University
Logo

Explore Specific Applications of Quantum Computing in Fields Such as Cryptography, Material Science, And Machine Learnng

Full name of author*

Affiliation*

Name of department, Name of University, Country

Full name of Supervisor*

Affiliation*

Name of department, Name of University, Country

- Month 2024 –

C5K Research Publishing

website: https://www.c5k.com

DECLARATION

This thesis, entitled "Explore Specific Applications of Quantum Computing in Fields Such as Cryptography, Material Science, and Machine Learning," has not been previously submitted for any degree or professional qualification at any other academic institution or university. I, hereby, declare that it is entirely my own work. All references, sources, and contributions from others have been appropriately cited.

I attest that the data presented in this thesis are original and that all conclusions drawn are solely mine. Furthermore, I confirm that the text adheres to the norms and regulations governing academic research, particularly in terms of ethical considerations..

Statement of Originality and Author Details

Statement of Originality

The Statement of Originality is a formal assertion by the author that the thesis represents their own independent work and has not been previously submitted for any other degree or qualification.

The Author Details section provides personal and academic information about the author. This section typically includes:

Full Name: The author's full legal name.

Institutional Affiliation: The name of the institution where the research was conducted.

Department: The specific department or faculty within the institution.

Degree Program: The degree for which the thesis is submitted (e.g., Master of Science, Doctor of Philosophy).

Contact Information: Optional inclusion of email address or other contact details.

Brief Biography: A short academic biography may be included, outlining the author's educational background, research interests, and any relevant professional experience.

ACKNOWLEDGEMENT

The completion of this research would not have been possible without the invaluable advice and support of my advisors, to whom I am eternally grateful. Their support and constructive criticism have been invaluable in helping me develop as a researcher and have a profound impact on my work. I am incredibly grateful to my family for their constant encouragement and empathy during this ordeal. I was able to overcome obstacles because of the support and encouragement I received from their love and faith in me. In addition, I want to express my deepest gratitude to my friends, whose friendship and encouragement have been priceless. Their unfailing support and tolerance have been an inspiration to me. Without the help of these extraordinary people, this study would not have been feasible; for their generosity, I am eternally grateful.

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 clearly 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.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction

1.1 Background and Context

Classical computers have been around for a long time and have played a crucial role in driving scientific progress. However, quantum computing (QC) has recently shown promising results in addressing complex, large-scale problems. Quantum computers operate by leveraging quantum mechanics principles such as superposition and entanglement, which allow for the creation of exponentially increasing states as the number of qubits, or quantum bits, grows (Bova et al., 2021). While classical computers use binary bits represented as 0 and 1 to store information, quantum computers take advantage of the probabilistic nature of quantum states before measurement. This enables them to process significantly more data compared to traditional computers. Quantum computers perform operations using qubits, which are derived from the quantum state of an object, rather than the binary bits used by classical computers (Hassija et al., 2020). These qubits, due to their quantum properties, exhibit phenomena like superposition, which allows a quantum system to exist in multiple states at once, and entanglement, which creates a highly correlated relationship between quantum particles. These characteristics give quantum computers an advantage in performing complex calculations that are either impossible or would take an extremely long time for classical systems to achieve (Hassija et al., 2020). The potential of QC to drastically reduce the time and space complexity of various algorithms, such as those for solving linear systems of equations, has sparked significant interest among researchers (Harrow et al., 2009). This advancement, however, poses a growing threat to data security, as many encryption methods rely on the difficulty of the mathematical problems they employ. Classical computers, with their limited computational power, have been unable to provide optimal solutions to these problems within a reasonable timeframe. However, with the advent of QC, encryption now faces a serious risk (Bernstein & Lange, 2017). Progress in PQC offers hope for securely transitioning all encrypted data to these 'quantum-safe' systems. Additionally, quantum simulation, a particularly exciting area within QC, holds great promise for unraveling the complex nature of molecular and chemical interactions, potentially leading to the development of new treatments and materials. (Nejatollahi et al., 2019).

1.2 Difference Between Quantum and Classical Computing

Richard Feynman introduced the quantum computer in 1982. Quantum mechanics studies exceedingly tiny physical occurrences and their characteristic features. Traditional computing uses bits, which can only be 0 or 1. Instead, quantum computers use qubits (Nielsen & Chuang, 2010). Qubits may superpose in both the 0 and 1 states, making them unique. When seen, a qubit collapses into one of these states. Quantum computers solve complicated issues using this skill. A qubit's superposition operation affects both potential values simultaneously. Quantum computing also uses entanglement. Entangled qubits constitute a single system with four states. Regardless of distance, a change in one entangled qubit's state would instantly affect the other, allowing real parallel computing (Jozsa, 1997). These quantum phenomena increase the number of values that may be processed in a single operation exponentially as the number of entangled qubits rises. Thus, a quantum computer with n qubits may execute 2^n operations concurrently. Universal and non-universal quantum computers exist. Universal quantum computers can perform any work, but non-universal ones are optimized for particular purposes like ML algorithm optimization. D-Wave's non-universal quantum computer has more than 2,000 qubits, whereas IBM's universal quantum computer has 17 qubits with improved error correcting (Tichy, 2017). Both D-Wave and IBM offer online access to their quantum computers for research purposes. In October 2017, Intel and QuTech unveiled a 17-qubit global quantum computer (Soeken et al., 2018). According to Bone and Castro (1997) quantum computers have a different design than conventional computers, which use transistors and diodes. Researchers have made quantum computing liquids and quantum dots, which are electrons in superposition. They also emphasized that quantum computers outperform conventional computers only when coupled with quantum parallelism methods. Quantum computers may not multiply faster than conventional computers.

1.3 Fundamental of Quantum Computing

QC relies on the principles of quantum phenomena to address intricate computational problems. QC research is simultaneously enhancing our basic comprehension of quantum phenomena and striving to usher in a new age of expedited computing, while also influencing the trajectory of technological progress in the 21st century (Kanamori & Yoo, 2020).

QC is currently a developing technology that requires expertise from several multidisciplinary domains, including physicists, computer scientists, mathematicians, chemists, and engineers. Academics and industry researchers must collaborate to address technical and management challenges associated with implementing this state-of-the-art computational technology. Scientists worldwide are engaged in a mission to enhance the performance of quantum hardware, creating and refining quantum algorithms, and tackling the many obstacles in order to make quantum computers a reality. The five essential stages for QC machines, as depicted in Fig. 1 (DiVincenzo, 2000), are the initialization of quantum states, the preservation of qubit information with extended functional ability, the achievement of efficient decoherence time, the implementation of a universal quantum gate architecture, and the accuracy of qubit measurement capability.

.

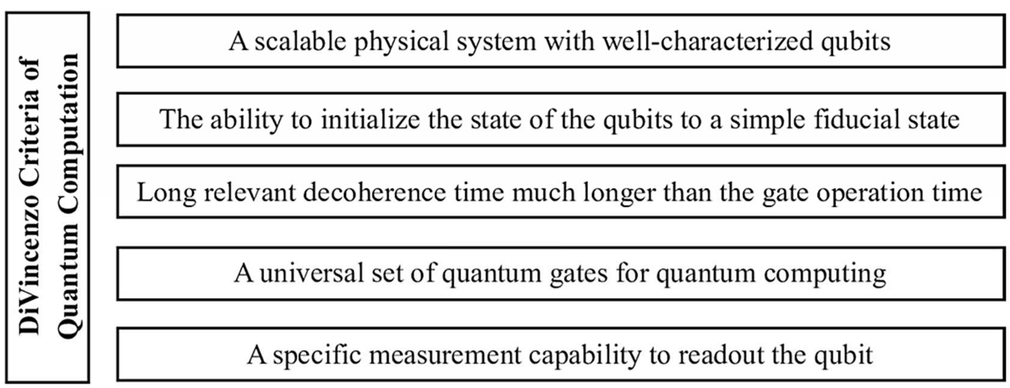

Fig 1. Quantum computing's fundamental stages (DiVincenzo, 2000).

1.4 Objective of this study

The objective of this study is to systematically investigate and elucidate the specific applications of quantum computing (QC) in the domains of cryptography, material science, and ML. This study is designed to accomplish the following key objectives:

- To explore and document how QC is currently being applied in the fields of cryptography, material science, and ML.
- To conduct an empirical survey to quantify the actual extent of QC adoption within these fields. By gathering and analyzing data from practitioners, researchers, and industry professionals, this study seeks to provide an accurate representation of how widely QC is being implemented and its perceived effectiveness in various real-world scenarios.

- To assess the perceptions of stakeholders regarding the potential and effectiveness of QC in cryptography, material science, and ML.
- Finally, the study will identify gaps in the current application of QC in the selected fields and propose directions for future research.

1.5 Thesis Outline

This thesis, "Explore Specific Applications of QC in Fields Such as Cryptography, Material Science, and ML," is structured into eight chapters.

Chapter 1 provides an introduction to the subject, outlining the significance of quantum computing and the objectives of the research. Chapter 2 offers a comprehensive literature review, exploring existing studies on quantum computing and its applications. Chapter 3 details the research methodology employed in this study. Chapters 4, 5, and 6 delve into the specific applications of quantum computing in cryptography, material science, and ML, respectively, providing an in-depth analysis of how quantum computing can revolutionize these fields. Chapter 7 presents the findings and analysis, drawing connections between the research objectives and outcomes. Finally, Chapter 8 concludes the thesis by discussing the challenges encountered, summarizing key insights, and offering recommendations for future research.