International Journal of Core Engineering & Management
Volume-6, Issue-11, 2021 ISSN No: 2348-9510

QUANTUM COMPUTING AND CRYPTOGRAPHY

Anvesh Gunuganti
maverickanvesh@gmail.com

Abstract

Quantum computing is evolving and is a major threat to classical cryptography methods. These views, along with a detailed contour of current and prospective threats of quantum computing and prospects of quantum-resistant cryptography, are discussed in this paper. It describes recent progress, analyzes the quantum cryptography strengths, weaknesses, opportunities, and threats assessment, and suggests the main research topics. Stressing the importance of anticipation in performing changes, the paper identifies measures for risk reduction and applies the benefits of quantum technologies in cybersecurity.

Keywords— Quantum computing, cryptography, vulnerabilities, quantum-resistant solutions, cybersecurity adaptation

I. INTRODUCTION

Quantum computing is a significant revolution in the theory and development of computational systems that aims to use the laws of quantum mechanics to solve problems that are impossible or inefficient to be solved by classical systems [1]. Unlike classical computing, which uses bits (0s and 1s) to process data, quantum computers use quantum capital or qubits to exist in two states simultaneously through superposition and entanglement. This inherent parallelism helps quantum computers work with huge data sets and solve problems much faster than classical computers at their roots.

Incredibly, cryptography is at the core of quantum computing change potential. Cryptography is the basis of protecting such valuable and crucial information as messages and conversations, transactions, and even data in this world ruled by computer technology [2]. However, with the evolution of quantum computing, these algorithms are under the threat of being easily compromised. Shor's and other quantum algorithms mean that many mathematical problems categorized as difficult for computational machines, specifically integer factorization and discrete logarithms, have become notably easier for quantum computers to solve [3].

Quantum cryptography becomes a task to be solved since, as quantum computation is slowly moving towards real-world application, the cryptographic community will be forced to look for post-quantum algorithms that are secure against attacks by classical and quantum computers. Due to these, it is paramount to focus more research and development in post-quantum cryptography to safeguard the confidentiality and integrity of relevant and sensitive information once quantum computers surface [4].

A. Overview of Quantum Computing and Its Potential Impact on Cryptography

Quantum computing radically changes computational theory and implementation, solving problems faster than traditional computers through quantum mechanics [5]. While a classical computer processes information in data referred to as bits, being units of 0 and 1, a quantum computer processes information in quantum bits or qubits. QU, or quantum bits, can be in multiple states at once because of quantum superposition and can be entangled. Thus, it makes quantum computers capable of processing huge data content, combined with the ability to solve problems at high speed.

Cryptography studies on quantum computing are one of the most significant areas that have been discovered. Cryptography is very important for protecting communication, such as telephone and electronic transactions, banking, and data protection using data authentication and hashing techniques, which use mathematical algorithms that currently cannot be broken by conventional computing techniques [6]. Nonetheless, such cryptographic algorithms may become easily breakable with quantum computers due to algorithms such as Shor's algorithm, which relatively takes a short time to factor large numbers, which is believed to be hard for classical computers. Also, fig. 1 explains the impact of Quantum Computing.

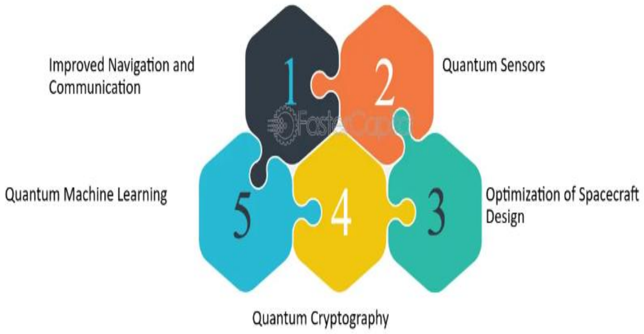

Improved Navigation and Communication
1
2
Quantum Sensors
Quantum Machine Learning
5
4
3
Optimization of Spacecraft Design
Quantum Cryptography

Fig. 1. Quantum Computing and its Impact [10]

B. *Importance of Understanding the Intersection Between Quantum Computing and Cryptography*

Convening the relationship between quantum computing and cryptography is crucial due to several factors. First, as quantum computing moves closer to being real and applicable in real-life scenarios, it presents a large threat to the security structures used in electronic communication and business worldwide. Cryptographic algorithms utilized in banks, governments, and other electronic commerce networks and transactions used today may become insecure by quantum computers, implying that information is no longer safe in such facilities [7].

Second, there is a need for active research into and development of quantum-resistant cryptography to help avoid these risks. Scholars and practitioners should design and use cryptographic protocols that can prevent cracking by the present powerful quantum machines. Now, this involves research on algorithms that should resist quantum computing attacks and the QKD systems that can be used for secure communication when quantum computing becomes prevalent [8].

Third, if knowing how quantum computing can improve cryptography unlocks new approaches, the view is also valid. Quantum cryptography, for example, is said to provide the highest level and unassailable encryption through the application of Quantum mechanics, and this is the bedrock for a future wired world.

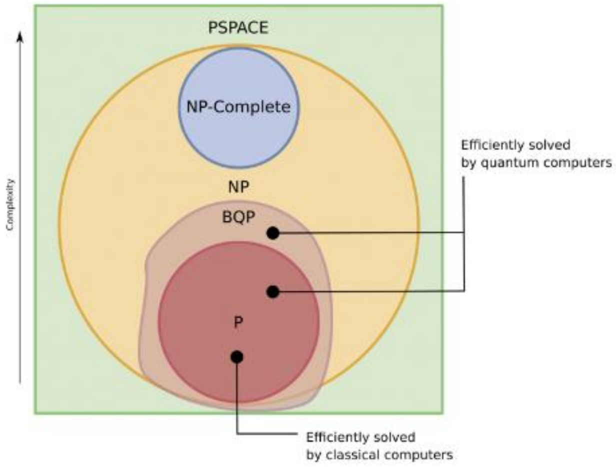

PSPACE
NP-Complete
NP
BQP
P
Complexity
Efficiently solved by quantum computers
Efficiently solved by classical computers

Fig. 2. Quantum computing and cryptography [11]

C. *Research Objectives and Scope*

This discussion paper intends to provide a detailed overview of the state-of-the-art and prospects of quantum computing and cryptography. It aims to:

- Examine new developments in quantum computing technologies and analyze how they can influence cryptography.
- Make a SWOT analysis regarding quantum computing and cryptography's strengths, weaknesses, opportunities, and threats.
- Enumerate what has been discovered from the current literature and establish the trends associated with this concept and other emergent themes.
- Identify valuable future research topics and guidelines for exploring quantum-safe cryptography and optimization of quantum computing in cybersecurity.

D. *Research Questions*

- How can cryptography be adapted to defend against emerging threats posed by quantum computing advancements?

II. LITERATURE REVIEW

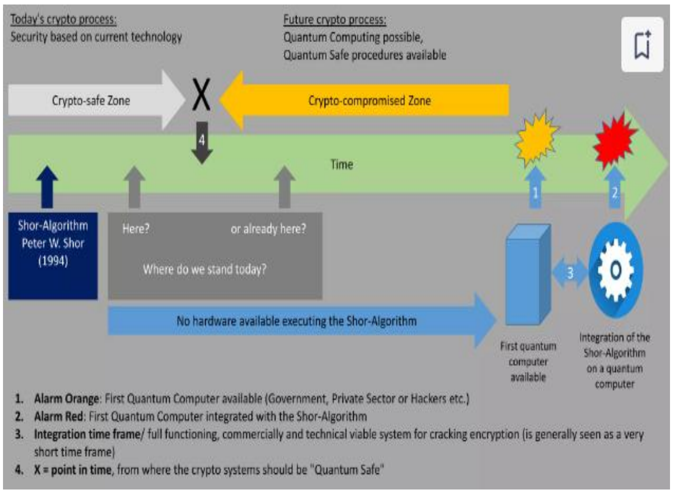
A. *Overview of Recent Advancements in Quantum Computing Technologies*

The recent years have marked enormous progress in quantum computing that transitioned from abstract ideas to viable prototypes for research and development laboratories and centers. The main milestones achieved are the scaling of qubit systems, error correction methods like quantum error correction codes, and quantum supremacy, a quantum computer's ability to carry out specific computations much faster than classical computers [9].

The performance of quantum quantum computer Sycamore, with 53 qubits in 2019 of quantum supremacy, can be considered an achievement that helped demonstrate the ability of quantum computers to perform calculations beyond the capabilities of traditional ones. Other players, including IBM and Microsoft on their part, and other young entrepreneurs like Rigetti Computing and IonQ, are also investing time and resources in creating more powerful processors with greater numbers of qubits and better coherence times, which are fitting for performing more complex calculations.

B. *Review of Current Cryptographic Standards and Vulnerabilities to Quantum Attacks*

Modern encryption algorithms, present in RSA and ECC (Elliptic Curve Cryptography), are based on factoring large and solving Discrete Logarithm Problems, which no classical computers can solve because they are NP-hard problems. Yet, quantum computers, especially with the help of Shor's algorithm in execution, pose a potential danger to these cryptographic fundamentalisms [8]. Fig. 3. explains the Shor's Algorithm.


Today's crypto process:
Security based on current technology
Future crypto process:
Quantum Computing possible,
Quantum Safe procedures available
Crypto-safe Zone
X
Crypto-compromised Zone
4
Time
1
2
Shor-Algorithm
Peter W. Shor
(1994)
Here?
or already here?
Where do we stand today?
3
No hardware available executing the Shor-Algorithm
First quantum computer available
Integration of the Shor-Algorithm on a quantum computer

1. **Alarm Orange**: First Quantum Computer available (Government, Private Sector or Hackers etc.)
2. **Alarm Red**: First Quantum Computer integrated with the Shor-Algorithm
3. **Integration time frame**/ full functioning, commercially and technical viable system for cracking encryption (is generally seen as a very short time frame)
4. **X = point in time**, from where the crypto systems should be "Quantum Safe"

Fig. 3. Quantum Computing Shor algorithm [12]

Out of all the quantum algorithms, Shor's algorithm, which was created in 1994, can efficiently factorize large numbers and solve discrete logarithm problems. This capability undercuts a keyholding of RSA and ECC-based encryption systems and may make them 'crackable' by a sufficiently large quantum computer.

C. *Review of Literature on Quantum-Resistant Cryptography and Quantum Key Distribution (QKD) Systems*

Scholars are researching quantum-resistant cryptography indicators to meet the threats inherent in quantum computing. These algorithms, frequently derived from mathematical problems and considered by most experts as intractable for quantum computers, protect quantum communications from quantum-based attacks [5].

Some of the types of post-quantum cryptography
are Lattice cryptography, Code Complexity cryptography, and Hashed cryptography. These approaches utilize problems that are not easy to solve with quantum algorithms of the near future, such as Shor's algorithm, thus providing solutions for post-quantum cryptography [8].

Two main secure communication categories include quantum-resistant cryptography and quantum key distribution –QKD systems. QKD uses the principles of quantum mechanics to allow the secure generation/exchange of cryptographic keys that cannot be intercepted/decoded by third-party intruders as per the principles of quantum uncertainty .

Scientists are also working on various QKD protocols, including continuous-variable and measurement-device-independent QKD, to make QKD more efficient, distant, and practical for quantum secure communication.

As a result, this literature review gives an understanding of the state of the art of the current advances in quantum computing technologies, highlights the susceptibility of today's cryptographic standards to quantum attacks, and presents existing and further investigations on quantum-resistant cryptography and quantum key distribution systems. This lays a foundation for analysis and discussion on the consequences of quantum computing on cryptography in the following sections of the discussion paper. Fig. 4 shows Shor's Algorithm for Factoring Quantum Algorithms.

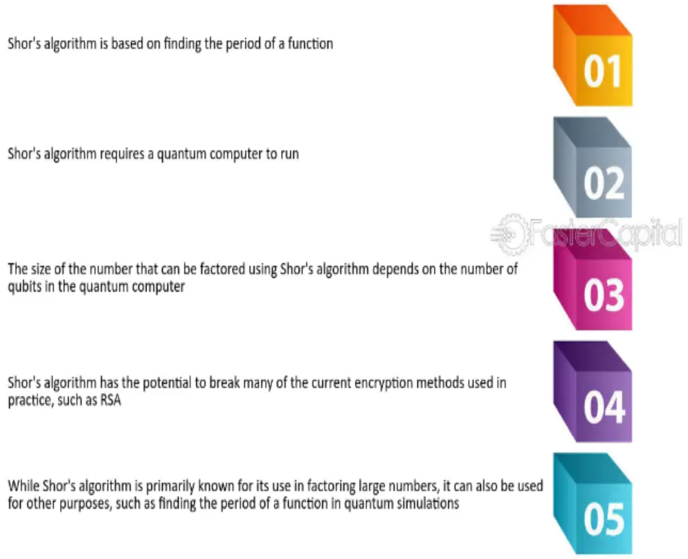

Shor's algorithm is based on finding the period of a function
01
Shor's algorithm requires a quantum computer to run
02
The size of the number that can be factored using Shor's algorithm depends on the number of qubits in the quantum computer
03
Shor's algorithm has the potential to break many of the current encryption methods used in practice, such as RSA
04
While Shor's algorithm is primarily known for its use in factoring large numbers, it can also be used for other purposes, such as finding the period of a function in quantum simulations
05
FasterCapital

Fig. 4. Shor's Algorithm for Factoring Quantum Algorithms [13]

III. METHODOLOGY

1. **Strengths**

Internal Strengths

- **Enhance security through quantum key distribution (QKD) systems:** Quantum mechanics principles allow the exchange of encryption keys with the help of which communication is protected from interception, based on the laws of quantum mechanics.
- **Potential for solving complex mathematical problems used in encryption:** Thus, they have a property to solve those problems effectively that is hard for classical computers like integer factorization and discrete logarithms [15].

External Opportunities

- **Development of quantum-resistant cryptographic algorithms:** Scientists are searching for more secure cryptography suitable for defending against quantum machine attacks to remain safe in future communication technology applications.
- **New opportunities for secure communication channels in quantum networks:** Quantum networks utilize quantum mechanics to build security into the very communication mechanisms, which is why it can provide unprecedented security.

2. **Weaknesses**

Internal Weaknesses

- **Current cryptographic standards vulnerable to quantum attacks:** RSA and ECC encryption techniques can be susceptible to quantum computers using algorithms such as Shor's algorithm.
- **Complexity and cost of transitioning to quantum-safe cryptography:** Deploying and integrating quantum-resistant cryptography algorithms require a very technical process and a lot of money [15].

External Threats

- **Potential decryption of current encrypted data by future quantum computers:** New quantum computers that may be developed shortly may be able to break into existing data codes, and thus, secure information can be invaded.
- **Uncertainty in the timeline and readiness of mainstream quantum computing:** The suitability of large-scale, fault-tolerant quantum computers in practical applications remains unknown, influencing the timelines for quantum-safe cryptography.

3. **Opportunities**

Internal Opportunities

- **Advancements in quantum-resistant algorithms and protocols:** Current research focuses on producing algorithms immune to quantum attacks, thereby preserving the reliability of digital security.
- **Exploration of new cryptographic techniques leveraging quantum mechanics:** Quantum cryptography provides new ideas for data protection, which can change the sphere of digital trust and security.

External Strengths

- **Potential for innovation in cybersecurity solutions:** The research discovers that the development of quantum computing in cybersecurity creates positive impacts to increase innovative solutions.
- **Emerging applications in financial transactions and data privacy:** Quantum technologies can revolutionize secure financial transactions, healthcare data protection, and more.

4. **Threats**

Internal Threats

- **Risk of quantum computing disrupting current encryption standards:** This is because the development of master quantum computing systems is fast and may easily surpass today's encryption mechanisms, making it an area that needs to be adapted quickly.
- **Challenges in regulatory compliance and international standards adoption:** Mitigating the risks of modern and future cryptography creates problems in creating worldwide standards in the quantum application space.

External Weaknesses

- **Resistance to adopting quantum-safe cryptography among industries:** Organizations or industries may not adopt quantum-safe cryptography, fearing costs, and the complexity of the approach, as well as the benefits gained, is not very clear.

- **Lack of universal agreement on quantum-resistant standards:** The lack of agreement on quantum-resistant standards would cause the development of disparate systems and integration issues in the international community.

This SWOT analysis will assess the potential advantages and risks of the relationship between quantum computing and cryptography. This piece provides points of focus for additional research and elaboration when examining quantum technologies and their implications for future cybersecurity.

IV. FINDINGS AND DISCUSSION

Integrated Analysis of Strengths, Weaknesses, Opportunities, and Threats Obtained from the SWOT Framework

The SWOT analysis of quantum computing and cryptography reveals several critical insights:

- **Strengths:** Quantum computing can strengthen security and establish a new generation of secure communication techniques, such as quantum key distribution (QKD) and fast problem-solving compared to classical computers. This could even bring a drastic change in the approach to encryption in quantum networks and the means that can be used to have secure quantum communication.
- **Weaknesses:** Today's cryptographic standards, which can be attacked using quantum computing, are at the crossroads of migrating to post-quantum cryptography, a complex and expensive process. However, the rates for mainstream quantum computing are still unknown, presenting a security concern to today's encryption mechanisms.
- **Opportunities:** There are novelties in the progress of quantum-resistant algorithms and protocols that will enable cryptographers to develop sturdy cryptographic strategies resistant to quantum attacks. Considering the potential of brand-new cryptographic algorithms based on quantum mechanics, one can describe valuable opportunities to advance novel classes of security and technologies for numerous industries.
- **Threats:** The idea of decrypting new information, which quantum computers will be able to create in the future, is a severe challenge to the confidentiality of contemporary encrypted information.

However, regulatory and international standards issues might slow down or complicate the adoption of quantum-safe cryptography worldwide.

A. Comparative Analysis of Different Perspectives from Recent Literature

Recent literature offers varying perspectives on the intersection of quantum computing and cryptography:

- **Technological Readiness:** Some researchers insist that quantum computing remains a hope for the future, while the actual quantum computers with the potential to break current cryptography are still under development as the first full-fledged quantum computers.
- **Security Implications:** It leads to stressed talks on the importance of quantum-resistant cryptography to ensure cyber security as quantum developments proceed rapidly. Today's cryptographic paradigms are universally understood to be unsafe against quantum assaults.
- **Innovation Opportunities:** It also describes how quantum technologies can provide opportunities for advancements in cybersecurity, healthcare data privacy, financial transactions, etc. This includes developments such as using quantum mechanics to develop strong and reliable communication networks and data protection methods.

B. Key Trends and Emerging Themes in Quantum Computing and Cryptography Research

Several key trends and emerging themes are shaping current research in quantum computing and cryptography:

- **Advancements in Quantum Technologies:** Advancements in underlying quantum architecture, particularly concerning numbers of qubits and coherence times, affect the implantation of quantum-safe cryptographic operations.
- **Algorithmic Innovations:** The field of interest is the creation and enhancement of post-quantum computational techniques, which encompass lattice cryptography, code cryptography, and post-quantum cryptographic standards.
- **Policy and Regulatory Landscape:** This is evidenced by debates on international standards and accredited regulations in quantum-safe cryptography and the consensus that enhanced cybersecurity against threats posed by modern quantum computing is achievable through cooperation on the international level.

Interdisciplinary Collaboration: The growth of cooperation between quantum physicists, cryptographers, mathematicians, and members of the commercial sphere contributes to new paradigm development and real application of quantum-safe cryptographic systems.

This findings discussion section combines the insights derived from the SWOT analysis and the recent literature, ostensibly painting the contemporary picture and identifying the challenges, opportunities, and trends acutely present in quantum computing and cryptography. It defines the course of future directions for research and strategies to prepare the cybersecurity world for the quantum computing age.

V. FUTURE RESEARCH DIRECTIONS

A. Areas for Further Exploration Based on Gaps Identified in the Literature

- **Quantum-Resistant Cryptographic Algorithms:** Further investigation into improving and fine-tuning the quantum-safe cryptographic techniques is necessary. This includes delving into new mathematical solutions like multivariate cryptography, hash-based signatures, and code-based cryptography, all to enhance security against quantum invasions.
- **Implementation and Standardization:** Analyze how quantum-safe cryptographic solutions have been employed and adopted in different platforms and settings. Overcome issues concerning compatibility, performance, and integration of the system with the existing structure and policies compatible with international policies.
- **Quantum Key Distribution (QKD) Systems:** Optimize technology used in QKD systems to boost their speed, range, and capacity in creating secure links in quantum networks. Invent new specific QKD strategies, such as measurement-device-independent and continuous-variable QKD, to increase the accuracy and feasibility of implementation in practice.
- **Post-Quantum Cryptography Deployment Strategies:** Auditing the possibility of the gradual transition to using post-quantum cryptographic algorithms in industries that can be termed susceptible ones, including the financial and healthcare sectors and government agencies. Implement transition procedures and policies that have to be used when changing from the currently used cryptographic standards to the quantum-safe ones.

B. *Recommendations for Researchers and Practitioners to Address Challenges and Leverage Opportunities*

- **Collaborative Research Initiatives:** Build interprofessional relationships between quantum physicists, cryptographers, mathematicians, and other relevant players from the business world. Promote cooperation in addressing multifaceted issues and enhance the pace of creating quantum-safe cryptographies.
- **Investment in Quantum Computing Infrastructure:** The survey to increase funding and resources for constructing highly sustainable and robust quantum computers is as follows: Fund research on increasing the coherence times of qubits, develop error correcting strategies, and quantum hardware platforms for people to gain practical quantum computing.
- **Education and Awareness:** Inform the stakeholders about the possible effects of quantum computing in cybersecurity. Increase the understanding of policymakers, decision-makers in industries, and the public about the necessity for preventative measures to implement quantum-safe cryptographic standards.
- **Ethical Considerations and Governance:** Discuss potential ethical and governance concerns regarding quantum computing and essential steps in the legal and regulatory framework. Pave the way for guidelines on the appropriate use and implementation of applications involving quantum computing.

C. *Potential Methodologies and Approaches for Future Studies in Quantum-Safe Cryptography and Quantum Computing Applications*

- **Simulation and Modeling:** The best plan is to employ simulation and modeling to estimate the functioning of quantum-resistant cryptographic algorithms in various situations. Assess and compare charges, security promise, and versatility for the direction of implementations.
- **Experimental Validation:** Perform certification of quantum-safe cryptographic algorithms by testing on lab conditions. Determine their resistance against quantum attacks and analyze the possibilities of their implementation every day.
- **Quantum Network Security Testing:** Pave way for researching the techniques for penetration testing and accreditation of the security of the quantum networks, including QKD systems. Set guidelines and operation parameters to assess quantum communication schemes' performance and security resiliency.
- **Cross-Disciplinary Research Platforms:** Create cross-disciplinary quantitative platforms and experiments to encourage innovation and technological usability in quantum computing and cryptography. Facilitate information sharing between academia, industry, and government, particularly on research and innovation.

This section identifies research venues with potential for further investigation, suggests ways to address problems and shift opportunities in quantum-safe cryptography and quantum computing applications, and outlines possible methodologies for future studies. Its purpose is to inform current and future scholars and practitioners about contributing to this body of knowledge and anticipating the change those quantum technologies will bring to cybersecurity and other sectors.

VI. CONCLUSION

The SWOT analysis and the subsequent discussion on the impact of quantum computing and cryptography on business have revealed some important pointers. Another of the biggest advantages of quantum computing is its security, which is enabled by using quantum key distribution and other security systems, and its high efficiency in solving complex mathematical problems. However, a major drawback is that the current standard of cryptography can be easily braced through quantum attacks, thus requiring migration to post-quantum cryptography, which is complex and expensive. Regarding opportunities, algorithmic and protocol innovations such as quantum-resistant algorithms and protocols offer opportunities to create stronger, quantum-threat secure cryptographic systems. Also, quantum technologies include new developments in cryptography, safe communication, and defense against cyber threats. On the other hand, the possible ability to decrypt such data by future quantum computers threatens the confidentiality of now-encrypted data. Moreover, it is also seen that regulations and reluctance to transition to quantum-safe computation may still hinder preparations for the quantum computing age.

A. Implications for the Future of Cryptography in the Context of Advancing Quantum Computing Technologies

The advancement of quantum computing technologies poses profound implications for cryptography:

- **Security Paradigm Shift:** Quantum computing threatens many cryptographic standards today, most of which can be rendered useless. It becomes necessary to look at additional solutions to adapt itself to notions of quantum-computing cryptography that can be defenseless to quantum-centered hacking attempts.
- **Urgency in Adoption:** To mitigate the threat posed by present and future quantum computers, the encryption technologies that have to be developed are called quantum-safe cryptographic algorithms and protocols.
- Quantum-resistant standards must be adopted before quantum computing becomes widespread and more competitive; thus, industry players and policymakers must act.
- **Risk Management Strategies:** Organizations should incorporate risk mitigation plans for the future consequences of quantum computing on security. This includes putting money into assessments, upgrading cryptographic frameworks, and informing buyers about changes in security hazards.

As the transition toward quantum computing occurs, active preparation in cybersecurity becomes an essential step. The shift towards using quantum-safe cryptography promotes innovation in cybersecurity while, at the same time, improving the ability to counter new sophisticated threats that arise from the integration of quantum technologies. Due to the interdisciplinary nature of quantum computing applications and the multi-stakeholder environment, its implementation requires current best practices that involve agility and adaptability regarding its regulatory, ethical, and methodological facets. Also, as quantum technologies are gradually emerging, concerns about privacy, data protection, and security, especially in handling personal information, should be considered due to the introduction of quantum computing applications. Thus, it can be concluded that we need to take a rather proactive approach to decipher how quantum computing will influence cryptography. Thus, by preparing today, it is possible to protect tomorrow's digital environment from the radical changes caused by quantum technologies.

REFERENCES

1. J.-P. Aumasson, "The impact of quantum computing on cryptography," *Computer Fraud & Security*, vol. 2017, no. 6, pp. 8–11, Jun. 2017, doi: https://doi.org/10.1016/s1361-3723(17)30051-9.
2. A. Kumar and S. Garhwal, "State-of-the-Art Survey of Quantum Cryptography," Archives of Computational Methods in Engineering, Apr. 2021, doi: https://doi.org/10.1007/s11831-021-09561-2.
3. V. Bhatia and K. R. Ramkumar, "An Efficient Quantum Computing technique for cracking RSA using Shor's Algorithm," *2020 IEEE 5th International Conference on Computing Communication and Automation (ICCCA)*, Oct. 2020, doi: https://doi.org/10.1109/iccca49541.2020.9250806.
4. C. J. Mitchell, "The impact of quantum computing on real-world security: A 5G case study," *Computers & Security*, vol. 93, p. 101825, Jun. 2020, doi: https://doi.org/10.1016/j.cose.2020.101825.
5. V. Hassija *et al.*, "Present landscape of quantum computing," *IET Quantum Communication*, vol. 1, no. 2, Nov. 2020, doi: https://doi.org/10.1049/iet-qtc.2020.0027.
6. A. Nanda, D. Puthal, S. P. Mohanty, and U. Choppali, "A Computing Perspective of Quantum Cryptography [Energy and Security]," *IEEE Consumer Electronics Magazine*, vol. 7, no. 6, pp. 57–59, Nov. 2018, doi: https://doi.org/10.1109/MCE.2018.2851741.
7. R. R. Palle, "Explore the recent advancements in quantum computing, its potential impact on various industries, and the challenges it presents," *International Journal of Intelligent Automation and Computing*, vol. 1, no. 1, pp. 33–40, Jan. 2018, Available: https://research.tensorgate.org/index.php/IJIAC/article/view/101
8. R. de Wolf, "The potential impact of quantum computers on society," *Ethics and Information Technology*, vol. 19, no. 4, pp. 271–276, Sep. 2017, doi: https://doi.org/10.1007/s10676-017-9439-z.
9. B. Muruganantham, P. Shamili, S. G. Kumar, and A. Murugan, "Quantum cryptography for secured communication networks," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 1, p. 407, Feb. 2020, doi: https://doi.org/10.11591/ijece.v10i1.pp407-414.
10. "Quantum Computing And Its Impact On Space Exploration," *FasterCapital*. 2021. https://fastercapital.com/topics/quantum-computing-and-its-impact-on-space-exploration.html
11. "On quantum computing and cryptography – Quantum Bits," Apr. 23, 2018. https://www.quantum-bits.org/?p=2059
12. "Quantum Computing Shor algorithm crypto graphic IoT risk management," *SlideShare*, May 11, 2017. https://www.slideshare.net/slideshow/quantum-computing-shor-algorithm-crypto-grafic-iot-risk-management/75878308
13. "Shors Algorithm And Its Implications," 2021. *FasterCapital*. https://fastercapital.com/topics/shors-algorithm-and-its-implications.html
14. D. Alvarez and Y. Kim, "Survey of the Development of Quantum Cryptography and Its Applications," *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*, Jan. 2021, doi: https://doi.org/10.1109/ccwc51732.2021.9375995.
15. "Optimized data lake to minimize downtime and enhanced business clarity for a manufacturing company," *Yalantis*. https://yalantis.com/works/data-lake-solution-logistics/
16. J.-P. Aumasson, "The impact of quantum computing on cryptography," *Computer Fraud & Security*, vol. 2017, no. 6, pp. 8–11, Jun. 2017, doi: https://doi.org/10.1016/s1361-3723(17)30051-9.

ACRONYMS

1. **Qubit** - Quantum Bit
2. **QKD** - Quantum Key Distribution
3. **RSA** - Rivest-Shamir-Adleman (encryption algorithm)
4. **ECC** - Elliptic Curve Cryptography
5. **SWOT** - Strengths, Weaknesses, Opportunities, Threats (analysis framework)
6. **IBM** - International Business Machines Corporation
7. **NP-hard** - Nondeterministic Polynomial-time hard (complexity class)