©IDOSR PUBLICATIONS ISSN: 2579-0803

©IDOSR PUBLICATIONS
International Digital Organization for Scientific Research IDOSRJCAS10200
IDOSR JOURNAL OF COMPUTER AND APPLIED SCIENCES 10(2):22-29, 2025.
https://doi.org/10.59298/JCAS/2025/1022229

Quantum Computing: Implications for Data Security

Kabiga Chelule Kwemoi

Faculty of Engineering Kampala International University Uganda

ABSTRACT

Quantum computing is rapidly evolving from theoretical exploration to practical implementation, raising both immense opportunities and critical concerns, particularly in the realm of data security. While traditional cryptographic techniques like RSA and ECC have long protected sensitive digital communications, the computational prowess of quantum machines poses a severe threat to their reliability. Leveraging principles such as superposition and entanglement, quantum algorithms like Shor's and Grover's can break classical encryption in polynomial time, potentially rendering existing cybersecurity infrastructures obsolete. This paper examines the fundamentals of quantum computing and its divergence from classical systems, details the workings of quantum algorithms, evaluates the current state of quantum hardware, and examines the threat to encryption systems. Furthermore, it investigates post-quantum cryptographic strategies and the emerging field of Quantum Key Distribution (QKD), highlighting both their potential and implementation challenges. In light of these transformative developments, the paper argues for urgent global efforts toward adopting quantum-resistant cryptographic standards to protect future digital systems.

Keywords: Quantum Computing, Data Security, Public Key Cryptography, Quantum Algorithms, RSA, ECC, Post-Quantum Cryptography.

INTRODUCTION

As technology advances, both opportunities and threats to data security grow. Strong encryption has traditionally ensured private online transmission, integral for e-commerce, financial transactions, secure authentication, identity verification, and cloud storage. Current standards for protecting sensitive data include RSA-2048 and ECC schemes, which are based on long-validated mathematical assumptions. Universal schemes have emerged for nondestructive encryption of classical and quantum data. RSA and ECC protect the online activities of computer users, but recent quantum technology advances pose risks to public key cryptography. Quantum computers can factor large integers and calculate discrete logarithms faster than classical algorithms, making RSA and ECC vulnerable to these new adversaries. This vulnerability has fueled concern that quantum computers could undermine current digital security. With quantum hardware manufacturing on the rise, the capabilities of these computers are becoming a reality. Pilot quantum computers are now executing calculations that surpass classical machines, heralding the quantum era. Consequently, there is a shift in perception and a surge of studies predicting a quantum "apocalypse," leading to potential attacks on data security infrastructure with significant implications for individuals, organizations, and nations [1, 2].

Fundamentals of Quantum Mechanics

Interference and superposition are examined in the first wave-particle duality test. A beam of pulse-train light is dissected by a rotating disk. The light alternately reflects off and transmits through a perpendicular beam splitter. In the light-transmitted regions, a lens focuses the light onto a monochrome video camera. At the same time, a halo generates plume-shift shadows on a monochrome video camera. The image sequence of the beam-arrival and beam-departure televisions automatically dissects the beams and non-destructively windows a certain number of circuits. In a deeper test of the wave-particle duality of interference in time and energy, a random sequence of single photon pulses is generated independently. The use of a time-stretched pulse of light prevents energy discrimination. The pulses arrive at a

beamsplitter with delay, causing a time and space division. Interference is observed as the spectra of the intensity array across the television cameras are combined. Global interference nevertheless disappears when they are observed individually, demonstrating that the result observed depends on the process of measurement. The timeliness of conservation laws is probed in terms of digital quantum detour games. The effect of both classical measurement and quantum mechanical measurement is examined. The non-locality of quantum mechanics as a theory of wave-particle duality is considered, and its implication for the causality of the Universe is examined. The duality principle in the reciprocal realm of real and unreal numbers is examined. A comparison gives rise to a unique number that governs the structure of everything in the two realms. The direction of the expansion of real numbers in the first order determines the cosmic arrow of time as well as the hot arrow of time. The divergences of unreal numbers under the rules of relativity are considered. The impossibility of realizing the Mach Principle in quantum mechanics is discussed. The strong version of the Mach Principle and its implications on Cosmology are reviewed [3, 4].

Classical Vs Quantum Computing

Digital computing, an incredibly advanced system that involved turning power on and off at an incredible pace, slowly but surely took hold of the world's imagination. Then, it was only a question of time before enormous mainframe machines were developed, able to perform hundreds of millions of operations each second. With advances in microelectronics, these machines became considerably smaller and less expensive, giving birth to "personal" computers. Conventional computers process information redundantly, with billions or trillions of bits, each one separate, on and off. The power of classical computers depends on how many bits are used. Quantum computers, however, process information using qubits, the unit of quantum information. A qubit can be simultaneously 0 and 1, corresponding to both states at once. A quantum register is built up by multiple qubits. Quantum algorithms can manipulate each qubit simultaneously, thereby "executing" all of the classical computations concurrently. The power of quantum (or, equivalently, binary) computers depends on how many qubits are used. Classical computing power increases exponentially with additional bits, while quantum computers become vastly more powerful with additional qubits, potentially opening up new avenues to solving problems intractable for conventional computers. Users of encryption methods want to keep their messages secret. They use compression pens to code their messages, knowing that only the negotiator has access to the pens. Similarly, the bank holds the secret key to code and decode its ATM signals. The secret is in a mathematical problem; it is known to ten agents and not to anyone else. Number theory is used; the secret is a very large product of two prime numbers. 10-, 170-, and 1024-digit numbers are used. Finally, the quasi-inverse problem becomes hard to solve for dense numbers, but due to quantum computing, it becomes solvable; observers can figure out messages using Grover [5, 6].

Quantum Algorithms

In July 2021, NASA's D-Wave Systems announced its Isothermal 500-quad Oak Ridge Quantum Computing System, capable of performing computations faster than classical computers. Testing showed a significant time-to-solution quantum advantage over state-of-the-art classical supercomputers. Researchers examined its ability to solve 56-variable Diabolical Point Ising spin-3 models, achieving 1.067 million samples in just 3.4 minutes. Quantum computing represents a new information processing paradigm based on quantum mechanics. It operates with input and output in quantum formats, utilizing a hybrid model of quantum CPUs (QPU) and classical systems for control. Problems are expressed through quantum processors and manipulated with quantum gates. Qubits are foundational components of quantum circuits, where unitary operations on qubits yield output states. The emergence of quantum computers promises to transform computing capabilities, enabling computations currently impossible for high-performance multicore systems. They will exploit quantum mechanics to address problems lacking classical solutions and tackle challenges beyond the reach of present-day supercomputers, even those with massive core counts. While the potential applications are vast, quantum computers could also pose threats, notably in cryptanalysis, which examines encrypted data interpretation techniques. Many mathematical challenges supporting current cryptographic algorithms will become solvable with quantum computing, potentially exposing secured data and endangering secure communication systems [7, 8].

Current State of Quantum Technology

Once considered a far-off dream of science fiction, quantum computing has rapidly transformed into a credible reality. In the early 1980s, physicist Richard Feynman proposed the eventual creation of "quantum computers," machines that could solve complex and computationally vexing problems in quantum physics. The term "quantum computing" and the first quantum algorithms were created in the 1990s by Lov Grover and Peter Shor. Grover's algorithm will allow the analysis of any unordered data

set in $O(N^{1/2})$ time, while Shor's algorithm will allow the factoring of large numbers in $O(N^3)$ time. This was groundbreaking news for those who cherished the security of conventional public key encryption, based on the difficulty of factoring operations. With the advent of such powerful machines, classical algorithms for cryptography that are currently in use will likely be easily broken. In addition, the advent of quantum counting will allow for accelerated brute-force attacks on security keys. Post-quantum cryptography efforts are underway, particularly utilizing lattice-based problems that have yet to be solved in polynomial time on quantum machinery. In the late 1980s, early efforts began to explore quantum information and cryptography. The events of 9/11 heightened fears of breaches of privacy on a national level due to the growth of supercomputing and surveillance technologies. The advent of quantum cryptography, in which the laws of quantum mechanics were utilized to more rigorously protect the privacy of information than conventional methods that relied merely on assumptions of intractability of decoding, was ideal. Quantum teleportation would allow the passing of data that had not been extracted in measurement by the sender to the receiver. Quantum information possesses hidden features that are not possessed by classical information. Even if a classical copier makes a perfect recording of a classic information bit, the bit can be destroyed. However, this is not possible with quantum information. Quantum teleportation attempts to transport only entangled qubits to the sender. For the transport process, the sender performs a joint measurement on his/her qubits and transmits two bits of classical information to the receiver. Measurement of the channels using a local measurement operation would collapse the state of either qubit into an eigenstate of the Bell state, preventing any local information about the original qubit from being obtained. Entanglement of the information in quantum cryptography makes it impossible to obtain the data through any local measurement operation [9, 10].

Data Security Basics

Cybersecurity frameworks rely on cryptographic methods to secure data and prevent unauthorized access to sensitive information. Attackers exploit various methods, including social engineering and vulnerability exploitation, to gain access. Traditional encryption scrambles data, rendering it unreadable without a key. Techniques in use include Advanced Encryption Standard (AES), RSA, and elliptic-curve cryptography (ECC). Over the past thirty years, infrastructure has developed heavily around RSA and ECC for authentication and data protection. Security protocols such as Transport Layer Security (TLS) and Secure Sockets Layer (SSL) are widely used to protect data in transit across diverse industries like e-commerce and banking, safeguarding trillions in transactions. Currently, AES-128, AES-256, RSA-3072, and ECC-256 are considered unbreakable within the infrastructure's operational lifetime. However, quantum computing presents a potential threat as it leverages quantum mechanics to create powerful new computer architectures that could undermine these encryption techniques. The security of RSA, Diffie-Hellman, and ECC hinges on number-theoretic problems thought to be impractical for classical algorithms but feasible for quantum computers using algorithms like Vanhood's quantum version of Pollard's rho. If quantum computers reach capabilities of 10,000 qubits and handle 10^19 two-qubit gates per second, they could launch trillion attacks, posing a significant threat to key security. Although these attacks may not affect current cryptography, the concern arises that key exposure could compromise stored data intercepted prior to the advent of quantum computing. To ensure the continuity of secure online commerce and national security, preparations must begin now to transition to quantum-resistant public key infrastructure [11, 12].

Encryption Methods

The currently used data encryption methods stem from classical computing and depend on classical problems that are hard to solve. Their security is based on the assumption that these problems remain difficult to tackle. Notable encryption types include symmetric encryption, such as Data Encryption Standard (DES) and Advanced Encryption Standard (AES), and asymmetric encryption, like RSA, ElGamal, and Elliptic Curve Cryptosystem. These methods assume that classical computers cannot efficiently solve the underlying problems. Symmetric encryption divides plaintext into blocks, which are transformed into ciphertext using an encryption algorithm. Popular block ciphers, including DES and AES, are increasingly vulnerable due to the growth in conventional computer power. Stream ciphers combine plaintext bits with key bits without needing padding. However, ensuring long-term security against quantum computing poses challenges. Asymmetric encryption, developed about 40 years ago, uses separate public and private keys, enabling secure key exchanges and digital signatures. Its security depends on the difficulty of factoring large numbers or computing discrete logarithms. Unfortunately, quantum computers can easily solve these problems, making it crucial to revise current cryptographic schemes, particularly for E-commerce and other sensitive areas [13, 14].

Impact of Quantum Computing on Encryption

Quantum Computers – Potential Threats to Well-Established Encryption Techniques As quantum computers advance, they pose a significant threat to established encryption methods like RSA and ECC. With large-scale, fault-tolerant quantum computers, traditional cryptosystems may be compromised, prompting necessary responses. Quantum algorithms can enhance information processing and potentially break the security of RSA, Diffie-Hellman, DSA, and ECC, leading to increased malicious activities. Attackers could harness quantum computing for large-scale assaults on asymmetric encryption, allowing them to intercept previously encrypted data, which threatens confidentiality. This phenomenon, known as data harvesting, risks revealing sensitive information such as emails and passwords. Additionally, weak symmetric schemes might suffer from key exposure. Quantum systems could also undermine digital signatures within digital certificates, enabling impersonation or man-in-the-middle attacks on private key communications, leading to identity theft. As we anticipate that fault-tolerant quantum computers will be operational in the near future, transitioning to a quantum-safe framework becomes imperative. Exploring new post-quantum cryptographic methods is vital for securing critical infrastructure, including web services, cloud computing, and blockchain applications. However, while customers shift to quantum-safe algorithms, third-party providers might still rely on backup keys from conventional public key systems, risking data confidentiality and exposing financial institutions to significant dangers [15, 16].

Quantum Key Distribution (QKD)

Quantum Key Distribution (QKD) is a groundbreaking approach to safeguarding sensitive data, intertwining information theory and physics, and extending beyond computer science and traditional cryptography. It offers unconditional security for transmitting encrypted messages, allowing parties to detect eavesdropping attempts. This has fostered the emergence of a QKD market focused on high-value data transmissions. Public key cryptography (PKC) protects data from potential attacks but has limitations regarding computation power and algorithm knowledge. As quantum computing advances, concerns arise about the effectiveness of classical cryptography, with estimates suggesting it could become obsolete in five to thirty years. However, the QKD market is still developing and needs significant investments to mature and build trust comparable to PKC. The fundamental concept of QKD involves Alice and Bob sharing a random key through the transmission of Qbits (0s and 1s) with mutual encoding bases. They retain matching bits, which are secure by quantum mechanics principles, while discarding others. BB84 is the most common protocol used. Any compromise of security parameters can lead to private information leakage, affecting the integrity of QKD efforts. Such leaks can occur either intentionally or accidentally, with subtle undetected causes posing a risk to the system. Countermeasures against such leaks may inadvertently introduce new vulnerabilities. Recent findings reveal new loopholes in SIDH and LR protocols concerning their security linked to existing information leaks [17, 18].

Challenges In Implementing QKD

While QKD is very promising for secure communications, several key challenges remain for QKD to be widely used for securing everyday interactions. In this article, some of the important challenges are highlighted, and various approaches that are being taken to tackle them are discussed. Much effort has been directed at increasing the communication rate and range of QKD. On the one hand, researchers continue to propose new techniques, such as quantum repeaters and time-based entanglement swapping, to make QKD practical over longer distances. On the other hand, protocols based on the use of weak coherent pulses have been improved through theories and experiments to achieve higher secret key rates. In addition to increasing the communication rate, making QKD systems low-cost, compact, robust, and ready for better-than-thermo-optical-loss operations is also being pursued. Recent advances in silicon photonics are expected to be key to low-cost and compact QKD systems. Integrating the control electronics into the chips is also believed to yield more robust and reliable QKD systems. The security of practical QKD systems is another very important challenge. Component imperfections in the QKD systems can create vulnerabilities, leading to various attacks, such as side channel attacks and collective attacks. To gain a better understanding of these attacks and develop efficient countermeasures, researchers across different backgrounds, such as quantum communications and quantum optics, have made collaborative efforts. Increasing the QKD rate while maintaining an acceptable overall channel error is paramount for long-distance QKD systems [19, 20].

Regulatory and Ethical Considerations

Emerging from breakthroughs in quantum algorithms, quantum computers are expected to operate on distinct technological principles compared to classical systems. They will use quantum states to represent qubits and perform complex computations with potentially unlimited capabilities, undermining public-key cryptography. This change could jeopardize protocols used for establishing symmetric keys and

signatures, impacting states, companies, and individuals reliant on cryptography for security. The threat posed by quantum algorithms necessitates analyzing their potential impacts on classic cryptographic methods before they materialize. Quantum algorithms have shown speed advantages over classical ones, yet issues persist as more qubits and gates lead to complexity. Problems that challenge classical computers can prove even more difficult for quantum machines, raising concerns about quantum tools revealing secrets in secure protocols based on classical systems. The path toward effective demonstration of quantum resistance will vary, offering different timelines for effects. The crypto community is now actively engaging with this evolving landscape, previously viewed as distant, driven by government and international collaborations. Thorough evaluation of quantum devices and their operational contexts is critical before making decisions on the future of widely deployed classical cryptographic systems [21, 22].

Case Studies

To date, quantum computing has begun to find applications in various industries, alleviating concerns about a potential "quantum winter" due to a shortage of expertise. Quantum communication enhances existing classical protocols like dense coding, leveraging insights from quantum physics in protocol design. Quantum teleportation enables data transfer without prior measurement by the sender. Unlike classical information, which consists of predictable bits, quantum information possesses unique hidden attributes. The concept of entanglement in quantum cryptography significantly enhances security, making it impossible to access data through local measurements. Quantum cryptography is emerging as a secure solution for cyberspace, with a notable feature being its unconditional security. The advancements in quantum computing using superconducting qubits simplify the resolution of complex quantum physics problems, focusing on quantum-safe data transportation. After years of research, quantum computing is now showing promise, with capabilities to potentially break existing encryption methods. Growing fears surrounding quantum computers have prompted increased interest and competition in quantum technology among nations, enterprises, and academic institutions, driven by both military and market incentives. Quantum computers, utilizing smaller hardware than classical counterparts, are anticipated to achieve unprecedented tasks, possibly posing significant risks to cybersecurity [23, 24].

Future of Quantum Computing in Data Security

Considering the rapid advancements in quantum computing and their implications for data security, the future of this technology, its risks, challenges, and opportunities, is increasingly interesting. Quantum computers are anticipated to become commercially available within the next five years and large developers are working on scaling quantum hardware so that it can solve problems impervious to classical computing. Currently, mature quantum computers with about 40 qubits operated in a laboratory setting are available to researchers and the public through the cloud. However, a superposition of quantum parallelism can only be achieved when the number of operational qubits exceeds 1000, which is still a few years away. Once available, the financial landscape will change dramatically, as some of the mathematics used to secure government, business, and personal information will be easy to crack. Quantum computing, when coupled with better command technologies to obtain massive amounts of data, will increase crime, including hacking into social security numbers, health profiles, financial data, banking accounts, and anything about stock market information. It is anticipated that the average hacker will be able to hack into encrypted data in a short period. New security measures and provisioning will be needed and must be in place before quantum computing advances to these capabilities, and financial havoc is created. Data operations/A-to-B information flow will remain the same (i.e., the transmission of bits across the channels of connectivity). The basic mathematics to encode, process, encrypt, and decrypt will remain the same as well. Adversarial entities will continue to search for ways to tap A-to-B information flow equations. Encryption is key to thwarting encryption as well as any computer's attempts to decrypt it through brute force, math-based, and physical attacks. The future of data and its security is assured via data encoding and cryptography. This holds regardless of what computers exist in the future, and even if quantum computers advance to a situation where they outperform all currently available computers [25, 26].

Industry Responses to Quantum Threats

The growth of quantum computing is expected to impact various sectors significantly. Quantum threats can be divided into concrete threats, like vulnerabilities in current cryptography, and abstract threats, including new types of attacks. Although it will take time for quantum computers to mature, their threat is already acknowledged. The Quantum Threat Timeline outlines phases of these threats, containing three before-quantum phases and two after-quantum phases. It emphasizes that threats can arise indefinitely, regardless of the deployment of post-quantum cryptography (PQC). Even with PQC in place, new attacks might emerge that cryptographic primitives cannot address. Quantum computers may serve

as both powerful adversaries and tools for confronting these challenges. Recently, private companies and governments have accelerated their quantum computing efforts, with Google announcing "quantum supremacy" in 2019. This includes measuring the efficiency of post-quantum encryption algorithms and the SHA3 hashing process, where a minimum wait time is required to surpass classical machines. Furthermore, the potential for quantum computers to compromise cryptographic key generation and management raises concerns about the sources of randomness used. It is crucial to evaluate the devices generating hash function outputs and encrypted communications at issuance. This risk extends to quantum key distribution systems, which could be vulnerable to eavesdropping. These factors prompt essential inquiries about the sustainability of cryptography in the face of quantum threats [27, 28].

Research and Development Trends

Cybersecurity faces unprecedented challenges today due to rapid technological advances, evolving threats, and geopolitical tensions. Disruptive technologies like artificial intelligence (AI), machine learning, and quantum computing (QC) offer significant benefits but also pose serious security and privacy risks. Concerns about quantum-induced threats are rising, as the realization of powerful quantum computers capable of solving complex problems may jeopardize various cybersecurity protocols, particularly blockchain technologies. Consequently, a new field known as quantum cybersecurity is emerging to address these quantum-enabled risks and opportunities. Challenges include large preparation errors from noisy intermediate-scale quantum (NISQ) devices and limited access for the general public, causing skepticism surrounding the benefits of quantum technology. Quantum threat assessments can enhance proactive risk management, aiding in the development of quantum-resilient cybersecurity solutions and cryptographic mechanisms across digital assets, cloud infrastructures, and key establishment protocols. Simultaneously, quantum opportunity assessments could help evaluate the security and feasibility of existing systems. This review highlights emerging trends in quantum computing, including technologies, architectures, implementations, and their associated advantages and limitations. It discusses research from both academia and industry, the potential transition to more profitable incentive models for quantum technologies, and strategies for mainstream adoption. Recent initiatives and funding to promote technology and workforce development are also examined, alongside the exchange of innovations between academia and industry. Lessons from the early development of qubit computers emphasize the need for open-access resources and knowledge sharing to foster a human-centric quantum ecosystem. The discussion includes challenges related to global quantum relations, investment divergence, collaboration in research, and pathways for sustainable, mutually beneficial relationships moving forward [29, 30].

CONCLUSION

The advent of quantum computing represents a paradigm shift in computational science with profound implications for data security. As quantum machines evolve, the foundational assumptions underlying modern cryptographic systems are being challenged. Algorithms once deemed secure are now vulnerable to quantum attacks, necessitating a swift transition toward quantum-resistant frameworks. While Quantum Key Distribution offers a theoretically secure alternative, practical limitations and scalability challenges must be addressed before widespread adoption. Collaborative international efforts between academia, industry, and government agencies are essential to standardize and implement robust post-quantum encryption methods. Ensuring a secure digital future demands proactive planning, investment, and innovation to stay ahead of the impending quantum revolution.

REFERENCES

1. Ekerå M. Quantum algorithms for computing general discrete logarithms and orders with tradeoffs. Journal of Mathematical Cryptology. 2021 Jan 1;15(1):359-407.
2. Tom JJ, Anebo NP, Onyekwelu BA, Wilfred A, Eyo RE. Quantum computers and algorithms: a threat to classical cryptographic systems. Int. J. Eng. Adv. Technol. 2023 Jun;12(5):25-38. researchgate.net
3. HAO L. Philosophy and physics meet in quantum world. Bulletin of Chinese Academy of Sciences (Chinese Version). 2021;36(1):28-36.
4. Mavroeidis V, Vishi K, Zych MD, Jøsang A. The impact of quantum computing on present cryptography. arXiv preprint arXiv:1804.00200. 2018 Mar 31.
5. Rietsche R, Dremel C, Bosch S, Steinacker L, Meckel M, Leimeister JM. Quantum computing. Electronic Markets. 2022 Dec;32(4):2525-36. springer.com
6. Carrera Vazquez A, Tornow C, Riste D, Woerner S, Takita M, Egger DJ. Scaling quantum computing with dynamic circuits. arXiv e-prints. 2024 Feb:arXiv-2402.

7. Bavdekar R, Chopde EJ, Bhatia A, Tiwari K, Daniel SJ. Post quantum cryptography: Techniques, challenges, standardization, and directions for future research. arXiv preprint arXiv:2202.02826. 2022 Feb 6.
8. Mavroeidis V, Vishi K, Zych MD, Jøsang A. The impact of quantum computing on present cryptography. arXiv preprint arXiv:1804.00200. 2018 Mar 31.
9. Niraula T, Pokharel A, Phuyal A, Palikhel P, Pokharel M. Quantum computers' threat on current cryptographic measures and possible solutions. Int. J. Wirel. Microw. Technol. 2022 Oct;12(5):10-20. researchgate.net
10. Cheng JK, Lim EM, Krikorian YY, Sklar DJ, Kong VJ. A survey of encryption standard and potential impact due to quantum computing. In2021 IEEE Aerospace Conference (50100) 2021 Mar 6 (pp. 1-10). IEEE. researchgate.net
11. Ajala OA, Arinze CA, Ofodile OC, Okoye CC, Daraojimba AI. Exploring and reviewing the potential of quantum computing in enhancing cybersecurity encryption methods. Magna Sci. Adv. Res. Rev. 2024 Feb;10(1):321-9. researchgate.net
12. Jowarder RA, Jahan S. Quantum computing in cyber security: Emerging threats, mitigation strategies, and future implications for data protection. World Journal of Advanced Engineering Technology and Sciences. 2024 Sep;13(1):330-9. cryptodeeptech.ru
13. Yang Z, Zolanvari M, Jain R. A survey of important issues in quantum computing and communications. IEEE Communications Surveys & Tutorials. 2023 Mar 8;25(2):1059-94. ieee.org
14. Abdulwahab HM, Alabdeli H, Singh S, Pareek S, Kaur A, Dasi S. Advances in Quantum Computing for Enhancing Network Security and Encryption Techniques. In2024 International Conference on Information Science and Communications Technologies (ICISCT) 2024 Nov 7 (pp. 56-61). IEEE. [HTML]
15. Szikora P, Lazányi K. The end of encryption?–The era of quantum computers. InSecurity-Related Advanced Technologies in Critical Infrastructure Protection: Theoretical and Practical Approach 2022 Sep 6 (pp. 61-72). Dordrecht: Springer Netherlands. researchgate.net
16. Sood N. Cryptography in post Quantum computing era. Available at SSRN 4705470. 2024. ssrn.com
17. Jain N, Stiller B, Khan I, Elser D, Marquardt C, Leuchs G. Attacks on practical quantum key distribution systems (and how to prevent them). Contemporary Physics. 2016 Jul 2;57(3):366-87.
18. Diamanti E, Lo HK, Qi B, Yuan Z. Practical challenges in quantum key distribution. npj Quantum Information. 2016 Nov 8;2(1):1-2.
19. Sood N. Cryptography in post Quantum computing era. Available at SSRN 4705470. 2024.
20. Bova F, Goldfarb A, Melko RG. Commercial applications of quantum computing. EPJ quantum technology. 2021 Dec 1;8(1):2.
21. Gupta B, Agrawal DP, Yamaguchi S, editors. Handbook of research on modern cryptographic solutions for computer and cyber security. IGI global; 2016 May 16.
22. Nagori V, Varadarajan V. Quantum computing posing a challenge to the businesses. Int. J. Res. Eng. Sci. Manag. 2023;6(1):52-5.
23. Vaishnavi A, Pillai S. Cybersecurity in the quantum era-a study of perceived risks in conventional cryptography and discussion on post quantum methods. InJournal of Physics: Conference Series 2021 Jul 1 (Vol. 1964, No. 4, p. 042002). IOP Publishing.
24. Singh S, Kumar D. Enhancing cyber security using quantum computing and artificial intelligence: A review. algorithms. 2024 Jun;4(3).
25. Bayerstadler A, Becquin G, Binder J, Botter T, Ehm H, Ehmer T, Erdmann M, Gaus N, Harbach P, Hess M, Klepsch J. Industry quantum computing applications. EPJ Quantum Technology. 2021 Dec 1;8(1):25. springer.com
26. Scholten TL, Williams CJ, Moody D, Mosca M, Hurley W, Zeng WJ, Troyer M, Gambetta JM. Assessing the benefits and risks of quantum computers. arXiv preprint arXiv:2401.16317. 2024 Jan 29. [PDF]
27. Agrawal S. Harnessing Quantum Cryptography and Artificial intelligence for next-gen payment Security: A Comprehensive analysis of threats and countermeasures in distributed ledger environments. International Journal of Science and Research. 2024;13(3):682-7.
28. Sodiya EO, Umoga UJ, Amoo OO, Atadoga A. Quantum computing and its potential impact on US cybersecurity: A review: Scrutinizing the challenges and opportunities presented by quantum technologies in safeguarding digital assets. Global Journal of Engineering and Technology Advances. 2024 Feb;18(02):049-64. researchgate.net

29. Baseri Y, Chouhan V, Ghorbani A. Cybersecurity in the quantum era: Assessing the impact of quantum computing on infrastructure. arXiv preprint arXiv:2404.10659. 2024 Apr 16.
30. Faruk MJ, Tahora S, Tasnim M, Shahriar H, Sakib N. A review of quantum cybersecurity: threats, risks and opportunities. In2022 1st International Conference on AI in Cybersecurity (ICAIC) 2022 May 24 (pp. 1-8). IEEE.

CITE AS: Kabiga Chelule Kwemoi (2025). Quantum Computing: Implications for Data Security. IDOSR JOURNAL OF COMPUTER AND APPLIED SCIENCES 10(2):22-29. https://doi.org/10.59298/JCAS/2025/10212229