ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA
CAMPUS DI CESENA

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

SYNDROME-BASED PIGGYBACKING FOR QUANTUM NETWORKS

Elaborato in
Teoria dell'Informazione e Crittografia LM

Presentata da:
LORENZO DOMENICO
MAGNANI

Relatore:
Chiar.mo Prof. Ing.
MARCO CHIANI
Correlatori:
Prof. Ing.
ENRICO PAOLINI
Dott. Ing.
LORENZO VALENTINI

SESSIONE II
ANNO ACCADEMICO 2019-2020

Contents

Introduction

On October 29, 1969, at 10:30 am, the Leonard Kleinrock's team sent the first text message over a super tiny internet network, called the ARPANET. The team sent the letter "L" from the University of California (UCLA) to the Stanford Research Institute (SRI), and phoned the colleagues at SRI asking: "Which letter do you see?", they answered: "L". Then UCLA sent the letter "O", and SRI answered by phone: "O". When UCLA sent the "G", the computer at the SRI crashed. The complete word should have been "LOGIN". In the following two decades the ARPANET turned into internet, and from those days, the internet had a revolutionary impact on our world.

Nevertheless, the fledgling quantum information technologies undertake to provide a ground-breaking improvement, both in communications and computing fields. In the last decade, the quantum information has received a lot of interest, making the quantum internet an exciting topic, being now at the same early stage as the classical internet was in 1969.

A long-term vision on the quantum internet anticipates the potential applications, which would be impossible to implement using classical means. However, the quantum internet is thought to work in collaboration with the classical one. Some example of applications are quantum key distribution (QKD), which is provably secure,[1,2] extending the baseline of telescopes,[3] and clock synchronization.[4]

The security of quantum communications, as the quantum information technologies, are based on the laws of quantum mechanics, which describe the physical property of the nature on an atomic scale. Instead of looking at quantum systems purely as phenomena to be explained, quantum systems can be designed so that they can be controlled. Since it does not matter which is the physical support of the information, the basic idea is to associate the information with the state of a quantum particle. Controlling the state and exploiting the properties of the particles, efficient information

computations can be done. A machine that can do this is called quantum computer. Quantum computers work with quantum bits (qubits) instead of bits; a qubit represents the state of a quantum particle, so it represents the quantum information.

Unfortunately, qubits and the operations on them are intrinsically noisy. On one hand, classical gates have the property to regenerate the signal. In fact, despite possible large input variations, classical gates produce a clear two-level output. On the other hand, there are no information besides level 0 or 1. Conversely, before being measured, qubits carry a lot of information. As a consequence, variations on them, caused by noise in physical circuits, correspond to errors propagating across the quantum gates. Furthermore, any operation on qubits increases the noise level, and then, the probability of error.[5] Since the quantum computation is limited by noise, quantum algorithms must be designed to obtain a certain functionality using the least number of quantum gates. For practical reasons, the noisy level of each quantum computer is characterized by a parameter called Fidelity. The higher the Fidelity, the lower the error rate introduced by quantum computing.
Noise is not the only enemy; in fact, one of the main difficulties in realizing quantum computers is that quantum decoherence tends to destroy the information held by qubits.[1] This gives an insight about the central role of the quantum error correcting codes (QECC), and the need to use fault-tolerant quantum computation.[6,7]

Currently, few companies in the world have built their own quantum computer. For example IBM, Google, Microsoft, Alibaba, Rigetti and Honeywell built gate-based quantum computers. Nonetheless, many emerging spin-offs are looking to build their own quantum computer. In addition, the Canadian company D-Wave proposes quantum annealers, that are well suited to minimize multidimensional functions having a large number of local minima.[8]

Although building quantum computers is a very challenging task, quantum computation promises to solve problems that are untractable with classical computers. Many quantum algorithms have been developed for both gate-based computers and quantum annealers. These algorithms have found applications in many fields, like cryptography, chemistry, financial modelling, drug development, quantum systems simulations and optimization. A comprehensive catalog of quantum algorithms is available here: http://quantumalgorithmzoo.org/. A well-known task in which quantum computers are exponentially faster than classical one is to solve the prime factorization problem.[9] The Shor's Algorithm allows to solve this problem, and its

fundamental building block is the Quantum Fourier Transform (QFT). This algorithm undermines the security of the widely used RSA-based cryptography, which relies on the not yet demonstrated, but true so far conjecture that the prime factorization is an untractable problem for classical computers. Another well-known quantum algorithm is the Grover's Algorithm, which provides a quadratic speed up in finding a unique input to an unknown function, that produces a particular output.

These algorithms, like most of others, require a large number of high-quality qubits in order to be useful, likely requiring QECC far beyond the quantum resources available in known prototypical devices. In addition, the current inability to load large quantities of input data efficiently, suggests that many of these algorithms would be difficult to implement in practice.[5]

Despite the difficulties to building quantum computers, on October 2019 Google confirmed the "quantum supremacy" over classical computers. This is deemed as a milestone, and validates the theoretical anticipations about the efficiency of quantum computation. Using the 53-qubits quantum computer Sycamore, Google completed in about 200 seconds the task of sampling a million times the output of simulated pseudo-random quantum circuits. The state-of-the-art classical supercomputer counterpart would take approximately 10,000 years to complete the same task.[10]
On the other hand, IBM affirms that, although Google's experiment is an excellent demonstration of the progress in quantum computing, it should not be viewed as proof that quantum computers are "supreme" over classical computers. Indeed, as discussed in this link,[11] IBM claims that a simulation of the same task can be performed on a classical system in 2.5 days, and with far greater fidelity.

After this brief introduction, the aims of the present thesis are to introduce the fundamental quantum information concepts, discuss the main protocols allowing long-range quantum communications, and give a global view of the current companies involved in quantum computing. Furthermore, the piggybacking technique permitting to transmit classical information through quantum networks, without involving classical channel is investigated. The present work is organised as follows: in the chapter 1 the fundamental concepts on qubits and entanglement are addressed; while, in chapter 2, the communication protocols are discussed. The chapter 3 delves into the piggybacking technique, describing its implementation and experimental results. At last, the chapter 4 draws the conclusions. To give a global view of the quantum area of interest, the Appendix A reports the quantum solutions

proposed by the companies all over the world. Also, the Appendixes B, C, D and E provide further information about the covered topics.

Chapter 1

Fundamental Concepts of Quantum Information

According to the Copenhagen interpretation of quantum mechanics, the state of an isolated quantum system is completely characterized by its state vector. The state vector is a mathematical entity, and by using the Dirac notation, it is denoted as $|\psi\rangle$. For example, considering an isolated quantum system composed by a single electron. The quantum theory indicates that the spin of this electron is described by a state vector $|\psi\rangle \in \mathbb{C}^2$.
The time evolution of the state vector is described by the time dependent Schrödinger equation:

$$i\hbar\frac{\partial |\psi\rangle}{\partial t} = H |\psi\rangle \ . \tag{1.1}$$

Where i is the imaginary unit, $\hbar$ is the Planck's constant divided by 2π, H is the Hamiltonian hermitian operator for the closed system, and t is the time. This equation means that starting from a known state vector, it is possible to modify it as desired, by designing a proper Hamiltonian operator. This is the basis of quantum computation.

1.1 Single Qubit

As said in the introduction, the physical support for the information is the state of a quantum particle. For example, focusing on electron spin, the spin direction of this quantum particle is mathematically described by a state vector $|\psi\rangle$ in the two-dimensional Hilbert space. This state vector is a qubit, and is the basic unit element of the quantum information.
An important property of qubits is the superposition. This property is a fundamental principle in quantum mechanics and represents the main difference

between qubits and bits. Superposition is a linear combination of states, and an insight into this feature comes still thinking about the spin of an isolated single electron. Before the spin is observed, it can be up, it can be down, or it can be in a superposition of the two at same time. Mapping up and down into $|0\rangle$ and $|1\rangle$ respectively, the state vector associated to the spin of a single electron in a superposition state is:

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle \ . \tag{1.2}$$

Where α_0 and α_1 are complex numbers. The vectors $|0\rangle$ and $|1\rangle$ are the standard computational basis chosen as follows:

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

Note that $|0\rangle$ and $|1\rangle$ are an orthonormal basis for the two-dimensional Hilbert space. The physical meaning of the equation (1.2) is that, upon a measurement of the spin, the outcome probability of the state $|0\rangle$ is $|\alpha_0|^2$, (a 0 classical bit is obtained), and the outcome probability of the state $|1\rangle$ is $|\alpha_1|^2$ (a 1 classical bit is obtained). As a consequence, the equation (1.3) must hold:

$$|\alpha_0|^2 + |\alpha_1|^2 = 1 \, . \tag{1.3}$$

A complex number has two degrees of freedom, then, apparently, the degrees of freedom of the state vector are four. However, the equation (1.3) removes a degree of freedom, and with a mathematical manipulation, an irrelevant global phase turns out as follows:

$$|\psi\rangle = e^{i\gamma} \left[\cos\left(\frac{\theta}{2}\right) |0\rangle + e^{i\varphi} \sin\left(\frac{\theta}{2}\right) |1\rangle \right] \ . \tag{1.4}$$

Since the probabilities are related to the square of the absolute value, the global phase $e^{i\gamma}$ has no influence on the measurement of the qubit, and the equation (1.4) can be simply rewritten as:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right) |0\rangle + e^{i\varphi} \sin\left(\frac{\theta}{2}\right) |1\rangle \ . \tag{1.5}$$

Therefore, the state vector of a single qubit has two degrees of freedom, θ and φ.

Equation (1.5) leads to the Bloch sphere representation of the qubit. The Bloch sphere has a unitary radius, and the real numbers θ and φ define a point on the continuous sphere surface. Referring to figure 1.1, the north

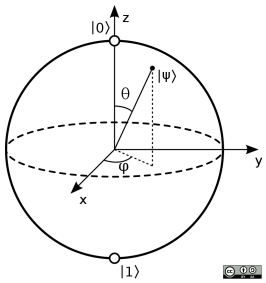

Figure 1.1: Bloch Sphere

and the south poles are typically chosen to correspond to the standard basis vector $|0\rangle$ and $|1\rangle$. The infinite states of a qubit can thus be represented mathematically by the state vector, or geometrically by the Bloch sphere. The electron spin is just an example of physical support for qubits. For the sake of completeness, in Appendix B some other examples of qubits physical implementations are reported.

1.2 Multiple Qubits

To implement the applications mentioned in the introduction, more than one qubit is required. Considering a two-qubit system, the state vectors of each qubit can be composed by using the Kronecker product, also called tensor product. For example:

$$\underbrace{|1\rangle}_{\text{First qubit}} \otimes \underbrace{|0\rangle}_{\text{Second qubit}} = |10\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} .$$

Due to the superposition, the state vector of the whole two-qubit system can be written as follows:

$$|\psi\rangle = \alpha_{00}\,|00\rangle + \alpha_{10}\,|10\rangle + \alpha_{01}\,|01\rangle + \alpha_{11}\,|11\rangle \ . \tag{1.6}$$

As for a single qubit, $|\alpha_i|^2$ is the probability to obtain the i^{th} vector basis upon a measurement, and $\sum_i |\alpha_i|^2 = 1$. More in general, the state vector of a quantum system composed by an arbitrary number n of qubits can be written as:

$$|\psi\rangle = \sum_{i \in \{0,1\}^n} \alpha_i\,|i\rangle \ . \tag{1.7}$$

This means that the state of an n-particle system is represented by a 2^n-dimensional Hilbert space.

1.3 Why qubits are so interesting?

Thinking about classical information, n bits can represent one of the 2^n possible combinations (state) at a time. On the other hand, using the qubits and exploiting the superposition, it is possible to create a state in which all the 2^n combinations are present at the same time. Looking for a particular combination, using classical computers no efficient algorithm is known. If no further information about the correct combination is provided, the only possible approach using classical computer is to try all the combinations, one by one. Conversely, using quantum computers, all the combinations can be checked at the same time, regardless of how big is n. Referring to the equation (1.7), the idea behind quantum computation is to harness the ability of nature to manipulate the exponential number of α_i's. This gives to quantum computing a huge advantage.

1.4 Quantum gates

According to the Schrödinger equation (eq. 1.1), a state vector can be manipulated by applying to it a proper unitary operator. Such unitary operators applied to qubits are called quantum gates, and are the building blocks of quantum circuits. The quantum gates are mathematically represented by unitary matrices, and operate on a small number of qubits. The principal quantum gates are represented by the four Pauli matrices I, X, Y and Z, which operate on a single qubit.

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

$$Y|0\rangle = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ i \end{bmatrix} = i|1\rangle \qquad Y|1\rangle = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} -i \\ 0 \end{bmatrix} = -i|0\rangle$$

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

Note that X, Y, and Z provide a rotation of π radians about the relative axes of the Bloch sphere. I is the identity matrix and it does nothing when applied to a qubit.

Among the single-qubit gates, probably the most important one is the Hadamard gate. Starting from a standard computational basis, i.e. $|0\rangle$ and $|1\rangle$, it gives a superposed state in which any outcome, upon a measurement, has the same probability. More precisely:

$$H|0\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\ 1\end{bmatrix} = \frac{|0\rangle+|1\rangle}{\sqrt{2}} = |+\rangle$$

$$H|1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}0\\ 1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\ -1\end{bmatrix} = \frac{|0\rangle-|1\rangle}{\sqrt{2}} = |-\rangle\ .$$

Note that the states $|+\rangle$ and $|-\rangle$ are an orthonormal basis for the two-dimensional Hilbert space, so they are an alternative computational basis.

Furthermore, two-qubit gates and three-qubits gates exist too. They are very useful in quantum circuits as they allow to perform controlled operations on qubits. The controlled X gate, also called CNOT, applies the X gate on the target qubit only if the control qubit is $|1\rangle$, leaving unchanged the control qubit; otherwise it does nothing. It follows an example of the CNOT gate operation, in which the control qubit on the left and the target qubit is on the right:

$$CNOT|10\rangle = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}\begin{bmatrix}0\\ 0\\ 1\\ 0\end{bmatrix} = \begin{bmatrix}0\\ 0\\ 0\\ 1\end{bmatrix} = |11\rangle\ .$$

More in general: $CNOT|a,b\rangle = |a, a \oplus b\rangle$ with $a, b \in \{0,1\}$.
Another two-qubit gate is the controlled Z gate. It applies the Z gate on the target qubit only if the control qubit is $|1\rangle$, leaving unchanged the control qubits; otherwise it does nothing.

Finally, the Toffoli gate, sometimes referred as CCNOT, works on three qubits. It applies the X gate to the target qubit only if the two control qubits are both $|1\rangle$, leaving unchanged the control qubit; otherwise it does nothing.

1.5 Bell pairs

Qubits are profoundly different from bits. If the aforementioned superposition property sounds weird, the entanglement property could leave stunned. Let us consider a two-qubit system, and apply to it the simple quantum circuit shown in figure 1.2. The first gate is the Hadamard gate and the second is the CNOT gate.

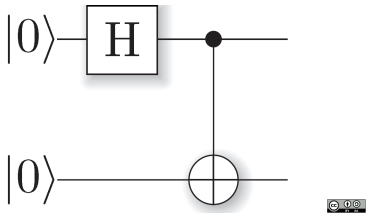

Figure 1.2: Quantum circuit to generate the Bell pair $|\Phi^+\rangle$

Starting with all qubits in the state $|0\rangle$, the initial state vector $|\psi\rangle = |00\rangle$ evolves as follows:

$$|\psi\rangle = |00\rangle \xrightarrow{\text{H}} \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)|0\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |10\rangle\right)$$
$$\xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) = |\Phi^+\rangle \ . \tag{1.8}$$

The state $|\Phi^+\rangle$ is a Bell pair, and the other Bell pairs $|\Phi^-\rangle$, $|\Psi^+\rangle$, $|\Psi^-\rangle$ can be obtained starting with the states $|10\rangle$, $|01\rangle$, $|11\rangle$, respectively. The Bell pairs, also called EPR states, represent entangled states.

The entanglement is a strong correlation that allows qubits to express higher correlation than it is possible in classical systems. Mathematically, the state of two (or more) quantum systems, is considered an entangled state if it is not factorizable into two (or more) independent states. For example, focusing on the $|\Phi^+\rangle$ Bell pair, since it is an entangled state, it is impossible to find two quantum states $|a\rangle$, $|b\rangle$ such that $|\Phi^+\rangle = |a\rangle \otimes |b\rangle$. In other words, an entangled state is not a composite state. To prove this statement it is possible to compose two quantum states, $|a\rangle = a_0|0\rangle + a_1|1\rangle$ and $|b\rangle = b_0|0\rangle + b_1|1\rangle$, resulting in

$$\begin{aligned} |a\rangle \otimes |b\rangle &= (a_0|0\rangle + a_1|1\rangle) \otimes (b_0|0\rangle + b_1|1\rangle) \\ &= a_0b_0|00\rangle + a_0b_1|01\rangle + a_1b_0|10\rangle + a_1b_1|11\rangle \ . \end{aligned}$$

To obtain the Bell pair $|\Phi^+\rangle$ it is necessary to keep only the states $|00\rangle$ and $|11\rangle$. Then, $a_0, b_0, a_1, b_1 \neq 0$. However, this latter condition keeps also the states $|01\rangle$ and $|10\rangle$, showing that it is impossible to obtain the Bell pair by composing two quantum states. This holds for all Bell pairs, and proves that an entangled state composed by two qubits is not factorizable into two independent qubits.

Looking at the equation (1.8), since the α coefficients are all equal to $1/\sqrt{2}$, upon a measurement of the first qubit, both the states $|0\rangle$ or $|1\rangle$ have the same outcome probability 1/2. However, despite the uncertainty about the outcome, the knowledge about the first qubit implies the knowledge of the second qubit, instantaneously. E.g. if the outcome of the first qubit measurement is $|1\rangle$, instantaneously the state of the second qubit must be $|1\rangle$ with probability 1. It does not matter which qubit is measured first, and how physically far the two qubits are from each other.

1.6 CHSH Test

Two qubits can show a level of correlation unreachable by classical bits. Indeed, by testing the maximum correlation reached by two systems, it is possible to declare whether they are quantum systems or not. To this purpose, the CHSH test can be performed in form of game, playing it by using bits or qubits. Let A and B be two classical systems, and let the bits $x \in \{0,1\}$ and $y \in \{0,1\}$ be the inputs of A and B respectively. Each possible combinations of x and y has the same probability of outcome, which is 1/4. Moreover, the outputs of A and B are represented by $a \in \{0,1\}$ and $b \in \{0,1\}$ respectively. To win the game, A and B must accomplish the condition $x \cdot y = a \oplus b$. Since A and B are two isolated systems, A guesses the output a knowing only its input x. Similarly, B guesses the output b knowing only its input y. The goal of the game is to maximise the probability of winning p_{win}, expressed as follows:

$$p_{win} = Pr\{x \cdot y = a \oplus b\}\,. \tag{1.9}$$

Let a_0 and a_1 be the outputs of A when $x = 0$ and $x = 1$ respectively. Also, b_0 and b_1 are the outputs of B when $y = 0$ and $y = 1$ respectively. Referring to table 1.1, in the first row the winning condition is accomplished if $a_0 = b_0$. In the second row, it is necessary that $a_0 = b_1$, then $a_0 = b_0 = b_1$. Also, in the the third row, it needs that $a_1 = b_0$, then $a_0 = b_0 = b_1 = a_1$. Since the fourth row requires $a_1 \neq b_1$, in this case it is impossible to win. Hence, the maximum probability of winning is $p_{win} = 3/4 = 0.75$.[12]

x	y	$x \cdot y$	$= a \oplus b$
0	0	0	$= a_0 \oplus b_0$
0	1	0	$= a_0 \oplus b_1$
1	0	0	$= a_1 \oplus b_0$
1	1	1	$= a_1 \oplus b_1$

Table 1.1: Classical CHSH test

By switching to the quantum case, A and B are quantum systems able to measure qubits in different bases. In this quantum case, A and B share a Bell pair. Referring to figure 1.3, if $x = 0$, A measures in the basis $\{|0\rangle, |1\rangle\}$, producing the outputs $a = 0$ when the measure outcome is $|0\rangle$ and $a = 1$ when the outcome is $|1\rangle$. If $x = 1$, A measures in the basis $\{|+\rangle, |-\rangle\}$, producing the outputs $a = 0$ or $a = 1$ respectively. As for B, if $y = 0$, it measures in a basis rotated of $\pi/8$ with respect to $\{|0\rangle, |1\rangle\}$, producing the outputs $b = 0$ or $b = 1$, and if $y = 1$, B measures in a basis rotated of $-\pi/8$ with respect to $\{|0\rangle, |1\rangle\}$, producing the outputs $b = 0$ or $b = 1$ as indicated in figure.
Since for entangled pairs the rotation invariance property holds, neglecting the multiplicative factor, the quantum state shared by A and B is described as $|00\rangle + |11\rangle = |++\rangle + |--\rangle$. The system A holds the first qubit and B holds the second one. Furthermore, after the A measurement, the quantum state is leaved in one of the A bases elements, then, the probability that B accomplishes the condition to win is always $\cos^2 \frac{\pi}{8}$.
This can be showed by writing two quantum states $|\psi\rangle$ and $|\varphi\rangle$, one rotated of $\pi/8$ with respect to the other, as follows:

$$|\psi\rangle = \cos\theta\,|0\rangle + \sin\theta\,|1\rangle$$
$$|\varphi\rangle = \cos(\theta + \frac{\pi}{8})\,|0\rangle + \sin(\theta + \frac{\pi}{8})\,|1\rangle\ .$$

By measuring the state $|\psi\rangle$ in the basis $\{|\varphi\rangle, |\varphi^{\perp}\rangle\}$, the probability to obtain $|\varphi\rangle$ is the squared module of the projection of $|\psi\rangle$ on $|\varphi\rangle$, i.e. the squared module of the inner product $|\langle\varphi|\psi\rangle|^2$. By using the trigonometric identity $\sin\sigma\sin\gamma = \cos(\sigma - \gamma) - \cos\sigma\cos\gamma$, this probability can be expressed as follows:

$$|\langle\varphi|\psi\rangle|^2 = \left|\cos(\theta + \frac{\pi}{8})\cos\theta + \sin(\theta + \frac{\pi}{8})\sin\theta\right|^2 = \cos^2\frac{\pi}{8} \approx 0.85\,.$$

To conclude, the CHSH test provides a probability of winning $p_{win} > 0.75$. Therefore, using two quantum systems the correlation between them is greater than any possible correlation achievable with classical systems. Hence, this is a proof of quantumness.

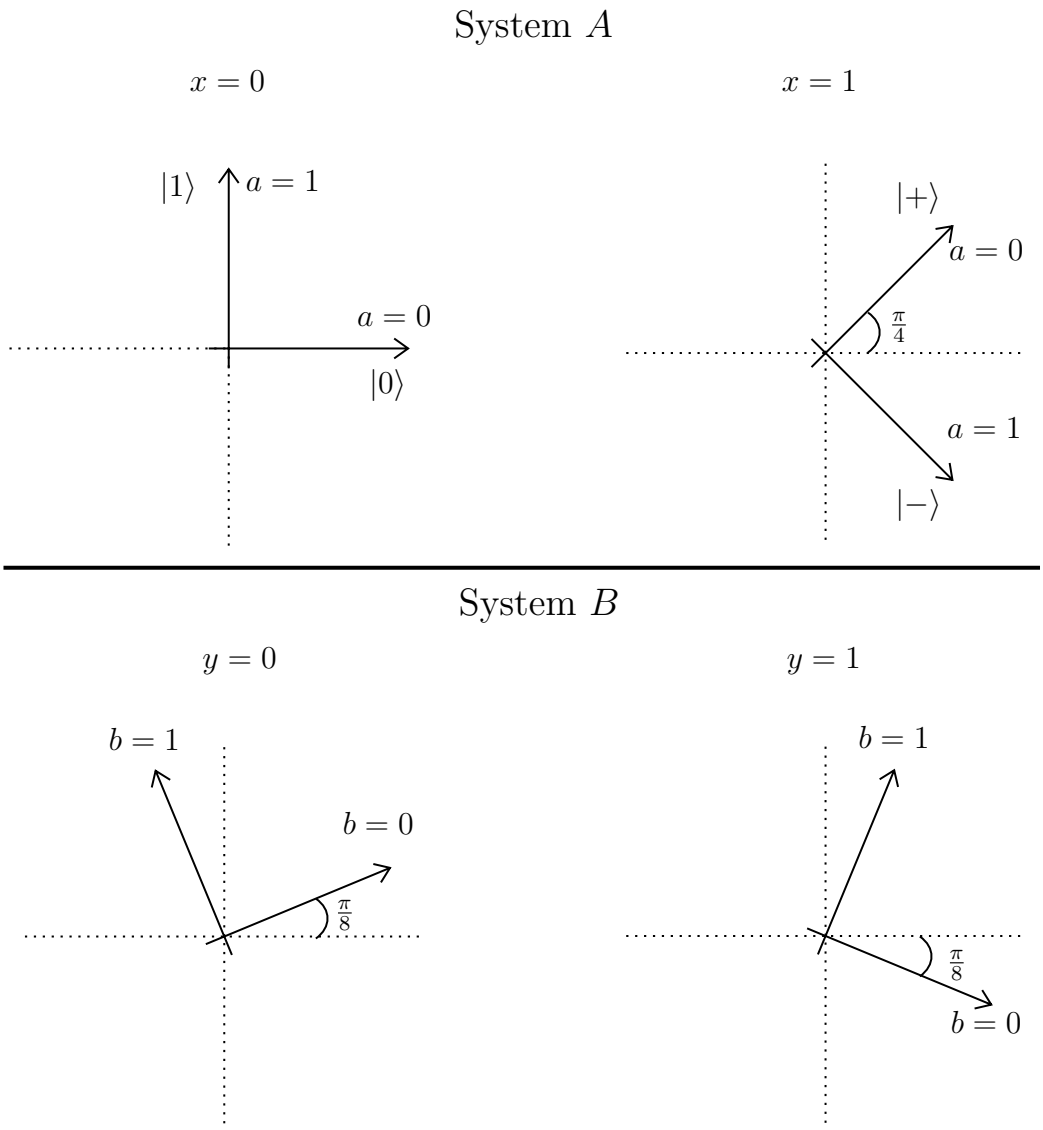

Figure 1.3: Measurement bases for quantum CHSH test

Chapter 2

Quantum Internet

The quantum internet is a communication network, that enables quantum communications among remote quantum nodes. The quantum internet is composed by a set of new technologies, which support functionality with no direct counterpart in the classical internet. Such technologies involve many disciplines like physics, electronic engineering, telecommunication and computer science. One of the biggest challenges in making quantum computers and quantum internet, is to combine these fields by creating multidisciplinary knowledge.

2.1 From qubits to quantum internet

Qubits can not be copied.[13] This is stated by the no-cloning theorem, and it represents a fundamental aspect of quantum information. To prove this theorem, suppose that it exists a unitary operator U able to copy a qubit. The inputs of U are the qubit to copy $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$ and the qubit $|s\rangle$, which is, for example, one element of the standard basis that U must transform into $|\psi\rangle$. Therefore, it should be $U|0\rangle \otimes |s\rangle = |0\rangle \otimes |0\rangle$ and $U|1\rangle \otimes |s\rangle = |1\rangle \otimes |1\rangle$. Then, for linearity, by coping $|\psi\rangle$ the outputs of U will be the two qubits expressed as follows:

$$\begin{aligned} U[(\alpha_0 |0\rangle + \alpha_1 |1\rangle) \otimes |s\rangle] &= \alpha_0 U |0\rangle \otimes |s\rangle + \alpha_1 U |1\rangle \otimes |s\rangle \\ &= \alpha_0 U |0s\rangle + \alpha_1 U |1s\rangle = \alpha_0 |00\rangle + \alpha_1 |11\rangle \ . \end{aligned} \tag{2.1}$$

Actually, the correct output should have been

$$\begin{aligned} |\psi\psi\rangle &= (\alpha_0 |0\rangle + \alpha_1 |1\rangle)(\alpha_0 |0\rangle + \alpha_1 |1\rangle) \\ &= \alpha_0^2 |00\rangle + \alpha_0\alpha_1 |01\rangle + \alpha_1\alpha_0 |10\rangle + \alpha_1^2 |11\rangle \ . \end{aligned} \tag{2.2}$$

The equation 2.1 is equal to the equation 2.2 only if $\alpha_0 = 1, \alpha_1 = 0$ or $\alpha_0 = 0, \alpha_1 = 1$, proving that only the basis elements can be coped. In other words, it proves that it is impossible to make independent copies of an unknown quantum state.

The no-cloning theorem makes qubit well suited for security applications, like secure communications and secure access to remote quantum computers in the cloud. Moreover, any attempt to copy a qubit can be detected.[14] The best-known application is QKD, which enables two nodes to share a secret key, whose security relies on the laws of quantum mechanics.
Another exclusive feature of qubits is the aforementioned quantum entanglement. Entanglement is a strong correlation between two particles, which can not be shared with any other particle. These two particles could be, for example, photons, which in turns represent two entangled qubits. This feature matches with applications that require coordination; as, for example, clock synchronization, leader election and efficient agreement on distributed data. It is remarkable that these applications are out of reach for the classical internet. Since it is impossible for any third qubit to be entangled with two already maximally entangled qubit, entanglement is an inherently private feature. Hence, the entanglement is well suited for secure identification applications too.[14] Quantum internet is a new subject area, requiring new concepts and new technologies, therefore, it is currently hard to predict all its possible applications. Nevertheless, some other applications leveraging it are discussed in the literature, like quantum sensor network, byzantine agreement for distributed systems and quantum metrology.[14]

2.2 Communicating qubits

To communicate qubits from one place to another is the foundation of the quantum internet. However, due to the nature of qubit, transmitting them over long distances is a huge challenge. Because of qubits can not be copied, or amplified, the classical signal repetition can not be used to extend the communication range. Building quantum internet leads to redefine the internet elements. Beginning from a simple division, three hardware elements are needed:

- Quantum channels
- Quantum repeaters
- Quantum end nodes

The quantum channel is the physical layer, i.e. the physical connection, which typically consists of optical fiber. Fibers are already in use today, therefore the deployment of new physical connections is not required. However, quantum channels are inherently lossy. For example, fiber transmissivity scales down exponentially with distance. As a consequence, in order to reach long distances, an intermediate quantum element is needed, namely, the quantum repeater. Finally, the end nodes must be able to manipulate, send and receive qubits.

2.2.1 Teleportation

Teleportation is a protocol used to transmit quantum information. The main idea of teleportation is to send an unknown data qubit from the transmitter to the receiver, exploiting the entanglement. Teleportation does not care about how the entanglement is created. Indeed, the starting point of the protocol is one of the four Bell pairs. For example:

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

in which each qubit is named communication qubit. The communication qubits can be, for example, the representation of two photons in an entangled state. The two communication qubits, after being created, are separated, and each of them are sent to one end node. One might wonder if, due to the physical distance, the two photons are still strongly correlated or not. Anyway, the answer is yes, they are.[15]

Referring to figure 2.1, the transmitter (A end node) starts the teleportation manipulating two qubits: the data qubit $|\psi\rangle_A$, and the communication qubit $|\Phi^+\rangle_A$, which is entangled with the receiver (B end node) communication qubit $|\Phi^+\rangle_B$. The transmitter performs a Bell State Measurement on the data qubit and the communication qubit, sending the result to the receiver. The results of measurements are classical bits, thus a classical channel is required. This is an example of why the quantum internet is thought as an enhancement of the classical internet. Indeed, there are a lot of quantum protocols that enable new quantum applications, but typically they need a classical internet channel too.
As shown in figure 2.1, the receiver applies X and/or Z gates to its communication qubit, only if the control classical bit is 1, getting the data qubit $|\psi\rangle_B = |\psi\rangle_A$.[1] Note that the teleportation does not need information about the data qubit. It destroys the state of the data qubit at the sender, and recreates that state at the destination, teleporting information rather than matter. In other words, teleportation moves quantum information, rather

than transmitting it.[16]

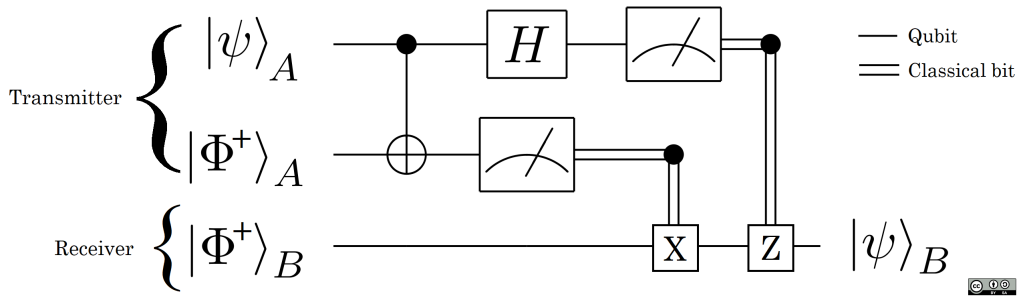

Figure 2.1: Quantum teleportation circuit

A proof of the teleportation protocol is provided by describing the state evolution of the system showed in figure 2.1. Considering an unknown data qubit $|\psi\rangle_A = \alpha_0 |0\rangle + \alpha_1 |1\rangle$, the initial state of the system is expressed as:

$$|\psi\rangle_A \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}} [\alpha_0 |0\rangle (|00\rangle + |11\rangle) + \alpha_1 |1\rangle (|00\rangle + |11\rangle)] .$$

After the CNOT gate, the state evolves as:

$$\frac{1}{\sqrt{2}} [\alpha_0 |0\rangle (|00\rangle + |11\rangle) + \alpha_1 |1\rangle (|10\rangle + |01\rangle)] .$$

The next step is to apply the Hadamard gate to the data qubit, and the state can be expressed as:

$$\begin{gathered}
\frac{1}{2} [\alpha_0(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \alpha_1(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)] = \\
\frac{1}{2} [\alpha_0(|000\rangle + |011\rangle + |100\rangle + |111\rangle) + \alpha_1(|010\rangle + |001\rangle - |110\rangle - |101\rangle)] = \\
\frac{1}{2}[|00\rangle (\alpha_0 |0\rangle + \alpha_1 |1\rangle) + |01\rangle (\alpha_0 |1\rangle + \alpha_1 |0\rangle) + \\
|10\rangle (\alpha_0 |0\rangle - \alpha_1 |1\rangle) + |11\rangle (\alpha_0 |1\rangle - \alpha_1 |0\rangle)] .
\end{gathered}$$

The measurement of the first two qubits determines the state of the third qubit, i.e. the data qubit at the receiver. Also, the measurement determines which gate the receiver must apply to correct the state. The four possible

outcomes are described as follows:

$$\begin{aligned}
00 &\rightarrow \alpha_0 |0\rangle + \alpha_1 |1\rangle &&\longrightarrow && |\psi\rangle_B = \alpha_0 |0\rangle + \alpha_1 |1\rangle \\
01 &\rightarrow \alpha_0 |1\rangle + \alpha_1 |0\rangle &&\xrightarrow{\mathrm{X}} && |\psi\rangle_B = \alpha_0 |0\rangle + \alpha_1 |1\rangle \\
10 &\rightarrow \alpha_0 |0\rangle - \alpha_1 |1\rangle &&\xrightarrow{\mathrm{Z}} && |\psi\rangle_B = \alpha_0 |0\rangle + \alpha_1 |1\rangle \\
11 &\rightarrow \alpha_0 |1\rangle - \alpha_1 |0\rangle &&\xrightarrow{\mathrm{ZX}} && |\psi\rangle_B = \alpha_0 |0\rangle + \alpha_1 |1\rangle
\end{aligned}$$

This shows that the received is always able to reconstruct the correct data qubit, proving the teleportation protocol.

2.2.2 Entanglement swapping

In order to teleport data qubits, entangled pairs of communication qubits are needed. As said before, fiber are lossy, and photons can be lost. Furthermore, the greater the distance, the greater the probability that the photons detector apparatus may not detect the incoming photon. To handle this problem, quantum repeaters are placed along the path of the fiber connection, so that each single link has its private entangled pair. However, the two end nodes are not entangled. Entanglement swapping allows to overcome this latter problem, ending up with an entangled pair between the two end nodes. This means, at least in theory, that it is possible to perform a teleportation of an unknown data qubit over arbitrary long distances.
Referring to figure 2.2, each end node shares a Bell pair with the repeater. To perform the entanglement swapping, the repeater operates a Bell State Measurement on its two qubits, after that it sends the classical bits to the respective end node. Finally, the A end node corrects its qubit by applying the Z gate if it receives a classical bit equal to 1; similarly, the B end node corrects its qubit applying the X gate if it receives a classical bit equal to 1. Notice that classical channels are needed for the entanglement swapping too.[1,16]

A proof of the entanglement swapping protocol is provided by describing the state evolution of the system showed in figure 2.2. The initial state of the system is expressed as:

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{2}(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle)\,.$$

By applying the CNOT gate, the state evolves as:

$$\frac{1}{2}(|0000\rangle + |0011\rangle + |1110\rangle + |1101\rangle)\,.$$

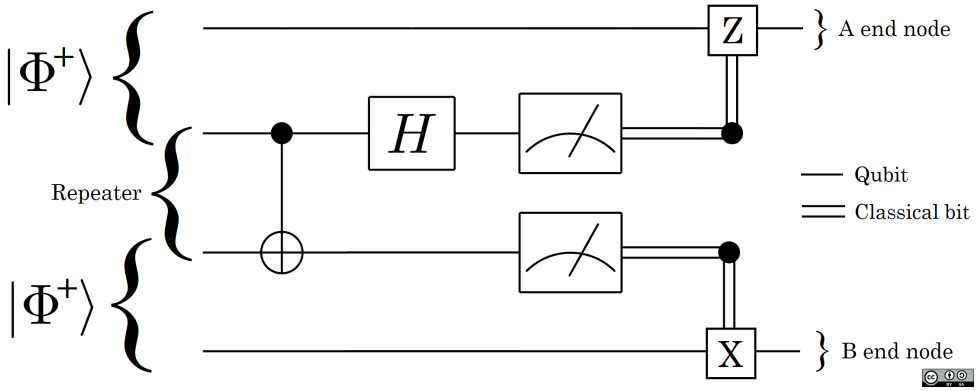

Figure 2.2: Entanglement swapping circuit

Next, the Hadamard gate is applied to the second qubit

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

The repeater measures its two qubits, i.e. the second and the third qubit. The measurement determines the state of the A end node, i.e. the first qubit, and the state of the B end node, i.e. the fourth qubit. Also, depending on measurement outcomes, A and B apply $Z^{(A)}$ and $X^{(B)}$ gates on their qubit respectively. The four possible measurement outcomes are described as follows:

$$\begin{aligned}
00 \quad &\rightarrow \quad \frac{1}{\sqrt{2}}(|0\rangle|0\rangle+|1\rangle|1\rangle) \quad \longrightarrow \quad \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle=|\Phi^+\rangle\\
01 \quad &\rightarrow \quad \frac{1}{\sqrt{2}}(|0\rangle|1\rangle+|1\rangle|0\rangle) \quad \xrightarrow{X^{(B)}} \quad \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle=|\Phi^+\rangle\\
10 \quad &\rightarrow \quad \frac{1}{\sqrt{2}}(|0\rangle|0\rangle-|1\rangle|1\rangle) \quad \xrightarrow{Z^{(A)}} \quad \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle=|\Phi^+\rangle\\
11 \quad &\rightarrow \quad \frac{1}{\sqrt{2}}(|0\rangle|1\rangle-|1\rangle|0\rangle) \quad \xrightarrow{Z^{(A)}X^{(B)}} \quad \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle=|\Phi^+\rangle
\end{aligned}$$

This shows that A and B always end up with a shared Bell pair, proving the entanglement swapping protocol.
In a more complex scenario, where many quantum repeaters must be used,

the entanglement swapping can be done in parallel. For example, if the communication, due to the distance, needs to use three repeaters R_1, R_2, and R_3, the entanglement swapping on R_1 and R_3 can be executed in parallel. Afterwards, the repeater R_2 completes the process executing the swapping, so that a shared entangled pair between the two end nodes is created in only two steps.

2.2.3 QECC-based communication protocols

Entanglement swapping and teleportation allow quantum communication over long distances. These protocols rely on existing techniques to create and support entanglement across a link. Creating the physical entanglement is a probabilistic mechanism, therefore an acknowledgement indicating which attempt succeeded is needed. Although so far the entanglement is thought as a service on-demand, as it is consumed by the teleportation, a possible solution is to create a continuous stream of Bell pairs between end nodes and repeaters.[16] Nevertheless, resource management may be more difficult in this approach.

Alternatively, QECC-based protocols can also be used to communicate quantum information. In this approach, the qubits holding the quantum information are called logical qubits and, as in the classical case, they are encoded into a greater number of qubits, called physical qubits. The role of the added qubits is to protect the quantum information against noise, since the physical qubits are sent through the channel. On the other side, the receiver waits for the physical qubits, storing them as they arrive. Finally, it decodes them, getting the original logical qubits.
Since the quantum channels are lossy, and the longer the channel, the greater the probability of error, large-scale QECCs should be employed to communicate qubits over long distances. This implies the ability to store many qubits; but currently, making good quantum memories, that store qubits for a useful period of time, is a very challenging task. As a consequence, the QECC approach also requires to divide the quantum channel into many low-loss segments, introducing the quantum repeaters.[17] Therefore, using the QECCs, the repeater decodes the received physical qubits getting the original logical ones. After that, it re-encode the logical qubits, sending the physical ones to the next repeater or to the end node. As a result, although the quantum channel noise could modify some physical qubits, leveraging the code capability to correct errors the quantum information gets through the steps, reaching the receiver end node unchanged. It is worth noting that the

QECC approach needs neither entanglement nor a classical channel.

2.3 Classification of Quantum Repeaters

The different approaches to communicate qubits over long distances involve quantum repeaters and quantum gates. Entanglement swapping and teleportation require Bell State Measurements, while QECCs require encoding and decoding blocks. As a consequence, both quantum channels and quantum gates could introduce errors. Depending on different strategies to deal with errors, quantum repeaters can be classified into three categories.
The first generation (1G) of quantum repeaters suppresses the quantum-channel errors by implementing the entanglement swapping and teleportation approach. Also, they suppress the quantum-gate errors by means of entanglement purification. In this latter protocol, multiple low-fidelity Bell pairs are consumed to probabilistically generate a smaller number of higher-fidelity Bell pairs.[16] The second generation (2G) of quantum repeaters, although it suppresses quantum-channel errors as the 1G does, it suppresses quantum-gate errors by implementing QECCs. Thereby, 2G repeaters share Bell pairs to communicate encoded states fault-tolerantly prepared using, for example, the Calderbank-Shor-Steane (CSS) code. Finally, the third generation (3G) of quantum repeaters implements QECCs to suppress both errors types.
Since these three generations need different hardware from each other, they should not be viewed as one better than another, but rather as different methods to suppress loss and operation errors. In fact, currently is not clear which quantum repeater generation is more suitable for the different applications mentioned above. Nevertheless, a possible idea is to integrate different generations to achieve a universal and secure quantum internet.[18]

2.4 Interim conclusion

Summing up, the basic concepts about qubits, their gate-based manipulation and how to transmit them have been discussed in these first two chapters. By composing the fundamental quantum gates, it is possible to create algorithms that run on quantum computer; and as for the quantum communications, thanks to quantum repeaters, the qubits can be transmitted from one end node to another over long distances, using different approaches. In order to design a quantum network, the next step is to tackle the problem of qubits routing. For this reason, the focus of this thesis is to analyse this problem, and propose a possible solution.

Chapter 3

Piggybacking Technique

Quantum repeaters are the key elements that enable to communicate qubits over long distances. As described in the section 2.2, to perform the entanglement swapping and teleportation protocols, the quantum repeaters must be able to manipulate and measure qubits. Alternatively, employing the QECC approach, quantum repeaters must be able to store and manipulate qubits. So far the dissertation has referred to a single quantum link, however, in a quantum network scenario, each quantum end node should be able to communicate with everyone else, and this means that quantum repeaters must also implement router functionality.

For example, consider the simple network showed in figure 3.1. To send a data qubit from the end node A to the end node B, how can the repeater R1 be notified to forward the traffic toward B, instead of to repeater R2?
If the entanglement swapping and teleportation approach is employed, a possible way to properly route the traffic is to establish the path before sending the data qubit. Therefore, using the classical channel, A informs the repeater R1 that the destination is the end node B; thereby, as shown in figure 3.2, R1 operates the entanglement swapping over the right pair of communication qubits, establishing the entanglement between A and B. For the sake of clarity, it is assumed that the repeaters know the network topology. Afterwards, exploiting the end-to-end entanglement, the teleportation protocol can transmit the data qubit over the right path.
Conversely, using the QECC approach, the classical channel is not required to send qubits. By adopting this approach, in combination with the piggybacking technique (described in the following section 3.2), the classical information about the destination can be put over the quantum stream, allowing not to involve the classical channel.[19] Following the previous example, A encodes the qubits to be transmitted, and piggybacks on them the classi-

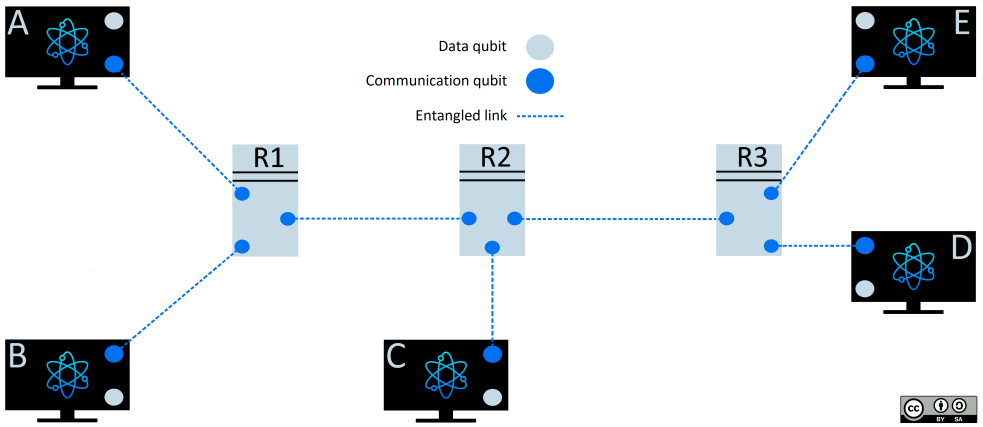

Figure 3.1: Example of a simple quantum network
(the repeaters do not route qubits)

cal information about the destination; then, it sends the quantum stream to R1 through the quantum channel. After receiving the stream, R1 can read the classical information and find out to forward the qubits to B. Finally, B can decode the qubits, retrieving the quantum information sent by A. It is worth noting that this technique has the remarkable property of leaving the quantum information unchanged.[19]

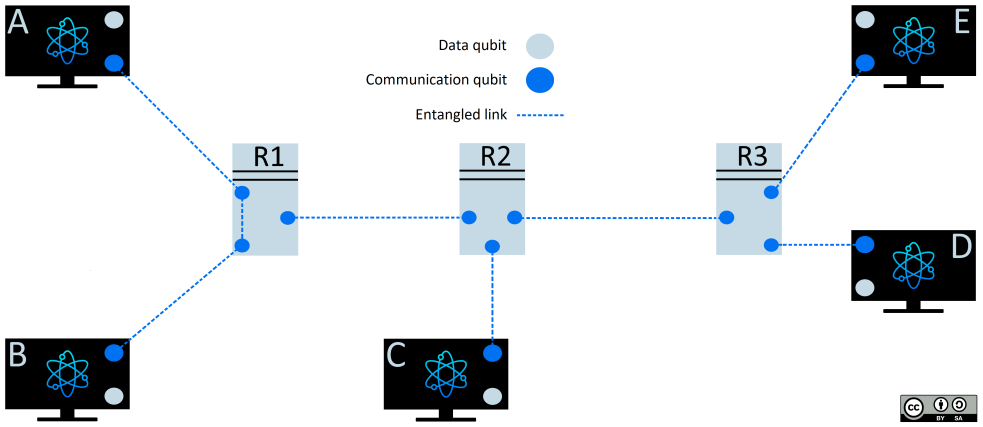

Figure 3.2: Example of a simple quantum network
(the repeater R1 routes qubits)

By performing many times the processes described above, qubits can be routed through many quantum repeaters, allowing all end nodes to communicate with any other. Although in both approaches the routing can be done,

the ability to transmit and route qubits without using the classical channel is very attracting. For this reason, the piggybacking technique is analysed in detail.

3.1 Stabilizer Formalism and Stabilizer Codes

Referring to classical linear block codes, an efficient way to decode them is to use the error syndrome. In the case of QECCs, the usage of error syndrome is still possible; however, a new formalism is needed. This formalism is called stabilizer formalism and it is based on group theory. The group of principal interest is the Pauli group $\mathcal{G}_n$ on n qubits, composed by all the n-fold tensor products of the four Pauli operators, together with the multiplicative factors ± 1 and $\pm i$. These factors ensure that $\mathcal{G}_n$ is closed under multiplication, and thus forms a legitimate group. The simplest example is the Pauli group on a single qubit, which is defined as follows:

$$\mathcal{G}_1 \stackrel{\text{def}}{=} \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\} \equiv \langle X, Y, Z \rangle .$$

Consider a subgroup of $\mathcal{G}_n$, called $\mathcal{S}$, whose elements commute and do not contain $(-I)$. The n-qubits states $|\psi\rangle$ that satisfy the equation (3.1) form the vector space $\mathcal{V}_s$ stabilized by $\mathcal{S}$, and $\mathcal{S}$ is said to be the stabilizer of the vector space $\mathcal{V}_s$.

$$\mathcal{S}_i |\psi\rangle = |\psi\rangle \qquad i = 1, 2, ..., |\mathcal{S}| . \tag{3.1}$$

A clever and compact way to express a group, or a subgroup, is by using its generators $G_1, ..., G_l$. The generator set has at most $log(|\mathcal{G}|)$ elements, and all the items of the group can be expressed as a product of elements in the list $G_1, ..., G_l$. As a consequence, the equation 3.1 can be simplified as:[1]

$$G_i |\psi\rangle = |\psi\rangle \qquad i = 1, 2, ..., l . \tag{3.2}$$

Consider a Pauli group $\mathcal{G}_n$ and a set of $n-k$ generators $G_i \in \mathcal{G}_n$. Let these generators create a subgroup whose elements commute and do not contain $(-I)$. Thereby, the stabilizer code $\mathcal{C}$ is defined as the set of quantum states $|\psi\rangle$ satisfying the equation 3.2, where $l = n - k$.
Given an $[[n, k]]$ QECC, and referring to figure 3.3, a k-qubit quantum state $|\varphi\rangle$ is encoded in an n-qubit quantum codeword (q-codeword) $|\psi\rangle \in \mathcal{C}$. Notice that the single lines are used for qubits, and double lines for bits. Afterwards, the q-codeword is sent through the quantum channel which, in turn,

could introduce an error $E \in \mathcal{G}_n$. As for the quantum error correction, the received state $E|\psi\rangle$ is measured according to the generators $G_1, ..., G_{n-k}$, resulting in an error syndrome $s(E) = (s_1, s_2, ..., s_{n-k})$. Mathematically, $s_i = \langle\psi| E^\dagger G_i E |\psi\rangle$ where $s_i = \pm 1$, i.e. s_i is one of the two eigenvalues of G_i. Finally, the syndrome is mapped into classical bits following the convention $+1 \to 0, \quad -1 \to 1$. It worth highlighting that the syndrome depends only on the error E and not on $|\psi\rangle$; and the measurement of the syndrome can be done leaving the state $E|\psi\rangle$ unchanged.
Since the possible syndromes are $m = 2^{n-k}$, let $\mathcal{S} = \{s^{(1)}, s^{(2)}, ..., s^{(m)}\}$ be the set of possible syndromes, and $\mathcal{Q} = \{Q^{(1)}, Q^{(2)}, ..., Q^{(m)}\}$ the set of the operators corresponding to the errors that can be corrected. Thanks to the stabilizer formalism, the quantum decoder, upon the measure of the syndrome $s^{(i)}$, applies the recovery quantum operator $Q^{(i)\dagger}$ to produce a valid q-codeword.[19]

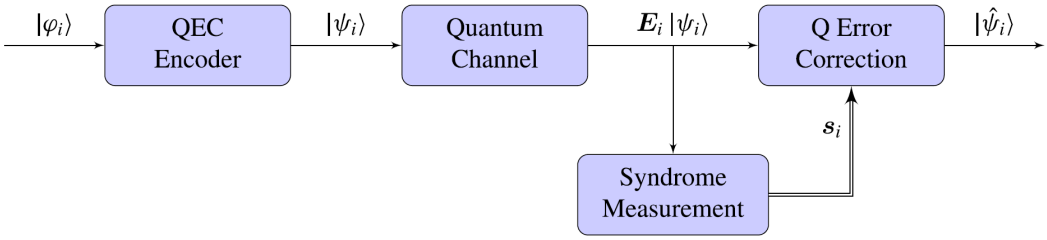

Figure 3.3: Quantum link employing quantum error correction (QEC) based on error syndrome (figure from[19])

3.2 Piggybacking in Noiseless Quantum Channel Conditions

The basic idea of the piggybacking technique is to introduce an intentional error after the encoding process. Referring to figure 3.4, the transmitter encodes the state $|\varphi_i\rangle$ in the state $|\psi_i\rangle$, and then it applies an operator $P_i \in \mathcal{Q}$ on $|\psi_i\rangle$ introducing an intentional error on the q-codeword. Thereby, since $E = I$, when the receiver measures the syndrome $\hat{s}_i = s(P_i) = s_i$, it gets the $n - k$ classical bits that have been put on the q-codeword as intentional error by the transmitter. Consequently, mapping s_i in the relative intentional error P_i, the receiver can apply the operator $P_i^\dagger$ to reconstruct the original q-codeword. Note that here the subscript i is a time index.
Consider for example a $[[3, 1]]$ repetition QECC, that encodes a generic state $|\varphi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ in the state $|\psi\rangle = \alpha_0|000\rangle + \alpha_1|111\rangle$. This code has

generators $G_1 = ZZI$ and $G_2 = IZZ$. Since it can correct at most one qubit-flip error, i.e. an X-gate error per q-codeword, the set of correctable error is $\mathcal{Q} = \{III, IIX, IXI, XII\}$. Furthermore, being $m = 2^{n-k} = 4$, the set of syndromes is $\mathcal{S} = \{s^{(1)}, s^{(2)}, s^{(3)}, s^{(4)}\}$.
From a classical point of view, the resulting channel is a classical m-ary discrete-input discrete-output channel with alphabet $\mathcal{S}$, referred to as piggybacking syndrome channel (PSC).

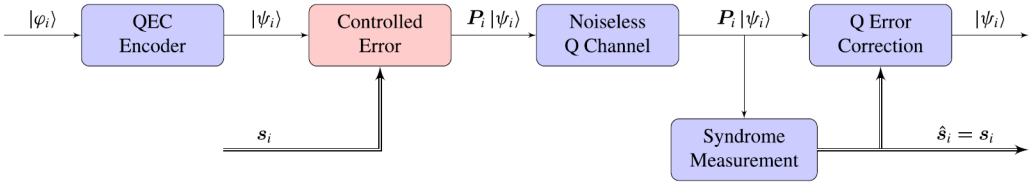

Figure 3.4: Block diagram of piggybacking technique in noiseless quantum channel conditions (figure from[19])

Summing up, to inform the quantum repeaters about the destination address, classical information can be piggybacked over quantum stream. Moreover, this paragraph shows that this can be done without using classical channels, without consuming additional quantum resources, and without disturbing entangled pairs.[19]

3.2.1 Method of Implementation

To further analyse the piggybacking technique, a quantum circuit simulating transmitter, channel and receiver is designed. This quantum circuit is executed on a classical computer, which in turn simulates a quantum computer. In the present work, this process will be referred as simulation. In addition, the same quantum circuit is also executed on a real quantum computer. To these aims, the IBM Quantum Experience (IBMQ) cloud platform is used. The IBM's SKD is called Quantum Information Software Kit (QisKit), and it is based on Python. By exploiting QisKit, IBMQ allows to execute quantum circuits up to 32 qubits by means of classical computers that simulate quantum computers (simulation). Also, IBMQ allows to execute quantum circuits over a set of quantum computers up to 15 qubits. Moreover, it permits to save the outputs in .txt files and download them. Finally, these outputs are analysed and plotted using MATLAB, comparing the results of the simulations with those of quantum computer.
IBM uses a parameter called quantum volume as a rank for its quantum

computers, the higher the quantum volume, the better. This parameter takes into account the architecture, the errors introduced by gates, by decoherence, by measurements, and the number of qubits. Among the available quantum computers, the only one that reaches a quantum volume of 32 is the 5-qubit one called Santiago, which appears to be the best choice. Furthermore, QisKit allows to extract the noise model from a quantum computer, and to use it in the simulations. This is useful when a circuit involves too many qubits to be executed on a quantum computer. However, this is not the case for the present thesis; but simulations implementing the noise model of Santiago are done to assess the model. These simulations will be referred as noisy simulations.

Consider the previous example of a $[[3, 1]]$ repetition QECC. Let the logical qubit be $|\varphi\rangle = |1\rangle$, hence the encoded state is $|\psi\rangle = |111\rangle$. Since all qubits are initialized to the $|0\rangle$ state, the quantum circuit performing the encoding is composed by two CNOT gates. As shown in figure 3.5, both the CNOTs are controlled by the logical qubit q_1. Such an arrangement of qubits is due to fact that Santiago has a linear architecture, and to reduce the CNOT error rate, the control and target qubits should be adjacent.
Suppose to piggyback the classical bits [0 1] over the q-codeword $|\psi\rangle$ by intentionally applying the error $IIX \in \mathcal{Q}$, i.e. an X gate to q_0. Afterwards, the three qubits are sent through the noiseless quantum channel represented by three identity operators. As for the receiver, since the quantum gates are reversible, the decoder is a mirrored copy of the encoder. Moreover, a clever way to correct the logical qubit state is by using a Toffoli gate. Actually, the two qubits controlling the Toffoli gate are the quantum version of the error syndrome. Therefore, the receiver can measure them, obtaining the two-bit syndrome [0 1].

3.2.2 Discussion of the Experimental Results

By simulating the quantum circuit, ideal outcomes are expected; on the contrary, by executing it on quantum computer, the results will take into account the error rate of quantum gates.
The figure 3.6 shows the results of 8192 (the maximum allowed by IBMQ) simulation runs of the quantum circuit described in figure 3.5. The resulting 3-bit string is composed by the measure of the syndrome, in the first two positions starting from the right; and the measure of the logical qubit in the last position on the left. As expected, the receiver is able to retrieve the

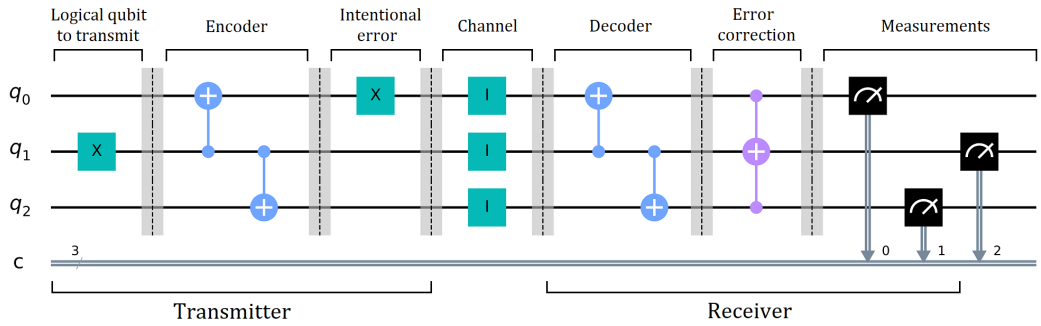

Figure 3.5: Quantum circuit to piggyback the [0 1] bit string over a 3-qubit q-codeword

correct classical bits [0 1] and the correct logical qubit state $|\varphi\rangle = |1\rangle$, whose measure is 1.

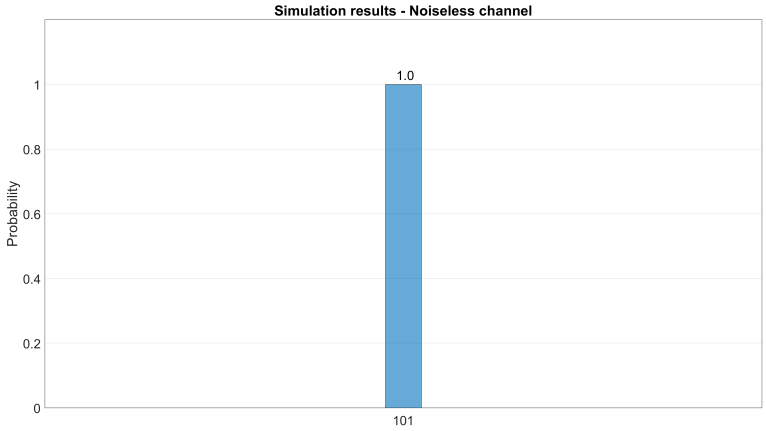

Figure 3.6: Simulation results piggybacking the [0 1] bit string

Executing 8192 times the same quantum circuit on the quantum computer Santiago, the probability of success, as expected, decreases. Indeed, as shown in figure 3.7, the correct result is obtained in 88% of cases. This is due to the fact that, as explained in the introduction, manipulating qubits by quantum gates unavoidably introduces noise.

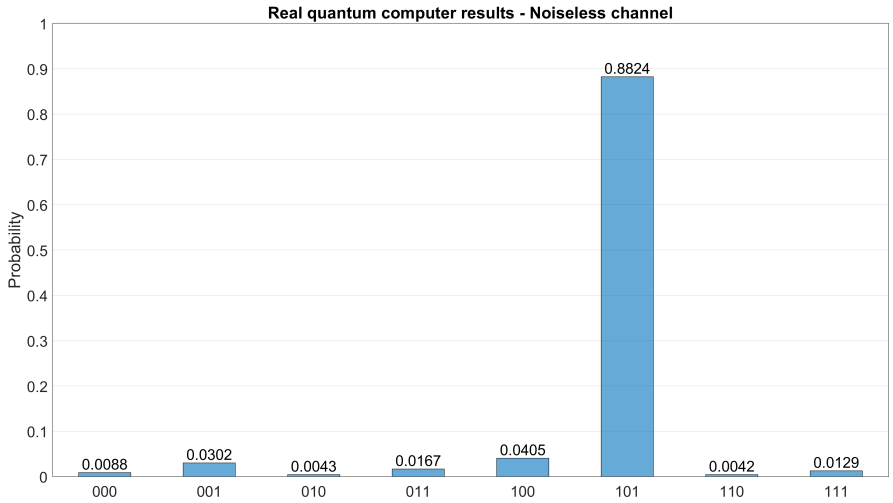

Figure 3.7: Quantum computer results piggybacking the [0 1] bit string

To further analyse the quantum computer results, it might be interesting to separate the error rate that occurs on logical qubit from those that occurs on syndrome. Referring to figure 3.7, the resulting bit error rate (BER) of bits composing the syndrome is $BER = 1 - (0.0302 + 0.8824) = 0.0874$, and regarding the logical qubit, the resulting qubit error rate (QBER) is $QBER = 1 - (0.0405 + 0.8824 + 0.0042 + 0.0129) = 0.06$. Actually, in this case the Toffoli gate is not used, as the correction of the logical qubit is not needed. To show how much the probability of success can decrease by adding a gate in the computation, the intentional error is put on the qubit q_1. In this case the error syndrome is the bit string [1 1]. The figure 3.8 shows the quantum circuit to be executed on quantum computer, and the results of the execution are shown in figure 3.9.

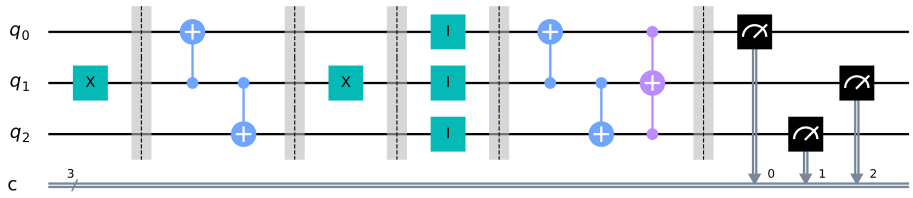

Figure 3.8: Quantum circuit to piggyback the [1 1] bit string over a 3-qubit q-codeword

As expected, the probability to obtain the correct result decreases, lowering to 85%. Moreover, the BER and the QBER result to be $BER = 1-(0.0402+$

$0.8547) = 0.1051$ and $QBER = 1-(0.006+0.0237+0.024+0.8547) = 0.0916$. Comparing these values with those obtained when the Toffoli gate did not act, it gives an insight about the importance to reduce as much as possible the number of quantum gates to achieve a task.

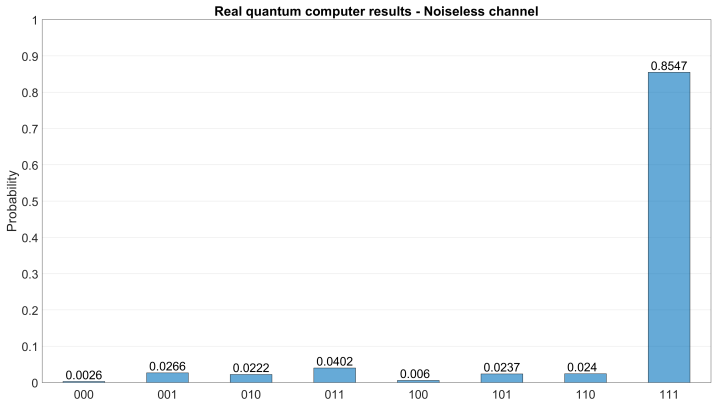

Figure 3.9: Quantum computer results piggybacking the [1 1] bit string

To conclude, in figures 3.10 and 3.11 are reported the results of noisy simulations. In these simulations the noise model of the quantum computer Santiago has been added, and it appears to be conservative compared to the quantum computer results. Indeed, the noise model predicts a success probability of 87% when the intentional error is put on q_0, and of 84% when on q_1. In both cases, about 1% less that the quantum computer.

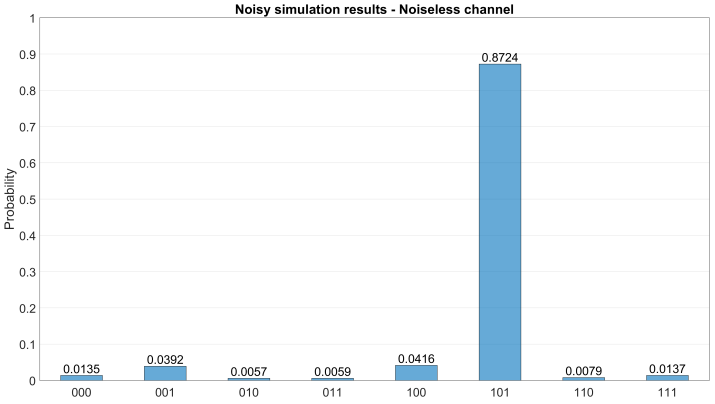

Figure 3.10: Noisy simulation results piggybacking the [0 1] bit string

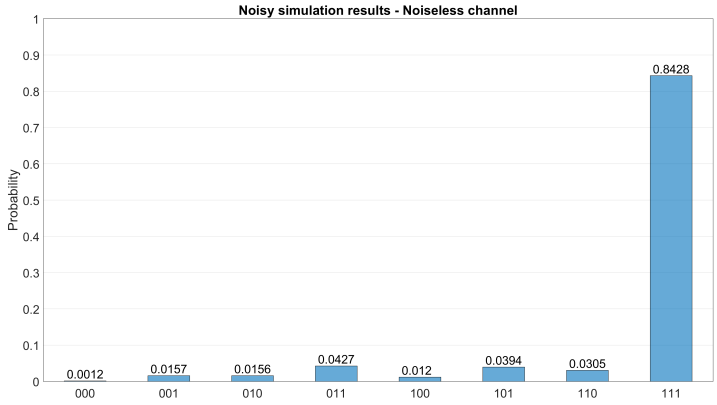

Figure 3.11: Noisy simulation results piggybacking the [1 1] bit string

3.3 Piggybacking in Noisy Quantum Channel Conditions

In a real quantum network scenario, quantum channels could introduce errors and alter the information carried through them. It is still possible to piggyback classical information over quantum stream, however, more complex techniques are needed. As well as in the noiseless channel case, an intentional error is introduced by applying $P_i \in \mathcal{Q}$ on the q-codeword $|\psi_i\rangle$; but now, as shown in figure 3.12, the quantum channel could introduce an error $E_i \in \mathcal{G}_n$. As a consequence, the measured syndrome will be $\hat{s_i} = s(E_i P_i)$.
Recalling that $\mathcal{Q}$ is the set of correctable errors, although $P_i \in \mathcal{Q}$, the composite operator $E_i P_i$ may not be a correctable error, i.e. $E_i P_i \notin \mathcal{Q}$, even if $E_i \in \mathcal{Q}$. For example, an intentional error P_i on the first qubit of a q-codeword, combined with a channel error E_i on the second qubit of the same q-codeword, produces an uncorrectable error for a QECC with single qubit error correction capability.
To deal with this problem, a possible solution proposed in the literature is to introduce a classical error-correcting code (CECC). This CECC is applied to the piggybacked classical bits, protecting them against channel noise. Consider an (n_c,k_c) block CECC with alphabet $\mathcal{S}$, i.e. the alphabet is the set of possible syndromes. To handle with the CECC it might be convenient to design the code in GF($|\mathcal{S}|$), then, each syndrome can be mapped into a symbol, which in turn can be mapped into bits.
Referring to figure 3.12, to transmit k_c syndromes, the CEC encoder block encodes them into n_c syndromes s_i, which compose the transmitted classical codeword (c-codeword) c_w. Afterwards, the controlled error block maps each syndrome s_i to the relative controlled error P_i. The n_c q-codewords pass

through the noisy quantum channel, whereupon the receiver side performs the syndrome measurements $\hat{s}_i = s(E_i P_i), \quad i = 1, 2, ..., n_c$. The classical error correction block, relying on the CECC, corrects the received syndromes providing a valid c-codeword $\breve{c}_w$ composed by the syndromes $\breve{s}_i = s(\hat{P}_i)$, where $\hat{P}_i$ is the estimated intentional error operator. Suppose that the CECC is able to correct the errors introduced by the quantum channel, retrieving the correct c-codeword. This means that the P_i's are known, and if $E_i \in \mathcal{Q}$ the E_i's operators can be determined. In fact, observing that $\hat{s}_i = s(E_i P_i) = s(E_i) \circ s(P_i)$, where $\circ$ is the Hadamard product, since the syndrome elements are ± 1, it follows that $s(E_i) = \hat{s}_i \circ s(P_i)$.
The error computation block computes $s(\hat{E}_i) = \hat{s}_i \circ \breve{s}_i$; thereby, it can estimate which quantum channel error $\hat{E}_i$ is occurred. Finally, the quantum error correction block, by applying the composite operator $\hat{P}_i^{\dagger} \hat{E}_i^{\dagger}$, is able to retrieve the correct quantum state.[19]
To conclude, if the CECC is able to successfully correct the errors on the measured syndrome, the quantum state will be correctly retrieved, thus $|\hat{\psi}_i\rangle = |\psi_i\rangle$. On the other hand, if the classical error correction fails, i.e. $\breve{s}_i \neq s_i$ for some i, the quantum state will not be correctly retrieved, thus $|\hat{\psi}_i\rangle \neq |\psi_i\rangle$. In other words, due to the piggybacking, the probability of error of logical qubits is equal to the probability of the residual syndrome error after decoding, i.e. $Pr\{\breve{s}_i \neq s_i\}$.

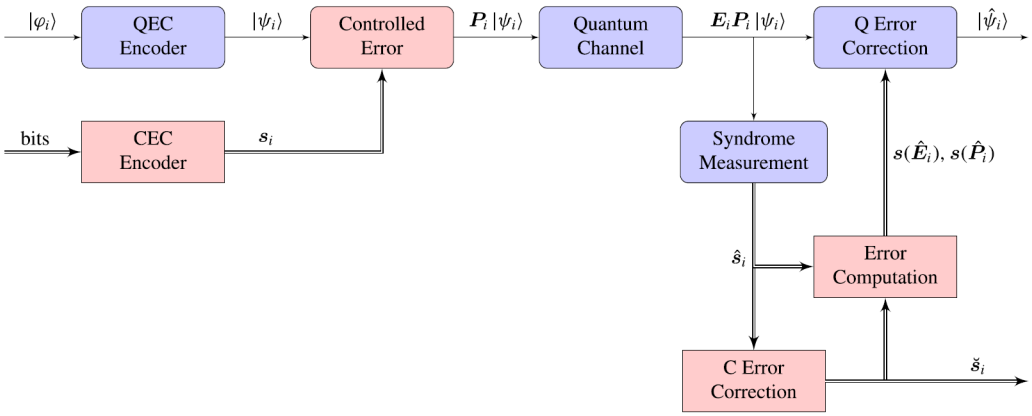

Figure 3.12: Block diagram of piggybacking technique in noisy quantum channel conditions (figure from[19])

3.3.1 Piggybacking Syndrome Channel Analysis

The PSC is a classical channel, thus it can be analysed by using classical concepts like the Shannon entropy and channel capacity. Let the input of

the PSC be $\mathbf{s}$ with probability distribution $p(\mathbf{s})$, and $\hat{\mathbf{s}}$ be the output. Also, let the errors process of the quantum channel be memoryless, i.e. E_i, E_j are independent for $i \neq j$. Under the aforementioned hypothesis, the PSC can be viewed as a classical discrete memoryless channel, whose capacity C_{PSC} is defined as:

$$C_{PSC} = \max_{p(\mathbf{s})} \{H(\mathbf{s}) - H(\mathbf{s}|\hat{\mathbf{s}})\} \quad \left[\frac{\text{bits}}{\text{q-codeword}}\right]. \tag{3.3}$$

Where $H(\mathbf{s})$ is the Shannon entropy.
The worst case for the PSC capacity is represented by a quantum channel error that maps the transmitted syndrome into one of the others $2^{n-k} - 1$ syndromes with equal probability. Hence, defining the probability that the received syndrome is different from the transmitted one as $p_{PSC} = Pr\{\hat{\mathbf{s}} \neq \mathbf{s}\}$, the PSC capacity in (3.3) can be written as:

$$C_{PSC} = (n-k) - h(p_{PSC}) - p_{PSC}\log_2(2^{n-k} - 1) \quad \left[\frac{\text{bits}}{\text{q-codeword}}\right]. \tag{3.4}$$

Where $h(p) = -p\log_2 p - (1-p)\log_2(1-p)$ is the binary entropy function. Notice that, if $p_{PSC} = 0$, the capacity tends to the noiseless case, i.e. $n - k$ [bits/q-codeword]. In fact, as shown in the noiseless quantum channel simulation results (figure 3.6), the capacity is $n - k = 3 - 1 = 2$ [bits/q-codeword].
Consider a memoryless quantum depolarizing channel, and an n-qubit q-codeword passing through it. Each qubit undergoes an error X, Y, or Z with equal probability $p_d/3$, and no errors with probability $1 - p_d$. Since undetectable errors can be introduced by the quantum channel, i.e. $s(E_iP_i) = s(P_i)$, it follows that[19]

$$p_{PSC} < Pr\{E_i \neq I\} = 1 - (1 - p_d)^n. \tag{3.5}$$

Fixing a QECC, the exact p_{PSC} can be evaluated, then, by substituting it into the equation (3.4), the PSC capacity is provided.

3.3.2 Method of Implementation

Consider the same $[[3, 1]]$ repetition QECC already used in the noiseless quantum channel case. This code is able to work with X-type errors only, therefore, a qubit-flip quantum channel has been implemented. As before, let $|\varphi\rangle$ be $|1\rangle$, thus $|\psi\rangle = |111\rangle$, also, let p be the probability of error per qubit, hence $p_d = p$. Referring to figure 3.13, the noisy qubit-flip quantum channel is implemented by applying the rotation operator on each qubit of the

q-codeword. Recalling the Bloch sphere, by rotating a qubit of an angle $\theta = 2\cos^{-1}(\sqrt{1-p})$ [rad] about the x-axis, a qubit-flip with probability p is introduced. In fact, if a state $|0\rangle$ and $p = 0.1$ are considered, the angle will be $\theta = 2\cos^{-1}(\sqrt{0.9})$ [rad]. By substituting θ in the equation (1.5), the probability to obtain the state $|0\rangle$ upon a measurement is 0.9. An analogous result can be obtained starting from the state $|1\rangle$.

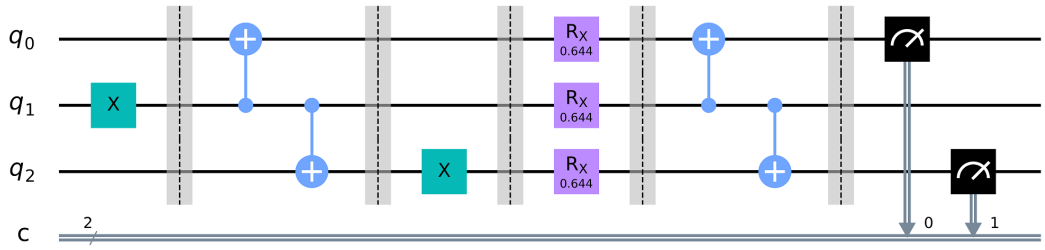

Figure 3.13: Quantum circuit to piggyback the [1 0] bit string over a 3-qubit q-codeword

Since it is convenient to design the CECC in GF(4), a possible mapping between the classical symbols, the syndromes and the intentional errors is proposed below:

$$\begin{array}{rcccc} \text{Classical symbols} = & \{0, & 1, & 2, & 3\} \\ & \downarrow & \downarrow & \downarrow & \downarrow \\ \text{Syndromes } \mathcal{S} = & \{00, & 01, & 11, & 10\} \\ & \downarrow & \downarrow & \downarrow & \downarrow \\ \text{Intentional errors } P = & \{\underbrace{III}_{q_2q_1q_0}, & \underbrace{IIX}_{q_2q_1q_0}, & \underbrace{IXI}_{q_2q_1q_0}, & \underbrace{XII}_{q_2q_1q_0}\} \end{array} \tag{3.6}$$

The error rate of CECCs is defined as: $\frac{\#(\check{c}_w \neq c_w)}{W}$ where W is the number of c-codewords transmitted. As for the QECC error rate, as described in paragraph 3.3, it corresponds to the CECC one.
In the literature no typical values for p are indicated. However, considering that there are four possible syndromes, $p_{PSC} > \frac{3}{4}$ does not make sense. Therefore, by using the equation $1-(1-p)^n < \frac{3}{4}$, it follows that $p < 0.37$. Nonetheless, a fiber with error rate 0.37 is considered very bad, so the following values for p are used:

$$p = 0,\ 0.01,\ 0.02,\ 0.04,\ 0.06,\ 0.08,\ 0.1,\ 0.12,\ 0.14,\ 0.16,\ 0.18,\ 0.2\,.$$

Due to the fact that each q-codeword carries a classical symbol, and the simulations, or the quantum computer executions, are limited to 8192 runs, it is possible to transmit at most $8192/n_c$ c-codeword. This means that the resulting error rate of the CECC could not be statistically meaningful. To get around this problem, a two-step strategy is adopted.
The first step is implemented in QisKit. By fixing a probability of error per qubit p, the quantum circuit transmitting the symbol $sym = 0$, i.e. no intentional errors, is run 8192 times. The measured syndromes $\hat{s_i}$ are mapped to the corresponding symbols, according to the convention in (3.6), and these symbols are saved in a txt file. Afterwards, the quantum circuit transmitting the symbol $sym = 1$, i.e. an intentional X-error on q_0, is run, generating another txt file; and so on for the other symbols. By repeating this process, sweeping all the values of p, a set of 48 txt files is obtained. Each file is referred to as $p\_sym.txt$, and it contains 8192 received symbols. For example, by transmitting the symbol $sym = 2$ with probability of error per qubit $p = 0.01$, the QisKit output will be the file $0.01\_2.txt$
The second step is implemented in MATLAB. Given a CECC, the possible c-codewords are previously stored, and a probability of error per qubit p is fixed. Then, the first symbol of the first c-codeword is set as transmitted symbol sym. Therefore, the received symbol $s\hat{y}m$ is obtained by randomly picking a symbol into the right txt file $p\_sym.txt$. The same procedure is reiterated considering the second symbol of the first c-codeword; and so on n_c times. Thereafter, the resulting n_c received symbols can be decoded by computing the nearest c-codeword. For this purpose, the adopted convention is: distance = 0 if the two symbols do not differ from each other, distance = 1 if they do. If the resulting c-codeword at the output of the decoder and the transmitted one are not the same, the $\#(\breve{c}_w \neq c_w)$ is incremented.
The c-codewords are transmitted by picking them cyclically from first to last, until 10^5 c-codeword transmissions are performed. Thereby, $W = 10^5$ c-codewords have been transmitted, received end decoded, bypassing the limit of 8192 runs. Finally, by sweeping the values of p and repeating the whole process, the error rates of a CECC for each p are obtained.
In the decoding process described above, two tacit hypotheses are adopted: i) all symbols have the same probability to occur, ii) all c-codewords have the same probability to occur. Hence, from the decision theory, the adopted maximum likelihood approach minimises the error rate.

The uncoded case is used as reference point to compare the performance of the other codes. Its theoretical probability of error P_e coincides with p_{PSC},

and considering the [[3, 1]] QECC, the exact expression of p_{PSC} is given by:

$$P_e = p_{PSC} = \sum_{l=1}^{2} \binom{3}{l} p^l (1-p)^{3-l} . \tag{3.7}$$

Note that, as described in paragraph 3.3.1, $p_{PSC} < 1 - (1-p)^3$. In fact, if an X-error occurs on all the qubits of a q-codeword, the syndrome does not change.
The considered CECCs in GF(4) are linear block codes designed by factorizing the polynomial $X^{n_c} - 1$. These codes are listed below reporting the minimum distances d_{min} between c-codewords and the number of correctable errors t:

- (3,1) symbol repetition $d_{min} = 3 \quad \rightarrow \quad t = 1$
- (4,2) $d_{min} = 3 \quad \rightarrow \quad t = 1$
- (10,4) $d_{min} = 5 \quad \rightarrow \quad t = 2$
- (17,9) $d_{min} = 7 \quad \rightarrow \quad t = 3$

For the codes listed above, the upper bound of the theoretical probability of error P_e is expressed as:

$$P_e \leq \sum_{l=t+1}^{n} \binom{n}{l} p_{PSC}^l (1-p_{PSC})^{n-l} .$$

In addition, simple codes in GF(2) are considered:

- (3,1) bit repetition $d_{min} = 3 \quad \rightarrow \quad t = 1$
- (5,1) bit repetition $d_{min} = 5 \quad \rightarrow \quad t = 2$
- (7,4) Hamming code $d_{min} = 3 \quad \rightarrow \quad t = 1$

Since these latter codes in GF(2) have an odd n_c, and each q-codeword carries two bits, a possible way to implement these codes is by concatenating two c-codewords. Hence, there will be q-codewords carrying one bit belonging to one c-codeword, and the other bit belonging to the other c-codeword. This leads to more complex theoretical probabilities of error, for this reason the P_e's of these codes are discussed in Appendix C.

3.3.3 Discussion of the Experimental Results

By analysing the obtained results in noisy quantum channel conditions, the PSC behaviour can be further investigated and a PSC model can be inferred. On the right side of figure 3.14, the resulting error rates for a fixed probability of error per qubit $p = 0.1$ are shown. On the left side, the figure shows the efficiencies of the codes in [info bits/channel use], i.e. [info bits/qubit]. Since it is possible to piggyback two bits over a q-codeword, all the efficiencies are less than 2/3.
Regarding the uncoded case and the CECCs in GF(2), as expected by equations (3.7), (C.1), (C.2) and (C.3), the probabilities of error P_e's correspond to the simulated error rates; while, for the codes in GF(4), P_e represents an upper bound. Furthermore, comparing the noisy simulation results with those of the quantum computer Santiago, the noise model confirms the trend in predicting higher error rates. Another view of the gap between the noise model and the quantum computer results is shown in figure D.2 in Appendix D.

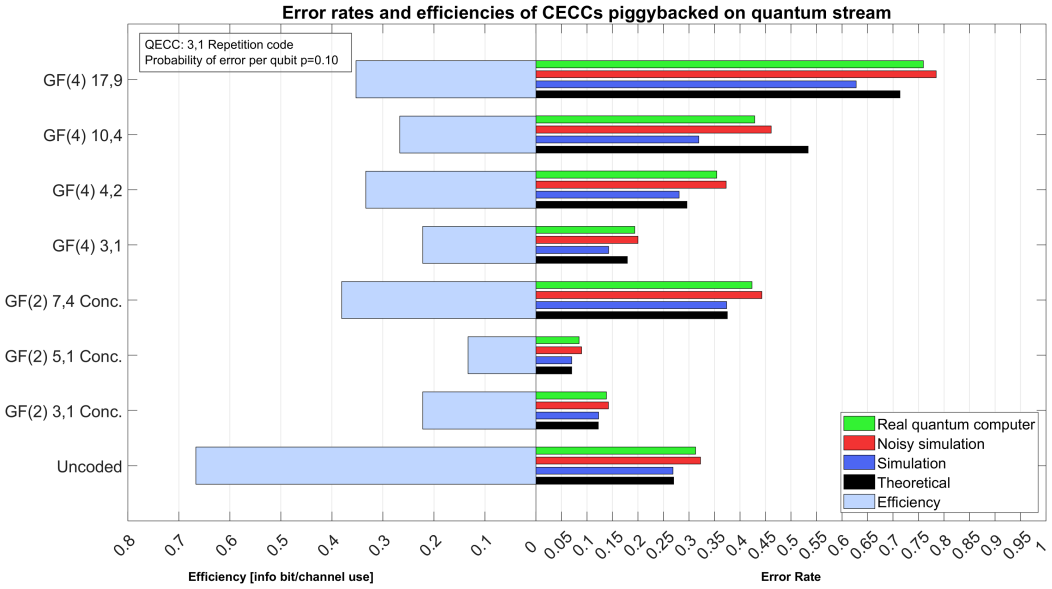

Figure 3.14: Error rates and efficiencies of piggybacked CECCs for p=0.1

From the point of view of error rates, the best code seems to be the (5,1) bit-repetition. The reason is that this code is able to correct at least two bits by transmitting only five q-codewords. For example, the (10,4) is also able to correct at least two bits (two symbols), but it can do so by transmitting ten q-codewords. The greater the number of q-codewords to be sent, the

greater the probability of erroneous bits. However, as for the efficiency, the (5,1) bit-repetition is the worst case. Moreover, as shown in figure 3.16, if the probability of error per qubit p is increased, the longest used codes (i.e. the most efficient) show very high error rates. This explains why longer and more efficient codes are not being considered in the present work.
Since the figure 3.16 reports all the results for each code, it could be difficult to read. Hence, the more clear figure D.1 reporting only the simulations results is showed in Appendix D.

By setting $p = 0.01$, the code (17,9) in GF(4) becomes interesting. Indeed, referring to figure 3.15, this code shows an error rate comparable to that of the (5,1) bit-repetition code; thus, comparing the efficiencies, the (17,9) seems to be the best choice. As for the quantum computer results, the error rates are dominated by the errors introduced by the computer; so the errors introduced by the channel are negligible. To prove this, is possible to compare the quantum computer results in noiseless channel conditions (figure 3.7), where the error rate is $1 - 0.8824 = 0.1176$, with those in uncoded noisy channel conditions (figure 3.16), where, for $p = 0.01$, the error rate is approximatively the same. Since to deal with small p's, quantum computers with higher fidelity would be needed, for these p's, the best way to compare the behaviour of CECCs piggybacked over quantum stream is by the simulations results.

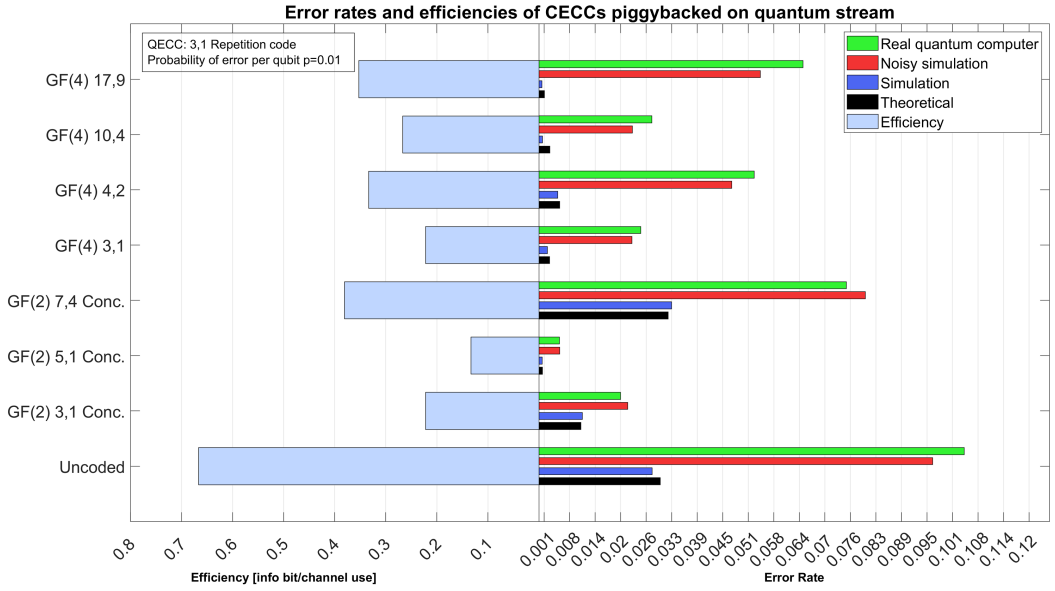

Figure 3.15: Error rates and efficiencies of piggybacked CECCs for p=0.01

Furthermore, it is quite interesting that lowering the probability of error per qubit from $p = 0.1$ to $p = 0.01$, as shown in figure 3.16, the error rates of the longest codes decrease quickly. In fact, the uncoded case, the codes in GF(2) and the (3,1) symbol-repetition in GF(4) all have a linear trend in a log log scale; whereas, the other codes in GF(4) (i.e. (4,2), (10,4), (17,9)), decreasing p, their error rates rapidly decrease, although for large p's their error rates are very high. Notice that, referring to these latter codes, for each one of them there is a value of p beyond which the uncoded transmission is better that the coded one.
However, an exception is represented by the concatenated (7,4) Hamming code in GF(2). Due to the fact that it transmits relatively long c-codewords, and only one erroneous bit can be corrected, this code shows error rates always worse than the uncoded case.

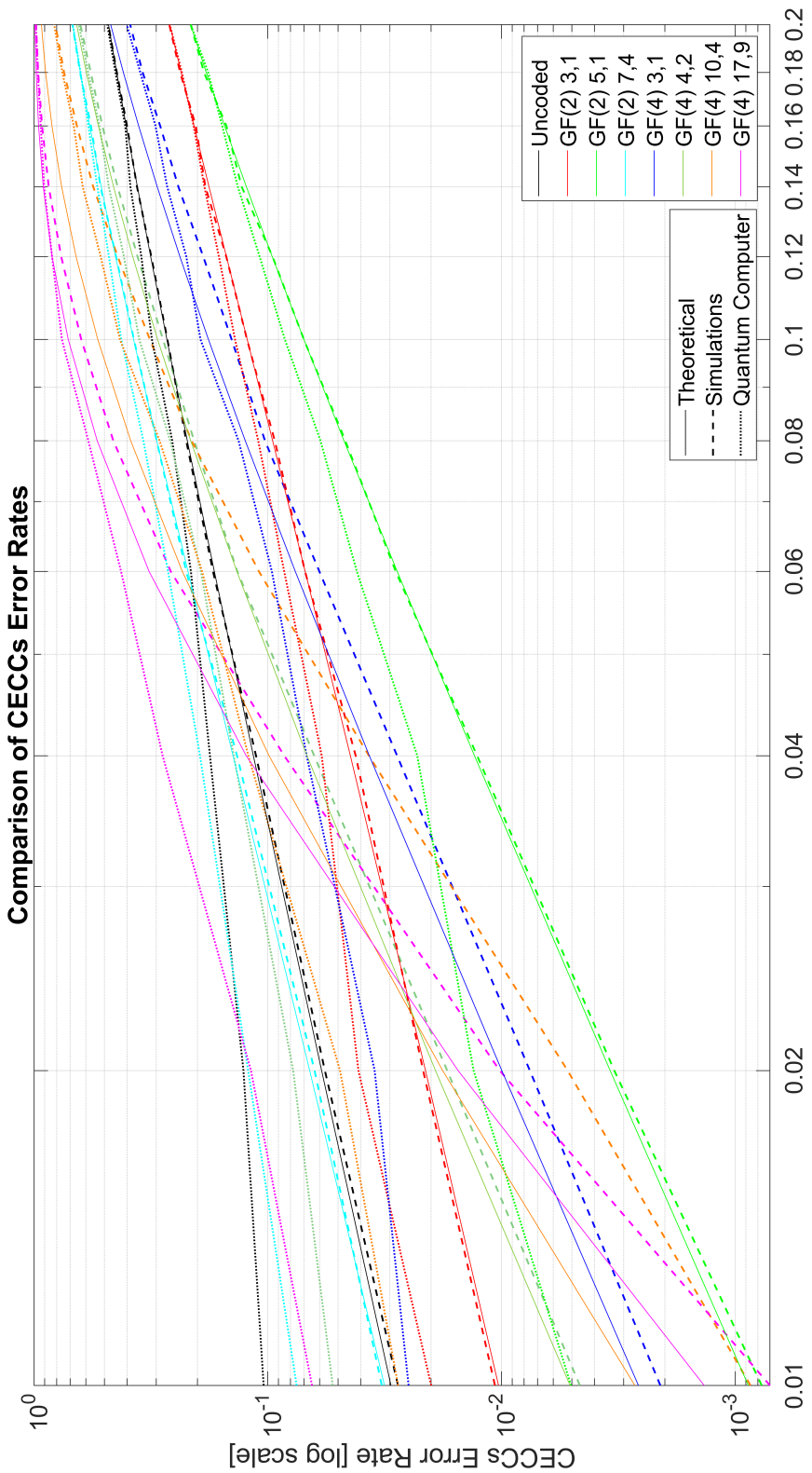

Figure 3.16: Theoretical probability of errors, simulated error rates and quantum computer error rates for CECCs piggybacked over quantum stream

To further analyse the results, the PSC capacity can be determined. By referring to equation (3.4), and substituting the p_{PSC} for the $[[3, 1]]$ repetition QECC expressed in (3.7), the capacity C_{PSC} is provided.
To compare the performance of CECCs with respect to the theoretical C_{PSC}, an error rate of 10^{-3} is fixed. Then, by interpolating the data obtained from the simulations results, the values of p for which each code reaches an error rate of 10^{-3} are extrapolated.

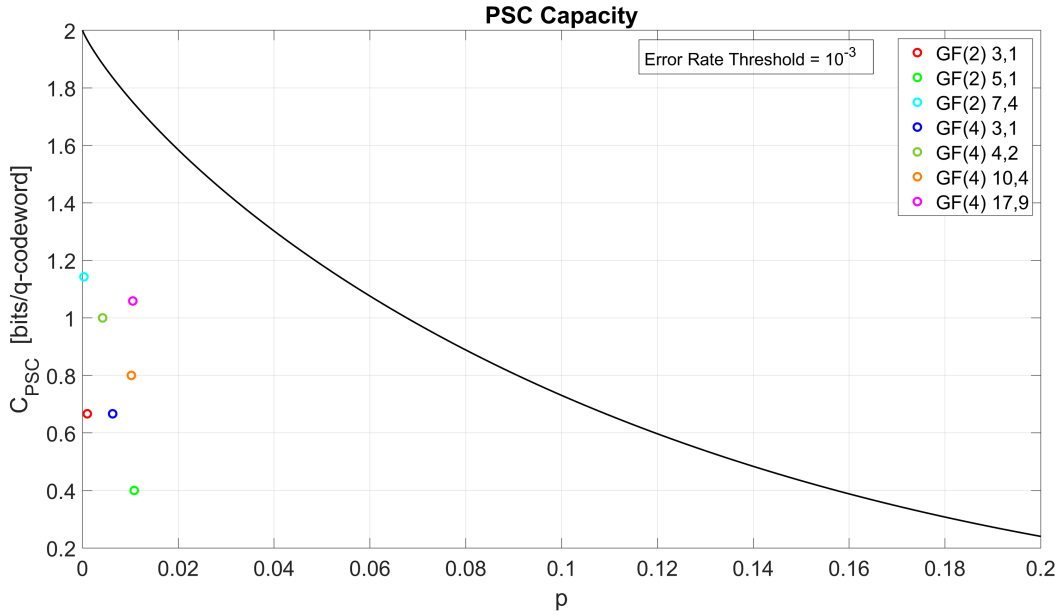

Figure 3.17: CECCs performances with respect to the theoretical PSC capacity

By evaluating the bits/q-codeword ratio for each code, is possible to identify each code as a point under the capacity curve. However, as shown in figure 3.17, the considered codes are far away from the theoretical curve.

Lastly, exploiting the simulations results stored in txt files, a model for the PSC is proposed. This model is valid only when a $[[3, 1]]$ repetition QECC is employed, and, to be more general, it does not take into account the errors introduced by a particular quantum computer. The model is extrapolated by counting the number of occurrences of each received symbol into a particular txt file. For example, by transmitting the symbol 3 over a quantum channel with probability of error per qubit $p = 0.1$, the error rate with which the symbol 0 is received can be approximated by counting how many 0's there are in the file $0.1\_3.txt$, and dividing the result by 8192. The table E.1 in the Appendix E shows the approximated values composing the model. Recalling

the PSC capacity (equation 3.4), a quantum channel mapping the transmitted symbol into one of the others $2^{n-k}-1$ symbols with equal probability was supposed. It is worth notice that, although the model is an approximation, it confirms the supposed behaviour of the quantum channel.

Chapter 4

Conclusions

Quantum information is evolving very rapidly and dynamically. In the last decade, the development of quantum technologies has reached the engineering phase, allowing to execute quantum circuits on quantum computers through cloud platforms. Moreover, small quantum networks have been implemented, mainly for QKD experiments.
As shown in this work, considering the QECC approach to communicate quantum information, the piggybacking technique allows to carry classical information through noisy quantum channels. Hence, a possible application of this technique is to provide routing information to quantum repeaters.
Since the quantum channels introduce noise, CECCs must be employed in the PSC. By analysing the experimental results it comes out that, for large probability of error per qubit p (approximatively $p \geqslant 0.1$), short CECCs, like the repetition codes, show lower error rates, at the cost of lower efficiency. Conversely, decreasing p, long and more efficient CECCs show error rates comparable or better than short codes. Moreover, the approximated model for the PSC allows to simulate the behaviour of any CECC piggybacked over a $[[3, 1]]$ repetition QECC.
A further investigation of the piggybacking technique could take into account more efficient QECCs, implementing longer CECCs than those designed in this work. For example, BHC or RS codes. Thereby, it should be possible to approach the PSC capacity theoretical limit. However, it is worth noting that, by using optical fiber, the probability of error per qubit is time independent. As a consequence, the errors are spread along the stream, and not positioned within bursts. For this reason, CECCs using long symbols might lead to high error rates.

Appendix A

Appendix: Companies Effort and Software Segmentation

A lot of companies around the world, supported by universities, are involved in quantum information, research and development. The table A.1 reports the biggest companies that provide public access to their quantum computers. Even though many companies have already built their own quantum computers, only IBM gives free access to its quantum computer in the cloud. Other companies like Rigetti, D-Wave, and IonQ allow paid access to their quantum computer through the AWS. As a consequence, simulating quantum computer using a classical one is an alternative that must be considered. Although the world of quantum information is at its early stage, it is growing fast and changing rapidly.
To implement quantum algorithms, several SDKs, packages, and libraries have been developed. Almost all of them are based on C/C++ or Python programming languages; in addition, Microsoft has developed its own quantum programming languages named Q# as part of the Microsoft QKD, which in turns is a part of the .NET Framework.

To interface the high-level commands with the electronic devices controlling the qubits, low level quantum assembly languages are needed. One of the most used open source assembly language is OpenQASM, which was initially described in a 2017 paper,[20] and the source code was later released by IBM. As for the quantum computer simulators, the Oxford University has developed a multiplatform open source quantum simulation toolkit, named QuEST. It works in C/C++ and it can be used both on laptops and on supercomputers, exploiting GPU-accelerated, multithreaded and distributed systems. Furthermore, it can be integrated in Wolfram's software Math-

ematica using the package QuESTlink. A lot of others software packages to simulate quantum computers have been developed to date, some of they are mentioned in this thesis, and many others are listed in this web site: https://www.quantiki.org/wiki/list-qc-simulators.
Since software segmentation could hinder the quantum-algorithm developers, the Estonian company Quantastica proposes a software conversion tool. Quantastica provides an editor to write quantum circuits in QASM or QUIL. Afterwards, it is possible to convert the code in a large number of languages: pyQuil (Rigetti), QUIL, QisKit (IBM), QASM, Qobj, Cirq (Google), TensorFlow Quantum, Q# (Microsoft), QuEST, Quirk, JavaScript and json. Quantastica can also export the quantum circuit in SVG or PNG file, and finally it can convert the circuit in a unitary matrix.

Company	Affiliate University	Cloud Access	Technology	Quantum Computer Name	# of qubits	Layout	SDK/Programming language
IBM	MIT	Yes	Superconducting	IBM Q Melbourne	15	Lattice 2x7+1	QisKit/Python
				IBM Q London	5	T	QisKit/Python
				IBM Q Santiago	5	Linear	QisKit/Python
Rigetti	Berkeley	Through AWS	Superconducting	Aspen-8	32	Connected octagons	Amazon Braket/Python
D-Wave	-	Through AWS	Superconducting, Quantum Annealer	D-Wave 2000Q	2048	-	Amazon Braket/Python
IonQ	University of Maryland, Duke University	Through AWS	Trapped Ion	-	79	Fully Connected	Amazon Braket/Python
Google	UCSB	No	Superconducting	Bristlecone	72	Lattice 6x12	Cirq/Python
				Sycamore	53	-	Cirq/Python
Honeywell	Caltech, Georgia Tech	On-demand	Trapped Ion	System Model HØ	6	Fully Connected	-
Xanadu	-	Yes	Photonic Quantum Computing	-	12	-	Strawberry Fields/Python
OriginQ	-	Yes	Superconducting	Wu Yuan	6	-	QPanda/C++

Table A.1: Companies that have built quantum computers

Appendix B

Appendix: Physical Implementations of Qubits

Physical support	**Name**	**Information support**	$\|0\rangle$	$\|1\rangle$
Photon	Polarization encoding	Polarization of light	Horizontal	Vertical
	Number of photons	Fock state	Vacuum	Single photon state
	Time-bin encoding	Time of arrival	Early	Late
Coherent state of light	Squeezed light	Quadrature	Amplitude-squeezed state	Phase-squeezed state
Electrons	Electron Spin	Spin	Up	Down
	Electron number	Charge	No electron	One electron
Nucleus	Nuclear spin addressed through NMR	Spin	Up	Down
Optical lattices	Atomic spin	Spin	Up	Down
Josephson junction	Superconducting charge qubit	Charge	Uncharged superconducting island ($Q = 0$)	Charged superconducting island ($Q = 2e$), one extra Cooper pair)
	Superconducting flux qubit	Current	Clockwise current	Counterclockwise current
	Superconducting phase qubit	Energy	Ground state	First excited state
Singly charged quantum dot pair	Electron localization	Charge	Electron on left dot	Electron on right dot
Quantum dot	Dot spin	Spin	Down	Up
van der Waals heterostructure	Electron localization	Charge	Electron on bottom sheet	Electron on top sheet

Table B.1: Examples of qubit physical implementation (from Wikipedia)

Appendix C

Appendix: Probabilities of Error for CECCs in GF(2)

Consider the (3,1) bit-repetition CECC in GF(2). To maximize the efficiency, the c-codeword are concatenated, then 6 bits (two c-codewords) are piggybacked over 3 q-codewords. As a consequence, as shown in figure C.1, the first 5 qubits of the quantum stream influence the first c-codeword, and the last 5 qubits of the quantum stream influence the second c-codeword.
Considering a c-codeword and the five qubits that can influence it, the errors occurring on each qubit have different consequences on bits. For this reason, all combination of errors must be examined separately.

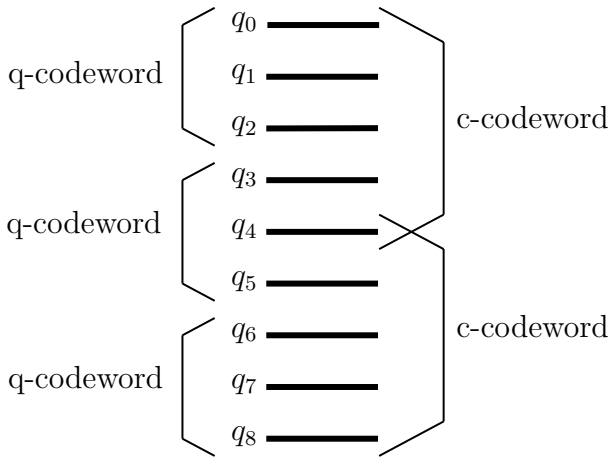

Figure C.1: Scheme of concatenated (3,1) bit-repetition CECC piggybacked over [[3,1]] repetition QECC

The probability that no errors occur on the two bits piggybacked by the

first 3 qubits is expressed as:

$$P_0^{(3)} = \sum_{l=0,3} \binom{3}{l} p^l (1-p)^{3-l} .$$

Also, the probability that no errors occur on the bit piggybacked by the last two qubits is expressed as:

$$P_0^{(2)} = \sum_{l=0,2} \binom{2}{l} p^l (1-p)^{2-l} .$$

Furthermore, the probability that one error occurs on the two bits piggybacked by the first 3 qubits is expressed as:

$$P_1^{(3)} = 2p(1-p)^2 + 2p^2(1-p) .$$

And the probability that one error occurs on the bit piggybacked by the last two qubits is expressed as:

$$P_1^{(2)} = 2p(1-p) .$$

By using the expression above, the probability of error of the (3,1) bit-repetition CECC is:

$$P_e = 1 - (P_0^{(3)} P_0^{(2)} + P_1^{(3)} P_0^{(2)} + P_0^{(3)} P_1^{(2)}) . \tag{C.1}$$

Considering the (5,1) bit-repetition CECC in GF(2), the 10 bits (two c-codewords) are piggybacked over 5 q-codewords. Then, the first 8 qubits of the quantum stream influence the first c-codeword, and the last 8 qubits of the quantum stream influence the second c-codeword. The probability that two errors occurs on the bits piggybacked by a q-codeword is:

$$P_2^{(3)} = p(1-p)^2 + p^2(1-p) .$$

Therefore, considering a c-codeword and the 8 qubits that can influence it, the probability of error of the (5,1) bit-repetition CECC is:

$$\begin{aligned} P_e = 1 - (&P_0^{(3)} P_0^{(3)} P_0^{(2)} + P_1^{(3)} P_0^{(3)} P_0^{(2)} + P_0^{(3)} P_1^{(3)} P_0^{(2)} + \\ &P_0^{(3)} P_0^{(3)} P_1^{(2)} + P_2^{(3)} P_0^{(3)} P_0^{(2)} + P_0^{(3)} P_2^{(3)} P_0^{(2)} + \\ &P_1^{(3)} P_1^{(3)} P_0^{(2)} + P_1^{(3)} P_0^{(3)} P_1^{(2)} + P_0^{(3)} P_1^{(3)} P_1^{(2)}) . \end{aligned} \tag{C.2}$$

Finally, considering the (7,4) Hamming code, the 14 bits (two c-codewords) are piggybacked over 7 q-codewords. Then, the first 11 qubits of the quantum

stream influence the first c-codeword, and the last 11 qubits of the quantum stream influence the second c-codeword. Considering a c-codeword and the 11 qubits that can influence it, the probability of error of the (7,4) Hamming CECC is:

$$P_e = 1 - (P_0^{(3)} P_0^{(3)} P_0^{(3)} P_0^{(2)} + P_1^{(3)} P_0^{(3)} P_0^{(3)} P_0^{(2)} + P_0^{(3)} P_1^{(3)} P_0^{(3)} P_0^{(2)} + P_0^{(3)} P_0^{(3)} P_1^{(3)} P_0^{(2)} + P_0^{(3)} P_0^{(3)} P_0^{(3)} P_1^{(2)}) \,. \tag{C.3}$$

Appendix D

Appendix: Additional Figures of Experimental Results

In the following pages the plots of experimental results are reported. The figure D.1 shows the simulated error rates for all values of p, while the figure D.2 shows the differences between the noise model proposed by IBM and the quantum computer results.

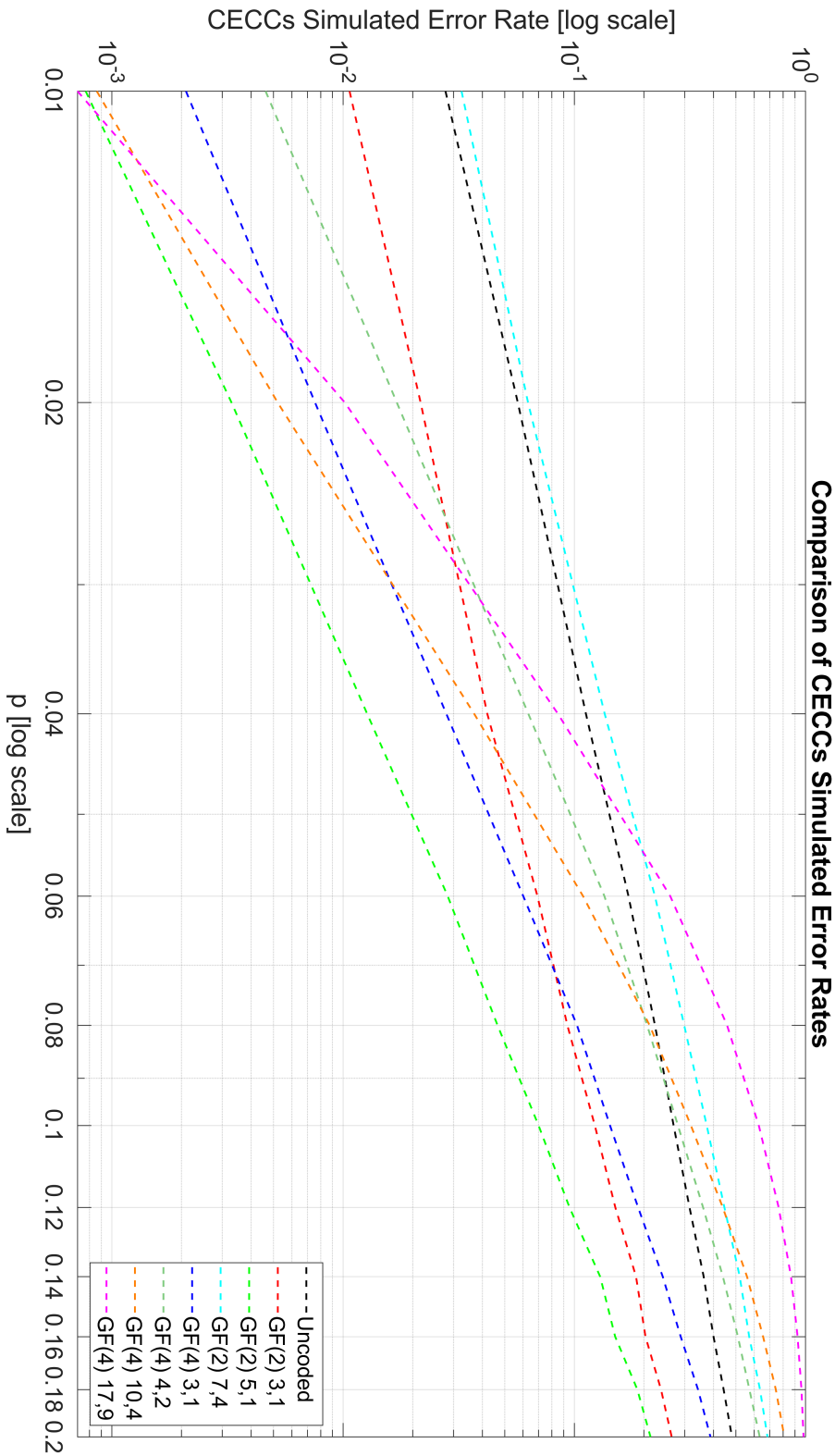

Figure D.1: Simulated error rates for CECCs piggybacked over quantum stream

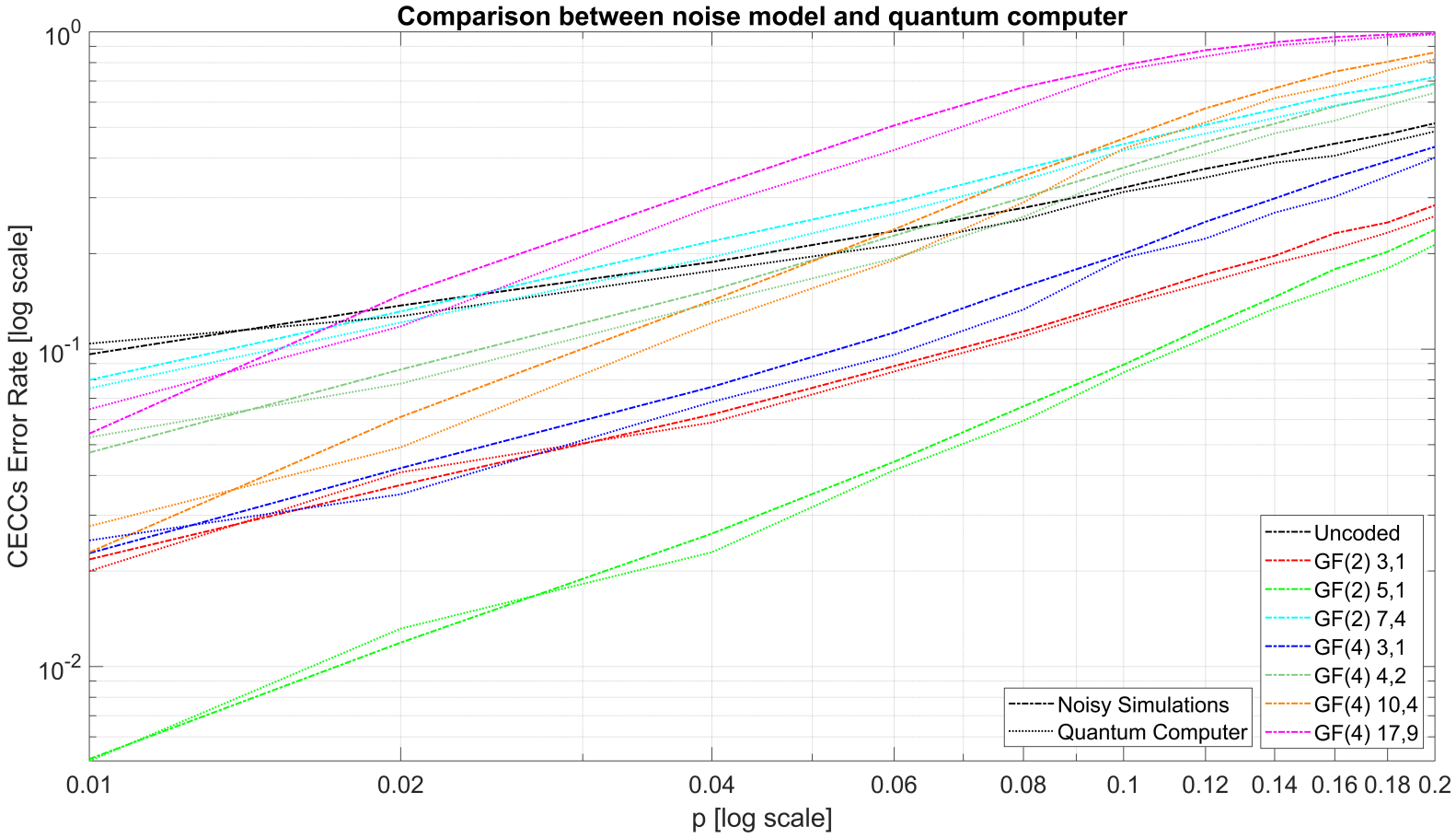

Figure D.2: Noisy simulation and quantum computer error rates for CECCs piggybacked over quantum stream

Appendix E

Appendix: PSC Model

In the following table the model of the PSC is reported. The table is divided in sections referring to a fixed value of probability of error per qubit p. The columns of each section represent the transmitted symbol, and the rows the received one. In the intersections, the estimated probability of receiving the symbol indicated in the rows is showed. For example, the probability to receive the symbol 3 upon a transmission of the symbol 1, with $p = 0.04$ is 0.0381.

p=0.01	0	1	2	3
0	0.9729	0.0082	0.0112	0.0099
1	0.0098	0.9724	0.0099	0.0100
2	0.0092	0.0087	0.9698	0.0107
3	0.0082	0.0107	0.0090	0.9694
p=0.02	0	1	2	3
0	0.9421	0.0210	0.0199	0.0181
1	0.021	0.9404	0.0177	0.0183
2	0.0198	0.0204	0.9399	0.0155
3	0.0171	0.0182	0.0225	0.9481
p=0.04	0	1	2	3
0	0.8848	0.0369	0.0389	0.0354
1	0.0364	0.8851	0.0349	0.0347
2	0.0361	0.0399	0.8866	0.0387
3	0.0427	0.0381	0.0396	0.8912
p=0.06	0	1	2	3
0	0.8284	0.0530	0.0533	0.0593
1	0.0579	0.8308	0.0632	0.0607
2	0.0577	0.0581	0.8285	0.0536
3	0.0560	0.0581	0.0549	0.8264

p=0.08	0	1	2	3
0	0.7806	0.0793	0.0701	0.0751
1	0.0732	0.7681	0.0699	0.0710
2	0.0725	0.0754	0.7852	0.0789
3	0.0736	0.0771	0.0748	0.7750
p=0.1	0	1	2	3
0	0.7207	0.0874	0.0923	0.0886
1	0.0948	0.7407	0.0852	0.0898
2	0.0905	0.0852	0.7329	0.0916
3	0.0940	0.0867	0.0896	0.7300
p=0.12	0	1	2	3
0	0.6907	0.1045	0.1090	0.1088
1	0.1045	0.6869	0.1044	0.1027
2	0.1038	0.1025	0.6863	0.1083
3	0.1011	0.1061	0.1003	0.6803
p=0.14	0	1	2	3
0	0.6274	0.1152	0.1271	0.1229
1	0.1209	0.6479	0.1172	0.1179
2	0.1278	0.1199	0.6344	0.1155
3	0.1238	0.1169	0.1213	0.6437
p=0.16	0	1	2	3
0	0.5988	0.1344	0.1375	0.1274
1	0.1346	0.5984	0.1288	0.1317
2	0.1279	0.1340	0.5964	0.1345
3	0.1388	0.1332	0.1373	0.6063
p=0.18	0	1	2	3
0	0.557	0.1412	0.1501	0.1423
1	0.1423	0.5601	0.1444	0.1520
2	0.1558	0.1473	0.5588	0.1498
3	0.1449	0.1514	0.1466	0.5559
p=0.2	0	1	2	3
0	0.5176	0.1561	0.1608	0.1670
1	0.1584	0.5220	0.1595	0.1569
2	0.1631	0.1559	0.5266	0.1599
3	0.1609	0.1660	0.1531	0.5162

Table E.1: Extrapolated model of the PSC over a [[3,1]] repetition QECC

Bibliography

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2010. 1, 2, 17, 19, 25

[2] A. Tajima *et al.*, "Quantum key distribution network for multiple applications," *Quantum Science and Technology*, vol. 2, p. 034003, jul 2017. 1

[3] D. Gottesman, T. Jennewein, and S. Croke, "Longer-baseline telescopes using quantum repeaters," *Phys. Rev. Lett.*, vol. 109, p. 070503, Aug 2012. 1

[4] P. Kómár, E. M. Kessler, M. Bishof, L. Jiang, A. S. Sørensen, J. Ye, and M. D. Lukin, "A quantum network of clocks," *Nature Physics*, vol. 10, pp. 582–587, Aug 2014. 1

[5] E. National Academies of Sciences and Medicine, *Quantum Computing: Progress and Prospects*. Washington, DC: The National Academies Press, 2019. 2, 3

[6] D. Gottesman, "An introduction to quantum error correction and fault-tolerant quantum computation," *arXiv preprint quant-ph/0904.2557*, 2009. 2

[7] P. W. Shor, "Fault-tolerant quantum computation," in *Proc. of 37th Annual Symposium on Foundations of Computer Science,IEEE Press*, (Los Alamitos, CA), pp. 56–65, 1996. 2

[8] A. Finnila, M. Gomez, C. Sebenik, C. Stenson, and J. Doll, "Quantum annealing: A new method for minimizing multidimensional functions," *Chemical Physics Letters*, vol. 219, no. 5, pp. 343 – 348, 1994. 2

[9] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proc. of 35th Annual Symposium on Foundations of Computer Science,IEEE Press*, (Los Alamitos, CA), 1994. 2

[10] A. Frank, A. Kunal, B. Ryan, *et al.*, "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, pp. 505–510, Oct 2019. 3

[11] "On quantum supremacy." https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/. 3

[12] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theories," *Phys. Rev. Lett.*, vol. 23, pp. 880–884, Oct 1969. 11

[13] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, p. 802, 1982. 15

[14] S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: A vision for the road ahead," *Science*, vol. 362, no. 6412, 2018. 16

[15] B. Hensen, H. Bernien, A. E. Dréau, *et al.*, "Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres," *Nature*, vol. 526, pp. 682–686, Oct 2015. 17

[16] R. Van Meter and J. Touch, "Designing quantum repeater networks," *IEEE Communications Magazine*, vol. 51, no. 8, pp. 64–71, 2013. 18, 19, 21, 22

[17] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," *Nature Communications*, vol. 8, p. 15043, Apr 2017. 21

[18] S. Muralidharan, L. Li, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, "Optimal architectures for long distance quantum communication," *Scientific reports*, vol. 6, p. 20463, 2016. 22

[19] M. Chiani, A. Conti, and M. Z. Win, "Piggybacking on quantum streams," *Phys. Rev. A*, vol. 102, p. 012410, Jul 2020. 23, 24, 26, 27, 33, 34, 65

[20] A. W. Cross, L. S. Bishop, J. A. Smolin, and J. M. Gambetta, "Open quantum assembly language," 2017. 47

List of Figures

List of Tables