Transactions on Engineering and Computing Sciences - Vol. 13, No. 03
Publication Date: May 25, 2025
DOI:10.14738/tmlai.1303.18824.
Quddus, S., Siddique, S. A., & Ramadan, R. A. (2025). Quantum Computing and Applications: Its Effects on Cybersecurity. *Transactions on Engineering and Computing Sciences*, 13(03). 28-32.

Quantum Computing and Applications: Its Effects on Cybersecurity

Syed Quddus
Department of Computer Science,
DHA-Suffa University, DCK

Saad Ali Siddique
Department of Computer Science,
DHA-Suffa University, DCK

Rabie A. Ramadan
Department of Information Systems,
University of Nizwa, Sultanate of Oman

ABSTRACT

Quantum computing is a developing field with the prospective to revolutionize the current advanced computing, it represents a fundamental shift from classical computing principles towards superposition, entanglement, and quantum interference, which are quantum mechanical principles. By using these distinctive principals and properties of quantum mechanics, 'Quantum Computing' processes information in the ways that are principally different from classical computers. This paper examines the fundamental concepts of quantum computing, its current and potential diverse applications, and the effects it has on cybersecurity. As quantum computing continues to advance, it proposes both forecasts and challenges, especially in cryptography, data protection, and security systems. This review paper focusses to discuss a comprehensive understanding of the junction between quantum computing and cybersecurity. It also point-outs the risks to current encryption theory and the new quantum-safe cryptography practices.

Keywords: Superposition, entanglement, and quantum interference, quantum mechanical, cybersecurity.

INTRODUCTION

During the last decade, the field of quantum computing has been emerging as one of the distracting and promising fields in this age of science and technology. The basic component of information in classical computing is a bit and in quantum computing, the purpose is served by the qubit (or "quantum bit"). In contrast to classical computing where a bit can exist in a single state (0 or 1) at a time, a qubit can exist in a superposition of its two "basis" states, a state that is in an abstract sense "between" the two basis states. When evaluating a qubit, the result is a stochastic output of a classical bit. The quantum computing, performs calculations in a fundamentally different ways by using the principles of quantum mechanics like, superposition, entanglement, and quantum interference. This hypothesis enables quantum computers to solve complex problems considerably faster than their classical computing, suggesting vast improvements in fields ranging from optimization and artificial intelligence to molecular

modeling and big data analysis. One of the most critical fields affected by the rise of quantum computing is cybersecurity. As information systems become more advanced and the volume of sensitive data increases, ensuring secure data transmission and storage has become paramount.

However, the same quantum properties that facilitate unique computational power also present a risk to current cryptographic systems. Algorithms such as RSA and ECC, which emphasize current encryption standards, are exposed to quantum attacks—particularly through Shor's algorithm, which can factor large prime numbers exponentially faster than classical approaches.

This review paper aims to lookout the transformative effect of quantum computing on cybersecurity. It presents an overview of quantum computing principles, its current applications, and a detailed analysis of its consequences for recent cryptographic protocols. Furthermore, the paper elucidates evolving quantum-resistant cryptographic approaches that help to defend digital infrastructure in the quantum age.

LITERATURE REVIEW

Quantum computing has emerged from theoretical models to a substantial technological advancement, significantly redesigning our perception of computational boundaries. The foundational work of Shor (1997) introduced quantum principles-based polynomial-time algorithms for prime factorization and discrete logarithms. This raised a challenge to the classical public-key cryptography, emphasizing the need for quantum-resistant based alternatives. Similarly, Bennett and Brassard (1984) initiated a new era in secure communication by the introduction of quantum key distribution (QKD) and by exploiting quantum mechanics for theoretically unbreakable encryption.

current research has further explored the quantum computing's applications in the cybersecurity. (NIST, 2022), the frontline national institute of standards and technology in assessing postquantum cryptographic (PQC) algorithms, highlighting a pre-emptive response to expanding quantum threats. Developing this narrative, Chen et al. (2016) given a detailed evaluation of post-quantum cryptography, underlining lattice-based and code-based schemes as encouraging solutions.

The intersection between quantum computing and security in connected environments has gained prominence. For example, Chawla and Mehra (2023) reviewed the role of quantum computing in securing the Internet of Things (IoT), emphasizing the integration of QKD and post-quantum cryptography to mitigate vulnerabilities in IoT networks. Similarly, Abd El-Aziz et al. (2022) explored optimization techniques for IoT platforms using modified quantum computing models, indicating the growing reliance on quantum-enhanced frameworks for secure and efficient computation.

The application of quantum principles in software and hardware systems also shows significant progress. Ali, Yue, and Abreu (2022) and De Stefano et al. (2022) examined the intersection of software engineering with quantum technologies, addressing the challenges in programming

and modeling quantum systems for cybersecurity applications. These insights are crucial for developing quantum-aware software architecture, as also explored by Khan et al. (2023) in their systematic review on quantum software architecture.

Component-level novelties are also progressing. Research by Al-Khafaji et al. (2023) focused on optimizing nanoscale carry-skip adders based on quantum dots, offering potential improvements in energy-efficient and secure hardware for future quantum-IoT systems. Similarly, Faghih et al. (2023) proposed quantum-balanced ternary reversible multipliers to facilitate sustainable and secure computing infrastructure.

Quantum computing's general incorporation is studied in broader contexts. Bashirpour Bonab et al. (2023a, 2023b) depicted the ample-reviews on quantum skills in urban substructure and smart cities, strengthening the importance of quantum security protocols in real-world systems. Their findings support the necessity of integrating quantum technologies into smart governance and digital urban services with robust cybersecurity frameworks.

Security aside, quantum computing also fosters new opportunities in quantum-enhanced algorithms. Arufe et al. (2023) investigated coding schemes for quantum approximate optimization algorithms (QAOA), indicating future pathways for solving complex decisionmaking and cryptographic challenges. Furthermore, studies like Feng and Li (2023) advanced theoretical perspectives by applying abstract and incorrectness logic to quantum programs, laying a foundation for secure quantum programming.

Emerging technology such as PyQBench (Jałowiecki et al., 2023) points out endeavors to benchmark and assess the performance of quantum devices, certifying that security-related declarations can be attested experimentally. This is particularly, significant in establishing trust in quantum-enhanced secure systems.

The focus of the literature is to highlight the crucial role of quantum computing in cybersecurity. From overcoming the cryptographic challenges to designing architectural innovations, scientists, engineers, and researchers are practically making for the future where quantum tools redesign the way information is protected, transmitted, and managed.

DISCUSSION

The evolution of quantum computing presents an uncertainty for cybersecurity due to its dual nature: threat and an opportunity. The quantum computers have the potential to settle with existing cryptographic setup. Algorithms like RSA, which depend on the computational difficulty of factoring large numbers, are particularly defenseless. By implementing Shor's algorithm on adequately powerful quantum machines, encrypted data could be uncovered. This depicts substantial concerns for governments, financial institutions, healthcare providers, and other bodies that depend strongly on data confidentiality. Instead, quantum mechanics also proposes the tools to revise digital security.

Quantum Key Distribution (QKD) denotes an essential change toward theoretically robust encryption. By exercising entangled particles to transmit encryption keys, any endeavor to

distract or measure the particles introduces detectable changes, alerting users to potential security breaches. Though QKD is currently limited by infrastructure requirements and transmission distances, ongoing research promises to overcome these challenges.

As quantum computing technology is continuously becoming mature, so there is need to upgrade classical systems with quantum-safe cryptography and invest in native quantum security solutions. The cybersecurity community must also highlight education, research, and policymaking to mitigate quantum danger and threats for achieving its potential benefits Practical struggles today will evaluate the strength of tomorrow's digital world.

References

Shor, P. W. (1997). "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer." SIAM Journal on Computing, 26(5), 1484-1509.

Bennett, C. H., & Brassard, G. (1984). "Quantum cryptography: Public-key distribution and coin tossing." Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing. National Institute of Standards and Technology (NIST). (2022). Post-Quantum Cryptography. Retrieved from https://www.nist.gov/news-events .

Chen, L. K., et al. (2016). "Post-Quantum Cryptography: State of the Art and Research Directions." Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security.

Abd El-Aziz, R.M., Taloba, A.I. and Alghamdi, F.A. (2022). "Quantum Computing Optimization Technique for IoT Platform using Modified Deep Residual Approach". Alexandria Engineering0020Journal, Vol 61(12), pp 12497–12509. https://doi.org/10.1016/j.aej.2022.06.029

Ali, S., Yue, T. and Abreu, R. (2022). "When software engineering meets quantum computing". Communications of the ACM, Vol 65(4), pp 84–88. https://doi.org/10.1145/3512340

Al-Khafaji, H.M.R. et al. (2023). "Performance optimization of the nano-scale carry-skip adder based on quantum dots and its application in the upcoming Internet of Things". Optik, Vol 287, pp 170976. https://doi.org/10.1016/j.ijleo.2023.170976

Alonso, D., Sánchez, P. and Sánchez-Rubio, F. (2022). "Engineering the development of quantum programs: Application to the Boolean satisfiability problem". Advances in Engineering Software, Vol 173, pp 103216. https://doi.org/10.1016/j.advengsoft.2022.103216

Arufe, L. et al. (2023). "New coding scheme to compile circuits for Quantum Approximate Optimization Algorithm by genetic evolution". Applied Soft Computing, Vol 144, pp 110456. https://doi.org/10.1016/j.asoc.2023.110456

Bashirpour Bonab, A. et al. (2023a). "In complexity we trust: A systematic literature review of urban quantum technologies". Technological Forecasting and Social Change, Vol 194, pp 122642. https://doi.org/10.1016/j.techfore.2023.122642

Bashirpour Bonab, A. et al. (2023b). "Urban quantum leap: A comprehensive review and analysis of quantum technologies for smart cities". Cities, Vol 140, pp 104459–104459. https://doi.org/10.1016/j.cities.2023.104459

Chawla, D. and Mehra, P.S. (2023). "A Survey on Quantum Computing for Internet of Things Security". Procedia Computer Science, Vol 218, pp 2191–2200. https://doi.org/10.1016/j.procs.2023.01.195

Levac, D., Colquhoun, H. and O'Brien, K.K. (2010). "Scoping studies: Advancing the Methodology". Implementation Science, Vol 5(1), pp.1–9. https://doi.org/10.1186/1748-5908-569

De Stefano, M. et al. (2022). "Software engineering for quantum programming: How far are we?" Journal of Systems and Software, Vol 190, pp 111326. https://doi.org/10.1016/j.jss.2022.111326

Faghih, E. et al (2023). "Efficient realization of quantum balanced ternary reversible multiplier building blocks: A great step towards sustainable computing". Sustainable Computing: Informatics and Systems, Vol 40, pp 100908. https://doi.org/10.1016/j.suscom.2023.100908

Feng, Y. and Li, S. (2023). "Abstract interpretation, Hoare logic, and incorrectness logic for quantum programs". Information and Computation, Vol 294, pp 105077. https://doi.org/10.1016/j.ic.2023.105077

Arksey, H. and O'Malley, L. (2005). "Scoping studies: Towards a Methodological Framework". International Journal of Social Research Methodology, Vol 8(1), pp.19–32. https://doi.org/10.1080/1364557032000119616

Harikrishnakumar, R. and Nannapaneni, S. (2023). "Forecasting Bike Sharing Demand Using Quantum Bayesian Network". Expert Systems with Applications, Vol 221, pp 119749. https://doi.org/10.1016/j.eswa.2023.119749

Hildebrand, B. et al. (2023). "A comprehensive review on blockchains for Internet of Vehicles: Challenges and directions". Computer Science Review, Vol 48, pp 100547. https://doi.org/10.1016/j.cosrev.2023.100547

Jałowiecki, K., Lewandowska, P. and Pawela, Ł. (2023). "PyQBench: A Python library for benchmarking gate-based quantum computers". SoftwareX, Vol 24, pp 101558. https://doi.org/10.1016/j.softx.2023.101558

Khan, A.A. et al. (2023). "Software architecture for quantum computing systems - a systematic review". Journal of Systems and Software, Vol 201, pp 111682. https://doi.org/10.1016/j.jss.2023.111682

Li, K. et al. (2022). "A novel privacy-preserving multi-level aggregate signcryption and query scheme for Smart Grid via mobile fog computing". Journal of Information Security and Applications, Vol 67, pp 103214. https://doi.org/10.1016/j.jisa.2022.103214

Li, N. et al. (2023). "Quantum image scaling with applications to image steganography and fusion". Signal Processing: Image Communication, Vol 117, pp 117015. https://doi.org/10.1016/j.image.2023.117015