Journal of Quantum Algorithms and Cryptography (JQAC)
https://utilitasmathematicapublishing.com
Vol: 1, ISSUE: 1, 2025
Pg No: 12-15

The Effects of Quantum Computing on Secure Communication

Ahmed AIT AMEUR[1], Hichem ELMOSSAOUI[2], Nadia OUKID[3]

[1,2,3] LAMDA-RO Laboratory, Department of Mathematics, Faculty of Sciences, University Saad Dahlab Blida1, BP 270 Soumâa, Blida, Algeria

Abstract: This paper's abstract aims to provide a basic overview of post-quantum algorithms and how quantum computing works in relation to existing cryptography. The following areas are impacted: community key encoding approaches, symmetric structures, upright quantum cryptography, differences between quantum and conventional computing, challenges in quantum computation, and quantum processes (Shor's and Grover's). Chapters on Post-Quantum Cryptography include topics like as code-based encoding, hash-based signs, lattice-built cryptography, multivariate-built cryptography, and other mathematically based quantum critical circulation approaches. Quantum computing is one of the contemporary technologies that our civilization uses. Many groups and organizations throughout the globe are working to improve quantum computing applications. At the same time, artificial intelligence is a steady emerging area. Finding out how AI-related applications will change as a result of progress in quantum computing research is the primary objective of this effort. So, computational approaches are used in the methodology of the research. In order to draw conclusions on the growing influence of quantum computing research on a specific AI application from this study. In addition to discussing the effects of quantum computing on the field of artificial intelligence, this paper also delves into the implications and possibilities of this technology for that area.

I. INTRODUCTION

The philosophical implications of quantum computing for global finance are substantial. When it's for sale, it will improve related technologies and help us tackle complex issues in ways we've never imagined, with benefits seen across many industries. Many industries that rely on large datasets and intricate computations stand to benefit greatly from the advent of commercial quantum computers. This includes healthcare, economics, artificial intelligence, big data, and scientific and medical research. On the other hand, the technology might be harmful as the same computer capacity could be used to breach cybersecurity. According to this, a quantum computer running Shor's algorithm could theoretically decrypt all of the world's encryption in a matter of days, perhaps even hours. To provide some perspective, the identical job would take an antiquated computer thousands of years to accomplish. Quantum computing is one of the most cutting-edge technologies in use today. Numerous groups and organizations throughout the globe are working to advance the field of quantum computing and its potential uses. Artificial intelligence is another rapidly evolving but more stable area of study today. Finding out how AI applications will change as a result of progress in quantum computing research is the primary objective of this effort. So, computational approaches are used in the methodology of the research. in order to derive conclusions on the growing influence of quantum computing research on a specific AI application from this study. In addition to discussing the effects of quantum computing on the field of artificial intelligence, this paper also delves into the implications and possibilities of this technology for that area. This study examines the potential societal impacts of the rapidly expanding subject of quantum computing. Three main areas are covered: optimization, cryptography, and simulation of quantum systems. We will also address the ethical considerations and safety measures that should be taken in light of these advancements. In the next five to ten years, effective quantum computing will be a reality, say several experts. Major breakthroughs in the study of quantum computers in the last few years lend credence to the idea. Once quantum computing becomes a reality, current asymmetric algorithms will be obsolete. This will have an effect on many parts of network security, including e-commerce, SSL/TLS, authentication mechanisms, and more. Cybersecurity experts need to know what quantum computing means and where research into quantum proof algorithms stands. The impact of post- and quantum computing on cryptography is explored in this journal's comprehensive overview of the field.

https://utilitasmathematicapublishing.com

Vol: 1, ISSUE: 1, 2025

Pg No: 12-15

II. QUANTUM COMPUTING

One useful use of quantum-powered ideology is quantum computing. Quantum computing takes use of sophisticated computer equipment, and physical material exhibits properties of both particles and waves at microscopic scales. In addition to the fact that the workings of quantum diplomacies remain a mystery to conventional physical science, a fully functional quantum computer may do some functions 10 times faster than a little more conventional "standard" computer. The unusual moment is stationary, mostly experimental, and impractical, but a complete quantum computer may crash known encoding techniques and allow physicists to execute physical imitations. The qubit, analogous to the bit in traditional digital computing, is the basic building block of quantum computing. Unlike a traditional bit, a qubit may exist in both states at the same time by use of the principle of superposition of its two "base" conditions. Measuring a qubit still yields a probabilistic standard bit as a consequence. By manipulating the qubit in a certain way, a quantum computer may enhance the intended measurement results via wave interference effects. In order for a quantum computer to do calculations efficiently, designers must create practices that are known as quantum algorithms. In order to build a functional quantum computer, it is required to keep an item in a superposition state for an extended period of time so that it may undergo several operations. Regrettably, when interacting with materials that make up a measured system, a superposition loses its transitory state, called decoherence, and becomes just a regular classical bit. Quantum states must be readable while also being shielded from decoherence by use of devices. Several processes are working on different angles to tackle this issue, such as creating more robust error-checking methods or using more trustworthy quantum processes.

III. CRYPTOGRAPHY

Cryptography is the study and practice of constructing and evaluating methods that prevent unauthorized parties from deciphering private communications. Current cryptography is at the crossroads of several disciplines, including mathematics, computer science, electrical engineering, digital signal distribution, physical science, and information security. Data secrecy, data integrity, verification, and non-negotiation are cornerstones of cryptography and of information security more generally. Commonplace applications of cryptography include online transactions, digital currencies, computer passwords, and military communications. Mathematics and computer science are strongly influencing modern cryptography. Cryptographic systems are difficult for adversaries to break in real usage because they are built on standards of computational strength. Exploiting a well-constructed building is doable in theory, but doing it in practice is intolerable. The continuous reevaluation and, if required, modification of these procedures is important in light of hypothetical expansions and faster computing expertise. These strategies are called computationally protected if they are well-planned. In contrast to information-theoretically secure schemes, such as the one-time pad, which can be shown to be unbreakable even with unlimited computer power, the most computationally secure approaches that are theoretically breakable are more difficult to plan in advance.

You will briefly learn about the role of hash functions, proportional algorithms, and irregular algorithms in modern cryptography in this chapter. We examine the problem of factoring large numbers and the difficulty of discrete logarithms. Secure asymmetric cyphers are built upon this basis.

A. Symmetric Cryptography: In symmetric cryptography, the sender and the receiver use the same secret key and same cryptographic process to encrypt and decode data. Bob, for instance, may decipher a plaintext message encrypted by Alice using the same cryptographic process and shared secret key. Due to the critical need for secrecy, no one other than Bob should know the secret key, so a trustworthy means of transmitting secret keys over the Internet is required.

B. Asymmetric Cryptography: Asymmetrical cryptography. Asymmetric cryptography, or public key cryptography (PKC), continues to be an encoding method where the solutions are shared in pairs. It is recommended that each party get both a public key and a private key. For instance, if Bob wanted to encrypt a message, Alice could provide him her public key and then Bob could use it to encrypt the message. After then, Bob would send the encrypted message to Alice, who, using her private key, could decode it. Consequently, the message is encrypted using a public key, and only the person in possession of the private key may decipher it.

https://utilitasmathematicapublishing.com

Vol: 1, ISSUE: 1, 2025

Pg No: 12-15

IV. IMPACT OF QUANTUM COMPUTING IN CRYPTOGRAPHY

The advent of quantum computing has completely altered our perspective on computer security. Quantum computers not only threaten the privacy and security of cryptographically-reliant data and communications, but they can also handle computational glitches orders of magnitude faster than current classical computing architectures. Some network traffic may be being recorded and stored by malicious actors who may decode it when powerful enough quantum computers become accessible. As a result, we need to start thinking about the future now by making our products and industrial infrastructures easy to update and modify. Commercially available quantum computers will have a profound effect on many different industries that rely on large amounts of data and complex planning, including economics, statistics, artificial intelligence, and many more. The technique may do harm, however, since the same computing volume may be used to undermine cybersecurity. Particularly worrisome are terrorist threats to public key cryptography. In 1994, MIT scientist Peter Shor foresaw this danger and developed "Shor's algorithm," a quantum algorithm for factoring integers (also known as prime factorization, the method used to generate solutions in public key cryptography). This suggests that in a matter of days, or perhaps hours, a quantum computer running Shor's algorithm could decrypt the majority of the world's encryption. For a traditional computer to do the same process, it would take thousands of years to establish this hooked on perception. Using a computational system based on the irrational and irregular physical properties of matter at a real tiny gauge, known as a quantum mechanism, a calculation called "quantum computing" is carried out. One qubit in a quantum computer may encrypt more than two conditions, unlike a traditional computer constructed on an electrical transistor, which can only encode data in binary digits (or "bits") that can only be "1" or "0" ("on" or "off"). Although it is theoretically possible for each qubit to hold a superposition of several states, the mathematics involved is too complex for the purposes of this article's conclusions. Avoiding confusion with "quantum cryptography," which is still the study of applying quantum physics to cryptographic procedures, is the goal of quantum computing. An excellent example of this is Quantum Key.
Both symmetrical essential processes and traditional community crucial procedures are significantly threatened by quantum computers. The goal of building a fully operational global quantum computer capable of running strong quantum algorithms like Shor's and Grover's algorithms seems to be getting closer by the day. This technological advancement is crucial since it guarantees the complete failure of the present community-essential, well-planned safe processes, such RSA and Elliptic Curve Cryptosystems. A survey of cryptographic arrangements that are immune to quantum computing, such as quantum key distribution systems, protocols, mathematically constructed keys, framework-grounded cryptography, hash-based signatures, and code-based cryptography, is the response scheduled to that danger.

V. CONCLUSION

Data storage and transmission in the modern day must be as secure as possible since data is so important. With the advent of quantum computers, two long-standing symmetric key processes and public-key algorithms like RSA, El Gamal, ECC, and DSA are in serious danger (3DES, AES). It seems like we're getting closer to building a fully functional global quantum computer that can use impactful quantum algorithms. The current harmless public key approaches, such RSA and Elliptic Curve Cryptosystems, have completely collapsed as a consequence of this technical breakthrough. To counter this threat, quantum-proof encryption methods like quantum vital have recently emerged.

REFERENCES

[1] M. Dusek, N. L ˇ utkenhaus, and M. Hendrych, "Quantum cryptography," ¨ Progress in Optics, vol. 49, pp. 381 –454, 2006.

[2] C. Paar and J. Pelzl, "Introduction to Public-Key Cryptography," in Understanding Cryptography. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 149–171.

[3] Z. Kirsch, "Quantum Computing: The Risk to Existing Encryption Methods," Ph.D. dissertation, Tufts University, Massachusetts, 2015, http://www.cs.tufts.edu/comp/116/archive/fall2015/zkirsch.pdf.

[4] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information: 10th Anniversary Edition, 10th ed. New York, NY, USA: Cambridge University Press, 2011.

[5] R. Jozsa, "Entanglement and Quantum Computation," in Geometric Issues in the Foundations of Science, S. Huggett, L. Mason, K. Tod, S. Tsou, and N. Woodhouse, Eds. Oxford University Press, July 1997.

[6] W. Tichy, "Is quantum computing for real?: An interview with catherine mcgeoch of d-wave systems," Ubiquity, vol. 2017, no. July, pp. 2:1–2:20, Jul. 2017. [Online]. Available: http: //doi.acm.org/10.1145/3084688

[7] M. Soeken, T. Haner, and M. Roetteler, "Programming quantum com- ¨ puters using design automation," arXiv preprint arXiv:1803.01022, 2018.

[8] S. Bone and M. Castro, "A Brief History of Quantum Computing," Surveys and Presentations in Information Systems Engineering (SURPRISE), vol. 4, no. 3, pp. 20–45, 1997, http://www.doc.ic.ac.uk/□nd/ surprise 97/journal/vol4/spb3/.

[9] J. Muhonen and T. Dehollain, "Storing Quantum Information For 30 Seconds In a Nanoelectronic Device," Nature Nanotechnology, vol. 9, pp. 986–991, 2014. [10] D-Wave, "Quantum Computing: How D-Wave Systems Work," http: //www.dwavesys.com/our-company/meet-d-wave.

[10] J. Buchmann, E. Dahmen, and A. Hulsing, "XMSS-a Practical Forward ¨ Secure Signature Scheme Based on Minimal Security Assumptions," Post-Quantum Cryptography, pp. 117–129, 2011.

[11] R. Overbeck and N. Sendrier, "Code-based Cryptography," in PostQuantum Cryptography. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 95–145.