Lecture Notes on Data Engineering
and Communications Technologies 133

Adarsh Kumar
Sukhpal Singh Gill
Ajith Abraham *Editors*

Quantum and Blockchain for Modern Computing Systems: Vision and Advancements

Quantum and Blockchain Technologies: Current Trends and Challenges

Springer

Lecture Notes on Data Engineering and Communications Technologies

Volume 133

The aim of the book series is to present cutting edge engineering approaches to data technologies and communications. It will publish latest advances on the engineering task of building and deploying distributed, scalable and reliable data infrastructures and communication systems.

The series will have a prominent applied focus on data technologies and communications with aim to promote the bridging from fundamental research on data science and networking to data engineering and communications that lead to industry products, business knowledge and standardisation.

Indexed by SCOPUS, INSPEC, EI Compendex.

All books published in the series are submitted for consideration in Web of Science.

Adarsh Kumar · Sukhpal Singh Gill ·
Ajith Abraham
Editors

Quantum and Blockchain for Modern Computing Systems: Vision and Advancements

Quantum and Blockchain Technologies: Current Trends and Challenges

Springer

Editors

Adarsh Kumar
Department of Systemics
University of Petroleum and Energy Studies
Dehradun, Uttarakhand, India

Ajith Abraham
Scientific Network for Innovation
and Researsch Excellence
Machine Intelligence Research
Labs (MIR Labs)
Auburn, WA, USA

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

ISSN 2367-4512 ISSN 2367-4520 (electronic)
Lecture Notes on Data Engineering and Communications Technologies
ISBN 978-3-031-04612-4 ISBN 978-3-031-04613-1 (eBook)
https://doi.org/10.1007/978-3-031-04613-1

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

Preface

In recent decades, advancements in Blockchain and quantum technology have been the subject of technical, professional and business discussions in a variety of venues. As a result of these technologies and their combination with other valuable technologies of recent years, several applications and abilities have been created, including the ability to provide transparent and redundant safe, responsible, and efficient settings. For example, Blockchain technology provides a secure, distributed, peer-to-peer and decentralised network that is based on sophisticated cryptographic primitives and protocols that may be used to transact in real time. These cryptographic primitives and protocols aid in the achievement of high-security needs that are resource-dependent. Quantum physics and Blockchain solutions may now be merged with other technologies. These include Internet of Things (IoT), cloud/fog/edge computing, Serverless computing and Next Generation Networks. Incorporating diverse technologies requires comparative study, rules and application-specific use. Thus, our work encourages people from other sectors to develop technology-integrated solutions that are low-cost, high-quality, secure and fulfil future expectations. As a conclusion, this book helps readers and practitioners develop abilities in developing next generation systems based on security cryptographic primitives and protocols. Finally, IT professionals may use this study to better understand the need for technological transitions and quantum computing activities. Constructing quantum computing systems and communicating with them are novel technological features that may greatly affect future applications. Among research challenges, this book provides a comprehensive study over those approaches that improve quantum computing and cryptography protocols. For example, Quantum Key Distribution methods are studied and improved using security proofs against individual and collective computing environments. These computing environments can help in producing more than a few GB/s of security bits in the computing world that are sufficient to protect the network against quantum attacks. This book provides strong knowledge insight into various issues identified about Quantum and Blockchain networks and helps to develop solutions towards trust management in a secure network, quantum computing and quantum science, quantum memories, quantum repeaters and many more. This book aims to provide technical insight into Quantum and Blockchain technology aspects such as the current state-of-the-art requirements, performance, evaluation and challenging aspects, to the readers in one place. The book is organised as follows:

Chapter "Quantum Technologies I: Information, Communication, and Computation" presents fundamental quantum information science ideas and methods and how these concepts and tools may be helpful to quantum Blockchain technology. Starting with quantum mechanics postulates, which define the theory's fundamental laws that deviate from classical mechanics. Next, this chapter introduces the abstract concepts of quantum information science. Next, this work presented multiple controlled Tooli gates, which may be used in quantum computing and quantum Blockchain. Further, this chapter discusses quantum error correction, a method for protecting qubits (quantum information units) from environmental noise and developing fault-tolerant quantum technology.

Chapter "Quantum Technologies II: Cryptography, Blockchains, and Sensing" expands on the concept of quantum technology introduced in the preceding chapter. The main responsibilities of quantum information processing are quantum communication and quantum sensing. Quantum data is further separated into quantum cryptography and quantum Blockchain. Quantum cryptography discusses the security of quantum cryptosystems. Quantum Blockchain is a decentralised, distributed and public digital ledger in quantum world. Finally, quantum sensing emerges from quantum mechanical particles/systems like photons.

Chapter "Empirical Analysis of Security Enabled Quantum Computing for Cloud Environment" studies that quantum cloud computing is a popular tool in the digital industry. Most quantum experts think it will improve cloud services. It includes installing quantum computation sources in a cloud environment to tackle atomic plus software-based cloud computing. Further, this work presented an analysis of the advantages and disadvantages of utilising quantum computing with cloud systems. The same goes for recent updates and quantum as a cloud service. This work showcases quantum services as well.

Chapter "Photonic Quantum Computing" focuses on photonics quantum computing and its uses. Due to minimal or negligible loss and ability to work at ambient temperature, the Photonic Quantum Computers meet five of Vincenzo's seven requirements. As a result, substantial research has been done on the practical implementation of scalable Photonic Quantum Computers. Quantum Machine Learning, Quantum Cryptography and Quantum Key Distribution are all uses of Photonic Quantum Computers.

Chapter "A Conceptual Framework for Scaling and Security in Serverless Environments Using Blockchain and Quantum Key Distribution" explains that today, Serverless computing is a popular deployment strategy. It is a concept where the execution environment is not predefined but scaled on demand. Cloud computing, which relies on this concept, has gained importance. This chapter has explored cloud computing concepts, Blockchain concepts and networking concepts for futuristic applications.

Chapter "Implications of Quantum Science on Industry 4.0: Challenges and Opportunities" explains the current capability of quantum leaves some processes vulnerable, yet its immense power of computation opens doors to amazing developments in the field. This review discusses the consequences in various domains, and a comprehensive road map of future occurrences is drawn.

Chapter "Quantum Generative Modelling and Its Use Cases" discusses that a generative model shows how a probability model samples a dataset. It also includes techniques for generative model optimization and quantum generative model-based. The variational quantum Eigen solver is explained for molecular simulation and optimization. Our quantum generative model can generate pharmaceuticals and financial option pricing. Several applications have compared quantum generator algorithms to traditional machine learning techniques. Quantum generator algorithms outperform traditional machine learning algorithms. This brings us to quantum advancement in Artificial Intelligence (AI).

Chapter "A Comprehensive Overview of Quantum Internet: Architecture, Protocol and Challenges" presents that the Quantum Internet is an interconnected network of distant quantum devices. The main benefits of Quantum Internet are its independence from traditional internet, safe data transfer and cutting-edge bling computing. This work examines the foundations of Quantum Computing and Quantum Internet. Further, it explores quantum entanglement, quantum bits and quantum states.

Chapter "Quantum Solutions to Possible Challenges of Blockchain Technology" presents that the quantum computing has made existing Blockchain cryptosystems more vulnerable. Modern algorithms like Shor's massive integer factorization and Grover's unstructured database search are exponentially faster than quantum methods. Public-key and asymmetric key cryptosystems are both susceptible, needing quantum-secure encryption. Further, it investigates conventional scalability and security primitives. The key sizes, hash lengths, execution times, computing overhead, and energy efficiency of Bitcoin, Ethereum, and Corda are listed and compared.

Chapter "Futuristic Technologies for Supply Chain Management: A Survey" prepares thorough and critical insights into the present advances and future visions of technologies associated with supply chain management such as IoT, Artificial Intelligence/Machine Learning, Blockchain and Quantum Computing. Today's supply chain is more complex than ever, combining people, processes and technology. Businesses must balance resilience and profitability in the face of global pandemics like Ebola. Customer and supplier network awareness may help many organisations. Along with AI and machine learning, supply chain organisations need IoT to automate product monitoring, fleet tracking and other processes.

Chapter "Quantum Computing and Quantum Blockchain: Recent Advancements, Analysis and Future Directions" examines recent developments in Quantum Computing (QC). This study explores quantum physics, quantum gates and quantum circuits. A case study that illustrates the QC-based concepts is presented.

Chapter "Secure Blockchain-Based Mental Healthcare Framework: —A Paradigm Shift from Traditional to Advanced Analytics" educates the reader about the Blockchain technology, its influence on mental healthcare, and to bring attention to a conceptual framework for safe mental health analytics that will be implemented in nearby future. It's important to keep in mind that figuring out the full advantages of Blockchain technology is still a work in progress.

This book servers as an essential knowledge resource for the students at the graduate level from different engineering disciplines such as Physics, Computer Science and Engineering, Applied Computer science, space engineering, Data Science, and Business Analytics. This book acts as a bridging information resource between basic concepts and advanced level contents from technical experts to quantum and Blockchain communities and hobbyists towards enhancing their knowledge and proficiency. This book facilitates the research group to publish novel work towards the advancement of emerging technologies in applications of quantum and Blockchain disciplines.

Dehradun, India	Adarsh Kumar
London, UK	Sukhpal Singh Gill
Auburn, WA, USA	Ajith Abraham

Contents

Quantum Technologies I: Information, Communication, and Computation

Emilio Peláez, Minh Pham, and U. Shrikant

Abstract In this chapter, we introduce some of the notions of quantum information science including aspects of information, information security, entanglement states, quantum gates, teleportation, direct secure communication, quantum secret sharing, quantum noise, quantum operations, quantum error correction, quantum circuits and quantum Toffoli gate. Most of these aspects are of importance in quantum enhanced technologies including quantum blockchain. The objective of this chapter is to introduce the basic notions of quantum information science aspects with its real-time need and usage, including some notes on how the above mentioned concepts and tools might be helpful in quantum blockchain technology. The chapter is organized into three major sections as follows. Starting from postulates of quantum mechanics, which set the basic rules of the theory which drastically deviates from the classical mechanics. Then we introduce, in Sect. 1 the basic notions of quantum information (QI) science as described in the abstract. Section 2 is dedicated to multiple controlled Toffoli gate, which may find its application in may areas of quantum computing and also in quantum blockchain. Section 3 is dedicated to certain aspects of quantum error correction, a scheme to protect qubits (units of quantum information) from environmental noise, which helps develop fault-tolerant quantum technologies. In Conclusion section, we note how the content in this chapter might be relevant to quantum blockchain technology. A table of symbols is given in Appendix.

E. Peláez (✉) · M. Pham
The University of Chicago, Chicago, IL, USA
e-mail: epelaez@uchicago.edu

M. Pham
e-mail: mpham26@uchicago.edu

U. Shrikant
The Institute of Mathematical Sciences, Chennai, India
e-mail: shrikantu@imsc.res.in

A. Kumar et al. (eds.), *Quantum and Blockchain for Modern Computing Systems: Vision and Advancements*, Lecture Notes on Data Engineering and Communications Technologies 133, https://doi.org/10.1007/978-3-031-04613-1_1

1 Quantum Information

Quantum information (QI) science [1] is now attracting scientists from different disciplines. Last decade has been intense for QI science, in theory and even in experiments. There have been announcements by various companies and academia about achieving the so-called "quantum supremacy", a term coined by John Preskill. On the one hand, a quantum computer is purported to outperform any existing classical (digital) one, which is still a debated topic today. However, there are instances of true quantum supremacy that challenges any classical algorithm even in theory. On the other hand, unconditional security provided by quantum cryptography holds enormous promise for future quantum technologies and secure communication. Not to mention, very long distance and also satellite based quantum key distribution have been achieved. Currently, we are living in the Noisy Intermediate Scale Quantum (NISQ) era [2] where NISQ devices are already in use for academic and industrial purposes.

It pertinent to point out that quantum information finds its utility in foundations of physics, such as condensed matter theory, statistical mechanics, thermodynamics, black hole information paradox, foundations of quantum theory, and approaches to solving the long-standing puzzle of finding a quantum theory of gravity including string theory through AdS/CFT correspondence, to name a few. It provides a universal language to study theories without having to worry about what physical system one is using. For example, a quantum state (in discrete variable setting) is a density operator whether we are talking in terms of non-relativistic or relativistic quantum theory. The wonder about quantum theory is that it finds enormous applications in QI science, yet remains mysterious at the foundational level.

However, the aim and scope of this section of the chapter is restricted to introduce the basic notions of QI science. The reader is expected to have basic knowledge in quantum mechanics and linear algebra, and some basics of probability theory. We do not hope to cover all the topics in this section but only basics of QI that finds application in quantum blockchain technology. Quick instances of application to quantum cryptography and communication will be mentioned.

1.1 Postulates of Quantum Mechanics

Here we will take density matrix approach to quantum mechanics since it provides the most generic language for QI theory.

States and operators. A quantum state is given by a vector in a Hilbert space. A state is is more generally represented by a density matrix with the properties that it is hermitian: $\rho = \rho^\dagger$, has unit trace: $\mathrm{Tr}(\rho) = 1$, and is positive semi-definite: $\rho \geq 0$. Since every hermitian operator has a spectral decomposition, the state can be written as $\rho = \sum_i \lambda_i \left|e_i\right\rangle \left\langle e_i\right|$. Here, $\left|e_i\right\rangle$ are the eigenvectors of ρ with the corresponding eigenvalues λ_i, with the requirement that $\sum_i \lambda_i = 1$ and $0 \leq \lambda_i \leq 1$. All *observables* are necessarily Hermitian operators and hence possess real eigenvalues. This is in conformity with what one sees in real experiments. An average of an observable is given by $\langle O \rangle = \mathrm{Tr}(O\rho)$.

Mixed states are those for which $\mathrm{Tr}(\rho^2) < 1$ and *pure states* are those for which $\mathrm{Tr}(\rho^2) = 1$. We will later see that under a noisy evolution, a pure state is transformed into a mixed state, hence the density matrix formalism provides the most generic language for QI and the theories that are statistical in nature.

Dynamics. Quantum dynamics is given by a unitary matrix which takes a quantum state to a quantum state: $\rho' = U\rho U^\dagger$, where $U = \exp\{-iHt/\hbar\}$ is the unitary matrix with H being the Hamiltonian which is the generator of translation in time. The dynamics are unitary and reversible only for a closed system and a unitary operator maps orthogonal states to orthogonal states. We shall later see that for a more general (such as noisy) evolution, the dynamics need not be unitary and reversible.

Measurement and Probabilities. A measurement in quantum mechanics is given by the set of measurement operators $\{M_i\}$ satisfying $\sum_i M^\dagger M \leq \mathbb{1}$. The probability of obtaining an outcome i and the updated state after measurement, respectively, are given by

$$p(i) = \mathrm{Tr}[M_i \rho M_i^\dagger] \quad ; \quad \rho \to \rho' = \frac{M_i \rho M_i^\dagger}{p(i)}. \tag{1}$$

The theory of measurements in quantum mechanics involves two types: projective operator measure (PVM) and positive operator valued measure (POVM). In fact, measurement is an *irreversible* process through which one learns the state of the system. Once measured, the state irreversibly *collapses* to a one of the basis states in which the measured state in expanded into. What quantum theory predicts is the probability of getting a particular basis state which is revealed only after measurement. Quantum measurement indeed acts as a bridge between quantum and classical worlds. Once measured, collapsing the quantum state, quantum information reduces to classical information!

Composite systems. A multipartite state is given by the tensor product of individual parts. For example, a generic two qubit state may be given by $|\psi\rangle^{AB} = \sum_{i,j} p_{ij} |\phi_i\rangle \otimes |\phi_j\rangle$, where $\otimes$ represents the tensor product. A multipartite state is said to be *separable* if it can be written as a tensor product of individual parts. However, quantum mechanics allows for states that cannot be written as a tensor product of marginal states, and the particles represented by such a non-separable joint state are said to be quantum correlated. Examples will be introduced in subsequent sections.

1.2 Classical and Quantum Information

Classical and quantum information are *fundamentally* different [1, 3]. The basic unit of classical information is a *bit* such as a logical/physical 0 or a 1. Quantum information talks of information in terms of a "quantum bit", *qubit* which is a quantum *superposition* of two states: $|\text{qubit}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, where $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$. These matrices may be thought of as corresponding to the orthogonal states of a two-level quantum system such as polarization degrees of a photon or spin degrees of an electron. In fact, these degrees of freedom define what type of quantum system we are talking about, and to be more precise the dimension determines the type of the system. In this subsection we will define some of the main measures of information, classical and quantum. And further mention some of the uses of these definitions in quantum information science.

In 1948, Shannon [4] gave an abstract theory of information which revolutionized the field of information science. Given a binary sequence of bits, which occur with some probability p_i, then the information contained in the signal is simply $I = -\sum_i \log p_i$. This tells us that the less probable an event is the more information it contains! Generally, such an abstract theory is able to provide a language for information processing which doesn't depend on what physical systems are being used. It is now well known that *information is physical* in the sense that, quoting Landauer [5], "information is not an abstract entity but exists only through a physical representation", and hence limited by laws of physics.

As noted earlier, classical information is represented generally by binary bits 0 and 1. Classical computation follows the Boolean algebra. We shall not dwell much on classical computation here and we will focus on the ingredients that are useful in quantum communication and cryptography. Classical communication is done by encoding these bits into physical systems and sent down a communication channel. Most commonly used form of communication is using electromagnetic waves while the communication channel being free air or an optical fiber cable.

In classical information theory [4, 6], information in a signal is encoded as classical bits corresponding to events which occur with certain probability. Consider a random variable $A \in \{a_1, a_2 ...\}$, called the source with symbols $a_1, a_2 ...$ and so on, which occur with probability $p_1, p_2 ...$ and so on, respectively. Then the *Shannon entropy* (SE), which quantifies information in A, given as the negative average of the logarithm of the probability:

$$H(A) = -\sum_a p(A = a) \log(p(A = a)). \tag{2}$$

Here, $H(A)$ is SE and $p(A = a)$ is the probability with which the random variable A takes the random value a. The logarithm is always taken to be base 2, unless otherwise stated. Based on the above definition, one can go on defining various measures of information originating from more than one source, say the random variables A and B. *Conditional entropy* (CE) quantifies the amount of information gained by measuring A when that of Y is known:

$$H(A|B) = -\sum_{a,b} p(a|b)\log[p(a|b)]. \tag{3}$$

Joint entropy (JE) of A and B is given by the information gained from measuring both A and B:

$$H(A, B) = -\sum_{a,b} p(a, b)\log[p(a, b)] \tag{4}$$

where $p(a, b)$ is the joint probability distribution of A and B. JE actually measures total uncertainty about A, B. In fact, CE and JE are related by the expression $H(A, B) = H(A) + H(A|B)$. And Shannon entropy has the sub-additivity property given by $H(A, B) \leq H(A) + H(B)$, with the inequality holding when A and B are dependent and equality holding when they are independent.

Since a quantum state can be thought of as a compendium of probabilities, by simply replacing probability distribution with the density matrix, one can write down the *von Neumann entropy*: $S = -\mathrm{Tr}(\rho\log\rho)$. Since every Hermitian operator is a normal operator, it can be given a spectral decomposition ($\rho = \sum_i p_i |i\rangle\langle i|$) and hence von Neumann entropy reduces to Shannon entropy (2) in the basis $\{|i\rangle\}$, which are the eigenvectors of ρ, and p_i are the eigenvalues of the operator ρ.

Quantum version of every definition of the classical entropy measures can be obtained by replacing the classical probability distribution (p_i) with the density matrix (ρ) and summation $\sum_i$ with Trace operation. For example, conditional entropy is $S(\rho_A|\rho_B) = S(\rho_{AB}) - S(\rho_A)$, where $S(\rho_A) = -\mathrm{Tr}(\rho_A\log\rho_A)$ and $S(\rho_{AB}) = -\mathrm{Tr}\rho_{AB}\log\rho_{AB}$, is the joint entropy of A and B.

1.2.1 Distance Measures and Fidelity

A common question in classical information theory is to ask how close any two probability distributions are and how well can one tell them apart. A distance measure tells how much two probability distributions differ. In classical information theory, one learns about Kolmogorov distance [1]: given two probability distributions p and q, the distance between them is given by $d(p, q) = \frac{1}{2}\sum_i |p_i - q_i|$. Whereas in quantum information theory, a number of equivalent distance measures are defined. For example, trace distance between any two quantum states ρ_1 and ρ_2 is defined as

$$D(\rho_1, \rho_2) = \frac{1}{2}\|(\rho_1 - \rho_2)\|_1 \tag{5}$$

where $\|A\|_1 = \sqrt{A^\dagger A}$ is the L_1 norm or trace norm of an operator A. Trace distance in fact gives a maximum bound on how much information one can reliably send down a quantum channel while the distance is taken between the states $\Phi[\rho]$ and ρ, where Φ is the quantum channel.[1]

One can also define a measure to quantify how close two states are which is given by the fidelity: $F = \mathrm{Tr}(\rho_1 \rho_2)$. Fidelity has other useful forms such as the one due to R Josza:

$$F = (\mathrm{Tr}\sqrt{\sqrt{\rho_2}\rho_1\sqrt{\rho_2}})^2. \tag{6}$$

Uhlmann's theorem for fidelity states that given a *purification* $\left|\phi_{\rho_1}\right\rangle$ of the a state ρ_1

$$\left|\phi_{\rho_1}\right\rangle = \sum_{i=1}^{k} \sqrt{p_i}\, |i\rangle \otimes |i\rangle \tag{7}$$

where $\{|i\rangle\}$ are the orthonormal basis in $\mathcal{H}^k$, then the fidelity

$$F(\rho_1, \rho_2) = \max_{|\phi_{\rho_1}\rangle} |\langle \phi_{\rho_1} | \phi_{\rho_2} \rangle|^2 \tag{8}$$

quantifies the maximum overlap between purifications. Interestingly, trace distance (5) is an upper bound of the fidelity:

$$F(\rho_1, \rho_2) \leq 1 - \frac{1}{4}\|\rho_1 - \rho_2\|^2. \tag{9}$$

Another well-known distance measure is Bures distance: $\mathcal{B} = \sqrt{2 - 2\sqrt{F(\rho_1, \rho_2)}}$, where $F(\rho_1, \rho_2)$ is the fidelity given in Eq. (6).

1.2.2 Entangled States

Quantum entanglement [7] is a type of spatial correlation between quantum systems that can not be created with classical resources. It finds applications in many areas of quantum information science, specifically quantum communication and cryptography.

An example of a spatially quantum-correlated state is an entangled (Bell) state:

$$|\phi\rangle_{ij} = \frac{1}{\sqrt{2}}(|0j\rangle + (-1)^i)\left|1\bar{j}\right\rangle \tag{10}$$

[1] We shall define what a quantum channel is in a moment.

Here, when $|j\rangle = |0\rangle$, $|\bar{j}\rangle = |1\rangle$. The above four Bell states $|\phi\rangle_{ij}$ are orthonormal and form the so-called Bell basis $\{|\phi\rangle_{00}, |\phi\rangle_{01}, |\phi\rangle_{10}, |\phi\rangle_{11}\}$. However, there are other special class of *mixed* entangled states such as Werner state: a convex mixture of the four Bell states given in (10)

$$|\Psi\rangle^{\text{Werner}} = f\,|\phi\rangle_{00} + \frac{1}{3}(1-f)(|\phi\rangle_{01} + |\phi\rangle_{10} + |\phi\rangle_{11}) \tag{11}$$

which is entangled only for $\frac{2}{3} \leq f \leq 1$. This shows that a superposition of maximally entangled states need not be maximally entangled.

Even today, multi-particle entanglement theory is not fully developed. However, there are a class of states, called GHZ[2] states, which find applications in quantum information science. A multi-*qubit* GHZ state given by [8]

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\cdots 0\rangle + |111\cdots 1\rangle). \tag{12}$$

Here, the notion $|000\cdots 0\rangle \equiv |0\rangle \otimes |0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle$. Another class of multipartite entangled state, that finds numerous applications, is the W state. A simple 3-qubit W state is given by [9]

$$|W\rangle = \frac{1}{\sqrt{2}}(|001\rangle + |010\rangle + |100\rangle), \tag{13}$$

GHZ and W states can be generalized for arbitrary higher (finite) dimensional systems, which we omit in this section for simplicity.

Entanglement need not necessarily be between only discrete variables. One can even create *hybrid* states of particles that are entangled between their continuous and discrete degrees of freedom. Entangled states, which were of theoretical interest, are now being exploited as resources in quantum computing [10]. Another class of states are the *hyper*-entangled states [11, 12] in which two particles are entangled in more than one discrete degrees of freedom.

1.2.3 Mutual Information, Holevo Bound and Information Security

Let A and B be two systems with corresponding quantum states ρ_A and ρ_B, respectively. Quantum mutual information quantifies the amount of information common to both systems. Moreover, it is the measure of correlations between the two system states. It is given by [1]

$$I(A:B) = S(A) + S(B) - S(A, B) \tag{14}$$

[2] This abbreviation stands for the authors Greenberger, Horne , and Zeilinger and independently due to Mermin.

where $S(A : B)$ is the joint entropy. Now suppose Alice wants to send information to Bob via general mixtures ρ_i prepared with probabilities p_i. This situation can occur when Alice sends pure states $|\psi\rangle_i$ down a *noisy* quantum channel, due to which the pure state becomes a mixed state. The total message is given by $\rho = \sum_i p_i \rho_i$. Given that, how much information Bob can decode on his side? The amount of *classical* information he can extract is bounded by

$$I(A : B) \leq S(\rho) - \sum_i p_i S(\rho_i). \tag{15}$$

The right hand side is called Holevo information or the χ quantity. The amount of classical information that can be encoded in, and hence extracted from, a quantum system is upper bounded by χ quantity.

In quantum cryptography and communication, a protocol is provably secure if the mutual information between the legitimate parties $I(A : B)$ is greater than that between Alice and the eavesdropper, Eve, i.e., $I(A : B) > I(A : E)$ which leads to positive secure key rate: $\kappa = I(A : B) - I(A : E) > 0$. However, this kind of security is in general true only for individual attacks, where Eve attacks the particle at every round of communication. More generally, Eve can adopt a strategy where she chooses to attack all the particles at the end, which is called the collective attack. In such a case the secure key rate is given by $\kappa = I(A : B) - \chi(E)$, where $\chi(E)$ is the Holevo information learned by Eve.

The above definition of information security of quantum key distribution based on mutual information is not "composable". It is in the sense that it is valid if one is restricted to only one cryptosystem. When more than one cryptosytems are used, one needs a composable definition. However, for many general purposes, it suffices to use the above definitions.

1.2.4 The No-Cloning Theorem

No cloning theorem states that given a quantum state $|\psi\rangle$, there is no unitary operator such that $U|\phi\rangle \rightarrow |\phi\rangle |\phi\rangle$. The proof the theorem ultimately stems from the linearity of quantum mechanics. Let us assume that there exists a unitary U which clones the state $|\phi\rangle$ such that $U|\psi\rangle = |\phi\rangle \otimes |\phi\rangle$. If $|\phi_1\rangle = |0\rangle$, then $U|0\rangle = |0\rangle |0\rangle$. However, if the state is *unknown* i.e., an arbitrary superposition $|\phi\rangle = \alpha |\phi_1\rangle + \beta |\phi_2\rangle$, then due to linearity the copying machine should output $U|\phi\rangle = |\alpha|^2 |\phi_1\phi_1\rangle + |\beta|^2 |\phi_2\phi_2\rangle$ which is not the same as

$$\begin{aligned} |\psi\rangle \otimes |\psi\rangle &= (\alpha |\phi_1\rangle + \beta |\phi_2\rangle) \otimes (\alpha |\phi_1\rangle + \beta |\phi_2\rangle) \\ &= |\alpha|^2 |\phi_1\phi_1\rangle + |\beta|^2 |\phi_2\phi_2\rangle + \alpha^*\beta |\phi_1\phi_2\rangle + \beta^*\alpha |\phi_2\phi_1\rangle . \end{aligned} \tag{16}$$

In other words, no cloning theorem states that an *unknown* quantum state cannot be cloned perfectly. Once measured, it collapses into a classical state which then can be obviously cloned. No cloning theorem also says that a pair of non-orthogonal states can't be copied with perfect fidelity since they can't be reliably distinguished in a measurement. Let ψ_1 and ψ_2 be two orthogonal states. Then $U\,|\psi_1\rangle = |\psi_1\rangle \otimes |\psi_1\rangle$ and $U\,|\psi_2\rangle = |\psi_2\rangle \otimes |\psi_2\rangle$. Now, the overlap between the two states before and after cloning should be equal i.e. $\langle\psi_1|\psi_2\rangle = (\langle\psi_1|\psi_2\rangle)^2$ which is possible only when either both states are same, or both are orthogonal. For example, when $|\psi_1\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|\psi_2\rangle = |0\rangle$, these two states cannot be cloned with perfect fidelity because they are not orthogonal to each other.

No cloning has important and fundamental implications in quantum cryptography [13]. An eavesdropper won't be able to copy a quantum state without producing detectable disturbance, which then can be detected by the legitimate parties who wish to communicate secretly. More the disturbance one creates during a measurement process, the more information one will be able to gather about the quantum system being disturbed. This is at the heart of cryptographic security. The more an eavesdropper gets information by her measurements, the more she disturbs the system, hence gets caught in the process. However, there are necessary conditions that the communicating parties need to ensure for such a situation. For example, they need to randomly switch their basis with which they encode information in the system, and a classical public channel (assumed to be authentic) through which they share their basis information rather than measurement outcome.

1.2.5 Quantum Gates and Operations

In quantum computing, circuit formalism is most often preferred. One can realize a task by performing quantum gates on qubits. One of the important aspect to compare between classical and quantum computing is the notion of a universal gate set [1]. In classical theory of computation, a set of AND and NOT gate together suffice to form a universal set. Interestingly, a Toffoli gate alone is sufficient for universality, and so is the Fredkin gate. Quite generally, a logic gate is a function $f : \{0, 1\}^i \rightarrow \{0, 1\}^j$, with i inputs and j outputs. For example, an exclusive-OR gate is given by 2-input-1-output map: $XOR : \{x, y\} \rightarrow x \oplus y$, where $\oplus$ represents addition modulo 2.

A quantum circuit is made of gates which transform an input state to an output state, and of wires that carry the quantum information via quantum states. Wires carry the bits around in space and time. A simplest set of quantum gates are the qubit gates. In fact, a set of all single qubit gates and a single two qubit gate suffice to form a universal set. It means that any qubit quantum gate as well as qubit circuit can be realized with the combination of these gates. Suppose a qubit quantum gate has k inputs and outputs, then the matrix, representing the gate, will be of 2^k degree. A two-qubit gate will be $2^k = 4$, i.e., a 4×4 matrix.

Single-qubit gates An important group of transformations in quantum information is the Pauli group with operators

$$\sigma_1 = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_2 = Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_3 = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ and } \sigma_0 = \mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \tag{17}$$

which generate the dynamics of a two-level system, which can be realized on a Bloch sphere. Pauli operators are the generators of rotation in 2D Hilbert space. For example, rotation about an arbitrary direction $\hat{n}$, the unitary matrix is given by $R_{\hat{n}}(\theta) = \exp\big(-i\theta\frac{\hbar}{2}(\boldsymbol{\sigma}\cdot\hat{n})\big)$, where $\boldsymbol{\sigma} = a_1\sigma_1 + a_2\sigma_2 + a_3\sigma_3$ is the Pauli operator vector. An equal superposition of X and Y gives us a crucial transformation known as the Hadamard gate

$$H = \frac{1}{\sqrt{2}}(X + Z) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{18}$$

Complex phases play a central role in quantum dynamics. It is pertinent to introduce a phase gate:

$$P = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}, \tag{19}$$

where $\theta \in \{0, 2\pi\}$ value of which determines a particular action on the qubit. For example, one of the famous gate is the so-called $\frac{\pi}{8}$ gate: $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{pmatrix} = e^{\frac{i\pi}{8}}\begin{pmatrix} e^{-\frac{i\pi}{8}} & 0 \\ 0 & e^{\frac{i\pi}{8}} \end{pmatrix}$. Note that for $\theta = \pi$ one recovers the Z gate, which is nothing but a phase-flip.

Two-qubit gates It is important in quantum information and computation to exploit quantum resources such as entanglement. Two qubit gates are used to manipulate two-qubit states, entangled or otherwise. A generic controlled-unitary qubit gate is given by

$$C_U = |0\rangle\langle 0| \otimes \mathbb{1}_2 + |1\rangle\langle 1| \otimes U \tag{20}$$

which says that if the state of the control qubit is $|0\rangle$, then do nothing ; and if it is $|1\rangle$, then apply the unitary U. For $U = X$, we get a controlled-NOT (CNOT) gate. Similarly, one can construct C-Y and C-Z gates.

CNOT gate finds many interesting applications. Note that the CNOT gate is an entangling operation, which finds its use in going from computational basis $\{|0\rangle, |1\rangle\}$ to Bell basis $\{|\phi\rangle_{00}, |\phi\rangle_{01}, |\phi\rangle_{10}, |\phi\rangle_{11}\}$. For example, in the Bell state measurement, as shown in the below quantum circuit Fig. 1, a Hadamard gate is applied on the first qubit, followed by a CNOT gate and then both qubits are measured in computational basis with measurement operators M_i satisfying $\sum_i M_i = \mathbb{1}$. Note, however, that it is not necessary to use CNOT for Bell state measurement.

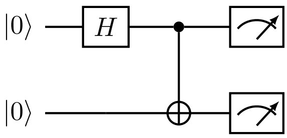

Fig. 1 Bell state measurement [1]. The initial states are chosen to be $|0\rangle$ for simplicity

1.2.6 Quantum Operations

Quantum systems are fragile since they are inevitably subject to ubiquitous environmental interactions. In reality, there is no such thing as perfectly closed quantum system, the system is alway *open* [14]. When quantum system interacts with the environment, it loses its coherence, hence undergoes *decoherence*. That is, when a system is completely decohered, the off-diagonal terms (also called the coherences) in the density matrix vanish. Moreover, it may also lose its energy undergoing *dissipation*. Open system quantum mechanics now follows different set of axioms: (1) states are density matrices, (2) measurements are POVMS and (3) dynamics is fixed by a completely positive (CP) trace preserving (TP) map. The density matrix captures both pure and mixed state representations, POVMs are convex combination of PVMs and the dynamics is no more unitary but linear and CP, thus representing a physically valid evolution. That is, a not CP evolution is unphysical in the sense that corresponding dynamical map outputs a negative state.

Quantum technologies face the challenge of reducing errors due to noise and the aim and purpose of quantum error-correcting codes is to facilitate the functioning of a fault tolerant quantum computer which is robust against environmental hazards and faulty device induced errors. Studying decoherence is an important aspect of quantum information since any quantum computer must satisfy the so-called DiVincenzo criteria; one of them being the *long decoherence time* for qubit evolution.

Suppose a qubit is interacting with an environment. Its evolution is governed by a master equation famously known as Gorini-Kossakowski-Lindblad-Sudarshan (GKSL) equation [15, 16], which is obtained assuming the so-called Born-Markov approximation. An equivalent representation, useful in quantum information science, is the operator-sum (KSMR)[3] representation [17, 18] of a CPTP map (a quantum channel):

$$\Phi[\rho] = \sum_i K_i \rho K_i^\dagger \tag{21}$$

where K_i are called the KSMR operators [1], satisfying $\sum_i K^\dagger K = \mathbb{1}$, which can be obtained by tracing out the environmental degrees of freedom from the global unitary that generates system-environment evolution: $\Phi[\rho] = \mathrm{Tr}\{U(\rho \otimes \rho_{\text{env}})U^\dagger\}$. For simplicity, let us assume that the initial environmental state is $\rho_{\text{env}} = |0\rangle\langle 0|$ and

[3] K stands for Kraus and SMR stands for the first founders of this representation: Sudarshan, Mathews and Rau.

$\{|e_i\rangle\}$ are the environmental degrees of freedom, then $K_i = \langle e_i|U|0\rangle$. KSMR operators representation is a powerful way of essentially capturing the noisy evolution of the qubit. We must remember that decoherence is basis dependent. That is, for example, what is decoherence in $\{|0\rangle, |1\rangle\}$ is not decoherence in $\{|-\rangle, |+\rangle\}$ basis! This has implications to how one develops errors correcting codes.

Simple examples of errors that are commonly found for qubits are the bit-flip, phase-flip and bit-phase-flip errors. And others include depolarizing, amplitude damping and generalized amplitude damping errors. A class of qubit errors is known as Pauli errors that involve only Pauli group hence the name, These errors occur without dissipation that is they induce only decoherence. A qubit flip error can be written as

$$\Phi_i[\rho] = (1-p)\rho + pU_i\rho U_i^\dagger \tag{22}$$

where U_i represents the a Pauli operator depending on which error occurs with probability p, e.g., $U_{i=1,2,3} = \sigma_1, \sigma_2, \sigma_3$ for bit-flip, bit-phase-flip and phase-flip errors, respectively. There may be situations where more than one or all of the qubit errors occur. Another important qubit error is given by the depolarizing channel

$$\Phi^{\text{depol}}[\rho] = (1-p)\rho + \frac{p}{3}\sum_{i=1}^{3}\sigma_i\rho\sigma_i^\dagger \tag{23}$$

Another type of quantum channel is amplitude damping which captures dissipation or relaxation process. In this case, a particle not only lose coherence, but also population (or energy) while it relaxes or damps. It is given by the channel $\Phi^{\text{AD}}[\rho] = \sum_i A_i\rho A_i^\dagger$ with KSMR operators

$$A_1 = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\lambda} \end{pmatrix} \quad A_2 = \frac{1}{2}\begin{pmatrix} 0 & \sqrt{\lambda} \\ 0 & 0 \end{pmatrix} \tag{24}$$

where λ is called the damping factor, determined by the type of process. More will be talked about quantum error correction later in the chapter.

1.2.7 Choi-Jamiolkowski Isomorphism

One of the central tools of quantum information theory is the Choi-Jamiolkowski (CJ) isomorphism [19]. It is mainly used to exploit the channel-state duality. Namely, any CPTP map (a channel) can be used to transform a state which will be isomorphic to the map. And the CJ matrix [19] or B matrix[4] [18] is given by

[4] Importantly, CJ matrix is nothing but the B matrix of Sudarshan, Mathews and Rau which was implicitly discovered about a decade before Choi.

$$\xi = (\Phi \otimes \mathbb{1})[\left|\psi^{+}\right\rangle\left\langle\psi^{+}\right|] \tag{25}$$

where $\left|\psi^{+}\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is a maximally entangled state in the computational basis. If the state (25) is negative, then Φ is a not-completely positive (NCP) map. Nevertheless, such a map will output a valid quantum state for single qubit space, it doesn't do so in an extended Hilbert space; that is when it is acting on a part of the Bell state. This result follows from the Stinespring dilation theorem. Historically, Eq. (25) (now known as Sudarshan B matrix) was first demonstrated in the seminal work of Sudarshan, Rao and Mathews [18], which was later independently discovered by Choi and Jamiolkowski. One should note that while it is possible to transform a dynamical map or a physical process to a state, the converse is necessarily not possible. One of the applications of a NCP map is to *witness* entanglement in a state—a method known as the Positive Partial Transpose (PPT) criterion [7]: Given a bipartite state, if a partial transpose map acting on one half of the state renders the CJ matrix negative, then the state is entangled. We shall later see one of the applications of quantum operations applied to study open quantum system evolution.

1.3 Quantum Information Science—Applications

Here we will discuss some of the major applications of quantum information science namely teleportation, superdense coding and entanglement swapping that are not possible classically. It means that there exist no resources in the classical world with which one can reproduce the rather counter-intuitive effects applied to transmitting and manipulating information using quantum systems. In this subsection, our main motivation will be to explain how quantum entanglement plays the role of a resource in quantum communication and quantum technologies in general. We will also mention about the peaceful coexistence of quantum mechanics with the theory of special relativity in the sense that there will be no faster-than-speed-of-light communication involved when performing quantum information processing tasks.

1.3.1 Superdense Coding

How does one send information using quantum particles? Quantum particles possess degrees of freedom in which information can be encoded. In fact, a particular degree of freedom, say polarization of a photon, can be used as a qubit. That is our quantum system which we manipulate in the lab. Now, bits of information can be encoded in the polarization of a photon and sent down a quantum channel. How many bits can Alice send to Bob with a single particle? With an isolated uncorrelated photon, she can send a single classical bit of information. Suppose, Alice and Bob share a maximally entangled pair of particles, then Alice can send two bits of information on a single qubit. This is known as superdense coding. Given an initial Bell state

$$|\phi\rangle_{00} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \tag{26}$$

if Alice wants to send bits 00, she does nothing to her particles and send it to Bob. If Alice locally applies a σ_x gate, then the state transforms as

$$(\sigma_x \otimes \mathbb{1})\, |\phi\rangle_{00} = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) = |\phi\rangle_{01}\,. \tag{27}$$

Similarly, if she locally applies $i\sigma_y$ and σ_z gates, she transforms the state, respectively, as

$$(i\sigma_y \otimes \mathbb{1})\, |\phi\rangle_{00} = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = |\phi\rangle_{11}\,, \tag{28}$$

$$(\sigma_z \otimes \mathbb{1})\, |\phi\rangle_{00} = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = |\phi\rangle_{10}\,. \tag{29}$$

When Bob receives the qubit, he makes Bell measurements to find out one of the Bell states $\{|\phi\rangle_{00}\,, |\phi\rangle_{01}\,, |\phi\rangle_{10}\,, |\phi\rangle_{11}\}$ corresponding to the bits {00, 01, 10, 11} that Alice wanted to send him.

1.3.2 Quantum Teleportation

Quantum teleportation is one of the striking features of quantum mechanics which allows communicating an unknown qubit using entanglement. The protocol goes as follows. Suppose that Alice wants to send an unknown quantum state $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ to Bob, who is space-like separated from her i.e., light or information takes finite time to reach. Alice and Bob pre-share an entangled pair of qubits, an EPR-Bell state, say, $|\phi\rangle_{00} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Now the initial total state of all the parities is:

$$\begin{aligned} |\Psi\rangle_{\text{initial}} &= |\psi\rangle \otimes |\phi\rangle_{00} \\ &= (\alpha\,|0\rangle + \beta\,|1\rangle)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \end{aligned} \tag{30}$$

Alice *entangles* her part of the EPR-Bell pair with the unkown state $|\psi\rangle$ to be teleported i.e., she performs a CNOT gate $C_N = |0\rangle\,\langle 0| \otimes \mathbb{1}_2 + |1\rangle\,\langle 1| \otimes \sigma_x$ on her pair. Subsequently, she performs a Hadamard gate $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ on the *first* qubit. Here, $\mathbb{1}_2$ and σ_x are qubit identity and Pauli-X operators. After all of this, simple algebra gives the resulting total state:

$$\begin{aligned}\left|\tilde{\Psi}\right\rangle &= \frac{\alpha}{2}(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \frac{\beta}{2}(|0\rangle - |1\rangle)(|10\rangle + |01\rangle) \\ &= \frac{1}{2}[|00\rangle\,(\alpha\,|0\rangle + \beta\,|1\rangle) + |01\rangle\,(\alpha\,|1\rangle + \beta\,|0\rangle) + |10\rangle\,(\alpha\,|0\rangle - \beta\,|1\rangle) + |11\rangle\,(\alpha\,|1\rangle - \beta\,|0\rangle)].\end{aligned} \tag{31}$$

As before, Alice possesses her first two qubits of the state $\left|\tilde{\Psi}\right\rangle$ and Bob the third one. Now comes the magical part of quantum teleportation. Alice now measures her pair of qubits in the computational basis $\{|0\rangle\,, |1\rangle\}$,[5] which *teleports* the unknown state $|\psi\rangle$ to Bob *instantaneously*! If Bob makes a measurement on his qubit now, then he has $\frac{1}{4}^{\text{th}}$ probability of getting either of the 4 states $\{(\alpha\,|0\rangle \pm \beta\,|1\rangle), (\alpha\,|1\rangle \pm \beta\,|0\rangle)\}$ depending on which Bell basis Alice finds her pair to be in. For example, if she finds her pair's state to be $|01\rangle$ then the state teleported to Bob is $(\alpha\,|1\rangle + \beta\,|0\rangle)$. Alice now communicates her basis information, for which she has to send 2 bits of information over a classical channel. This part of communication is restricted by special relativity: she can't send her information faster than speed of light. Therefore, unless Alice tells Bob her basis information, Bob never recovers the state $|\psi\rangle$ which Alice actually wanted to send him! The final stage of the protocol is that based on Alice's basis information, Bob does a corresponding Pauli operation to transform the state to the actual state $|\psi\rangle$ Alice wanted to send. That is, if Alice's finds her pair to be in $|10\rangle$, the Bob performs a σ_z to recover the state. Therefore, they *must* use classical communication to achieve teleportation!

Interestingly, no-cloning theorem and no-faster-than-speed-of-light transfer of information are related. If Bob can make a large copies of his particle, then he can make a measurement on each of them, and the basis which returns the same result is the basis Alice would have encoded in. But again, copying an unknown state is prohibited by no-cloning! Therefore, Bob can never recover his state without Alice's classical message.

Quantum teleportation finds enormous applications in quantum technologies. One of the immediate application is in quantun internet—a quantum network to exchange quantum states between the nodes with distributed entanglement. Another application is in teleportation based quantum computing. In fact, teleportation has been achieved for very long distances, about 143 km long [20], and also using satellite based quantum entangled particles achieving 1,400 km distance [21]. Such practical, long distance teleportation will be key to a global quantum internet.

[5] The operations by Alice until now together are equivalent to making a Bell measurement on the initial product qubits in her possession; i.e., a Hadamard on the first qubit and a CNOT on the both the qubit and measuring both qubits in computational basis each.

1.3.3 Entanglement Swapping

Yet another type of process which doesn't have a classical analog is entanglement swapping which finds its use in quantum network based communication. Here, we briefly explain it below.

Generally, for two quantum particles to be entangled, they must have interacted sometime in the past through some physical process. Entanglement swapping is a technique of exploiting quantum measurement and entanglement itself to entangle two particles that have never interacted before! Suppose, $\{a, b\}$ and $\{c, d\}$ are pairs of particles with Alice and Bob, respectively. a is entangled with b; and c is entangled with d. Now, a and c have never interacted in the past. Question is: Can $\{a, c\}$ get entangled? The answer turns out to be yes, and this is one of the spooky phenomena allowed by quantum mechanics! It goes as follows.

Suppose Alice has an entangled pair $|\phi\rangle_{ab} = \frac{1}{\sqrt{2}}(|00\rangle_{ab} + |11\rangle_{ab})$. Similarly, Bob has $|\phi\rangle_{cd} = \frac{1}{\sqrt{2}}(|00\rangle_{cd} + |11\rangle_{cd})$. So the initial state is:

$$|\psi\rangle_{\text{initial}} = |\phi\rangle_{ab} \otimes |\phi\rangle_{cd} \,. \tag{32}$$

Now, this initial state is sent to a third party Charlie who does a Bell-state measurement on $\{b, d\}$, as explained previously, and as a result $\{a, c\}$ get entangled! This shows one of the spooky features of measurement and entanglement in quantum physics. Note that entanglement swapping has been realized experimentally [22, 23].

1.3.4 Quantum Cryptography and Communication

Ever since Bennett and Brassard proposed the famous BB84 quantum key distribution protocol in 1984, there has been an intense research toward developing more secure communication protocols for more than 3 decades now. And that has been achieved to a significant extent. Still there appears to be much more to be achieved at theoretical and experimental frontiers. Specifically, there is a challenge of building a *scaleable* quantum secure communication system and quantum computing machines, that will outperform the existing classical information processing systems. Nevertheless, there are also efforts being put to develop classical encryption algorithms that will provide post-quantum cryptographic security, meaning that they will provide security against a threat from attacks by a quantum computer.

One of the striking application of entanglement is in secure *direct* quantum communication protocol. Here, it is pertinent to briefly explain one such protocol, fist introduced in 2002 by Bostrom and Felbinger [24]:

- Bob has a pair of photons entangled in polarization degree, say, $\left|\phi^{+}_{ht}\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ one of which he keeps with himself (home photon in the state ρ_h) and the other (travel photon in the state ρ_t) he sends to Alice who is at a long distance from him.

- Once Alice receives the qubit, she does either an identity or Pauli-Z operation on it, each with probability $\frac{1}{2}$ and sends it back to Bob.
- After receiving the travel qubit back, Bob does a Bell state measurement on them, and finds his pair of particles either in $|\phi^+\rangle$ or $|\phi^-\rangle = (\mathbb{1} \otimes \sigma_z)[|\phi^+\rangle]$, depending whether Alice wants to send him 0 or 1, respectively.
- If Bob finds the pair to be anti-correlated, then they abort the protocol. If he finds his particles to be in either of the Bell states $|\phi^\pm\rangle$ then the protocol is repeated.

Now, if an eavesdropper tries to measure the flying qubit, all she finds is perfectly random outcomes, since the reduced density matrix $\rho_t = \mathrm{Tr}_h(|\phi^+_{ht}\rangle\langle\phi^+_{ht}|)$ of a *maximally* entangled state ρ^{AB} is a maximal mixture i.e., $\rho_t = \frac{I}{2}$. Note that Alice and Bob never used a classical channel to communicate the basis information and the information transmitted was direct and deterministic. Here, we immediately see the advantage of using an entanglement for the security of QKD as well as direction quantum communication. However, Wojcik [25] introduced a clever attack on this protocol using which the eavesdropper could get as much information as Alice and Bob will have at the end. Thence, the security check was extended to analyzing channel losses induced due to eavesdropping. The reader is referred to Refs. [25, 26] for further study.

This protocol has a disadvantage that it is quasi-secure when it is used for direct communication but comes with an advantage of being fully secure when used for a key distribution. Moreover, all two-way protocols suffer from the point of view of resources needed for an extra round of sending the particle down a quantum channel. Some of the one-way QKD protocols, couterfactual or otherwise, will be introduced in a later section. Surprisingly, in a counterfactual key distribution protocol, Alice and Bob can choose to generate a secret key for which the particle actually doesn't travel through the quantum channel (interferometric arm, in this case) with certain probability! This interesting feature for secure QKD will be discussed in a later chapter.

1.3.5 Quantum Secret Sharing

The idea of sharing a secret among untrusted individuals is a very relevant problem. A brief introduction is given [as in Ref. [27] and the reference therein] below [see Fig. 2]:

1. An individual (Alice) has to share a secret among two or more untrusted parties (Bob, Charlie, Dave,...) so that no single party can decode it, but at least half of them must come together to do so.
2. E.g., key $K \equiv 11010 \Longleftrightarrow b(=10001) + c(=01001)$ is shared b/w Bob and Charlie. Thus b and c are shares for the key. Knowing only one of them, no information of K obtainable.

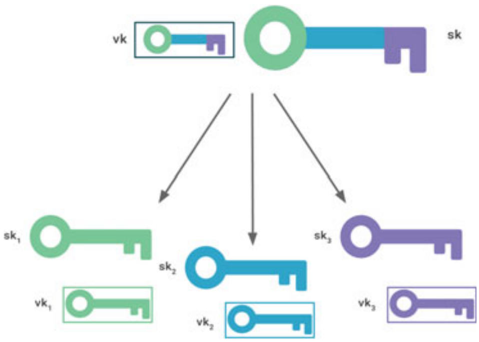

Fig. 2 A schematic of a secret sharing protocol for the case of a key shared with three untrusted parties

3. Secret S is to be divided between n parties such that:
   a. $\# \geq k$ parties necessary and enough number to reconstruct S.
   b. $\# \, k - 1$ parties get zero info.
4. For a polynomial of degree $k - 1$ (over a prime # field), at least k points are required. Each share is the triple $(x, f(x), P)$.
5. Example: quadratic polynomial $f(x) = a_0 + a_1 x + a_2 x^2$ where a_0 is the secret (a prime number). We share $(x, f(x))$ for n number of parties, then at least three parties must come together to get a_0.

Quantum secret sharing schemes offer security based on no-go theorems in quantum mechanics, unlike computational hardness of a problem, as in classical counterpart. A simple protocol is given below.

1. Four parties $\{A, B, C, D, E\}$: collection of sets that can reconstruct secret: $\mathcal{G} = \{\{A, B, C\}, \{C, D\}, \{A, B, E\}\}$. Here $\mathcal{G}$ is the access structure [27].
2. Quantum case: no-cloning theorem $\Rightarrow$ no two disjoint elements in $\mathcal{G}$.
3. Classical keys + QKD solves the eavesdropping problem; thus QSS best motivated for **quantum** secrets.

Let us suppose a GHZ triplet is shared between three parties, Alice, Bob and Charlie in the state [28]

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \tag{33}$$

Alice and Bob choose randomly to measure their particle in either X or Y direction, which can give eigenvalues of ±1, represented by ±X or ±Y. Writing GHZ state in XY bases, we construct the Table 1 [29].

1.3.6 Open Quantum System Dynamics

Quantum operations provide a clean method to represent and study open quantum system dynamics—Markovian and non-Markovian [30, 31]. In realistic situations, most

Table 1 A table representing the Pauli bases in which the particle in measured

	+ X	– X	+ Y	– Y
+ X	$\vert 0\rangle + \vert 1\rangle$	$\vert 0\rangle - \vert 1\rangle$	$\vert 0\rangle - i\vert 1\rangle$	$\vert 0\rangle + i\vert 1\rangle$
– Y	$\vert 0\rangle - \vert 1\rangle$	$\vert 0\rangle + \vert 1\rangle$	$\vert 0\rangle + i\vert 1\rangle$	$\vert 0\rangle - i\vert 1\rangle$
+ Y	$\vert 0\rangle - i\vert 1\rangle$	$\vert 0\rangle + i\vert 1\rangle$	$\vert 0\rangle - \vert 1\rangle$	$\vert 0\rangle + \vert 1\rangle$
– Y	$\vert 0\rangle + i\vert 1\rangle$	$\vert 0\rangle - i\vert 1\rangle$	$\vert 0\rangle + \vert 1\rangle$	$\vert 0\rangle - \vert 1\rangle$

of the open system dynamics are non-Markovian (NM) as Born-Markov approximation may not hold. Recently there have been enormous efforts to study NM dynamics from an information theoretic viewpoint. For example, the first simple method of detecting and quantifying non-Markovianity (NM-ity) was proposed by Breuer-Laine-Piilo (BLP) [32] which exploits that fact that trace distance (TD) (5) is a monotone under a Markovian CPTP map $\Phi(t)$: $D(\Phi(t)[\rho_1], \Phi(t)[\rho_2]) \leq D(\rho_1, \rho_2)$, where D is TD and ρ_1 and ρ_2 are two orthogonal initial states. This means that as the initial orthogonal states become more and more indistinguishable as time evolves. This has been interpreted as quantum information-loss to the environment. Crucial observation is that under a NM channel this monotonicity will be broken, in the sense that the information lost to the environment flows back to the system. Hence, the non-monotonous regions can be used to quantify NM-ity. The BLP measure is given by $N_{\text{BLP}} = \int_{\sigma>0} \sigma(\Phi, \rho_1, \rho_2)$ where $\sigma = \frac{dD}{dt}$. Another method of detecting and quantifying NM-ity is due to Rivas-Huelga-Plenio (RHP) [33] based on the divisibility of the channel. Given a CPTP map Φ, it can be decomposed into a concatenation of intermediate maps for, say, simple 3 instances: $\Phi(t_2, t_0) = \Phi(t_2, t_1)\Phi(t_1, t_0)$. If the CJ matrix (25) of the intermediate map $\Phi(t_2, t_1)$ is negative (i.e., if the intermediate map is not a channel), then the CPTP map $\Phi(t_2, t_0)$ is CP-*indivisible* and termed NM according to RHP. And the NM-ity is quantified as $N_{\text{RHP}} = \int_0^\infty g(t)$, where $g(t) = \lim_{\epsilon \to 0^+} \frac{\|\xi(\Phi,\epsilon)\|_1 - 1}{\epsilon}$, where ϵ is infinitesimal time and $\xi(\Phi, \epsilon)$ represents the CJ matrix of the map in the infinitesimal time limit. Note that both BLP and RHP measures need not be normalized, and suitable normalization can be used to fit them in the range 0 to 1.

Other than the above two, there have been a number of approaches to quantify NM-ity—based on fidelity [34], capacity of channel [35], causality measure [36], interferometric power, accessible information and many more. However, there are in-equivalences. When multiple decoherence channels are involved in a process, then BLP and RHP need not be equivalent. But for a qubit dynamics involving a single decoherence channel they are known to be equivalent. Another interesting and intriguing way NM-ity may arise is through convex combination of Markovian channels. In the case of unital channels,[6] it is known that the space of Pauli Markovian (CP-divisible) channels is not convex [37–39]. If one takes a convex combination of two Pauli semigroups, the resulting channel is non-Markovian in the sense that it is CP-indivisible. Moreover, it can be eternally non-Markovian according RHP

[6] A channel Φ is said to be unital if $\Phi[\frac{\mathbb{1}}{2}] \to \frac{\mathbb{1}}{2}$. Else, it is called non-unital.