ISSN: 2162-5751 Volume 13, Number 2, June 2023

Scientific Research Publishing

Journal of Quantum Information Science

ISSN: 2162-5751

https://www.scirp.org/journal/jqis

Journal Editorial Board

ISSN 2162-5751 (Print) ISSN 2162-576X (Online)

https://www.scirp.org/journal/jqis

Executive Editor-in-Chief

Editorial Board

Scientific Research Publishing

Journal of Quantum Information Science, 2023, 13, 33-77
https://www.scirp.org/journal/jqis
ISSN Online: 2162-576X
ISSN Print: 2162-5751

Table of Contents

Volume 13 Number 2 June 2023

Journal of Quantum Information Science (JQIS)
Journal Information

SUBSCRIPTIONS

The *Journal of Quantum Information Science* (Online at Scientific Research Publishing, https://www.scirp.org/) is published quarterly by Scientific Research Publishing, Inc., USA.

Subscription rates:
Print: $79 per issue.
To subscribe, please contact Journals Subscriptions Department, E-mail: sub@scirp.org

SERVICES

Advertisements
Advertisement Sales Department, E-mail: service@scirp.org

Reprints (minimum quantity 100 copies)
Reprints Co-ordinator, Scientific Research Publishing, Inc., USA.
E-mail: sub@scirp.org

COPYRIGHT

PRODUCTION INFORMATION

For manuscripts that have been accepted for publication, please contact:
E-mail: jqis@scirp.org

Scientific Research Publishing

Journal of Quantum Information Science, 2023, 13, 33-44
https://www.scirp.org/journal/jqis
ISSN Online: 2162-576X
ISSN Print: 2162-5751

Accelerating Quantum Computing Readiness: Risk Management and Strategies for Sectors

Abdullah Ibrahim Salman Alsalman

Executive Office, Riyadh Region Municipality, Riyadh, Saudi Arabia
Email: abdullh.70@gmail.com

How to cite this paper: Alsalman, A.I.S. (2023) Accelerating Quantum Computing Readiness: Risk Management and Strategies for Sectors. *Journal of Quantum Information Science*, **13**, 33-44.
https://doi.org/10.4236/jqis.2023.132003

Received: March 2, 2023
Accepted: June 10, 2023
Published: June 13, 2023

Abstract

The potential impact of quantum computing on various industries such as finance, healthcare, cryptography, and transportation is significant; therefore, sectors face challenges in understanding where to start because of the complex nature of this technology. Starting early to explore what is supposed to be done is crucial for providing sectors with the necessary knowledge, tools, and processes to keep pace with rapid advancements in quantum computing. This article emphasizes the importance of consultancy and governance solutions that aid sectors in preparing for the quantum computing revolution. The article begins by discussing the reasons why sectors need to be prepared for quantum computing and emphasizes the importance of proactive preparation. It illustrates this point by providing a real-world example of a partnership. Subsequently, the article mentioned the benefits of quantum computing readiness, including increased competitiveness, improved security, and structured data. In addition, this article discusses the steps that various sectors can take to achieve quantum readiness, considering the potential risks and opportunities in industries. The proposed solutions for achieving quantum computing readiness include establishing a quantum computing office, contracting with major quantum computing companies, and learning from quantum computing organizations. This article provides the detailed advantages and disadvantages of each of these steps and emphasizes the need to carefully evaluate their potential drawbacks to ensure that they align with the sector's unique needs, goals, and available resources. Finally, this article proposes various solutions and recommendations for sectors to achieve quantum-computing readiness.

Keywords

Quantum Computing, Consultancy, Governance Solutions, Quantum Readiness, Benefits of Quantum Readiness, Increased Competitiveness, Improved Security, Structured Data, Quantum Algorithms, Quantum Service

Provider, Cybersecurity, Data Management

1. Introduction

Quantum computing has the potential to change the future by solving problems that are currently impossible to solve by using classical computing. Sectors need to be proactive in their preparation for technology and explore their exponential growth if they are looking to get ahead in their field. If a sector wants to remain competitive and benefit from the opportunities presented by quantum computing, it needs to understand the risks and benefits of quantum computing, determine where it could be applied, and develop strategies to take advantage of its power. According to Mario Piattini, Guido Peterssen, and Ricardo Pérez-Castillo in their paper titled "Quantum Computing: A New Software Engineering Golden Age," they state, "We are sure that quantum computing will be the main driver for a new software engineering golden age during the present decade of the 2020s" [1]. Here is the essence of readiness, and governance solutions in quantum computing have come into play. Whether they are public or private sectors, large or small, the importance of quantum computing readiness cannot be overstated. Providing consultation with the correct knowledge, tools, and processes can ensure that they are ready to take advantage of quantum computing. This article addresses the need for quantum computing readiness and its benefits. Moreover, will also highlight the importance of risk management and provides specific recommendations for sectors to mitigate the potential risks associated with quantum computing. With the accelerating pace of quantum computing development, it is essential that sectors now act and prepare for the future.

2. Need for Quantum Computing Readiness

Quantum computing is a field that will eventually evolve in the future. Advancements in technology have changed the way businesses operate over the past decade. However, some sectors struggled to keep up with the rapid pace of change and to obtain advantages. Quantum computing is one such area that has the potential to significantly disrupt industries and markets. To avoid being left behind, it is crucial for organizations to take proactive steps to prepare for the future of quantum computing. The author of "An Environmentalist's Guide to Quantum Computing" argues that falling too far behind in technological advancements, such as AI, has clear consequences. Therefore, sectors should proactively prepare for the future of quantum computing by seeking guidance from specialized experts and investing in early adoption strategies. The goal is not just to study the risks but also to prevent them, encourage innovation, and accelerate the introduction of sustainable technologies into the marketplace, rather than hinder it (Rejeski, 2022) [2]. This suggests that organizations should not just wait and watch but should also take action to keep up with fast-paced technolo-

gical changes and innovate accordingly. In 2021, NEOM recognized the benefits and risks of quantum computing; thus, they partnered with Arqit to seek expert guidance in building the foundations of NEOM. The development of a quantum secure cognitive-city system by Arqit and NEOM is a clear example of the potential applications of quantum computing in different sectors and industries. Therefore, sectors need to have a deep understanding of quantum technology, its implications, and its potential applications in their respective industries. Despite the novelty of quantum computing and the lack of qubits, which may impede its ability to yield significant results, advances in this field are rapidly occurring and require immediate preparation. The optimal approach is to utilize scientific knowledge and adapt to changes by consulting those who specialize in quantum computing to determine potential benefits and risks. Consultants can help provide sectors with guidance regarding their preparation. For example, consultants can identify areas where quantum computing can be applied, and change the sector's strategy to avail its power and prevent the risks associated with its use. Moreover, they can create quantum-ready data management and security frameworks as well as prepare teams to work with quantum technologies. With the aid of accelerating quantum readiness for sectors, they will be confidently ready to exploit the benefits of quantum computing.

3. Benefits of Quantum Computing Readiness

Quantum computing is a revolutionary innovation that offers tremendous potential for solving complex problems with large datasets, thereby optimizing processes and boosting productivity and efficiency in various sectors. However, many companies face challenges in implementing this cutting-edge technology, owing to the intricate technicalities and lack of a skilled workforce. Seeking quantum computing readiness consultancy can help overcome these hurdles and facilitate the effective adoption of quantum technology. With the growing realization of quantum computing benefits, an increasing number of companies are likely to partner with quantum computing providers or specialists to enhance their operations. Moreover, the constantly increasing number and quality of quantum computing use cases are opening up new avenues for its widespread application in solving previously intractable challenges in diverse industries. By proactively preparing for the implementation of quantum computing technology, sectors can gain a competitive advantage and become better equipped to solve complex problems. The benefits of quantum computing readiness range from increased efficiency and productivity to the ability to tackle challenges that were previously considered unsolvable. With the help of quantum computing specialists and consultants, sectors can ensure a smooth transition to the new technology and maximize the potential advantages it offers, in the subsequent sections, an explanation for some of the benefits.

3.1. Increased Competitiveness

Preparing for quantum computing enables sectors to reach their highest level of

performance earlier or once the service is available from the quantum service provider. Sectors can make informed decisions about the future and process them to take advantage of the quantum computing benefits. Therefore, reducing the cost of services or opening new avenues will allow sectors to gain a competitive advantage. The implementation of quantum algorithms can reduce the cost of data processing by increasing efficiency or reducing the number of resources used. Staying up-to-date with the latest advancements helps sectors differentiate themselves from their competitors by discovering new innovative applications and services to leverage quantum computing or prioritize the sharing of knowledge and resources as an accredited sector.

3.2. Improved Security

Improved security is a critical aspect of sectors seeking to harness the power of cutting-edge technologies. Sectors with large amounts of data can avoid cyberattacks by having robust data management and security frameworks in place. Thus, they must ensure that the environment is secure and that the data are protected from unauthorized access. As the emergence of quantum computing also introduces significant risks, particularly to traditional cybersecurity protocols such as RSA encryption, readiness consulting by experienced readiness consultants is a way to identify the potential security risks of quantum computing. This includes conducting a thorough risk assessment of the IT infrastructure, systems, and data to identify vulnerabilities and potential threats to quantum risks. In addition, governance solutions can help sectors establish secure and compliant quantum computing environments, such as guiding data privacy, security regulations, and best practices for data management. Sectors should consider adopting post-quantum encryption standards, start planning for the adoption of quantum key distribution (QKD), and develop quantum-safe software and hardware as part of their risk management strategy. This includes developing existing policies and procedures for data protection and management as well as protocols for incident response and disaster recovery.

3.3. Structured Data

Formatting big data to be easily processed by quantum computers accelerates the benefits to take advantage of increasing efficiency, solving problems, and analyzing data. However, structuring and managing data compatible with quantum computing is complex and time-consuming. This often requires significant overhaul by sectors without the necessary expertise. Experienced in quantum computing can provide valuable guidance and support to help sectors make the transition smoothly. This can be accomplished with some key steps, such as the following:

1) Structuring the data in a manner that can be easily analyzed and processed by quantum algorithms by cleaning, formatting, and transforming it as necessary.

2) Understanding the data and identifying the parts that may be suitable for

quantum processing using statistical analysis techniques to identify trends, correlations, and other key features.

3) Quantum algorithms are used to uncover insights and relationships within data that may not be visible to traditional processing methods.

4) Evaluating the effectiveness and efficiency of quantum computing results in handling big data compared to those obtained using traditional processing methods.

4. How to Achieve Quantum Readiness

To prepare for the emergence of quantum computing, sectors should take five concrete steps, including following industry developments and screening quantum-computing use cases, understanding the significant risks and opportunities in their industries, considering partnerships or investments in quantum-computing players, recruiting in-house quantum-computing talent, and building the digital infrastructure that can meet the basic operating demands of quantum computing. These steps are essential to achieving quantum readiness, according to a report by McKinsey & Company (Biondi *et al.*, 2021) [3]. Sectors should accelerate quantum computing readiness by preparing for its emergence. The challenge is to ensure that sectors are fully prepared for quantum risks and to obtain the advantage of all available opportunities. In this regard, this article proposes several solutions for preparing a sector for quantum computing readiness by consulting for process governance. The proposed solutions ultimately lead to providing guidance for the sector to attain quantum computing readiness.

4.1. Quantum Computing Office

Sectors could establish an office specializing in quantum computing and hire an in-house team who works more closely with other departments, which offers numerous advantages:

1) Develop a strategy and solutions tailored to fulfill the sector's needs.

2) Investment in a specialized team can pay dividends in the long run.

3) Maintaining confidentiality and control over sensitive information.

4) Investing in the necessary equipment and expertise allows for better cost management.

5) Facilitating integration and collaboration within a sector.

The decision to establish an in-house team specializing in quantum computing depends on a variety of factors, including the sector's size, resources, expertise, and long-term goals. Therefore, several drawbacks must be considered.

1) High startup costs that require significant investment in infrastructure, hardware, software, and talent.

2) Difficulty in acquiring and retaining skilled professionals in the field of quantum computing due to high demand and intense competition.

3) Risk of obsolescence, which requires a long-term commitment to stay up-to-date with the latest advancements and technologies.

4) Limited access to expertise, which may be restricted to the knowledge and

experience of in-house team members.

In order to take the first step towards leveraging the potential benefits of quantum computing, it may be advisable for sectors to engage the services of a consulting company with expertise in this field. Boston Consulting Group (BCG) is an example of such a company that offers specialized consulting services related to quantum computing. While the establishment of an in-house team specializing in quantum computing can offer substantial advantages, it is essential to carefully evaluate the potential drawbacks of consulting or hiring experts. The decision to establish such a team should be based on a comprehensive analysis of the sector's unique needs, goals, and available resources.

4.2. Quantum Computing Contract

Sectors can contract with major quantum computing companies to provide access to the best-proven results and technology. Partnering with major companies accelerates the achievement of the desired results or the results agreed upon before starting work. Sectors can determine the appropriate partner based on their need. For instance, sectors that have sensitive data and want to secure it may partner with KETS, Toshiba, or Honeywell. "In July 2020 JPMorgan Chase revealed that they put Honeywell's quantum computer…that may help the financial industry secure accounts and make better investing decisions" [4]. However, sectors that want to develop urban services may collaborate with Arqit where they have previous use cases that have already been applied in NEOM. Figure 1 shows quantum market maps [5] that categorize companies based on their areas of expertise within the quantum computing market. This map did not mention all existing companies but could help sectors determine the appropriate partner for their specific needs.

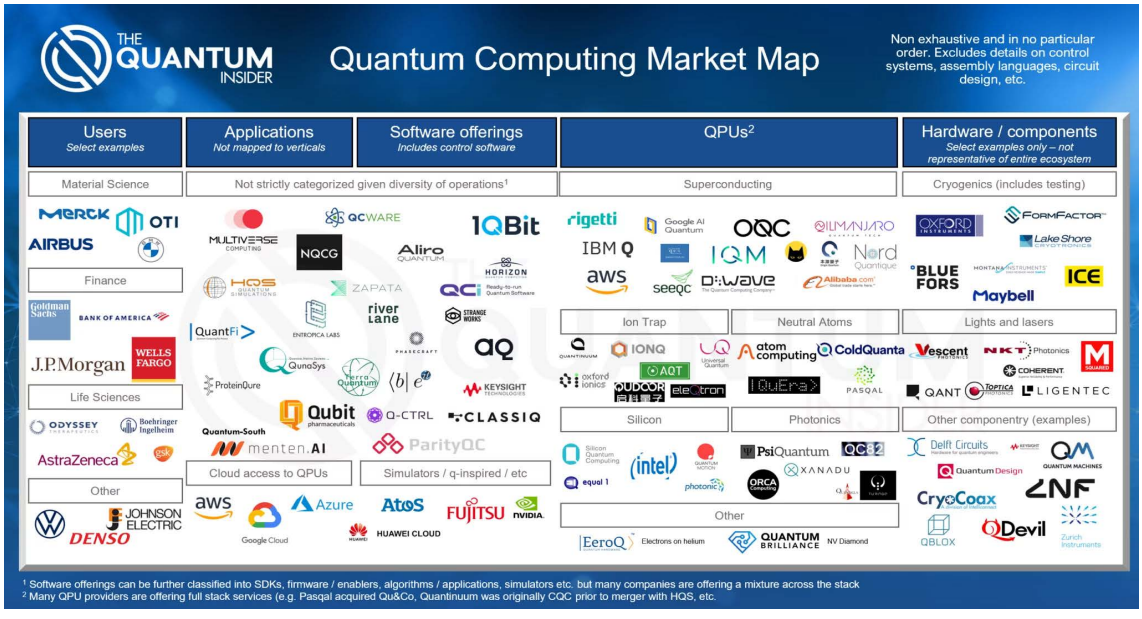


Figure 1. The map is sourced from the Quantum Insider website and was published in the article "Quantum Computing Market Map and Data 2022" by Alex Challans.

A sector may gain several advantages when it contracts with major quantum computing companies.

1) Access a technology that has already been applied to get the best-proven results.

2) Accelerating achieving the desired results by quantum companies' expertise and experience.

3) Evaluate the sector's status and assess its real requirement to focus on obtaining the best results.

The decision to contract with major quantum computing companies also depends on various factors, including the sector's size, resources, expertise, and long-term goals. Therefore, there are some potential disadvantages to contracting with major quantum computing companies.

1) The risk of sharing sensitive information with a third-party company could limit its ability to fully leverage the benefits of a partnership.

2) Dependency on that company for continued support and development without access to critical resources and expertise.

3) Limited access to intellectual property could limit the sector's ability to innovate or commercialize products and services.

In summary, partnering with major quantum computing companies can provide several benefits and potential drawbacks. Thus, the decision to contract with a major quantum computing company should be carefully evaluated to ensure that it aligns with the sector's needs, priorities, and resources.

4.3. Quantum Computing Organization

Most countries have an organization responsible for computer technology, and in recent years, many of these organizations have started to focus on quantum technology as well. Quantum computing organizations represent a strategic approach to guide the quantum computing sectors in many countries, as they provide various services that accelerate quantum development to win the global race to lead the quantum computing revolution. Governmental and nonprofit organizations within a country can guide sectors to prepare fully for quantum risks and opportunities. One effective way to achieve this is learning from quantum computing organizations. The following are a few examples of quantum computing organizations from different countries, established for various purposes:

4.3.1. National Quantum Coordination Office (United States)

The National Quantum Coordination Office (NQCO) was established in 2020 to coordinate quantum activities across departments, US government agencies, industry, and academia. Its goals include promoting collaboration, accelerating development and commercialization, and educating the public and policymakers about the potential of quantum technologies [6].

4.3.2. European Quantum Flagship (European Union)

The European Quantum Flagship is a 1 billion euro research and innovation initiative launched by the European Union in 2018. It supports research in areas

such as quantum computing, communication, simulation, and sensing, and aims to accelerate the development of quantum technologies for the benefit of society and the economy [7].

4.3.3. National Laboratory for Quantum Information Sciences (China)

The National Laboratory for Quantum Information Sciences is a $10 billion research facility established by the Chinese government in 2017 as part of its push to advance the development of quantum science and technology. This laboratory has played a significant role in China's advancements in the field, particularly in quantum communications, and has created the prototype quantum computer called Jiuzhang. In 2019, Tencent also established a Quantum Lab that aims to connect fundamental theory with practical applications in quantum information technology [8].

4.3.4. Quantum Industry Canada (QIC) (Canada)

Quantum Industry Canada (QIC) is a consortium of Canadian companies specializing in quantum technologies. Its goal is to ensure that Canadian quantum innovation and talent are translated into Canadian business success and economic prosperity. QIC members collaborate to promote Canada's quantum readiness globally, support quantum start-ups and established companies, and provide expertise in intellectual property and go-to-market strategies. The consortium works with federal and provincial governments to support the emerging quantum industry in Canada [9].

4.3.5. The Vision of Quantum Future Society (Japan)

The Vision of Quantum Future Society is a new strategy formulated by the Japanese government in April 2022 to expand on initiatives for social innovation through quantum technology. The vision aims to embed quantum technology throughout social and economic systems, creating opportunities for industrial growth, achieving a carbon-neutral society, and addressing social issues raised by the SDGs. Quantum computing is seen as an important technology for achieving these goals, and the Japanese government is accelerating research and development in this field as part of the vision [10].

4.3.6. Russian Quantum Center (Russia)

The Russian Quantum Center (RCC) is a scientific research center that focuses on the development of quantum technologies. It was established in 2012 as a collaboration between the Russian Federation's Ministry of Education and Science, the Russian Academy of Sciences, and the private investment company Rusnano. The RCC is located in the Skolkovo Innovation Center and currently has 17 scientific groups working on fundamental research in the field of quantum technologies, which include Russian and international scientists, as well as students and graduates of the RCC department at MIPT [11].

After listing a few examples of quantum computing organizations from different countries, it is important to note that many more organizations have a

connection to quantum technology. The list provided is by no means exhaustive, and there are likely more organizations in the mentioned countries as well as in other countries. Sectors interested in quantum computing should reach organizations in their respective countries to see what they can provide. These organizations established to help sectors prepare for the future and take advantage of quantum computing. As the development of quantum computing continues, more organizations are expected to emerge in the future.

5. Recommendations

As quantum computing continues to grow and develop, it is becoming necessary for the legislative authorities to intervene to unify efforts and support the country to achieve the hoped-for progress in the field of quantum computing technology. This provides a supportive environment for quantum service providers, which will help in innovation and rapid development. Moreover, working together can promote the growth and success of the quantum technology industry. By pooling their resources, knowledge, and expertise, sectors can achieve common objectives that may be difficult or impossible to achieve individually. The following two recommendations will help sectors accelerate quantum computing readiness by following the standards as a guide for full preparation.

5.1. Governmental Standardization for Quantum Computing

The first recommendation is setting standards by the government for all stakeholders in the quantum computing field. Standardization will ensure that everyone is working towards the same goals and following the same guidelines, promoting a cohesive and productive ecosystem. By establishing such standards, the government can also help mitigate risks associated with quantum computing, such as the potential for cyber threats and ethical concerns surrounding the use of sensitive information. Additionally, the adoption of these standards can help foster collaboration between sectors, and facilitate the exchange of knowledge and expertise, ultimately benefiting the quantum computing ecosystem. Standardization in the field of Quantum Computing is crucial as it allows stakeholders to unify their efforts to maximize gains. "The availability of a supply chain of such modules from different vendors will enable research teams to concentrate their research on breaking new grounds, without spending much effort on duplicating known solutions. This is where standardisation can play an important role" (van Deventer *et al.*, 2022) [12]. The establishment of standards for quantum computing by the government can lead to the achievement of quantum readiness by providing guidelines and promoting a cohesive ecosystem, mitigating potential risks, fostering collaboration between sectors, and facilitating the exchange of knowledge and expertise.

5.2. Quantum Computing Standards Organization

The second recommendation is to create an international Quantum Computing

Standards organization (QCS) that publishes standards and provides guidance and qualification for public and private sectors. Similar to ISO, B Corp SDG, etc., the organization provides sectors with a diverse group of experts and a framework for preparing for quantum technology. Experts will help the sectors apply quantum services by following the guidance and then giving them certification when a sector is qualified. The main goal is to follow the most effective approach using quantum computing technology. The existence of such an organization will provide a sense of trust and assurance for both sectors and consumers. Moreover, the QCS will encourage sectors to activate in-house quantum computing protocols and test quantum services. This will motivate quantum computing companies to develop more services owing to high demand.

Responsible Research and Innovation (RRI) aims to align research and innovation processes with societal values, needs, and expectations to ensure that the outcomes are beneficial and acceptable to society [13]. The QCS can use the RRI to direct its criteria and encourage sectors to be involved in its program. Therefore, the alignment will proactively address challenges, future uncertainties, ethical issues, and implications of a particular decision to prepare for the potential consequences of different choices.

Providing QCS certification can provide a competitive advantage among sectors by demonstrating to customers and investors that the sector is taking a proactive approach to staying ahead of the curve, reducing its risks, and taking advantage of opportunities. The following are suggested steps that a Quantum Computing Standards organization (QCS) may take to award a certification:

1) Assessing the status quo: QCS evaluates a sector's current technological capabilities, including hardware and software, to determine where quantum computing can provide value.

2) Building a strategy and framework: Based on the evaluation, the QCO provides a standard guide for developing a roadmap for building and implementing quantum computing into the sector's existing technology and business processes.

3) Implementation: The QCS supports the execution of the plan, provides consultancy, trains employees, and ensures that new technology is integrated into the existing systems.

4) Evaluation: Once the implementation is complete, the QCS evaluates the sector to determine whether it meets the standards set forth by the QCS. Thorough evaluation is essential to serve as the basis for certification. Thereafter, a sector can proudly demonstrate its readiness for a quantum era through QCS certification.

Despite the idea of establishing a QCS to provide guidance and certification for sectors that are compelling, it also has its disadvantages. One major drawback is that creating such an organization will take time, require significant financial resources, a global consensus on the standards it provides, and political support. Moreover, it may take a considerable amount of time for sectors to comply with the QCS's certification requirements, which may deter some from seeking certification. However, despite these challenges, creating a QCS will be a

significant step towards ensuring that quantum computing technology is applied effectively and safely across various sectors in different countries. The QCS can empower sectors to leverage quantum services based on their individual requirements, thereby prompting quantum computing companies to develop various quantum services in response to increasing demand.

6. Conclusion

As we continue to witness the advancement of quantum computing, sectors across various industries must take steps to prepare for this technology's impact. Quantum computing is a promising technology with the potential to transform our lives and industries. However, it also introduces significant risks, particularly to traditional cybersecurity protocols. The emergence of quantum computing threatens to render current encryption methods obsolete, putting sensitive data at risk. To address these potential risks, sectors must develop a comprehensive risk management strategy for quantum computing. This strategy should include risk assessment, planning for the adoption of post-quantum encryption standards, the adoption of quantum key distribution, the development of quantum-safe software, and the adoption of quantum-safe hardware. Conducting a thorough risk assessment is crucial to identifying potential vulnerabilities and threats to quantum risks. This process involves analyzing infrastructure, systems, and data to identify weaknesses that could be exploited by hackers. Software developers and hardware manufacturers must also start planning for the development of quantum-safe software and hardware that are resistant to quantum attacks. Sectors should start planning for the adoption of these solutions as part of their risk management strategy. Additionally, governance solutions can help sectors establish secure and compliant quantum computing environments, such as guiding data privacy, security regulations, and best practices for data management. In conclusion, sectors across various industries should be aware of the potential risks and benefits of quantum computing and take steps to prepare for its impact. By developing a comprehensive risk management strategy that includes risk assessment, planning for the adoption of post-quantum encryption standards, the adoption of QKD, the development of quantum-safe software and hardware, and adopting governance solutions, sectors can mitigate potential risks effectively and take advantage of the transformative power of quantum computing.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Piattini, M.G., Peterssen, G. and Pérez-Castillo, R. (2021) Quantum Computing. *ACM SIGSOFT Software Engineering Notes*, **45**, 12-14.

https://doi.org/10.1145/3402127.3402131

[2] Rejeski, D. (2022) An Environmentalist's Guide to Quantum Computing. Network for the Digital Economy and the Environment. Network for Digital Economy & Environment. https://www.networkdee.org/publications/an-environmentalist%E2%80%99s-guide-to-quantum-computing

[3] Biondi, M., Heid, A., Henke, N., Mohr, N., Pautasso, L., Ostojic, I., *et al.* (2021) Quantum Computing: An Emerging Ecosystem and Industry Use Cases. McKinsey & Company.

[4] GreyB Services LLP. (2021) Top 12 Quantum Computing Companies: A Comprehensive Guide. GreyB Blog. https://www.greyb.com/blog/quantum-computing-companies/#Rigetti-Computing

[5] Challans, A. (2022) Quantum Computing Market Map and Data 2022. The Quantum Insider. https://thequantuminsider.com/2022/05/09/quantum-computing-market-map-and-data-2022/

[6] National Quantum Coordination Office (n.d.) The National Quantum Coordination Office. https://www.quantum.gov/nqco/

[7] Quantum Flagship (n.d.) Introduction to the Quantum Flagship. Quantum Flagship.https://qt.eu/about-quantum-flagship/introduction-to-the-quantum-flagship/

[8] Chang, Y.-A. (2021) Quantum Wars. CKGSB Knowledge. https://english.ckgsb.edu.cn/knowledges/quantum-wars/

[9] Quantum Industry Canada (n.d.) About Quantum Industry Canada. Quantum Industry Canada. https://www.quantumindustrycanada.ca/

[10] Government of Japan (2022) Touching the Cutting Edge of Quantum Technology in the Homeland of the Superconducting Qubit. Government of Japan. https://www.japan.go.jp/kizuna/2022/05/cutting_edge_of_quantum_technology.html

[11] Tadviser (n.d.) Russian Quantum Center, Russian Quantum Center, RQC. https://tadviser.com/index.php/Company:Russian_Quantum_Center_%28RCC%2C_Russian_Quantum_Center%2C_RQC%29

[12] van Deventer, O., Spethmann, N., Loeffler, M., *et al.* (2022) Towards European Standards for Quantum Technologies. *EPJ Quantum Technology*, **9**, Article No. 33. https://doi.org/10.1140/epjqt/s40507-022-00150-1

[13] Coenen, C. and Grunwald, A. (2017). Responsible Research and Innovation (RRI) in Quantum Technology. *Ethics and Information Technology*, **19**, 277-294. https://doi.org/10.1007/s10676-017-9432-6

Scientific Research Publishing

Journal of Quantum Information Science, 2023, 13, 45-55
https://www.scirp.org/journal/jqis
ISSN Online: 2162-576X
ISSN Print: 2162-5751

Toward Constructing a Continuous Logical Operator for Error-Corrected Quantum Sensing

Cameron Cianci

Physics Department, University of Connecticut, Storrs, CT, USA
Email: cameron.cianci@uconn.edu

How to cite this paper: Cianci, C. (2023) Toward Constructing a Continuous Logical Operator for Error-Corrected Quantum Sensing. *Journal of Quantum Information Science*, **13**, 45-55.
https://doi.org/10.4236/jqis.2023.132004

Received: May 20, 2023
Accepted: June 26, 2023
Published: June 29, 2023

Abstract

Error correction has long been suggested to extend the sensitivity of quantum sensors into the Heisenberg Limit. However, operations on logical qubits are only performed through universal gate sets consisting of finite-sized gates such as Clifford + T. Although these logical gate sets allow for universal quantum computation, the finite gate sizes present a problem for quantum sensing, since in sensing protocols, such as the Ramsey measurement protocol, the signal must act continuously. The difficulty in constructing a continuous logical operator comes from the Eastin-Knill theorem, which prevents a continuous signal from being both fault-tolerant to local errors and transverse. Since error correction is needed to approach the Heisenberg Limit in a noisy environment, it is important to explore how to construct fault-tolerant continuous operators. In this paper, a protocol to design continuous logical z-rotations is proposed and applied to the Steane Code. The fault tolerance of the designed operator is investigated using the Knill-Laflamme conditions. The Knill-Laflamme conditions indicate that the diagonal unitary operator constructed cannot be fault tolerant solely due to the possibilities of X errors on the middle qubit. The approach demonstrated throughout this paper may, however, find success in codes with more qubits such as the Shor code, distance 3 surface code, [15, 1, 3] code, or codes with a larger distance such as the [11, 1, 5] code.

Keywords

Quantum Sensing, Quantum Error Correction, Steane Code, Heisenberg Limit

1. Introduction

Quantum sensors have found utility in a variety of fields including commercial applications such as geoscience, mining, and various sensors in industry [1] [2].

There have been many recent studies examining the potential utility of error correction to improve the sensitivity of quantum sensors in noisy environments [3]-[9]. Error correction in quantum sensors promise to surpass the Standard Quantum Limit, where sensitivity scales as $\frac{1}{\sqrt{t}}$, and instead approach the Heisenberg Limit, scaling as $\frac{1}{t}$ where t is time [3]. This scaling is the best allowed by the laws of quantum mechanics.

Current studies into quantum error-corrected sensors propose codes which can correct the most prevalent type of noise in a system but are still vulnerable to other local errors [10]. For an example, [7] utilized a code to correct relaxation in a quantum magnetometer, but the sensor designed is still vulnerable to single qubit phase errors. Although the paper proposes mitigating these phase errors by leveraging dynamical decoupling [11] [12], the designed sensor will realistically still accumulate uncorrected errors over time from random environmental fluctuations in the magnetic field. Therefore, this design will be reduced to the Standard Quantum Limit on time scales dictated by the strength of this environmental noise [3] [13]. This can be addressed by using stronger error-correcting codes such as a distance 3 code, which has the ability to correct single qubit errors. However, codes of distance 3 and above have yet to be used in quantum error-corrected sensors due to the difficulty of constructing a continuous logical operator in these codes. The protocol put forth in this paper begins to address this problem by designing potential logical operators which may be constructed through diagonal commuting gates.

To start, let us consider a common quantum sensing protocol, the Ramsey measurement protocol described below [14].

1) A sensor qubit begins in the state $|0\rangle$.

2) A Hadamard gate is applied bringing the state to, $H|0\rangle = |+\rangle$.

3) The signal is applied to the qubit, giving it a signal dependent phase,

$$P_L(\phi)|+\rangle = P_L(\phi)\times\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right) = \frac{1}{\sqrt{2}}\left(|0\rangle+\mathrm{e}^{i\phi}|1\rangle\right).$$

4) A Hadamard gate is applied again, bringing the state to

$$H\frac{1}{\sqrt{2}}\left(|0\rangle+\mathrm{e}^{i\phi}|1\rangle\right) = \frac{1+\mathrm{e}^{i\phi}}{2}|0\rangle+\frac{1-\mathrm{e}^{i\phi}}{2}|1\rangle.$$

5) Measuring in the z-basis, the probability of obtaining $|1\rangle$ is $\left|\frac{1-\mathrm{e}^{i\phi}}{2}\right|^2$, from which ϕ can be inferred.

The continuous phase gate $P_L(\phi)$ is the signal and acts on the computational basis states as,

$$P_L(\phi) = \begin{bmatrix} 1 & 0 \\ 0 & \mathrm{e}^{i\phi} \end{bmatrix} \tag{1}$$

The Ramsey measurement protocol requires that there is a continuous symmetry around the z-axis of the qubit for $P_L(\phi)$ to be fault tolerantly applied.

As logical gate sets do not typically include any continuous gates, it is not straightforward to apply this protocol directly to an error-corrected logical qubit of distance 3 or larger. Instead, current error-corrected sensing protocols use codes with smaller distances, leaving the logical qubit vulnerable to certain local errors. For example, these sensors often employ codes such as the bit flip or amplitude damping codes [7] [8] [9]. This design choice ultimately allows for transverse operators to generate the signal, for example, magnetic fields in flux tunable superconducting qubits [7].

The reason for this difficulty in designing error-corrected quantum sensors fault tolerant to single qubit errors comes from the Eastin-Knill theorem. This theorem states that no quantum error-correcting code that can correct local errors can also have a continuous symmetry which acts transversely on the qubits [10]. This is proven by demonstrating that the set of fault tolerant gates on any local error-correcting code is finite and cannot have any continuous symmetries as a continuous symmetry would imply an infinite number of fault tolerant gates. Since a continuous symmetry is required in many sensing protocols such as Ramsey measurement shown above, the Eastin-Knill theorem complicates the design of error-corrected quantum sensors. This is the reason why current error-corrected quantum sensors leave a degree of freedom uncorrected and therefore preserve a continuous symmetry for the signal. However, as was proven in [3], the presence of any noise along this symmetry will make these sensors revert to the Standard Quantum Limit as they will no longer satisfy the HNLS criterion.

The Eastin-Knill theorem uncovers an interesting question in quantum sensing, is it possible to realize continuous logical operators for error-corrected sensing on a logical qubit? Therefore, in Sections 3 and 4 we will construct a non-transverse logical phase operator, $P_L(\phi)$, acting on the logical subspace for the purpose of creating quantum error-corrected sensors. The difficulty constructing this operator is likely what has prevented prior exploration into correcting arbitrary local errors in quantum sensors.

2. Arbitrary Diagonal Unitary Gate

One problem in creating a fault tolerant phase operator is that errors may occur between the gates constructing this operator. This would increase the number of possible errors, requiring a larger code which can recognize these new error syndromes. To circumvent this problem, we will consider diagonal unitary operators and demonstrate that they can be built from commuting gates which could be applied simultaneously. Additionally, restricting the operator to be diagonal greatly reduces its complexity from $(2^n)^2$ to 2^n degrees of freedom. We will also find the requirements for a creating logical phase gate are simpler when restricted to a diagonal unitary.

This operator can be constructed from a single qubit z-axis rotation gate, $R_Z(\phi)$, controlled by n qubits where $n \in \{0,1,\cdots,N\}$ with the total number of

qubits N (ex. $R_{Z_1}(\phi)$, $C_1R_{Z_2}(\phi)$, $C_1C_3R_{Z_4}(\phi)\ldots$). As these controlled-phase gates are all diagonal and therefore commute, it may be possible to realize them simultaneously and prevent errors from occurring between these gates. Whether these multi-qubit gates can be created in superconducting quantum circuits is a topic for future investigation, and we will focus only on constructing the logical operators.

Alternatively, other ways to efficiently create diagonal unitaries have been previously explored [15]. However, these diagonal unitaries are built from non-commuting single and two-qubit gates, increasing the number of distinct errors which can occur.

Next, we will programmatically construct an arbitrary diagonal unitary operator from controlled-phase gates. We begin by noting that, for any given N, there are 2^N degrees of freedom in a diagonal unitary, and 2^N-1 different controlled-phase gates. We will eliminate the first diagonal entry through the application of a global phase, without any loss of generality.

We can now construct an arbitrary diagonal unitary operator through the following protocol.

1) Initialize an array to the Identity, in which we will store the constructed operator, $U_C = \mathbb{1}$.

2) Let the index i loop through each diagonal entry of the desired operator U_d.

a) Convert the current index i into binary. This binary representation shows the basis state on which this entry will act (ex. $i=9 \Rightarrow |1001\rangle$).

b) Apply a $R_Z(\phi)$ gate to one of the qubits in a $|1\rangle$ state, which is controlled by all other qubits in a $|1\rangle$ state. This gate is given a value such that, when applied to the constructed operator, the current diagonal element will obtain the desired phase, $\left(CC\cdots R_Z(\phi)\times U_C\right)[i][i] = U_d[i][i]$.

c) Update the constructed operator with this new gate. $U_C' = CC\cdots R_Z(a)\times U_C$.

3) Return the constructed operator U_C, and the phases applied at each index.

This protocol will construct any desired diagonal unitary from commuting controlled-phase gates, as the list of applied phases at each index can be used to determine the gates applied. The correctness of this protocol can be proven through induction, as each gate affects only the current and later diagonal entries in the constructed operator. Each diagonal entry has a unique operator which can tune its phase without affecting previously considered entries, except for the first entry which can be removed through an application of a global phase. This unique operator is found by applying a phase gate controlled by the binary representation of the state corresponding to the index of the entry. Therefore, we can simply construct the desired operator by making greedy decisions at each entry. Now that the construction of diagonal unitary operators from commuting gates has been stated, we will put forward a simple example to clarify.

Constructing a Simple Diagonal Unitary Operator

Here is an example of this protocol used to construct the following desired uni-

tary U_d,

$$\begin{matrix} |00\rangle & |01\rangle & |10\rangle & |11\rangle \end{matrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & e^{i\phi} & 0 & 0 \\ 0 & 0 & e^{i2\phi} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

First we loop through each diagonal entry. For each entry, the value can be changed by the phase gate controlled by the values of $|1\rangle$ in the binary representation of the index.

$$U_d|01\rangle = e^{i\phi}|01\rangle \Rightarrow R_{Z_1}(\phi) \tag{2}$$

which in turn gives our constructed operator (previously initialized to $\mathbb{1}$) as,

$$U_C = R_{Z_1}(\phi) \times \mathbb{1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & e^{i\phi} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\phi} \end{pmatrix} \tag{3}$$

Next we find,

$$U_d|10\rangle = e^{i2\phi}|10\rangle \Rightarrow R_{Z_2}(2\phi) \tag{4}$$

This makes our constructed operator,

$$U_C = R_{Z_1}(\phi) \times R_{Z_2}(2\phi) \times \mathbb{1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & e^{i\phi} & 0 & 0 \\ 0 & 0 & e^{i2\phi} & 0 \\ 0 & 0 & 0 & e^{i3\phi} \end{pmatrix} \tag{5}$$

Lastly, viewing the final entry,

$$U_d|11\rangle = |11\rangle \tag{6}$$

Currently, our constructed operator gives the value,

$$U_C|11\rangle = e^{i3\phi}|11\rangle \tag{7}$$

This indicates that we must apply $C_1R_{Z_2}(-3\phi)$, giving us the final operator,

$$U_C = R_{Z_1}(\phi) \times R_{Z_2}(2\phi) \times C_1R_{Z_2}(-3\phi) \times \mathbb{1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & e^{i\phi} & 0 & 0 \\ 0 & 0 & e^{i2\phi} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{8}$$

Which is exactly the desired operator, decomposed into two phase gates and one controlled-phase gate. As was discussed previously, these gates commute and could therefore be applied simultaneously to prevent errors from occurring between them.

3. Creating a Logical Phase Gate

Next we want to create a logical phase gate from a diagonal operator. To start,

we must consider the code words of the chosen code on which we will be acting. Since our operator must function as a logical z-rotation gate, it must satisfy the two conditions,

$$P_L(\phi)|0\rangle_L = |0\rangle_L \tag{9}$$

$$P_L(\phi)|1\rangle_L = \mathrm{e}^{i\phi}|1\rangle_L \tag{10}$$

These constraints are straightforward when applied to a diagonal operator, as we simply must ensure that all diagonal elements which are multiplied by the non-zero basis states in $|1\rangle_L$ have a value of $\mathrm{e}^{i\phi}$ while all diagonal elements which are multiplied by the nonzero basis states in $|0\rangle_L$ have a value of $|1\rangle$.

For an example, if the logical eigenstates of a desired code were,

$$|0\rangle_L = |000\rangle + |001\rangle + |000\rangle + |100\rangle = [1 \quad 1 \quad 1 \quad 0 \quad 1 \quad 0 \quad 0 \quad 0]$$

$$|1\rangle_L = |101\rangle + |110\rangle + |101\rangle + |011\rangle = [0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 1 \quad 1 \quad 1]$$

These code words would restrict our diagonal logical phase operator to

$$P_L(\phi) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathrm{e}^{i\phi} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \mathrm{e}^{i\phi} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \mathrm{e}^{i\phi} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathrm{e}^{i\phi} \end{pmatrix}$$

as this diagonal unitary uniquely results in,

$$P_L(\phi)|0\rangle_L = |0\rangle_L \tag{11}$$

$$P_L(\phi)|1\rangle_L = \mathrm{e}^{i\phi}|1\rangle_L \tag{12}$$

Through application of the protocol from Section 2, we find this operator can be realized by the simultaneous application of the gates $C_1R_{Z_2}(\phi)$, $C_1R_{Z_3}(\phi)$, $C_2R_{Z_3}(\phi)$, and $C_1C_2R_{Z_3}(-2\phi)$.

Ambiguous Entries

In most codes, however, code words do not include a superposition of every basis state. This leaves ambiguous or unconstrained degrees of freedom in the constructed operator. For an example, consider a code with the code words $|0\rangle_L = |00\rangle$ and $|1\rangle_L = |11\rangle$. This leaves an ambiguous logical phase operator,

$$P_L(\phi) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & a & 0 & 0 \\ 0 & 0 & b & 0 \\ 0 & 0 & 0 & \mathrm{e}^{i\phi} \end{pmatrix} \tag{13}$$

We can therefore tune these variables *a* and *b* as needed. For another more applicable example, the Steane code logical states include a superposition of 8

states out of 128 basis states.

$$|0\rangle_L = \frac{1}{\sqrt{8}}\big(|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle + |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle\big) \tag{14}$$

This logical code word restricts only 8 of the 128 diagonal values of the logical operator. The $|1\rangle_L$ state similarly restricts 8 more leaving 112 tunable values. In the next section, we will consider constraining these values in the Steane code in an attempt to make our logical phase operator fault tolerant through satisfying the Knill-Laflamme conditions.

4. The Fault Tolerance of Designed Logical Phase Gates

Now that we can construct a diagonal logical phase operator for any error-correcting code given its logical code words, we may now test if the constructed logical operator is fault tolerant. This can be done by satisfying the Knill-Laflamme conditions, which are both sufficient and necessary for error correction [16].

The Knill-Laflamme conditions for a code with code words W_σ fault tolerant to errors $K_i = \{K_1, K_2, \cdots, K_n\}$ is,

$$\langle W_\sigma | K_l^\dagger K_k | W_{\sigma'} \rangle = \alpha_{lk}\delta_{\sigma\sigma'} \tag{15}$$

The coefficients α_{lk} must have no dependence on σ or σ'. When considering local errors, the Kraus Operators K_i are the single qubit Pauli gates $K_i \in \{X_i, Y_i, Z_i, \mathcal{I}\}$.

Assuming we want to make our logical phase operator fault tolerant, we need to expand the Kraus operators such that we account for errors taking place both before and after the application of the logical operator. Since we can construct this operator from simultaneously applied commuting gates as shown in Section 2, we will not consider errors occurring between gates constructing the logical operator.

With $P_L(\phi)$ as a logical operator, we need to expand the Knill-Laflamme conditions to the following four equations.

$$\langle W_\sigma | P_L^\dagger(\phi) K_l^\dagger K_k P_L(\phi) | W_{\sigma'} \rangle = \alpha_{lk}\delta_{\sigma\sigma'} \tag{16}$$

$$\langle W_\sigma | K_l^\dagger P_L^\dagger(\phi) K_k P_L(\phi) | W_{\sigma'} \rangle = \beta_{lk}\delta_{\sigma\sigma'} \tag{17}$$

$$\langle W_\sigma | P_L^\dagger(\phi) K_l^\dagger P_L(\phi) K_k | W_{\sigma'} \rangle = \beta_{lk}\delta_{\sigma\sigma'} \tag{18}$$

$$\langle W_\sigma | K_l^\dagger P_L^\dagger(\phi) P_L(\phi) K_k | W_{\sigma'} \rangle = \gamma_{lk}\delta_{\sigma\sigma'} \tag{19}$$

A logical phase gate which satisfies these conditions will additionally be fault tolerant to single qubit errors. The error detection and correction operators can then be derived from the Knill-Laflamme equations [16].

We must now return our attention to the tunable elements of the logical phase unitary noted in Section 3.1. We will attempt to satisfy the Knill-Laflamme conditions shown in Equations (16)-(19) by using these values.

Consider the simple example explored in section 3.1 with code words $|0\rangle_L = |00\rangle$ and $|1\rangle_L = |11\rangle$, in the presence of X_1 errors, $K_i = \{X_1\}$. Equations (16)-(19) require $a = 1$ and $b = e^{i\phi}$, making the following logical phase gate tolerant to these X_1 errors,

$$P_L(\phi) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\phi} & 0 \\ 0 & 0 & 0 & e^{i\phi} \end{pmatrix} \tag{20}$$

As can be seen by applying the protocol from section 2, this is simply a z-axis rotation gate on the second qubit $R_{Z_2}(\phi)$. Now we will attempt to apply this approach to a more powerful error-correcting code, the Steane Code.

5. Results in the Steane Code

The Steane Code is one of the simplest and most well-studied error-correcting codes of distance 3, meaning it can correct any single local error [17]. Since this code can correct local errors, the Eastin-Knill theorem requires the signal to be non-transverse. However, the approach designed in Sections 2, 3, and 4 is not restricted to transverse operators, and therefore is not forbidden from creating a fault tolerant continuous operator. We will now apply our process for making logical phase gates to the Steane Code.

Using the code words of the Steane code (shown below), we restrict the corresponding diagonal elements of our operator as shown in Section 3.

$$\begin{aligned} |0\rangle_L = \frac{1}{\sqrt{8}}\big(&|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle \\ &+ |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle\big) \end{aligned} \tag{21}$$

$$\begin{aligned} |1\rangle_L = \frac{1}{\sqrt{8}}\big(&|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle \\ &+ |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle\big) \end{aligned} \tag{22}$$

The diagonal elements of the desired logical operator U_d must behave as,

$$U_d|0\rangle_L = |0\rangle_L \tag{23}$$

$$U_d|1\rangle_L = e^{i\phi}|1\rangle_L \tag{24}$$

This leaves 112 unconstrained degrees of freedom in the logical phase operator. However, when applying the Knill-Laflamme conditions as shown in Section 4, it is found that the following condition is unsatisfiable.

$$\langle W_0|X_4P_L^\dagger(\phi)X_4P_L(\phi)|W_0\rangle = \langle W_1|X_4P_L^\dagger(\phi)X_4P_L(\phi)|W_1\rangle \tag{25}$$

This can be interpreted as an error on the middle qubit of the Steane code before $P_L(\phi)$, which is indistinguishable from an error after the application of $P_L(\phi)$ when restricting $P_L(\phi)$ to be diagonal.

More precisely, the value of β in $\langle W_\sigma|X_4P_L^\dagger(\phi)X_4P_L(\phi)|W_{\sigma'}\rangle = \beta\delta_{\sigma\sigma'}$ changes sign based on the value of σ and σ'. This indicates that an X_4 error

before $P_L(\phi)$ changes the state differently than an X_4 error after $P_L(\phi)$, but both errors are recognized by the same error syndromes and are indistinguishable. Therefore, this approach unfortunately does not succeed in creating a logical phase operator in the Steane code.

6. Conclusions and Future Directions

In this paper a protocol for designing fault tolerant continuous logical operators from diagonal unitary gates is proposed and tested. This protocol greatly reduces the complexity of the potential fault tolerant operator by restricting it to be a diagonal unitary, reducing its degrees of freedom from $\left(2^N\right)^2$ to 2^N. This restriction also has the added benefit that the designed operator may be constructed from simultaneous application of commuting diagonal gates, and therefore errors between gates constructing the logical operator can be disregarded.

Current error-corrected quantum sensor designs are limited to codes of distance less than 3 due to the Eastin-Knill theorem. The protocol introduced here may be able to overcome this limitation as the designed operator is non-transverse. Although this protocol is unable to create a fault tolerant operator in the Steane code due to X errors on the middle qubit of the code, this protocol may be able to design Heisenberg limited quantum sensors when applied to larger codes, or codes with a larger distance. Additionally, a continuous logical operator may have other benefits, such as a logarithmic speedup in fault tolerant quantum computation.

The [11, 1, 5] code is typically tolerant to two qubit errors and may still be tolerant to a single local error when designing a continuous logical operator. Due to the increased code distance, it is possible that even if an error propagates through the multi-qubit gates of the logical operator, the larger distance of this code may still be able to correct these errors.

Additionally, the Shor Code and the distance 3 surface code [18] [19] have a higher qubit count, which may be able to accommodate more error syndromes and correct more errors than the Steane code. Therefore, diagonal operators in these codes may still be fault tolerant.

Also, as the Solovay-Kitaev theorem allows for universal computation to be achieved from Clifford + T gates in $O\left(m\log^c\left(m/\varepsilon\right)\right)$ [20], a logarithmic speedup may be possible using a continuous operator instead of the T gate. However, a logarithmic speedup is not often significant compared to the quadratic or exponential speedups commonly provided by quantum algorithms.

One of the most interesting outcomes may be that it is impossible to construct a fault tolerant continuous logical operator in error-correcting codes that can be decomposed into physically realizable gates. If this is the case, it would potentially indicate the presence of new and interesting theorems for error correction and quantum sensing.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Foley, C. (2014) SQUID Use for Geophysics: Finding Billions of Dollars in APS March Meeting Abstracts 2014 (Mar.), F23.004.

[2] De Luna, F.D., da Silva, A.G. and dos Santos Vianna Junior, A. (2020) The Influence of Geometry on the Fluid Dynamics of Continuous Settler. *Open Journal of Fluid Dynamics*, **10**, 164-183. https://doi.org/10.4236/ojfd.2020.103011

[3] Zhou, S., *et al.* (2019) Error-Corrected Quantum Sensing. *Optical, Opto-Atomic, and Entanglement-Enhanced Precision Metrology*, Vol. 10934, 109341J.

[4] Kessler, E.M., Lovchinsky, I., Sushkov, A.O. and Lukin, M.D. (2014) Quantum Error Correction for Metrology. *Physical Review Letters*, **112**, Article ID: 150802. https://doi.org/10.1103/PhysRevLett.112.150802

[5] Shettell, N., Munro, W.J., Markham, D. and Nemoto, K. (2021) Practical Limits of error Correction for Quantum Metrology. *New Journal of Physics*, **23**, Article ID: 043038. https://doi.org/10.1088/1367-2630/abf533

[6] Rojkov, I., Layden, D., Cappellaro, P., Home, J. and Reiter, F. (2022) Bias in Error-Corrected Quantum Sensing. *Physical Review Letters*, **128**, Article ID: 140503. https://doi.org/10.1103/PhysRevLett.128.140503

[7] Herrera-Marti, D.A., Gefen, T., Aharonov, D., Katz, N. and Retzker, A. (2015) Quantum Error-Correction-Enhanced Magnetometer Overcoming the Limit Imposed by Relaxation. *Physical Review Letters*, **115**, Article ID: 200501. https://doi.org/10.1103/PhysRevLett.115.200501

[8] Matsuzaki, Y. and Benjamin, S. (2017) Magnetic-Field Sensing with Quantum Error Detection under the Effect of Energy Relaxation. *Physical Review A*, **95**, Article ID: 032303. https://doi.org/10.1103/PhysRevA.95.032303

[9] Reiter, F., Sorensen, A.S., Zoller, P. and Muschik, C.A. (2017) Dissipative Quantum Error Correction and Application to Quantum Sensing with Trapped Ions. *Nature Communications*, **8**, Article No. 1822. https://doi.org/10.1038/s41467-017-01895-5

[10] Eastin, B. and Knill, E. (2009) Restrictions on Transversal Encoded Quantum Gate Sets. *Physical Review Letters*, **102**, Article ID: 110502. https://doi.org/10.1103/PhysRevLett.102.110502

[11] Viola, L., Lloyd, S. and Knill, E. (1999) Universal Control of Decoupled Quantum Systems. *Physical Review Letters*, **83**, 4888-4891. https://doi.org/10.1103/PhysRevLett.83.4888

[12] Bylander, J., *et al.* (2011) Noise Spectroscopy through Dynamical Decoupling with a Superconducting Flux Qubit. *Nature Physics*, **7**, 565-570. https://doi.org/10.1038/nphys1994

[13] Wang, S. (2022) Does Design Thinking Run Counter to Design? *Art and Design Review*, **10**, 41-46. https://doi.org/10.4236/adr.2022.101004

[14] Degen, C., Reinhard, F. and Cappellaro, P. (2017) Quantum Sensing. *Reviews of Modern Physics*, **89**, Article ID: 035002. https://doi.org/10.1103/RevModPhys.89.035002

[15] Welch, J., Greenbaum, D., Mostame, S. and Aspuru-Guzik, A. (2014) Efficient Quantum Circuits for Diagonal Unitaries without Ancillas. *New Journal of Physics*, **16**, Article ID: 033040. https://doi.org/10.1088/1367-2630/16/3/033040

[16] Girvin, S.M. (2023) Introduction to Quantum Error Correction and Fault Tolerance. https://doi.org/10.21468/SciPostPhysLectNotes.70

[17] (1996) Multiple-Particle Interference and Quantum Error Correction. *Proceedings*

of the Royal Society of London. Series A: *Mathematical*, *Physical and Engineering Sciences*, **452**, 2551-2577. https://doi.org/10.1098/rspa.1996.0136

[18] Fowler, A.G., Mariantoni, M., Martinis, J.M. and Cleland, A.N. (2012) Surface Codes: Towards Practical Large-Scale Quantum Computation. *Physical Review A*, **86**, Article ID: 032324. https://doi.org/10.1103/PhysRevA.86.032324

[19] Krinner, S., *et al*. (2022) Realizing Repeated Quantum Error Correction in a Distance-Three Surface Code. *Nature*, **605**, 669-674. https://doi.org/10.1038/s41586-022-04566-8

[20] Nielsen, M.A. and Chuang, I.L. (2000) Quantum Computation and Quantum Information. Cambridge University Press, Cambridge.

Scientific Research Publishing

Journal of Quantum Information Science, 2023, 13, 56-77
https://www.scirp.org/journal/jqis
ISSN Online: 2162-576X
ISSN Print: 2162-5751

Navigating the Quantum Threat Landscape: Addressing Classical Cybersecurity Challenges

Sabina Sokol

Girls in Quantum, CA, USA
Email: sabinaeinatsokol@gmail.com

How to cite this paper: Sokol, S. (2023) Navigating the Quantum Threat Landscape: Addressing Classical Cybersecurity Challenges. *Journal of Quantum Information Science*, **13**, 56-77.
https://doi.org/10.4236/jqis.2023.132005

Received: May 20, 2023
Accepted: June 27, 2023
Published: June 30, 2023

Abstract

This research paper analyzes the urgent topic of quantum cybersecurity and the current federal quantum-cyber landscape. Quantum-safe implementations within existing and future Internet of Things infrastructure are discussed, along with quantum vulnerabilities in public key infrastructure and symmetric cryptographic algorithms. Other relevant non-encryption-specific areas within cybersecurity are similarly raised. The evolution and expansion of cyberwarfare as well as new developments in cyber defense beyond post-quantum cryptography and quantum key distribution are subsequently explored, with an emphasis on public and private sector awareness and vigilance in maintaining strong security posture.

Keywords

Quantum Computing, Post-Quantum Cryptography (PQC), Quantum Hacking, Cybersecurity, Internet of Things (IoT), Shor's Algorithm, Quantum Random Number Generators (QRNGs), Pseudorandom Number Generators (RNGs), Quantum Key Distribution (QKD), Symmetric Key Cryptography, Asymmetric Key Cryptography

1. Introduction

Since the moment Peter Shor first proposed his famous algorithm in 1994—which has been mathematically proven to break some modern cryptographic standards—the international community has raced to build the first cryptanalytically relevant quantum computer (CRQC) that can apply it. The recent surge of new quantum companies and research groups has raised the prospect of developing such a technology closer, with experts predicting that a CRQC will be available—though likely not commercially—in the next five to seven years [1].

Asymmetric cryptographic algorithms—those that use a combination of pub-

lic and private keys to encrypt data, such as Rivest-Shamir-Adleman (RSA), Elliptic Curve Cryptography (ECC), and Diffie-Hellman—will be highly vulnerable to attacks by these devices. These schemas are designed around difficult mathematical problems—such as large prime number factorization—for which there are no efficient classical algorithmic solutions. Moreover, the principle of "Harvest Now, Decrypt Later"—the phenomenon of stealing encrypted, highly confidential data with the intent of later decrypting it with a CRQC—asserts that it ultimately does not matter when such a technology will be developed because the information possessed by adversaries—such as personal health records—will still be socially, politically, or economically damaging. Therefore, it is critical that the public and private sectors migrate towards post-quantum cryptography (PQC)—a class of CRQC-resistant algorithms designed to be implemented on classical computers—as soon as possible. The process of transitioning to these new standards will take many years depending on the size and complexity of the agency. As a result, industry experts and government officials urge starting the process now to protect sensitive data. Regulators in several western countries have released requirements or recommendations urging organizations to commence the migration process immediately. However, PQC migration should not be the only area of concern regarding the threat quantum poses to national and international security. One should go beyond current corporate trends and media hysteria to understand the rest of the picture. Doing so will reveal the vast landscape of largely unaddressed concerns within the quantum cybersecurity space, all of which may have a significant impact on digital privacy and integrity in the near future.

2. The Current Federal Quantum/Cyber Landscape

In October 2020, the National Security Agency (NSA) released a statement giving a high-level overview of quantum key distribution (QKD)—quantum-secure communication protocols that harness properties of quantum mechanics to ensure the confidentiality and integrity of data being transmitted—and quantum cryptography. It outlined the limitations of the former technology, namely the incredibly high cost of implementation [2]. The agency declared that it will not support QKD's usage for national security systems (NSS) and will not invest in certifying QKD products in the near future [2].

In March 2021, the Cybersecurity and Infrastructure Security Agency (CISA) released a statement outlining the four main areas of focus for cyber resiliency and defense, which include transportation systems, election security, critical supply chains, and ransomware protections [1]. The agency emphasized that cyber attacks are inevitable, referencing the major data breach at the federal level in 2019-2020: a state-sponsored group compromised several hundred organizations worldwide, both in the public and private sectors, exposing millions of customers' personal information. CISA also instructed federal agencies to inventory all cryptologic systems, infrastructure, security standards, and critical

data that will need to be updated once the official post-quantum cryptographic standards are released by the National Institute of Standards and Technology (NIST) [1]. Additionally, the statement emphasized the much-needed focus on Diversity, Equity, Inclusion, and Accessibility (DEIA) in the cyber workforce, foreshadowing the Department of Defense's (DoD) release of the 2023-2027 Cyber Workforce Strategy two years later.

In May 2022, the White House released a national security memorandum outlining the threat of CRQCs to military and civilian infrastructure [3]. It called for further quantum information science (QIS) education, research, and workforce development. It also stated that all corporations and agencies working in the field of quantum should establish a liaison with the Office of Science and Technology Policy (OSTP) by August 2022 to begin the transition to quantum-resistant cryptography immediately [3]. NIST announced the establishment of a working group for NSS owners to ensure all further guidance on PQC meets industry needs. The agency also mandated that all Federal Civilian Executive Branch (FCEB) agencies should report on all systems that are vulnerable to CRQCs to CISA by May 2023; funding for the migration to PQC will be evaluated accordingly. On the same note, NSA, NIST, and other security agencies confirmed the release of official PQC migration guidelines to NSS customers by May 2023 as well [3].

In June 2022, NIST announced the first four quantum-resistant algorithms: CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, and SPHINCS+ [4].

In August 2022, CISA released guidelines for PQC preparation and migration primarily for NSS customers [5]. However, it recommended that all organizations with critical infrastructure follow the PQC roadmap, which highlights everything discussed in the March 2021 statement. The agency also emphasized that quantum computing poses a substantial threat to 55 national critical functions (NCFs) [5].

In September 2022, as an extension of the national security memorandum released in May 2022, the NSA announced that NSS customers are to start migrating towards approved quantum-resistant algorithms—CRYSTALS-Kyber and CRYSTALS-Dilithium—immediately [6]. The agency expects to fully use these algorithms by 2035. However, it is requiring all NSS services, equipment, and operating systems to initially support CSNA 2.0 by 2025-2030, and shift to exclusive use of CSNA 2.0 by 2030-2033 [6]. This means that any NSS systems that use the CSNA 1.0 algorithms should either be removed or brought up to compliance. Currently, SHA-384, SHA-512, and AES-256 still stand as symmetric cryptographic algorithms—those that use a single encryption key for two-party exchanges—for CSNA 2.0. The NSA also declared that it should approve any and all deviations from complete CSNA 2.0 implementation for NSS systems [6].

In November of 2022, the White House sent out its own extension to the May memorandum directed for non-NSS. The Office of Management and Budget (OMB) called for agencies to inventory all information systems and technologies

that are vulnerable to CRQC-based attacks, starting with those that handle the most sensitive information [7]. The memorandum also required all agencies to designate someone to head this PQC migration initiative. OMB's statement assured FCEBs that CISA and the NSA will provide more guidance on next steps in the PQC process by February 2023, including guidance for PQC testing [7]. Lastly, the memo announced the establishment of another working group—headed by OMB—for agency representatives that deal with non-NSS.

In December 2022, NIST held its 4th PQC standardization conference, during which the finalists—Classic McEliece, BIKE, HQC, and SIKE—were presented [8]. The organization also declared that it is planning to standardize the Round 3 finalists: CRYSTALS-Kyber, CRYSTALS-Dilithium, SPHINCS+, and FALCON [8]. It also announced that the first official PQC standards will be published in early 2024, but called for new submissions for non-lattice-based digital signature schemes—methods of ensuring a message's authenticity and integrity—by June 2023. The National Cybersecurity Center of Excellence (NCCoE) underscored the fact that most organizations lack a firm understanding of the cryptographic standards currently employed in their information technology (IT), stating this as the primary reason for immediate PQC migration efforts [8].

A week later, the White House held the National Quantum Initiative (NQI) Centers Summit, emphasizing DEIA in the QIS and greater STEM workforce. The idea of a "quantum-smart"/"quantum-capable" society was raised, establishing a long-term goal for teachers, students, and families to be knowledgeable about and comfortable working with quantum technologies [9]. President Biden then appointed the 15-person National Quantum Initiative Advisory Committee (NQIAC) to advise his cabinet and Congress about the latest NQI developments, specifically in QIS [9].

At the end of December 2022, President Biden signed the "Quantum Computing Cybersecurity Preparedness Act" into law, raising the urgency for PQC migration of federal IT, excluding NSS [10]. The act assured agencies that OMB would issue guidance about an IT inventorying process akin to CISA's framework in March 2021. It also confirmed that OMB will oversee all PQC migration communication with CISA and Congress, as well as PQC testing and IT risk assessments following NIST's release of the 2024 guidance [10].

In March 2023, the Biden-Harris administration released the latest "National Cybersecurity Strategy," outlining their mission to strengthen cyber defense by defending critical infrastructure, disrupting and dismantling threat actors, shaping market forces to drive security and resilience, investing in a resilient future, and forging international partnerships to pursue shared goals [11]. The federal government pledged to continue investing in quantum computing and security research and education, citing its May 2022 memorandum to re-emphasize the urgency of PQC migration for public networks and systems [11].

3. The Internet of Things

In the era of Web 3.0—the third generation of Internet innovation, characterized

by ubiquitous computing across decentralized networks such that users have greater control over their data—cybersecurity has become more critical than ever before. With over fifteen billion Internet of Things (IoT) devices—physical objects such as thermostats and refrigerators that connect to and send data over the Internet—constantly collecting and processing user information, the threat of data leakage and exploitation is now too high [12]. Because IoT hardware is typically compacted into very small objects, it often has very limited energy and data storage banks. Thus, unlike most standard-sized machines, these devices physically cannot employ resource-intensive cryptographic schemas to ensure the highest level of information security possible. As such, it can be reasonably inferred that most if not all PQC algorithms being currently tested simply exceed current IoT processing capabilities, making PQC migration unviable for this entire class of pervasive technologies.

Just as lighter-weight classical cryptographic schemas have been devised and implemented to ensure an acceptable level of IoT security, a similar class of PQC algorithms should be developed as well. Unfortunately, there has been no federal guidance specifically for IoT vendors on this matter, indicating a lack of strong public-private communication channels as well as urgency in addressing *all* quantum-impacted areas. This is a concern because PQC migration for IoT technologies is already predicted to take longer than standard device migration because of the sheer quantity and variety of products on the market. Moreover, many are single-use machines designed with custom operating systems and firmware, which further complicates the task of developing universal schemas.

To address this, NIST and other agencies overseeing this quantum shift should establish methods of keeping IoT vendors apprised of the latest—particularly light-weight—PQC developments and provide strict guidelines on their implementation. Inaccurate, incomplete, and simple lack of proper security configurations is already a widespread issue within the classical cybersecurity space because products are so diverse and the demands for the maximum, most simple end-user experience are so high. This issue will only be exacerbated by quantum, and should be addressed specifically within the IoT sector as it continues to grow exponentially in the coming years. An industry feedback mechanism should also be established to facilitate more effective collaboration with PQC governance bodies so that future recommendations better align with vendors' needs. Similarly, the private sector should prioritize research into quantum-safe options and start preparing for hardware and software updates and upgrades to comply with new standards.

IoT maintenance is also a widespread issue, with many users leaving device software non-updated for years, allowing the number of exploitable—but avoidable—vulnerabilities accumulate, which significantly increases the risk of cyber attacks and personally identifiable information (PII) breaches [13]. It can be reasonably assumed that this concern will only grow as the threat of CRQCs looms closer. Thus, even if all 400+ current IoT vendors make a collective effort with the federal quantum guidance body to develop and implement light-weight PQC

algorithms in a timely manner, the likelihood that more than a small fraction of those devices will indeed be fully upgraded to meet quantum-safe standards is extremely low [14]. Hence, the IoT quantum security discussion should also include measures of better ensuring user compliance to PQC standards. It is indeed evident that a large-scale effort is needed to bring the billions of soon-to-be "legacy" devices—ones that are critically outdated—up to par. The cost of *not* doing so will be at least in the range of hundreds of billions of dollars [15].

4. The Public Key Infrastructure

It has been widely documented that asymmetric cryptographic schema—most notably RSA, ECC, and Diffie-Hellman—can and will be broken by the aforementioned Shor's algorithm. However, it is important to note that other aspects of public key infrastructure (PKI)—which employs asymmetric schema to maintain the confidentiality and integrity of Internet communications using a structure of certificate-based trust relationships—may be vulnerable to quantum attacks as well. In particular, most secure Internet protocols may be at risk. These include Transport Layer Security (TLS), which is used to secure web traffic as part of Hypertext Transfer Protocol Secure (HTTPS); Secure Shell (SSH), which is a secure communication protocol used for network operations and remote computer management; and Pretty Good Privacy (PGP/OpenPGP), which is primarily used to secure email communication [16]. These hybrid cryptosystems leverage asymmetric standards—namely RSA and Diffie-Hellman—in combination with symmetric standards—namely Blowfish, Triple Data Encryption Standard (3DES), and Advanced Encryption Standard (AES) for more secure and efficient encryption.

Most quantum security researchers agree that symmetric cryptography is currently not as vulnerable to quantum attacks as its asymmetric counterpart is [17] [18]; however, the hybrid models discussed still need to be revised and/or replaced because of the asymmetric attack surface. NIST and other bodies including the Institute of Electrical and Electronics Engineers (IEEE) as well as the Quantum Security Alliance (QSA) are currently analyzing and testing PQC algorithms, but have not released any formal communication regarding how these will then be integrated with the rest of PKI. While OpenSSL, OpenSSH, and some other collaborative open-source task forces have begun proactively prototyping quantum-safe schemas, unfortunately, most public and private entities have decided to remain passive on post-quantum mitigation and migration [19] [20].

Cloud computing—the practice of utilizing resources and processing power on demand via the Internet without direct management of these capabilities—has emerged as a key method of increasing availability to and reducing costs of infrastructure, platform, and software requirements [21]. In the era of Everything-as-a-service (E/XaaS) where even PKI deployments have moved off premises, it is critical to retain cyber resiliency, especially with such heavy re-

liance on a single or handful of providers to satisfy a broad spectrum of service needs. The cloud model is unfortunately not inherently quantum-resistant as it too relies on hybrid cryptosystems, whose vulnerabilities—as discussed previously—are too prevalent to ignore.

Fully homomorphic encryption (FHE)—which utilizes the fact that it is very difficult to calculate the distance data is from a point in a lattice—offers a practical solution [22] [23]. This classically- and quantum-safe schema allows for encrypted data to be utilized and processed without first decrypting it, thereby preserving confidentiality and integrity at the highest level [24]. Such a leakage-resistant technology—one that is not susceptible to side-channel attacks in which a malicious actor exploits design flaws in the physical system—can be leveraged specifically in cloud computing [22]. Providers and other third parties can safely operate on outsourced, private information without requiring access to or the possession of the secret key, which is largely impossible with other cryptographic standards where operations can only be performed once data is decrypted.

While FHE is yet to be standardized due its inefficiency and large storage requirements, it has great potential for implementation as a secure, quantum resistant algorithm in the near future. The Homomorphic Encryption Standardization Consortium led by global government, industry, and academia leaders—including the NIST, the entity overseeing the PQC standardization conference—has made recent strides in the optimization of this schema, suggesting the realization of real-world applications in the near future [25]. The widespread dependency on cloud technologies will likely be supported by this new security model, with data privacy and client-provider trust at its core.

5. The Symmetric

The quantum impact on symmetric cryptography is substantially less significant than that on asymmetric cryptography, namely because attack vectors like Grover's algorithm—which offers a polynomial speedup for unstructured search problems—are currently too time and resource intensive to substantially threaten private-key exchanges, under the condition that key sizes are at least doubled [16]. However, this recommendation should still be taken seriously and implemented quickly, as organizational IT and cyber departments may be susceptible to leaving their security configurations on now-vulnerable, default standards.

Psychologically speaking, humans generally avoid unnecessary decision making, commonly characterized by leaving default settings—whether for organ donor registration or web account creation—as they are [26]. This principle of nudge theory—the concept of influencing individuals' behavior and decision-making—can and should be applied to aid global quantum-safe cryptography efforts by standardizing and mandating the removal of insecure options from hardware and software products, if possible. In practice, consumers within the public and private sectors will be automatically more secure, as the path of

least resistance will support the updated security guidelines. Regardless of implementation procedures, the time and resource costs associated with this shift to larger key sizes should be evaluated and planned accordingly with hardware and software capacity constraints in mind, as longer schemas require longer data processing times.

However, consistently doubling key sizes will not be viable in the long-term. Artificial intelligence (AI)—machine intelligence that harnesses computer science and data analysis to solve complex problems—has and will inevitably continue to accelerate quantum computing, which in turn will accelerate AI, thus creating a virtuous cycle of endless exponential growth across both fields. As such, all current PQC algorithms—as standardized by NIST—will likely be broken at some point; a continuous evolution of these solutions will be required, along with a standardized process for phasing out and replacing the freshly insecure ones. This synergy of AI and quantum will be harnessed to successfully implement Grover's—among others, as algorithm development will also be accelerated—within the next couple decades, a direct threat to current symmetric cryptographic schema. Therefore, revisions and/or replacements to existing algorithms should be developed in the near future.

Aside from the principle of doubling private keys, it has become apparent that the integrity of the exchanges themselves can no longer be guaranteed with the application of Simon's algorithm—a precursor to Shor's algorithm. Message Authentication Codes (MACs)—which serve as checksums for message digests to ensure that data has not been intentionally or unintentionally modified in transit—are widely used with SSL/TLS and are constructed from block ciphers—those that encrypt data in specific chunk sizes [27] [28]. Moreover, they are often integrated in Authenticated Encryption with Added Data (AEAD) algorithms, which bind additional, variable data to encrypted messages, preventing adversaries from "replaying" ciphers that were previously sent during a communication session. Unfortunately, the prospect of using Simon's to break most MAC and AEAD schema is substantially high, especially because newer, more robust modes are commonly constructed from deprecated ones, which are not quantum-secure [29]. Most notably, Cipher Block Chaining Message Authentication Code (CBC-MAC), Cipher Block Chaining Hash-Based Message Authentication Code (CBC-HMAC), Offset Codebook Mode (OCB), and Advanced Encryption Standard Galois/Counter Mode (AES-GCM) have all been deemed breakable [17] [29] [30]. Thus, the development of new integrity-ensuring mechanisms for symmetric-reliant systems is critical in ensuring longer-term security.

6. The Other

Beyond assessing high-level cryptographic algorithms for quantum vulnerabilities, one should examine the more primitive technologies embedded within secure systems. Debates on the efficacy of pseudo-random number generators (PRNGs)—deterministic algorithms that generate sequences of quasi-random

numbers using initial values—in a post-quantum era have recently surfaced [31] [32]. Quantum-random number generators (QRNGs)—in deterministic algorithms that harness specific principles of quantum mechanics to generate sequences of truly unpredictable random numbers—have also garnered a significant amount of attention because of their use in QKD [32]. They are classified as true random number generators (TRNGs)—algorithms that leverage natural randomness, such as in variations in background radiation, to generate random sequences of numbers. While there are non-quantum-based TRNGs, many cryptography experts argue that these algorithms are not certifiably random because it is unclear whether the phenomena they exploit would be impossible to model in the future with more advanced technology. Therefore, this branch has similarly been under scrutiny by quantum researchers over whether they are vulnerable to quantum attacks. Both PRNGs and TRNGs are widely used in cryptographic key generation, digital signing, initialization values, security pins, and salts—additional, random strings of information added to passwords for added security. The consequences of breaking these critical algorithms would thus be devastating.

Some researchers have argued that PRNGs are just as effective as QRNGs particularly in machine learning methods, generalizing that the former is thus no less secure than the latter within cryptographic applications [33]. However, they do note that the outputs of both algorithms are explicitly differentiable, which raises a concern of whether one could accurately determine the class of RNG being used [33]. If evidence of a QRNG is detected, for example, one can affirm the existence of quantum nodes on a network. Such information would be highly valuable to an adversary who could tailor their attack strategy to exploit specific quantum or classical system vulnerabilities.

Other researchers have demonstrated that sub-classes of PRNGs currently employed in public and private infrastructure—namely the Blum-Micali family—can be broken with a variation of Grover's and Shor's algorithms combined [32], [34]. The subsequent conclusion that cryptographic systems are also vulnerable to this new set of attack vectors—namely compromised identity authentication and password confidentially mechanisms—is alarming, particularly because there has not been any federal quantum-oriented guidance on this matter. Just as agencies are being implored to establish inventories of their vulnerable asymmetric cryptographic systems, they should similarly analyze the use of P/TRNGs in their infrastructure. While PQC migration would address concerns over P/TRNGs used in key and digital signature generation, the other areas discussed should not be overlooked.

Though QRNGs have been established as highly attack-resistant because it is theoretically impossible to predict the random sequences they generate, implementing them is quite costly. Significant research and development of smaller, faster models has yet to be conducted. However, the European Union (EU) will likely lead this effort in the near future as this technology is a critical part of QKD, which is one of the countries' primary technological investments in prep-

aration for the post-quantum era [35] [36]. Alternatively, the United States (US) has directed its attention towards the development of PQC, so the extent to which the federal government will allocate resources towards QRNGs or more secure P/TRNGs remains unclear [2]. These vastly different approaches to quantum cybersecurity shall be analyzed and compared as the advent of CRQCs grows ever-closer.

7. The Race

Dozens of countries from all around the world are currently investing billions of dollars into QIS research, furthering quantum computing innovation, and harnessing applications for quantum technologies across industries from finance to drug discovery. It is critical that the US remain at the forefront of such developments, as highlighted in National Security Memorandum 10 and implied in the 2023 National Cybersecurity Strategy. While the incoming quantum revolution is expected to usher in a new era of technological and social progress marked by rapid optimization and innovation across the public and private sectors, threat actors ranging from terrorist groups to nation states have been eyeing this trend as an opportunity to launch devastating attacks with incredibly large payouts. The prospect of widespread attacks on US critical infrastructure—such as power grids—is well within reach as evidenced by Russia's history of such schemes on Ukraine, among other nations [37].

Cyber warfare has been rising at an alarming rate over the past few decades, with both the US and its greatest enemies—including but not limited to Iran, North Korea, and Russia—rigorously attempting to compromise each other's abilities to flourish economically [37]. The lack of international guidance surrounding this global issue is already deeply troubling and will only be exacerbated with the continuous advancement of emerging technologies. Just as world powers were initially reluctant to establish policies limiting and then prohibiting the use of chemical warfare following the world wars because it subsequently hindered their own ability to use the weaponry, one can infer that current leaders—including those within the US—are hesitant about taking similar steps in this digital age [38]. Offensive and defensive quantum-cyber strategies and laws should be developed and coordinated across the international community to ensure the security of civilians, industries, and infrastructure. Failing to do so may allow a number of unprecedented attacks to wreak havoc on society.

Moreover, effective emergency response on all levels to those attacks cannot be developed and maintained without a dynamic collective understanding of what the threats are in the first place. Just as a fire department builds its incident command system (ICS) protocols off of baselines surrounding known fire behaviors and patterns, intelligence agencies should similarly continue to track potentially dangerous or suspicious activity and communicate as much of that information to corporations, critical infrastructure authorities, and ordinary users as possible. The challenge of collaborating with foreign entities while remaining

wary of attempts to undermine or exploit domestic systems—as well as maintaining an open dialogue with the general public while staying cautious of insider threats—is significant. However, greater transparency and cooperation are vital to protecting social, economic, and political order worldwide. The effort to facilitate this—particularly surrounding cyberwarfare defense and policy—should continue to grow.

8. The Defense

Beyond the PQC dialogue, several nations have invested heavily into other areas of quantum cybersecurity, most notably harnessing the power of quantum neural networks (QNNs)—quantum-classical models inspired by the construction of the human brain that perform complex processes, such as image recognition [39]. This technology has been implemented in next-generational intrusion detection systems (IDSs)—hardware or software packages used to monitor network traffic for abnormal and malicious behavior [40]. As cyber attacks have become further automated and more pervasive with AI enhancements, the need for effective IDS solutions—particularly for large enterprises that manage tens of thousands of devices simultaneously—has risen significantly.

The use of QNNs for faster, more robust pattern recognition allows for greater visibility across infrastructure as well as quicker incident response times. China's cyber mimic defense (CMD) system, for example, employs QNNs in a polymorphic solution that dynamically adapts to hostilities by concealing and manipulating a network's external—Internet-facing—appearance [40]. Such a strategy has been demonstrated to effectively defend against millions of simultaneous network attacks, as evidenced by the 24-hour global white-hat competition several years ago, during which China gave thousands of cybersecurity researchers and enthusiasts free reign to pummel a network using the CMD system in an attempt to bring it down [40]. The use of QNNs to maintain such resiliency is quite impressive, and its applications should be explored by the US government as well; the technology may be a viable mechanism for protecting highly sensitive infrastructure beyond PQC, the area that has been dominating the post-quantum preparation conversation for the past several years.

Quantum computing has thus proven to be a vehicle of both cyber offense and defense within the international community. Heavy investment in the latter area—beyond cryptography—is necessary for the US to retain its lead in this emerging technology field. Allies and adversaries alike do not only concern themselves with the confidentiality and integrity of communications and critical assets ensured by strong encryption standards. The majority of cyber attacks are not perpetuated on these schemas in the first place [41]!

Resiliency requires holistic analysis and implementation of quantum-enhanced technologies across attack surfaces, rather than hyper-focus on a smaller subset of vulnerabilities. The development of these mechanisms is analogous to the use of unified threat management (UTM) platforms—hardware or software pack-

ages that address a wide variety of security necessities. Ideally, one would deploy separate devices that are each highly adept at mitigating each class of threats, but in cases where the capacity to do so is limited, one settles for just one device that is decently capable of wholly addressing several classes of common threats. Because quantum is still nascent, highly effective mechanisms designed to mitigate specific, quantum-based cyber vulnerabilities have not been developed yet. Therefore, it is critical to invest significant time and resources into ensuring UTM-like, "basic coverage" across a wide range of these vulnerabilities before directing that attention towards narrower areas of concern, such as strictly asymmetric cryptography. Otherwise, a determined attacker could simply discard PQC-protected attack vectors and focus on the other areas described throughout this paper. Being ready for post-quantum means being cognizant of the broader cyber problem and actively addressing it by investing into a broader range of post-quantum defense mechanisms.

Several quantum researchers have advocated for a "shared service" model—where services are funded, resourced, and provisioned by a particular department in an organization—asserting that this approach will lessen the burden on individual entities who seek to implement the necessary quantum-resistant measures [42] [43]. Prioritizing collaboration and establishing interdependent relationships between the public and private sectors is therefore necessary to democratize access to relevant materials and tools. In particular, consolidating the varying levels of guidance and research surrounding quantum will better enable agencies and vendors to follow and implement the latest developments in quantum-resistant algorithms and other technologies faster. Further centralization in this area among the international community is also critical in leveraging the wide variety of ideas, strategies, and developments to only foster greater innovation and ensure greater "coverage" over a larger attack surface, benefiting all parties involved.

9. The Concern

In preparing for the next generation of quantum—and the new class of cybersecurity vulnerabilities that comes with it—it is important to analyze and subsequently strengthen approaches to addressing existing digital privacy and integrity challenges. Based on data compiled in early April 2023, there were over 236 million ransomware attacks worldwide in just the first six months of 2022, with businesses losing roughly $4.35 million per data breach that year [44]. The rate and severity of cybercrime overall has significantly increased in the past several years, with twenty percent of all Internet users globally—over one billion people—having had an alarming one billion email addresses compromised [44]. These issues will only be exacerbated by the incoming quantum technology revolution and should be dealt with more aggressively than ever before.

The lack of secure programming practices has similarly been a widespread issue in software and firmware development, with many companies prioritizing

rapid product releases over slower—but more hygienic—testing procedures. The 2023 Gartner report concluded that "90% of employees who admitted undertaking a range of unsecure actions during their work activities knew that their actions would increase risk to the organization and undertook the actions anyway," thereby emphasizing the rampant inadequacy of cybersecurity awareness [45]. As further underscored in the 2023 National Cybersecurity Strategy, there is currently a lack of legislation surrounding vendors' liability for failing to comply with secure development frameworks [46]. Further discussion and Congressional action on this issue is needed to incentivize the practice of secure-by-design principles and adequate pre-testing amidst heavy market competition. Financial resources should also be allocated towards properly educating current and future generations of developers and engineers on working with quantum-safe algorithms and protocols.

Quantum workforce development begins with K-12; younger generations will make up the future body of technology innovators and policymakers in this field. As such, current STEM education should be revised and restricted to better cultivate understanding of emerging technologies. However, due to the current lack of standardization across quantum computing, programming, algorithm development, and cryptography, there is no clear direction for getting involved in the field. With companies vying to attain quantum advantage—the point where a quantum computer can solve a problem faster and more efficiently than a classical computer—it has become increasingly overwhelming to discern a proper starting point, particularly one that does not require sifting through highly technical documentation. This decentralization then serves as a significant barrier for the dissemination of quantum-cyber hygiene principles, which is detrimental to post-quantum cybersecurity as humans continue to lie at the crux of threat mitigation [47]. In fact, the most common recommendation made by industry and government leaders for maintaining greater resiliency has been emphasizing user education through textbooks, workshops, and gamification [47]. However, it is evident these protocols are not enough to curb the alarming rate of data breaches and resultant expenses. Research shows that "current training programs … have no impact" on "users' cyber hygiene behaviors or knowledge" [48]. These existing solutions have leveraged extrinsic factors—such as money or status—to incentivize individuals to take more precautions surrounding their digital privacy and integrity, and fail to incorporate alternative mechanisms that may be more effective.

In exploring cognitive psychology and the literature surrounding behavioral change, it's become apparent the intersection between these areas and cybersecurity has yet to be thoroughly explored. Very little literature exists on harnessing intrinsic drive and other innate human factors to compel populations to truly invest in important public issues like digital safety. Governing bodies and industry leaders within the classical and quantum cybersecurity policy space should consider investing in the development and analysis of intrinsic models to improve civilians' knowledge and practices within both fields. These entities will

be responsible for executing solutions should they prove to be more effective than existing user training programs, which will require significant structural and procedural changes within organizations nationwide. While this process may seem daunting in the short-term, the cost of not investigating and implementing serious changes in classical cybercrime mitigation will result in a continuous surge of attacks—the consequences of which will continue to devastate individuals and small and large businesses alike—and subsequently exacerbate security challenges within the quantum space. Government agencies cannot disregard existing threats to digital privacy and integrity when developing comprehensive post-quantum defense frameworks because quantum computing and PQC will likely not be implemented ubiquitously. Rather, many hardware researchers and manufacturers are currently working to develop hybrid models—quantum and classical, together—for public and private use [49] [50]. A serious investment should therefore be made in the synthesis and centralization of quantum-cyber resources.

10. Conclusions

Evidently, there are many areas of quantum cybersecurity beyond asymmetric cryptography that should be discussed and addressed right now. The common fixation on PQC has left the IoT and cloud technology spaces; once relatively secure Internet structures; primitives of symmetric cryptosystems; several classes of RNGs; and the quantum workforce grasping for some attempt at navigating the looming post-quantum world. All entities invested in cultivating the new era of stronger digital privacy and integrity share the responsibility of building stronger public-private communication channels, encouraging collaboration between both domestic and international academic and industry spaces, standardizing and centralizing the roadmap for a safer post-quantum future, and cultivating a "quantum-smart" society.

Unfortunately, the majority of end-users, institutions, thought leaders, government officials, and policy makers are not properly educated nor vehemently concerned about the future of cybersecurity and their own cyber and physical safety. PII is not the only source of exploitation and long-term disruption to the global economy. Critical infrastructure—ranging from energy to healthcare to nuclear technologies—has been and will continue to be a prime target for state-sponsored adversaries that are determined to further undermine world powers [37]. The cost of not acknowledging and not adequately addressing this reality is too significant to ignore. In the meantime, a concise list of the proposed action items highlighted in this paper is provided below.

Proposed Action Items:

• Government entities should continue constructing and releasing post-quantum guidance in a timely manner such that it is readily available and highly readable by both vendors and consumers of technology products.

• NIST and other agencies overseeing large-scale post-quantum migration shift should establish methods of keeping IoT vendors apprised of the lat-

est—particularly light-weight—PQC developments and provide strict guidelines on their implementation.

• An industry feedback mechanism should be established to facilitate more effective communication with PQC governance bodies so that future recommendations better align with vendors' needs.

• The private sector should prioritize research into quantum-safe options and start preparing for hardware and software updates and upgrades to comply with new post-quantum standards.

• The principle of nudge theory—the principle of influencing individuals' behavior and decision-making—should be applied to aid global quantum-safe cryptography efforts by standardizing and mandating the removal of insecure options from hardware and software products, if possible.

• New schema—particularly MAC and AEAD—should be developed for symmetric-reliant systems to ensure longer-term security beyond doubling key sizes.

• In addition to establishing inventories of their vulnerable asymmetric cryptographic systems, agencies should similarly analyze the use of P/TRNGs in their infrastructure.

• Offensive and defensive quantum-cyber strategies and laws should be developed and coordinated across the international community to ensure the security of civilians, industries, and infrastructure.

• Intelligence agencies should continue to track potentially dangerous or suspicious activity and communicate as much of that information to corporations, critical infrastructure authorities, and ordinary users as possible.

• The effort to facilitate greater transparency and cooperation surrounding cyberwarfare defense and policy should continue to grow because it is vital to protecting social, economic, and political order worldwide.

• The US should prioritize holistic analysis and implementation of quantum-enhanced technologies across attack surfaces, rather than hyper-focus on a smaller subset of vulnerabilities.

• The international community should prioritize collaboration and the establishment of interdependent relationships between the public and private sectors to democratize access to relevant materials and tools via a "shared services" model.

• Entities should analyze and subsequently strengthen approaches to addressing existing digital privacy and integrity challenges.

• The federal government should incentivize the practice of secure-by-design principles and adequate pre-testing amidst heavy market competition.

• Financial resources should be allocated towards properly educating current and future generations of developers and engineers on working with quantum-safe algorithms and protocols.

• Governing bodies and industry leaders within the classical and quantum cybersecurity policy space should consider investing in the development and analysis of intrinsic models to improve civilians' knowledge and practices within

both fields.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] (2021) Post-Quantum Cryptography. Homeland Security. https://www.dhs.gov/quantum

[2] NSA/CSS (2020) Quantum Key Distribution (QKD) and Quantum Cryptography (QC). National Security Agency/Central Security Service. https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

[3] (2022) National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems. Proclamation No. NSM-10 F.R. The White House. https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

[4] NIST (2022) NIST Announces First Four Quantum-Resistant Cryptographic Algorithms. NIST. https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

[5] (2022) Preparing Critical Infrastructure for Post-Quantum Cryptography. CISA Insights. https://www.cisa.gov/sites/default/files/publications/cisa_insight_post_quantum_cryptography_508.pdf

[6] NSA Media Relations. (2022) NSA Releases Future Quantum-Resistant (QR) Algorithm Requirements for National Security Systems. NSA. https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3148990/nsa-releases-future-quantum-resistant-qr-algorithm-requirements-for-national-se

[7] (2022) Proclamation No. M-23-02 F.R. Executive Office of the President Office of Management and Budget. https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf

[8] NIST (2022) Fourth PQC Standardization Conference. NIST. https://csrc.nist.gov/events/2022/fourth-pqc-standardization-conference

[9] (2022) Readout: National Quantum Initiative Centers Summit. The White House. https://www.whitehouse.gov/ostp/news-updates/2022/12/05/readout-national-quantum-initiative-centers-summit/

[10] (2022) Quantum Computing Cybersecurity Preparedness Act. Congress. https://www.congress.gov/bill/117th-congress/house-bill/7535/text

[11] (2023) FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy. The White House. https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

[12] Statista (2022) Number of Internet of Things (IoT) Connected Devices Worldwide

from 2019 to 2021, with Forecasts from 2022 to 2030. Statista. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

[13] Prakash, V., Xie, S. and Huang, D. Y. (2022) Software Update Practices on Smart Home IoT Devices. ArXiv. https://arxiv.org/pdf/2208.14367.pdf

[14] Nick, G. (2023) How Many IoT Devices Are There in 2023? Techjury. https://techjury.net/blog/how-many-iot-devices-are-there/#gref

[15] Statista (2018) Projected Market Revenue of the Internet of Things (IoT) and Analytics Worldwide from 2015 to 2021, by Segment. Statista. https://www.statista.com/statistics/913299/projected-global-revenue-of-the-internet-of-things-segment/

[16] Bogomolec, X., Underhill, J.G. and Kovac, S.A. (2019) Towards Post-Quantum Secure Symmetric Cryptography: A Mathematical Perspective. International Association for Cryptologic Research. https://eprint.iacr.org/2019/1208

[17] Krelina, M. (2021) Quantum Technology for Military Applications. *EPJ Quantum Technology*, **8**, Article No. 24. https://doi.org/10.1140/epjqt/s40507-021-00113-y

[18] Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., Pereira, J.L., Razavi, M., Shamsul Shaari, J., Tomamichel, M., Usenko, V.C., Vallone, G., Villoresi, P. and Wallden, P. (2020) Advances in Quantum Cryptography. *Advances in Optics and Photonics*, **12**, 1012-1036. https://doi.org/10.1364/AOP.361502

[19] Leyden, J. (2022) OpenSSH 9.0 Bakes in Post-Quantum Cryptography to Future Proof against Attacks. The Daily Swig. https://portswigger.net/daily-swig/openssh-9-0-bakes-in-post-quantum-cryptography-to-future-proof-against-attacks

[20] Easterbrook, K. and Paquin, C. (n.d.) Post-Quantum TLS. Microsoft. https://www.microsoft.com/en-us/research/project/post-quantum-tls/

[21] Mell, P. and Grance, T. (2011) The NIST Definition of Cloud Computing. Computer Security. NIST. https://doi.org/10.6028/NIST.SP.800-145 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[22] Albrecht, M., Chase, M., Chen, H., Ding, J., Goldwasser, S., Gorbunov, S., Helevi, S., Hoffstein, J., Lauter, K., Lokam, S., Micciancio, D., Moody, D., Morrison, T., Shahai, A. and Vaikuntanathan, V. (2018) Homomorphic Encryption Standard. http://homomorphicencryption.org/wp-content/uploads/2018/11/HomomorphicEncryptionStandardv1.1.pdf

[23] Will, M.A. and Ko, R.K.L. (2015) Chapter 5-A Guide to Homomorphic Encryption. In: *The Cloud Security Ecosystem*, Elsevier, Amsterdam, 101-127. https://doi.org/10.1016/B978-0-12-801595-7.00005-7

[24] Armknecht, F., Boyd, C., Carr, C., Gjosteen, K., Jaschke, A., Reuter, C.A. and Strand, M. (2015) A Guide to Fully Homomorphic Encryption. Cryptology ePrint Archive. https://eprint.iacr.org/2015/1192.pdf

[25] (n.d.) Homomorphic Encryption Standardization. https://homomorphicencryption.org/introduction/

[26] Van dalen, H.P. and Henkens, K. (2014) Comparing the Effects of Defaults in Organ Donation Systems. *Social Science & Medicine*, **106**, 137-142. https://doi.org/10.1016/j.socscimed.2014.01.052

[27] McGrew, D.A. (2008) An Interface and Algorithms for Authenticated Encryption. RFC. (Memo) https://www.rfc-editor.org/rfc/pdfrfc/rfc5116.txt.pdf https://doi.org/10.17487/rfc5116

[28] (2009) Chapter 3-An Introduction to Cryptography. In: Liu, D. and Author, L., Eds., *Next Generation SSH2 Implementation*, Elsevier, Amsterdam, 41-64. https://doi.org/10.1016/B978-1-59749-283-6.00003-9

[29] Santoli, T. and Schaffner, C. (2017) Using Simon's Algorithm to Attack Symmetric-Key Cryptographic Primitives. Rinton Press, Princeton. https://doi.org/10.26421/QIC17.1-2-4 https://dl.acm.org/doi/10.5555/3179483.3179487

[30] Takagi, T. (2016) Post-Quantum Cryptography. *Proceedings of 7th International Workshop* (PQCrypto 2016), Fukuoka, 24-26 February 2016, 3. https://link.springer.com/chapter/10.1007/978-3-319-29360-8_4#citeas

[31] Barker, E., Barker, W., Burr, W., Polk, W. and Smid, M. (2016) Recommendation for Key Management—Part 1: General. Revision 3, NIST. https://doi.org/10.6028/NIST.SP.800-57pt1r4 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-57p1r3.pdf

[32] Guedes, E.B., De Assis, F.M. and Lula, B. (2012) Quantum Attacks on Pseudorandom Generators. *Mathematical Structures in Computer Science*, **23**, 608-634. https://doi.org/10.1017/S0960129512000825

[33] Bird, J.J., Ekárt, A. and Faria, D.R. (2019) On the Effects of Pseudorandom and Quantum-Random Number Generators in Soft Computing. *Soft Computing*, **24**, 9243-9256. https://doi.org/10.1007/s00500-019-04450-0

[34] Kelsey, J., Schneier, B., Wagner, D. and Hall, C. (1998) Cryptanalytic Attacks on Pseudorandom Number Generators. In: Vaudenay, S., Ed., *FSE* 1998: *Fast Software Encryption*, *Lecture Notes in Computer Science*, Vol. 1372, Springer, Berlin, 168-188. https://doi.org/10.1007/3-540-69710-1_12 https://www.schneier.com/wp-content/uploads/2017/10/paper-prngs.pdf

[35] European Commission (n.d.) The European Quantum Communication Infrastructure (EuroQCI) Initiative. European Commission. https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci

[36] (2023) QKISS: Developing Ready-to-Deploy European Quantum Key Distribution (QKD) Systems. Photonics & Space. https://www.ixblue.com/north-america/qkiss-developing-ready-to-deploy-european-quantum-key-distribution-qkd-systems/

[37] Egloff, F.J. and Smeets, M. (2020) Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's most Dangerous Hackers. *Journal of Cyber Policy*, **5**, 326-327. https://doi.org/10.1080/23738871.2020.1808032

[38] Gibney, A., Director. (2016) Zero Days. (Film) Magnolia Pictures. https://www.amazon.com/Zero-Days-Colonel-Gary-Brown/dp/B01I2C0UV6

[39] Qiskit (2023) Quantum Neural Networks. Qiskit. https://qiskit.org/documentation/machine-learning/tutorials/01_neural_networks.html

[40] Middleton, A. and Till, S. (2020) Quantum Information Processing Landscape 2020: Prospects for UK Defence and Security. DSTL. https://uknqt.ukri.org/wp-content/uploads/2021/10/Quantum-Information-Processing-Landscape-2020.pdf

[41] (n.d.) Cybersecurity: A Global Priority and Career Opportunity. University of North Georgia, Dahlonega. https://ung.edu/continuing-education/news-and-media/cybersecurity.php

[42] Johnson, J. (Host). (2023) ICYMI: The Race to Secure Federal Cryptographic Sys-

tems [Audio Podcast Episode]. In: Larsen, C. (Producer), The Buzz, ACT-IAC. https://www.actiac.org/buzz

[43] IBM (2021)Shared Services. IBM. https://www.ibm.com/docs/en/psww2500/2.3.2.0?topic=reference-shared-services

[44] Griffiths, C. (2023) The Latest 2023 Cyber Crime Statistics (updated April 2023). AAG. https://aag-it.com/the-latest-cyber-crime-statistics/

[45] Gopal, D., McMullen, L., Walls, A., Addiscott, R., Furtado, P., Porter, C., Isaka, O. and Winckless, C. (2023) Predicts 2023: Cybersecurity Industry Focuses on the Human Deal. Gartner. https://www.bitsight.com/thank-you/gartner-predicts-2023

[46] Jr Biden, J. and Harris, K. (2023) National Cybersecurity Strategy. The White House. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[47] Dortch, M. (2017) User Education for Cybersecurity: Yes, It's Worth It. invanti. https://www.ivanti.com/blog/user-education-cybersecurity-yes-worth

[48] Cain, A.A., Edwards, M.E. and Still, J.D. (2018) An Exploratory Study of Cyber Hygiene Behaviors and Knowledge. *Journal of Information Security and Applications*, **42**, 36-45. https://doi.org/10.1016/j.jisa.2018.08.002

[49] Hirayama, Y., Ishibashi, K. and Nemoto, K., Eds. (2021) Hybrid Quantum Systems. Springer Nature, Berlin. https://doi.org/10.1007/978-981-16-6679-7

[50] IONQ (2023) What Is Hybrid Quantum Computing. IONQ. https://ionq.com/resources/what-is-hybrid-quantum-computing

Appendix

AEAD: Authenticated Encryption with Additional Data—bind additional, variable data to encrypted messages, preventing adversaries from "replaying" ciphers that were previously sent during a communication session

AES: Advanced Cryptography Standard

AES-GCM: Advanced Encryption Standard Galois/Counter Mode

AI: Artificial Intelligence—machine intelligence that harnesses computer science and data analysis to solve complex problems

Asymmetric Cryptography: use a combination of public and private keys to encrypt data

CBC-HMAC: Cipher Block Chaining Hash-Based Message Authentication Code

CBC-MAC: Cipher Block Chaining Message Authentication Code

CISA: Cybersecurity and Infrastructure Security Agency—subset of DHS

Cloud Computing: the practice of utilizing resources and processing power on demand via the Internet without direct management of these capabilities

CMD: Cyber Mimic Defense—employs QNNs in a polymorphic solution that dynamically adapts to hostilities by concealing and manipulating a network's external, Internet-facing, appearance

CNSA 1.0: Commercial National Security Algorithm suite 1.0—most have been deemed non-quantum-resistant (legacy)

CNSA 2.0: Commercial National Security Algorithm suite 2.0—approved quantum-resistant algorithms

CRQC: Cryptanalytically Relevant Quantum Computer

DEIA: Diversity, Equity, Inclusion, and Accessibility

DHS: Department of Homeland Security

Digital Signing: a method of ensuring a message's authenticity and integrity

DoD: Department of Defense

ECC: Elliptic Curve Cryptography

EU: European Union

E/XaaS: Everything-as-a-service—a business model by which any form of computing, storage, network security, etc. can be outsourced to a cloud provider

FCEB: Federal Civilian Executive Branch

FHE: Fully Homomorphic Encryption—utilizes the fact that it is very difficult to calculate the distance data is from a point in a lattice

Grover's Algorithm: quantum algorithm that offers a polynomial speedup for unstructured search problems

HTTPS: Hypertext Transfer Protocol Secure—encrypted web communication protocol

Hybrid Cryptosystem: leverage asymmetric and symmetric cryptography for more secure and efficient encryption

ICS: Incident Command System—standardized organizational risk management structure

IDS: Intrusion Detection System—hardware or software packages used to monitor network traffic for abnormal and malicious behavior

IEEE: Institute of Electrical and Electronics Engineers

IoT: Internet of Things—physical objects such as thermostats and refrigerators that connect to and send data over the Internet

IT: Information Technology—the use of networking devices, infrastructure, and processing to create, exchange, store, and secure electronic data

Leakage: the susceptibility to side-channel attacks in which a malicious actor exploits design flaws in the physical system

Legacy: critically outdated systems

MAC: Message Authentication Code—serves as a checksum for message digests to ensure that data has not been intentionally or unintentionally modified in transit

NCCoE: National Cybersecurity Center of Excellences

NCF: National Critical Function

NIST: National Institute of Standards and Technology

NQI: National Quantum Initiative

NQIAC: National Quantum Initiative Advisory Committee

NSA: National Security Agency

NSS: National Security Systems—any system involved in intelligence gathering or handling for military purposes, weapons systems, and the like

Nudge Theory: the concept of influencing individuals' behavior and decision-making

OCB: Offset Codebook Mode

OMB: Office of Management and Budget

OSTP: Office of Science and Technology Policy

PII: Personally Identifiable Information—any information by which an individual can be readily identified, directly or indirectly

PGP: Pretty Good Privacy—primarily used to secure email communication

PKI: Public Key Infrastructure—employs asymmetric schema to maintain the confidentiality and integrity of Internet communications using a structure of certificate-based trust relationships

PQC: Post-Quantum Cryptography—a class of quantum computer-resistant algorithms designed to be implemented on classical computers

PRNG: Pseudo-Random Number Generator—deterministic algorithms that generate sequences of quasi-random numbers using initial values

QIS: Quantum Information Science—the study of harnessing properties of quantum mechanics to circumvent current information and computer processing limitations of classical computers

QKD: Quantum Key Distribution—quantum-secure communication protocols that harness properties of quantum mechanics to ensure the confidentiality and integrity of data being transmitted

QNN: Quantum Neural Network—a quantum-classical model inspired by the construction of the human brain that is used to perform complex processes, such

as image recognition

QRNG: Quantum-Random Number Generator—an indeterministic algorithm that harnesses specific principles of quantum mechanics to generate sequences of truly unpredictable random numbers

QSA: Quantum Security Alliance

Quantum Advantage: the point where a quantum computer can solve a problem faster and more efficiently than a classical computer

RSA: Rivest-Shamir-Adleman

Simon's Algorithm: a precursor to Shor's algorithm

Shared Service: a service that is funded, resourced, and provisioned by a particular department in an organization

Shor's Algorithm: can break asymmetric cryptographic algorithms via rapid integer factorization

SSH: Secure Shell—a secure communication protocol used for network operations and remote computer management

STEM: Science, Technology, Engineering, and Math

Symmetric Cryptography: use a single encryption key for two-party exchanges

TLS: Transport Layer Security—most notably used to secure web traffic

TRNG: True Random Number Generator—an algorithm that leverages natural randomness, such as in variations in background radiation, to generate random sequences of numbers

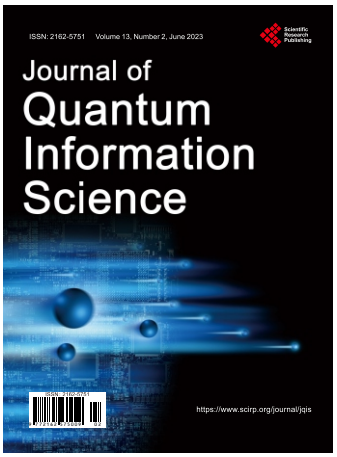
US: United States

UTM: Unified Threat Management—hardware or software packages that address a wide variety of security necessities

Web 3.0: the third generation of Internet innovation, which is characterized by ubiquitous computing across decentralized networks such that users have greater control over their data

3DES: Triple Data Encryption Standard

Call for Papers



Journal of Quantum Information Science

ISSN 2162-5751 (Print) ISSN 2162-576X (Online)
https://www.scirp.org/journal/jqis

Executive Editor-in-Chief

Editorial Board

Subject Coverage

The field of Quantum Information Science is the most challenging and hot topic among all branches of science. This field is also quite interdisciplinary in character, and people from quantum theory, computer science, mathematics, information theory, condensed matter physics, many-body physics and many more have been actively involved to understand implications of quantum mechanics in information processing. JQIS aims to publish research papers in the following areas:

- Dynamical Maps
- Experimental Implementation
- Geometric Quantum Computation
- Quantum Computation
- Quantum Cryptography
- Quantum Entanglement
- Quantum Information Processing Protocols
- Quantum Information Theory
- Relativistic Quantum Information Theory

JQIS will consider original Letters, Research articles, and short Reviews in the above and related areas. Before publication in JQIS all the submitted papers will be peer-reviewed by the experts in the field. We can plan to bring out JQIS as a monthly journal, hence all the authors can take advantage of rapid publications of their results in this fast growing field. Being an open access journal we can hope to reach a much wider readership compared to other journals in the related areas.

Website and E-Mail

https://www.scirp.org/journal/jqis **E-mail: jqis@scirp.org**

What is SCIRP?

Scientific Research Publishing (SCIRP) is one of the largest Open Access journal publishers. It is currently publishing more than 200 open access, online, peer-reviewed journals covering a wide range of academic disciplines. SCIRP serves the worldwide academic communities and contributes to the progress and application of science with its publication.

What is Open Access?

All original research papers published by SCIRP are made freely and permanently accessible online immediately upon publication. To be able to provide open access journals, SCIRP defrays operation costs from authors and subscription charges only for its printed version. Open access publishing allows an immediate, worldwide, barrier-free, open access to the full text of research papers, which is in the best interests of the scientific community.

- High visibility for maximum global exposure with open access publishing model
- Rigorous peer review of research papers
- Prompt faster publication with less cost
- Guaranteed targeted, multidisciplinary audience

Scientific Research Publishing

Website: https://www.scirp.org

Subscription: sub@scirp.org

Advertisement: service@scirp.org