UNED

Facultad
de Ciencias

Máster de física médica
Trabajo fin de máster

Aplicaciones del tratamiento cuántico de la información en medicina

Quantum Information Applications in Medicine

Luis Trigo Vidarte

Marzo 2020
Directora: Cristina María Santa Marta Pastrana

Acknowledgements

Me gustaría empezar con unas líneas de agradecimiento en español a mi tutora, Cristina Santa Marta. Muchas gracias por haber aceptado dirigir este TFM en primer lugar, pero también por los ánimos para completarlo, la coordinación del máster durante los últimos años, la gestión de las prácticas en Madrid y las asignaturas impartidas.

Muchas gracias a José Carlos Antoranz Callejo por su labor como coordinador del máster durante mis primeros años en el mismo. No menos gracias a todos los docentes con los que he compartido asignaturas o momentos en las prácticas.

Quiero aprovechar para enviar un saludo y agradecimiento a mis compañeros de promoción (de prácticas por lo menos): Antonio, Carmen, Eduardo, Javier, Jonatan y Jorge. ¡Un abrazo a todos!

Por último, gracias a mi familia por su continuo apoyo durante todos estos años. Y a Lucía, por no negarme nunca su ayuda.

Luis Trigo Vidarte

Detailed Contents

Figures

Summary 1

1.1 Español

Las tecnologías cuánticas han recibido mucha atención durante los últimos años, siendo presentadas como la próxima revolución en nuestras vidas. Su naturaleza, fundamentalmente distinta a la de los sistemas a los que estamos acostumbrados presenta muchos retos, tanto a los investigadores como a los posibles usuarios finales, creando muchas falsas ideas. Presentamos los conceptos básicos para entender los posibles beneficios aplicables en el entorno médico, centrando el análisis en la mejora de dos características: el incremento en capacidad de cálculo gracias al uso de ordenadores cuánticos y a la posibilidad de comunicarse manteniendo la privacidad durante largos periodos de tiempo gracias a la distribución cuántica de clave.

La habilidad de procesar rápidamente las grandes cantidades de información involucradas en la era digital es una característica relevante para las aplicaciones médicas. La imagen médica ya es capaz de sintetizar gran cantidad de información proveniente del cuerpo del paciente en datos analizables pour un experto. La reciente relevancia del tratamiento médico personalizado hará que en el futuro próximo los requisitos de cálculo sean más relevantes. Veremos que algunos problemas que actualemente son intratables informáticamente (incluso con un superordenador), pueden tener una solución factible trabajando con la información de manera cuántica. Esto facilitará probablemente el desarrollo de nuevos medicamentos, ya que la interacción de los fármacos con otras moléculas del cuerpo podrá ser simulada de una manera eficiente en un corto espacio de tiempo. Sus efectos sobre el cuerpo del paciente podrían ser simulados en función de la información genética disponible y el registro de tratamientos anteriores. Comentaremos la viabilidad de estas afirmaciones e indicaremos los supuestos necesarios en cada caso.

La naturaleza sensible de la información médica requiere el máximo nivel de privacidad a largo plazo. Los ordenadores cuánticos pueden poner en riesgo algunos sistemas de intercambio de clave actuales, pero la información cuántica también nos da la oportunidad de cambiar información de forma segura utilizando las propiedades de la mecánica cuántica. Aunque posible en la práctica, todavía son necesarios ciertos avances tecnológicos y en políticas de seguridad antes de su implantación comercial.

1.2 English

Quantum technologies have received a lot of attention in the recent years, being presented as the next revolutionizing step in our lives.

Its fundamentally different nature with respect to previous systems presents many challenges for the researchers developing the technology but also for the potential users, creating many misconceptions. Here we present the basic ideas necessary to understand the possible benefits that can arise in the medical domain, focusing the analysis in the improvement of two aspects: the increase of calculation capabilities by the use of quantum computers and the possibility of long time privacy in the communication of information by the use of quantum key distribution.

The ability to process quickly the ever increasing amounts of information of the digital world is a relevant challenge for medical applications. Medical imaging already synthesizes successfully information from the body of the patient to data that can be analysed by an expert. The increasing relevance of personalized medicine will make the calculations requirements more relevant in the near future. We will see that some problems cannot be tackled directly with the current computers (even the so called supercomputers), but they could be tractable treating the information in a quantum mechanical way. This will likely facilitate the synthesis of new drugs, since its interaction with other elements could be efficiently simulated in a relatively short time. The effects over the body of a particular patient could also be simulated depending on genetic information and previous treatment record. We will discuss the feasibility of those claims and indicate the required conditions.

The sensitive nature of medical information requires the maximum level of privacy in the long term. Quantum computers can threaten some of the cryptographic schemes that have been used until now, but quantum information also gives us the opportunity to exchange information more securely using the properties of quantum mechanics. Although possible in practice, it still requires technological improvements and the development of new security practices before dynamic commercial deployment.

Introduction 2

2.1 Quantum mechanics

Quantum mechanics is a theory of nature developed during the first half of the 20th century that revolutionized our understanding of the world. Its counter-intuitive properties caused incredulity at first, but the accordance of its predictions and the experimental results at nanoscopic scales have guaranteed the theory a consolidated status in modern science, although it cannot be considered yet a complete theory of nature, since many effects at macroscopic scales do not fit the model correctly.

The theory gets its name by the fact that some physical quantities (energy, momentum...) can only take a discrete set of values (they are quantized) and it can be formulated using many different mathematical formalisms. Each formalism can be applied to facilitate the treatment of a particular problem, but all formalisms are fundamentally equivalent. For example, if we want to describe the position and momentum of a particle using quantum mechanics, we can use a mathematical formalism that uses a wave function to indicate the probability of a particle to be in a determinate state. They also have in common a surprisingly reduced mathematical tool kit: linear algebra (complex numbers, eigenvectors/values), functional analysis (Hilbert spaces, linear operators, spectral theory), differential equations and harmonic analysis (Fourier) are sufficient to understand quantum mechanics.

2.2 First quantum revolution

Although quantum mechanics can be considered simple in a mathematical sense it is far from being intuitive. Famous phrases regarding this perception are Niels Bohr's: "Anyone who is not shocked by quantum theory has not understood it." and Richard Feynman's "I think I can safely say that nobody understands quantum mechanics.". This lack of understanding has not prevented scientists from applying the previously mentioned formalisms to particular problems successfully during the second half of the 20th century. The use of quantum mechanics facilitated the creation of new technologies such as the laser, global navigation satellite systems (GNSS: GPS, Galileo, Glonass), magnetic resonance imaging (MRI) and most of all the understanding of solid state physics, in particular the transistor, the undisputed king of current information age. Those technological advents are now considered part of the first quantum revolution.

The first landmarks of this initial quantum technological revolution were far from being understood at the time, even for its inventors.

Theodore Maiman, one of the inventors of the laser, famously said that "a laser is a solution seeking a problem" because the relevance of the new device was not clear. Now lasers are widely applied to many problems and the sentence seems naive, so the tendency with current developments in quantum information technology is to be optimistic (but we should not be over-optimistic).

2.3 Second quantum revolution

Quantum information scientists consider that we are now living the second quantum revolution, which consists on the use of all the potential of quantum mechanics to treat practical problems. The first quantum revolution consisted mainly on technological achievements that allowed the deployment of reliable and affordable technologies that facilitate current information age, but the operational logic of current computers could also be implemented with mechanical relays, pneumatic valves, an abacus or a piece of paper (it would only be much slower). The second quantum revolution is about taking advantage of the quantum mechanical properties of the microscopic world to process the information.

Quantum computing

The origins of quantum computing can be traced back to 1982 when Richard Feynman, realising that the use of computers to simulate problems of many-body physics was very inefficient, proposed the use of quantum mechanical systems to simulate quantum mechanical problems [1]. This concept was generalized to a generalized quantum computer in 1985 by David Deutsch and in 1996 Seth Lloyd proved that a system of this kind could efficiently simulate local quantum systems [2]. Some remarkable algorithms making use of quantum computers also appeared, perhaps the most famous are Shor's algorithm to calculate the discrete logarithm and factorize big numbers [3] in 1995 and Grover's algorithm to improve unstructured search [4] in 1997. Many algorithms followed, and their improvement with respect to their classical counterparts varies, but it can be exponential in some cases, which transforms some currently intractable problems into potentially solvable in a reasonable amount of time.

Quantum key distribution

In parallel to quantum computing, focused on improving calculations, other branch of quantum information came to light. Stephen Wiesman realized that, due to the fact that a quantum state cannot be perfectly copied, it was possible to create unforgeable sets of states if some conditions were satisfied. The initial objective was to provide unforgeable quantum money (not very practical in reality), but the idea evolved to the use of these states to guarantee that the exchange of key between two trusted parties could be performed securely. The exchanged key could be used later on to encrypt sensitive data. The first protocol was published by Charles Bennett and Gilles Brassard in 1984, hence the name BB84 [5], and many similar protocols followed. This family of schemes is known as quantum key distribution (QKD) and if implemented correctly guarantees that the key exchanged by two entities that trust each other is perfectly secret up to an arbitrary parameter ϵ even if the quantum channel between them is insecure, but they require an auxiliary classical authenticated channel. QKD is considered the first practical application of the second quantum revolution, but technical improvements are still required in order to extend its current market, restricted mainly due to the limited achievable distance, secret key rate and cost.

Quantum sensing

The properties of quantum mechanics can be used to create a sensor that interacts with a physical quantity and responds in discrete energy levels that can be resolved coherently. This can improve the sensitivity, size, speed and cost of detectors. Many experts foresee this branch of quantum information as the first one to show practical advantages over current technologies and it is already giving promising results in the sensing of electromagnetic fields.

2.4 Applications in medicine

Medicine will certainly profit from the quantum treatment of information. Quantum computing will accelerate the development of new drugs, as well as the simulation of its behaviour in a particular patient facilitating the extension of personalized medicine. The transmission of sensitive information will be more secure thanks to the use of quantum key distribution and other quantum communication primitives. Even in the case of requiring the off-sourcing of calculation to an untrusted entity it can be guaranteed that the sensitive information is kept private. Quantum technologies are also expected to extend the sensitivity limits of classical devices, improving the capabilities of instruments used in medicine, for example in MRI.

Hypothesis and objectives | 3

The field we are studying can be considered an attractive overlap of physics, computer science and engineering.

Quantum mechanics was born more than 100 years ago and it is now considered a well established theory[6]. The progressive understanding of quantum mechanics opened the way to new fields such as quantum electrodynamics (QED) [7] and quantum chromodynamics (QCD) that provide an accurate and elegant explanation of the subatomic world. More complete theories such as quantum field theory (QFT) follow the path including more effects in the assumptions. Although the previous theories can explain many natural phenomena with outstanding precision, at this point in history a theory comprising all the possible observable phenomena has not been achieved, and quantum mechanics cannot be proven to be a universal theory [8].

The remarkable agreement between the predictions of quantum mechanics and all the experiments formulated so far at microscopic distances seem to indicate that quantum mechanics is a valid theory in those settings. Working in environments of molecular, atomic and subatomic scales we will assume that quantum mechanics is true.

The computer science elements that come into play are mainly information theory, pioneered by Claude Shannon [9] in the mid of the 20th century and complexity theory [10]. The complexity theory assumes that problems can be categorized into different levels of difficulty and surprisingly many categories (more than 500!) have been identified so far in the Complexity Zoo [11]. We will assume that different complexity classes exist and that machines that make use of certain quantum mechanical properties (quantum computers) can experiment advantages over machines that do not use these properties (classical computers).

With these assumptions we aim the following objectives:

1. Provide a basic understanding of the quantum information paradigm.
2. Identify potential applications useful for the medical practice and related research.
3. Clarify misunderstandings associated with quantum technologies.
4. Create a link between the current quantum technologies and tools used in medical imaging.

Only basic knowledge of physics and computer science is assumed to treat these matters.

Methodology 4

The field of quantum mechanics and quantum technologies is extremely broad. In order to cover the initial objectives of the project an exploration of the most relevant scientific literature related to quantum computing and quantum key distribution was performed, following a review approach targeting people who want to have an idea of the possibilities of quantum technologies from an abstract level, but acquiring sufficient background on the operation fundamentals.

Particularly informative articles such as review papers and seminal articles in the field were privileged. Approachable references are provided when possible in order to extend the information on a particular topic. I adapted the introduction of my PhD manuscript [12] on quantum key distribution for the related chapter.

4.1 Ethical aspects

The most remarkable ethical aspect covered in this document is the importance of private information. This becomes more relevant in the information age and we provide alternatives to preserve sensible data private for long periods of time. Unfortunately this privacy depends on a chain of players that can break by the weakest point. It is important to gain conscience about these facts and make an effort to maintain information concerning us and other people private.

Workplan 5

Quantum information (QI) science is a very multidisciplinary field involving physics, computer science and engineering. Even thought its beginnings date only to the last quarter of the 20th century, it is already quite a vast field, with many branches and sub-fields. Covering it completely would exceed the purpose of this document, so a review approach targeting medical applications has been followed, keeping in mind that the reader might not have previous experience in those topics and might be a practician who only has this question: *What can I expect from the quantum world?*.

In this review process the first step was to identify the most interesting applications of QI in medicine, considering both the short and long term. As this is a scientific text a simple enumeration is not considered sufficient, so the basic building blocks of these applications need to be identified and explained to the non expert, avoiding technicalities. Typical confusion points driven from experience and preconceptions are also mentioned in order to clarify the understanding.

The contribution of this article consists on been a document extending typical dissemination articles [13], providing a fundamental explanation of the phenomena and its limitations, avoiding the detail of thorough reviews on the topic [14, 15].

Results and discussion

Quantum computing 6

6.1 Introduction

Information and communication technologies (ICT) have drastically reshaped our lives during the last 60 years. The key player in this phenomenon was the electronic transistor, particularly useful to work as a fast switch able to perform a great variety of operations. For many decades transistors could be provided in sets of integrated circuits whose integration density grew exponentially, roughly doubling every two years in what is known as Moore's law [16]. This growth cannot be sustained for fundamental physical reasons, being the most important the reduction of size of the individual components. Transistors are made of atoms and they cannot work deterministically (quantum effects appear) if their dimensions approach the atomic scale (a few nanometers). Even if this effect is bypassed (using dispositions in three dimensions for example) there is the need of dissipating the heat generated by the conduction of the electrons required to perform the operations, and this posses many challenges to the characteristics of the devices and the consumption per gate. Alternatives to continue progress circumventing Moore's law exist [17], but we will focus on a new way of processing information: quantum computing.

The computers we use today, that we will denote as classical computers, use binary digits (bits) as the basic representation building block. Bits can be use to represent information as well as to store the instructions of the a program. A set of integrated systems (microprocessor, dynamic memory, long term memory, graphic card...), typically implemented in silicon, can perform the desired operations. The binary representations fits particularly well with the behaviour of transistors as switches and the philosophical branch of logic. In particular it can be demonstrated that any logical operation can be decomposed in a set of interconnected simpler logical gates[1] , which can be applied combining sequentially operations in the microprocessor and accesses to memory. This sequential operation and the requirement of memory will pose a fundamental limit to the efficiency of the algorithms that can be executed in this kind of devices.

6.2 Fundamentals

A fully programmable quantum computer is based on similar building blocks, but in this case we can make use of all the properties of quantum mechanics. In particular we will be interested in states that are prepared as a superposition of two states, with certain probability to be in one of the two. We start by choosing a reference basis and some complex coefficients that weight each element of the basis[2] . We will use the so called computational basis $\{|0\rangle, |1\rangle\}$[3] . Denoting the complex

[1] 1: The typically used gates are Negative OR (NOR) and Negative AND (NAND).

[2] 2: The square of the complex coefficient represents the probability.

[3] 3: In the computational basis $|0\rangle = \binom{1}{0}$ and $|1\rangle = \binom{0}{1}$

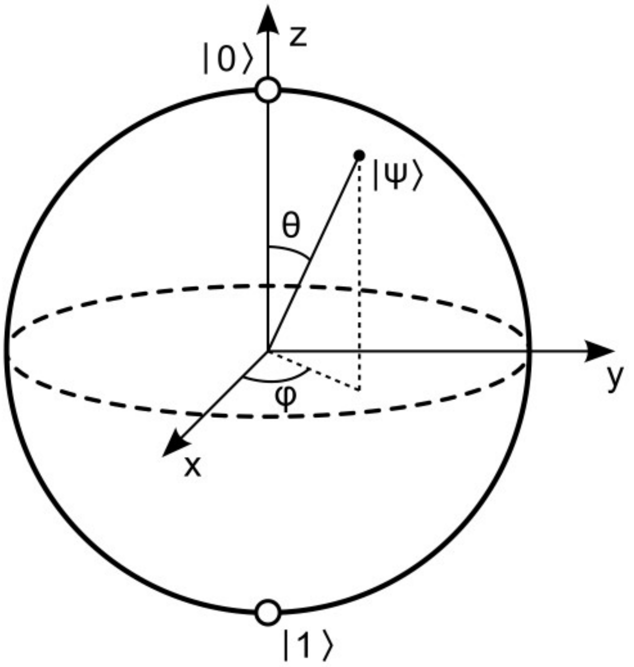


Figure 6.1: Bloch sphere representation of a qubit. Figure credits: Smite-Meister (CC BY-SA 3.0).

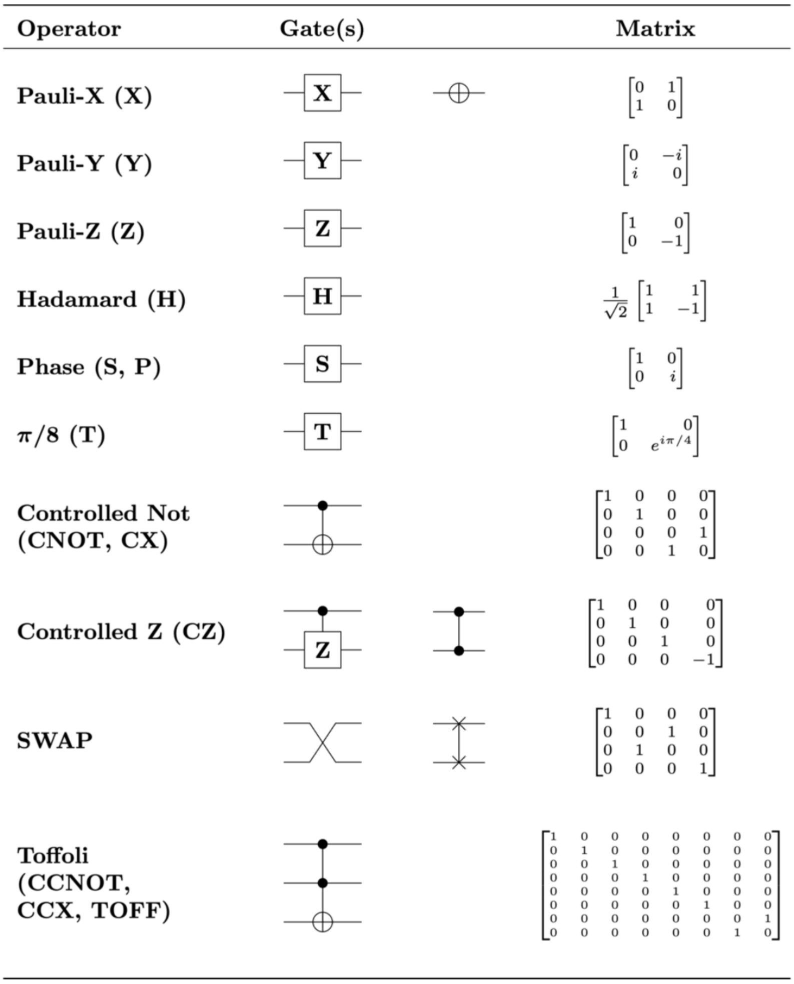
coefficients as α and β the superposition state $|\psi\rangle$ can be constructed as:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{6.1}$$

A state that can be described in this form, with the unitary sum of probabilities $|\alpha|^2 + |\beta|^2 = 1$ is said to be a pure state and it has an intuitive graphical representation in the Bloch sphere of figure 6.1. The two basis elements are in the poles of the sphere and pure states can be placed at any point of the surface of the sphere. More general states that do not accept the decomposition of equation 6.1 are called mixed states and occupy internal points in the Bloch sphere.

States with the structure of equation 6.1 will form the basic building blocks of our quantum computing scheme and will be called qubits. Qubits are up to a certain point analogous to the classic bits, but were bits can take only two discrete values, qubits can exhibit an infinite continuum of possible values. Other interesting property of quantum states is that they can exhibit entanglement, i.e. the state of two or more particles cannot be described independently of the state of the others, even when the particles are separated. This is a very interesting property of quantum mechanics that allows to have perfect correlation (or anticorrelation) in the measurement of two distinct particles. It is also a concept that can greatly simplify the mathematical framework involving the interaction of many particle.

The interest of quantum computing is to work with multiple qubits



Operator	Gate(s)		Matrix
Pauli-X (X)	X		$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)	Y		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)	Z		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)	H		$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Phase (S, P)	S		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$ (T)	T		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
Controlled Not (CNOT, CX)			$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
Controlled Z (CZ)	Z		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
SWAP			$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Toffoli (CCNOT, CCX, TOFF)			$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$

Figure 6.2: Most relevant quantum gates. Credits: Wikipedia (CC BY-SA 3.0).

since if we can make N qubits interact together we can construct an 2^N-dimensional complex vector[4] . As an example let's imagine that we can build a quantum computer capable of performing any operations over 300 input qubits (e.g. efficiently simulate the interactions between 300 particles). To perform the same operations a classical computer would need to cover a complex vector space of 2^{300}, i.e. it would require a memory with more bits than the number of particles in the observable universe, something clearly not tractable.

As it happens with classical bits, logical operations can be performed on a qubit or a set of qubits. The abstract boxes performing these operations are called gates and following our notation they can be represented as matrices[5] . Typical classical gates are NOT, OR, AND, XOR, NAND and NOR, while the basic quantum gates are represented in figure 6.2. The particularity of quantum gates is that they are reversible, i.e. each gate establishes a one-to-one correspondence between the input and the output. For this to be possible some gates use ancillary qubits in the input or output. To learn more about these topics a good pedagogic book is [18].

It can be demonstrated that any quantum algorithm can be executed using a circuit of gates with a limited set of gates types[6] . If we are able to generate states that act as qubits and devices that act as quantum

[4] This statement is a simplified version of one of the Dirac-Von Neumann axioms of quantum mechanics, which relates the qubit interactions as tensor products. Unfortunately there is not an intuitive visual representation for more than one qubit, as the Bloch sphere is for one qubit.

[5] Gates involving one qubit will be 2×2 matrices. Gates involving 2 qubits will be 4×4 matrices. In general gates involving n qubits can be represented as $2n \times 2n$ matrices. Note that while in the classical paradigm the only useful one bit operations are 0, 1 and NOT, in the quantum paradigm more options arise

[6] Different sets are possible. The easiest to implement globally will be used in each case. Note that due to the reversibility of the quantum gates, the original inputs can be recovered running the circuit backwards.

gates we would be capable of running any quantum algorithm that we can imagine. This of course has caveats, that we will discuss in the following sections.

6.3 Types of quantum computing

The previously discussed corresponds to the most general version of a quantum computer. It can be understood as a circuit of quantum gates that perform a set of operations and measurements over a set of inputs. An example can be seen in figure 6.3, but it is not the only type of quantum computer. In 2000 David DiVicenzo [21] gave five criteria that a quantum computer should fulfil to be considered such:

- It should be possible to initialize the state of the qubits to simple fiducial states.
- The times of decoherence should be sufficiently long.
- A universal set of gates should be available.
- The resulting qubits should be measurable.
- The physical system should be scalable.

An alternative to circuit-based quantum computing is noiseless adiabatic quantum computing and they can be proven to have the same computational power [22]. Quantum annealing is a noisy version of adiabatic quantum computing that is not believed to provide relevant quantum advantage, but it is already available commercially by the company D-Wave. Note that the number of announce qubits are in the order thousands, but the machine is not a universal quantum computing, although there is some interest in testing possible weaker forms of quantum advantage using those devices.

Also equivalent to circuit-based quantum computing is one-way quantum computer (also known as measurement based quantum computing, MBQC) where an entangled state state is prepared and single qubit measurements are performed. The measurement bases depend on previous results, so not all the measurements can be performed simultaneously. The measurement collapses the state hence the name one-way, since it is not reversible.

Topological quantum computing is a mathematical framework, equivalent in power to circuit-based quantum computing, that presents in theory certain advantages against decoherence compared to other

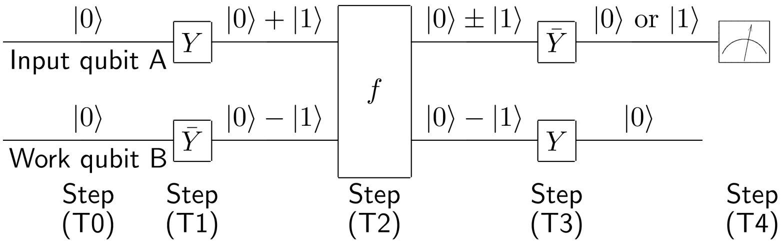


Figure 6.3: Example of quantum circuit [19]. The circuit solves the Deutsch-Jozsa quantum algorithm that determines if a function is constant or balanced. It was the first experimental implementation of a quantum algorithm in [19] and [20].

systems. It remains an abstract conception, and although an implementation should be theoretically possible using anyons its practical implementation remains elusive.

Instead of building a general purpose system that can be programmed to solve any quantum algorithm, it is possible to build specialized systems focussed on solving particular tasks. For example, it is possible to construct a system where N states can be initialized, configured to interact with each other in a a particular manner (not necessarily through quantum gates) and measure the resulting states. This is particularly useful to simulate effects in many body physics [2, 23], reason why these systems are usually called quantum simulators[7] . These systems are typically easier to construct than universal quantum computers, so they are expected to be the first to provide significant results compared to classical computers. For example, the simulation of 54 entanglement particles would require a memory size in the order of petabytes, but it could be efficiently simulated with a quantum simulator capable of managing 54 quantum states[8] .

6.4 Implementations

At this point in history we can safely say that the theoretical understanding of quantum computer is more advanced than the outcomes of the experimental implementations. If we analyse DiVicenzo's conditions for a quantum computer we can understand why: we need to construct a system that manages an ensemble of states that can arbitrarily interact among themselves, but at the same time interact very weakly with the environment, and that is very hard to do in practice.

This challenge is very exciting for scientists and technicians, since the many research opportunities arise. At these moment several operational quantum computers have been built, but it is not yet clear that a technology will impose over the others as occurs in the classical case with silicon. The general purpose quantum computers built so far (and the ones expected in the near term) have a limited number of operational qubits subject to a lot of noise. The term NISQ (Near Intermediate-Scale Quantum) technology has been popularized [24] to denominate those devices and although they are expected to demonstrate some quantum speed up, their main objective is to serve as learning platforms for the development of more advanced quantum computers in the future.

A lot of effort is required to build those systems, so it is not strange that multinational companies such as Google, IBM, Intel and Microsoft are taking the lead on their development, but also some dedicated companies are making substantial efforts like Rigetti, Xanadu and ionQ, as well as many academic research labs worldwide. Important landmarks are the availability of quantum computing as a cloud service[9] or the publication of the first task were a quantum computer clearly outperforms a classical computer [25].

[7] The denomination can be confusing. A quantum simulator is a specific purpose quantum computer, while a quantum emulator is a classical computer that mimics the behaviour of a quantum computer, although in loose language the latter can also be called classical quantum simulator.

[8] A classical supercomputer could simulate up to 50-56 particles, but as the number of particles increase the memory size would grow exponentially.

[9] For example IBM offers free access to a 5-qubit quantum computer using the cloud and a pay-to-access service to more advanced quantum processors.

In the following we will briefly discuss some of the proposed technologies at the time of writing. Remember that they should fulfil the five DiVicenzo conditions, being decoherence, interaction and scalability the most difficult to implement.

Ion traps

Atomic ions (or charged particles) can be suspended in an electromagnetic field (a trap) and moved relatively inside the trap. The qubit can be stored in the stable electronic state of each ion and lasers can be applied over the ion in order to perform a one qubit operation. For two qubit operations the properties of entanglement between qubits can be used and the control can also be done by lasers [26–28].

Computers up to 20 qubits have been built and they are expected to continue evolving. Their main advantage is probably the possibility of establishing networks of ion trap quantum computers relatively easily and their operation at room temperature.

Superconducting

Electrons are the basic carrier of information in classical computing and they behave as fermions. In the superconducting variation of quantum computer the carriers of information are pairs of electrons (Cooper pairs) that behave as a boson, hence a Bose-Einstein condensate occupying a single quantum level at cryogenic temperatures. The technical manoeuvre comes from the use of Josephson junctions, a weak connection between two leads of superconducting wire that allows the creation of an anharmonic oscillator, with two addressable states. Charge, phase or resonance (most typically) can be used to interact with the qubits and perform the quantum logic gates [29, 30].

Although the control of the qubits tends to be noisy, the possibility of lithofabrication on a chip and the development of dilution refrigerators to get temperatures lower than 100 mK, makes them a very interesting option to construct a quantum computer. Superconducting qubits are the current technology of choice for many of the current players (Google, IBM, Rigetti, Intel) and systems of up to 72 qubits have been announced.

Nuclear magnetic resonance

Instead of using a single pure quantum state as physical support for the qubits, the nuclear magnetic resonance quantum computing (NMRQC) systems use an ensemble of molecules for this tasks [31–33]. In this case each addressable spin of the molecule (distinguishable by NMR spectroscopy) corresponds to a qubit, but it is distributed along the entire solution in liquid state NMR or solid in solid state NMR. When the ensemble of molecules is under the influence of a strong magnetic field, the family of processes used in magnetic resonance imaging (MRI) [34] can be used to prepare qubits, implement gates and read results.

NMR was the first technology used to implement a quantum algorithm [19, 20] but poses the drastic problem of scalability in the number of qubits as it is difficult to find molecules with a great number of different addressable spins. The technology and principles are very related to superconducting quantum computers as the same type of resonance processes are used to prepare and read quantum states. It shares also many common points with MRI.

Other technologies

Many other technologies and variations can be used to implement a universal quantum computer and each one faces the same challenges with different struggles. It is likely that in several years we will see implementations combining different technologies for different tasks.

Some of the relevant technologies are cold atoms, similar in principle to the trapped ions with neutral atoms and different trapping mechanisms; linear optics (under some conditions) can be used to implement a universal quantum computer, which is a very interesting option since it would allow a high level of integration using photonic chips and operation at room temperature; the defects in the atomic lattice of diamond can also be used as qubits and a quantum computer would be possible; quantum dots (semiconductor ensembles of few nanometers behaving like an artificial atom) are also good candidates to act as qubits.

6.5 Algorithms

Quantum computers are built with the intention of running quantum algorithms. This is interesting because a tool with the capabilities of a quantum computer can solve efficiently more problems that a classical computer. This can be represented using complexity classes. P represents the set of problems solvable in polynomial time and NP (nondeterministic polynomial time) represents the set of problems whose solution can be verified in polynomial time. Classical computers are believed to be efficient to solve problems in the P set, but quantum computers would be efficient to solve problems in BQP (bounded-error polynomial time) which is strongly believed to contain P and other sections of NP (but not NP-complete problems), as can be seen in the representation of figure 6.4.

A famous problem that lies in BQP and not P is the factorization of large numbers, for which there exists a quantum algorithm that provides exponential speed up with respect to the classical counterpart [3]. For the implementation of algorithms lying in BQP we would need a universal quantum computer, which will focus the rest of this section. Note that the speed up gain is not always exponential, for example

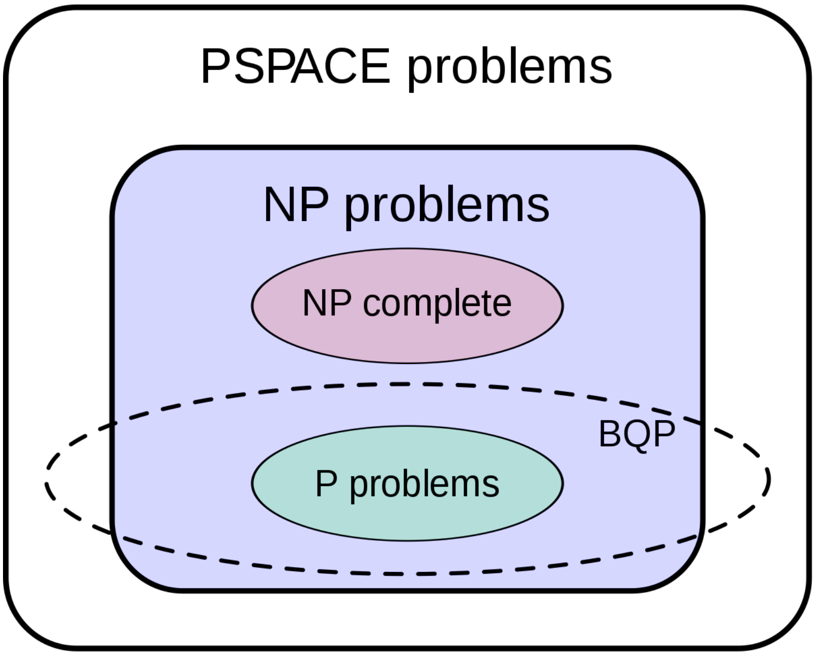


Figure 6.4: Scheme of relevant complexity classes. The BQP relation is not formally proven, but suspected to be true. Image source: Wikipedia.

Grover's algorithm to search in an unstructured list requires $\mathcal{O}(\sqrt{N})$ steps against the $\mathcal{O}(N)$ required by the best classical algorithm.

The universal quantum computer relies on the fact that its qubits will be reliable and will not suffer decoherence with time, but we have seem that in practice they are noisy. As in classical communications it is possible to make the transmission more robust sacrificing rate and using redundancy, the same thing can be done in quantum computing. A set of noisy physical qubits can be used to construct an ideal logical qubit in what is called quantum error correction [35]. This will probably allow the advent of useful universal quantum computers making them fault-tolerant, but it comes with a great price to pay: the current quantum error correcting codes known to us require a lot of redundancy (in the order of 10 000 physical qubits to obtain a single logical qubit). For example, to obtain the prime factors of a 1 000 bit number (typical value used in RSA) using Shor's algorithm a quantum computer with 10 million physical qubits would be required (at the time of writing we are struggling with 72 qubits).

The previous paragraph might seem disappointing, quantum computing is tremendously hard to implement, at least to be able to apply it to useful problems. The reason to push forward is that we have provable reasons to believe that the capabilities of a quantum computer are strictly higher than those of a classical computer [36] and we are exploring new ways to overcome the obstacles [37]. This fact is commonly refer as quantum supremacy (or quantum advantage to use a less controversial term) and to experimentally prove it has become one of the challenges of current developers. Researchers from Google have recently published [25] their results on a sampling problem that can be performed in seconds in their quantum computer, but it would take years in the most powerful supercomputer available today. The issue is that the problem has not relevant practical applications and it seems to be designed to fit the capabilities of current NISQ computers.

A much broader set of algorithms exist [38] and most of them would be useful. A very generic one would facilitate the resolution of systems of linear equations [39], but in many occasions these algorithms have requirements that might decrease their performance. For example, we might want to process classical data but the algorithm we are using requires that the input data is provided in a quantum superposition costly to prepare in order to be effective. Other algorithms require storing N d-dimensional input states into a qRAM (quantum random access memory) formed by $\log(Nd)$ qubits, which is a device costly to implement (in technological terms). This reduces the applicability of certain quantum algorithms when applied to a set of data only once, but the advantage remains valid if the algorithm can be run multiple time over the same set of data.

Optimization problems are relatively common in human life, and some of them are NP-hard problems for which we do not expect a substantial quantum speed up as such. But in some cases, if we are willing to accept an approximative answer we might get an advantage by using quantum computers. A paradigm is to prepare an input quantum state in a quantum computer, run the evolution and mesure the state; the output is fed to a classical optimizer that modifies the input state of the quantum computer for the next run; the process is run iteratively until an acceptable solution is found. When applied to classical combinatorial optimization problems these algorithms receive the name of quantum approximative optimization algorithm (QAOA), while they go by the name variational quantum eigensolver (VQE) when applied to many-body physical problems (the minimum energy state is usually the target). These classical-quantum hybrid algorithms are very interesting since they are feasible with NISQ devices. A more restricted sub-branch of optimization, quantum semi-definite programming might be implementable using near term quantum computers, without an external classical optimizer.

Classical machine learning was a hot topic during the last few years, specially with the advent of deep learning, which is still giving surprising results in the classical world. Quantum machine learning (QML) or perhaps more accurately quantum enhanced machine learning (QEML) [40–42] is the quantum version of machine learning and it could be implemented using hybrid classical-quantum systems, since the data will typically be classical and this impairs the efficiency of the protocols. Some of them cannot be proven to be more efficient that classical counterparts but they rely on heuristics that need to be better understood before formulating solid claims. A first approach, using small sets of classical data, can be recommendations systems [43]. Quantum algorithms might inspire improvements in classical algorithms as well.

It is important to remark that for many problems (like the ones we can already perform with a personal computer) it would not make sense to have a quantum computer [44]. For this reason it is likely that quantum computers will act as accelerators for particular tasks of interest (like current graphic cards in a personal computer) and not as the main entity of processing. As they will be costly (at least in the first years) they will probably be accessed remotely, which might be a concern if the data or algorithms to be performed are of sensitive nature. Fortunately there are solutions that would help us in this case: blind quantum computing and quantum verification. Blind quantum computing [45] allows the possibility of running a program remotely without letting the entity operating the quantum computer know the nature of the data involved. Quantum verification [46] allows a user with limited quantum capabilities to verify that the calculations performed by a quantum computer were really quantum.

6.6 Discussion

Applications in medicine

The applications in the biological science are wide and diverse, but perhaps the first beneficiary will be computational chemistry [15, 47–49]. The possibility of simulating big ensembles of particles will facilitate the development of new drugs, as its molecular conformation could be configured and optimized in a quantum computer. This could be done with a universal quantum computer or more likely in the near term by specialized quantum simulators.

As the capacity of those systems increases the capacity to simulate bigger molecules like proteins will be efficient, being the understanding of protein folding one of the first targets [50]. This also opens the door to more personal treatments, since the the effect of particular drugs and treatments could be previously simulated as a function of the genetic information of the patient.

More general results in the biological sciences are covered in the review [14], highlighting genetics and sequence analysis, functional genomics and mapping of neuro-behavioural variations. Many of these algorithms would require a universal quantum computer with qRAM, which might be lay far ahead in the future, but some of the applications could benefit from QEML algorithms already applicable to NISQ machines. In fact one of the main challenges of quantum computer scientist is to develop new algorithms that could run in this kind of devices.

Regarding the application to the medical practice, some reflections are shared in [13], illustrating several possible scenarios. The quantum computer is expected to be a complement to the practician, not a substitute. The most immediate improvements will be the increase in treatment precision (drug prescription, radiation therapy, surgery, psychological response...) and the time of response to obtain the results (as calculation speed would be improved), but probably the most disruptive effect the transformation of some previously intractable problems into reality. Some examples could be the use of quantum simulators to predict the effect certain drug in a particular patient or QEML to better determine the diagnostic and prognostic of a particular patient. Applications could also be extended to particular population of arbitrary size.

Chapter conclusions

Quantum computing is a complex branch of science and technology, still in its infancy and with a long way ahead, but it is already giving the first interesting results. Its holy grail, the universal fault-tolerant quantum computer, might be technologically distant in the future, but progress is robust and steady. In the meantime we will make use of NISQ devices to better understand the possibilities that this new technology is offering us.

Quantum simulators (non universal quantum computers) are a very interesting midpoint for natural sciences, including medicine, since it allows the efficient simulation of large ensembles of particles which will boost the development of materials and chemical elements, some of them of interest for medicine, such as drugs.

The great potential of quantum computing should not be neglected in the medical practice, since it can open the opportunities to new treatments and the improvement of the current ones. The counter-intuitive nature of quantum mechanics should not pose an obstacle and user friendly interfaces should be put to the disposition of the practician, clearly stating what can and cannot be done by a quantum computer.

Emphasize that at least in the short term quantum computers will be accessed remotely, using a client-server approach where the client might not be fully trusted. In this scenario, blind quantum computation and quantum verification can be used to hide data and/or sequence of operations to the untrusted server. This is an important resource for medical applications.

Regarding the fourth initial objective of this document, the relation of nuclear medical imaging with some of the quantum computing technologies is clear since similar techniques are used when preparing and probing quantum states using resonance. We recommend going through the provided references to investigate this similarities as it would be too technical to cover in this text.

Quantum Key Distribution 7

7.1 Introduction

Quantum computers provide fantastic calculation advantages against certain problems. One of these problems is the one that facilitates the exchange of keys over public channels and allows us to perform secure communications over the Internet. The most widespread algorithm to distribute key is RSA (Rivest-Shamir-Adleman) and its security is based on the difficulty of factorizing big numbers... with a classical computer. But as we have seen a quantum computer could solve this problem in linear time [3] and this method (as many similar ones) will not be secure in a world where a quantum computer exists.

An alternative to solve this problem is to invent new algorithms that are not vulnerable to attacks by a quantum computer. This is currently being done in a branch of cryptography called post-quantum cryptography, which consists on classical algorithms despite the quantum in the name. The problem is that with our current knowledge it is not possible to prove if an algorithm is completely secure against any kind of attacker, much less a quantum computer. These systems are said to provide computational security, i.e. the security depends on the computational resources of the attacker.

The non-existence of an efficient algorithm at a certain point of time does not imply that it cannot exist in the future. This opens the window to an attack in the future if the information was stored since the moment of the information exchange, compromising the security. In computational security security will always decrease with time.

Another possibility is to devise a system whose security does not decrease with time. This is indeed possible using the properties of quantum mechanics, and the technologies allowing the generation of secret (up to an arbitrary factor ϵ) keys between two parties that trust each other receive the name of quantum key distribution (QKD) systems.

The importance of long term security is illustrated in figure 7.1. It is specially relevant for medical information that must be kept secure during the subject life time.

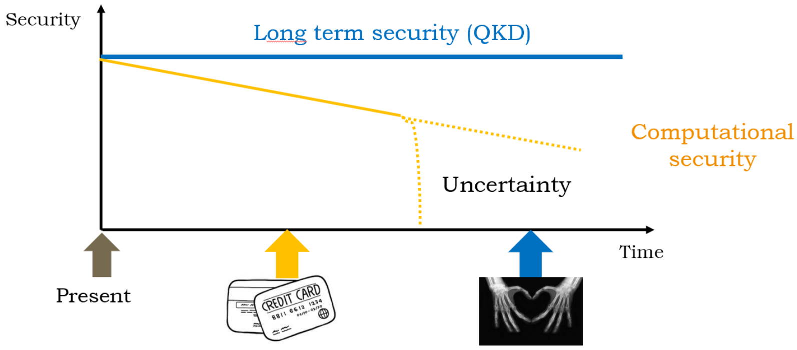


Figure 7.1: Importance of long term security. The computational security provided by post-quantum cryptography might be perfectly useful for applications that have a short life span, such as economic transactions. Medical data should be secure for long periods of time and requires long term security.

7.2 Brief history of QKD

An article by Nick Herbert on superluminal communication [51] triggered two famous counter articles by Wootters and Zurek [52] and Dieks [53] formally proving the impossibility of creating an identical copy of an unknown quantum state. This concept is known today as no-cloning theorem and the idea is related to the 1970 article by James Park [54] showing that it is not possible to create a non-disturbing measuring mechanism.

During the decade of 1970 Stephen Wiesner had the idea of using the properties of quantum mechanics to devise a system that could prevent the forgery of bank notes [55]. In a generalization of his scheme the banknotes are released by the bank with a serial number and a series of quantum states[*]. The quantum states can have four possible values forming conjugate observables that are chosen randomly and are only known to the bank[11] . When the users want to exchange the banknote with the bank, they need to send the quantum states associated with the serial number for verification. An honest user would have no problems passing the verification, but the user of a cloned banknote would only pass the test with probability p^N, with N the number of states[12] . As N becomes large the probability of detecting forged money approaches 1.

[11] In his article Wiesner used the photons in four polarization states $|H\rangle$, $|V\rangle$, $|+\rangle$ and $|-\rangle$ as quantum states. This is equivalent to choosing randomly two values in two non-orthogonal bases.

[12] For the set of states in the article $p = 3/4$.

The same idea of conjugate observables was used by Charles Bennett and Gilles Brassard with a new purpose. They assumed that the two trusted entities Alice and Bob have at their disposal a quantum insecure channel and a classical authenticated channel. Then they can exchange information through the quantum channel and characterize if the channel has been eavesdropped revealing some information through the classical channel. This opens the possibility of indefinitely expanding a secret key using an insecure medium. In their famous BB84 protocol [5] they provide a possible implementation of this idea. Many variations and protocols with the same purpose but focusing in different principles were later developed.

[*] The storage of the quantum states is one of the most important practical impairments of this protocol, since it requires the use of quantum memories, which are currently in an early development stage.

7.3 Basic principles

Most of the available QKD protocols can be divided into the following steps:

- **Distribution of quantum states.** Quantum states are created, transmitted and measured between the two entities. A process to agree on the used bases (sifting) is usually needed. After this phase Alice and Bob share two sets of partially correlated values.
- **Parameter estimation.** Alice and Bob reveal a random part of their correlated values in order to estimate the channel. The revealed values will not be used in the final key, so there is a trade-off between the values revealed to have an accurate estimation of the channel and the final length of the key.
- **Reconciliation.** The correlation in the first phase is not perfect and needs to be corrected. Classical error correcting codes can be used in most cases. The output of this phase is a shared string of values with no errors.
- **Privacy amplification.** Not all the values in the previous string are secret, so a classical process is performed in order to adapt the string to the secret key length predicted by the security proof as a function of the estimated parameters[13] . The result is a shared secret key.

Remark that only the first phase involves quantum mechanics directly, the rest of the steps being completely classical. For this reason in proof-of-principle scenarios it is typical to complete the quantum distribution and obtain the estimated parameters. The security proof will predict the length of the key if the reconciliation efficiency is known. While a commercial product would require the completion of all phases we will use the proof-of-principle approach.

Relevant concepts

In 1991 Artur Ekert [56] published E91 a QKD algorithm that was conceptually different from BB84, since the security was based on the use of entangled photons. Other protocols based on entanglement like BBM92 [57] followed soon. This opened the division between entanglement-based protocols and non-entanglement-based ones. Very soon it was realized that there is a framework where an entanglement-based protocol has a non-entanglement equivalent and vice-versa. In some occasions the implementation is more natural using entangled states, but generally the non-entanglement version (also called prepare and measure) is preferred.

The concept of using entanglement for QKD is interesting because it expanded the idea of entanglement swapping to its use as quantum repeaters[58]. Optical amplifiers as used in classical communications would irreversibly corrupt the quantum states, so they cannot be used to recover the signal lost due to the channel attenuation. The idea behind quantum repeaters is to use quantum teleportation in order to guarantee the distribution of entangled photons between two locations.

[13] The size of the key will decrease for worse conditions of the estimated parameters, becoming null after certain parameter conditions are exceeded.

It is a promising but challenging field that would be useful not only for QKD, but for other communication protocols as well.

The losses in the channel will degrade the achievable key exchange between the trusted parties. As the losses are function of the channel distance this seriously limits the range of QKD. The limits for a repeaterless setting can be calculated independently of the protocol [59], although in practice some protocols will perform better than others at longer distances. A recently developed family of protocols called twin-field (TF-QKD) [60, 61] has been able to surpass the repeaterless limit, but it can be interpreted as a repeater model simplified for implementation.

One possible bypass to overcome the distance limit is the use of trusted nodes, i.e. dividing a long communication distance into several shorter point-to-point links. An interesting aspect of trusted nodes is that a network of trusted users could be constructed, but the inconvenience is that all the nodes have information about the key, so they need to be trusted. There should be also some physical security mechanism to ensure that the intermediate devices are not tampered with. The most extensive trusted node network at the moment of writing expands for more than 2 000 km between several major cities in China[62].

A possible concern with the proposals so far is that a malfunction (imperfection or malicious attack) in some of the components of the system could compromise the security of the system. In 1998 Mayers and Yao [63] introduced the idea that self-testing quantum systems would be useful to reduce this device dependence on QKD. Self-testing only considers the input-output statistics of a black box performing some operations, and in order to prove honesty from the black box a suitable function should be used. Ten years later Colbeck [64] proposed the use of Bell tests in order to verify the honesty of the devices. The protocols working under this settings have the advantage of removing unnecessary trust in the components, hence their name device independent protocols (DI-QKD). The concept can be extended to randomness expansion and randomness amplification. The main drawback is their complex implementation since it is difficult to obtain loophole-free Bell test measurements or equivalent [65–67].

A less restrictive approach is to assume that only the detectors can be untrusted leading to the family of measurement device independent [68] protocols (MDI-QKD). They are more easily implementable than DI protocols [69] and eliminate the dependence on the trustfulness of the detector (the measurements can even be done by a third untrusted party).

So far we have considered the exchanged states independently. It is possible to use some relation between the different states as the source of correlation between Alice and Bob. The family of protocols that uses the phase between consecutive states as resource is called distributed-phase reference QKD. The two main examples are differential phase shift (DPS)[70, 71] and coherent one-way (COW)[72]. Their main advantage is the simplification under some operational settings.

The great majority of the previous protocols work with states that can take only a discrete set of values. This simplifies the analysis of the system, but can make the implementation difficult since those states can be difficult to generate or detect. QKD can also be extended to an infinite dimensional Hilbert space in what is called continuous variable QKD (CV-QKD) in contrast to the previous ones, referred as discrete variable (DV-QKD). The infinite dimensional Hilbert space can be simplified to a finite dimension working in phase space, and for Gaussian states (and in particular coherent states) the information can be bounded in order to obtain security proofs. The main advantage of this family is the simplification of the implementation, as it is possible to construct a commercial QKD system using only standard telecommunication technology.

Some of the previous characteristics can be combined in order to adapt to different scenarios. For example it is possible to have MDI-CV-QKD taking the advantage of CV and MDI approaches. Not all the combinations are possible but many of the concepts can be combined.

7.4 QKD today

At the time of writing QKD is an emerging technology that is continuously evolving and expanding. Numerous groups in the world work on the development of new ideas and the improvement of the technology in order to facilitate the access to high secret key rates at convenient distances. Other groups focus on the weak points of protocols and implementations to ensure that they work as expected under malicious conditions in what is known as quantum hacking. This provides an iterative approach where protocols and implementations are improved to work in more realistic conditions. A simple example would be BB84 with decoy states[73], an evolution of BB84 that can work with weak coherent states of light instead of perfect single-photon sources.

It is not the purpose of this document to cover the whole field since extensive general QKD reviews can be found in the literature [74, 75], as well as more specific ones on CV-QKD [76]. We will only mention the features more closely related to this document.

The use of photonic integrated chips (PIC) for applications in quantum technology has grown extensively over the last years. Researches in Bristol [77] have recently developed silicon chips capable of running several DV-QKD protocols. The use of PICs for CV-QKD has also recently proven viable [78, 79] obtaining levels of shot noise compatible with the generation of key.

7.5 Discussion

Applications in medicine

Information security, and privacy in particular, should be a topic of major concern in medicine. It is a topic that gain importance with the onset of personalized medicine. If more precise treatment of genetic information allows more efficient treatments and becomes widespread, it becomes necessary to maintain great amounts of private information away from untrustworthy eyes. This includes the clinical record, genetic information and other personal information.

Most of the delicate information concerns the complete life span of the individual, so long-term security approaches should be enforced in order to guarantee that they will remain secure against possible future attacks.

Chapter conclusions

The future quantum computer compromises the current schemes to distribute secret keys between trusted entities. At this moment there are two possible solutions available:

- ▶ Update the old classical algorithms to new classical algorithms robust against attacks by a quantum computer (post-quantum crypto).

  Pros It is a software solution, easy to deploy and a smooth continuity to current solutions.

  Cons It cannot be proven to be secure (new quantum algorithms might appear in the future), so long term security cannot be guaranteed.

- ▶ Update the old classical algorithms to new classical algorithms robust against attacks by a quantum computer.

  Pros Secure in the long term.

  Cons Depends on additional hardware and quantum channels, which makes its deployment more complex. It is also more susceptible to denial of service attacks and should be combined with classical systems for redundancy.

Medical deserve long term privacy, so QKD should be preferred when possible. This would solve the security problem in the exchange of the key. Current symmetric cryptography is believed to be secure against attacks by a quantum computer.

It is important to emphasize that those system focus on point to point security, assuming that the trusted entities do not leak any information. This means that the user terminal should be properly used in order to profit the gain in security. This might affect policies in how sensible information is treated along the medical process.

Conclusions and prospects 8

The value of information seems to become more and more relevant in society. Although this can be beneficial in many aspects it can also be used against some individuals. For this reason it is important that particularly delicate information, such as the related to the health of individuals or groups of population, remains private for a long time. This can be a problem when we need to communicate this information through a public channel, but fortunately we have several alternatives that might be combined to offer the best results.

The point to point security provided by QKD or post-quantum crypto should be accompanied by strict policies concerning the medical community (doctors, nurses, radiologists, administration staff...) and the concerned users.

Quantum computing is expected to provide breakthrough changes in our communities, including the improvement of medical attention. The first results will probably appear at the research level, but practitioners will progressively become active users. From a medical point of view it will be important, not only to understand the possibilities of quantum computing from a user level, but to understand also the basic underlying concepts in order to optimize its potential usage.

The future of quantum is quite speculative, especially regarding the time scope of the technological advances. The optimistic vision is that in a few decades relevant quantum computers will be up and running, offering solutions to the human kind. More pessimistic are those who believe that quantum computers could be put to bad uses (which cannot be discarded) or those who believe that it will never attain the technical maturity required to tackle the most promising problems. In any case quantum technologies should be regarded as a source of possible advancements in medicine that could be combined with progress in other fields.

Bibliography

Here are the references in citation order.

[1] Richard P. Feynman. ‘Simulating physics with computers’. In: *International Journal of Theoretical Physics* 21.6 (1982), pp. 467–488. DOI: 10.1007/BF02650179 (cited on page 4).

[2] Seth Lloyd. ‘Universal Quantum Simulators’. In: *Science* 273.5278 (1996), pp. 1073–1078. DOI: 10.1126/science.273.5278.1073 (cited on pages 4, 19).

[3] Peter W. Shor. ‘Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer’. In: *SIAM Journal on Computing* 26.5 (Oct. 1997), pp. 1484–1509. DOI: 10.1137/s0097539795293172 (cited on pages 4, 21, 27).

[4] Lov K. Grover. ‘Quantum Mechanics Helps in Searching for a Needle in a Haystack’. In: *Physical Review Letters* 79.2 (July 1997), pp. 325–328. DOI: 10.1103/physrevlett.79.325 (cited on page 4).

[5] Charles H. Bennett and Gilles Brassard. ‘Quantum cryptography: Public key distribution and coin tossing’. In: *Theoretical Computer Science* 560 (2014). Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84, pp. 7–11. DOI: https://doi.org/10.1016/j.tcs.2014.05.025 (cited on pages 5, 28).

[6] P. A. M. Dirac. *The Principles of Quantum Mechanics*. Clarendon Press, 1930 (cited on page 7).

[7] Richard Phillips. Feynman. *QED : the strange theory of light and matter / Richard Feynman*. English. Princeton University Press Princeton, N.J, 1985, x, 158 p. : (cited on page 7).

[8] Peter R. Holland. ‘Is Quantum Mechanics Universal?’ In: *Bohmian Mechanics and Quantum Theory: An Appraisal*. Ed. by James T. Cushing, Arthur Fine, and Sheldon Goldstein. Dordrecht: Springer Netherlands, 1996, pp. 99–110. DOI: 10.1007/978-94-015-8715-0_7 (cited on page 7).

[9] C. E. Shannon. ‘A Mathematical Theory of Communication’. In: *Bell System Technical Journal* 27.3 (1948), pp. 379–423. DOI: 10.1002/j.1538-7305.1948.tb01338.x (cited on page 7).

[10] Larry J. Stockmeyer. ‘The polynomial-time hierarchy’. In: *Theoretical Computer Science* 3.1 (1976), pp. 1–22. DOI: https://doi.org/10.1016/0304-3975(76)90061-X (cited on page 7).

[11] Scott Aaronson and Chris Bourke. ‘The Complexity Zoo’. In: (Jan. 2008) (cited on page 7).

[12] Luis Trigo Vidarte. *Design and implementation of high-performance devices for continuous-variable quantum key distribution*. 2019 (cited on page 9).

[13] Dmitry Solenov, Jay Brieler, and Jeffrey F. Scherrer. ‘The Potential of Quantum Computing and Machine Learning to Advance Clinical Research and Change the Practice of Medicine’. In: *Missouri medicine* 115.5 (2018). PMC6205278[pmcid], pp. 463–467 (cited on pages 11, 24).

[14] Prashant S. Emani et al. *Quantum Computing at the Frontiers of Biological Sciences*. 2019 (cited on pages 11, 24).

[15] Yudong Cao et al. *Quantum Chemistry in the Age of Quantum Computing*. 2018 (cited on pages 11, 24).

[16] Gordon E Moore et al. *Cramming more components onto integrated circuits*. 1965 (cited on page 15).

[17] Thomas N. Theis and H. -S. Philip Wong. ‘The End of Moore’s Law: A New Beginning for Information Technology’. In: *Computing in Science and Engg.* 19.2 (Mar. 2017), pp. 41–50. DOI: 10.1109/MCSE.2017.29 (cited on page 15).

[18] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000 (cited on page 17).

[19] Isaac L. Chuang et al. ‘Experimental realization of a quantum algorithm’. In: *Nature* 393.6681 (1998), pp. 143–146. DOI: 10.1038/30181 (cited on pages 18, 21).

[20] J. A. Jones and M. Mosca. 'Implementation of a quantum algorithm on a nuclear magnetic resonance quantum computer'. In: *The Journal of Chemical Physics* 109.5 (Aug. 1998), pp. 1648–1653. DOI: 10.1063/1.476739 (cited on pages 18, 21).

[21] David P. DiVincenzo. 'The Physical Implementation of Quantum Computation'. In: *Fortschritte der Physik* 48.9-11 (2000), pp. 771–783. DOI: 10.1002/1521-3978(200009)48:9/11<771::AID-PROP771>3.0.CO;2-E (cited on page 18).

[22] Dorit Aharonov et al. *Adiabatic Quantum Computation is Equivalent to Standard Quantum Computation*. 2004 (cited on page 18).

[23] Hans De Raedt et al. 'Massively parallel quantum computer simulator, eleven years later'. In: *Computer Physics Communications* 237 (2019), pp. 47–61. DOI: https://doi.org/10.1016/j.cpc.2018.11.005 (cited on page 19).

[24] John Preskill. 'Quantum Computing in the NISQ era and beyond'. In: *Quantum* 2 (Aug. 2018), p. 79. DOI: 10.22331/q-2018-08-06-79 (cited on page 19).

[25] Frank Arute et al. 'Quantum supremacy using a programmable superconducting processor'. In: *Nature* 574.7779 (2019), pp. 505–510. DOI: 10.1038/s41586-019-1666-5 (cited on pages 19, 22).

[26] Colin D. Bruzewicz et al. 'Trapped-ion quantum computing: Progress and challenges'. In: *Applied Physics Reviews* 6.2 (June 2019), p. 021314. DOI: 10.1063/1.5088164 (cited on page 20).

[27] J. I. Cirac and P. Zoller. 'Quantum Computations with Cold Trapped Ions'. In: *Phys. Rev. Lett.* 74 (20 May 1995), pp. 4091–4094. DOI: 10.1103/PhysRevLett.74.4091 (cited on page 20).

[28] D. Kielpinski, C. Monroe, and D. J. Wineland. 'Architecture for a large-scale ion-trap quantum computer'. In: *Nature* 417.6890 (2002), pp. 709–711. DOI: 10.1038/nature00784 (cited on page 20).

[29] J. Q. You and Franco Nori. 'Atomic physics and quantum optics using superconducting circuits'. In: *Nature* 474.7353 (2011), pp. 589–597. DOI: 10.1038/nature10122 (cited on page 20).

[30] A. Wallraff et al. 'Strong coupling of a single photon to a superconducting qubit using circuit quantum electrodynamics'. In: *Nature* 431.7005 (2004), pp. 162–167. DOI: 10.1038/nature02851 (cited on page 20).

[31] Jonathan A. Jones. 'Quantum computing with NMR'. In: *Progress in Nuclear Magnetic Resonance Spectroscopy* 59.2 (2011), pp. 91–120. DOI: https://doi.org/10.1016/j.pnmrs.2010.11.001 (cited on page 20).

[32] Dawei Lu et al. *NMR quantum information processing*. 2015 (cited on page 20).

[33] Harpreet Singh. *Generation, estimation, and protection of novel quantum states of spin systems*. 2018 (cited on page 20).

[34] C. Westbrook, C.K. Roth, and J. Talbot. *MRI in Practice*. Wiley, 2011 (cited on page 21).

[35] Daniel Gottesman. *An Introduction to Quantum Error Correction and Fault-Tolerant Quantum Computation*. 2009 (cited on page 22).

[36] Aram W. Harrow and Ashley Montanaro. 'Quantum computational supremacy'. In: *Nature* 549.7671 (2017), pp. 203–209. DOI: 10.1038/nature23458 (cited on page 22).

[37] Earl T. Campbell, Barbara M. Terhal, and Christophe Vuillot. 'Roads towards fault-tolerant universal quantum computation'. In: *Nature* 549.7671 (Sept. 2017), pp. 172–179. DOI: 10.1038/nature23460 (cited on page 22).

[38] Ashley Montanaro. 'Quantum algorithms: an overview'. In: *npj Quantum Information* 2.1 (Jan. 2016). DOI: 10.1038/npjqi.2015.23 (cited on page 23).

[39] Aram W. Harrow, Avinatan Hassidim, and Seth Lloyd. 'Quantum Algorithm for Linear Systems of Equations'. In: *Physical Review Letters* 103.15 (Oct. 2009). DOI: 10.1103/physrevlett.103.150502 (cited on page 23).

[40] Jacob Biamonte et al. 'Quantum machine learning'. In: *Nature* 549.7671 (Sept. 2017), pp. 195–202. DOI: 10.1038/nature23474 (cited on page 23).

[41] Carlo Ciliberto et al. 'Quantum machine learning: a classical perspective'. In: *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences* 474.2209 (Jan. 2018), p. 20170551. DOI: 10.1098/rspa.2017.0551 (cited on page 23).

[42] Alejandro Perdomo-Ortiz et al. 'Opportunities and challenges for quantum-assisted machine learning in near-term quantum computers'. In: *Quantum Science and Technology* 3.3 (June 2018), p. 030502. DOI: 10.1088/2058-9565/aab859 (cited on page 23).

[43] Iordanis Kerenidis and Anupam Prakash. *Quantum Recommendation Systems*. 2016 (cited on page 23).

[44] Charles H. Bennett et al. 'Strengths and Weaknesses of Quantum Computing'. In: *SIAM Journal on Computing* 26.5 (1997), pp. 1510–1523. DOI: 10.1137/S0097539796300933 (cited on page 23).

[45] Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi. 'Universal Blind Quantum Computation'. In: *2009 50th Annual IEEE Symposium on Foundations of Computer Science* (Oct. 2009). DOI: 10.1109/focs.2009.36 (cited on page 24).

[46] Alexandru Gheorghiu, Theodoros Kapourniotis, and Elham Kashefi. 'Verification of Quantum Computation: An Overview of Existing Approaches'. In: *Theory of Computing Systems* 63.4 (July 2018), pp. 715–808. DOI: 10.1007/s00224-018-9872-3 (cited on page 24).

[47] Jonathan Olson et al. *Quantum Information and Computation for Chemistry*. 2017 (cited on page 24).

[48] Sam McArdle et al. *Quantum computational chemistry*. 2018 (cited on page 24).

[49] Alexander J. McCaskey et al. *Quantum Chemistry as a Benchmark for Near-Term Quantum Computers*. 2019 (cited on page 24).

[50] Anton Robert et al. *Resource-Efficient Quantum Algorithm for Protein Folding*. 2019 (cited on page 24).

[51] Nick Herbert. 'FLASH—A superluminal communicator based upon a new kind of quantum measurement'. In: *N. Found Phys* 12.12 (1982), pp. 1171–1179. DOI: https://doi.org/10.1007/BF00729622 (cited on page 28).

[52] W. H. Zurek W. K. Wootters. 'A single quantum cannot be cloned'. In: *Nature* 299 (1982), pp. 802–803. DOI: https://doi.org/10.1038/299802a0 (cited on page 28).

[53] D. Dieks. 'Communication by EPR devices'. In: *Physics Letters A* 92.6 (1982), pp. 271–272. DOI: https://doi.org/10.1016/0375-9601(82)90084-6 (cited on page 28).

[54] James L. Park. 'The concept of transition in quantum mechanics'. In: *Foundations of Physics* 1.1 (1970), pp. 23–33. DOI: https://doi.org/10.1007/BF00708652 (cited on page 28).

[55] Stephen Wiesner. 'Conjugate Coding'. In: *SIGACT News* 15.1 (Jan. 1983), pp. 78–88. DOI: 10.1145/1008908.1008920 (cited on page 28).

[56] Artur K. Ekert. 'Quantum cryptography based on Bell's theorem'. In: *Phys. Rev. Lett.* 67 (6 Aug. 1991), pp. 661–663. DOI: 10.1103/PhysRevLett.67.661 (cited on page 29).

[57] Charles H. Bennett, Gilles Brassard, and N. David Mermin. 'Quantum cryptography without Bell's theorem'. In: *Phys. Rev. Lett.* 68 (5 Feb. 1992), pp. 557–559. DOI: 10.1103/PhysRevLett.68.557 (cited on page 29).

[58] Nicolas Sangouard et al. 'Quantum repeaters based on atomic ensembles and linear optics'. In: *Rev. Mod. Phys.* 83.1 (Mar. 2011), pp. 33–80. DOI: 10.1103/RevModPhys.83.33 (cited on page 29).

[59] Stefano Pirandola et al. 'Fundamental limits of repeaterless quantum communications'. In: *Nature Communications* 8.1 (Apr. 2017). DOI: 10.1038/ncomms15043 (cited on page 30).

[60] M. Lucamarini et al. 'Overcoming the rate–distance limit of quantum key distribution without quantum repeaters'. In: *Nature* 557.7705 (May 2018), pp. 400–403. DOI: 10.1038/s41586-018-0066-6 (cited on page 30).

[61] M. Minder et al. 'Experimental quantum key distribution beyond the repeaterless secret key capacity'. In: *Nature Photonics* 13.5 (Mar. 2019), pp. 334–338. DOI: 10.1038/s41566-019-0377-7 (cited on page 30).

[62] Qiang Zhang et al. 'Large scale quantum key distribution: challenges and solutions [Invited]'. In: *Optics Express* 26.18 (Aug. 2018), p. 24260. DOI: 10.1364/oe.26.024260 (cited on page 30).

[63] Dominic Mayers and Andrew Yao. *Quantum Cryptography with Imperfect Apparatus*. 1998 (cited on page 30).

[64] Roger Colbeck. *Quantum And Relativistic Protocols For Secure Multi-Party Computation*. 2009 (cited on page 30).

[65] B. Hensen et al. 'Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres'. In: *Nature* 526 (Oct. 2015), 682 EP - (cited on page 30).

[66] Marissa Giustina et al. 'Significant-Loophole-Free Test of Bell's Theorem with Entangled Photons'. In: *Phys. Rev. Lett.* 115 (25 Dec. 2015), p. 250401. DOI: 10.1103/PhysRevLett.115.250401 (cited on page 30).

[67] Lynden K. Shalm et al. 'Strong Loophole-Free Test of Local Realism'. In: *Phys. Rev. Lett.* 115 (25 Dec. 2015), p. 250402. DOI: 10.1103/PhysRevLett.115.250402 (cited on page 30).

[68] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. 'Measurement-Device-Independent Quantum Key Distribution'. In: *Physical Review Letters* 108.13 (Mar. 2012). DOI: 10.1103/physrevlett.108.130503 (cited on page 30).

[69] Feihu Xu et al. 'Practical aspects of measurement-device-independent quantum key distribution'. In: *New Journal of Physics* 15.11 (Nov. 2013), p. 113007. DOI: 10.1088/1367-2630/15/11/113007 (cited on page 30).

[70] Kyo Inoue, Edo Waks, and Yoshihisa Yamamoto. 'Differential Phase Shift Quantum Key Distribution'. In: *Phys. Rev. Lett.* 89 (3 June 2002), p. 037902. DOI: 10.1103/PhysRevLett.89.037902 (cited on page 30).

[71] K. Inoue, E. Waks, and Y. Yamamoto. 'Differential-phase-shift quantum key distribution using coherent light'. In: *Phys. Rev. A* 68 (2 Aug. 2003), p. 022317. DOI: 10.1103/PhysRevA.68.022317 (cited on page 30).

[72] Damien Stucki et al. 'Fast and simple one-way quantum key distribution'. In: *Applied Physics Letters* 87.19 (2005), p. 194108. DOI: 10.1063/1.2126792 (cited on page 30).

[73] Won-Young Hwang. 'Quantum Key Distribution with High Loss: Toward Global Secure Communication'. In: *Physical Review Letters* 91.5 (Aug. 2003). DOI: 10.1103/physrevlett.91.057901 (cited on page 31).

[74] S. Pirandola et al. *Advances in Quantum Cryptography*. 2019 (cited on page 31).

[75] Feihu Xu et al. *Quantum cryptography with realistic devices*. 2019 (cited on page 31).

[76] Eleni Diamanti and Anthony Leverrier. 'Distributing Secret Keys with Quantum Continuous Variables: Principle, Security and Implementations'. In: *Entropy* 17.9 (2015), pp. 6072–6092. DOI: 10.3390/e17096072 (cited on page 31).

[77] P. Sibson et al. 'Chip-based quantum key distribution'. In: *Nature Communications* 8.1 (2017), p. 13984. DOI: 10.1038/ncomms13984 (cited on page 31).

[78] Mauro Persechino et al. 'Correlations with on-chip detection and modulation for CVQKD (poster)'. In: *QCrypt 2017*. Cambridge, United Kingdom, Sept. 2017 (cited on page 31).

[79] G. Zhang et al. 'An integrated silicon photonic chip platform for continuous-variable quantum key distribution'. In: *Nature Photonics* (2019). DOI: 10.1038/s41566-019-0504-5 (cited on page 31).