Information Systems Engineering and Management 2

Habiba Drias
Farouk Yalaoui *Editors*

Quantum Computing: Applications and Challenges

Springer

Information Systems Engineering and Management 2

The book series "Information Systems Engineering and Management" (ISEM) publishes innovative and original works in the various areas of planning, development, implementation, and management of information systems and technologies by enterprises, citizens, and society for the improvement of the socio-economic environment.

The series is multidisciplinary, focusing on technological, organizational, and social domains of information systems engineering and management. Manuscripts published in this book series focus on relevant problems and research in the planning, analysis, design, implementation, exploration, and management of all types of information systems and technologies. The series contains monographs, lecture notes, edited volumes, pedagogical and technical books as well as proceedings volumes.

Some topics/keywords to be considered in the ISEM book series are, but not limited to: Information Systems Planning; Information Systems Development; Exploration of Information Systems; Management of Information Systems; Blockchain Technology; Cloud Computing; Artificial Intelligence (AI) and Machine Learning; Big Data Analytics; Multimedia Systems; Computer Networks, Mobility and Pervasive Systems; IT Security, Ethics and Privacy; Cybersecurity; Digital Platforms and Services; Requirements Engineering; Software Engineering; Process and Knowledge Engineering; Security and Privacy Engineering, Autonomous Robotics; Human-Computer Interaction; Marketing and Information; Tourism and Information; Finance and Value; Decisions and Risk; Innovation and Projects; Strategy and People.

Indexed by Google Scholar. All books published in the series are submitted for consideration in the Web of Science.

For book or proceedings proposals please contact Alvaro Rocha (amrrocha@gmail.com).

Habiba Drias · Farouk Yalaoui
Editors

Quantum Computing: Applications and Challenges

Springer

Editors

Habiba Drias
Algerian Academy of Science
and Technology (AAST)
Algiers, Algeria

Head of the Computer Science Section
AAST
Algiers, Algeria

University of Science and Technology Houari
Boumediene (USTHB)
Algiers, Algeria

Head of the laboratory of Research in A.I.
(LRIA)
USTHB
Algiers, Algeria

Farouk Yalaoui
Algerian Academy of Science
and Technology
University of Technology of Troyes (UTT)
Troyes, France

ISSN 3004-958X ISSN 3004-9598 (electronic)
Information Systems Engineering and Management
ISBN 978-3-031-59317-8 ISBN 978-3-031-59318-5 (eBook)
https://doi.org/10.1007/978-3-031-59318-5

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

This volume contains papers from the Symposium on Quantum Sciences, Applications and Challenges (QSAC'2023), held in Algiers during September 24–25, 2023. The event was organized by the computer science section of the Algerian Academy of Science and Technology (AAST), aiming to explore the frontiers of one of the most captivating fields of modern science. Its objective was to inspire innovative research in the realm of quantum sciences. Articles from quantum computing are included in this book. The themes addressed during the scientific event revolved cover the latest developments in quantum computing and their applications. They embrace the fields of quantum machine learning, quantum cryptography, quantum optimization, and quantum artificial intelligence and applications. The book is the first of its kind among the instigators of this discipline in the world. It will allow scientific research to embark on these new and strategic domains.

Quantum computing promises exponentially faster computation and the ability to solve problems that are intractable by classical computers. This challenging field has the power to revolutionize cryptography, optimization, artificial intelligence, and simulations that could transform industries ranging from finance to drug discovery.

The opportunities of quantum technologies are enormous. The calculations carried out by quantum systems are very fast and their spin-offs in industry are very beneficial. This advance will be more talented by hybridizing it with artificial intelligence. Unlike this gainful progress for our society, quantum technologies unfortunately pose threats. The most striking example is the attack on cryptography. Computer security is highly threatened by quantum technologies.

Both opportunities and threats favor the emergence of start-ups, particularly in the fields of quantum computing, quantum communications, quantum post-cryptography and quantum artificial intelligence. Classical computing dealing with data will have to migrate to quantum computing and the sooner the better to ensure data protection.

Sixty-four submissions from quantum sciences were received following the call for papers. Each article was double-blind reviewed by at least three members of the program's international committee and external reviewers. Only 18 top-rated papers from quantum computing were selected for oral presentation, and 15 of them are included in the proceedings, as they all reflect Springer's publication policy. The accepted and presented papers deal with novel research and innovative applications and stimulated fruitful debates and knowledge acquisition. We hope the future readers find these contributions useful and inspiring.

The proceedings editors would like to thank all the contributors who made the symposium successful: the organizing group, the program committee chairs, the scientific committee, the external reviewers, the keynote speakers, the authors for submitting their work, the participants for their discussions and for the rich debates they aroused during the sessions, and our sponsors who helped in terms of logistics.

Our special thanks goes to Springer for publishing a part of the proceedings of QSAC'2023.

Habiba Drias
Farouk Yalaoui

Invited Speakers

From Einstein's Doubts To Technology: The Second Quantum Revolution

Alain Aspect

Institut d'Optique, Paris-Saclay University, France
alain.aspect@institutoptique.fr

Alain Aspect was awarded the 2022 Nobel Prize in Physics, jointly with John Clauser and Anton Zeilinger, "for experiments with entangled photons, establishing the violation of Bell inequalities and pioneering quantum information science".

Abstract

Thanks to the mysterious concept of wave–corpuscle duality, the first quantum revolution made it possible to describe the structure of matter, its electrical, mechanical and optical properties, and its interaction with light. It then provided the technologies—transistor, laser, integrated circuits—that led to the information and communication society.

The second quantum revolution, based on the notion of entanglement, is even more surprising in conceptual terms, since it forces us to reject Einstein's cherished local realist vision of the world, as demonstrated by the violation of Bell's inequalities. It also opens up fascinating prospects for applications, with emerging technologies ranging from quantum sensors to quantum communications and quantum computers. Will these technologies bring about a new upheaval in society? If so, we could truly speak of a second quantum revolution.

Biography

Alain Aspect was awarded the 2022 Nobel Prize in Physics, jointly with John Clauser and Anton Zeilinger, "for experiments with entangled photons, establishing the violation of Bell inequalities and pioneering quantum information science".

Prof. Alain Aspect is a former student of ENS Cachan and Paris-Sud University (currently Paris-Saclay University). He has held positions at the Institut d'Optique, ENS Yaoundé (Cameroon), ENS Cachan, ENS/Collège de France, CNRS. He is currently professor (Augustin Fresnel chair) at the Institut d'Optique Graduate School (Paris-Saclay University), professor at the Ecole Polytechnique (Polytechnic Institute of Paris) and director of research emeritus at the CNRS.

Prof. Aspect is a member of several science academies in France, Italy, the USA, Austria, Belgium, and the UK. He received numerous accolades and honors. In 2005, he was named Knight of the Legion of Honor. He received the Medal of the City of Paris, was named Commander of the Palmes academics and received the title of Officer of the National Order of Merit in the same year (2011). In 2014, he was named Officer of the Legion of Honor. And in 2022, he received the title of commander of the Legion of Honor.

Among many awards, he received the CNRS Gold Medal (2005), the Wolf Prize in Physics (2010), the Balzan Prize for Quantum Information (2013), the Niels Bohr Gold Medal (2013), Albert Einstein Medal (2013) and Ives Medal from the Optical Society of America (2013). *Alain Aspect was awarded the Nobel Prize in Physics in 2022 by the Royal Swedish Academy of Sciences.*

Alain Aspect's experimental work focused on testing Bell's inequalities with pairs of entangled photons (PhD, 1974-1983); wave–particle duality for single photons (1984-86, with Philippe Grangier); the cooling of atoms by laser under photon recoil (1985-1992, with Claude Cohen-Tannoudji); ultra-cold atoms, quantum gases and quantum simulators (1992-, in the atomic optics group he created at the Institute of Optics).

Next Generation Secure Communication

Mohamed Bourennane

Stockholm University, Sweden

Abstract

The financial and defense sectors crucially depend on communication through channels that cannot be intercepted by unauthorized people. Today's cryptographic protocols rely on RSA or so-called elliptical curves methods. But there is no guarantee that today's cryptographic protocols will remain safe in the near future. Fortunately, quantum mechanics makes it possible to solve the key transfer problem in a new and proven safe manner. Unlike classical methods, it is the nature's laws that guarantee the security of quantum cryptography. I will introduce and review quantum secure communication advances and also the worldwide and our effort in quantum technologies.

Biography

Mohamed Bourennane is a professor at Stockholm University. He is a graduate of the University of Science and Technology—Houari Boumediene, Algiers, Algeria. He has obtained his PhD from the Royal institute of Technology, Stockholm. He was a researcher at Ludwig Maximilians University, Munich and Max Planck Institute for Quantum Optics, Garching, Germany. He has obtained the six years senior research fellow from the Swedish Research Council (VR). Today, he has established very young and dynamics research group in quantum information and quantum optics at Stockholm University. He has initiated, managed and led projects financed from, VR, Knut and Alice Wallenberg Foundation (KAW), Stiftelsen Olle Engkvist, Carl Tryggers Foundation and the Swedish Agency for Exchange Programs (STINT), Defence Material Administration (FMV), ABB-Hitachi, EU and Polish National Foundation. He is an elected member of the Royal Swedish Academy of Sciences.

The Alchemy of Vacuum

Thomas W. Ebbesen

USIAS & ISIS, University of Strasbourg & CNRS, France

Abstract

Over the past decade, the possibility of manipulating material and chemical properties by using hybrid light–matter states has stimulated considerable interest [1-3]. Such hybrid light–matter states can be generated by strongly coupling the material to the spatially confined electromagnetic field of an optical resonator. Most importantly, this occurs even in the dark because the coupling involves the electromagnetic fluctuations of the resonator, the vacuum field. After introducing the fundamental concepts, examples of modified properties of strongly coupled systems, such as chemical reactivity, charge and energy transport, superconductivity and magnetism, will be given to illustrate the broad potential of light–matter states.

[1] Garcia Vidal, F. J., Ciuti, C., Ebbesen, T. W.: Science **373**, eabd336 (2021)
[2] Genet, C., Faist, J., Ebbesen, T. W.: Phys. Today **74**, 42 (2021)
[3] Nagarajan, K., Thomas, A., Ebbesen, T. W.: J. Am. Chem. Soc. **143**, 16877 (2021)

Biography

Thomas W. Ebbesen is a Norwegian physical chemist who has done research in nanoscience around the world. He studied in the U.S., obtaining his bachelor's at Oberlin College in Ohio before moving to France, where he obtained his PhD at the Pierre and Marie Curie University in the early 1980s. He then moved back to the USA to work at the Notre Dame Radiation Laboratory, where he spent several years doing research in photo-physical chemistry.

His contribution to nanoscience began in 1988 when he moved to NEC in Tsukuba, Japan. He started working on the synthesis and on the properties of fullerenes, in particular, superconductivity, before drifting his attention toward carbon nanotubes. In 1992, working in collaboration with Pulickel Ajayan, he discovered an easy way to produce carbon nanotubes in large quantities. He went on to study the mechanical and electronic properties of single nanotubes.

He unexpectedly observed light propagation through holes much smaller than the light wavelength. The phenomenon was explained by the interaction of light with electron waves at the metal surfaces (plasmons), and published in 1998, just before Ebbesen returned to France.

Since 1999, Ebbesen has worked at the Institut de Science et Ingénierie Supramoléculaires (ISIS) in Strasbourg, which he directed from 2004 to 2012. His research interest still focuses on the properties of plasmonic nanostructures and the interactions between plasmons and molecules.

He has received several awards for his contribution to nanoscience, including the Agilent Europhysics Prize in 2001 for his work on nanotubes, the France Telecom Prize of the French Academy of Sciences in 2005, and the Quantum Electronics and Optics Prize of the European Physical Society in 2009. He is also a member of the Institut Universitaire de France, the Norwegian Academy of Science and Letters, the French Academy of Science and the Royal Flemish Academy of Belgium.

Advances in Quantum Medical Image Analysis Using Machine Learning

Khaled Elleithy

Bridgeport University, Connecticut, USA

Abstract

Quantum machine learning (QML) is an interdisciplinary field combining quantum computing (QC) and machine learning (ML). It has gained increased attention due to advances in near-term hardware implementations of quantum devices. The use of QML has proven to result in a significant improvement in performance and computational speed. Consequently, QML has become an effective technique for data processing and classification. Researchers have recently proposed various QML solutions in the medical image analysis field to gain an advantage of quantum supremacy. The main objective of this speech is to present a holistic review of current leading-edge published works in the quantum medical image analysis field with a focus on supervised learning using artificial neural networks. A comparative study is used to pinpoint the potential of existing techniques, the most promising techniques and the future of research in this area.

Biography

Dr. Elleithy has worked in academia for the past 30 years in various administrative and teaching roles, including a PhD Program Director, Online MS Program Advisor, Associate Dean for Engineering, Associate Vice President for Graduate Studies and Research, Associate Dean of Engineering, Business and Education and Dean of the College of Engineering, Business and Education.

Dr. Elleithy published over 400 research papers in national/international journals and conferences with 5,000+ Google Scholar citations. His most recent research results in quantum computing, security of wireless communications, steganography and data fusion in wireless sensor networks represent noteworthy contributions to the sciences and technology fields.

Dr. Elleithy was the PI or Co-PI of over three million dollars funded research projects in the past twenty years. Sponsors include ARDEC, United Nations, Connecticut NASA Space Grant, CISCO, the University of Connecticut START program, the University of Bridgeport CTNEXT, Saudi Aramco and King Abdul Aziz City of Science and Technology (KACST).

Dr. Elleithy was the PhD dissertation advisor for 27 students. PhD students in his research group won more than forty awards at the state and national levels for their research papers and posters. Many have participated in funded research projects and published their research results in quality journals and conferences.

Dr. Elleithy has been heavily involved with numerous professional societies during the past 30 years, including the Institute of Electrical Engineering (IEEE), the Association for Computing Machinery (ACM), and the American Society of Engineering Education (ASEE). This involvement includes conference and workshop organizations, leadership, journal editing, and other endeavors.

Dr. Elleithy is the founder and co-chair of the International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering (CISEE), the most significant online engineering conference successfully running from 2005 to 2014. CISSE was technically co-sponsored by CT IEEE several times. He was the Co-chair of the 2014 Zone 1 Conference of the American Society for Engineering Education, Bridgeport, Connecticut, April 3–5, 2014, technically co-sponsored by the IEEE CT section. He was the Chairman of the IEEE Connecticut Conference on Industrial Electronics, Technology & Automation, Bridgeport, October 14–15, 2016. Dr. Elleithy was the IEEE Connecticut Communications Chapter Chair from 2006–2008. Dr. Elleithy was the Chair of the Northeast Conference of the American Society for Engineering Education, Bridgeport, Connecticut, October 16–17, 2020.

Dr. Elleithy received the Distinguished Professor of the Year Award from the University of Bridgeport in 2005. He received the 2015 Connecticut Quality Improvement Award (CQIA) Gold Innovation Award. In December 2017, he was elected Fellow of the African Academy of Sciences to recognize his contributions to Wireless Sensor Networks and Wireless Communications. In 2020, Dr. Elleithy received IEEE Connecticut Section Outstanding Member in Academia Award.

Post-Quantum Cryptography: Scientific, Technological and Geopolitical Challenges

Abdellah Mokrane

Paris 8 University, France

Abstract

Since the evidence of the reality of the quantum computer in the 90s and Peter Shor's publication of a fast quantum algorithm for solving encryption problems that had previously been considered very hard, the scientific community and especially researchers in cryptography began intense research over the last 20 years to propose new (classical) encryption algorithms resistant to quantum computing. In this talk, we will explain what are the proposed solutions to this academic and technological challenge. We will also discuss the geopolitical consequences resulting from this coming digital revolution. Along the way, based on Algeria's past experience in the field of encryption and cybersecurity, we will propose a 20-year strategy to tackle this challenge.

Biography

Abdellah Farid Mokrane received a Master's degree in Pure Mathematics from Paris Sud University in June 1988 and a PhD in the field of Algebraic Geometry from the same university in February 1992, then an "Habilitation à Diriger des Recherches" (HDR) from Paris Nord University in November 2003. He held the position Maître de Conférences at the Galilée Institute a college of University of Paris Nord from 1993 to 2004. Since 2004, he has held a full professor position at Paris 8 university. His area of expertise includes algebraic geometry, arithmetic as well as cryptography. He has supervised a dozen doctoral theses, and he was Project Manager at the Ministry of Higher Education and Research in France in charge of the evaluation of research teams and international relations. He has been a visiting professor in different universities around the world and in different international conferences (Japan, India, China, Germany, Italy, USA, UK, Lebanon, Egypt, Mali, Netherlands, Spain, etc). For 20 years, he has been in charge of the Master's degree in Mathematics at Paris 8 university, creating a speciality in arithmetic, cryptography and coding, then a speciality in big data and recently a speciality in cybersecurity and data sciences. He developed a very intense collaboration with Algeria in the fields of teaching, PhD advising, research and development through notably the following institutions: CF-DAT, IHESN, EMP, DGRSDT, USTHB, etc.

Contents

An Overview of Quantum Key Agreement Protocols

Youssouf Achouri[1](✉), Rima Djellab[2], and Khaled Hamouid[3]

[1] LaSTIC laboratory, University of Batna 2, 05000 Batna, Algeria
y.achouri@univ-batna2.dz
[2] LAMIE laboratory, University of Batna 2, 05000 Batna, Algeria
r.djellab@univ-batna2.dz
[3] LIGM, ESIEE Paris, University of Gustave Eiffel, 93162 Noisy-le-Grand, France
khaled.hamouid@esiee.fr

Abstract. Quantum Key Agreement (QKA) stands as a pivotal protocol in quantum cryptography, facilitating the shared creation of a secret key among participants over an insecure communication medium. This study explores the complex theoretical foundations and intricate mathematical frameworks integral to QKA. Additionally, it presents a structured analysis and categorization of various multi-party Quantum Key Agreement mechanisms, an increasingly significant topic in the quantum computing era. Each approach is scrutinized for its strengths and weaknesses, providing a comprehensive comparative study that covers their real-world applications and the unique challenges they face. Striking a balance between detailed technical exposition and perceptive observations on the broader implications of these quantum technologies, this paper offers a well-rounded view on advancing secure quantum communication systems. The goal of this research is to furnish readers with a thorough understanding of QKA principles and an insightful perspective on the diverse opportunities and obstacles presented by different multi-party QKA frameworks.

Keywords: quantum key agreement · multiparty quantum key agreement · quantum key distribution

1 Introduction

Key agreement protocols, also recognized as key exchange protocols, are central to the practice of cryptography. They enable parties to generate cryptographic keys collaboratively, allowing for the secure transmission of information over public channels without the prior exchange of secret keys.

The landmark research by Diffie and Hellman in 1976 unveiled a technique for two entities to share a secret key securely, thereby protecting their exchanges from unauthorized snooping [1]. This innovation spurred further investigation into expanding the protocol to include multiple parties, as documented in subsequent academic research [2–4].

H. Drias and F. Yalaoui (Eds.): QSAC 2023, ISEM 2, pp. 1–14, 2024.
https://doi.org/10.1007/978-3-031-59318-5_1

Quantum cryptography introduces a transformative approach to securing communications, deeply rooted in the core principles of quantum mechanics, and offers unparalleled levels of security [5]. The introduction of the BB84 protocol for quantum key distribution by Bennett and Brassard in 1984 sparked significant excitement and progress in this field [6]. This pivotal moment led to the development of multiple quantum cryptography applications, such as techniques for distributing quantum keys [7,8], mechanisms for sharing quantum secrets [9,10], systems for secure direct quantum communication [11,12], and methods for conducting quantum comparisons in private [13,14]. Quantum Key Agreement (QKA) leverages quantum mechanics to equitably and securely generate cryptographic keys, inherently protecting against the potential risks brought by quantum computing. This is achieved through adherence to quantum phenomena like the Heisenberg uncertainty principle and the no-cloning theorem, creating an effective shield against advanced quantum threats [15,16]. The introduction of QKA was marked in 2004 with the presentation of the first protocol for quantum-based key agreement [17], which has led to the creation of a comprehensive array of protocols tailored for both dyadic [18–22] and collective frameworks [23–34].

Quantum key agreement models are generally differentiated by their design and operational efficiency [35]. This differentiation includes the Tree MQKA protocol, enabling the exchange of sensitive information through quantum communication; the Complete Graph MQKA protocol, facilitating information sharing among all protocol participants; and the Circle MQKA protocol, in which participants circulate a sequence of particles that represent their private keys to others in a circular manner, ensuring the encryption of data returns to the initiator.

This paper aims to offer a detailed exploration of quantum key agreement (QKA), beginning with an introduction to the principles of quantum computing and its specific language. We will outline QKA, contrast it with Quantum Key Distribution (QKD), and highlight the advantages of QKA for secure, sustainable communication networks. Further, we will examine the three main multi-party QKA configurations-circle, tree, and complete graph-analyzing their benefits and drawbacks. This discussion aims to provide a systematic framework for classifying QKA approaches, facilitating strategic decision-making among researchers and practitioners.

2 Preliminary Knowledge

The focal point of this section lies in comprehending quantum computing. Our exploration begins with an introduction to bra-ket notation, establishing a foundational understanding. We then delve into the captivating phenomena of superposition and entanglement. Lastly, we demystify the operation and measurement processes by delving into the realm of quantum gates [36].

2.1 Unraveling Quantum Notation: The Essence of Bra and Ket

Quantum computing operates with qubits as its core elements, which are the quantum analogs of classical bits. The handling and interaction of these qubits lay the groundwork for quantum computational processes. For the articulation of a qubit's state and its basis within this field, a distinct notation known as bra-ket notation is predominantly employed.

Understanding Bra Notation. At the forefront of Bra notation is the symbol $\langle . |$, playing a pivotal role. In this setting, the symbols '0' and '1' under the Bra category act as essential elements on a two-dimensional vector plane. To elaborate, $\langle 0|$ is equivalent to the vector [1 0], and conversely, $\langle 1|$ aligns with the vector [0 1].

Exploring Ket Notation. Conversely, within the quantum realm, the notation $|.\rangle$, where the dot symbolizes the core aspect, signifies Ket notation. As an example, the Ket notations can be articulated as: $|0\rangle =[1\ \ 0]^*$ and $|1\rangle =[0\ \ 1]^*$. It is crucial to acknowledge that Bra notation is essentially the conjugate transpose of Ket notation.

The notations $|0\rangle$ and $|1\rangle$, along with their corresponding Bra notations $\langle 0|$ and $\langle 1|$, establish the conventional bases on a two-dimensional plane. These notational forms are chiefly utilized to depict and define a qubit's state within quantum computational operations.

2.2 Exploring Superposition and Measurement in Quantum Systems

Quantum computing introduces the fascinating concept of superposition, where qubits are in a state that encompasses both $|0\rangle$ and $|1\rangle$ simultaneously. This state of superposition is typically expressed in the Z-basis, with a qubit's state represented as $(\alpha\,|0\rangle + \beta\,|1\rangle)$. When measuring this superposed state, the likelihood of finding the qubit in the $|0\rangle$ state is $|\alpha|^2$, and in the $|1\rangle$ state is $|\beta|^2$, ensuring the sum of these probabilities equals one, $|\alpha|^2 + |\beta|^2 = 1$.

Observing the qubit along varying axes yields different measurement outcomes. Notably, the X-basis offers an alternative perspective on the qubit's state:

Quantum States Along the Z-Axis.

$$|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle); |1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle) \tag{1}$$

Quantum States Along the X-Axis.

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle); |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{2}$$

2.3 The Phenomenon of Quantum Entanglement and Its Effects

Quantum mechanics unveils that when two photons are entangled, their connection persists across vast distances, whether they are mere nanometers or several kilometers apart. Quantum entanglement suggests that the act of measuring the properties of one photon immediately influences the state of its counterpart, irrespective of the spatial gap separating them.

Entanglement's significance shines through in the example of Bell states, illustrating how the observation of one qubit instantly sets the state of its entangled partner. For example, given the Bell state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{12}$, a measurement resulting in $|0\rangle$ for the first qubit means the second qubit is also in the state $|0\rangle$, even in the absence of direct observation.

We proceed to explore the intricacies of qubits within Bell and GHZ states:

Bell States Revisited.

$$\begin{aligned} |\Phi^{\pm}\rangle_{AB} &= \tfrac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)_{AB} \\ |\Psi^{\pm}\rangle_{AB} &= \tfrac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)_{AB} \end{aligned} \tag{3}$$

GHZ States Elaborated.

$$\begin{aligned} |\Psi_{1,5}\rangle_{ABC} &= \tfrac{1}{\sqrt{2}}(|000\rangle \pm |111\rangle)_{ABC} \\ |\Psi_{2,6}\rangle_{ABC} &= \tfrac{1}{\sqrt{2}}(|001\rangle \pm |110\rangle)_{ABC} \\ |\Psi_{3,7}\rangle_{ABC} &= \tfrac{1}{\sqrt{2}}(|010\rangle \pm |101\rangle)_{ABC} \\ |\Psi_{4,8}\rangle_{ABC} &= \tfrac{1}{\sqrt{2}}(|011\rangle \pm |100\rangle)_{ABC} \end{aligned} \tag{4}$$

2.4 Quantum Gates: Building Blocks of Quantum Computation

Quantum gates play a crucial role in quantum computation, serving as the fundamental building blocks for various quantum algorithms and operations. These gates are unitary transformations that can be applied to individual qubits or multiple qubits collectively.

In some cases, a unitary operation may act on a single qubit without affecting the entire entangled state. This ability to address individual qubits independently is a significant advantage in quantum computing.

In the upcoming subsections, we will introduce the four fundamental single-qubit gates, each of which contributes to the versatility and power of quantum computing:

$$\begin{aligned} I &= \begin{pmatrix} 1\,0 \\ 0\,1 \end{pmatrix}, \sigma_x = \begin{pmatrix} 0\,1 \\ 1\,0 \end{pmatrix} \\ \sigma_y &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{aligned} \tag{5}$$