Journal of Mathematics and Statistics Studies
ISSN: 2709-4200
DOI: 10.32996/jmss
Journal Homepage: www.al-kindipublisher.com/index.php/jmss

JMSS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Quantum Computing Applications in the Fields of Cryptography, Material Science, and Machine Learning

Md Samiun[1]✉, Nur Mohammad[2], Mohammad Hossain[3] and Jahanara Akter[4]
[1]*Department of Computer science and engineering, Daffodil International University, Dhaka, Bangladesh*
[2]*Department of Computer science and engineering, Sonargaon University, Dhaka, Bangladesh*
[3]*Department of Electrical and electronics engineering, University of Information Technology and Sciences (UITS), Dhaka, Bangladesh*
[4]*Department of Business Administration, Islamic University, Kushtia, Bangladesh*
Corresponding Author: Md Samiun, **E-mail**: engineersamiun@gmail.com

| ABSTRACT
Despite the significant scientific and engineering hurdles in advancing quantum computers, notable strides are being made toward utilizing this technology in commercial domains. Quantum computers are projected to exceed the computational power of classical computers within the next decade, potentially revolutionizing various industries. This study explores a range of fields that have already begun integrating quantum hardware. By presenting these as examples of combinatorial problems, we demonstrate their applications across three key sectors: cryptography, material science, and Machine Learning. Further, we will conduct a survey on various industries and companies to identify the broader usage of quantum computing in their manufacturing. The survey will analyze the diverse potential applications and current advantages of quantum hardware and algorithms. The results will help further researchers identify and segment the companies and understand the rapid application of quantum computing.

| KEYWORDS

Quantum Computing, Cryptography, Machine Learning, Material science, Qubits.

| ARTICLE INFORMATION

ACCEPTED: 03 November 2020 **PUBLISHED:** 26 December 2020 **DOI:** 10.32996/jmss.2020.1.2.5

1. Introduction

Quantum computing (QC) has shown promising results in addressing complex, large-scale problems by leveraging quantum mechanics principles such as superposition and entanglement. These principles allow for exponentially increasing states as the number of qubits, or quantum bits, grows (Dunjko & Briegel, 2018). Quantum computers take advantage of the probabilistic nature of quantum states before measurement, enabling them to process significantly more data compared to traditional computers (Nawaz et al., 2019). They perform operations using qubits, which are derived from the quantum state of an object, rather than the binary bits used by classical computers. These qubits exhibit phenomena like superposition, allowing a quantum system to exist in multiple states at once, and entanglement, creating a highly correlated relationship between quantum particles. This gives quantum computers an advantage in performing complex calculations that classical systems would take extremely long to achieve (Harrow et al., 2009; Vogel, 2011). However, this advancement poses a growing threat to data security, as encryption methods rely on the difficulty of mathematical problems. Progress in quantum computing (PQC) offers hope for securely transitioning all encrypted data to quantum-safe systems (Nejatollahi et al., 2019). Additionally, quantum simulation holds great promise for unraveling the complex nature of molecular and chemical interactions, potentially leading to the development of new treatments and materials.
Richard Feynman introduced the quantum computer in 1982, which uses qubits instead of traditional bits (Feynman, 1986). Qubits can superpose in both 0 and 1 states, making them unique and solving complex issues (Vogel, 2011). Quantum computing also

uses entanglement, allowing real parallel computing. As the number of entangled qubits increases, the number of values that can be processed in a single operation increases exponentially. Universal and non-universal quantum computers exist, with universal computers capable of performing any work and non-universal ones optimized for specific purposes like machine learning algorithm optimization. D-Wave's non-universal quantum computer has over 2,000 qubits, while IBM's universal quantum computer has 17 qubits with improved error-correcting (Ciliberto et al., 2018). In October 2017, Intel and QuTech unveiled a 17-qubit global quantum computer(Dhawan et al., 2018). Quantum computers have a different design than conventional computers, using liquids and quantum dots, electrons in superposition. They outperform conventional computers only when coupled with quantum parallelism methods, and may not multiply faster than conventional computers (Orús et al., 2019).

Quantum computing (QC) is a rapidly developing technology that uses quantum principles to solve complex computational problems. It aims to enhance our understanding of quantum phenomena and accelerate computing, influencing technological progress in the 21st century (Schuld & Petruccione, 2018). QC requires expertise from various disciplines, including physicists, computer scientists, mathematicians, chemists, and engineers. Collaboration between academics and industry researchers is crucial to address technical and management challenges (Hu et al., 2019). Scientists worldwide are working to improve the performance of quantum hardware, create and refine quantum algorithms, and overcome obstacles to make QC computers a reality. The five essential stages for QC machines include initializing quantum states, preserving qubit information, achieving efficient decoherence time, implementing a universal quantum gate architecture, and ensuring accurate qubit measurement capability (DiVincenzo & Ibm, 2000).

This study aims to investigate the specific applications of quantum computing (QC) in cryptography, material science, and machine learning (ML). The objectives include documenting QC's current application in these fields, conducting an empirical survey to measure its adoption, assessing stakeholder perceptions of QC's potential and effectiveness, and identifying gaps in QC's application in these fields. The research is structured into five chapters, with Chapter 1 providing an introduction to the subject, Chapter 2 a comprehensive literature review, Chapter 3 detailing the research methodology, and chapter 4 focusing on the research results and detailing the specific applications of QC in cryptography, material science, and ML, respectively. The research concludes by discussing challenges encountered, summarizing key insights, and offering recommendations for future research in chapter 5. The research aims to provide a comprehensive understanding of QC's potential in these fields and to inform future research directions.

2. Literature review

The history of quantum computing (QC) dates back to the early 1980s, with contributions from physicist Richard Feynman and computer scientist David Deutsch. Feynman proposed that quantum mechanics could be used to simulate physical processes more efficiently than classical computers, laying the groundwork for QC (Feynman, 1986). Deutsch expanded on this by conceptualizing a universal quantum computer capable of simulating any physical process (Hidary & Hidary, 2019). In 1994, mathematician Peter Shor developed Shor's algorithm for factoring large integers exponentially faster than classical algorithms, highlighting the potential of quantum computers to tackle complex problems, particularly in cryptography (Bennett & Brassard, 2014). Lov Grover introduced Grover's algorithm, offering a quadratic speedup for unstructured search problems, further underscoring the power of quantum computation (Bennett et al., 1993). Experimental efforts to realize quantum computers began in the late 1990s and early 2000s, with initial demonstrations using nuclear magnetic resonance (NMR) techniques (Kitaev, 2003). In 2001, IBM and Stanford University successfully factored the number 15 using a 7-qubit NMR quantum computer. The 21st century has seen rapid advancements in QC technology, with companies like IBM, Google, and Rigetti Computing developing superconducting qubit-based processors. Quantum chemistry (QC) has gained global attention, leading to increased funding and research initiatives (A. Peruzzo et al., 2014). The European Union launched the Quantum Flagship initiative, while the US enacted the National Quantum Initiative Act. Researchers are working on overcoming technical challenges like qubit coherence and error correction to fully realize QC's potential. This synergy between theoretical and experimental advancements promises unprecedented computational capabilities and new scientific and technological horizons (Lubasch et al., 2019).

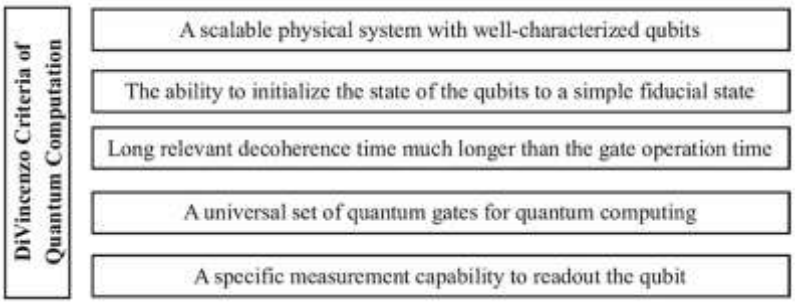

Figure 1: Quantum computing's fundamental stages (DiVincenzo & Ibm, 2000)

Figure 1 illustrate Quantum computing's fundamental stages. Quantum computing (QC) is a rapidly evolving field with significant technological advancements and growing momentum in academic research and commercial development (Gatla, 2018). Leading technology companies, startups, and academic institutions are developing quantum processors using various qubit technologies, such as superconducting qubits, trapped ions, and photonics (Liu et al., 2018). IBM's Quantum Experience and Google's Sycamore processor have become benchmarks in the industry, with Google's 2019 demonstration of quantum supremacy marking a significant milestone (Liu et al., 2018). Qubit coherence is a primary challenge, as qubits are highly sensitive to decoherence and noise, leading to computation errors. Researchers are advancing error correction methods and developing more robust qubit designs. Different qubit technologies, such as topological qubits and quantum dots, are being explored for their potential to offer higher stability and lower error rates compared to traditional superconducting qubits (Möller & Vuik, 2017). Software has also made significant progress in quantum algorithms and programming environments, with new algorithms being developed to exploit quantum parallelism for applications in optimization, cryptography, material science, and drug discovery (Arslan et al., 2018). Quantum software platforms like IBM's Qiskit, Google's Cirq, and Microsoft's Quantum Development Kit are fostering a growing community of developers and researchers. Government and industry investments in QC (Dinur et al., 2018), such as the U.S. National Quantum Initiative Act, the European Union's Quantum Flagship program, and substantial funding in China, are accelerating this progress (Perdomo-Ortiz et al., 2018). With continuous improvements in qubit stability, error correction, and algorithm development, QC is steadily progressing toward becoming a practical and revolutionary technology (Lamba et al., 2018). Since Feynman proposed the concept of quantum computing (QC), the field has been extensively researched due to its potential for groundbreaking technological advancements. The primary objective of QC research is to develop a universal and fault-resistant quantum computer that can perform tasks such as integer factorization and quantum simulation more efficiently than conventional computers (Neven et al., 2010). However, the goal has not yet been achieved, but the global community focused on quantum information processing has made significant progress in the past decade. Research in QC has its roots in early theoretical groundwork, with pioneers like Deutsch proposing the concept of a universal quantum computer in 1985 (Jhanwar & Nene, 2021). This work introduced the idea that quantum bits could exist in superposition, allowing quantum computers to perform multiple calculations simultaneously. In the 1990s, further strides were made with the development of quantum algorithms, particularly Shor's algorithm for factoring large integers. This revelation sparked significant interest and investment in QC research, particularly in cryptography (Himanen et al., 2019) .The late 1990s and early 2000s saw experimental implementations of QC principles, including successful demonstrations of quantum teleportation and the realization of simple quantum gates in various physical systems (Babikian, 2017). Error correction codes, such as the surface code, provided a pathway towards fault-tolerant QC, which is essential for the practical realization of quantum computers due to their susceptibility to decoherence and noise(Grimes, 2019). In recent years, research has increasingly focused on hybrid quantum-classical algorithms that aim to leverage near-term quantum devices, often referred to as Noisy Intermediate-Scale Quantum (NISQ) devices (Alberto Peruzzo et al., 2014). These algorithms have shown promise in solving specific problems in chemistry, optimization, and material science, albeit within the limitations of current quantum hardware (Alberto Peruzzo et al., 2014).

Quantum computing (QC) is a revolutionary approach to computational challenges, with significant potential in cryptography, material science, and machine learning. It presents both threats and opportunities in cryptography, as traditional techniques rely on factoring large numbers (Gheorghiu et al., 2019). QC can revolutionize secure communication by detecting eavesdropping attempts and ensuring unbreakable encryption (Anukool et al., 2018). In material science, QC enables the simulation and modeling of complex molecular structures with precision unattainable by classical computers. Quantum algorithms, such as VQE, can determine the ground state energies of molecules, offering insights into their stability and reactivity (Chawla & Mehra, 2023). This application could accelerate the development of new materials with customized properties for various industries, including pharmaceuticals, energy, and electronics. In machine learning, QC is expected to make significant strides, as quantum ML algorithms enhance the efficiency and capabilities of conventional models (Golestan et al., 2023). As the technology continues to develop, its potential to solve problems currently out of reach for classical computers is likely to drive significant advancements across various fields (Phillipson, 2020).

Quantum computing (QC) has been largely studied for its theoretical potential and technical advancements, leaving a significant gap in empirical research on its application in specialized domains. While there is a growing body of work on QC's capabilities in cryptography, their practical implementation and real-world effectiveness remain underexplored. In material science, QC's future potential to revolutionize material discovery is often discussed, but empirical data on current applications and their impact is scarce. In machine learning (ML), there is a lack of comprehensive studies quantifying the benefits and limitations of QC in practical settings. Additionally, there is limited research capturing industry perspectives or user experiences regarding the usefulness and challenges of integrating QC into these fields. This study aims to fill these gaps by conducting a survey to gather empirical data on QC applications in cryptography, material science, and ML, and understanding stakeholders' perceptions of QC's usefulness and impact.

3. Research Methodology

This study uses a blended approach, combining qualitative and quantitative methods, to explore the applications of quantum computing in cryptography, material science, and machine learning. Quantitative methods analyze trends, correlations, and

potential causal relationships between quantum computing advancements and their applications in these fields. Qualitative methods provide an in-depth exploration of expert opinions, theoretical frameworks, and the perceived future impact of quantum computing. This approach provides a comprehensive perspective on how quantum computing is revolutionizing various scientific and technological domains. Data collection is conducted through a multifaceted approach involving several techniques to ensure comprehensive coverage and reliability of the findings as shown in Figure 2:

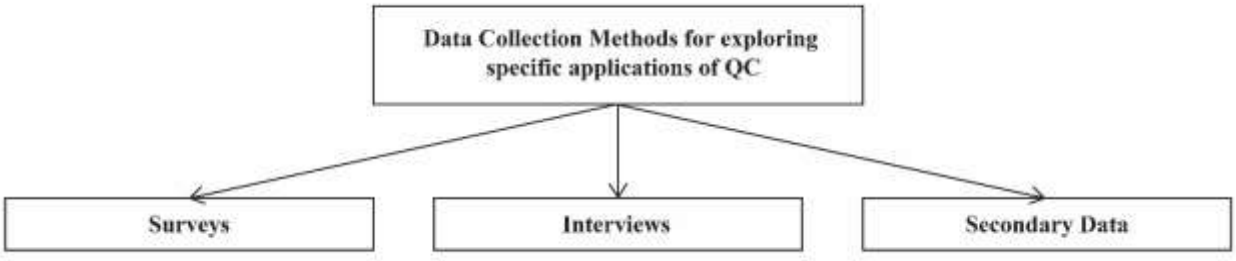

Figure 2: Data collection methods used for exploring specific applications of QC in various fields.

Structured surveys are distributed to professionals in cryptography, material science, and ML, as well as quantum computing (QC) experts, to gather quantitative data on the adoption, effectiveness, and challenges of QC in these fields. Closed-ended questions are used for statistical analysis, covering aspects like frequency of QC usage, types of quantum algorithms, and perceived benefits and challenges. Semi-structured interviews with key stakeholders provide qualitative data, offering insights into personal experiences, strategic perspectives, and theoretical considerations related to QC. Open-ended questions allow participants to elaborate on their views, revealing underlying factors influencing QC adoption and its perceived impact. Secondary data sources, such as academic journals and industry reports, supplement the primary data, providing background information and supporting the validation of primary data.

The analysis of data is performed using a range of techniques tailored to the nature of the data collected:

Quantitative Data Analysis: Statistical methods are employed to analyze survey data and other numerical inputs. Techniques such as descriptive statistics provide summaries of the data, while inferential statistics, including regression analysis, are used to explore relationships between variables and test hypotheses. Additionally, ML models are applied to uncover complex patterns and predictive insights from the data, particularly in assessing the potential future impact of QC in various fields.

Qualitative Data Analysis: Thematic analysis is utilized for examining qualitative data from interviews and open-ended survey responses. This method involves coding the data to identify recurring themes, patterns, and significant insights. Thematic analysis allows for a deep understanding of participants' perspectives and experiences, highlighting commonalities and differences in how QC is perceived and utilized across different scientific domains. This qualitative analysis complements the quantitative findings by providing contextual and explanatory details.

Integration of Data: The integration involves comparing and contrasting findings from both data types to draw holistic conclusions about the impact of QC on cryptography, material science, and ML. The combined analysis helps to validate results, uncover new insights, and offer a more nuanced interpretation of the data.

Ethical considerations are fundamental to this study, ensuring that research practices uphold the highest standards of integrity and respect for participants:

Confidentiality: All participant information is handled with strict confidentiality. Data is anonymized to protect individual identities, and secure methods are used to store and manage data.

Privacy: The study adheres to privacy regulations and guidelines, safeguarding personal information and ensuring that data collection and analysis practices comply with legal and ethical standards.

Transparency: The research process, including methodologies, data collection, and analysis procedures, is conducted transparently. Participants are informed about how their data will be used, and any potential conflicts of interest are disclosed.

The limitations that can affect the interpretation and generalizability of the findings:

Limited Scope of Fields: While the study focuses on the applications of QC in cryptography, material science, and ML, it inherently excludes other fields where QC may have a significant impact, such as optimization, pharmaceuticals, or financial modeling. This narrowed focus may overlook important developments and applications in these omitted areas.

Survey-Based Data Collection: The reliance on survey data to assess the adoption and perception of QC introduces potential biases, including self-selection bias and response bias. Participants who are more interested or knowledgeable about QC may be more likely to respond, potentially skewing the results. Additionally, the subjective nature of perceptions can lead to variability in responses that may not accurately reflect the broader industry's view.

Rapidly Evolving Technology: QC is a rapidly evolving field, and the applications and perceptions of QC may change significantly over a short period of time. This study captures a snapshot in time, and its findings may quickly become outdated as new advancements are made and new applications are discovered.

Complexity of QC: Due to the highly specialized and technical nature of QC, there may be limitations in fully capturing the nuances and complexities of its applications through a survey-based approach. The depth of understanding required to assess QC's impact accurately may not be fully attainable through the methods employed, potentially leading to oversimplified or incomplete interpretations of its current and potential applications.

By addressing these limitations, the study hopes to offer insightful information while recognizing the limitations of the research. The findings are trustworthy and significant thanks to the combination of strict methodologies and moral behavior, which advances our knowledge of QC in the future.

4. Results and Discussions

A summary of the demographic data gathered from survey respondents regarding the use of QC in diverse fields is shown in Table 1. Participants' marital status, age group, and gender are used to categorize the data. It provides insights into the varied demographic makeup of those participating in the study by displaying a distribution of respondents across age ranges, marital statuses, and gender identities. Understanding the viewpoints and possible biases in the survey results pertaining to the use of quantum computing requires an understanding of this demographic breakdown. Here table 1 elaborate Demographic information of employees for different condition.

Table 1: Demographic information of employees.

	No of participants	**Valid Percentages**
Gender		
Male	525	62.5
Female	315	37.5
Age		
18-30	567	67.5
31-50	257	30.5
>50	16	2
Marital status		
Married	233	27.7
Unmarried	607	72.3

The study also utilizes the use of QC in major fields. Figure 3 shows the utilization of quantum computing (QC) across three key domains: cryptography, material science, and machine learning. Cryptography is the leading application area, accounting for 42% of QC use due to its potential to break traditional cryptographic systems and develop quantum-resistant algorithms. Quantum algorithms like Shor's algorithm have significant implications for cryptography, enabling efficient factorization of large integers and posing challenges to widely-used cryptographic protocols. QC's research and development focus on securing data against potential quantum attacks and advancing post-quantum cryptographic methods. Material science follows closely, accounting for 38% of QC applications. QC's ability to handle complex quantum systems correlates with advancements in material discovery and the development of new materials with desirable properties. ML constitutes 20% of QC use, with quantum ML algorithms promising to speed up data processing and improve pattern recognition capabilities. The integration of QC with ML has the potential to revolutionize data analysis and interpretation, leading to more efficient and accurate predictive models.

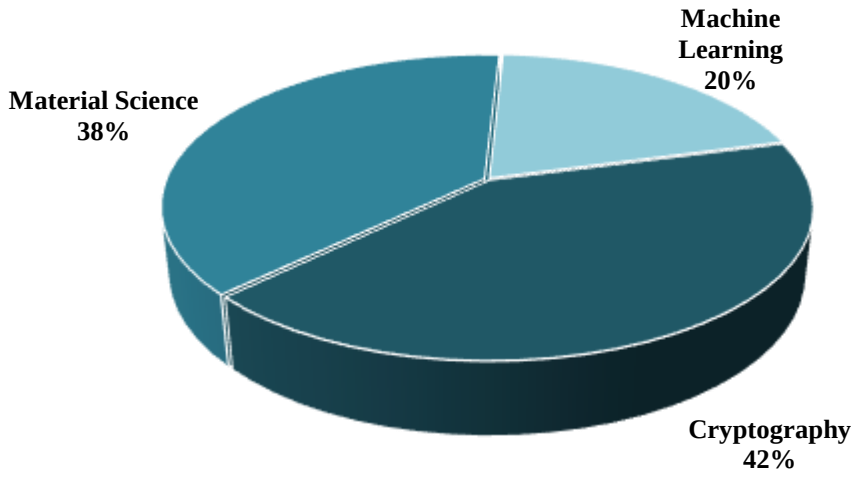

Figure 3: Use of Quantum Computing in major fields.

The survey reveals a majority of respondents, 38%, believe that Quantum Computers (QC) will enhance cryptographic systems' security and capabilities. 33% are confident, with a "Absolutely Yes" response, indicating their belief in QC's transformative potential. However, 10% are skeptical, with 5% disagreeing. The majority of respondents are optimistic about the role of QC in advancing cryptography, but a minority remain doubtful or unconvinced about its benefits. 14% of respondents did not provide an answer, suggesting uncertainty or a lack of knowledge on the subject matter. This data in figure 4 highlights the general optimism within the surveyed group about the future impact of QC on cryptography, but also highlights the need for further education or discussion to address lingering uncertainties.

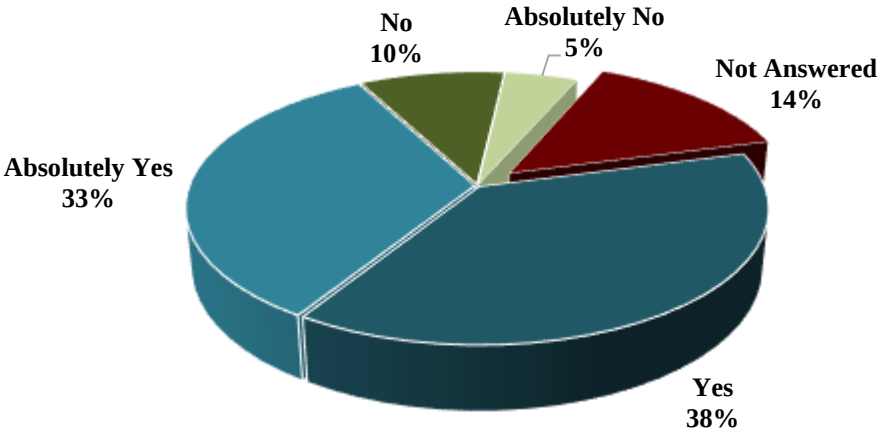

Figure 4: Respondents' belief on quantum computing for the advancement of cryptography.

The research question "I believe quantum computing is important for the advancement of fields such as material science, machine learning, and cryptography" was surveyed among respondents. The majority of respondents, 40%, strongly agree with the statement, indicating a strong understanding of its potential impact. However, 32% of respondents agree to some extent, indicating reservations or lack of confidence due to uncertainties in its practical application or existing technological limitations. A significant 16% chose not to answer, possibly due to a lack of knowledge about quantum computing. A minority, 9%, disagreed, indicating skepticism about the applicability of quantum computing to significantly advance these fields. The smallest segment, 3%, strongly disagreed, likely viewing quantum computing as irrelevant or too speculative to impact these fields. The overall distribution of figure 5 indicates a predominantly positive attitude towards the role of quantum computing in advancing key

scientific fields, with the majority of respondents either strongly agreeing or agreeing to some extent. The presence of dissenting views and non-responses highlights the ongoing debate and the need for further research and clarity in this emerging area.

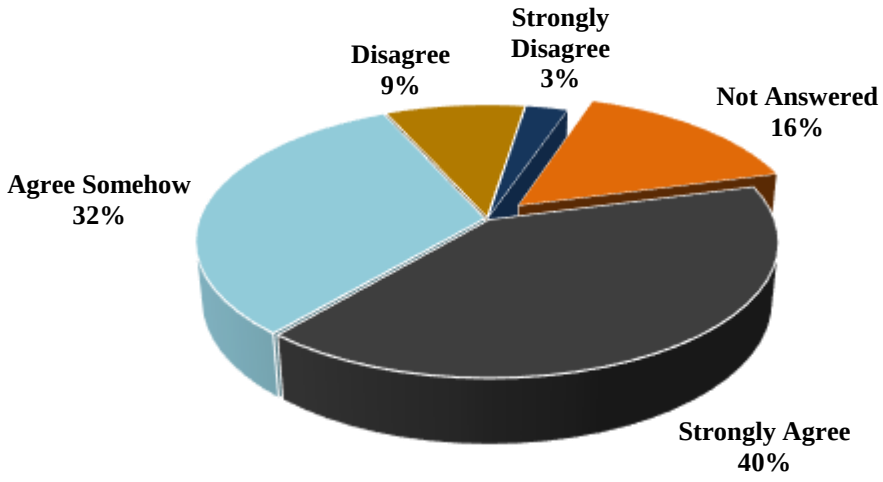

Figure 5: Response based on survey questions: "I believe quantum computing is important for the advancement of fields such as material science, ML, and cryptography."

From research and secondary data analysis, several important field effected by QC are further discussed.

4.1 Quantum Computing and cryptography

Cryptography, a crucial field in information technology, is essential for maintaining secrecy, integrity, authenticity, and non-repudiation in data transmission and storage. There are two types of cryptosystems: symmetric and asymmetric. The QC principle, first proposed by Richard Feynman in 1982, has been studied and is now seen as a potential threat to current asymmetric encryption. Symmetric cryptography may be vulnerable to certain quantum algorithms, but its security can be enhanced by using larger key spaces. Novel algorithms have been developed to circumvent current asymmetric cryptographic systems, such as elliptic curve encryption, which is vulnerable to quantum computers. As a result, there is a need for encryption algorithms that can withstand quantum computing.

- Symmetric cryptography involves the use of a shared secret key and cryptographic algorithm by both the sender and receiver to encrypt and decode data. However, maintaining the confidentiality of the key is crucial for exchanging secrets across public networks. Asymmetric cryptography, also known as public key cryptography, addresses this issue by using key pairs with distinct private and matching public keys. For example, Alice can encode a message using her mutually agreed upon secret key, while Bob can decode the message using the same cryptographic technique.
- Post-quantum cryptography (PQC) presents numerous challenges that researchers are diligently addressing. Quantum algorithms rely on probabilities, allowing quantum computers to generate multiple potential answers in a single operation, with only one being correct. However, the trial-and-error process used to measure and confirm the correct solution can undermine the speed advantages of QC. Qubits are highly error-prone and susceptible to high temperatures, ambient noise, and unintended electromagnetic interactions. Directly examining qubits for faults can disrupt their superposition state, causing the value to collapse.
- Maintaining coherence is another significant challenge. Qubits can only retain their quantum state for a short duration. Researchers at the University of New South Wales in Australia have developed two variations of a technology that, when integrated into a small silicon material called silicon 28, reduced magnetic interference, a common source of errors. They reported a Phosphorous atom precision of 99.99%, equating to an error rate of 1 in 10,000 quantum operations. To achieve long coherence times, qubits need to be isolated from their environment and kept at temperatures near absolute zero, which complicates their management without introducing additional interference.
- PQC aims to develop cryptographic systems impervious to attacks from both quantum and classical computers. In 2016, NIST called for algorithm submissions resistant to quantum attacks, receiving 82 proposals by the November 2017 deadline. In January 2018, NIST announced the results of the first round, with 59 encryption or key exchange methods and 23 signature techniques. The NSA has also announced plans to transition its encryption standards to PQC.

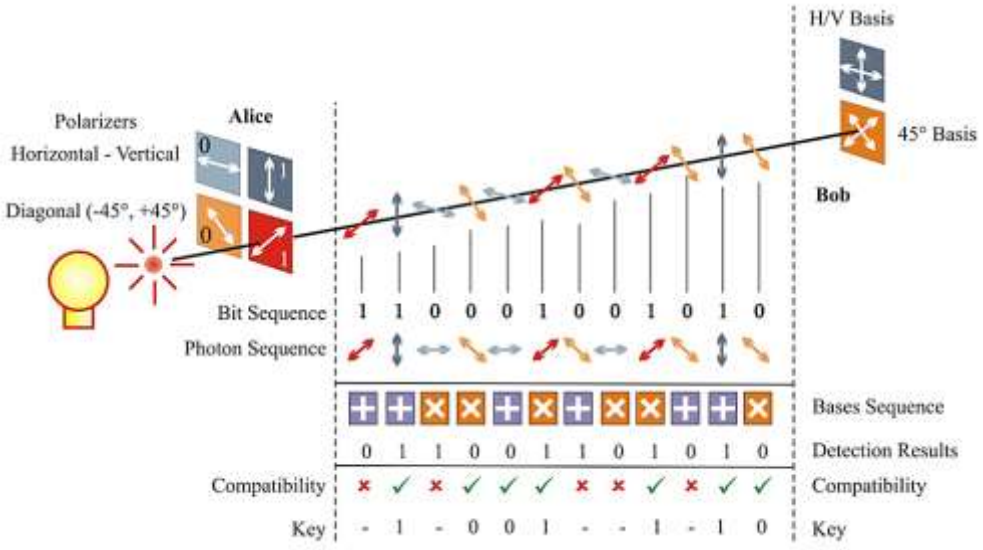

Figure 6: Process of QKD using the BB84 protocol (Durr et al., 2024).

- Quantum Key Distribution (QKD) addresses the secure sharing of cryptographic keys between parties over an insecure channel, utilizing quantum mechanics' properties that resist advances in computing power. QKD was first introduced by Charles Bennett and Gilles Brassard in 1984 with the BB84 protocol as shown in figure 6. Various QKD techniques have since been developed, primarily based on two principles: prepare-and-measure (P&M) methods and Entanglement-based (EB) protocols. Both techniques fall into three categories: discrete variable coding, continuous variable coding, and distributed phase reference coding, differing mainly in their detection methods.

4.2 Quantum Computing and Material Science

Materials science offers opportunities to improve existing materials and fabrication processes, as well as advance technology by identifying and developing new materials for quantum information devices. This involves developing accurate and scaleable fabrication processes. The NISQ era has revealed new challenges in multi-qubit systems and scaling up, but opportunities still exist. Acquiring a comprehensive understanding at the atomic level through synthesis, characterization, and theory/simulation will facilitate this progress. New types of dopants, such as acceptors, optically active dopants, and dopants with high-spin nuclei, can facilitate novel functionalities, such as controlling spin qubit arrays and reading out spin qubits optically. The performance of NV centers has significantly advanced, but challenges still exist. Investigating novel imperfections, such as the silicon-vacancy core, could unlock new functionalities that could impact modular or networked quantum systems.

Innovative concepts will reveal novel methods for storing quantum information in materials and electronics, especially for qubit modalities that have not been explored. Increased use of materials science tools and methodologies will be crucial for significant progress in these domains. Quantum information devices can be crucial for precise materials characterization due to their sensitivity to the surrounding environment.

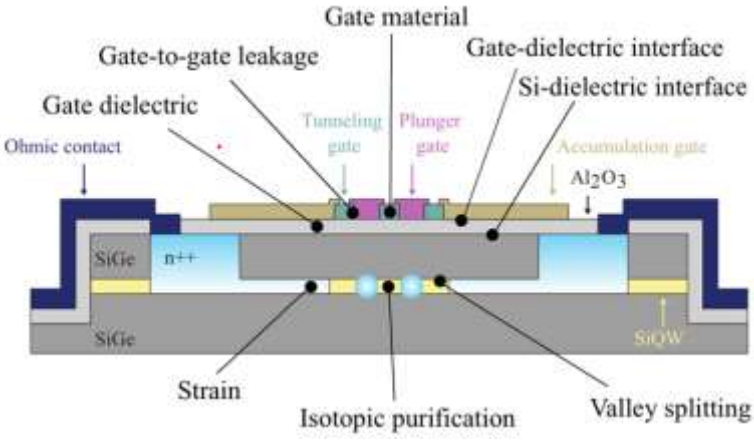

Figure 7: Example of material science application relevant to quantum computing (Lordi & Nichol, 2021).

Quantum-dot spin qubits, made from semiconductors, offer scalability but require specific processing. They face several materials science problems, including valley splitting, which is necessary for the states to be used as qubits. Large-scale manufacture is difficult due to tensile strain used to grow silicon quantum wells. The best quantum wells are generated using isotopically pure sources to reduce magnetic noise. Electrostatic potentials from overlapping gates restrict electrons. Design considerations like gate dielectric, gate metal, and inter-gate insulating layer also impact performance. All qubit devices have material selection, interface, flaw, and production issues. A detailed schematic of a silicon-germanium (SiGe) quantum well (SiQW) structure shown in Figure 7 indicates key components, including Ohmic contacts for electrical connectivity, gate dielectric for insulation, and gates for controlling quantum dot formation and manipulation. Strain and isotopic purification enhance electron mobility and coherence times. Valley splitting reduces energy level degeneracy for stable qubit operation.

4.3 Quantum Computing and Machine Learning

As quantum computing technologies become commercially available, it's crucial to consider potential applications. Machine learning (ML) is effective in solving challenging problems, such as image recognition, voice autonomous systems, medical applications, biology, and artificial intelligence. The scientific quantum information community is actively working on developing quantum algorithms to replace conventional ML routines. A graphic representation of QC assisted ML in sampling applications is shown in Figure 8. Some advantages of ML with QC can be discussed as:

- Unsupervised machine learning (ML) is a crucial tool for extracting information and structures from unlabeled data, such as images, videos, medical imaging, tweets, audio recordings, financial time series, and basic sensor data. Labeling can be costly and requires human specialists, making it essential to develop models and algorithms that can effectively extract information and structures from unlabeled data. Unsupervised techniques can acquire valuable representations of large dimensions with desired characteristics like simplicity and sparsity. When used with supervised methods like regressors and classifiers, unsupervised tools can significantly decrease the quantity of labeled data needed to achieve a desired level of generalization performance.
- Generative models are an unsupervised strategy that acquire knowledge about the combined probability of all variables related to an issue. They can be classified into explicit and implicit density estimators, which determine the method used to learn them. Explicit density estimators include models like Boltzmann machines, belief networks, and autoencoders, while implicit density estimators include models that include several layers of unobserved stochastic variables, known as hidden variables.

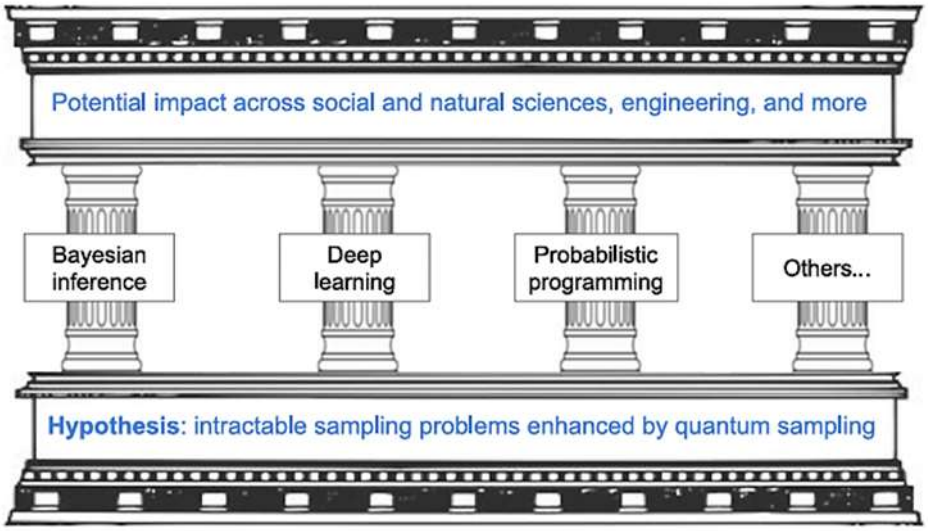

Figure 8: QC assisted ML in sampling applications(Perdomo-Ortiz et al., 2018).

- Quantum sampling has the potential to enhance intractable sampling problems across various scientific and engineering disciplines. Quantum computers containing just 50 qubits have shown potential to accelerate ML algorithms, but there is room for enhancement in other facets of ML and AI. Recent studies show that quantum mechanics may yield more succinct stochastic process models than classical ones, as measured by entropic complexity. This indicates that quantum models may greatly reduce the memory required to simulate a dataset.

- Statistical mechanics, a branch of science that emerged in the 19th century, has been beneficial in studying complex phenomena such as human behavior and developing high-performance algorithms. It has had a significant impact on the advancement of ML, with the Boltzmann machine serving as a notable example.

5. Conclusion

This paper explores the applications of quantum computing (QC) in cryptography, material science, and machine learning (ML), revealing its profound implications for these fields. The research demonstrates that QC, with its unparalleled computational capabilities, is poised to surpass classical methods, driving significant advancements across these sectors. In cryptography, 42% of current QC applications are directed towards this field, underscoring its critical importance. Quantum-resistant cryptographic methods are urgently needed to safeguard data security in the coming quantum era. Material science, representing 38% of QC applications, stands to benefit immensely from quantum simulations that allow for precise modeling of molecular and atomic interactions. The transformative impact of QC can have on industries ranging from pharmaceuticals to energy, where the development of novel materials is crucial. Quantum ML algorithms could revolutionize data processing and pattern recognition, leading to more efficient and accurate predictive models. A significant 73% of respondents believe in the importance of QC for advancing fields such as cryptography, material science, and ML. However, 10% disagreement and 16% non-responses suggest some skepticism and uncertainty remain, highlighting the need for continued research, education, and dialogue in this rapidly evolving field. Quantum computing presents several challenges that researchers are actively addressing. These include the reliance on probabilities in QC algorithms, the proneness of qubits to mistakes due to high temperatures, ambient noise, and unintended electromagnetic interactions, and the complexity of achieving coherence. Researchers from the University of New South Wales in Australia have successfully developed two distinct variations of a technology, mitigating magnetic interference and maintaining superposition for 35 seconds. However, managing qubits without generating further interference presents challenges.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1] Anukool, W., Lim, J., Song, Y., & Ahn, J. (2018). Quantum Computing Systems: A Brief Overview. *Journal of the Korean Physical Society*, *73*(6), 841-845. https://doi.org/10.3938/jkps.73.841

[2] Arslan, B., Ulker, M., Akleylek, S., & Sagiroglu, S. (2018). A study on the use of quantum computers, risk assessment and security problems. 2018 6th International Symposium on Digital Forensic and Security (ISDFS),

[3] Babikian, J. (2017). Navigating the Legal Landscape: Regulations for Artificial Intelligence, Quantum Computing, and Blockchain. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(1), 1-16.

[4] Bennett, C. H., & Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, *560*, 7-11. https://doi.org/https://doi.org/10.1016/j.tcs.2014.05.025

[5] Bennett, C. H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., & Wootters, W. K. (1993). Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical review letters*, *70*(13), 1895-1899. https://doi.org/10.1103/PhysRevLett.70.1895

[6] Chawla, D., & Mehra, P. S. (2023). A roadmap from classical cryptography to post-quantum resistant cryptography for 5G-enabled IoT: Challenges, opportunities and solutions. *Internet of Things*, *24*, 100950. https://doi.org/https://doi.org/10.1016/j.iot.2023.100950

[7] Ciliberto, C., Herbster, M., Ialongo, A. D., Pontil, M., Rocchetto, A., Severini, S., & Wossnig, L. (2018). Quantum machine learning: a classical perspective. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *474*(2209), 20170551.

[8] Dhawan, S., Gupta, B. M., & Bhusan, S. (2018). Global Publications Output in Quantum Computing Research: A Scientometric Assessment during 2007-16. *Emerging Science Journal*, *2*. https://doi.org/10.28991/esj-2018-01147

[9] Dinur, I., Dolev, S., & Lodha, S. (2018). *Cyber Security Cryptography and Machine Learning*. Springer.

[10] DiVincenzo, D., & Ibm. (2000). The Physical Implementation of Quantum Computation. *Fortschritte der Physik*, *48*. https://doi.org/10.1002/1521-3978(200009)48:9/113.0.CO;2-E

[11] Dunjko, V., & Briegel, H. J. (2018). Machine learning & artificial intelligence in the quantum domain: a review of recent progress. *Reports on Progress in Physics*, *81*(7), 074001.

[12] Durr, E. S., Imran, M., Altamimi, A., Khan, W., Hussain, S., & Alsaffar, M. (2024). Quantum Cryptography for Future Networks Security: A Systematic Review. *IEEE Access*, *PP*, 1-1. https://doi.org/10.1109/ACCESS.2024.3504815

[13] Feynman, R. P. (1986). Quantum mechanical computers. *Foundations of Physics*, *16*(6), 507-531. https://doi.org/10.1007/BF01886518

[14] Gatla, T. R. (2018). AN EXPLORATIVE STUDY INTO QUANTUM MACHINE LEARNING: ANALYZING THE POWER OF ALGORITHMS IN QUANTUM COMPUTING. *International Journal of Emerging Technologies and Innovative Research (www. jetir. org), ISSN*, 2349-5162.

[15] Gheorghiu, A., Kapourniotis, T., & Kashefi, E. (2019). Verification of Quantum Computation: An Overview of Existing Approaches. *Theory of Computing Systems*, *63*(4), 715-808. https://doi.org/10.1007/s00224-018-9872-3

[16] Golestan, S., Habibi, M. R., Mousazadeh Mousavi, S. Y., Guerrero, J., & Vasquez, J. (2023). Quantum computation in power systems: An overview of recent advances. *Energy Reports*, *9*, 584-596. https://doi.org/10.1016/j.egyr.2022.11.185

[17] Grimes, R. A. (2019). *Cryptography apocalypse: preparing for the day when quantum computing breaks today's crypto*. John Wiley & Sons.

[18] Harrow, A., Hassidim, A., & Lloyd, S. (2009). Quantum Algorithm for Linear Systems of Equations. *Physical review letters*, *103*, 150502. https://doi.org/10.1103/PhysRevLett.103.150502
[19] Hidary, J. D., & Hidary, J. D. (2019). *Quantum computing: an applied approach* (Vol. 1). Springer.
[20] Himanen, L., Geurts, A., Foster, A. S., & Rinke, P. (2019). Data-driven materials science: status, challenges, and perspectives. *Advanced Science*, *6*(21), 1900808.
[21] Hu, F., Wang, B. N., Wang, N., & Wang, C. (2019). Quantum machine learning with D-wave quantum computer. *Quantum Engineering*, *1*(2), e12.
[22] Jhanwar, A., & Nene, M. (2021). *Enhanced Machine Learning using Quantum Computing*. https://doi.org/10.1109/ICESC51422.2021.9532638
[23] Kitaev, A. Y. (2003). Fault-tolerant quantum computation by anyons. *Annals of Physics*, *303*(1), 2-30. https://doi.org/https://doi.org/10.1016/S0003-4916(02)00018-0
[24] Lamba, A., Pal, P., Singh, S., Singh, B., & Muni, S. S. R. (2018). Quantum computing technology (QCT)-a data security threat.
[25] Liu, J., Spedalieri, F. M., Yao, K.-T., Potok, T. E., Schuman, C., Young, S., Patton, R., Rose, G. S., & Chamka, G. (2018). Adiabatic quantum computation applied to deep learning networks. *Entropy*, *20*(5), 380.
[26] Lordi, V., & Nichol, J. M. (2021). Advances and opportunities in materials science for scalable quantum computing. *MRS Bulletin*, *46*(7), 589-595. https://doi.org/10.1557/s43577-021-00133-0
[27] Lubasch, M., Joo, J., Moinier, P., Kiffner, M., & Jaksch, D. (2019). *Variational Quantum Algorithms for Nonlinear Problems*. https://doi.org/10.48550/arXiv.1907.09032
[28] Möller, M., & Vuik, C. (2017). On the impact of quantum computing technology on future developments in high-performance scientific computing. *Ethics and information technology*, *19*, 253-269.
[29] Nawaz, S. J., Sharma, S. K., Wyne, S., Patwary, M. N., & Asaduzzaman, M. (2019). Quantum machine learning for 6G communication networks: State-of-the-art and vision for the future. *IEEE access*, *7*, 46317-46350.
[30] Nejatollahi, H., Dutt, N., Ray, S., Regazzoni, F., Banerjee, I., & Cammarota, R. (2019). Post-Quantum Lattice-Based Cryptography Implementations: A Survey. *ACM Computing Surveys*, *51*, 1-41. https://doi.org/10.1145/3292548
[31] Neven, H., Google, Denchev, V., Drew-Brook, M., Zhang, J., & Macready, W. (2010). NIPS 2009 Demonstration: Binary Classification using Hardware Implementation of Quantum Annealing.
[32] Orús, R., Mugel, S., & Lizaso, E. (2019). Quantum computing for finance: Overview and prospects. *Reviews in Physics*, *4*, 100028. https://doi.org/https://doi.org/10.1016/j.revip.2019.100028
[33] Perdomo-Ortiz, A., Benedetti, M., Realpe-Gomez, J., & Biswas, R. (2018). Opportunities and challenges for quantum-assisted machine learning in near-term quantum computers. *Quantum Science and Technology*, *3*. https://doi.org/10.1088/2058-9565/aab859
[34] Peruzzo, A., McClean, J., Shadbolt, P., Yung, M.-H., Zhou, X.-Q., Love, P. J., Aspuru-Guzik, A., & O'Brien, J. L. (2014). A variational eigenvalue solver on a photonic quantum processor. *Nature Communications*, *5*(1), 4213. https://doi.org/10.1038/ncomms5213
[35] Peruzzo, A., McClean, J., Shadbolt, P., Yung, M. H., Zhou, X. Q., Love, P. J., Aspuru-Guzik, A., & O'Brien, J. L. (2014). A variational eigenvalue solver on a photonic quantum processor. *Nat Commun*, *5*, 4213. https://doi.org/10.1038/ncomms5213
[36] Phillipson, F. (2020). *Quantum Machine Learning: Benefits and Practical Example*.
[37] Schuld, M., & Petruccione, F. (2018). *Supervised learning with quantum computers* (Vol. 17). Springer.
[38] Vogel, M. (2011). Quantum Computation and Quantum Information, by M.A. Nielsen and I.L. Chuang. *Contemporary Physics - CONTEMP PHYS*, *52*, 604-605. https://doi.org/10.1080/00107514.2011.587535