International Journal of Multidisciplinary and Current Educational Research (IJMCER)
ISSN: 2581-7027 ||Volume|| 6 ||Issue|| 4 ||Pages 14-18 ||2024||

Decrypting the Future: Quantum Computing's Role in Encryption

Alex Mathew
Department of Cybersecurity, Bethany College, USA

ABSTRACT : As quantum computing technology rapidly advances, the security of current encryption techniques faces unprecedented threats. Quantum computers can run algorithms like Shor's to crack widely used RSA and ECC public key systems. This literature review analyzes quantum computing's potential impact on encryption through a systematic examination of 15 sources. Quantum concepts like superposition and entanglement enable quantum algorithms to solve problems intractable for classical computers. Estimates suggest cryptographically relevant quantum computers could emerge in the next 10-30 years. Mathematical foundations behind RSA, ECC, and related techniques are vulnerable to quantum attacks. Symmetric ciphers face less risk but still require increased key sizes. Progress is underway on quantum-resistant cryptosystems using lattices, multivariate math, hash functions, and error-correcting codes. Initiatives like NIST's post-quantum cryptography standardization project are driving the development and adoption of quantum-safe algorithms. However, costs and hurdles remain in transitioning protocols and security infrastructure to the quantum-safe era. With prudent preparation and migration, organizations can harness quantum computing's power while mitigating its threats to encryption. This review covers key developments, vulnerabilities, and expert recommendations to decrypt quantum computing's role in the future of secure communications.
.

KEYWORDS - quantum computing, encryption, cybersecurity, quantum cryptography, post-quantum cryptography

I. INTRODUCTION

Encryption provides the vital foundation for security in the digital age [1], protecting sensitive data across sectors like finance, healthcare, government, and more [2]. Common public key techniques like RSA and ECC rely on the complexity of mathematical problems that make decryption computationally infeasible without the correct cryptographic key [3]. However, the advent of quantum computing threatens to upend the cryptography landscape [4]. Quantum computers leverage principles like superposition and entanglement to run algorithms capable of cracking encryption previously thought secure [1,4]. With cryptographically relevant quantum computers potentially emerging in the next 10-30 years, the clock is ticking to transition to quantum-safe encryption.

This systematic literature review scope includes 15 sources to identify the current status of quantum computing technology, its threats, and effects on cryptographic systems, quantum computing advancement in developing quantum-resistant algorithms, and expert opinions on managing the transition to the post-quantum world. While quantum computing can be a source of revolutionary advancements and tremendous threats, this review aims to assess the potential of quantum computing in the future of encryption. Thus, it offers computer scientists, cybersecurity specialists, and information security professionals a comprehensive reference to understanding quantum computing basics, threats, and protection measures to prepare for the quantum attack on encryption. This analysis comes at a crucial juncture, helping equip major stakeholders with actionable intelligence to secure user data and digital infrastructure against the quantum threat.

II. PROPOSED METHODOLOGY BLOCK DIAGRAM

This systematic literature review examined 15 sources on quantum computing and encryption published from 2020 to 2024. The following databases were searched: IEEE Xplore, ACM Digital Library, ScienceDirect, and Google Scholar. Search terms included "quantum computing," "encryption," "post-quantum cryptography," "quantum-resistant algorithms," and related keywords. Sources were screened for relevance based on title, abstract, and full-text review. Inclusion criteria comprised peer-reviewed conference papers, journal articles, and reports focused on the impact of quantum computing on encryption or post-quantum cryptography solutions. Editorials, short conference abstracts, and physics-focused quantum computing sources were all excluded. A PRISMA-style flow diagram depicts the stages of article identification, screening, assessment, and final inclusion. Findings were systematically analyzed and synthesized to evaluate quantum computing's implications for encryption security and strategies to enable a smooth transition to the quantum-safe cryptography era.

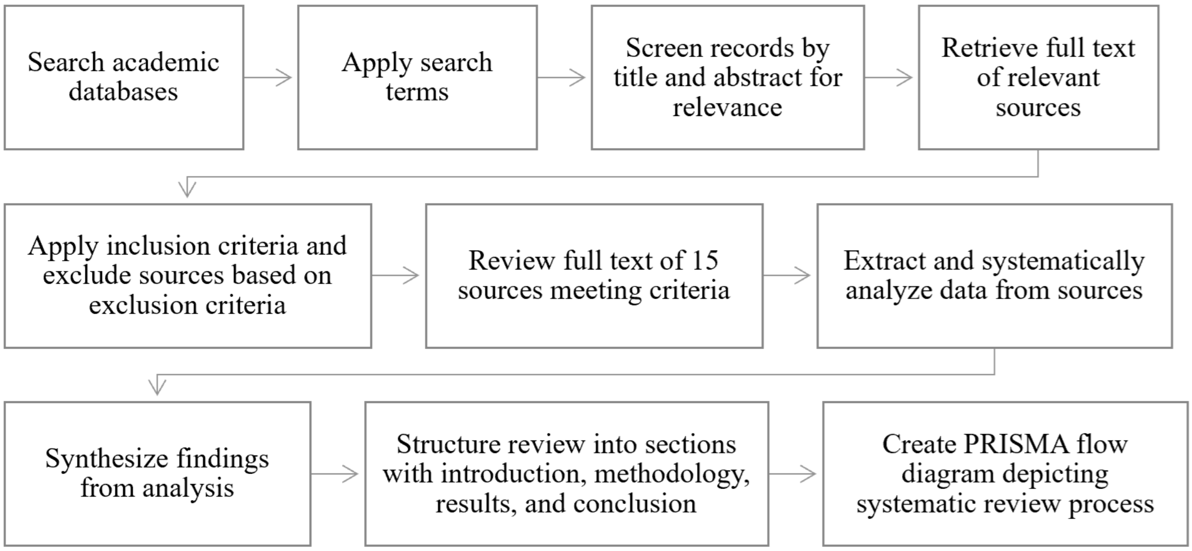
Search academic databases
Apply search terms
Screen records by title and abstract for relevance
Retrieve full text of relevant sources
Apply inclusion criteria and exclude sources based on exclusion criteria
Review full text of 15 sources meeting criteria
Extract and systematically analyze data from sources
Synthesize findings from analysis
Structure review into sections with introduction, methodology, results, and conclusion
Create PRISMA flow diagram depicting systematic review process

Fig. 1: Block Diagram

III. ALGORITHM

The systematic review of literature on quantum computing's impact on encryption followed these steps:

1. Comprehensively search academic databases (IEEE, ACM, ScienceDirect, Google Scholar) using selected keywords and queries related to "quantum computing," "post-quantum cryptography," "quantum-resistant algorithms," and synonyms.
2. Screen search results by title and abstract for relevance to the research questions on quantum computing's encryption capabilities and post-quantum solutions. Exclude sources focused purely on physics principles.
3. Retrieve full text of relevant sources and apply inclusion criteria: peer-reviewed papers, 2020-2024 date range, technical focus on cryptography and quantum computing. Exclude editorials, short abstracts, and unrelated topics.
4. Systematically review and extract data from 15 sources meeting inclusion criteria to analyze key themes: quantum computing concepts, encryption vulnerabilities, post-quantum progress, security implications, and transition recommendations.
5. Synthesize findings through a narrative summary identifying core insights, limitations, and gaps to be addressed by future research.
6. Structure synthesized review into logical sections with an introduction, methodology, results organized by theme, and conclusion.
7. Finalize the manuscript with a concise abstract, relevant visual aids like diagrams and charts, and properly formatted citations and references.
8. Have cryptography and quantum computing experts review the paper to validate the technical accuracy and merit of the literature review.
9. Submit systematic review paper to relevant peer-reviewed journals and conferences focused on cybersecurity, cryptography, and quantum computing for publication.

I. FLOW CHART

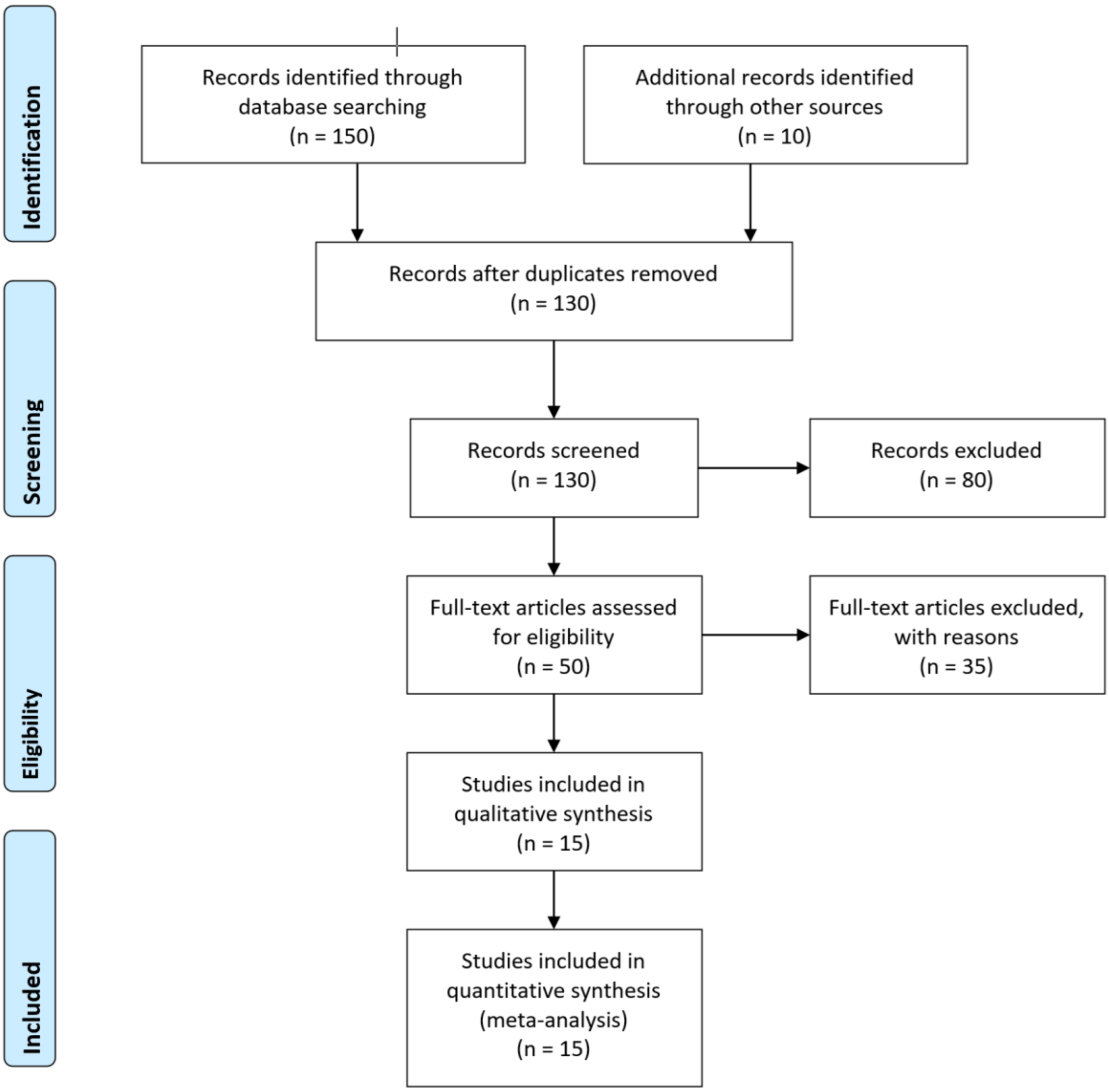
Identification
Screening
Eligibility
Included
Records identified through database searching (n = 150)
Additional records identified through other sources (n = 10)
Records after duplicates removed (n = 130)
Records screened (n = 130)
Records excluded (n = 80)
Full-text articles assessed for eligibility (n = 50)
Full-text articles excluded, with reasons (n = 35)
Studies included in qualitative synthesis (n = 15)
Studies included in quantitative synthesis (meta-analysis) (n = 15)

Fig. 2
A systematic review of the literature (PRISMA)

III. RESULT ANALYSIS

Quantum Computing Concepts: Quantum computing leverages principles of quantum physics to represent and process data in exponentially more efficient ways than classical computing [5]. Rather than binary bits, quantum computers use quantum bits (qubits) based on subatomic particles in a quantum superposition of 0 and 1 states [5,6]. Multiple qubits can become entangled, letting a set represent many combinations simultaneously [6]. This parallelism enables quantum algorithms like Shor's for factoring large primes and Grover's for database searching to solve problems intractable for classical systems [7]. Current quantum computers have reached the level of containing dozens to hundreds of qubits. However, eliminating noise and decoherence remains a key challenge in scaling up stable, error-corrected qubits to the thousands required to crack encryption keys [5,7]. Estimates suggest cryptographically relevant quantum computers capable of breaking RSA, ECC, and Diffie-Hellman could emerge in the next 10 to 30 years, underscoring the urgent need to transition to quantum-safe cryptography.

Vulnerabilities in Encryption : Widely used public key encryption schemes like RSA, ECC, and Diffie-Hellman rely on the difficulty of solving mathematical problems such as factoring large prime numbers [8]. However, Peter Shor's quantum algorithm leverages quantum parallelism to efficiently find prime factors and compute discrete logarithms, breaking the cryptographic foundations of these techniques [8]. Specifically, Shor's algorithm can crack RSA by factoring the public modulus n and ECC by computing the private key d [9].

Symmetric algorithms are less vulnerable but still at risk from Grover's search algorithm speedups. Authenticated encryption combines symmetric ciphers like AES with authentication mechanisms, which may face reduced security margins from quantum attacks [8,9]. Conservative key size increases can strengthen symmetric crypto against quantum, but full migration to quantum-safe public key encryption remains necessary for long-term defense against quantum computing capabilities.

Progress in Quantum-Resistant Cryptography : In response to quantum threats, researchers have developed new quantum-safe cryptography techniques designed to be secure against both classical and quantum attacks. Major approaches include lattice-based schemes such as Kyber and NewHope, which rely on the hardness of lattice problems; multivariate systems like Rainbow, which use systems of polynomial equations; hash-based signatures like SPHINCS exploiting cryptographic hash functions, and code-based cryptosystems like Classic McEliece using error-correcting codes [10,11]. NIST is leading standardization efforts for post-quantum algorithms with the goal of transitioning to quantum-safe cryptography [10]. Performance analyses show different trade-offs between key and signature sizes, encryption/decryption speed, and computational overhead for various quantum-resistant algorithms [10,11]. Ongoing work by academia, industry, and standards bodies like ETSI, IETF, and IRTF aims to integrate post-quantum cryptography into essential communication protocols, including TLS, SSH, IPSEC, DNSSEC, and VPNs to enable a smooth transition to the quantum-safe era [12].

Other Quantum Computing Security Implications : Beyond breaking encryption, quantum computing also enables new approaches to secure communication. Quantum key distribution (QKD) leverages quantum physics to generate and share random secret keys between parties, providing an information-theoretically secure alternative to RSA key exchange [13]. However, blockchain platforms and digital signatures remain dependent on classical cryptography and are vulnerable to quantum attacks. Ongoing research explores quantum-secured blockchain and signature schemes [14]. Quantum-safe multi-party computation and post-quantum zero-knowledge proofs offer other directions for resilient quantum communication protocols [14]. On the flip side, rapid advances in quantum algorithms, computing power, and accessibility raise concerns about misuse for malicious hacking, financial fraud, or decrypting sensitive archived data. Quantum computing arms a double-edged sword, necessitating vigilance and agility from cybersecurity stakeholders to steer computing breakthroughs toward social benefit while mitigating emerging digital risks.

Transitioning to the Quantum-Safe Era : It is suggested that post-quantum cryptography should be used alongside the current standards during the transition period [1,5,11]. However, expenses, integrations, and inexperience act as barriers to implementing new quantum-safe algorithms [15]. Entities such as the Consortium for Quantum Computing and Security are forging cooperation between various stakeholders from the business, public, and academic sectors. NIST post-quantum project supports the standard setting in the United States while the EU, UK, Japan, and China support quantum through research grants, infrastructures, and strategic plans [10,11]. Governments also build quantum competence through the expansion of academic courses and cooperation with companies. Thus, quantum readiness of the public and private sectors, including the incorporation of quantum-safe cryptography into critical infrastructures, along with the raising of awareness among the population, can lead society to the quantum realm and control the S-curve's turbulence for the sake of digital security.

IV. CONCLUSION

Overall, this systematic literature review focuses on explaining how quantum computing inherently threatens conventional cryptography. Algorithms such as Shor's quantum algorithm can easily crack RSA, ECC, and other common public key methods. However, the quantum risks are still present, and despite the increase in symmetric cipher resistance, the transition to post-quantum cryptography must be made. Lattice-based, code-based, multivariate mathematical, and cryptographic hash algorithms are expected to provide secure solutions that can replace the existing weak ones. NIST's standardization projects like these propel the advancement and utilization of quantum-safe encryption. Nonetheless, the costs and the compatibility issues are the factors that hamper the seamless integration of the system. Thus, the way to ensure security in the near future is to use post-quantum cryptography along with the existing standards while all the stakeholders gain the necessary experience in implementing quantum-safe solutions into the protocols and systems. While quantum computing is expected to bring great change and advancement in the future due to the digital revolution, it is high time that industry, government, and academics come together and work proactively to protect data and infrastructure for the quantum world.

REFERENCES

[1] Sharma, Moolchand, et al. "Leveraging the power of quantum computing for breaking RSA encryption." Cyber-Physical Systems, vol.7, no.2, 2021, pp.73-92. https://doi.org/10.1080/23335777.2020.1811384

[2] Goyal, Prachi. "The Importance of Data Encryption in Data Security." Journal of Nonlinear Analysis and Optimization, vol.13, no.1, 2022. https://jnao-nu.com/Vol.%2013,%20Issue.%2002,%20July-December%20:%202022/1.pdf

[3] Ferenc, Koczka. "Security of encryption procedures and practical implications of building a quantum computer." AARMS–Academic and Applied Research in Military and Public Management Science, vol.19, no.3, 2020, 5-22. https://doi.org/10.32565/aarms.2020.3.1

[4] Khodaiemehr, Hassan, Khadijeh Bagheri, and Chen Feng. "Navigating the quantum computing threat landscape for blockchains: A comprehensive survey." Authorea Preprints, 2023. https://doi.org/10.36227/techrxiv.24136440.v1

[5] Cavaliere, Fabio, John Mattsson, and Ben Smeets. "The security implications of quantum cryptography and quantum computing." Network Security, vol.2020, no.9, 2020, pp.9-15. https://doi.org/10.1016/S1353-4858(20)30105-7

[6] Chatterjee, Preeta, and Rishika Chakraborty. "A Brief Study on Quantum Computing." International Journal of Innovative Research in Physics, vol.1, no.4, 2020, pp.58-63. https://doi.org/10.15864/ijiip.1407

[7] Leider, Avery, et al. "Quantum computer search algorithms: Can we outperform the classical search algorithms?." Proceedings of the Future Technologies Conference (FTC) 2019: Volume 1. Springer International Publishing, 2020. https://doi.org/10.1007/978-3-030-32520-6_34

[8] Yang, Wenxin. "ECC, RSA, and DSA analogies in applied mathematics." International Conference on Statistics, Applied Mathematics, and Computing Science (CSAMCS 2021). Vol. 12163. SPIE, 2022. https://doi.org/10.1117/12.2628013

[9] Overmars, Anthony, and Sitalakshmi Venkatraman. "New semi-prime factorization and application in large RSA key attacks." Journal of Cybersecurity and Privacy, vol.1, no.4, 2021, pp.660-674. https://doi.org/10.3390/jcp1040033

[10] Alagic, Gorjan, et al. "Status report on the third round of the NIST post-quantum cryptography standardization process." National Institute of Standards and Technology: U.S. Department of Commerce, 2022, pp.07. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=934458

[11] Farooq, Sana, et al. "Resilience Optimization of Post-Quantum Cryptography Key Encapsulation Algorithms." Sensors, vol.23, no.12, 2023, 5379. https://doi.org/10.3390/s23125379

[12] Kampanakis, Panos, and Tancrède Lepoint. "Vision paper: Do we need to change some things? Open questions posed by the upcoming post-quantum migration to existing standards and deployments." International Conference on Research in Security Standardisation. Cham: Springer Nature Switzerland, 2023. https://doi.org/10.1007/978-3-031-30731-7_4

[13] Lyssenko, Dmitry, and Olufemi Komolafe. "Leveraging Quantum Key Distribution for Securing MACsec Communications." Proceedings of the 1st Workshop on Quantum Networks and Distributed Quantum Computing. 2023. https://doi.org/10.1145/3610251.3610555

[14] Banaeian Far, Saeed, and Maryam Rajabzadeh Asaar. "A blockchain-based quantum-secure reporting protocol." Peer-to-Peer Networking and Applications, vol.14, no.5, 2021, 2992-3011. https://doi.org/10.1007/s12083-021-01152-z

[15] Varner, Karolin, et al. "Agile, Post-quantum Secure Cryptography in Avionics." Cryptology ePrint Archive, vol.1, no.1, 2024. https://doi.org/10.48550/arXiv.2404.12854