ALMA MATER STUDIORUM - UNIVERSITÀ DI BOLOGNA
CAMPUS DI CESENA

Scuola di Ingegneria
Corso di Laurea Magistrale in
Ingegneria Elettronica e Telecomunicazioni per l'Energia

# Analysis of multi-hop Teleportation Protocols for Quantum Networks

*Tesi di Laurea Magistrale in*
Teoria dell'Informazione e Crittografia LM

*Relatore*
Chiar.mo Prof. Marco Chiani
*Correlatore*
Prof. Enrico Paolini

*Presentata da*
Silvia Avveduti

Anno Accademico 2018-2019

# Contents

# Chapter 1

# Introduction

Quantum mechanics for computation and information purposes has seen a burst of interest in the scientific community and companies, due to the potential unique computational power offered by quantum computers, not achievable through classical computers. In particular two technologies are used in most quantum computers, which are the trapped ions and artificial atoms, but many different technologies are currently being studied for the physical implementation of quantum information systems [1]. Quantum computers are challenging to build, because the element which represents information, the *qubit*, requires strict conditions such as isolation from the environment and a very refined control. Moreover, qubits cannot intrinsically reject noise as classical bits do.

In 2019 Google's Quantum AI Lab confirmed the Quantum Supremacy over classical computation, using the 53 qubit Sycamore quantum chip [2] and in the beginning of 2020 IBM announced a Quantum Volume (the metric IBM defined to measure the performance of a quantum computer) of 32, leading the way to Quantum Advantage [3].

The aim of this thesis is to investigate the basic components and protocols to build a Quantum Network by using fundamental elements of quantum mechanics, such as quantum teleportation and entanglement swapping. Also, we perform an experimental validation of the quantum circuits, which will be at the basis of the Quantum Internet, through the platform IBM Quantum Experience [4].

This thesis is organized as follows.
In Chapter 2 the essential concepts for Quantum Computation and Information are introduced; in Chapter 3 an overview of the main applications is displayed; in Chapter 4 the current results in entanglement and teleportation in Quantum Network protocols are shown. The experimental outcomes obtained in IBM Q are discussed in Chapter 5. Finally, Chapter 6 contains the conclusions.

# Chapter 2

# Quantum Computation and Information

With the purpose of studying quantum networks, the fundamental notions of quantum mechanics and the basic elements needed to perform quantum computation are discussed in this chapter, which is largely based on [5].

## 2.1 Quantum bits

At the basis of quantum applications there is the concept of *qubit* as an equivalent of the *bit* in the classic case. It is a mathematical object that finds physical realization in particular two-level systems (two-level quantum systems). As we know, while the status of a bit may assume the value 0 or 1, two possibilities provided for the qubit can be $|0\rangle$ and $|1\rangle$, with the fundamental difference that in general a qubit can be in a linear combination of these states, called superposition (continuum between 0 and 1 state). The generic quantum state, with computational basis $|0\rangle$ and $|1\rangle$, can therefore be written in the following form:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{2.1}$$

with $\alpha$ and $\beta$ complex numbers and $|0\rangle$ and $|1\rangle$ the basis vectors for the vector space. The orthonormality of the vectors makes it possible to physically distinguish the observables after the measurement procedure, the result of which will be the eigenvalue 1 corresponding to the eigenvector $|0\rangle$ with probability $|\alpha|^2$ or $-1$ corresponding to the eigenvector $|1\rangle$ with probability $|\beta|^2$. The sum of the probabilities associated with the possible outputs of the experiment will be equal to 1, by definition of probability itself:

$$|\alpha|^2 + |\beta|^2 = 1 \tag{2.2}$$

The choice of the system corresponding to the qubit must take into account its usability over time, i.e., the system has to maintain its quantum properties unaltered for as long as possible, so that the state can be processed before it is corrupt. In fact, we speak of decoherence time as the time that elapses before interactions with the environment damage the desired state of the qubit. These interactions are modeled as a noisy process, the quantum noise. In particular, systems whose states have a symmetrical description, for example a spin 1/2 particle, which lives in the space of states $|up\rangle$ and $|down\rangle$ will be preferred for the purpose of computation, and in this case they have characteristics of ideality if the system is isolated, in addition to the fact that the space of states is clearly finite (Hilbert space with finite size 2). A bad example of a system for realizing a qubit is instead offered by the position $x$ of a particle along one direction, as it is unrealistic for computational purposes to think of associating information with a continuous set of states, in addition to the fact that the presence of noise will make the number of states infinite. Good examples of physical systems that realize a qubit may be the two different polarizations of a photon, the alignment of a spin in a uniform magnetic field, the two states of an electron orbiting an atom.

For a closed quantum system, evolution over time is known to be determined by its Hamiltonian. Thus, for computational purposes it will be necessary to control the Hamiltonian in a way to evolve over time in the desired manner, according to a unitary transformation.

Returning to the mathematical description of the qubit, it is effectively represented in a geometric way through the so-called *Bloch's sphere.* By exploiting Equation 2.2 of normalization, we can rewrite the state expressed in Equation 2.1 as

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right) \tag{2.3}$$

with $\theta$, $\varphi$ and $\gamma$ real numbers. Furthermore, the same equation can be simply rewritten as it follows:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle \tag{2.4}$$

so it is possible to ignore the *global phase factor* $e^{i\gamma}$ which, since probabilities are related to modulus square, does not affect the measurement of the observable as $|e^{i\gamma}|$=1. Ultimately the real numbers $\theta$ and $\varphi$ define a point in the so called *Bloch's sphere*:

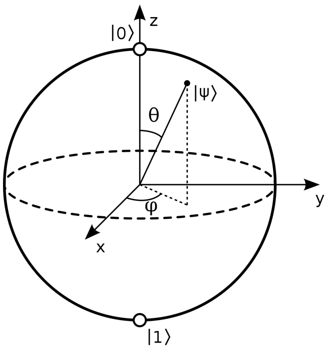


Figure 2.1: Bloch sphere representation of a quantum bit [6]

The possible states of a qubit are therefore all the possible infinite points of this sphere of unit radius. However, once the measurement is complete, only the value −1 or 1 can be obtained, therefore the continuum of states will be lost following the collapse of the state. The potential of quantum information is therefore all enclosed in the *hidden information* that occurs if the measurement is not performed on the qubit.

## 2.2 Single and multiple qubit gates

Quantum computation is based on quantum circuits. They are made up of wires, able to convey information, and quantum gates to manipulate information (quantum states).

### 2.2.1 Single qubit gates

Let $|\psi\rangle$ be a single qubit, described by two complex numbers $\alpha$ and $\beta$, hence represented as $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where the vectors of the computational basis are chosen as follows:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

The operations on the single qubit are represented by 2×2 matrices, with the only constraint of *unitarity*, which means that given an operation $\mathbf{U}$ that describes the gate behavior, then the relation $\mathbf{U}^\dagger\mathbf{U} = \mathbf{I}$ must hold.
The simplest operation that can be defined is the bit-flip, that is the quantum analogue of the classic NOT. This is represented by the matrix $\mathbf{X}$:

$$\mathbf{X} \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

The quantum NOT, applied to one qubit $\alpha|0\rangle + \beta|1\rangle$, turns it into $\alpha|1\rangle + \beta|0\rangle$, so it acts linearly on the state with a rotation of $\pi$ around the $X$ axis in the Bloch sphere.

Another important operation is represented by the gate $\mathbf{Z}$. It keeps the state $|0\rangle$ unchanged and instead it changes the sign of the state $|1\rangle$. It is therefore also called phase-flip operator, in which the phase undergoes a rotation of $\pi$. The matrix that describes it is the following one:

$$\mathbf{Z} \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Given the qubit $\alpha|0\rangle + \beta|1\rangle$, the $\mathbf{Z}$ will change it into the state $\alpha|0\rangle - \beta|1\rangle$.

Furthermore, a qubit can experiment both a bit-flip and a phase-flip, according to the transformation given by the gate $\mathbf{Y}$, represented by the following matrix:

$$\mathbf{Y} \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

In this case, the states $|0\rangle$ and $|1\rangle$ are mapped into $|1\rangle$ and $-i|0\rangle$ respectively, with an operation that is equivalent to a rotation of $\pi$ around the $Y$ axis of the Bloch sphere.

More generally, a qubit can undergo a phase variation dictated by the following matrix:

$$\mathbf{S} \equiv \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

The operator $\mathbf{S}$ is called *phase gate.*

$\mathbf{X}$, $\mathbf{Y}$ and $\mathbf{Z}$ are called Pauli matrices and their combination gives rise to three new matrices, called "rotation operators" with respect to the $X$, $Y$ and $Z$ axis, defined as it follows:

$$\mathbf{R}_x(\theta) \equiv e^{-i\theta\mathbf{X}/2} \tag{2.5}$$

$$\mathbf{R}_y(\theta) \equiv e^{-i\theta\mathbf{Y}/2} \tag{2.6}$$

$$\mathbf{R}_z(\theta) \equiv e^{-i\theta\mathbf{Z}/2} \tag{2.7}$$

Among the gates that act on a single qubit there is also the *Hadamard* gate, described by the following matrix:

$$\mathbf{H} \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

The operator $\mathbf{H}$ turns the state $|0\rangle$ into an intermediate state $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and the state $|1\rangle$ into $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$.

### 2.2.2 Multiple qubit gates

Let's consider a system made of two qubits. The computational basis is therefore formed by the four vector basis $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$. The quantum state describing the two qubits is:

$$|\psi\rangle = \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle \tag{2.8}$$

with $\alpha_{00}$, $\alpha_{01}$, $\alpha_{10}$ and $\alpha_{11}$ complex numbers.
The vector basis formerly considered are obtained through the Kronecker product of the respective vector basis in two-dimensions $|0\rangle$ and $|1\rangle$, as it follows:

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{bmatrix}1\\0\\0\\0\end{bmatrix} \quad ; \quad |01\rangle = |0\rangle \otimes |1\rangle = \begin{bmatrix}0\\1\\0\\0\end{bmatrix}$$

$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{bmatrix}0\\0\\1\\0\end{bmatrix} \quad ; \quad |11\rangle = |1\rangle \otimes |1\rangle = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}$$

One important example of gates with two input bits is the *controlled*-NOT, or more simply $CNOT$, which takes as input a qubit called "control qubit" and a second input called "target qubit". It acts in the following way: if the first qubit (control) is equal to $|0\rangle$, then the second qubit (target) remains unchanged, otherwise if the first qubit is $|1\rangle$, the second qubit is flipped (negation), hence the meaning of the gate's name. The transformations are shown below:

$$\begin{aligned}
|00\rangle &\to |00\rangle \\
|01\rangle &\to |01\rangle \\
|10\rangle &\to |11\rangle \\
|11\rangle &\to |10\rangle \ .
\end{aligned}$$

The $CNOT$ matrix representation is:

$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{2.9}$$

where the first column represents the transformation undergone by the vector $|00\rangle$, the second column the one undergone by $|01\rangle$ and similarly for the remaining respective columns and basis vectors.

## 2.3 Bell states

Supposing we want to describe the states of a composite system, consisting of two or more physical systems (qubits). The space-state of the composite system is built up from the state-space of the component systems, which means that if we have $n+1$ systems and the system number $i$ is prepared in the state $|\psi_i\rangle$, than the joint state of the total system is the tensor product $|\psi_1\rangle \otimes |\psi_2\rangle \otimes ... \otimes |\psi_n\rangle$.

However, there are states that describe composite systems that cannot be traced back to the tensor product of individual states: in this case it is said to be dealing with an *entangled* state. If we consider a two qubit system, it is equivalent to say that a state $|\psi\rangle$ is entangled if there are no single qubit states $|a\rangle$ and $|b\rangle$ such that $|\psi\rangle = |a\rangle|b\rangle$.

Among all possible two-level states we find the Bell states, fundamental for quantum information, also called EPR pairs (Einstein-Podolsky-Rosen)[7]. Bell states are listed below:

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{2.10}$$

$$|\Phi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \tag{2.11}$$

$$|\Psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}} \tag{2.12}$$

$$|\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \tag{2.13}$$

Bell states are four two-qubit states with the characteristic that the two qubit measurements are closely related in a quantum way and in particular they are maximally entangled quantum states. This means that by independently measuring the two qubits of the pair, a distribution of 0 and 1 is obtained with equal probability, but it is found that the two outputs of the experiment are linked together, based on the type of EPR state. For example for the state $|\Phi^+\rangle$, if the measurement of the first of the two qubits is equal to 0, then the same result will be obtained with certainty by measuring the second qubit. The measurement on the first qubit then determines one of the two possible values for the measurement of the second qubit, 0 or 1, depending on the type of Bell state considered.

To generate the state $|\Phi^+\rangle$ the *Hadamard* gate and the controlled-NOT gate con be used, by placing the computational basis $|0\rangle$ in both input lines. After the **H** operator, the state $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ is produced on the first line, which will act as *control qubit* for the state $|0\rangle$ on the second line.

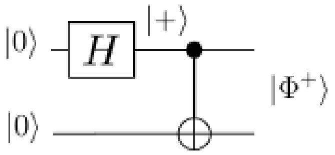


Figure 2.2: Circuit for the Bell state $|\Phi^+\rangle$ generation

To get the state $|\Phi^-\rangle$, we use as inputs $|1\rangle$ and $|0\rangle$, to obtain $|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ after the **H** gate on the first line of the circuit, which will act on the second qubit to give $\frac{|00\rangle - |11\rangle}{\sqrt{2}}$.

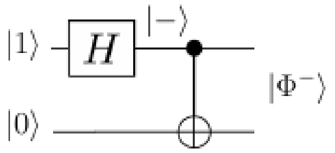


Figure 2.3: Circuit for the Bell state $|\Phi^-\rangle$ generation

The state $|\Psi^+\rangle$ is obtained by placing the qubits $|0\rangle$ and $|1\rangle$ in input, to obtain through the **H** gate the state $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$, which will act as the control qubit, to finally give the state $\frac{|01\rangle - |10\rangle}{\sqrt{2}}$.

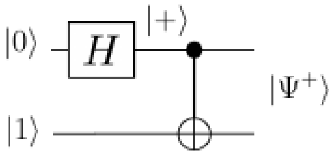


Figure 2.4: Circuit for the Bell state $|\Psi^+\rangle$ generation

Lastly, the $|\Psi^-\rangle$ state is found by imposing the qubits $|1\rangle$ and $|1\rangle$ in input, to obtain $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$ on the first line through the *Hadamard* gate, hence $\frac{|01\rangle - |10\rangle}{\sqrt{2}}$ is the final state.

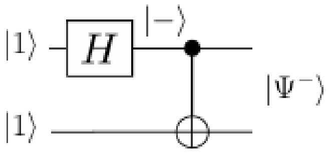


Figure 2.5: Circuit for the Bell state $|\Psi^-\rangle$ generation

## 2.4 Quantum Teleportation

Quantum Teleportation is a technique for transferring a quantum state, without an effective transmission of the particle with which the state is associated. Let Alice and Bob be the sender and receiver of a $|\psi\rangle$ state and imagine that they somehow generated an entangled pair they share. Alice wants to transfer the qubit to Bob not knowing the state and can send information to Bob only through a classic channel, moreover Alice cannot describe to Bob the state to be send because knowing it would mean having multiple copies of the state itself, forbidden by the no-cloning theorem, for which it turns out to be impossible to make a copy of an unknown quantum state, and in any case an infinite amount of classical information would be needed, as its description concerns a continuous space of values. So to send the qubit to Bob, Alice needs to make the state to be teleported interact with her half of the EPR pair.

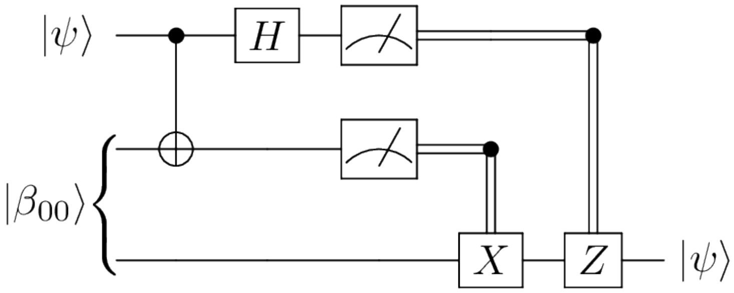


Figure 2.6: Quantum Teleportation circuit

As shown in Figure 2.6 Alice has the qubit $|\psi\rangle = \alpha|0\rangle{+}\beta|1\rangle$ to transmit and also has half of the EPR pair (the status $|\Phi^+\rangle$ is here considered), while the second half of the entangled pair belongs to Bob. In this way the initial state is described as

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}\Big[\alpha\,|0\rangle\,\Big(\,|00\rangle + |11\rangle\,\Big) + \beta\,|1\rangle\,\Big(\,|00\rangle + |11\rangle\,\Big)\Big] \tag{2.14}$$

considering the first two qubits as the Alice's ones, and the third qubit that of Bob's. Therefore Alice performs a $CNOT$ operation on her two qubits, so the state changes into

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\Big[\alpha\,|0\rangle\,\Big(\,|00\rangle + |11\rangle\,\Big) + \beta\,|1\rangle\,\Big(\,|10\rangle + |01\rangle\,\Big)\Big]. \tag{2.15}$$

Subsequently Alice applies the *Hadamard* gate on the first qubit, obtaining the quantum state below:

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}\left[\alpha\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)(|00\rangle + |11\rangle) + \beta\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)(|10\rangle + |01\rangle)\right]. \tag{2.16}$$

Rearranging the terms and regrouping them to put in evidence Alice's qubits, we obtain:

$$\begin{aligned} |\psi_2\rangle = \frac{1}{2}\Big[\,&|00\rangle\Big(\alpha\,|0\rangle + \beta\,|1\rangle\Big) \;+\; |01\rangle\Big(\alpha\,|1\rangle + \beta\,|0\rangle\Big) \\ &+\; |10\rangle\Big(\alpha\,|0\rangle - \beta\,|1\rangle\Big) \;+\; |11\rangle\Big(\alpha\,|1\rangle - \beta\,|0\rangle\Big)\Big]. \end{aligned} \tag{2.17}$$

Alice then measures her two qubits and sends the classical result (one of the four possibilities) to Bob, who will be able to recover the teleported state. In fact, if the outcome is 00, Bob's system will be in the state $|\psi\rangle = \alpha|0\rangle{+}\beta|1\rangle$ and in this case he will not intervene with any correction. If instead the measurements turns out to be 01, Bob will be in the state $\alpha|1\rangle{+}\beta|0\rangle$, so the $CNOT$ will be activated to correct the error bit-flip, to get $|\psi\rangle$. With outcome equal to 10 Bob will apply the phase-flip via controlled-Z because in this case his state is equal to $\alpha|0\rangle{-}\beta|1\rangle$. Finally, if Alice measures 11, then Bob is in the state $\alpha|1\rangle - \beta|0\rangle$: the $CNOT$ and controlled-Z operation will then restore the correct state by fixing the bit-flip and phase-flip error. The teleportation of a qubit doesn't imply that the information is transmitted instantly at a speed higher than the light's one, since in order to work it requires a classical communication channel which puts constraint in speed. It also does not violate the no-cloning theorem of qubits, because only the final state is maintained in the state $|\psi\rangle$, while the initial state is "lost": after reading Alice's qubits this state is inevitably collapsed in the basis $|0\rangle$ or $|1\rangle$, thus losing its original description.

# Chapter 3

# Applications

The main quantum network applications are discussed in this chapter, largely based on [5][8]. Quantum Information is currently a hot topic as it promises to solve classically unsolved problems, such as the factorization of non-trivial integers, through the use of Quantum Computers. The interest generated around these technologies, however, endangers the current cryptography systems, in particular the threat to the Rivest-Shamir-Adleman (RSA) algorithm becomes concrete. Moreover, nowadays the eavesdroppers may intercept cryptograms that they may be able to decrypt in the future, which means that the confidentiality of the message may have a very limited lifespan.

The tools offered by quantum mechanics, based on the unbreakable principles of nature, such as the uncertainty principle or entanglement, are well suited for tasks that require coordination, synchronization and privacy. In particular the applications made possible by a Quantum Network - a set of connected quantum nodes - are, among many, the efficient implementation of the Quantum Key Distribution (QKD) with long-distance high key rate, synchronization, protocols for distributed systems, position verification and secure identification.

## 3.1 Quantum Key Distribution

Quantum computers can be used to break some of the best public key cryptosystems such as the RSA. This is achievable due to the possibility to solve the *order-finding problem* and the *factoring problem* in an efficient way, that are the two methods by which one might hope to break the RSA with a quantum computer, while no efficient methods are currently known for classical computers.

On the other hand, a procedure called *quantum key distribution* exploits the fundamental principles of quantum mechanics to enable provably secure distribution of private information, conditioned only by fundamental laws of physics. Quantum key distribution (QKD) is a provably secure protocol, by which private key bits can be generated between two parties over a public channel. These key bits can be used in a classical private key cryptosystem to enable the two parties to communicate securely. The only constraint for the QKD protocol is that the error rate with which qubits can be communicated over the public channel must be lower than a certain threshold. The basic idea behind the protocol is that Eve cannot gain any information from the qubits transmitted from Alice to Bob without disturbing their state. First, Eve cannot clone Alice's qubit, thanks to the no-cloning theorem. Second, *information gain implies disturbance*: in any attempt to distinguish between two non-orthogonal quantum states adopted in the protocol, information gain is only possible at the expense of introducing disturbance to the signal. Using the idea of transmitting non-orthogonal qubit states between Alice and Bob, by checking for disturbance in their transmitted qubit, they establish an upper bound to any eavesdropping occurring in their communication channel. So these "check" qubits are interspersed randomly among data qubits, from which the key bits are later extracted. Subsequently Alice and Bob perform information reconciliation and privacy amplification to distill a secret key.

### 3.1.1 BB84 Protocol

One of the QKD protocols is the *BB84 protocol.* The purpose of the $BB84$ is to send the private key from Alice to Bob using a "prepare-and-measure" protocol, where Alice prepares the optical signals by encoding on them a discrete random variable, such as a bit. The optical signals are then sent to the receiving user Bob, who measures them in order to retrieve the information sent by Alice. At the beginning Alice generates a random string $b$ of vector basis not mutually orthogonal and a random sequence of data bits $a$ of the same length $n$.

Alice encodes the data bits as $\{|0\rangle,|1\rangle\}$ (**Z** basis) if the corresponding bit $b$ is 0, or $\{|+\rangle,|-\rangle\}$ (**X** basis) if $b$ is 1, obtaining the following product vector state:

$$|\psi\rangle = \bigotimes_{i=1}^{n} |\psi_{a_i b_i}\rangle \tag{3.1}$$

where each qubit is one of the four non-orthogonal states

$$\begin{aligned} |\psi_{00}\rangle &= |0\rangle\,, \\ |\psi_{10}\rangle &= |1\rangle\,, \\ |\psi_{01}\rangle &= |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \\ |\psi_{11}\rangle &= |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \end{aligned} \tag{3.2}$$

Then Alice sends the two encoded strings as the $|\psi\rangle$ state to Bob over a public quantum channel, and Bob chooses a random string $b'$ of vector bases. Then he performs a measurement of each qubit in these bases. Since only Alice knows $b$, it is impossible for either Bob or the eavesdropping Eve to distinguish the states of the qubits. This means that if Alice and Bob vector basis are not the same for the measurement of a qubit, then the outcome of the experiment for Bob will be 0 or 1 with probability one half. The state received by Bob contains noise in the channel and the possible presence of Eve and, after Bob has received the state $|\psi\rangle$, Eve cannot be in possession of

a copy of the states, by the no-cloning theorem. Moreover if Eve measures the received qubits, the risk of disturbing a qubit is concrete, with probability one half, if she guesses the wrong basis.
More precisely, Bob chooses his basis string $b'$ of the same length of $b$ and then measures the qubits received by Alice, $a'$. Bob announces publicly that he has received the qubits from Alice. Alice then tells which measurements to keep, by publicly announcing $b$. Through a public channel Alice and Bob keep only the bits where they both had the same basis, then Alice selects randomly one half of these qubits and announce it through the public channel. Both Alice and Bob announce and compare the values of the check-bits. If more than an acceptable number disagree, then the operation is canceled due to a possible attack by an eavesdropper and started again. Otherwise Alice and Bob proceed to use the information reconciliation and privacy amplification on the remaining qubits to obtain the secret key.

An example could be the following. Given the two non-orthogonal basis "+" and "×", Alice chooses the basis string $b$ and the bit string $a$ as

$$\begin{array}{l ccccccc} b: & + & + & \times & + & \times & \times & + \\ a: & 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{array}$$

Bob generates his basis string $b'$ randomly, then performs the measurement on the received qubits. If the bases agree the result is correct, otherwise it is 0 or 1 with probability 1/2.

$$\begin{array}{l ccccccc} b': & \times & + & \times & \times & + & \times & + \\ a': & 1/0 & {\color{blue}0} & {\color{blue}1} & 1/0 & 1/0 & {\color{blue}0} & {\color{blue}1} \end{array}$$

After the comparison between Alice and Bob basis, only the bits with the same Alice and Bob basis are kept (in blue). Then, half of them are chosen by Alice to be verified as a valid subset of the entire key to detect the possible interference by an attacker.

## 3.2 Satellite Quantum Communications

Proposals of the extension to space of quantum communications (QC) were supported by the long distance free-space QC experiments on the ground. In this way it was proved that significant portions of the atmosphere were suited not only for classical communications but also for the quantum ones. However the single photon discrimination at the correct wavelength, arrival time and the detection cutting out the background noise is much more demanding than the classical counterpart. The exchange of a single photon between a Low-Earth-orbit (LEO, 160-2000 km in altitude) satellite and the ground has been demonstrated exploiting satellites without active photon source in orbit, using optical retroflectors, starting in 2003 with an experimental campaign at the Matera Laser Ranging Observatory (Italy)[9]. In this case, even without an active photon source in orbit, the demonstration was obtained by directing to the satellites a train of pulses with energy such that the retroflected portion collected on the Earth is a coherent state associated to a single photon or less. This space QC is a candidate for a global Quantum Key Distribution and was considered since the beginning as an effective solution to join separated networks of fiber ground links, and also allows the key exchange between satellite and two ground terminals to generate a secure key via one-time pad between the two terminals. The interest in the realization of a satellite for QKD purpose flared up in Asia, in particular the Japanese SOTA satellite was launched in 2014 and the Chinese Micius in 2015. Moreover, the interest in using very compact payloads as nanosat or cubesat has recently grown in Europe [10].

The QKD rate, considering space links, is based on the analysis of the losses and fluctuations of the corresponding optical channel, where orbit altitude has relevant implications in the losses of the optical link and the impact of the atmosphere is asymmetric (the downlink is different from the uplink). The Low-Earth-orbit was the first choice to demonstrate the quantum communication protocols from space, and it was the first considered for the QKD. The $BB84$ protocol on a space link feasibility has been proved experimentally after the first source of single photons has been implemented in Ajisai, a LEO sat for geodynamic studies, using its corner-cube retroreflectors with the illuminating train of pulses from the Matera Laser Ranging Observatory, Italy, in a way that a single photon was reflected on average by the satellite.

With the aim of experimentally verifying QC protocols in space, the Chinese satellite Micius was announced as a major step in the Chinese Academy of Science space program and was launched in 2016. The spacecraft was equipped as a quantum optic lab capable not only to generate-transmit coherent and entangled states, but also to measure qubit sent by the ground device. Entangled-based QKD was also demonstrated by Micius, using a high visibility source onboard. Micius was also used for demonstrating an intercontinental quantum network, distributing the keys for a text and video exchange between the ground stations of Xinglong (China), Nanshan (China) and Graz (Austria) [11]. Beyond satellite-QKD [12], about test of quantum mechanics in space, the Chinese satellite allowed the demonstration of the persistence of entanglement at the record distance of 1200 km between the two ground stations of Delingha and Lijiang in China [13]. An intense activity is currently pursued to apply QKD via satellite, with several experiments and studies [14][15].

# Chapter 4

# Quantum Networks

A quantum network is made up of remote nodes that aim to communicate through the main tools offered by quantum mechanics, whose properties allow us to overcome the limits of communication in the classical sense. Although it is currently difficult to predict all future uses of a Quantum Internet [16][17], many applications of interest have already been identified, ranging from cryptography to sensing and metrology, to distributed systems [18]. In particular, the Quantum Internet allows to "transmit" qubits from one remote node to another or to extend an entangled state to multiple nodes of the network, with no classical equivalent. As previously seen, the qubits are deeply different from the classic bits, since a qubit can be in a superposition of states, so if $n$ classic bits can be only in one of the possible combinations of them, a system of $n$ qubits can be in a superposition of all $2^n$ possible states [19].

## 4.1 Quantum Teleportation for Quantum Networks

The simplest way to communicate a qubit to a remote node may seem at first to transmit it directly through an optical connection, after having mapped, for example, the qubit itself to a degree of freedom of a photon. Unfortunately, this solution is not realizable if network reliability is needed because, if the photon is corrupted, all the information is completely lost, and it is not possible to keep a copy of an unknown qubit. Therefore the direct route is not preferable unless the type of application can tolerate a low success rate, as happens in networks for the distribution of keys (QKD). The mode of transmission of qubits then uses the quantum teleportation technique [19], through which there is no real transfer of the particle involving the qubit. As explained in Chapter 2, this tool enables to transfer a quantum state without the presence of a quantum communication channel between source and destination, while needing two resources such as an entangled pair to share between source and destination and a classical channel between them for the exchange of two bits. Clearly one EPR pair is consumed following the measurement on the qubits of the source and, for this reason, for a new qubit to be sent, a new entangled pair must be made available. The generation of the entanglement between pairs of nodes is therefore the first problem to be addressed.

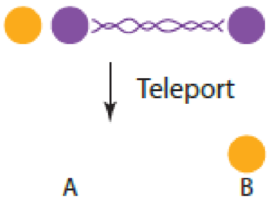


Figure 4.1: Teleportation of a qubit from node A to B, consuming the entangled pair [18]

## 4.2 Entanglement generation

To generate entanglement between two or more particles it is necessary that they are at first located close to each other in space. Three different ways to generate and distribute entanglement between source and destination can be described, which differ from each other depending on where the entanglement is generated. Referring to [19], we speak of entanglement generation *"at mid-point"*, *"at the source"* and *"at both end-points"*.

### 4.2.1 Schemes for entanglement generation and distribution

The first solution is shown in Figure 4.2.

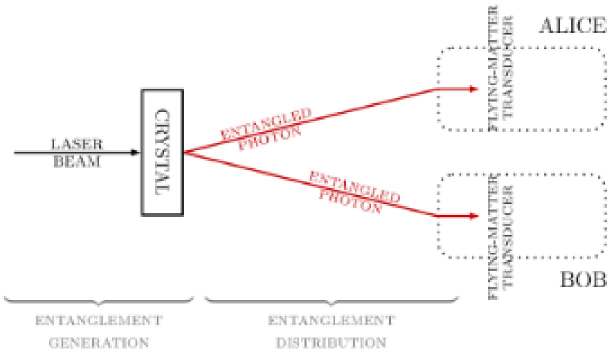


Figure 4.2: Spontaneous Parametric Down-Conversion [19]

This first method, called Spontaneous Parametric Down-Conversion [20], uses photons for both the generation of the entanglement and for its distribution and maps the entanglement using the polarization of photons. In fact, even if in principle any degree of freedom can be exploited for entanglement, polarization is usually simpler to use in practice, since very efficient polarization-control elements are available.

As it can be seen in Figure 4.3, pointing a laser beam directed towards a non-linear crystal (BBO, beta-barium borate), without the use of extra beam splitters or mirrors, the two down-converted photons are emitted in two cones, one "ordinary polarized", the other "extraordinary polarized".

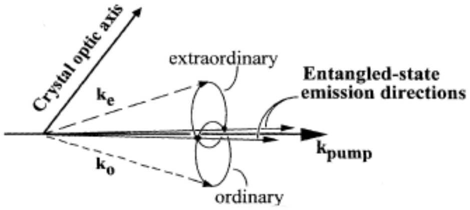


Figure 4.3: Spontaneous down-conversion cones (type-II phase matching) [20]

If the optical axis of the crystal and the pump beam axis are collinear, the two cones are tangent to each other. If this angle decreases, then the two cones gradually move away from each other. Finally, if the angle increases, the two cones will intersect in two points. In the directions that intercept these points, where the two cones overlap, the light can be described with an entangled state, that depends on the horizontal (extraordinary) and vertical (ordinary) polarizations:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\Big( |H_1, V_2\rangle + e^{i\alpha} |V_1, H_2\rangle \Big) \tag{4.1}$$

By exploiting optical phenomena it is possible to generate EPR-pairs based on this polarization-entanglement:

$$|\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}\Big( |H_1, V_2\rangle \pm |V_1, H_2\rangle \Big)$$

$$|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}\Big( |H_1, H_2\rangle \pm |V_1, V_2\rangle \Big) \tag{4.2}$$

Looking at Figure 4.2, the two entangled photons travel through a quantum channel to finally reach Alice and Bob, in which there is a transducer that maps the entanglement associated with the photons (also called *flying qubit*) to the *matter qubit*, which will act as a memory or will be immediately processed. Note that choosing to use photons as *flying qubits* is due to their advantages as entanglement carriers, presenting a moderate decoherence interacting with the environment and being easily controlled by optical components as previously mentioned.

A second way of generating and distributing entanglement is "at the source". As it can be seen in Figure 4.4 this scheme uses atoms in optical cavities connected together by optical fiber. At first, through a laser pulse, the atom coupled with the cavity is excited, producing the emission of a photon. The polarization of this photon is entangled with the atom of the cavity itself and, traveling through the fiber, reaches the second optical cavity, where it is absorbed. The atom-photon entanglement is then converted into atom-atom entanglement. According to this scheme, the cavity behaves like a transducer from flying qubit to matter qubit as seen previously.

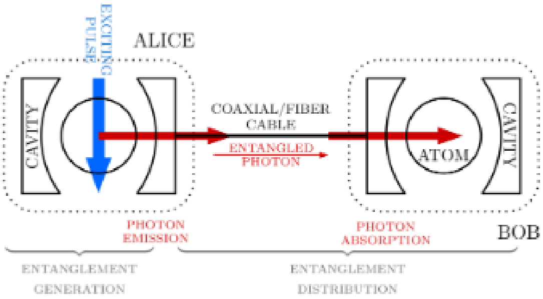


Figure 4.4: Entanglement generation "at the source" [19]

Lastly the third scheme, shown below in Figure 4.5, presents the entanglement generation in both cavities, hence this method is called "at both end-points".

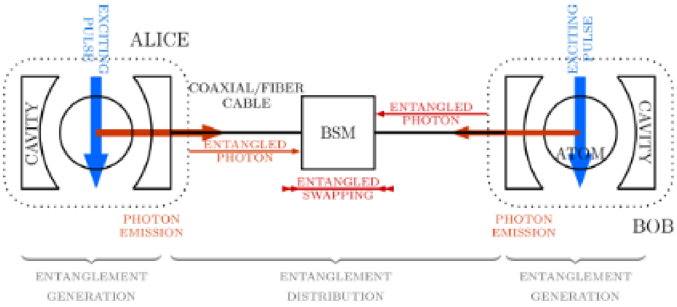


Figure 4.5: Entanglement generation "at both end-points" [19]

In this case both atoms are simultaneously excited by a laser pulse, therefore a photon is emitted in both cavities. The two photons arrive by fiber to a unit that measures according to the Bell basis, thus projecting the atom-photon entanglement on both atoms of the cavity (atom-atom entanglement). In particular referring to [18], this scheme was used in the context of the Nitrogen-Vacancy (NV) centers in diamond quantum processor: the key capabilities of this platform are those of having a lifetime qubit of 1.46 s, an entanglement produced faster than it is lost, and finally the possibility to use entanglement for teleporting qubits between separate NV centers.

### 4.2.2 Heralded Entanglement

At present, short-lived entanglement has been produced probabilistically over short distances ($\approx$ 100 km) on the ground by sending photons over standard telecom fiber, as well as from space over 1203 km from a satellite [13]. However, these systems do not allow the concatenation of themselves with the aim of transmitting the qubits over long distances. With reference to the latest generation and distribution scheme of entanglement, if long-distance quantum communication is to be established, a long-lived entanglement must be produced between two nodes that are capable of storing and manipulating qubits. To do this efficiently, *heralded* entanglement generation is implemented, using a heralding signal that announces the success of the attempt to generate the entanglement itself. This heralded entanglement allows long-distance quantum communication without additional resources to use.

Figure 4.6 shows how NV centers are point defects in diamond with an electronic spin as a communication qubit (purple) and carbon-13 nuclear spins as memory qubits (yellow). The attempt to generate the entanglement occurs following a trigger event that produces the entanglement between the communication qubit of A (diamonds) and the qubit (photon) emitted thanks to the trigger. This entanglement is generated in the same way in the two nodes A and B. The photon is then transferred to the heralding station by optical fiber. Subsequently, the heralding station interferes with both incoming photons on a beam splitter, performing a probabilistic so-called *entanglement swap*, that is a measurement of the incoming qubits in the Bell basis, where we can only obtain outcomes $|\Psi^+\rangle$, $|\Psi^-\rangle$ or "other" (which means failure). The heralding station measures the incoming photons by observing clicks in the left or right detector giving the heralding signal $s$, with unsuccessful result (none of both click), success with $|\Psi^+\rangle$ (left click) or success with $|\psi^-\rangle$ (right click):

$$\begin{aligned} |\Psi^+\rangle &= \frac{1}{\sqrt{2}}\Big( |0_A\rangle |1_B\rangle + |1_A\rangle |0_B\rangle \Big) \\ |\Psi^-\rangle &= \frac{1}{\sqrt{2}}\Big( |0_A\rangle |1_B\rangle - |1_A\rangle |0_B\rangle \Big) \end{aligned} \tag{4.3}$$

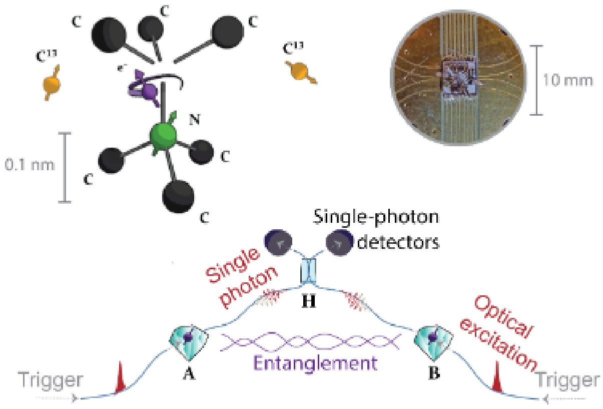


Figure 4.6: Heralded entanglement generation on the NV platform [18]

## 4.3 Long-distance communications through Entanglement Swap: repeater nodes

Once the entanglement is generated and distributed between pairs of nodes, long-distance entanglement from shorter segments can be created. The simplest case consists of three nodes, as shown in Figure 4.7, in which there is an entanglement between the nodes A and B, similarly for the pair B and C. The central node B realizes the task of extending the entanglement, to make node A and node C share the entangled pair. Node B, also called *repeater* [21], performing the *entanglement swapping* operation acts on its two qubits, respectively entangled with A and C, consuming them.

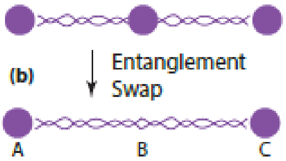


Figure 4.7: Entanglement swapping between nodes A and C [18]

This operation can be repeated in sequence on several nodes arranged linearly in a chain, so as to obtain the desired long-distance entanglement. Clearly for issues related to the life time of the entanglement, threatened by the decoherence due to the inevitable interactions with the environment, the preferable solutions are the ones in which multiple swaps are carried out in parallel in order to minimize the time required to achieve the goal, as shown in Figure 4.8: in this example of nodes chain the entanglement propagation is performed from A to E not sequentially, but in a parallel fashion, so that the time required to entangle A and E is shorter.

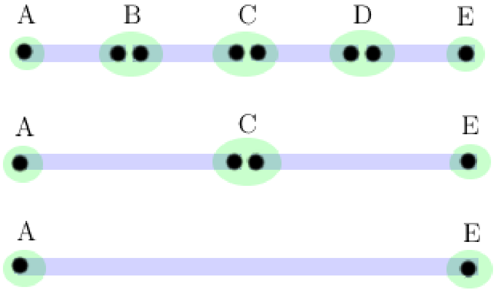


Figure 4.8: Example of parallel entanglement swapping to increase efficiency

In this way entanglement distribution over elementary links can be attempted in parallel in a nested way, where the key advantage is its efficiency. Distributing entanglement over a $L_0$-long link often requires the transmission and detection of a single photon, which is successful with a probability of order $e^{-\alpha L_0}$, where $\alpha$ is proportional to the channel attenuation. Using this technique over a total distance $L$ worsens the success rate, that scales with $e^{-\alpha L}$, while with the nested swapping the entanglement distribution over distance $L$ would scale with $e^{-\alpha L_0}$ [8].
It is clear that from a resource point of view, the *repeater* is a node that must be able to store the entanglement and to perform the Bell state measurement (BSM), and for an entangled pair in general both nodes need to store one qubit per entangled links. Alternatively, qubits can be communicated without using quantum memories, therefore avoiding entanglement swapping, using the quantum error correction [22]. However, due to the current technological limits, this is a solution not yet implementable, requiring the creation of entangled states consisting of a large number of photons (only 10 realized today) and densely placed repeater stations performing near perfect operations, while the use of the *heralded entanglement* doesn't require as many qubits.

Going into the detail of entanglement swapping, it is an operation articulated according to the blocks in Figure 4.9: starting from two entangled pairs - in the example we are dealing with states $|\Phi^+\rangle$ - a Bell state measurement is performed with the $CNOT$ gate followed by the $Hadamard$ gate, to then perform computational measurements and provide the results, that are two classical bits, respectively to the source and destination node of the entanglement. Finally, there are two correction gates such as the controlled-Z and $CNOT$ so that the nodes involved can recover the correct state.

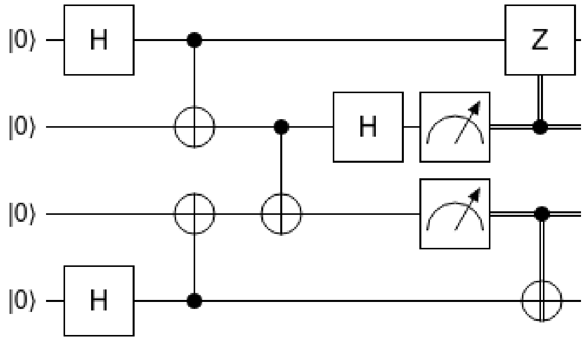


Figure 4.9: Entanglement Swapping circuit

In particular a fundamental role is played by the BSM (Bell state measurement), consisting in the *CNOT* followed by the *Hadamard* gate and the measurement blocks. To understand this operation let's consider the state $|\Phi^+\rangle$ in input to this configuration, so the action of the BSM is discussed below in formulas:

$$\begin{aligned}|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) &\xrightarrow{CNOT} \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \\ \xrightarrow{H} \frac{1}{\sqrt{2}}\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)|0\rangle &+ \frac{1}{\sqrt{2}}\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)|0\rangle = |00\rangle \qquad (4.4)\end{aligned}$$

If the BSM input is the $|\Phi^-\rangle$ state, than is will be changed as below:

$$\begin{aligned}|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) &\xrightarrow{CNOT} \frac{1}{\sqrt{2}}(|00\rangle - |10\rangle) \\ \xrightarrow{H} \frac{1}{\sqrt{2}}\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)|0\rangle &- \frac{1}{\sqrt{2}}\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)|0\rangle = |10\rangle \qquad (4.5)\end{aligned}$$

With $|\Psi^+\rangle$ state as input, the state $|01\rangle$ is then obtained:

$$\begin{aligned}|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) &\xrightarrow{CNOT} \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle) \\ \xrightarrow{H} \frac{1}{\sqrt{2}}\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)|1\rangle &+ \frac{1}{\sqrt{2}}\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)|1\rangle = |01\rangle \qquad (4.6)\end{aligned}$$

Finally the state $|\Psi^-\rangle$ will change into $|11\rangle$:

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}(|01\rangle - |11\rangle)$$
$$\xrightarrow{H} \frac{1}{\sqrt{2}}\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)|1\rangle - \frac{1}{\sqrt{2}}\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)|1\rangle = |11\rangle \tag{4.7}$$

The last part of the scheme concerns the corrections that may be applied to the obtained state. In fact, it should be noted that following the Bell state measurement, the status shared between Alice and Bob can be one of the following: $|00\rangle + |11\rangle$, $|01\rangle + |10\rangle$, $|00\rangle - |11\rangle$ or $|01\rangle - |10\rangle$, leaving out $\sqrt{2}$ at the denominator. A check on X-parity and Z-parity is therefore applied, providing the results of the measurement to Alice and Bob. The first measure concerns the possible phase-flip suffered by the state, which is repaired by the controlled-Z, the second measure concerns the possible bit-flip suffered by the state, which is instead corrected by the $CNOT$. For example, if the outcome turns out to be 10, it means that there has been a phase-flip but not a bit-flip, that is, that the two qubits are equal but opposite in phase, so the state $|00\rangle - |11\rangle$ is corrected into $|00\rangle + |11\rangle$ by controlled-Z and it is then left unchanged by the $CNOT$. Similarly, if the measurement in Bell's state turns out to be 11, it means that there has been both a phase-flip and a bit-flip, therefore a state $|10\rangle - |01\rangle$, which is corrected by the $CNOT$ into the state $|00\rangle - |11\rangle$ and then from the controlled-Z into $|00\rangle + |11\rangle$, allowing the recovery of the correct initial state between Alice and Bob.

## 4.4 Quantum Repeater Nodes

Quantum repeaters were first introduced in 1998 and three classes, or generations of them, have followed one another over time [23]. Furthermore, the introduction of quantum repeaters in a communication line makes it possible to beat the maximum rate (which is a capacity bound known as the PLOB bound [24]) at which two remote parties can distribute qubits, entangled

pairs or secret bits over a lossy channel [25].
Referring to [8], to the first generation it belongs the *Probabilistic Quantum Repeater*, whose operation is based on probabilistic techniques such as entanglement distribution and entanglement swapping, which means that it is required to repeat a certain operation until it succeeds, due to the fragility of photon-based systems against loss. As seen in Section 4.2.1 there are different ways of generating the entanglement and distributing it, in particular by making use of a BSM. Bell State Measurement in probabilistic quantum repeaters is typically done by first converting the state of quantum memories back into photonic states and then use linear optics modules to perform the BSM, which can be inefficient. An implication of the probabilistic BSM is that we cannot perform BSMs in a certain nesting level until we have learned about the results of the BSM in the previous level, which requires the exchanging of data between intermediate nodes, introducing delay. This would result in a strict requirement in decoherence time and a low entanglement generation rate. *Probabilistic Quantum Repeaters* are the simplest repeater technology to be implemented in practice, and even in the simplest setup (where there is only one repeater node in the middle) they offer an advantage for memory-assisted QKD. Anyway, as mentioned before, this solution offers a low key rate generation over long distances [8].

The next generation is represented by the *Deterministic Quantum Repeaters* class, that relies on deterministic but possibly erroneous gates or operations for BSM, assuming that the initial entanglement distribution and storage have taken place ending with a high quality entangled stated between nodes and assuming that the initial entangled pair over the elementary links was a maximally entangled state. Using this Deterministic Repeater we obtain modestly high key rate, with some limitations. The main one is that the initial links are still probabilistic. Moreover a trade-off between the number of nesting levels and the accumulated error must be taken into account [23].

The last generation of quantum repeaters is based on quantum error correction techniques to overcome loss and operation errors through *memory-less* quantum repeaters. The common way to distribute quantum information is to establish entanglement between nodes and then use quantum teleportation to transfer information from one node to another, then apply entanglement swapping to extend the entanglement range using repeater nodes. This approach is limited by the time required for the establishment of intermediary entangled links. In other words it necessitates quantum memories capable of storing a qubit for milliseconds or longer. Another way to transfer quantum information does not involve teleportation and does not require long-lived quantum memory, but it is based on directly transmitting quantum information in an encoded form in the quantum network. This solution relies on using quantum error correction codes [22] to overcome loss and operation errors. In this case the matter qubit of the cavity is not thought of as quantum memory, but instead as a processing qubit.

For example, a single photonic quantum state $\alpha|0\rangle + \beta|1\rangle$ can be encoded as [22]

$$|\Psi\rangle^{(m,n)} = \alpha\,|+\rangle_1^{(m)}\cdots|+\rangle_n^{(m)} + \beta\,|-\rangle_1^{(m)}\cdots|-\rangle_n^{(m)} \tag{4.8}$$

where $n$ is the number of logical qubits and $m$ is the number of physical qubits in each logical qubit. The logical qubit basis states are given by $|\pm\rangle^{(m)} \equiv |0\rangle^{\otimes m} \pm |1\rangle^{\otimes m}$. This encoded state has the property that the original quantum state can be recovered as long as at least one photon survives in each logical qubit, and one logical qubit with all its $m$ photons is fully received. This redundant quantum parity code can be used in a repeater scheme to transfer quantum information between remote nodes, with a transmitter unit that moves information from the matter qubits to photons, while the receiver operates in reverse to transfer information from the photonic form back to matter qubits. The direct transmission scheme also can be used in a butterfly arrangement to distribute entanglement between a source and a destination, without the need for long-lived quantum memories. Even if these memoryless repeaters offer a great improvement in the key rate generation (on the order of tens of MHz), they require a demanding set of properties, such as operation error as low as $10^{-4}$-$10^{-3}$, a large number of intermediate nodes and multiple photons per state, whose generation needs advanced technologies.

Hence, the restrictiveness of the requirements puts the memory-less class in a more distant future.

## 4.5 Routing Entanglement in the Quantum Internet

Since the fundamental role of a Quantum Network is to distribute entanglement to remote nodes, routing protocols have been developed to generate entanglement simultaneously between multiple pair of nodes in a quantum network. The routing entanglement strategies shown in this section are those described in [26]. Considering the *repeaters* as those nodes that are equipped with quantum memories for storing the entanglement, with classical resources and interfaces and the ability to perform the Bell state measurement between any pair of locally-held qubits, these protocols instruct the nodes, for each time slot, on how to dynamically choose which pair of nodes to perform the BSM, then the way to perform the entanglement swapping in order to generate a long-distance quantum entanglement.

The goal is to obtain a protocol that maximizes the entanglement generation rate for a collection of entanglement flows. As we can see in Figure 4.10, an example of quantum network consists in generic nodes that can be the source or destination of the information to be transferred (green nodes) and *repeater* nodes (in blue). They are equipped with quantum memories at least for how many entangled pairs are associated, and can perform the BSMs on pairs of qubits. Through chains of entanglement swapping they propagate the entanglement in the network, while the dotted lines that connect them are lossy optical channels.

With reference to Figure 4.10, let's consider a graph $G(V, E)$ describing the topology of the repeater network. Each node $v \in V$ is a repeater, and each edge $e$ is a physical link connecting two repeater nodes.

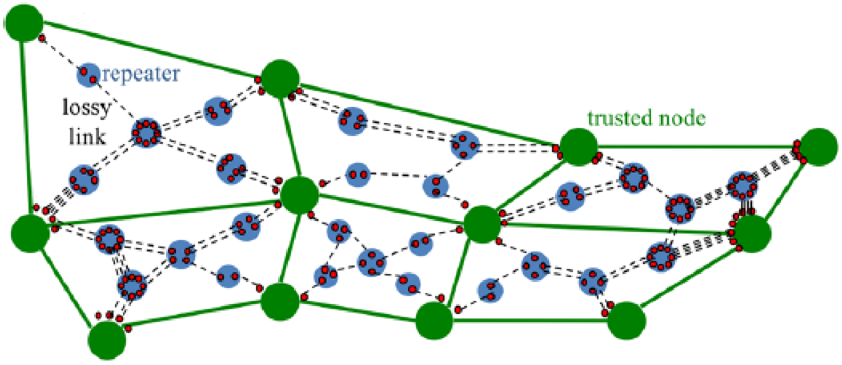


Figure 4.10: Example of Quantum Network [26]

Imagine that the time is slotted and that each memory can maintain a qubit for T ⩾ 1 time slots, beyond which the decoherence leads to the loss of information. Each time slot consists in two phases: the "external" and the "internal" phase. In the first phase, each repeater tries to establish an entanglement between its memories and the qubits of the adjacent nodes, whose success has probability $p_0(e) \sim \eta(e)$ where $\eta(e) \sim e^{-\alpha L(e)}$ is the *transmissivity* of a lossy optical channel. Through a two-way classical link the generic repeater knows which attempt of entanglement has been successful, in respect of the possible parallel links (dashed lines).

By simplifying to a square-grid topology, in the first phase of each time slot an attempt is made to establish entanglement with neighboring repeater nodes, whose success has probability $p$ (Figure 4.11a). In the internal phase, in the same time slot, entanglement swapping (BSM) is attempted on pairs of qubits that participate in the entanglement with the adjacent nodes in whose previous phase the entanglement was established. This second phase is successful with probability $q$ (Figure 4.11b). So after a time slot, along a path that includes $k$ edges, one e-bit (entangled pair) is successfully shared between the end points of the path with probability $p^k q^{k-1}$.

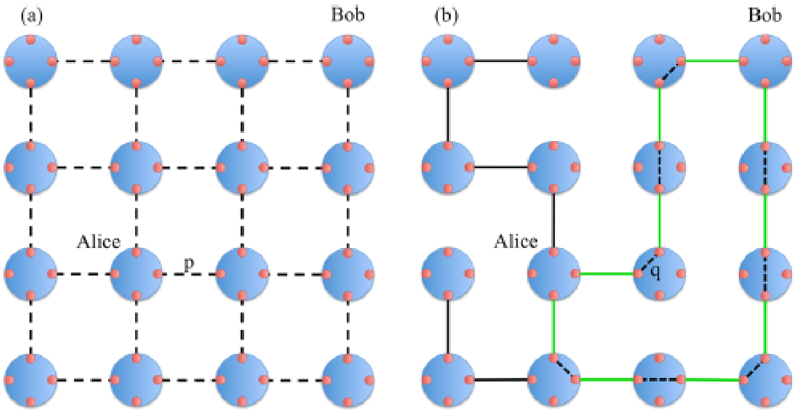


Figure 4.11: Square-grid topology [26]. a) In the external phase entanglement is attempted between neighboring repeaters b) In the internal phase entanglement swapping is attempted on a qubit pair within each repeater, based on the success of the entanglement generation in the previous phase

### Multipath routing of a single entanglement flow

A first way for repeaters to decide on which internal qubits to perform BSM is based on a simple greedy algorithm, for which it is assumed that a global link-state knowledge is available to each repeater node, i.e., the status of each external link after the first phase of the time slot ended is known to each repeater. To choose internal links, let's consider the subgraph consisting of successful external links and repeater nodes at the end of the external phase, then choose the shortest path that connects Alice to Bob. If a shortest path of length $k_1$ is found, all the internal links between the interested nodes are attempted, so the probability that all $k$-1 internal links are successful is $q^{k_1-1}$. At the next step of the greedy algorithm, all external and internal links of the next step are removed from the subgraph, and the shortest path in the remaining subgraph of length $k_2$ is searched.

The entanglement generation rate is the sum of expected rates (e-bits per time slot) from these paths, considering that for a square grid topology there can be a maximum of four disjoint paths between Alice and Bob. Considering Figure 4.11 we can see that, given the set of the created external links, the shortest path has length $k_1 = 4$ and the next path has length $k_2 = 6$.

These two are the only available paths between Alice and Bob, so using this greedy algorithm the expected number of shared e-bits generated in this time slot is $q^{k_1-1} + q^{k_2-1}$. The intuition behind this algorithm is that the entanglement generation rate along a path of length $k$ decays exponentially as $q^{k-1}$, suggesting that attempting internal links to facilitate connections along the shortest path first would optimize the expected rate.

### Entanglement routing with local link-state information

Unfortunately knowing the global link-state is unrealistic for a large network, as it requires memories whose coherence time increases with the network size, due to the time required for the traversal of link-state information across the entire network. A more realistic protocol therefore considers that the nodes have the link-state available only at the local level, that is the information related to the two adjacent nodes in the repeater chain.

Let's consider Alice and Bob as source and destination nodes and be $u$ the intermediate repeater node that must attempt entanglement swapping. The repeater will attempt the internal link based on which external links have been created, further assuming that each node knows the entire network topology and location of Alice and Bob. The rules followed by the $u$ repeater to attempt the internal link depends on the number of external links succeeded. If less than one external link with neighbor nodes has succeeded, then it doesn't attempt internal links, as the repeater $u$ cannot be part of the path that connects Alice to Bob. If two or more external links have been successful, then among all the nodes close to $u$ (which have established an external connection in that time slot) the node $v$ is labeled as that node with less distance from A (minimum $d_A$) and with $w$ the node closest to B (minimum $d_B$). If two neighbors have the same value of $d_A$ and $d_B$, then a coin is tossed to determine the choice of $v$ and $w$. If $v$ and $w$ are the same node, then $v$ (or $w$) is replaced by node $u$'s nearest-neighbor node with the smallest value of $d_A$ (or $d_B$). The choice on the node to replace $v$ or $w$ is made in such a way as to minimize the sum $d_A$+$d_B$. An internal link is then attempted between the memories connected to $v$ and $w$ respectively (as shown in Figure

4.12a).
If all four external links have been successful, then in addition to the previous internal link, the links between the remaining two memories are also tried, since it can only be an advantage for the entanglement generation rate (Figure 4.12b).

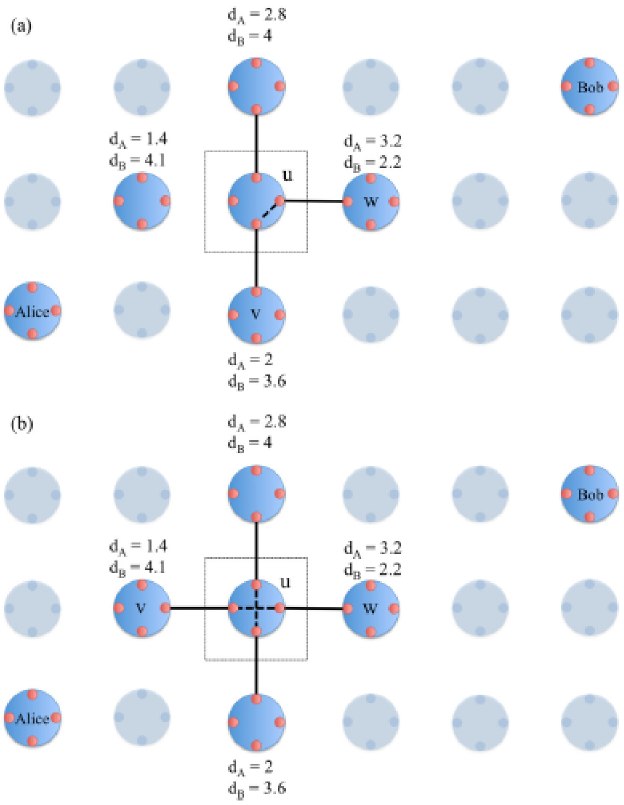


Figure 4.12: Entanglement swapping rules in the case of local link-state knowledge [26]

The local protocol has a scaling advantage over the global one, because the local rule allows the flow of entanglement-generation between Alice and Bob to find multiple paths simultaneously, in different time slots, and does not have to rely on all links along a linear chain to be successful, that is analogous to *multi-path routing* in classical computer networks.

### Simultaneous entanglement flows

Referring to local link state knowledge in repeater nodes, let's consider simultaneous entanglement generation flows between Alice and Bob pairs. Imagine that we have a node distribution as in Figure 4.13 and denote with $R_1$ and $R_2$ the entanglement generation rate obtained by the respective entangled Alice-Bob pairs.

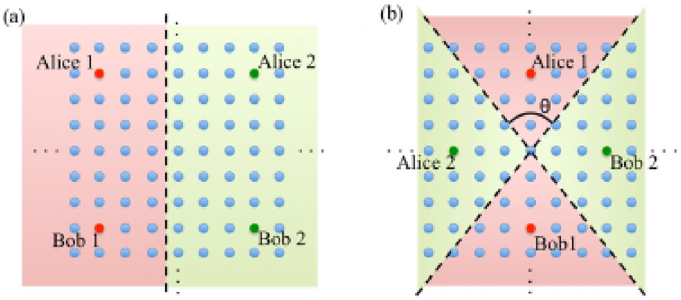
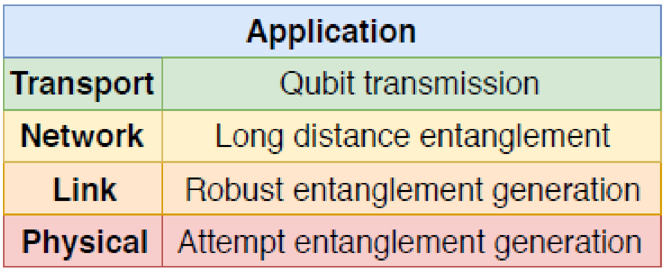


Figure 4.13: Multi-flow routing for two Alice-Bob pairs [26]

A simple strategy is the *single-flow time-share*, which uses the local rule previously described to follow the Alice1-Bob1 flow for a time $\lambda$, and in the fraction of time $1 - \lambda$ it follows the second flow Alice2-Bob2. If this strategy is followed by all repeaters except Alice and Bob, even when all repeaters support stream 1, there is still some leftover $R_2$ that is attained (*multi-flow time-share*). However, we note that only the repeaters that are part of the direct path between Alice and Bob are significant when applying the local rule, so another strategy is the so called *multi-flow spatial-division*, in which we divide the network between two spatial regions corresponding to the two flows (Figure 4.13a), so any repeater belonging to the red region applies the local rule tied to the Alice1-Bob1 flow and at the same time the repeaters in the green region operate with the local rules for the Alice2-Bob2 flow. This means that two flows can coexist and operate with a very small reduction from their individual best rates, because they benefit from almost disjoint paths. In the other extreme (Figure 4.13b) the rate region attained by multi-flow time sharing still provides an improvement over single-flow time sharing.

## 4.6 Quantum Network Stack

After showing the fundamental mechanisms for transporting quantum information and propagating entanglement in a network, we are going to define the network stack [18].



| | |
|---|---|
| **Application** | |
| **Transport** | Qubit transmission |
| **Network** | Long distance entanglement |
| **Link** | Robust entanglement generation |
| **Physical** | Attempt entanglement generation |

Figure 4.14: Quantum Network stack [18]

As in a classical network, we refer to the lowest element of the stack as the *physical layer*, that is realized by the quantum hardware devices and physical connections such as optical fibers. The physical layer contains no decision making elements and doesn't keep the state of the entanglement in a memory. This hardware generates time synchronization and laser pulse stabilization, required for attempting heralded entanglement, so the typical realizations involve two controllable quantum nodes connected by a chain of automated nodes, each one attempting the entanglement in well defined time slots. Over the physical layer, the *link layer* makes the entanglement attempts robust through the heralding station. On top of the link layer, the *network layer* is responsible for producing long-distance entanglement between nodes that are not directly connected by automated nodes, achievable by entanglement swapping, and also contains an entanglement manager that keeps track of the entanglement in the network. Finally, the *transport layer* makes it possible to transmit qubits in a deterministic way, using teleportation.

In particular the link layer allows higher layers to operate independently of the underlying hardware platform. The source and destination nodes can request entanglement through a *CREATE* packet request from the higher layer with parameters specifying the remote node with whom the entanglement generation is desired to establish, the type of request, the number of entangled pairs to be created, and other fields depending on the specific purpose, and moreover the request contains a purely quantum parameter that is the *desired minimum fidelity*, describing the quality of the entanglement that is needed, where the ideal target state has fidelity equal to 1 (i.e. the desired state is exactly the state that has been produced through entanglement generation). To confirm the entanglement production, an $OK$ message should be returned [18].

The standard metrics from networking also apply here, such as *throughput* which in this case is the entangled pairs/s rate, and the latency of the request. $Fairness$ is also demanded, because requests may originate at both source and destination, so the metrics should be independent of the origin of the request. We as well consider quantum quality metrics [27], such as the $fidelity$, that is important in applications such as QKD. The Physical and Link Layer protocols proposed in [18] are described in the next section.

## 4.7 Physical and Link Layer Protocols

The Midpoint Heralding Protocol (MHP) is meant to be implemented at the lowest layer subject to tight timing constraint (entanglement can only be produced if both photons arrive at the heralding station at the same time), that is the Physical Layer. This protocol polls the Link Layer at each timestep to determine whether entanglement generation is required, and keep no state. After the poll request, the higher layer may give back a negative response and in this case no attempt will be made, or a positive response, additionally providing parameters to use in the attempt of the entanglement. The parameters given to the MHP with a positive response contain the ID for the attempt, that is forwarded to the heralding station, generation parameters, the device qubits for storing the entanglement and the sequence of operations to perform on the device memory. Entanglement generation is then triggered at the start of the next time interval and a $GEN$ message is sent to the heralding station which includes a time-stamp and the given ID. The heralding station uses the timestamp to link the message to a detection window in which the accompanying photons arrived. If messages from both points arrive, the midpoint verifies the matching between the IDs sent with the $GEN$ message, and checks the detection counts from the corresponding detection window. The midpoint will then send a $REPLY$ message containing the state of the operation (success or failure), and in case of success which of the two states $|\Psi^+\rangle$ and $|\Psi^-\rangle$ was produced.

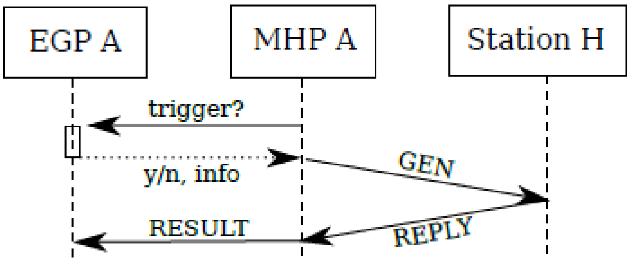


Figure 4.15: Scheme of the MHP checking for requests of entanglement generation from the higher layers [18]

Considering the two nodes A and B asking for the entanglement attempt, in the successful scenario the sequence diagram is depicted in Figure 4.16, where $p$ is the photon associated with the request.

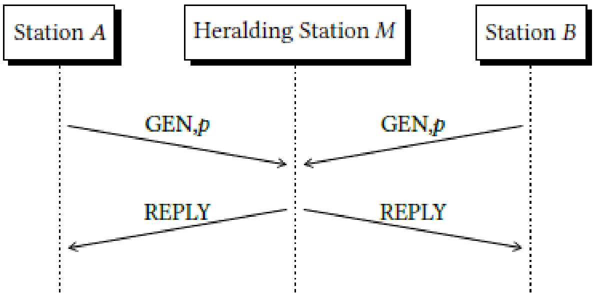


Figure 4.16: MPH sequence diagram in the successful case [18]

The Link-layer EGP (Entanglement Generation Protocol) begins when a higher layer at a controllable node issues a CREATE operation to the EGP specifying the desired number of entangled pair, along with the minimum fidelity and maximum latency time. Both nodes that wish to establish entangled links must trigger their MHP device in a coordinate fashion, so the EGP employs a distributed queue comprised of synchronized local queues at the controllable nodes. Upon receipt of a request the EGP will query the Fidelity Estimation Unit (FEU) to obtain hardware parameters. Then the scheduler generates a positive response to the MHP containing the parameters from the FEU, along with the ID containing the unique queue ID. The flow diagram of the MHP and EGP operations is shown in Figure 4.17 [18].

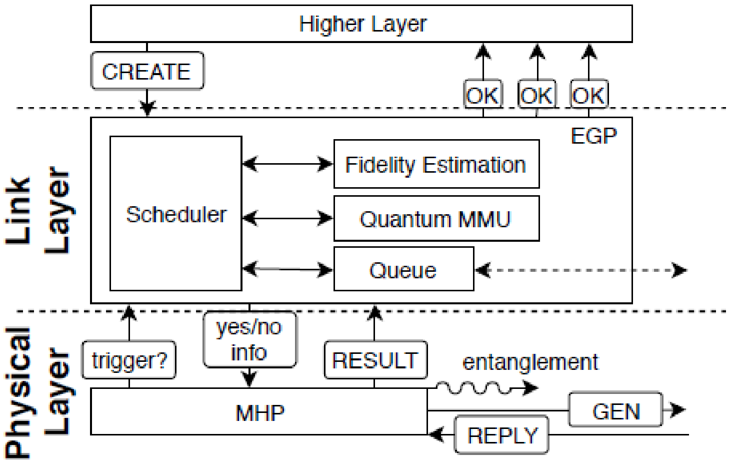


Figure 4.17: Flow diagram of the MHP and EGP operations [18]

It's worth noting that the control classical network where these protocol messages are employed can be replaced using a *piggybacking* technique, through which the classical information is encapsuled on quantum streams protected by quantum error correcting codes [28].

# Chapter 5

# Experimental results on IBM Q

A quantum circuit is made up of qubit operations - quantum gates - and, almost implicitly, of measurement elements. In this chapter the results of fundamental operations such as teleportation and entanglement swapping are shown, and then composed to display a simple quantum network. To write these circuits, the IBM Quantum Experience Circuit Composer [4] has been used. At first the proper operation of the circuits has been tested through the available circuit simulator, then the circuits have been tested through the real IBM quantum computers. IBM indeed provides a series of quantum computers online, with different interconnection architectures and noise levels, up to 15 qubits (IBM Q Melbourne).

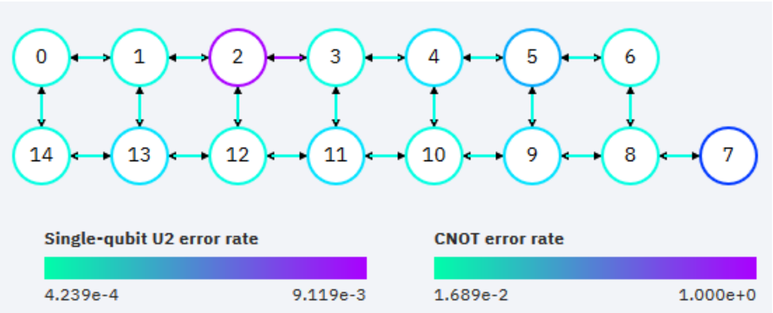


Figure 5.1: Interconnections and error rates of $CNOT$ gate and $U2$ gate ($U2$ performs a control over two different rotations within the gate) of the IBM Q Melbourne [4]

It is clear that while the simulator will give the ideal outcomes for a quantum circuit, testing the same circuit on the real quantum computer we'll obtain a result which takes into account the noisy nature of the circuit and the error rate of quantum gates. In Figure 5.1 it is shown the qubit connectivity, and the gate error rate, for the 15 qubit IBM Q Melbourne.

At the heart of IBM quantum system is the *transmon qubit*, developed in 2007 at the Yale University. Working as an artificial atom, it is a type of superconductive charge qubit designed to have reduced sensitivity to charge noise. Its name is an abbreviation of the term "transmission line shunted plasma oscillator qubits". To create an artificial atom a toolkit made of superconductive elements is used so there's no energy heated, hence no dissipation, which is a desired feature for quantum. Furthermore a Josephson junction, which is a non linear inductor element, kept at 0.015 Kelvin, is used to obtain unequally spaced energy levels, representing the quantum states of the qubit. The transmon achieves its reduced sensitivity to charge noise by significantly increasing the ratio of the Josephson energy to the charging energy, accomplish through the use of a large shunting capacitor [29].

## 5.1 Experimental Teleportation

As it has been described in Chapter 2, quantum teleportation is a technique that allows the transfer of a quantum state from one node to another, without a quantum communication channel between source and destination. It requires the transmission of two classical bits between the two parties and an entangled pair shared between them. For our experiments we fixed the state to be teleported, first at $|1\rangle$, then at $|0\rangle - e^{j\pi/4}|1\rangle$. The quantum circuit of teleportation of the quantum state $|1\rangle$ realized with the IBM Q Circuit Composer is shown in Figure 5.2.

### 5.1.1 Teleporting the state $|1\rangle$

The target here is to transfer the $|1\rangle$ quantum state from Alice (line $q[0]$) to Bob (line $q[2]$), consuming the entangled pair shared between them.

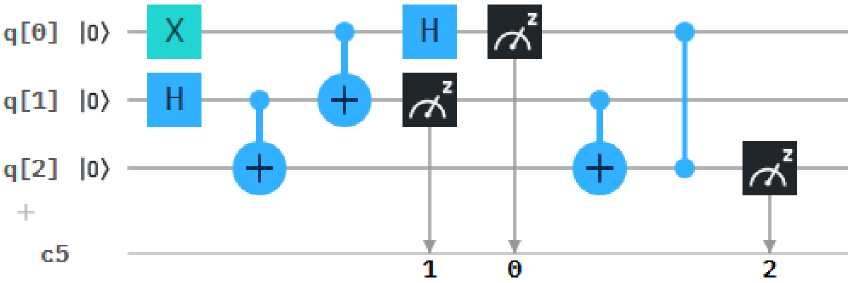


Figure 5.2: Quantum Circuit for the Teleportation of the $|1\rangle$ state

Since all the lines of the circuit are initialized at the state $|0\rangle$, we proceed to create the state $|1\rangle$ of Alice by adding the **X** gate in the Circuit Composer, which realizes the bit-flip. Alice also has a second qubit, in line $q[1]$, entangled with Bob's qubit, together belonging to the EPR pair $|\Phi^+\rangle$. Subsequently we have the Bell state measurement, with the collapse of the superposition of the possible entangled states, producing two classical bits that are then communicated to Bob via a classical channel. Thanks to this classical information, Bob will rebuild the original quantum state, after the correction via the controlled-NOT and controlled-Z gates. It's clear that after the measurement in the computational basis the original data is lost from the Alice perspective, so teleportation doesn't violate the no-cloning theorem at all.

Looking at the formulas in Equation 5.1, with the state $|\psi\rangle$=$|1\rangle$ to be transmitted, Alice firstly applies the *CNOT* gate to her half of the EPR pair, then the *Hadamard* gate on her first qubit, obtaining:

$$|1\rangle\left(\frac{|00\rangle+|11\rangle}{\sqrt{2}}\right)\xrightarrow{CNOT}|1\rangle\left(\frac{|10\rangle+|01\rangle}{\sqrt{2}}\right)\xrightarrow{H}\frac{(|0\rangle-|1\rangle)\,(|10\rangle+|01\rangle)}{2} \tag{5.1}$$

If we put in evidence Alice's two qubits, we can rewrite Equation 5.1 as follows:

$$|01\rangle\,|0\rangle + |00\rangle\,|1\rangle - |11\rangle\,|0\rangle - |10\rangle\,|1\rangle \tag{5.2}$$

The first term means that if the wave-function collapses to the $|01\rangle$ state, which means that Alice measured 01, then Bob will correct the state using a bit-flip gate **X** with the *CNOT* gate. If the outcomes are 00, then Bob does nothing, because the state is already correct. If the outcomes are 11, then Bob will perform a bit-flip **X** and phase-flip **Z** to recover the correct state, with both the controlled-X and the controlled-Z gates. Finally, if Alice measured 10 then Bob applies a phase-flip correction **Z** with the controlled-Z gate.

The outcomes are part of a classical line of 5 bits $c_4c_3c_2c_1c_0$. Through the circuit simulator we obtain the ideal behavior of the quantum circuit, which means that we'll read the outcome "1" corresponding to the eigenvector $|1\rangle$ in all of the 1024 runs (bit $c_2$ is always equal to 1, Figure 5.3). The same circuit was ran in the IBM Q Melbourne (15 qubits), where the measurement blocks in the circuit were all moved to the end of the lines because it is not currently hardware-level possible to renew a quantum state after the measurement itself. The results for the real quantum computer, in Figure 5.4, are probabilistic since they take into account the real quantum gate errors and noise. From the figure we see that in 86.6% of cases over 1024 shots Bob received the correct state $|1\rangle$.

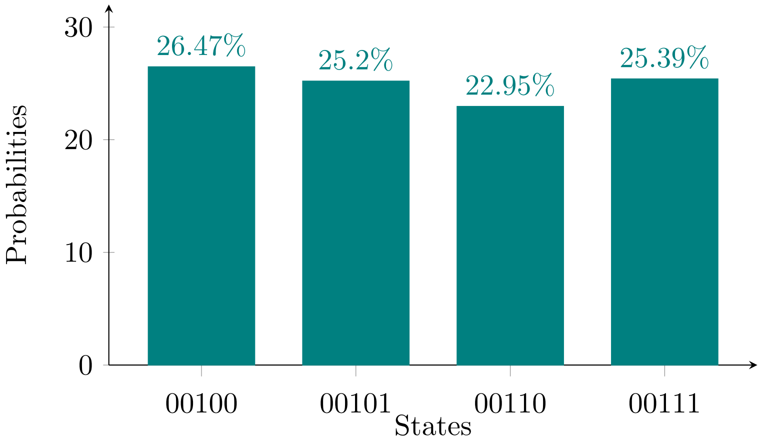


Figure 5.3: Histogram showing the results of teleporting state $|1\rangle$, simulation

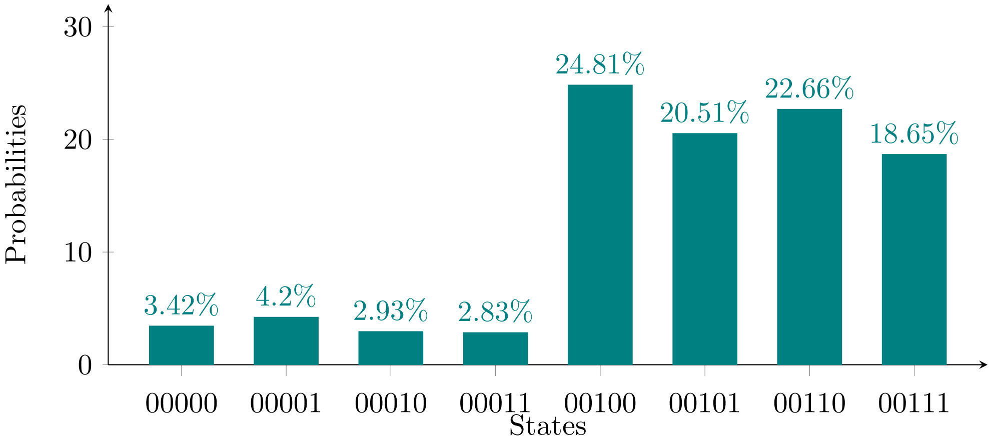


Figure 5.4: Histogram showing the results of teleporting state $|1\rangle$ on a real quantum computer, IBM Q Melbourne

### 5.1.2 Teleporting the state $|0\rangle - e^{j\pi/4}|1\rangle$

We experiment now the teleportation of a phase rotated quantum state. After Alice's processing of the state (lines $q[0]$ and $q[1]$) it is necessary to correct this rotation if we want to verify the correct operation of the circuit in transferring the $|1\rangle$ state. In the quantum circuit shown in Figure 5.5, a *Hadamard* gate and $\pi/4$ Z-rotation was chosen. After the rotation, the state is $|0\rangle - e^{j\pi/4}|1\rangle$.

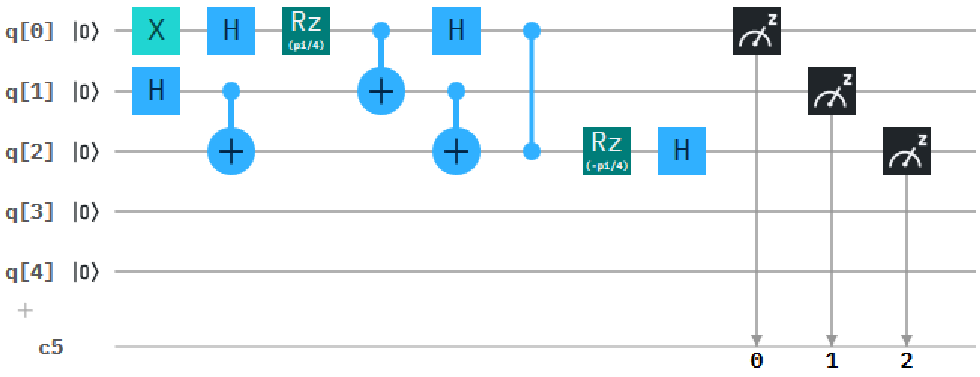


Figure 5.5: Quantum Circuit for the Teleportation of the state $|0\rangle - e^{j\pi/4}|1\rangle$ obtained with a *Hadamard* gate and a $\pi/4$ rotation gate

The operations carried out by Alice are the same, but the quantum state to transfer, before the measurement operation, will be

$$|\Psi_0\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

As shown in Figure 5.6 with the circuit simulator Bob receives the correct state with probability 1, while in Figure 5.7 with IBM Q Melbourne Bob obtains the desired state in 74,7% of cases ($c_2$=1) over 1024 runs, which means that the quality of the teleportation degraded, due to the quantum gate errors introduced by the *Hadamard* ad Z-rotation operations.

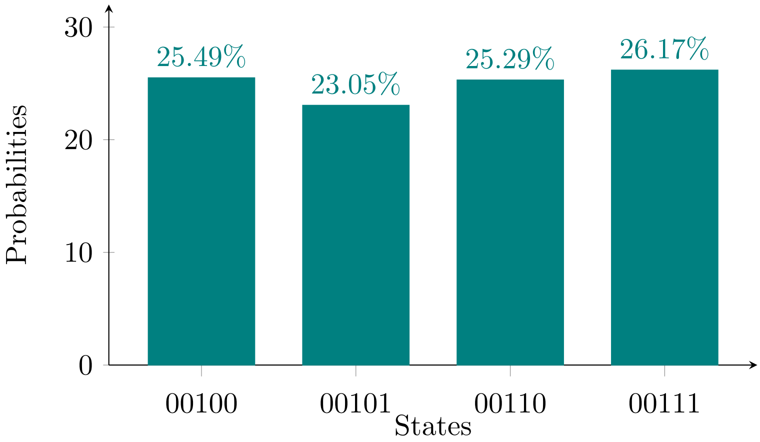


Figure 5.6: Histogram showing the results of state $|0\rangle - e^{j\pi/4}|1\rangle$ teleportation, simulation

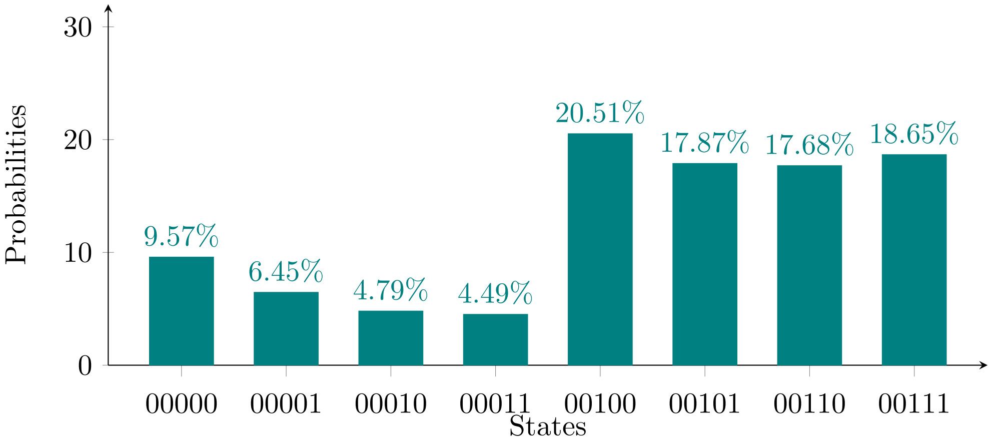


Figure 5.7: Histogram showing the results of state $|0\rangle - e^{j\pi/4}|1\rangle$ teleportation on a real quantum computer, IBM Q Melbourne

## 5.2 Experimental Entanglement Swapping

The Entanglement Swapping is a technique used to propagate the entanglement between remote nodes, which will end up with the same statistical description of the possible outcomes of the experiment. In other words, after this operation the nodes will behave in the same way from a quantum point of view. We consider the simple set of three nodes A, B and C, arranged linearly in space. The target is to propagate the entanglement from A to C, passing through B, which is called the *repeater* node.

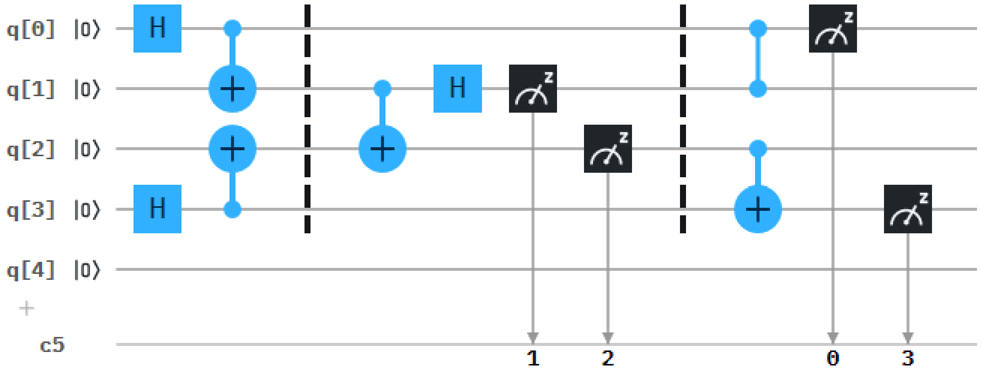


Figure 5.8: Quantum Circuit for the Entanglement Swapping

In the quantum circuit in Figure 5.8 node A corresponds to the $q[0]$ line, while the intermediate repeater node B is represented by the lines $q[1]$ and $q[2]$, and node C corresponds to the $q[3]$ line. These circuit lines are the quantum bits of the nodes, so to perform the entanglement swapping one qubit is needed for A and C, and two qubits are needed for C. The first step is to generate the two EPR pairs between A-B and B-C, that in this case are built from $|0\rangle$ states applying the *Hadamard* gate and *CNOT* gate. After these operations the $|\Psi^+\rangle$ state is obtained in both links:

$$|0\rangle \xrightarrow{H} \frac{|0\rangle + |1\rangle}{\sqrt{2}} \xrightarrow{CNOT} \frac{|00\rangle + |11\rangle}{\sqrt{2}} = |\Psi^+\rangle \tag{5.3}$$

Subsequently the node B performs the Bell basis measurement on his two qubits, consisting in the *CNOT* and *Hadamard* gates and the measurement in the computational basis, collapsing the superposition of the quantum Bell states for the two qubits:

$$\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right) = \frac{1}{2}\Big(|00\rangle\,|00\rangle{+}|00\rangle\,|11\rangle{+}|11\rangle\,|00\rangle{+}|11\rangle\,|11\rangle\Big)$$

$$\xrightarrow{CNOT} \frac{1}{2}\Big(|00\rangle\,|00\rangle + |00\rangle\,|11\rangle + |11\rangle\,|10\rangle + |11\rangle\,|01\rangle\Big)$$

$$\begin{aligned}\xrightarrow{H} \frac{1}{2\sqrt{2}}\Big[ |0\rangle \Big( |0\rangle + |1\rangle \Big) |00\rangle + |0\rangle \Big( |0\rangle + |1\rangle \Big) |11\rangle + \\ + |1\rangle \Big( |0\rangle - |1\rangle \Big) |10\rangle + |1\rangle \Big( |0\rangle - |1\rangle \Big) |01\rangle \Big] = \\ = \frac{1}{2\sqrt{2}}\Big[ |00\rangle \Big( |00\rangle + |11\rangle \Big) + |11\rangle \Big( |01\rangle - |10\rangle \Big) + \\ + |01\rangle \Big( |01\rangle + |10\rangle \Big) + |10\rangle \Big( |00\rangle - |11\rangle \Big) \Big]\end{aligned}$$

The outcomes of the measurement are then sent to A and C to choose how to correct the entangled state: if node B reads 00, then the state is correct ($|00\rangle$+$|11\rangle$) and no operation is required. If the outcome is 11, then bit-flip and phase-flip corrections are applied with a $CNOT$ and controlled-Z gates, to restore the $|\Psi^+\rangle$ to replace the incorrect state $|01\rangle$-$|10\rangle$. If node B reads 01, then the state $|01\rangle$+$|10\rangle$ is corrected by performing a bit-flip through a $CNOT$ gate. Finally if the outcome is 10, the $|00\rangle$-$|11\rangle$ state is corrected by using the phase-flip controlled-Z gate.

As shown in Figure 5.9, the quantum circuit simulation gives the expected value with probability 1, with $c_0$=$c_3$ for each run of the circuit. In Figure 5.10 the probability of success of the entanglement swapping is around 81%, running the circuit on a real quantum computer, the IBM Q Melbourne.

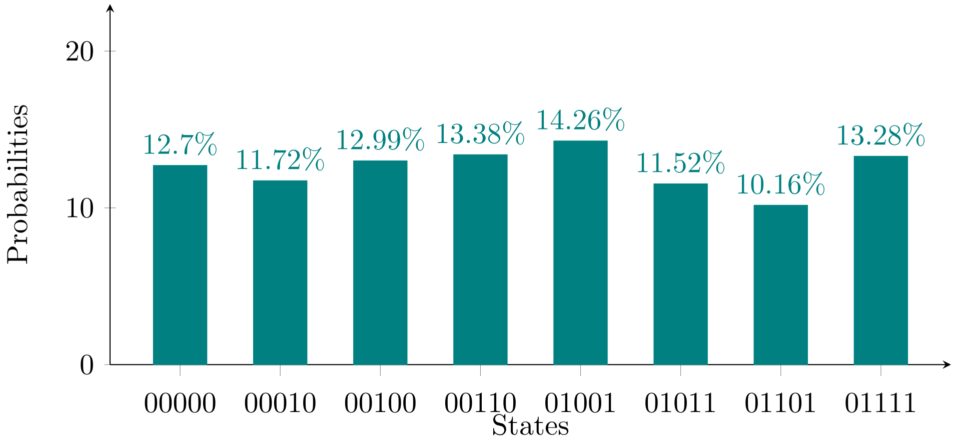


Figure 5.9: Histogram of the Entanglement Swapping results, simulation

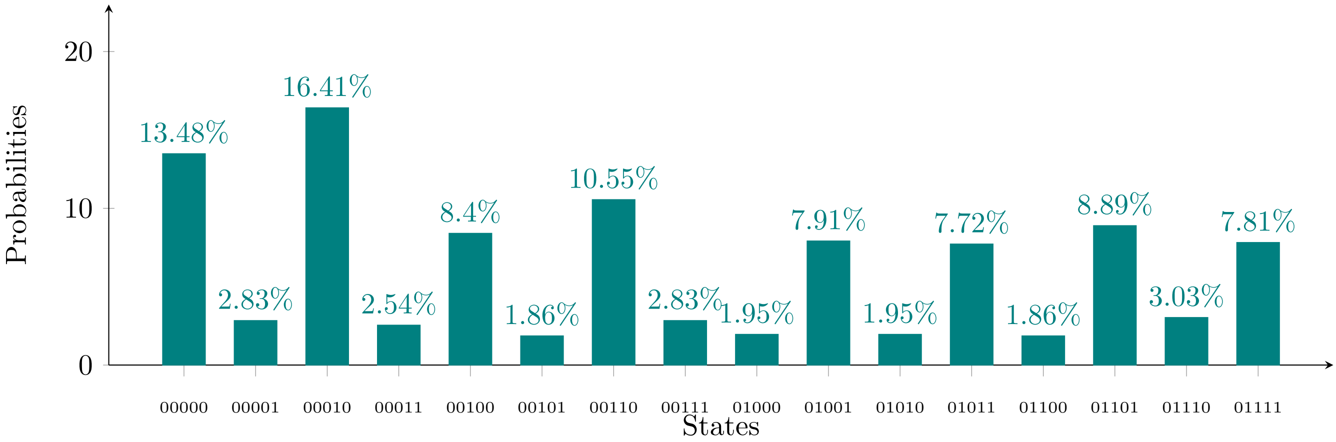


Figure 5.10: Histogram of the Entanglement Swapping results on a real quantum computer, IBM Q Melbourne

## 5.3 A simple quantum network

Let's consider a quantum network consisting of six nodes, linked as shown in Figure 5.11. Through this network we want to transfer qubits via teleportation and, to achieve this task, entanglement must be established between the source and destination remote quantum nodes.

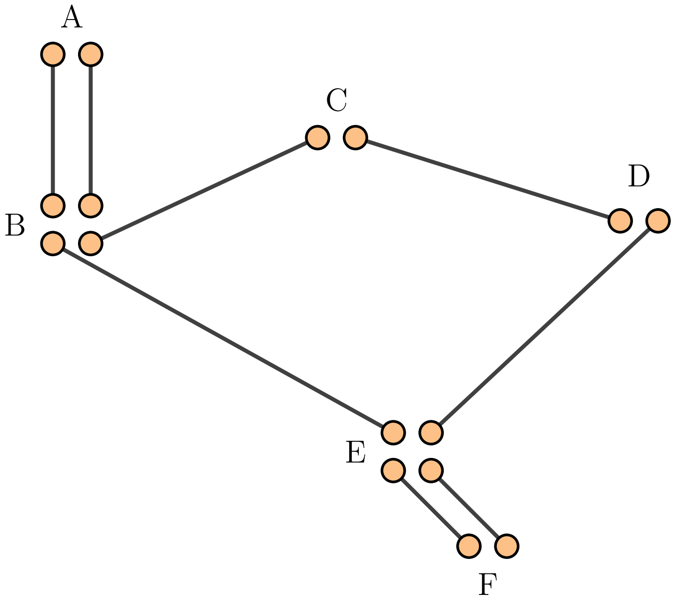


Figure 5.11: Quantum network

To propagate the entanglement it is necessary that the intermediate nodes act as quantum *repeaters*, so that they apply the entanglement swapping scheme. Each node must have a sufficient number of memory qubits to perform the entanglement swapping: this operation is done between pairs of qubit which are related to the respective entanglement links shared with the adjoining nodes. From this it follows that each node has a number of nodes equal to the links in which it participates. Moreover, for the no-cloning theorem it must be taken into account that node A and F must have two qubits, one for each path. In the proposed network the two paths are independent, hence the two paths can be studied separately.

### 5.3.1 Experimental implementation of the short link

The short path circuit includes nodes A, B, E and F. The first step is the generation of entangled links between pair of adjacent nodes (A-B, B-E, E-F). Then the entanglement swapping is performed sequentially: node B acts on the qubits linked to A and E by performing the Bell state measurement to extend to entanglement from A to E; hence, the same procedure is done by node E, to distribute the entanglement from A to F. The short path circuit is shown in Figure 5.12, where the qubit $q[0]$ belongs to the source node A, $q[1]$ and $q[2]$ to the repeater B, $q[3]$ and $q[4]$ to the repeater E, finally $q[5]$ to the destination node F.

As it can be seen in Figure 5.13, the histogram shows that in the simulation qubit $q[0]$ and qubit $q[5]$ behave in the same way after the entanglement swapping operation, so $c_0 = c_1$ with probability 1.

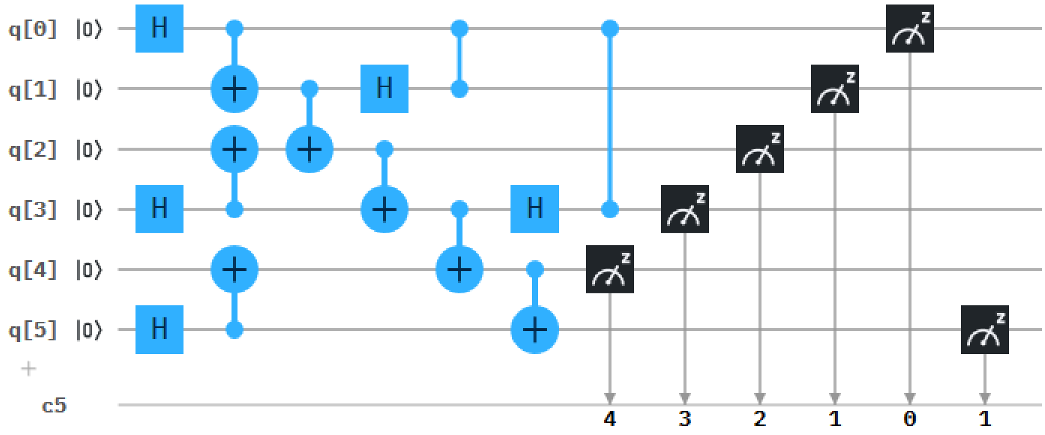


Figure 5.12: Quantum Circuit of the Entanglement Swapping for the short link

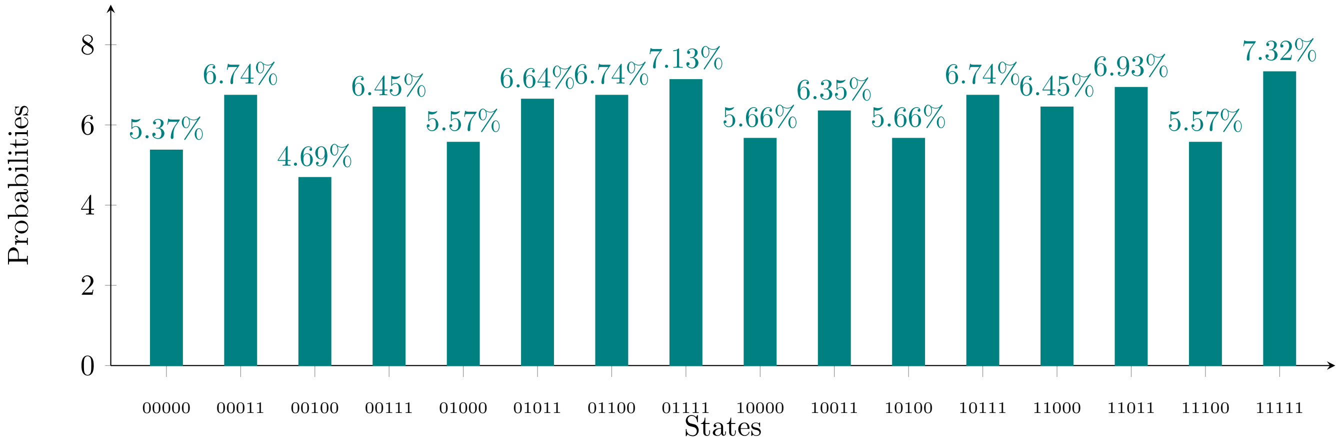


Figure 5.13: Histogram of the Entanglement Swapping results in the short link, simulation

In Figure 5.14 the histogram describes the outcomes for the entanglement swapping operation over a real quantum computer, the IBM Q Melbourne, for the short link, succeeding in 65% of the 1024 shots.

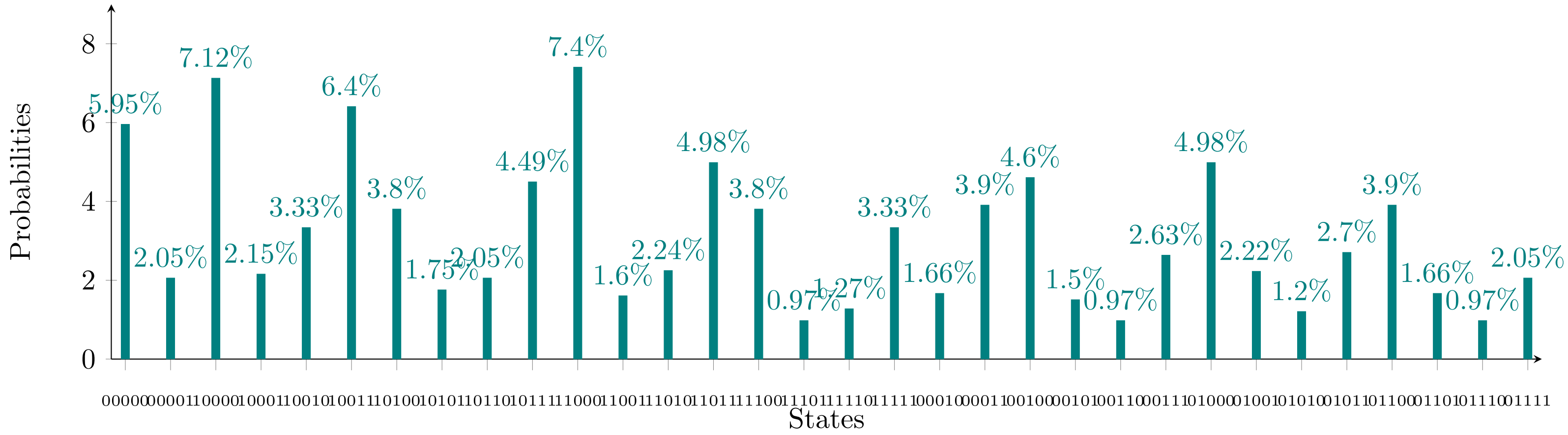


Figure 5.14: Histogram of Entanglement Swapping through the short link on a real quantum computer, IBM Q Melbourne

The short link is now ready to teleport a quantum state from A to F. In Figure 5.15 the quantum circuit for the teleportation of the state $|1\rangle$ is displayed.

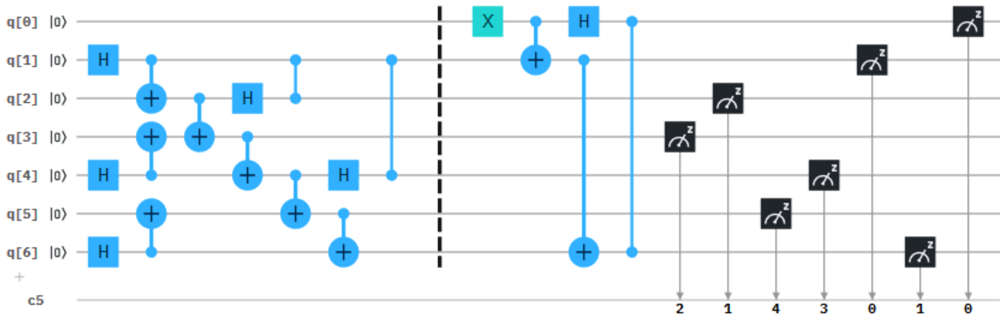


Figure 5.15: Quantum Circuit of the teleportation of state $|1\rangle$ through the short link

The results obtained in the circuit simulation are shown in Figure 5.16, showing that the state $|1\rangle$ teleportation from A ($q[0]$) to node F ($q[6]$), which is the $c_1$ bit, succeeded ($c_1$=1) with probability 1.

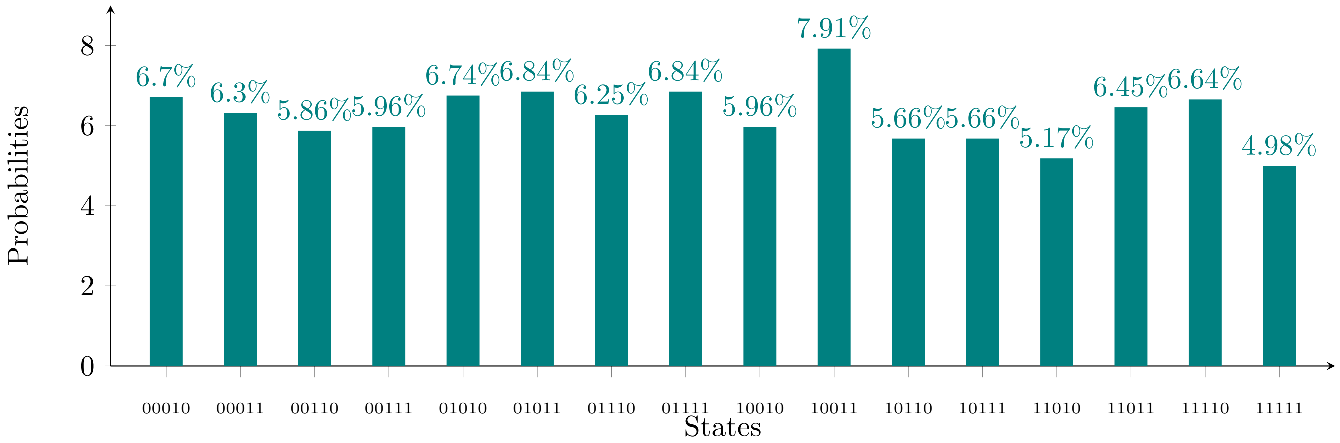


Figure 5.16: Histogram of the teleportation of state $|1\rangle$ through the short link, simulation

### 5.3.2 Experimental implementation of the long link

The long path circuit includes nodes A, B, C, D, E and F. To create a route from A to F, the generation of entangled links between pair of adjacent nodes (A-B, B-C, C-D, D-E, E-F) is required, then the entanglement swapping is performed sequentially with B, C, D, E working as *repeater* nodes to propagate the entanglement in the path.

The long path quantum circuit is shown in Figure 5.17.

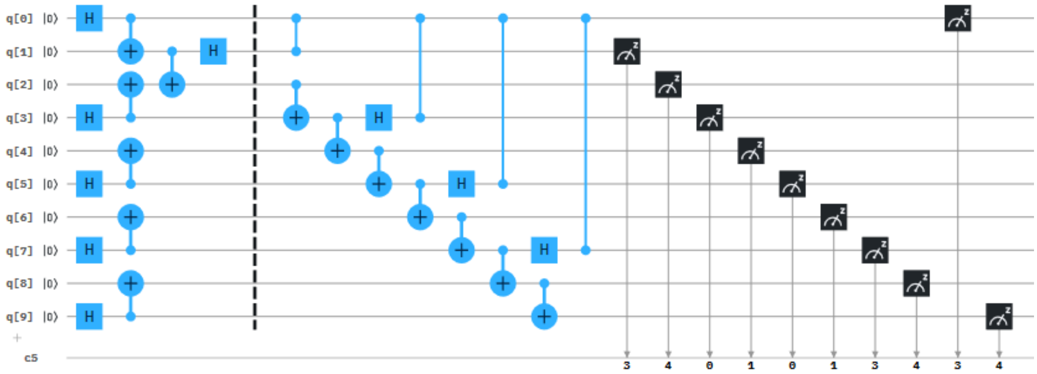


Figure 5.17: Quantum Circuit for the Entanglement Swapping through the long link

In Figure 5.18 it is displayed the histogram of the results obtained for the long path entanglement swapping for the circuit simulator, where $c_3$ has always the same value of $c_4$, confirming the entanglement propagation from the source to destination. For 4096 shots in the IBM Q Melbourne, the success in the creation of an entanglement between source and destination is around 54%, as shown in Figure 5.19.

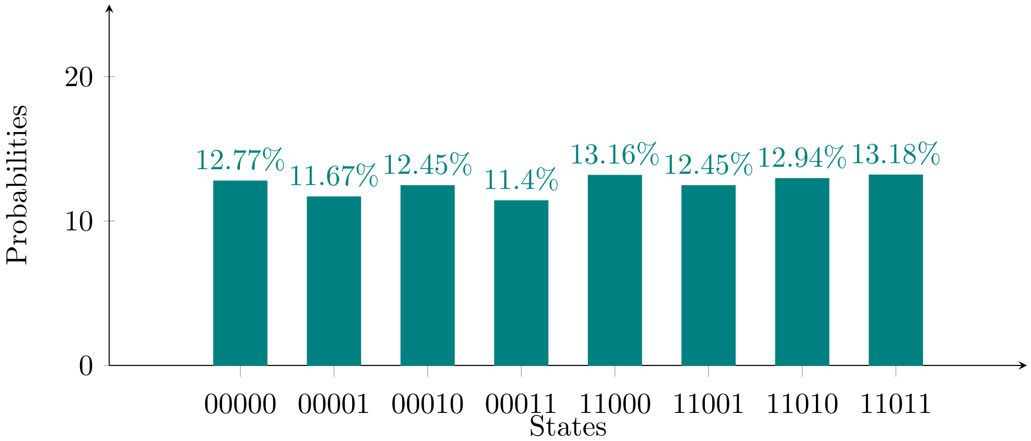


Figure 5.18: Histogram of the results of Entanglement Swapping through the long link, simulation

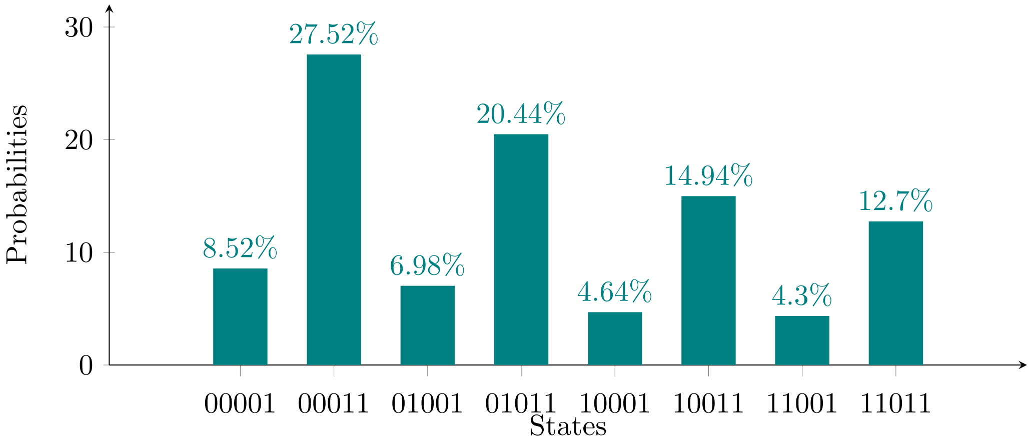


Figure 5.19: Histogram of the Entanglement Swapping through the long link on a real quantum computer, IBM Q Melbourne

### 5.3.3 Experimental implementation of the full network

The correct ideal functioning of the entire network is confirmed by the results of the circuit simulation in Figure 5.20. Here we observe that $c_0$=$c_1$ and $c_3$=$c_4$ with probability 1, hence the entanglement has been propagated from A to F along the two independent paths. This set of nodes, forming the quantum network, is now ready to perform operations such as the transfer of quantum information through the teleportation technique, since the quantum routes were built via entanglement swapping along the two paths. The full network circuit has not been run in the real quantum computer because the maximum number of qubits of the quantum computers made available by IBM Q Experience is not sufficient to do it. However, the performance would have been the same of the short and long link, since the two paths are disjoint. In Figure 5.21 the full quantum network circuit consisting in the two paths is shown.

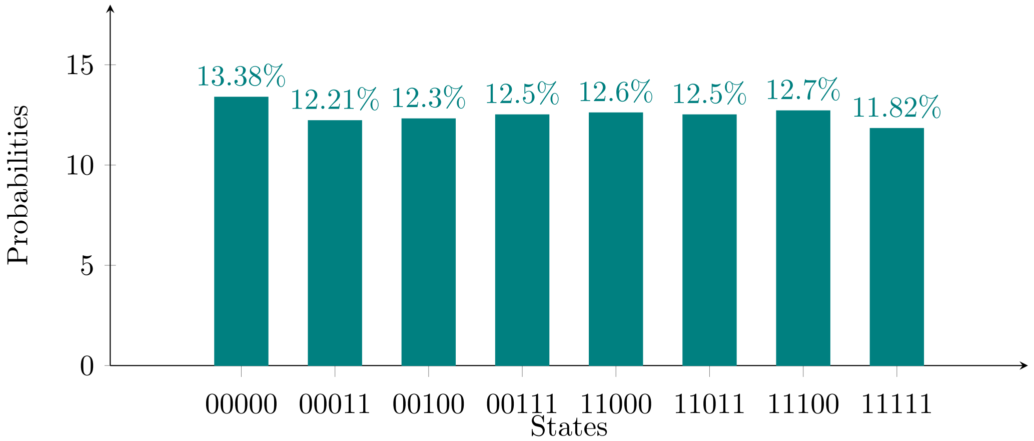


Figure 5.20: Histogram of the full quantum network, simulation

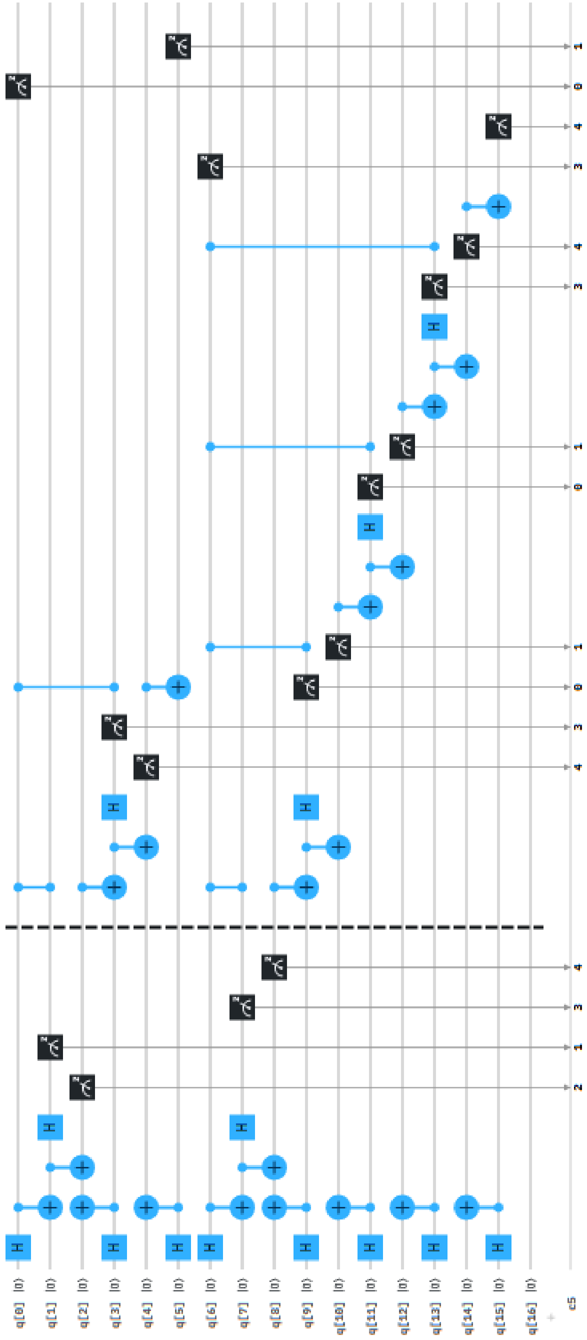


Figure 5.21: Quantum Network circuit

# Chapter 6

# Conclusion

Through this thesis work the functioning of the fundamental circuits to create a quantum network, based on the principles of quantum mechanics, were verified. Thanks to the *repeater*'s role, it was possible to propagate the entanglement so that remote nodes could be interconnected, with each route composed of a router chain. The actual transfer of a quantum state from source to destination was then verified on a real quantum computer. However, the modest size of the network was bounded to the maximum number of qubits of the computers made available by IBM Q Experience. In order to be able to make real experiments over more complex networks, for example a mesh network topology, many more qubits would be needed. Furthermore, having seen the results, we can say that the quantum computers are heavily affected by quantum noise and gate's errors, which increase with the size of the network, leading to low fidelity, far from ideal. Therefore, it would be necessary to adopt an error correction and fault tolerant techniques to protect quantum information from noise [5][30]. Looking at the evolution of quantum computing in time, since the fundamental theoretical concepts were shown only in the 1990's, it is imaginable that the 2020's will be the decade of quantum systems research, that will hopefully improve coherence, gates quality, stability, cryogenics components, integration and packaging of quantum circuits [3].

# Bibliography

[1] "National Academies of Sciences, Engineering, and Medicine", *"Quantum Computing: Progress and Prospects"*, E. Grumbling and M. Horowitz", Eds. "Washington, DC": "The National Academies Press", 2019. [Online]. Available: "https://www.nap.edu/catalog/25196/quantum-computing-progress-and-prospects"

[2] F. Arute, K. Arya, R. Babbush, D. Bacon, J. Bardin, R. Barends, R. Biswas, S. Boixo, F. Brandao, D. Buell, B. Burkett, Y. Chen, Z. Chen, B. Chiaro, R. Collins, W. Courtney, A. Dunsworth, E. Farhi, B. Foxen, and J. Martinis, "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, pp. 505–510, 10 2019.

[3] Jerry Chow, Jay Gambetta, "Quantum takes flight: Moving from laboratory demonstrations to building systems," January 8, 2020, https://www.ibm.com/blogs/research/2020/01/quantum-volume-32/.

[4] IBM, "What is ibm q," 2020, https://www.ibm.com/quantum-computing/learn/what-is-ibm-q/.

[5] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information.* Cambridge University Press, 2010.

[6] Smite-Meister, "Bloch sphere, a geometrical representation of a two-level quantum system," 30 January 2009, https://commons.wikimedia.org/wiki/Fil:Bloch_sphere.svge.

[7] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?" *Phys. Rev.*, vol. 47, pp. 777–780, May 1935. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRev.47.777

[8] S. Pirandola, U. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani *et al.*, "Advances in quantum cryptography," *arXiv preprint arXiv:1906.01645*, 2019.

[9] P. Villoresi, T. Jennewein, F. Tamburini, M. Aspelmeyer, C. Bonato, R. Ursin, C. Pernechele, V. Luceri, G. Bianco, A. Zeilinger, and et al., "Experimental verification of the feasibility of a quantum channel between space and earth," *New Journal of Physics*, vol. 10, no. 3, p. 033038, Mar 2008. [Online]. Available: http://dx.doi.org/10.1088/1367-2630/10/3/033038

[10] D. K. Oi, A. Ling, G. Vallone, P. Villoresi, S. Greenland, E. Kerr, M. Macdonald, H. Weinfurter, H. Kuiper, E. Charbon *et al.*, "Cubesat quantum communications mission," *EPJ Quantum Technology*, vol. 4, no. 1, p. 6, 2017.

[11] L. Shengkai, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, and J.-W. Pan, "Satellite-relayed intercontinental quantum network," *Physical Review Letters*, vol. 120, 01 2018.

[12] J. Yin, Y. Cao, Y.-H. Li, J.-G. Ren, S.-K. Liao, L. Zhang, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, M. Li, Y.-M. Huang, L. Deng, L. Li, Q. Zhang, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Satellite-to-ground entanglement-based quantum key distribution," *Phys. Rev. Lett.*, vol. 119, p. 200501, Nov 2017. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.119.200501

[13] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, G.-B. Li, Q.-M. Lu, Y.-H. Gong, Y. Xu,

S.-L. Li, F.-Z. Li, Y.-Y. Yin, Z.-Q. Jiang, M. Li, J.-J. Jia, G. Ren, D. He, Y.-L. Zhou, X.-X. Zhang, N. Wang, X. Chang, Z.-C. Zhu, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Satellite-based entanglement distribution over 1200 kilometers," *Science*, vol. 356, no. 6343, pp. 1140–1144, 2017. [Online]. Available: https://science.sciencemag.org/content/356/6343/1140

[14] S. Guerrini, M. Chiani, and A. Conti, "Secure Key Throughput of Intermittent Trusted-Relay Quantum Key Distribution Protocols," in *IEEE Global Communications Conference: Quantum Communications and Information Technology Workshop*, vol. 1, no. 1, Dec 2018, pp. 1–6.

[15] L. Bacsardi, "On the way to quantum-based satellite communication," *IEEE Communications Magazine*, vol. 51, no. 8, pp. 50–55, August 2013.

[16] H. J. Kimble, "The quantum internet," *Nature*, vol. 453, no. 7198, pp. 1023–1030, 2008.

[17] S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: A vision for the road ahead," *Science*, vol. 362, no. 6412, 2018. [Online]. Available: https://science.sciencemag.org/content/362/6412/eaam9288

[18] A. Dahlberg, M. Skrzypczyk, T. Coopmans, L. Wubben, F. Rozpedek, M. Pompili, A. Stolk, P. Pawelczak, R. Knegjens, J. de Oliveira Filho, R. Hanson, and S. Wehner, "A link layer protocol for quantum networks," in *SIGCOMM '19*, 2019.

[19] A. S. Cacciapuoti, M. Caleffi, R. V. Meter, and L. Hanzo, "When entanglement meets classical communications: Quantum teleportation for the quantum internet (invited paper)," 2019.

[20] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, "New high-intensity source of polarization-entangled photon pairs," *Phys. Rev. Lett.*, vol. 75, pp. 4337–4341, Dec 1995. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.75.4337

[21] W. J. Munro, K. Azuma, K. Tamaki, and K. Nemoto, “Inside quantum repeaters,” *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, no. 3, pp. 78–90, May 2015.

[22] W. J. Munro, A. M. Stephens, S. J. Devitt, K. A. Harrison, and K. Nemoto, “Quantum communication without the necessity of quantum memories,” *Nature Photonics*, vol. 6, no. 11, p. 777, 2012.

[23] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, “Quantum repeaters: the role of imperfect local operations in quantum communication,” *Physical Review Letters*, vol. 81, no. 26, p. 5932, 1998.

[24] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, “Fundamental limits of repeaterless quantum communications,” *Nature Communications*, vol. 8, no. 1, Apr 2017. [Online]. Available: http://dx.doi.org/10.1038/ncomms15043

[25] S. Pirandola, “End-to-end capacities of a quantum communication network,” *Communications Physics*, vol. 2, no. 1, pp. 1–10, 2019.

[26] M. Pant, H. Krovi, D. Towsley, L. Tassiulas, L. Jiang, P. Basu, D. Englund, and S. Guha, “Routing entanglement in the quantum internet,” *npj Quantum Information*, vol. 5, no. 1, pp. 1–9, 2019.

[27] S. Khatri, C. T. Matyas, A. U. Siddiqui, and J. P. Dowling, “Practical figures of merit and thresholds for entanglement distribution in quantum networks,” *Physical Review Research*, vol. 1, no. 2, Sep 2019. [Online]. Available: http://dx.doi.org/10.1103/PhysRevResearch.1.023032

[28] M. Chiani, “Method for sending classical data in quantum information processing systems and corresponding system,” Italian Patent, n. 102019000010797, July 2019.

[29] Alexandre Blais, Université de Sherbrooke, Québec, Canada, “Superconducting qubits,” 2015, http://www.quantum-lab.org/qip2015/slides/QIP2015-Alexandre%20Blais.pdf.

[30] R. Harper and S. T. Flammia, “Fault-tolerant logical gates in the ibm quantum experience,” *Physical Review Letters*, vol. 122, no. 8, Feb 2019. [Online]. Available: http://dx.doi.org/10.1103/PhysRevLett.122.080504