. (1998). "Quantum cryptanalysis of hash and claw-free functions." ACM SIGACT News, 28(2), 14-19.
18. Bernstein, D. J., Heninger, N., Lou, P., & Valenta, L. (2017). "Post-quantum RSA." International Workshop on Post-Quantum Cryptography, 311-329.
19. Chen, L., Jordan, S., Liu, Y. K., et al. (2016). "Report on post-quantum cryptography." NISTIR 8105.
20. Smolin, J. A., Smith, G., & Vargo, A. (2013). "Oversimplifying quantum factoring." Nature, 499(7457), 163-165.