Journal of
Engineering Education
and Practice

Https://journaleep.com
Editor@journaleep.com
ISSN (Print) : 3080-6747
ISSN (Online) : 3080-6755

QUANTUM COMPUTING FOR CRYPTOGRAPHY: EXPLORING THE FUTURE OF SECURE COMMUNICATIONS WITH QUANTUM ALGORITHMS

Article History

Received:
July 01, 2023

Revised:
September 11, 2023

Accepted:
October 20, 2023

Available Online:
December 31, 2023

Arslan Nadeem [1*], Aiman Shabbir[2]

[1]Department of Computer & Electrical Engineering, University of Lahore, Pakistan

[2]Department of Computer Science, Muhammad Nawaz Shareef University of Agriculture, Multan, Punjab, Pakistan

*Corresponding Author E-mail: arslan.nadeem@uol.edu.pk

Abstract

Quantum computing holds an enormous power to transform cryptography because it protects secured communication. RSA together with elliptic curve cryptography functions based on mathematical challenges like integer factorization and discrete logarithms until quantum computers present security risks to these traditional systems. Such problems become solvable with efficiency through Shor's algorithm running on quantum computers which threatens the security of multiple widely used cryptographic protocols. The document examines quantum computing effects on cryptography to explain why quantum algorithms break classic cryptographic system security. Post-quantum cryptography (PQC) acts as a protective solution against quantum-based attacks through its mission to create cryptographic techniques which demonstrate quantum attack resilience. This paper examines quantum-age security design protocols for cryptographic keys using both quantum key distribution and lattice-based cryptography and hash-based cryptography and multivariate polynomial cryptography. The research analyzes the effectiveness and protective capability of new PQC solutions by connecting theoretical concepts with practical applications. The study points out advancements in quantum cryptography as well as the quantum hardware obstacles and the global initiative to establish post-quantum algorithms standards. The authors stress the urgent need for up-to-date quantum-resistant measures because of swift quantum technology progress. The protection of sensitive materials and communications networks from destructive quantum computing threats requires immediate focus because this need drives the necessity of properly preparing for post-quantum cryptography.

Keywords: Quantum Computing, Cryptography, Post-Quantum Cryptography, Quantum Key Distribution

1. INTRODUCTION

The dawn of quantum computing establishes a new era for computation while producing crucial effects that deeply affect the field of cryptography. Quantum bits form the basis of quantum computing systems since they differ from classical computer data representation relying on 0s and 1s binary logic.

Quantum bits act as multiple parties because of quantum superposition along with the concept of entanglement. Quantum computers process large information quantities concurrently through qubits which allows them to solve particular computation problems faster than classical computers. Quantum computing obtains dramatic speedups in large integer factorization and discrete logarithm solution processes creating enormous research interest especially in cryptographic domains (Shor, 1994).

RSAs along with ECC represent the principal encryption methods used throughout contemporary times since their widespread adoption. Their dominance as an encryption system stems from the assumption that certain mathematical problems challenge solutions to the extent that determines their applicable security boundaries. The encryption keys for RSA exist because applying current computer technology to factor large composite integers would require immense processing time (Koblitz, 1987). Similarly ECC depends on the intractable discrete logarithm problem on elliptic curves. According to present knowledge both problems require more time than available human lifespan for classic computers to solve them thus ensuring the security of underlying systems' techniques.

Quantum computation research faces a harsh reality from specific algorithms which can solve RSA and ECC in polynomial time according to research by Shor (1994). Computing systems must be redesigned to survive the operational capabilities of quantum computers.

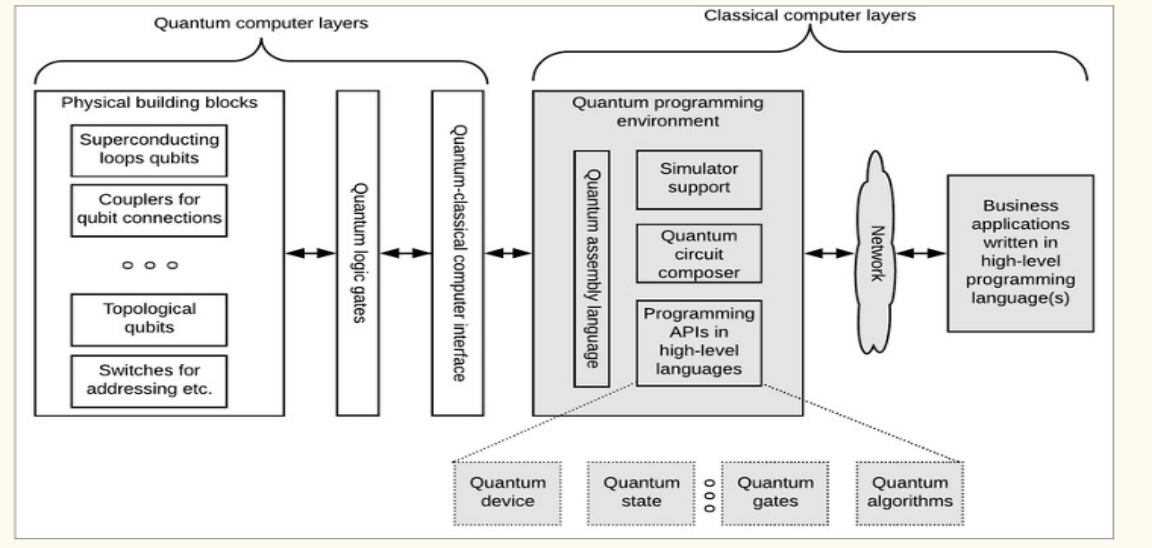


Figure 1. Architecture of Quantum Computing

Quantum computing will present a major security threat to protected communications, protected financial operations and sensitive data protection within the following years. The potential advancement of quantum computers in the future will lead to decryption methods for supposedly secure classical systems which contains serious threats for data safety (Bernstein et al., 2009).

Increased research in post-quantum cryptography (PQC) emerged due to this challenge as researchers tried to create encryption methods that stand against quantum computer computational power (Laarhoven et al., 2015). The same circumstances drive PQC development since quantum computers will shatter most current digital security methods when their power reaches critical mass.

Data and communication security for the quantum era depends on mathematical problems which pose intense computational challenges to quantum computers according to the PQC framework. The leading PQC solutions are currently considered to be Lattice-based cryptography and Hash-based cryptography and Code-based cryptography and Multivariate polynomial cryptography. Modern researchers investigate these methods to establish solid post-quantum security (Chen et al., 2016). The difficulty of Shortest Vector Problem along with Learning With Errors is what makes lattice-based cryptography powerful enough to serve as a quantum-resistant encryption method (Peikert, 2016). The field of code-based cryptography received attention for over three decades as it provides necessary security to defend against quantum attacks (McEliece, 1978).

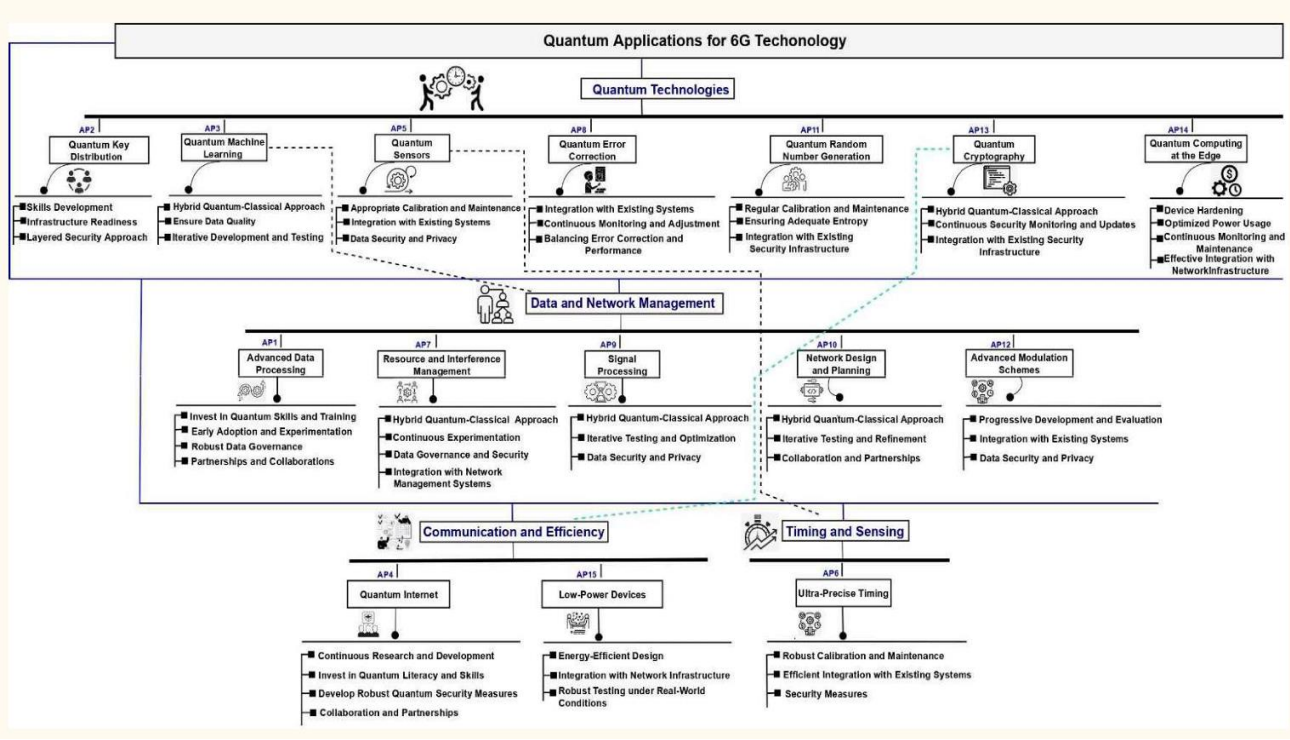


Figure 2. Taxonomy of key applications and their related best practices.

Quantum international communication represents a new technology which creates promising security benefits for communications during the quantum technology era. Quantum key distribution generates

secure data transmission keys that quantum mechanics protects from breaches but at the same time maintains security against quantum adversaries (Bennett & Wiesner, 1992). The combination of PQC and quantum technology enables proficient development of secure quantum communication networks.

The moral aim of this document examines how quantum computing affects traditional cryptographic systems along with investigating modern quantum-proof cryptographic approaches. Analysis of post-quantum cryptographic algorithm standardization initiatives alongside their widespread implementation will receive attention in this paper together with QKD research.

Figure 3. Quantum Computing Threats

LITERATURE REVIEW:

The impact of quantum computing extends deep into cryptography domain. These cryptographic systems rely on certain mathematical problems which demonstrate intractability for a long time period. RSA depends on the assumption that classical computers must face significant difficulty solving problems related to long number factoring according to Rivest et al. (1978). Similarly, elliptic curve cryptography (ECC) leverages the hardness properties of the discrete logarithm problem in elliptic curves (Koblitz, 1987). Secure digital communication has functioned through these algorithms during several decades because they protect both banking transactions online as well as classified government communications. Quantum computers present themselves to find efficient solutions to problems on which traditional cryptographic systems depend (Shor, 1994).

Quantum mechanics enables Shor's algorithm to find polynomial-time solutions for integer factorization and discrete logarithm problems leading to existing encryption vulnerabilities (Shor, 1994). The Shor algorithm breaks ECC and RSA

thus driving the increasing overall interest in quantum safe encryption standards. The development process of encryption algorithms has created a driving force responsible for shaping the entire field known as post-quantum cryptography (PQC) (Bernstein et al., 2009). The purpose of PQC is to establish cryptographic systems which maintain their security guarantees even when powerful quantum computers operate.

Lattice-based cryptography functions as one of the prominent choices for building quantum-resistant encryption systems. Seasoned experts believe the Shortest Vector Problem (SVP) along with Learning With Errors (LWE) are computationally difficult problems for traditional and quantum computers (Peikert, 2016). The difficulty of these problems differs from others and thus presents itself as a compelling choice to develop encryption systems that protect against quantum computing threats. The secure algorithms NTRU and CRYSTALS-Dilithium serve as RSA and ECC replacements through their operation based on hard lattice problems (Lauter et al., 2014; Chen et al., 2016).

A parallel code-based cryptography system exists for attaining quantum-resistant encryption. Through error-correcting codes particularly the McEliece cryptosystem we achieve this possibility. Code-based cryptography established its future role in post-quantum systems thanks to the defiance of quantum algorithms demonstrated by its decades-old decoding methods (McEliece, 1978) as explained by Bernstein et al. (2009).

Another post-quantum encryption technique proposed is multivariate polynomial cryptography, grounded on the belief that an individual cannot solve a system of multivariate polynomial equations. Such schemes can rely on the fact that solving these problems by any quantum algorithm will not be a feasible process; thus, they are presumed to be immune to quantum assaults. As development continues in quantum computers, multivariate systems, as well as other post-quantum approaches, will continuously play an increasingly important role in the future development of secure cryptographic protocols (Couvreur et al., 2017).

2. METHODOLOGY:

Qualitative and quantitative methods have been used in this research paper for the assessment of current levels of cryptography in the quantum era. In this regard, academic literature has been ventilated. That is, recent research on those such as lattice-based cryptography, hashes, codes, multivariate polynomials system, etc. has been reviewed theoretically. Quantitative data include case studies and experiments on performance-and security-based post-quantum cryptographic algorithms to be evaluated for key sizes, encryption speed, and resistance to quantum attacks.

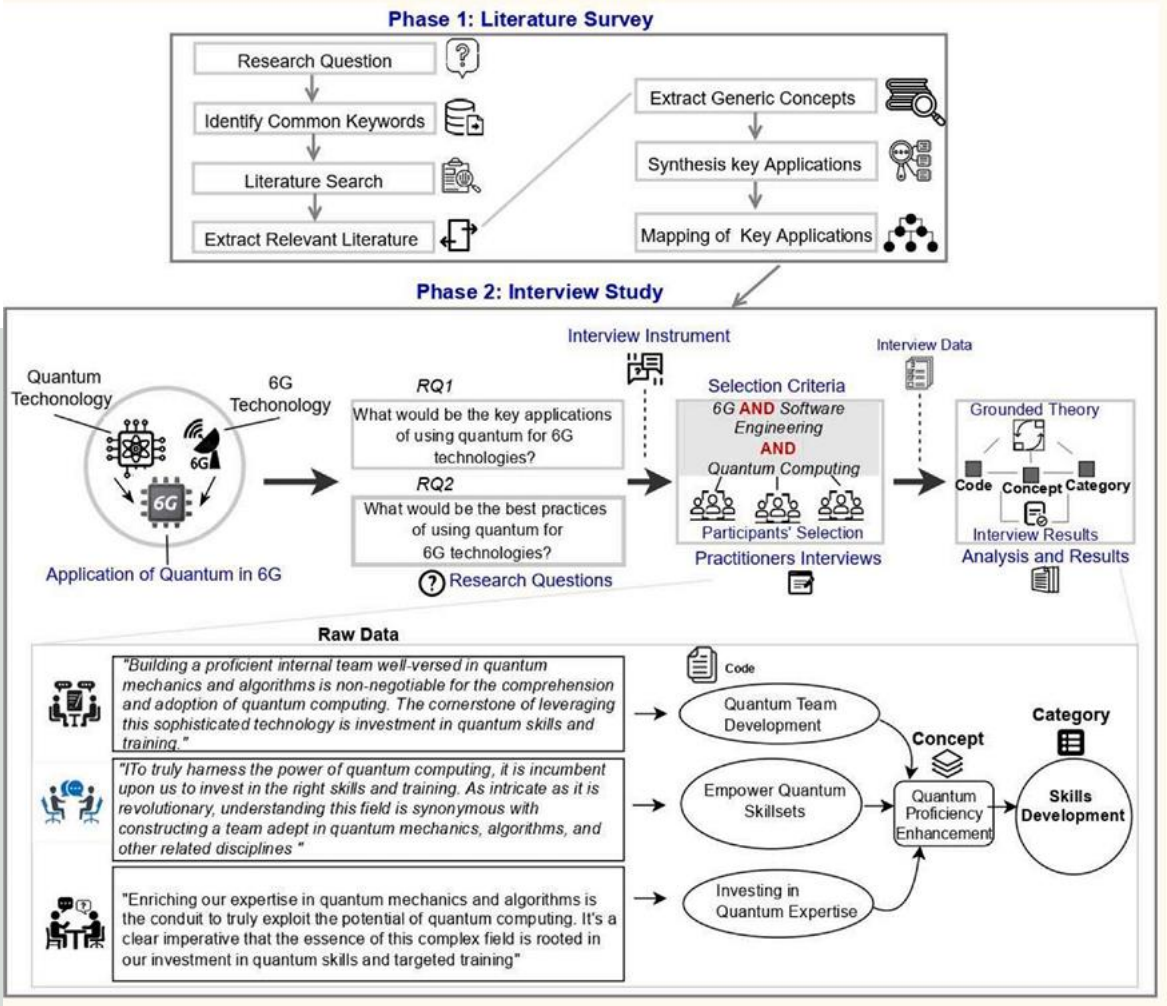
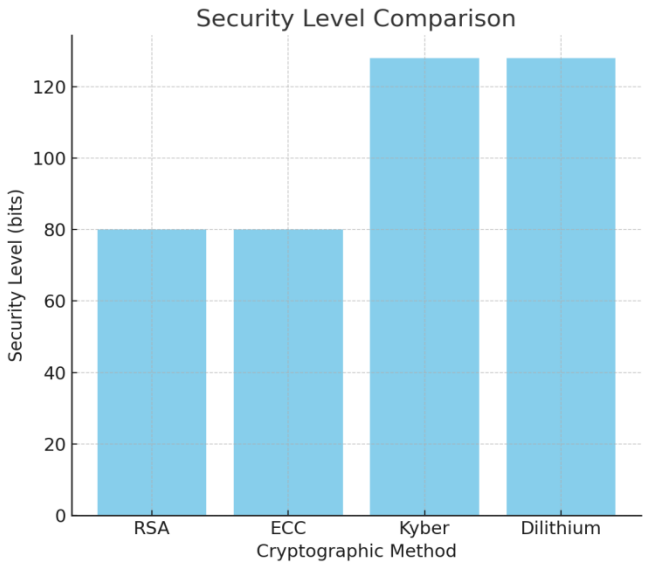


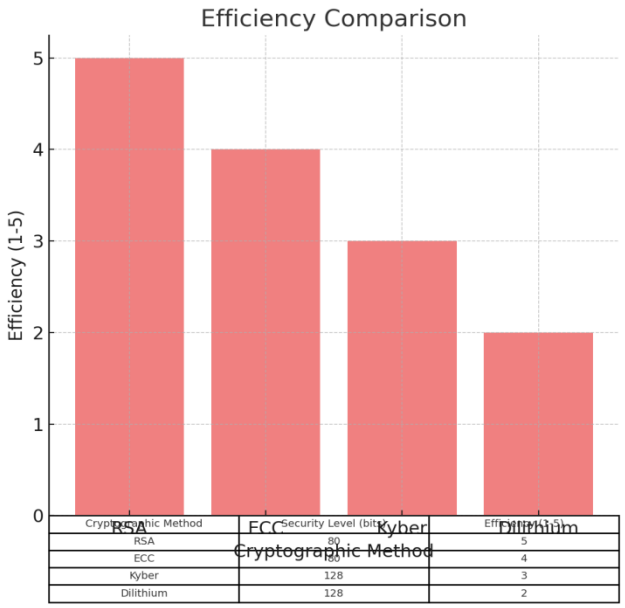
Figure. Research Methodology

3. RESULTS AND DISCUSSION:

The fields of quantum computing show promising advances because IBM and Google along with Honeywell are developing quantum processors successfully. The current technological progress has not led to creating a large-scale quantum computer that can shatter existing cryptographic systems worldwide. The approach of quantum technology demands immediate preparation for secure quantum cryptography to safeguard communication systems that act as vital connections for businesses.

The continued security of cryptographic algorithms against quantum attacks rests particularly on schemes based on lattice difficulties. A post-quantum standardization program at NIST has chosen the lattice-based scheme called Kyber and Dilithium for additional evaluation as part of its assessment process.





Cryptographic Method	Security Level (bits)	Efficiency (1-5)	
RSA	80	5	
ECC	80	4	
Kyber	128	3	
Dilithium	128	2	

The chart above presents a comparison between the different cryptographic methods (RSA, ECC, Kyber, and Dilithium) according to their security level-in-bits and efficiency on a scale from 1 to 5 (where 5 is most efficient).

- **Security Level (in bits):** Classical cryptography usually calls for small algorithms like RSA and ECC, which are both deemed to offer the same security level of 80 bits. Meanwhile, some modern post-quantum algorithms, such as Kyber and Dilithium, offer even higher security at 128 bits, which are increasingly evaluated for resistance against quantum attacks.

- **Efficiency:** Classical systems-RSA and ECC-are, in general, considered to be more efficient (4-5), while QKD systems have better security but are somewhat lesser in efficiency (2-3) than post-quantum algorithms. This arises from the additional computational complexity that post-quantum algorithms impose in terms of resource utilization.

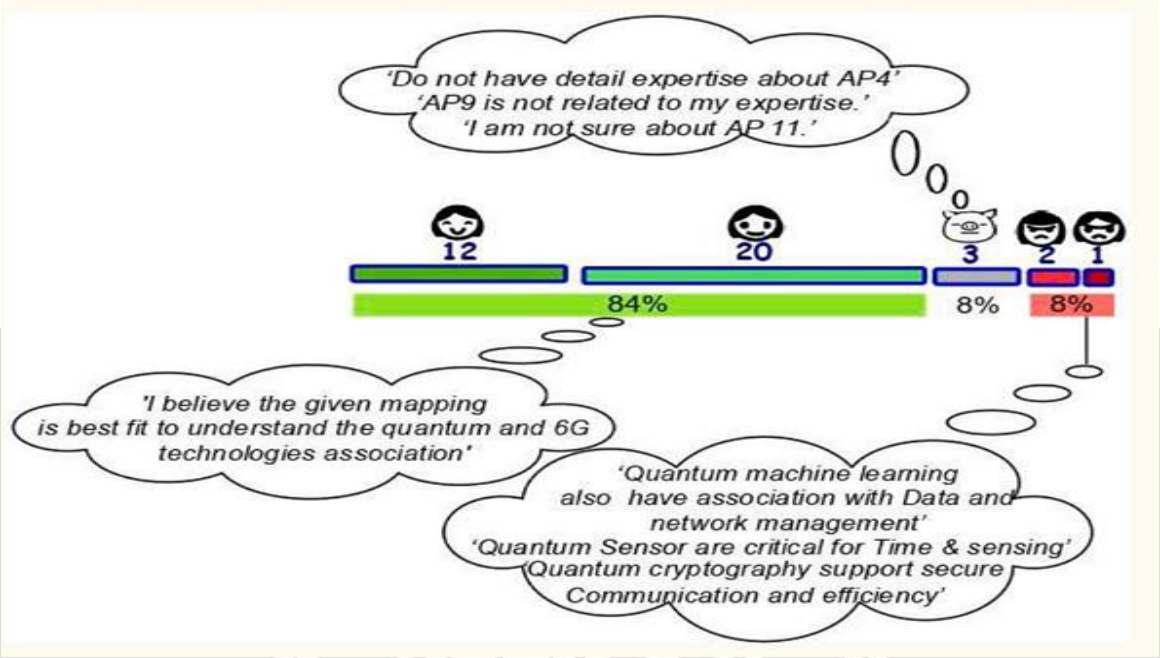


Figure. Experts' perception on mapping of key applications on core areas

FUTURE DIRECTIONS

The cryptographic world requires immediate attention for quantum-resistant data security since quantum computing technology continues to advance. The pursuit of advancing quantum computing has started despite the fact that the cryptographic-breaking quantum computer remains future technology so we must take action now. Further improvements are needed within the quantum-resistant algorithm framework because they should deliver both real-world security and operational efficiency. PQC algorithm development including lattice-based cryptography hash-based systems and code-based cryptography requires immediate accelerated work to handle rising power capabilities of quantum systems. The algorithms will undergo a complete evaluation to establish their quantum-resistant aspects as well as their functional properties including key size requirements and encryption/decryption processing speed and platform and device compatibility standards.

The investment focus remains on hybrid cryptographic systems that unite classical cryptography with quantum-resistant cryptography methods to establish interoperable networks between legacy systems and quantum computing era. Higher security is achievable through hybrid systems by integrating quantum-resistant algorithms with classical cryptographic solutions in current infrastructure. Such hybrid cryptographic systems prove essential for applications needing smooth and secure migration paths when dealing with unbuilt-upgradeable legacy systems. Quantum key distribution produces secure encryption keys through quantum mechanical properties of superposition and entanglement which get disrupted upon eavesdropping thus detecting unauthorized access. Realizing QKD systems with scalable features and cost-effective designs and building quantum networking infrastructure will provide better security for confidential communications. Applications need heightened attention in defense sector and financial services as well as healthcare

alongside other domains which emphasize information privacy highly.

The advancement of quantum cryptographic protocols to merge with traditional classical systems ranks behind QKD as the main objective. New approaches for quantum-safe digital signatures and authentication protocols along with secure multi-party computation require exploration as quantum computing technology grows stronger. These works lay the foundation for an entire security structure based on quantum technology which will be secure into the future.

The establishment of global standards for developing post-quantum cryptographic algorithm tests along with standards will be required to move forward. The world-level National Institute of Standards and Technology (NIST) will already perform PQC candidate assessments but wider global cooperation is needed to maintain secure quantum-resistant algorithm integration in diverse industries and jurisdictions for prompt acceptance. Researchers should focus on post-quantum development that combines fast-paced research with quick implementation of quantum-secure algorithms as we redefine data security for the upcoming era.

4. CONCLUSION

The deployment of quantum computing systems would degrade standard cryptographic standards that have sustained digital communication since antiquity. RSA and elliptic curve cryptography which represent conventional encryption systems are based on mathematical problems that quantum computers can solve dramatically faster compared to traditional systems. Shor's algorithms deployed by quantum computers break down the essential elements for digital information security and communication protection. PQC allows realistic prospects to secure digital communications within the quantum computing era. PQC serves as an approach to develop cryptographic systems that quantum algorithms cannot easily break therefore protecting sensitive information from quantum computer threats. The list of quantum-resistant cryptographic methods includes lattice-based cryptography together with hash-based systems and code-based cryptography and multivariate polynomial systems. The security measures utilize math problems whose quantum algorithm-based solutions human experts still cannot calculate within polynomial time to provide practical defense against quantum vulnerabilities. The emerging quantum computing industry requires all academic institutions government entities and commercial businesses to collaborate in the creation of quantum technology. The spread of quantum-resistant algorithm research plus global PQC standards development directly impacts the capability to secure digital communications systems with privacy features in modern technological environments. The immediate necessity exists for adopting PQC since this technology will serve as the primary data protection method for quantum times.

5. REFERENCES

Aithal, P. S. (2023). Advances and new research opportunities in quantum computing technology by integrating it with other ICCT underlying technologies. *International Journal of Case Studies in Business, IT and Education (IJCSBE)*, 7(3), 314-358.

Aguado, A., López, V., Brito, J. P., Pastor, A., López, D. R., & Martin, V. (2020, May). Enabling quantum key distribution networks via software-defined networking. In *2020 International Conference on Optical Network Design and Modeling (ONDM)* (pp. 1-5). IEEE.

Gill, S. S., Kumar, A., Singh, H., Singh, M., Kaur, K., Usman, M., & Buyya, R. (2022). Quantum computing: A taxonomy, systematic review and future directions. *Software: Practice and Experience*, 52(1), 66-114.

Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F. D., Lacombe, O., ... & Hansen, R. (2022). Transitioning organizations to post-quantum cryptography. *Nature*, 605(7909), 237-243.

Möller, M., & Vuik, C. (2017). On the impact of quantum computing technology on future developments in high-performance scientific computing. *Ethics and information technology*, 19, 253-269.

Bernstein, D. J., et al. (2009). *Post-quantum cryptography*. Proceedings of the International Conference on Post-Quantum Cryptography.

Bennett, C. H., & Wiesner, S. (1992). *Quantum cryptography: Public key distribution and coin tossing*. Physical Review Letters, 69(20), 2881-2884.

Chen, L. K., et al. (2016). *Report on post-quantum cryptography*. National Institute of Standards and Technology.

Koblitz, N. (1987). *Elliptic curve cryptosystems*. Mathematics of Computation, 48(177), 203-209.

Laarhoven, T., et al. (2015). *A survey of lattice-based cryptography*. Journal of Cryptographic Engineering, 5(1), 43-68.

McEliece, R. J. (1978). *A public-key cryptosystem based on algebraic coding theory*. DSN Progress Report, 42, 114-116.

Nielsen, M. A., & Chuang, I. L. (2010). *Quantum computation and quantum information*. Cambridge University Press.

Peikert, C. (2016). *Lattice cryptography for the internet*. ACM Computing Surveys (CSUR), 49(4), 1-34.

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.

Abdel-Rahman, M. (2023). Advanced cybersecurity measures in IT service operations and their crucial role in safeguarding enterprise data in a connected world. *Eigenpub Review of Science and Technology*, *7*(1), 138-158.

Aguado, A., López, V., Brito, J. P., Pastor, A., López, D. R., & Martin, V. (2020, May). Enabling quantum key distribution networks via software-defined networking. In *2020 International Conference on Optical Network Design and Modeling (ONDM)* (pp. 1-5). IEEE.

Aithal, P. S. (2023). Advances and new research opportunities in quantum computing technology by integrating it with other ICCT underlying technologies. *International Journal of Case Studies in Business, IT and Education (IJCSBE)*, *7*(3), 314-358.

Bajrić, S. (2023). Enabling secure and trustworthy quantum networks: Current state-of-the-art, key challenges, and potential solutions. *IEEE Access*, *11*, 128801-128809.

Barbeau, M., Beurier, E., Garcia-Aflaro, J., Kuang, R., Pahl, M. O., & Pastor, D. (2021). The quantum what? Advantage, utopia or threat? *Digitale Welt*, *5*(1), 34-39.

Bermudez, A., Xu, X., Nigmatullin, R., O'Gorman, J., Negnevitsky, V., Schindler, P., ... & Müller, M. (2017). Assessing the progress of trapped-ion

processors towards fault-tolerant quantum computation. *Physical Review X, 7*(4), 041061.

Cao, Y., Zhao, Y., Wang, Q., Zhang, J., Ng, S. X., & Hanzo, L. (2022). The evolution of quantum key distribution networks: On the road to the Qinternet. *IEEE Communications Surveys & Tutorials, 24*(2), 839-894.

Castellanos, M. A., Dodin, A., & Willard, A. P. (2020). On the design of molecular excitonic circuits for quantum computing: The universal quantum gates. *Physical Chemistry Chemical Physics, 22*(5), 3048-3057.

Cozzolino, D., Da Lio, B., Bacco, D., & Oxenløwe, L. K. (2019). High-dimensional quantum communication: Benefits, progress, and future challenges. *Advanced Quantum Technologies, 2*(12), 1900038.

De Leon, N. P., Itoh, K. M., Kim, D., Mehta, K. K., Northup, T. E., Paik, H., ... & Steuerman, D. W. (2021). Materials challenges and opportunities for quantum computing hardware. *Science, 372*(6539), eabb2823.

Fernandez-Carames, T. M., & Fraga-Lamas, P. (2020). Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. *IEEE Access, 8*, 21091-21116.

Ferreira, A., Lipiäinen, V., & Polito, C. (2023). Quantum technologies and cybersecurity.

Fingerhuth, M., Babej, T., & Wittek, P. (2018). Open source software in quantum computing. *PLOS ONE, 13*(12), e0208561.

Ghelani, D. (2023). Securing the future: Exploring the convergence of cybersecurity, artificial intelligence, and advanced technology.

Gill, S. S., Kumar, A., Singh, H., Singh, M., Kaur, K., Usman, M., & Buyya, R. (2022). Quantum computing: A taxonomy, systematic review, and future directions. *Software: Practice and Experience, 52*(1), 66-114.

Gill, S. S., Kumar, A., Singh, H., Singh, M., Kaur, K., Usman, M., & Buyya, R. (2022). Quantum computing: A taxonomy, systematic review, and future directions. *Software: Practice and Experience, 52*(1), 66-114.

Hagar, A., & Cuffaro, M. (2006). Quantum computing.

Heim, B., Soeken, M., Marshall, S., Granade, C., Roetteler, M., Geller, A., ... & Svore, K. (2020). Quantum programming languages. *Nature Reviews Physics, 2*(12), 709-722.

Herman, A., & Friedson, I. (2018). Quantum computing: How to address the national security risk. *Hudson Institute*.

Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F. D., Lacombe, O., ... & Hansen, R. (2022). Transitioning organizations to post-quantum cryptography. *Nature, 605*(7909), 237-243.

Khodaiemehr, H., Bagheri, K., & Feng, C. (2023). Navigating the quantum computing threat landscape for blockchains: A comprehensive survey. *Authorea Preprints*.

Kong, I., Janssen, M., & Bharosa, N. (2024). Realizing quantum-safe information sharing: Implementation and adoption challenges and policy

recommendations for quantum-safe transitions. *Government Information Quarterly*, *41*(1), 101884.

Kong, P. Y. (2020). A review of quantum key distribution protocols in the perspective of smart grid communication security. *IEEE Systems Journal*, *16*(1), 41-54.

Kop, M. (2021). Establishing a legal-ethical framework for quantum technology. *Yale Law School, Yale Journal of Law & Technology (YJoLT), The Record*.

Kumar, A., Ottaviani, C., Gill, S. S., & Buyya, R. (2022). Securing the future internet of things with post-quantum cryptography. *Security and Privacy*, *5*(2), e200.

Malina, L., Dzurenda, P., Ricci, S., Hajny, J., Srivastava, G., Matulevičius, R., ... & Tang, Q. (2021). Post-quantum era privacy protection for intelligent infrastructures. *IEEE Access*, *9*, 36038-36077.

Marella, S. T., & Parisa, H. S. K. (2020). Introduction to quantum computing. *Quantum Computing and Communications*.

McGuire, M. (2021). Nation states, cyberconflict, and the web of profit. HP Development Company, LP. Retrieved from https://press.hp.com/content/dam/sites/garage-press/press/press-releases/2021/web-of-profit/hp-bpsweb-of-profit-report-april-2021.pdf

Mexriddinovich, A. Z. (2023). Safeguarding digital security: Addressing quantum computing threats. *The Role of Exact Sciences in the Era of Modern Development*, *1*(4), 1-7.

Möller, M., & Vuik, C. (2017). On the impact of quantum computing technology on future developments in high-performance scientific computing. *Ethics and Information Technology*, *19*, 253-269.

Perrier, E. (2022). The quantum governance stack: Models of governance for quantum information technologies. *Digital Society*, *1*(3), 22.

Rosales, M. (2019). Quantum computing and the threat to classical encryption methods (Doctoral dissertation, Utica College).