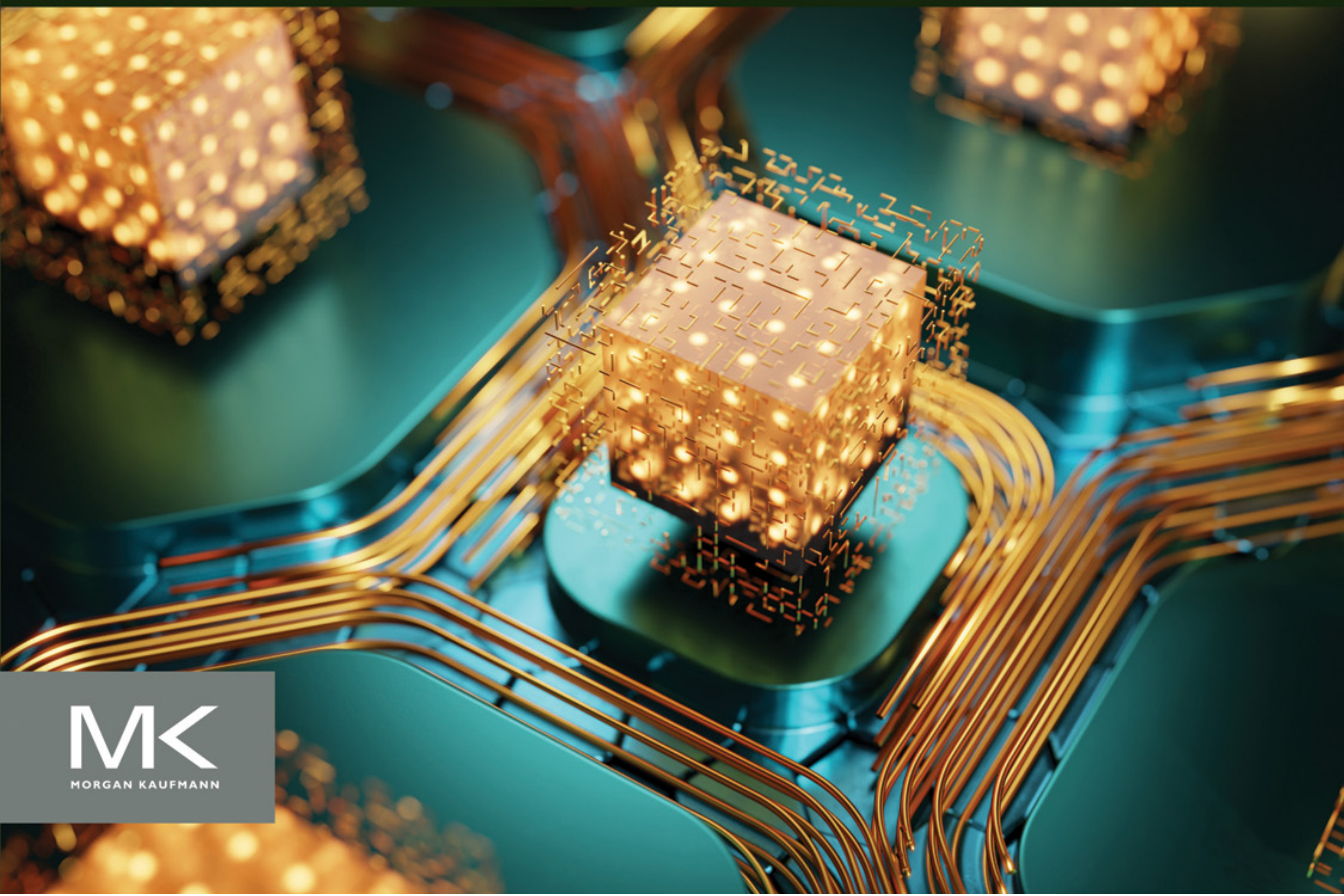
QUANTUM COMPUTING

Principles and Paradigms

Edited by
Rajkumar Buyya and Sukhpal Singh Gill



MORGAN KAUFMANN

Quantum Computing

This page intentionally left blank

Quantum Computing
Principles and Paradigms

Edited by

Rajkumar Buyya
Quantum Cloud Computing and Distributed Systems (qCLOUDS) Laboratory,
School of Computing and Information Systems,
The University of Melbourne, Parkville, VIC, Australia

Sukhpal Singh Gill
School of Electronic Engineering and Computer Science,
Queen Mary University of London, London, United Kingdom

ELSEVIER
MORGAN KAUFMANN

Morgan Kaufmann is an imprint of Elsevier
50 Hampshire Street, 5th Floor, Cambridge, MA 02139, United States

ISBN: 978-0-443-29096-1

For Information on all Morgan Kaufmann publications
visit our website at https://www.elsevier.com/books-and-journals

Publisher: Mara Conner
Acquisitions Editor: Chris Katsaropoulos
Editorial Project Manager: Himani Dwivedi
Production Project Manager: Punithavathy Govindaradjane
Cover Designer: Christian Bilbow

Typeset by MPS Limited, Chennai, India

Contents

List of contributors

Ajith Abraham Sai University, Chennai, Tamil Nadu, India; Machine Intelligence Research Labs, Auburn, WA, United States

Karmel Arockiasamy School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, Tamil Nadu, India

Priyansh Arora Microsoft, Schiphol, Netherlands

Rami Bahsoon School of Computer Science, University of Birmingham, Birmingham, United Kingdom

Rajkumar Buyya Quantum Cloud Computing and Distributed Systems (qCLOUDS) Laboratory, School of Computing and Information Systems, The University of Melbourne, Parkville, VIC, Australia

Oktay Cetinkaya Oxford e-Research Centre (OeRC), Department of Engineering Science, University of Oxford, Oxford, United Kingdom

K. Chandrasekaran Computer Science and Engineering Department, National Institute of Technology Karnataka, Surathkal, Karnataka, India

Daniel Claudino Quantum Information Science Section, Oak Ridge National Laboratory, Oak Ridge, TN, United States

Ahmed Farouk Department of Computer Science, Faculty of Computers and Artificial Intelligence, Hurghada University, Hurghada, Egypt

Soumya K. Ghosh Department of Computer Science and Engineering, Indian Institute of Technology, Kharagpur, West Bengal, India

Sukhpal Singh Gill School of Electronic Engineering and Computer Science, Queen Mary University of London, London, United Kingdom

Muhammed Golec School of Electronic Engineering and Computer Science, Queen Mary University of London, London, United Kingdom; School of Computer Engineering, Abdullah Gul University, Kayseri, Turkey

Emir Sahin Hatay School of Computer Science and Electronic Engineering, University of Essex, Colchester, United Kingdom

David Haunschild Detecon International GmbH, Munich, Germany

Mohammed Suhail Hussain School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, Tamil Nadu, India

Girija Jagannath Computer Science and Engineering, Bangalore Institute of Technology, Bangalore, Karnataka, India

Salil S. Kanhere School of Computer Science and Engineering, The University of New South Wales (UNSW), Sydney, NSW, Australia

G. Kanimozhi Centre for Smart Grid Technologies, Vellore Institute of Technology, Chennai, Tamil Nadu, India

Kamalpreet Kaur Cymax Group Technologies, Burnaby, BC, Canada

Bhanu Prakash Kolla Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India

Dilip Krishnaswamy Quantum Walks Technologies, Morris Plains, NJ, United States

Antonin Lefevre Université de Reims Champagne-Ardenne, Département de sciences exactes et naturelles, Reims, France

Ji Liu Mathematics and Computational Research Division, Argonne National Laboratory, Lemont, IL, United States

Xiaoyuan Liu Quantum Laboratory, Fujitsu Research of America, Inc., Santa Clara, CA, United States

Hanan Lutfiyya Department of Computer Science, University of Western Ontario, London, ON, Canada

Sree Pragna Machupalli Information Networking Institute, Carnegie Mellon University, Pittsburgh, PA, United States

Ying Mao Department of Computer and Information Science, Fordham University, New York City, NY, United States

Stefano Marrone Dipartimento di Matematica e Fisica, Università della Campania "Luigi Vanvitelli," Caserta, Italy

Hoa T. Nguyen Quantum Cloud Computing and Distributed Systems (qCLOUDS) Laboratory, School of Computing and Information Systems, The University of Melbourne, Parkville, VIC, Australia

Carlo Ottaviani Department of Computer Science and York Centre for Quantum Technologies, University of York, York, United Kingdom

Panos Patros Raygun Performance Monitoring, Wellington, New Zealand

Y.V.R. Naga Pawan Department of Computer Science and Engineering, Anurag Engineering College, Ananthagiri, Telangana, India

Bui Binh An Pham Quantum Cloud Computing and Distributed Systems (qCLOUDS) Laboratory, School of Computing and Information Systems, The University of Melbourne, Parkville, VIC, Australia

Junaid Qadir Department of Computer Science and Engineering, College of Engineering, Qatar University, Doha, Qatar

Kotagiri Ramamohanarao The University of Melbourne, Parkville, VIC, Australia

Omer Rana School of Computer Science and Informatics, Cardiff University, Cardiff, United Kingdom

Rizos Sakellariou Department of Computer Science, University of Manchester, Manchester, United Kingdom

Leon Schlote DB Cargo, Berlin, Germany

Manmeet Singh Jackson School of Geosciences, University of Texas at Austin, Austin, TX, United States

Houbing Herbert Song Department of Information Systems, University of Maryland, Baltimore County (UMBC), Baltimore, MD, United States

Tony Thomas School of Computer Science and Engineering, Kerala University of Digital Sciences, Innovation, and Technology, Thiruvananthapuram, Kerala, India

Steve Uhlig School of Electronic Engineering and Computer Science, Queen Mary University of London, London, United Kingdom

Muhammad Usman School of Physics, The University of Melbourne, Parkville, VIC, Australia; Data61, CSIRO, Clayton, VIC, Australia

Sumitha Valsalam School of Computer Science and Engineering, Kerala University of Digital Sciences, Innovation, and Technology, Thiruvananthapuram, Kerala, India

Roisan Wahlang Computer Science and Engineering Department, National Institute of Technology Karnataka, Surathkal, Karnataka, India

Huaming Wu Center for Applied Mathematics, Tianjin University, Tianjin, China

Minxian Xu Shenzhen Institute of Advanced Technology, Chinese Academy of Sciences, Shenzhen, China

This page intentionally left blank

About the editors

Dr. Rajkumar Buyya is a Redmond Barry Distinguished Professor and Director of the Quantum Cloud Computing and Distributed Systems (qCLOUDS) Laboratory at the University of Melbourne, Australia. He is also serving as the founding CEO of Manjrasoft, a spin-off company of the University of Melbourne, commercializing its innovations in cloud computing. He has authored over 850 publications and seven textbooks, including *Mastering Cloud Computing* published by McGraw Hill, China Machine Press, and Morgan Kaufmann for Indian, Chinese, and international markets, respectively. He is one of the highly cited authors in computer science and software engineering worldwide (h-index171 g-index369, and 158,000 citations). He has graduated 60 PhD students who are working in world-leading research universities and high-tech companies such as Microsoft, Google, and IBM. He has been recognized as IEEE Fellow, a "Web of Science Highly Cited Researcher" for seven times since 2016, the "Best of the World" twice for research fields (in Computing Systems in 2019 and Software Systems in 2021/2022/2023) as well as "Lifetime Achiever" and "Superstar of Research" in "Engineering and Computer Science" discipline twice (2019 and 2021) by the Australian Research Review. Software technologies for grid, cloud, and fog computing developed under Dr.Buyya's leadership have gained rapid acceptance and are in use at several academic institutions and commercial enterprises in 50 countries around the world. Manjrasoft's Aneka Cloud technology developed under his leadership has received the "Frost New Product Innovation Award." He served as a founding Editor-in-Chief of the *IEEE Transactions on Cloud Computing*. He is currently serving as an Editor-in-Chief of *Software: Practice and Experience*, a long-standing journal in the field established 54 years ago. He has presented over 750 invited talks (keynotes, tutorials, and seminars) on his vision of IT Futures, Advanced Computing technologies, and Spiritual Science at international conferences and institutions in Asia, Australia, Europe, North America, and South America. He has recently been recognized as a fellow of the Academy of Europe.

Affiliations and expertise
The University of Melbourne, Australia

Dr. Sukhpal Singh Gill is a fellow of the Higher Education Academy (FHEA) and an Assistant Professor in Cloud Computing at the School of Electronic Engineering and Computer Science, Queen Mary University of London, UK. He has coauthored 220 peer-reviewed papers (with Citations 13000 and H-index 55) and has published in prominent international journals and conferences such as *IEEE TCC, IEEE TSC, IEEE TSUSC, IEEE TCE, ACM TOIT, IEEE TII, IEEE TNSM, IEEE IoT Journal, Elsevier JSS/FGCS, IEEE/ACM UCC, and IEEE CCGRID*. He is serving as an Editor-in-Chief for *IGI Global IJAEC* and Area Editor for Springer *Cluster Computing*

Journal, also serving as an Associate Editor in *IEEE IoT Journal*, *Nature Scientific Reports*, *Elsevier IoT Journal*, *Wiley SPE Journal*, Wiley *ETT Journal*, *Elsevier TELER*, and *IET Networks Journal*. He has received several awards, including the Queen Mary University Education Excellence Award 2023, Outstanding Reviewer Award from IEEE IT Professional Magazine 2024, Elsevier Internet of Things Editor's Choice Award 2024, Elsevier Best Paper Award 2023, Distinguished Reviewer Award from SPE (Wiley), and Best Paper Award AusPDC at ACSW 2021 and has also served as the PC member for top conferences such as PerCom, UCC, CCGRID, PDP, CLOUDS, ICFEC, and AusPDC. He has edited and authored research on various books for Elsevier, Springer, and CRC Press. His research interests include cloud computing, edge computing, software engineering, Internet of things, and energy efficiency. For further information, please visit http://www.ssgill.me.

Affiliations and expertise

Queen Mary University of London, United Kingdom

Preface

Quantum computing (QC) is an emerging computing paradigm, with enormous potential to offer disruptive computational capabilities. It can revolutionize many areas of science, commerce, and industry, including data science, drug discovery, particle physics, materials design, and optimization tasks. This book aims to cover a broad range of topics, providing an up-to-date and comprehensive reference of the rapid progress in the field of QC and related technologies from major international companies (such as IBM, Google, Intel, Rigetti, Q-Control) and academic researchers.

To realize the full potential of QC, researchers and practitioners need to address several challenges and develop suitable conceptual and technological solutions for tackling them. They include the development of scalable and error-free architectures, quantum noise characterization and mitigation strategies, application programming models, quantum resource management systems, quantum application schedulers, and cloud computing integration systems. This book covers a broad range of comprehensive topics in the field of QC, including quantum simulations, algorithms, quantum–classical hybrid machine learning, quantum key distribution, quantum Internet, and quantum applications. It also discusses emerging topics such as quantum machine learning (QML) and quantum cloud computing.

The primary purpose of this book is to capture the state-of-the-art in QC architectures, technologies, and their applications. This book also aims to identify potential research directions and technologies that will facilitate insight generation in various application domains. We expect the book to serve as a reference for a larger audience such as system architects, practitioners, developers, new researchers, and graduate-level students.

With these basic goals, the book is composed of 12 chapters and the contributions are divided into three parts:

1. Vision and Applications
2. Architecture, Systems, and Services
3. New Trends and Emerging Topics

Part 1 focuses on Vision and Applications and is made up of four chapters. Chapter1 discusses the fundamental concepts of QC, including QC algorithms, quantum gates, quantum key distribution, quantum software tools, and QC applications. Chapter 2 examines the foundations and vision based on current research in this area. This chapter delves into the most recent advancements in quantum computer hardware, as well as the subsequent progress in quantum cryptography, quantum software, and high-scalability quantum computers. Finally, it highlights numerous potential challenges and exciting new trends for quantum technology research and development, fostering a wider discussion. Chapter 3 focuses on quantum simulations, algorithms, and the fundamental idea of quantum supremacy as it analyzes the intricate relationship between QC and classical machine learning (CML). This chapter provides an inclusive analysis of several quantum algorithms, their ramifications, and their incorporation into hybrid quantum–CML paradigms. Chapter 4 examines the current state of postquantum cryptography methods as well as their future prospects. It also seeks to delve into the workings of these various methods, their effectiveness, efficiency, strengths, and weaknesses. The primary purpose of this chapter is to investigate these various methods and their implementations, evaluate their feasibility, compare them with one another, and help the reader understand cryptography in the age of QC.

Part 2 focuses on Architecture, Systems, and Services and is made up of five chapters. Chapter 5 delves into the utilization of quantum annealing to bolster efficiency in high-frequency trading. Through the application of QC algorithms within a quantum cloud environment, the research aims to evaluate trade execution speed and complexity. Quantum annealing's potential is explored within the quantum cloud, where the scalability and computational efficiency of the algorithm in high-frequency trade execution are assessed. Through comprehensive analysis and comparative evaluation, the study aims to quantify the enhancement in execution speed and reduction in trade complexity achieved through quantum annealing. Chapter 6 looks into whether it is possible to reduce the number of dimensions by using an autoencoder neural network on lattice-based keys made by the Kyber key encapsulation mechanism scheme. Moreover, this work also presents a comparative analysis of the different implemented autoencoder models to showcase their relative performance. Chapter 7 bridges this gap by elucidating and implementing Q-means within a hybrid quantum–classical framework. This chapter begins by providing a comprehensive overview of the K-means and d-Kmeans clustering models. Then, it talks about quantum distance computation, finding the quantum minimum in a list, and QMeans, which is the quantum version of the K-means initialization method. It also discusses their mathematical forms, circuit designs, and their application with Qiskit. Finally, these elements are assembled to formulate the QMeans algorithm. Chapter 8 introduces the concept of serverless QC with examples using QFaaS, a practical Quantum Function-as-a-Service framework. This framework utilizes the serverless computing model to simplify quantum application development and deployment by abstracting the complexities of quantum hardware and enhancing application portability across different quantum software development kits and quantum backends. This chapter provides comprehensive documentation and guidelines for deploying and using QFaaS, detailing the setup, component deployment, and examples of service-oriented quantum applications. This framework offers a promising approach to overcoming current limitations and advancing the practical software engineering of QC. Chapter 9 introduces QSimPy, a novel discrete-event simulation framework that primarily focuses on facilitating learning-centric approaches for quantum resource management problems in cloud environments. QSimPy provides a lightweight simulation environment based on SimPy, a well-known Python-based simulation engine for modeling the dynamics of quantum cloud resources and task operations, underpinned by extensibility, compatibility, and reusability principles. Furthermore, a framework integrates the gym environment to facilitate the development and evaluation of reinforcement learning-based techniques for quantum cloud resource management optimization. The QSimPy framework includes all the complicated parts of how quantum clouds work and helps with research into dynamic task allocation and optimization using DRL methods. Additionally, QSimPy's ability to develop reinforcement learning policies for quantum task placement problems showcases its potential as a valuable framework for future quantum cloud research.

Part 3 focuses on New Trends and Emerging Topics and is made up of three chapters. Chapter 10 formulates resource management problems in a network graph that represents the network nodes, with varying edge weights reflecting the degree of coupling between the nodes. A distributed state variable, representing the solution to the resource problem, superposes the states of the respective nodes in the network. Such a distributed state lends itself very nicely to a quantum state variable representation in terms of a quantum superposition across the respective node states. Chapter 11 explores how it can be used in chemistry, material science, optimization, image processing, and language understanding. This chapter provides insights into the tools and platforms used for QML, reviews popular QML platforms and development frameworks, and discusses the use of quantum and CML libraries. This chapter assesses the current state of QML, summarizing achievements while highlighting challenges and limitations. This chapter also offers perspectives on open research questions and potential future directions. Finally, the discussion revolves around how various industries adopt QML, share success stories, and consider the broader implications for future technological advancements. Chapter 12 presents the top research priorities in QC, such as the development and utility of quantum software tools and their applications in diverse fields such as artificial intelligence (AI), optimization, and cryptography. It highlights the need to redefine the priorities for quantum research to unlock the potential, focusing on new innovations in quantum software and technology, quantum leaps in AI, quantum modeling and simulations, quantum sensing, and secure communication. Furthermore, it discusses the current trends in QC, such as QC for future 6G networks, quantum cloud and serverless computing, scalable qubit arrays for quantum computation, and robust and reliable QC. Finally, it highlights the promising research areas and their open challenges, which include theoretical advancements, disciplinary research, quantum multiverses, quantum-based education, ethical and societal implications, and their commercialization.

Readership

This book presents readers with the fundamental concepts of QC research, along with the challenges involved in developing practical devices and applications. This book covers a broad range of topics, providing a state-of-the-art and comprehensive reference for the rapid progress in the field of QC and related technologies from major international companies (such as IBM, Google, Intel, Rigetti, Q-Control) and academic researchers. This book appeals to a broad readership, as it covers comprehensive topics in the field of QC, including hardware, software, algorithms, and applications, with chapters written by both academic researchers and industry developers.

The essential book for wide engineering disciplines of students from physics, automotive engineering, computer science and engineering, applied computer science, mechanical engineering, data science, and business analytics. This book would be useful for academicians (in computer science and engineering), researchers (in computer science and engineering), postdoc fellows (in computer science and engineering), research scholars (in computer science and engineering), graduate and postgraduate students (in computer science and engineering), industry fellows, and software engineers. The secondary audience will be academicians (in all engineering disciplines), researchers (in all engineering disciplines), postdoc fellows (in all engineering disciplines), research scholars (in computer science and engineering), graduate and postgraduate students (in computer science and engineering), security professionals.

Benefits

The key value of our book lies in its comprehensive coverage of topics in the field of QC and a blend of contributing authors from academia and industry. Therefore the contents of this book will be very useful for learning fundamental science as well as the practical development of quantum devices and software. A comprehensive coverage of topics in the field of QC includes hardware, software, algorithms, and applications. Therefore this book will appeal to a broad readership. Both academic researchers and industry developers have contributed to this book. Hence, this book will not only present fundamental research but also challenges in developing practical devices. The key features and content in our book that will be most valuable to the reader are as follows:

- This book presents up-to-date progress in the field of QC, covering the latest key developments and future directions. Therefore current or future QC students and researchers who wish to start in QC will find the book a valuable resource.
- This book is useful for postgraduates and researchers in identifying the issues and challenges of recent quantum-integrated blockchain networks.
- The academic disciplines where this book can be useful include computer science and engineering, information technology, electronics and communication, and physics.
- The titles of courses where this book is useful include next-generation computing using QC, quantum mechanics in computing, post-quantum cryptography, quantum mechanics, and secure computing technologies.

Acknowledgments

First and foremost, we are grateful to all the contributing authors for their time, effort, and understanding during the preparation of the book. All chapters were reviewed, and authors have updated their chapters to address review comments.

We thank Muhammad Usman from CSIRO for his initial support and guidance during the early phases of the formulation of this book project.

Raj would like to thank his family members, especially Smrithi, Soumya, and Radha Buyya, for their love, understanding, and support during the preparation of this book. Sukhpal would like to express his deepest appreciation to his parents and all of his family members for their unwavering support and affection.

Finally, we would like to thank the staff at Elsevier, particularly Chris Katsaropoulos, Himani Dwivedi, and Punithavathy Govindaradjane. They were wonderful to work with!

Rajkumar Buyya
Sukhpal Singh Gill

This page intentionally left blank

PART 1

Vision and applications

This page intentionally left blank

1

Quantum computing at a glance

Muhammed Golec[1,2], Emir Sahin Hatay[3], Sukhpal Singh Gill[1], Ying Mao[4], and Rajkumar Buyya[5]

[1]SCHOOL OF ELECTRONIC ENGINEERING AND COMPUTER SCIENCE, QUEEN MARY UNIVERSITY OF LONDON, LONDON, UNITED KINGDOM [2]SCHOOL OF COMPUTER ENGINEERING, ABDULLAH GUL UNIVERSITY, KAYSERI, TURKEY [3]SCHOOL OF COMPUTER SCIENCE AND ELECTRONIC ENGINEERING, UNIVERSITY OF ESSEX, COLCHESTER, UNITED KINGDOM [4]DEPARTMENT OF COMPUTER AND INFORMATION SCIENCE, FORDHAM UNIVERSITY, NEW YORK CITY, NY, UNITED STATES [5]QUANTUM CLOUD COMPUTING AND DISTRIBUTED SYSTEMS (QCLOUDS) LABORATORY, SCHOOL OF COMPUTING AND INFORMATION SYSTEMS, THE UNIVERSITY OF MELBOURNE, PARKVILLE, VIC, AUSTRALIA

1.1 Introduction

The rapid progress in quantum technologies has shown that this technology also has tremendous potential in the field of computing (Lo et al., 2012). Unlike traditional computing, where data is processed using only binary bits, quantum computing uses qubits that work with the principles of quantum mechanics (Pirandola et al., 2015). This fundamental difference enables quantum computing to carry out transactions faster. Every day, the scientific world encounters more complex problems that push the limits of traditional computing. Some of these problems are encryption, chemistry, drug development and military operations, and quantum computing emerges as a promising development in solving these problems (Fauseweh, 2024). Quantum computing, for example, can easily break cryptographic algorithms that are still widely used in communication and data security. Additionally, using quantum computing, detailed simulations at the molecular level can be provided in the chemical and pharmaceutical industries (Pirandola et al., 2017).

Despite its advantages and potential, quantum computing is still in its infancy. In today's world, the majority of academic studies on quantum computing remain theoretical, and only the small-scale quantum processing unit (QPU) can be used operationally (Gill et al., 2022). Even quantum computers with small-scale processing units have shown their superiority over traditional computers in solving complex problems. Globally, quantum computer researchers and commercial companies continue to explore the potential of quantum computers by working on quantum computer applications (Gill & Buyya, 2024).

The work to unlock quantum computing's true potential also entails solving quantum-based technical challenges. These problems generally arise from the principles of superposition and entanglement (Pirandola et al., 2015). Moreover, the sensitivity of quantum computers to environmental effects and their high production costs pose significant challenges (Lo et al., 2012). Although distributing quantum computers through a central

Quantum Computing. DOI: https://doi.org/10.1016/B978-0-443-29096-1.00010-6

server is a smart solution to overcome these difficulties, major improvements in quantum algorithms and quantum error correction methods are still needed (Golec et al., 2024).

Modern technology has undergone a paradigm shift with the advent of quantum computing, which promises to revolutionize several industries with its unparalleled processing power. This chapter explains the concept of quantum computing, along with its differences from traditional computing. Further, it introduces fundamental elements of quantum computing, such as qubits, superposition, entanglement, and decoherence, for the readers. Finally, it explains the key components of quantum computing, including quantum algorithms, quantum gates, quantum key distribution (QKD), quantum software tools, and quantum computing applications. By using the ideas of quantum mechanics, quantum gates and algorithms can solve problems that classical computers cannot handle. The integration of trapped ions, advanced quantum software tools, and applications in Artificial Intelligence (AI), optimization, sensing, and cryptography underlines the versatile potential of this technology. Quantum cryptography offers unparalleled data protection in the digital age with robust security protocols, such as quantum digital signatures and quantum secret sharing. At the same time, technological innovation and problem-solving capabilities of quantum computing are heralding a new digital era. This overview aims to provide a basic understanding to the book readers, emphasizing the transformative capacity of quantum computing in addressing complex problems and revolutionizing several domains.

1.2 Quantum computing versus traditional computing

Today's computers and computing units use bits with values 0 and 1 to process the information (Briegel et al., 2009). Therefore all bit operations carry only these two values (deterministic), and all operations are performed with classical boolean logic (AND OR gates). Next generation computers based on the concept of quantum computing, process information using qubits that can be in 0, 1, and both states simultaneously (Gonzalez-Zalba et al., 2021). This means it can represent more states and higher processing power can be achieved. Qubit operations are performed using quantum gates (Barenco et al., 1995). Fig. 1–1 shows the key difference in processing information between quantum computing and conventional computing.

While in traditional computing, processor frequency speed and number of cores are used as performance units, for quantum computing this is expressed as the number of qubits (Pirandola, 2019). Quantum computers work much faster than traditional computers with their ability to accelerate exponentially in complex and large-scale problems (Lucamarini et al., 2018). However, it is a technology that is still in its infancy, with problems such as error correction and inconsistency caused by the sensitivity of qubits to the environment.

1.3 Fundamental concepts

Understanding the fundamental concepts covered in this section is necessary to comprehend the concept of quantum computing. These concepts include the qubit, which is the basic unit of

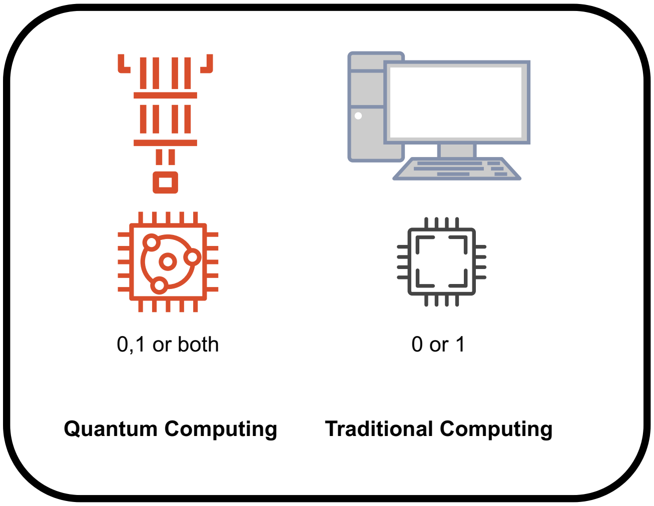


FIGURE 1–1 Main difference between quantum computing and traditional computing.

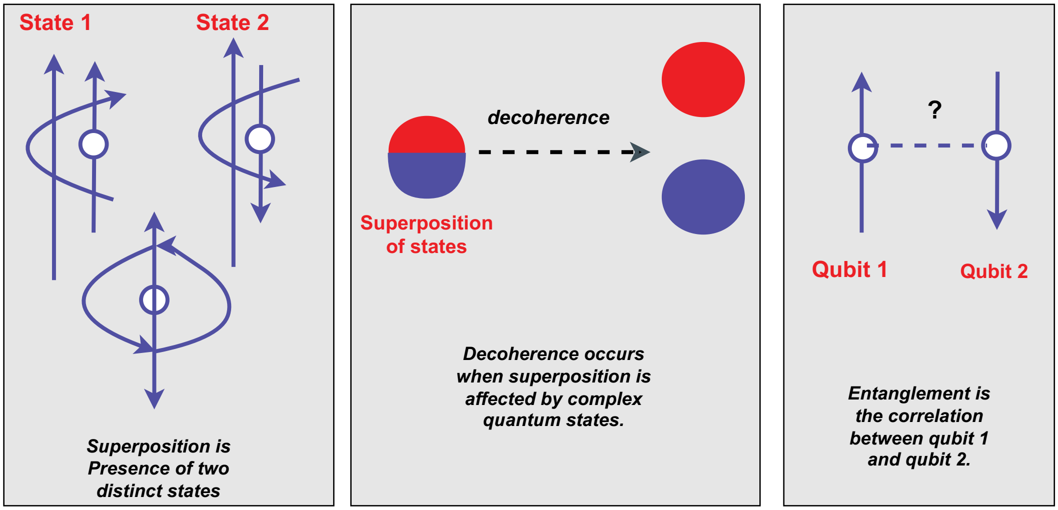


FIGURE 1–2 Fundamental concepts of quantum computing.

information in quantum computing, as well as the superposition, entanglement, and decoherence concepts, which are important in explaining quantum computing's operation and performance (Gill, Cetinkaya, et al., 2024). Fig. 1–2 shows the fundamental concepts of quantum computing.

1.3.1 Qubits

Qubits are the smallest structures used to process information in quantum computing (Steane, 1999). Unlike traditional computing, they can be 0 and 1 at the same time, except when 0 and 1 occur to process information (Nguyen, Usman, et al., 2024). In this way, more situations can be represented. The systems used to create qubits can be summarized as follows (Aslam et al., 2023): (1) Josephson connections, (2) qubits created with the help of an electromagnetic field (ion traps), and (3) qubits based on photon polarization.

1.3.1.1 Advantages of qubits

The advantages of qubits are as follows (Nguyen, Krishnan, et al., 2024):

- Qubits can represent many more situations with the superposition principle and thanks to this feature, they work faster than traditional computing.
- Qubits provide great advantages in solving complex and processing-intensive problems, especially quantum encryption.

1.3.1.2 Disadvantages of qubits

The disadvantages of qubits are as follows (Nguyen, Krishnan, et al., 2024):

- The superposition state is for a very short time and therefore the calculation time is limited.
- Since quantum technology is in its infancy, large-scale transactions cannot be made.
- Quantum computers are sensitive to environmental effects, so it is difficult to ensure process consistency.

1.3.2 Superposition

The situation where 0 and 1 states can exist simultaneously in qubits, unlike the bits used in traditional computing, is called superposition (Golec et al., 2024). Thanks to this special situation and parallel computing ability, quantum computers have the ability to work very fast (Ávila et al., 2023). This speed provides a great advantage in complex and difficult-to-solve problems such as drug production and genetic studies (Procopio et al., 2015). However, the sensitivity of qubits to environmental effects shortens the superposition time (Ren & Li, 2023). This will negatively affect the overall quantum computer performance, shown mathematically in Eq. (1–1). Here |0| and |1| indicate the classical state of the bits in traditional computing, while α and β indicate the probability values.

$$\omega = \alpha|0\rangle + \beta|1\rangle \tag{1–1}$$

1.3.3 Entanglement

The principle that qubits are dependent on each other regardless of the distance between them is called entanglement (Graham et al., 2022). Eq. (1–2) can be used to explain this better. Let's consider the case where two qubits are entangled and it will be sufficient to measure only one of them to make a qubit measurement. In this case, if the first qubit is measured as 0, the other qubit is also measured as 0 (Hidaka et al., 2023). This situation is the same when the qubit is 1. If one qubit is 1, the other qubit is also 1. Entanglement allows quantum computers to perform well on difficult problems such as quantum cryptography (Ren & Li, 2023).

$$\omega = (|00| + |11|)\sqrt{2} \tag{1–2}$$

1.3.4 Decoherence

This concept, decoherence, is used to negatively affect superposition and entanglement situations, which offer great advantages in quantum computing due to environmental effects (Barreiro et al., 2010). Qubits that undergo decoherence start to work like traditional computing bits, and the superiority of quantum computing over traditional computing is lost (Hidaka et al., 2023). This problem is still one of the biggest problems in the widespread use of quantum computing, and work continues on the development of error correction codes and isolation technologies to solve this problem.

1.4 Quantum gates

Quantum computers work with qubits, the fundamental units of quantum information, whereas conventional computers work with bits, which can only be 0 or 1 (Gruska, 1999). Fig. 1–3 shows quantum gates. In contrast to conventional bits, a qubit can exist in a superposition of 0 and 1, which leads to a much broader range of calculations (McMahon, 2007). Quantum computers deploy qubits representing quantum bits to store quantum information in values between 0 and 1. Qubits can represent numerous possible combinations of 1 and 0 at the same time. Qubits allow particles (e.g., electrons) to exist in more than one state at the same time, which makes it possible to increase the number of calculations which makes it possible to increase the number of calculations (Subramanian et al., 2022). Quantum gates, one of the most important features of quantum circuits and computation, are operations that manipulate the states of qubits through unitary transformations (Barenco et al., 1995). Several gate models manage qubits similarly to classical logic gates but can exploit quantum-specific properties such as entanglement and superposition. These features are crucial for the universal computational model to which quantum algorithms can be applied (Qiao et al., 2018).

- **Single-qubit Gates**: Single-qubit gates perform rotations on the Bloch sphere; thus, they change the state of a qubit and create superposition states where the qubit exists in a combination of 0 and 1 (Gottesman & Chuang, 1999).

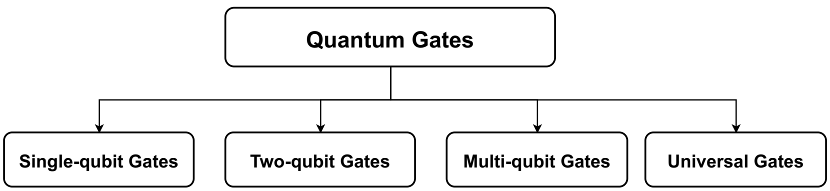


FIGURE 1–3 Types of quantum gates.

- **Two-qubit Gates**: Two-qubit gates, such as the Controlled-NOT (CNOT) gate, enable interactions between qubits, allowing them to become entangled and perform operations that are not possible with classical bits (Vatan & Williams, 2004). It creates a superposition corresponding to a rotation around the X-axis followed by a rotation around the Z-axis. Furthermore, it can be used to create quantum entanglement.
- **Multi-qubit Gates**: Multiple qubit gates, represented by higher-dimensional unitary matrices, acting on two or more qubits simultaneously, are effectively used to perform complex quantum work and can be decoupled into single-qubit and two-qubit gates using a technique called gate decomposition, allowing interaction and entanglement between qubits (Liu et al., 2022).
- **Universal Gates**: Universal gates are a collection of gates that can be used to implement any quantum operation using a technique called *gate synthe*sis and can be used to approximate an arbitrary degree of fecundity that can realize any quantum algorithm in a quantum computer (Brylinski & Brylinski, 2002).

1.4.1 Trapped ions with quantum gates

Trapped ion gates, which enable quantum logic operations to be performed by manipulating the states of trapped ion-charged atomic particles using electromagnetic fields, are an important and leading part of quantum computing with trapped ion qubits (Schäfer et al., 2018). Individual ions serve as qubits in trapped ion quantum computing, with the $|0\rangle$ and $|1\rangle$ states of a qubit being represented by the various electronic states of the ions. In quantum processes, these qubits are in control through the use of powerful laser or microwave pulses that manipulate interactions and transitions between quantum states (Wang, 2012). Using quantum control methods, which alter microwave pulses to strengthen the interaction’s defense against external noise, one can increase the dependability of quantum gates. Due to their efficient environmental isolation and sophisticated cooling methods, trapped ion gates, which exhibit near-maximum accuracy in desired functions, can maintain their quantum states over extended periods (Subramanian et al., 2022). Although there are different challenges, such as integrating the required technology into a practical industrial system and increasing the number of qubits, thanks to advanced quantum control techniques, trapped ion gates have a phenomenal potential to scale up to a larger number of qubits (Kumar, Gill, et al., 2022). Trapped ion technology, which has applications in other areas of quantum computing such as quantum communication and quantum sensing, is a key component in the progression of quantum computing from theoretical ideas to practical applications, providing the operations required to develop and run quantum algorithms (Gale et al., 2020).

1.5 Applications

Quantum computers, which use the advantages of quantum mechanics such as superposition and entanglement, are expected to cause groundbreaking developments in many fields and applications. Fig. 1–4 shows some of the most important of these applications.

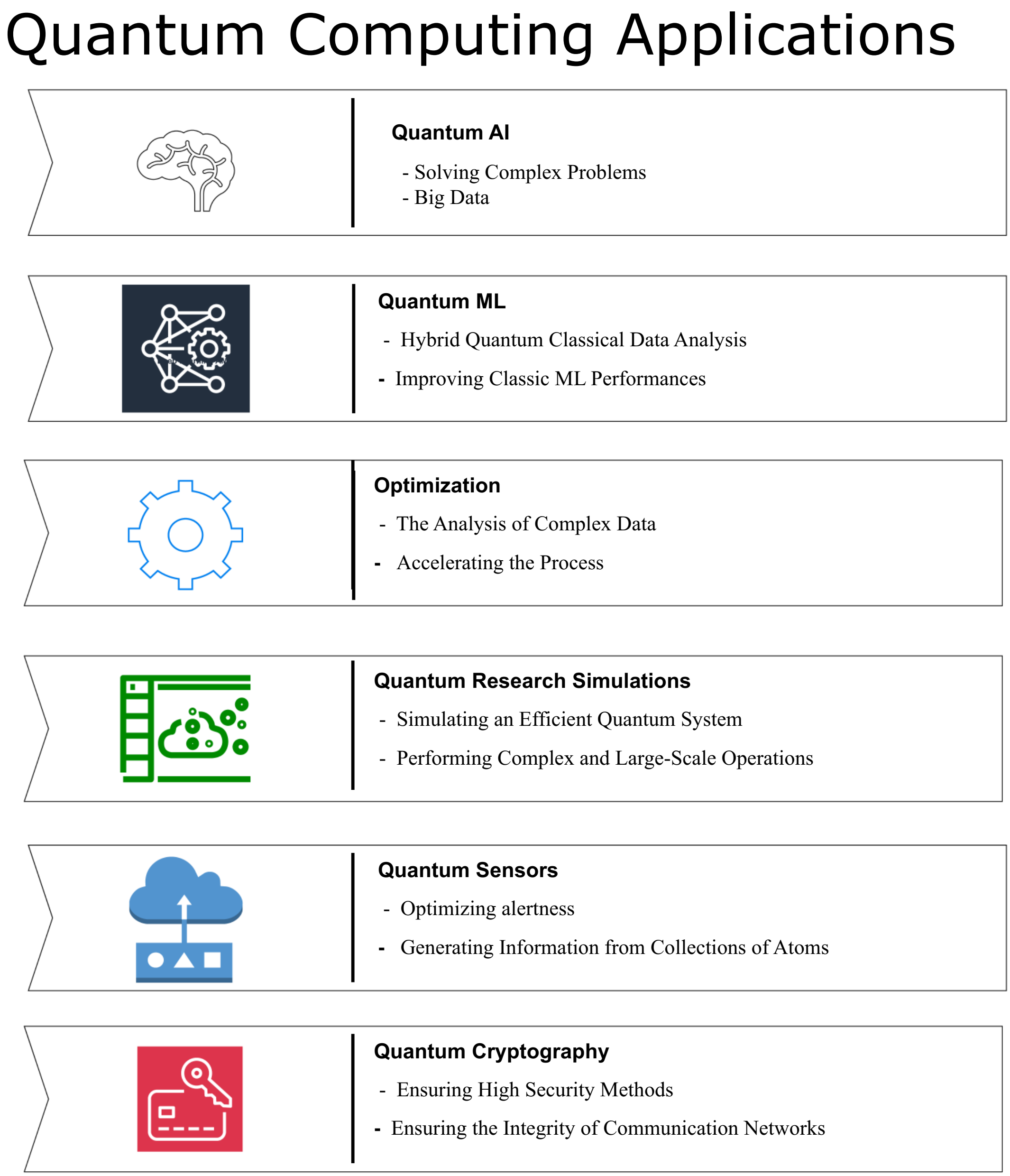


FIGURE 1–4 Quantum computing applications.

- **Quantum AI**: Quantum AI aims to obtain high-performance AI algorithms by combining the processing power of AI and quantum computing (Ying, 2010). Thanks to the high performance of quantum computers, AI models learn faster and show high performance in applications that require fast processing such as Natural Language Processing.

- **Quantum ML**: Quantum ML is aimed to increase complex problem-solving capacity and accelerate training processes by using quantum computers together with ML algorithms (Huang et al., 2021). This means that in the future there will be applications that will use better-optimized AI/ML models.
- **Optimization**: With the widespread use of quantum computers, solutions that can achieve the target in the most efficient way will be obtained for problems such as resource allocation and route optimization in transportation (Li et al., 2020).
- **Quantum Research Simulations**: This means that studies that require work at the atomic level (such as chemical reactions) can be simulated using quantum computers (Daley et al., 2022).
- **Quantum Sensors**: Quantum sensors are based on combining sensor technology with quantum mechanics to make them more accurate and sensitive (Aslam et al., 2023). It has great potential, especially in applications that require precise measurement, such as magnetic field-based electric fields.
- **Quantum Cryptography**: Quantum cryptography is a technology that uses quantum principles to ensure data security (Pirandola et al., 2008). It provides higher security than traditional encryption methods in scenarios where two parties exchange keys, such as QKD.

1.6 Algorithms

Quantum algorithms, such as Shor's algorithm (which can break RSA [Rivest–Shamir–Adleman] encryption) for factoring integers and Grover's algorithm for unstructured search, represent significant breakthroughs. Shor's algorithm demonstrates exponential speedup to classical algorithms, while Grover's algorithm offers a quadratic speedup for search problems (Bhatia & Ramkumar, 2020). A modern quantum computer is a much-desired step towards achieving the processing capability of its kind, and its revolutionary consequences would undoubtedly affect various fields such as AI (Abdelgaber & Nikolopoulos, 2020). Quantum algorithms have been introduced that rely on the Fourier transform, a mathematical process that facilitates the transformation of signals between different domains, such as from the time domain to the frequency domain or vice versa (Hales & Hallgren, 2000). The first quantum algorithm that beat classical algorithms, which were diverse and difficult to solve, in terms of performance, was revealed by (Shor, 2002). Among the quantum algorithms that aim to reduce the computing power used to analyze algorithms, first, the Deutsch–Jozsa Algorithm (Gulde et al., 2003), which focuses on faster calculations, and then the Bernstein–Vazirani algorithm, which solves the hidden shift problem, emerged (Zhou et al., 2023).

Moreover, Simon's Algorithm addresses the problem of finding a hidden period efficiently, while Shor's Algorithm is renowned for factoring integers and solving discrete logarithms exponentially faster than classical methods (Strubell, 2011). Further evidence that quantum algorithms are exponentially faster than classical algorithms includes Grover's algorithm, developed by Lov Grover, a pioneer in algorithms for quantum simulation and quantum

Machine Learning (ML) (Shor, 2002). Grover's algorithm is quadratically faster than classical algorithms for searching for an item in an irregular database or unordered list. Additionally, quantum counting algorithms and quantum optimization algorithms, which aim to minimize optimization problems, further demonstrate the superior speed of quantum computing (Gilyén et al., 2019).

1.7 Computational complexity classes

In classical computational theory, complexity classes, such as P and NP, categorize problems based on their solvability and verifiability within polynomial time by deterministic and nondeterministic Turing Machines, respectively (Abdelgaber & Nikolopoulos, 2020). In contrast, quantum algorithms solve certain problems more efficiently than classical algorithms, as demonstrated by the breakthroughs of Shor's and Grover's algorithms (Lo et al., 2012). To understand these speedups, it is essential to discuss the relevant complexity classes:

- **P (Polynomial Time)**: This class includes problems that can be solved by a deterministic classical computer in polynomial time relative to the size of the input. These problems are considered fast and easy to solve (Pirandola et al., 2015).
- **NP (Nondeterministic Polynomial Time)**: This class includes problems for which a given solution can be verified in polynomial time by a deterministic classical computer. However, in general, we have not yet discovered solutions for NP-Hard problems that can be solved in less than exponential time. Notice that no real nondeterministic computer has been built yet; thus, these polynomial times are not believed to be attainable by classical computers (Pirandola et al., 2017).
- **BQP (Bounded-Error Quantum Polynomial Time)**: This class includes problems that can be solved by a quantum computer in polynomial time with a probability of error that is at most 1/3 for all instances. In other words, a problem is BQP if a quantum algorithm can solve it in polynomial time with a probability of at least 2/3.

As such, discovering what problems can be placed in BQP and identifying their real-world applications becomes key to unlocking the potential of quantum computing (Lucamarini et al., 2018). For instance, Shor's algorithm is classified into BQP, providing an exponential speedup for factoring integers and computing discrete logarithms (Kumar, Ottaviani, et al., 2022). Classical algorithms for these problems are believed to require superpolynomial time, placing them in the NP class. By solving these problems in polynomial time, Shor's algorithm demonstrates that BQP can outperform NP for specific problems, such as breaking RSA encryption (Pirandola, 2019).

Additionally, Grover's algorithm provides a quadratic speedup for unstructured search problems. While classical algorithms require $O(N)$ time to search an unsorted array of N items, Grover's algorithm requires only $O(\sqrt{N})$ time, showing that BQP can significantly improve over P for certain problems.

1.7.1 Quantum key distribution

Beyond accelerating applications, quantum computing enables solutions to problems that are impossible to solve with classical systems (Lo et al., 2012). For instance, one of the most prominent applications of quantum cryptography is QKD, which allows two parties to securely share a random secret key used for encrypting and decrypting messages (Pirandola et al., 2015). QKD enables secure key exchange using quantum properties such as superposition and entanglement (NIST, 2024). The most well-known QKD protocol is BB84, developed by Charles Bennett and Gilles Brassard in 1984 (Pirandola et al., 2017). The fundamental principles of quantum mechanics guarantee the security of QKD:

- **No-Cloning Theorem**: Creating an identical copy of an arbitrary unknown quantum state is impossible, preventing an eavesdropper from duplicating qubits without detection.
- **Heisenberg Uncertainty Principle**: Measuring a quantum state disturbs it, introducing detectable errors if an eavesdropper tries to intercept and measure the qubits.

These principles ensure that any attempt to eavesdrop on the key exchange will be detected, providing a level of security that is impossible by classical cryptographic methods (Lucamarini et al., 2018). Unlike quantum algorithms, which offer a speedup over classical algorithms, QKD introduces a fundamentally new capability that classical computing cannot achieve, ensuring secure communication based on the inherent properties of quantum mechanics (Pirandola, 2019).

1.8 Software tools

IBM has released Qiskit, an open-source framework that allows users to design and run quantum circuits on the company's quantum computers (Burgholzer et al., 2020). Microsoft's Quantum Development Kit and the Q programming language offer a development environment for quantum programming, which provides resource estimation and simulation (Mykhailova & Soeken, 2021). More recently, NVIDIA published its CUDA-Q platform (Philippidis, 2024) for hybrid quantum-classical computing. It integrates QPUs, GPUs, and CPUs in one system for high-performance quantum-classical computing. Among the most famous are Google's Cirq (Pattanayak, 2021), which aims to focus on quantum devices facilitating the optimization and design of quantum circuits, D-Wave Ocean (Zubov et al., 2015), which provides tools to solve optimization problems using quantum annealing, and pyQuil (Koch et al., 2019), which supports the programming of quantum algorithms by Rigetti on Rigetti's quantum computers.

Quantum developers commonly provide these frameworks with open-source licenses and an Application Programming Interface in Python to promote their solutions. These platforms include rich features and libraries, including domain-specific applications in finance, chemistry, and optimization, as well as quantum ML, quantum circuit design, and quantum algorithm implementation (Gill, Cetinkaya, et al., 2024). They also facilitate hybrid quantum-classical computing. In this way, quantum computations are integrated with classical processing. Furthermore, platforms like Pennylane integrate and facilitate the development of quantum ML models that leverage the strengths of both quantum and classical computing (Gill & Buyya, 2024). Researchers and developers can more easily apply quantum algorithms because to Pennylane's without interruption integration with popular ML frameworks like TensorFlow and PyTorch. Pennylane enables the optimization of quantum circuits in conjunction with traditional neural networks by offering tools for differentiable programming and automatic differentiation (Gill et al., 2022). This contributes and opening the door to new applications in areas such as finance, AI and drug discovery. As long as the field of quantum computing continues to develop at breakneck speed, quantum software tools will strictly push the boundaries of what is possible in bridging the gap between quantum theory and its applications (Gill, 2024).

1.9 Application programming

Quantum computers work differently from the binary bit logic found in traditional computers (Hidaka et al., 2023). This difference can also be seen in the algorithms and applications created for quantum computers as discussed in Sections 1.5 and 1.6. The field of quantum application programming covers areas such as quantum circuit programming and quantum algorithms. Circuits exported from various quantum programming languages and tools can run on a wide variety of simulation and quantum machines (Williams & Williams, 2011). A few examples of such systems include Amazon Braket, Microsoft Quantum Development Kit, Google Cirq and TensorFlow Quantum, IBM Qiskit, and Rigetti Forest.

1.9.1 Circuit programming

Quantum Circuit Programming covers the processes of designing quantum circuits that will run quantum applications. Quantum circuits contain quantum gates, which are similar to the logic gates used for bit operations in traditional computing (Williams & Williams, 2011), which can be used in quantum computing to manipulate qubits (Tang et al., 2021). For examples, Shor's algorithm (Factorization) and Grover's algorithm (Search Problems) are often used to design quantum circuits (Shor, 2002) as discussed in Section 1.6.

1.10 Latest technological advancements

The principles of quantum mechanics are known to humans from the last century with limited technological developments but generally, it has been the stuff of science fiction movies (West et al., 2024). The rapid and real development of quantum-based devices is observed in recent years, which opened up new areas of research. During the same time, rapid progress made in AI with ML and space technology led to extraordinary accomplishments for the whole human race (Gill, Wu, et al., 2024). AI has emerged as an essential tool to upgrade any machine's working in an automated way. For instance, space technology has been recognized in developing and launching satellites to reach out to unknown planets and reveal the unfolding stories of the universe (Krenn et al., 2023). Today, these developments are being unified to question how quantum computing and AI may influence the advancement of satellites and drones into automated quantum satellites and drones.

A modern satellite and drone system involves advanced technology including quantum computing and AI. An automated satellite system, which can take decisions by itself, may be very helpful for data collection from the planets, which are very far from the operating station. Such operations require high-speed and very precise computation (Shuford, 2024). Hence, quantum computing is an essential need for such systems to improve performance, decrease computational costs in these satellite operations. Such quantum computations, using a quantum computer, are performed by exploiting quantum phenomena such as superposition, entanglement, and tunneling (Pooranam et al., 2023). Quantum computers are very fast in solving and analysis of very complex problems for which a classical computer would take thousands of years. Despite the acceleration and high performance, there are things, such as the size of the quantum computer and cryogenic temperature required, that still need attention and require improvements (Simões et al., 2023).

AI also plays an important role in addition to designing a modern satellite and quantum computation. The observed improvements by applying quantum computing in artificial intelligence (known as quantum AI) are the quick resolution of complex problems, optimization, ability to spot patterns in extremely large datasets, etc. (Tychola et al., 2023). The use of such quantum AI techniques in satellites or drones improves efficiency and applicability in a great manner. Quite recently, scientists have reported developing a quantum satellite ground station, which is not only very small but also capable of sending messages (data) anywhere in the world (Peral-Garca et al., 2024). These quantum satellites or drones also provide ultra-high data security. Unlike ordinary satellites, the encryption methods for data security used in such quantum satellites are based on fundamental laws of quantum physics instead of abstract mathematics-based algorithms (Gil-Fuster et al., 2024). Therefore, even a very fast computer cannot creak the transferring data and quantum key communication will remain intact because any attempt to eavesdrop will cause a physical change in the message and trigger a security alert to the sender or receiver.

1.11 Summary

Quantum computing is a new paradigm that works with quantum mechanical principles such as superposition and entanglement and offers higher performance than traditional computing. To better understand quantum computing, this chapter provides a quick look at fundamental concepts such as qubits' unique properties, superposition, and entanglement principles. Examining recent developments such as quantum applications, algorithms, software tools, and gates highlights the potential of quantum computing for researchers.

References

Abdelgaber, N., & Nikolopoulos, C. (2020). Overview on quantum computing and its applications in artificial intelligence. *2020 IEEE third international conference on artificial intelligence and knowledge engineering (AIKE),* 198–199 IEEE.

Aslam, N., Zhou, H., Urbach, E. K., Turner, M. J., Walsworth, R. L., Lukin, M. D., & Park, H. (2023). Quantum sensors for biomedical applications. *Nature Reviews Physics, 5*(3), 157–169.

Ávila, P., Okon, E., Sudarsky, D., & Wiedemann, M. (2023). Quantum spatial superpositions and the possibility of superluminal signaling. *Physical Review D, 108*(8), 086025.

Barenco, A., Bennett, C. H., Cleve, R., DiVincenzo, D. P., Margolus, N., Shor, P., Sleator, T., Smolin, J. A., & Weinfurter, H. (1995). Elementary gates for quantum computation. *Physical Review A, 52*(5), 3457.

Barreiro, J. T., Schindler, P., Gühne, O., Monz, T., Chwalla, M., Roos, C. F., Hennrich, M., & Blatt, R. (2010). Experimental multiparticle entanglement dynamics induced by decoherence. *Nature Physics, 6*(12), 943–946.

Bhatia, V., & Ramkumar, K. (2020). An efficient quantum computing technique for cracking RSA using shor's algorithm. *2020 IEEE 5th international conference on computing communication and automation (ICCCA),* 89–94 IEEE.

Briegel, H. J., Browne, D. E., Dür, W., Raussendorf, R., & Van den Nest, M. (2009). Measurement-based quantum computation. *Nature Physics, 5*(1), 19–26.

Brylinski, J.-L., & Brylinski, R. (2002). *Universal quantum gates. Mathematics of quantum computation*. Chapman and Hall/CRC, 117–134.

Burgholzer, L., Raymond, R., & Wille, R. (2020). Verifying results of the ibm qiskit quantum circuit compilation flow. *2020 IEEE international conference on quantum computing and engineering (QCE),* 356–365 IEEE.

Daley, A. J., Bloch, I., Kokail, C., Flannigan, S., Pearson, N., Troyer, M., & Zoller, P. (2022). Practical quantum advantage in quantum simulation. *Nature, 607*(7920), 667–676.

Fauseweh, B. (2024). Quantum many-body simulations on digital quantum computers: State-of-the-art and future challenges. *Nature Communications, 15*(1), 2123.

Gale, E. P., Mehdi, Z., Oberg, L. M., Ratcliffe, A. K., Haine, S. A., & Hope, J. J. (2020). Optimized fast gates for quantum computing with trapped ions. *Physical Review A, 101*(5), 052328.

Gil-Fuster, E., Eisert, J., & Bravo-Prieto, C. (2024). Understanding quantum machine learning also requires rethinking generalization. *Nature Communications, 15*(1), 2277.

Gill, S. S. (2024). Quantum and blockchain based serverless edge computing: A vision, model, new trends and future directions. *Internet Technology Letters, 7*(1), e275.

Gill, S. S., & Buyya, R. (2024). Transforming research with quantum computing. *Journal of Economy and Technology, 3*, 1–10.

Gill, S. S., Kumar, A., Singh, H., Singh, M., Kaur, K., Usman, M., & Buyya, R. (2022). Quantum computing: A taxonomy, systematic review and future directions. *Software: Practice and Experience, 52*(1), 66–114.

Gill,S.S., Cetinkaya,O., Marrone,S., et al. (2024). Quantum computing: Vision and challenges, *Technical Report: arXiv:2403.02240*.

Gill, S. S., Wu, H., Patros, P., Ottaviani, C., Arora, P., Pujol, V. C., Haunschild, D., Parlikad, A. K., Cetinkaya, O., Lutfiyya, H., et al. (2024). Modern computing: Vision and challenges. *Telematics and Informatics Reports, 13*, 100116.

Gilyén, A., Arunachalam, S., & Wiebe, N. (2019). Optimizing quantum optimization algorithms via faster quantum gradient computation. *Proceedings of the thirtieth annual ACM-SIAM symposium on discrete algorithms,* 1425–1444 SIAM.

Golec, M., Hatay, E. S., Golec, M., Uyar, M., Golec, M., & Gill, S. S. (2024). Quantum cloud computing: Trends and challenges. *Journal of Economy and Technology, 2*, 190–199.

Gonzalez-Zalba, M., De Franceschi, S., Charbon, E., Meunier, T., Vinet, M., & Dzurak, A. (2021). Scaling silicon-based quantum computing using cmos technology. *Nature Electronics, 4*(12), 872–884.

Gottesman, D., & Chuang, I. L. (1999). Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature, 402*(6760), 390–393.

Graham, T., Song, Y., Scott, J., Poole, C., Phuttitarn, L., Jooya, K., Eichler, P., Jiang, X., Marra, A., Grinkemeyer, B., et al. (2022). Multi-qubit entanglement and algorithms on a neutral-atom quantum computer. *Nature, 604*(7906), 457–462.

Gruska, J., et al. (1999). *Quantum computing, 2005*. London: McGraw-Hill.

Gulde, S., Riebe, M., Lancaster, G. P., Becher, C., Eschner, J., Häffner, H., Schmidt-Kaler, F., Chuang, I. L., & Blatt, R. (2003). Implementation of the deutsch-jozsa algorithm on an ion-trap quantum computer. *Nature, 421*(6918), 48–50.

Hales, L., & Hallgren, S. (2000). An improved quantum fourier transform algorithm and applications. *Proceedings 41st annual symposium on foundations of computer science,* 515–525 IEEE.

Hidaka, Y., Iso, S., & Shimada, K. (2023). Entanglement generation and decoherence in a two-qubit system mediated by relativistic quantum field. *Physical Review D, 107*(8), 085003.

Huang, H.-Y., Broughton, M., Mohseni, M., Babbush, R., Boixo, S., Neven, H., & McClean, J. R. (2021). Power of data in quantum machine learning. *Nature Communications, 12*(1), 2631.

Koch, D., Wessing, L., & Alsing, P.M. (2019). Introduction to coding quantum algorithms: A tutorial series using pyquil. *arXiv preprint arXiv:1903.05195*.

Krenn, M., Landgraf, J., Foesel, T., & Marquardt, F. (2023). Artificial intelligence and machine learning for quantum technologies. *Physical Review A, 107*(1), 010101.

Kumar, A., Gill, S. S., & Abraham, A. (2022). *Quantum and blockchain for modern computing systems: Vision and advancements*. Springer.

Kumar, A., Ottaviani, C., Gill, S. S., & Buyya, R. (2022). Securing the future internet of things with post-quantum cryptography. *Security and Privacy, 5*(2), e200.

Li, Y., Tian, M., Liu, G., Peng, C., & Jiao, L. (2020). Quantum optimization and quantum learning: A survey. *IEEE Access, 8*, 23568–23593.

Liu, W.-Q., Wei, H.-R., & Kwek, L.-C. (2022). Universal quantum multi-qubit entangling gates with auxiliary spaces. *Advanced Quantum Technologies, 5*(5), 2100136.

Lo, H.-K., Curty, M., & Qi, B. (2012). Measurement-device-independent quantum key distribution. *Physical Review Letters, 108*, 130503.

Lucamarini, M., Yuan, Z. L., Dynes, J. F., & Shields, A. J. (2018). Overcoming the rate- distance limit of quantum key distribution without quantum repeaters. *Nature, 557*, 400–403.

McMahon, D. (2007). *Quantum computing explained*. John Wiley & Sons.

Mykhailova, M., & Soeken, M. (2021). *Testing quantum programs using q# and microsoft quantum development kit*. CEUR Workshop Proceedings, (pp. 81–88).

Nguyen, H. T., Usman, M., & Buyya, R. (2024). iQuantum: A toolkit for modeling and simulation of quantum computing environments. *Software: Practice and Experience, 54*(6), 1141–1171.

Nguyen, H.T., Krishnan, P., Krishnaswamy, D., Usman, M., & Buyya, R. (2024). Quantum cloud computing: A review, open problems, and future directions. *arXiv preprint arXiv:2404.11420*.

NIST. (2024). *Nist post-quantum cryprography standardisation*. <https://csrc.nist.gov/Projects/post-quantum-cryptography/round-4-submissions>.

Pattanayak, S. (2021). *Quantum machine learning with Python: Using Cirq from Google research and IBM Qiskit*. Springer.

Peral-Garca, D., Cruz-Benito, J., & Garca-Peñalvo, F. J. (2024). Systematic literature review: Quantum machine learning and its applications. *Computer Science Review, 51*, 100619.

Philippidis, A. (2024). Gtc 2024: Nvidia's quantum expansion runs through the cloud. *GEN Edge, 6*(1), 249–254.

Pirandola, S. (2019). End-to-end capacities of a quantum communication network. *Communications Physics, 2*, 51.

Pirandola, S., Mancini, S., Lloyd, S., & Braunstein, S. L. (2008). Continuous-variable quantum cryptography using two-way quantum communication. *Nature Physics, 4*(9), 726–730.

Pirandola, S., Ottaviani, C., Spedalieri, G., Weedbrook, C., Braunstein, S. L., Lloyd, S., Gehring, T., Jacobsen, C. S., & Andersen, U. L. (2015). High-rate quantum cryptography in untrusted networks. *Nature Photonics, 9*, 397–402.

Pirandola, S., Laurenza, R., Ottaviani, C., & Banchi, L. (2017). Fundamental limits of repeaterless quantum communications. *Nature Communications, 8*, 15043.

Pooranam, N., Surendran, D., Karthikeyan, N., & Rajathi, G. I. (2023). Quantum computing: Future of artificial intelligence and its applications. *Quantum Computing and Artificial Intelligence: Training Machine and Deep Learning Algorithms on Quantum Computers, 163*.

Procopio, L. M., Moqanaki, A., Araújo, M., Costa, F., Alonso Calafell, I., Dowd, E. G., Hamel, D. R., Rozema, L. A., Brukner, Č., & Walther, P. (2015). Experimental superposition of orders of quantum gates. *Nature Communications, 6*(1), 7913.

Qiao, L.-F., Streltsov, A., Gao, J., Rana, S., Ren, R.-J., Jiao, Z.-Q., Hu, C.-Q., Xu, X.-Y., Wang, C.-Y., Tang, H., et al. (2018). Entanglement activation from quantum coherence and superposition. *Physical Review A, 98*(5), 052351.

Ren, Z., & Li, Y. (2023). Characterizing entanglement robustness of an n-qubit w superposition state against particle loss from quantum fisher information. *Results in Physics, 53*, 106954.

Schäfer, V., Ballance, C., Thirumalai, K., Stephenson, L., Ballance, T., Steane, A., & Lucas, D. (2018). Fast quantum logic gates with trapped-ion qubits. *Nature, 555*(7694), 75–78.

Shor, P. W. (2002). Introduction to quantum algorithms. *Proceedings of Symposia in Applied Mathematics*. (58, pp. 143–160). American Mathematical Society.

Shuford, J. (2024). Quantum computing and artificial intelligence: Synergies and challenges. *Journal of Artificial Intelligence General Science (JAIGS), 1*(1). ISSN: 3006–4023.

Simões, R. D. M., Huber, P., Meier, N., Smailov, N., Füchslin, R. M., & Stockinger, K. (2023). Experimental evaluation of quantum machine learning algorithms. *IEEE Access, 11*, 6197–6208.

Steane, A. M. (1999). Efficient fault-tolerant quantum computing. *Nature, 399*(6732), 124–126.

Strubell, E. (2011). An introduction to quantum algorithms. *COS498 Chawathe Spring, 13*, 19.

Subramanian, T., Dhyani, A., Kumar, A., & Gill, S. S. (2022). *Artificial intelligence, machine learning and blockchain in quantum satellite, drone and network*. CRC Press.

Tang, W., Tomesh, T., Suchara, M., Larson, J., & Martonosi, M. (2021). Cutqc: Using small quantum computers for large quantum circuit evaluations. In *Proceedings of the 26th ACM international conference on architectural support for programming languages and operating systems* (pp. 473–486). ACM.

Tychola, K. A., Kalampokas, T., & Papakostas, G. A. (2023). Quantum machine learning—An overview. *Electronics, 12*(11), 2379.

Vatan, F., & Williams, C. (2004). Optimal quantum circuits for general two-qubit gates. *Physical Review A -Atomic, Molecular, and Optical Physics, 69*(3), 032315.

Wang, S.X. (2012). *Quantum gates, sensors, and systems with trapped ions*. PhD thesis, Massachusetts Institute of Technology.

West, M. T., Heredge, J., Sevior, M., & Usman, M. (2024). Provably trainable rotationally equivariant quantum machine learning. *PRX Quantum, 5*(3), 030320.

Williams, C. P., & Williams, C. P. (2011). Quantum gates. *Explorations in Quantum Computing,* 51–122.

Ying, M. (2010). Quantum computation, quantum theory and ai. *Artificial Intelligence, 174*(2), 162–176.

Zhou, X., Qiu, D., & Luo, L. (2023). Distributed bernstein-vazirani algorithm. *Physica A: Statistical Mechanics and its Applications, 629*, 129209.

Zubov, D., Volponi, F., & Khosravy, M. (2015). D-wave quantum computing ising model: A case study for the forecasting of heat waves. *2015 international conference on control, automation and information sciences (ICCAIS),* 149–152 IEEE.