Analysis and computation of DV and CV-QKD information rates

Project for the Information Theory course of Professor M. Magarini

Gabriele Lecce[1] and Roberto Scardia[1]

[1]Dipartimento di Ingegneria Informatica, Elettronica e Bioingegneria, Politecnico di Milano, Master degree in Telecommunication Engineering

I. Introduction

In this literature review, we will lay out the necessary quantum mechanics and quantum information concepts needed to understand the meaning and consequences of the Holevo's bound in quantum information theory. We will show that classical information theory is a particular case of quantum information theory, and in the final part we will discuss some applications of quantum mechanics in the field of optical communications. In particular, we will focus on the adverse impact of non-ideal effects on the information rate of continuous-variable quantum key distribution protocols.

II. Quantum mechanics

Reasonably, a treatise on quantum mechanics should start with the definition of quantum states: historically, they evolved from the classical concept of "state" for a dynamic system. In classical physics, to describe the evolution of a dynamic system, it is not sufficient to know only the physical law that governs that particular system. It is also required to use the information given by the values of the state variables that describe the system, and, in general, it is possible to organize these values inside a "state vector". In the same way, a "quantum state" is the mathematical entity that embeds the information needed to describe the evolution of a quantum system.
In the context of quantum information, the most useful mathematical representation of a quantum state is the vectorial representation: in the same way classical states can be organized in vectors, the quantum states are thought to be components of a Hilbert space equipped with a scalar product. A Hilbert space is the generalization of the classical Euclidean vector space to possibly infinite dimension spaces where the classical ideas of (but not limited to) scalar product, distance, Pythagorean theorem, and Cauchy-Schwarz inequality still hold. The need for infinite-dimensional Hilbert space in quantum mechanics presents itself in the case, for example, of the more known wave representation of quantum states; however, it will be shown that in some areas of quantum information theory finite-dimensional Hilbert spaces are enough. In the vector representation, an isolated quantum state is a uni-dimensional subspace of a Hilbert space $\mathscr{H}$: every vector $|\psi\rangle \in \mathscr{H}$ represents a different state apart from a complex constant λ, and every vector belonging to the same "line" or "ray" represents the same (isolated) quantum state. This kind of isolated state (i.e., not considered in an ensemble with other quantum states) is called a pure state, and, in general, it is regarded as its representative vector an element of its subspace with norm one, that is, $\langle\psi|\,|\psi\rangle = 1$. Note that multiple such normalized vectors exist and are distinguished by a pure phase factor $e^{i\phi}$.

What we described in the previous section is the first postulate of quantum mechanics:

Postulate 1: Associated to any isolated physical system is a complex vector space with inner product (that is, a Hilbert space) known as the state space of the system. The system is fully described by its state vector, which is a unit vector in the state space of the system. [1]

From the theory of linear algebra, it is known that every element belonging to a vector (Hilbert) space can be expressed as a linear combination of the basis of the same space.

$$\mathscr{H} = \mathscr{L}\{B_{\mathscr{H}}\}$$

In quantum mechanics, this property of Hilbert spaces is called "superposition": each state can be expressed as the superposition of different states multiplied by a complex constant.
We said earlier that quantum information limits its scope to two-dimensional state space: the elements of such spaces are called qubits (from the portmanteau of quantum bits). Typically the canonical basis of a qubits space is denoted as

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

but others are known such as the computational basis

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

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

In general, a pure quantum state is nearly impossible to be physically realized and we have to resort to a probabilistic description of our quantum system. These uncertain states are called "mixed states" and arise not only in the preparation of real quantum systems but also in the case of entangled states.

Such description can be obtained by modeling it as an ensemble of pure quantum states ψ_i with a priori probabilities p_i using the concept of density operator ρ:

$$\rho = \sum_i p_i \left|\psi_i\right\rangle \left\langle\psi_i\right|$$

The density operator can also be defined for a pure state ψ as:

$$\rho_\psi = \left|\psi\right\rangle \left\langle\psi\right|$$

That can be generalized in the case that our quantum system is in a mixed state:

$$\rho = \sum_i p_i \rho_i$$

Where ρ_i is the density operator of the pure states that compose the ensemble. It's easy to verify that ρ is always positive and its trace is equal to one. Mixed states are not to be confused with the superposition of states: superposition results from the linearity of the operator that governs the quantum processes and no probability is involved until the measurement of such states occurs. The second postulate is of fundamental importance, because it states the properties of the evolution of a quantum system.

Postulate 2: The evolution of a closed quantum system is described by a unitary transformation. That is, the state $\left|\psi\right\rangle$ of the system at time t_1 is related to the state $\left|\psi\right\rangle'$ of the system at time t_2 by a unitary operator U which depends only on the times t_1 and t_2 [1]

In other words, in order to apply computation on qubits, "quantum" gates need to be unitary operators. Unitarity implies that U must be a linear operator and that its inverse exists and equal to its adjoin, i.e. $UU^\dagger = U^\dagger U = I$. Since also $U^\dagger$ is an unitary operator, this implies that all quantum gates need to implement a reversible operation.

What our discussion on quantum mechanics lacks at this point is a description of what happens during the measurement process: when a quantum state is measured, the quantum system has to interact with the measurement apparatus so it cannot be considered a closed quantum system and the second postulate cannot be considered valid. In the same way that QM doesn't describe the laws involved with the evolution of the system, it does not prescribe a particular apparatus or practical procedure to carry out a quantum measure but lays out the mathematical foundation to describe the results.
The third and last postulate of QM states the following:

Postulate 3: Quantum measurements are described by a collection M_m of measurement operators. These are operators acting on the state space of the system being measured. The index m refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is $\left|\psi\right\rangle$ immediately before the measurement then the probability that result m occurs is given by

$$p(m) = \left\langle\psi\right| M_m^\dagger M_m \left|\psi\right\rangle$$

and the state of the system after the measurement is

$$\frac{M_m \left|\psi\right\rangle}{\sqrt{\left\langle\psi\right| M_m^\dagger M_m \left|\psi\right\rangle}}$$

The measurement operators satisfy the completeness equation,

$$\sum_m M_m^\dagger M_m = I$$

The completeness equation expresses the fact that probabilities sum to one[1]:

$$\sum_m p(m) = \sum_m \left\langle\psi\right| M_m^\dagger M_m \left|\psi\right\rangle = 1$$

The states here are considered to have norm equal to one. A quantum measure involves necessarily a probabilistic description: while in classical physics we need a statistical description (being classical or Bayesian) to account for noise and measurement error, in QM the result of the measurement operation is intrinsically probabilistic. For example, a valid example of measurement operator collection on qubits is the set composed by the density operator of the canonical basis, $M_0 = \left|0\right\rangle \left\langle 0\right|$, $M_1 = \left|1\right\rangle \left\langle 1\right|$. If we consider a state $\psi = a\left|0\right\rangle + b\left|1\right\rangle$ the probability of measuring the state 0 or 1 is:

$$p(0/1) = \left\langle\psi\right| M_{0/1}^\dagger M_{0/1} \left|\psi\right\rangle = \left\langle\psi\right| M_{0/1} \left|\psi\right\rangle = |a/b|^2$$

where the hermiticity property of the density operator $(M_{0/1} = M_{0/1}^\dagger, M_{0/1}^2 = M_{0/1}$ is used. In this specific example, we choose to use the density operator of two orthogonal states ($\left\langle 0\right|\left|1\right\rangle = 0$, by definition of canonical basis) and if the state ψ were equal to 0 or 1 we would have been able to measure 0 or 1 with probability 1 respectively. However, this is only true for states that are orthogonal, and, in general, for two states that are not orthogonal it does not exist a measurement set with this property. For this reason, two states that are not orthogonal are called *non-distinguishable states*.
In general, the operators in the measurement set do not have to be unitary. In case they possess this property (i.e. the second postulate is respected during the measurement) and are orthogonal ($M_m M_n = 0 \; for \; m \neq n$) we are in the special case of *projective measurement*. In projective measurement, an operator M called *observable* is defined with spectral decomposition

$$M = \sum_m m P_m$$

where m is one of its eigenvalue and P_m the orthogonal projectors over its eigenspaces; those compose the measurement set. The previous example can be understood as a case of projective measurement and the same simplifications for

calculating the probability distribution can be applied:

$$p(m) = \langle\psi| P_m |\psi\rangle$$

The resulting state after a projective measurement is $\frac{P_m|\psi\rangle}{\sqrt{p(m)}}$ i.e. one of the states described by the eigenspaces of M.
Another special case of the third postulate that is thoroughly used in quantum information is the Positive Operator-Value Measure: instead of singularly choosing the measurement operators M_m such that they respect the completeness equation as a measurement set whatever choice of E_m such that $\sum_m E_m = I$. This formalism is useful whenever after the measure there is no interest in the state of the system or the measurement is not repeatable. By definition, projective measurement describes a repeatable procedure: after obtaining the state $|\phi_m\rangle$ as the result of the measure by repeating the measurement with the same set we re-obtain $|\phi_m\rangle$ with probability one. In quantum information we are often only interested in the statistics of the measure and not in the evolution of the system and the utility of this formalism will be shown in the following paragraphs.
A quantum phenomenon that plays an important role in both quantum information theory and quantum cryptography is the no-cloning theorem. Suppose that we have a device that can duplicate quantum states: if we want to copy a pure state $|\psi\rangle$ in a blank state $|X\rangle$ we have to apply a unitary operator on the system:

$$U |\psi\rangle |X\rangle = |\psi\rangle |\psi\rangle$$

And this is true for all the orthogonal $|\psi_i\rangle$ forming a space vector. However, it's not possible to duplicate a non-orthogonal state [2] e.g. $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$:

$$U\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|X\rangle = U\frac{1}{\sqrt{2}}(|0\rangle|X\rangle) + U\frac{1}{\sqrt{2}}(|1\rangle|X\rangle) =$$

$$= \frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|1\rangle$$

That is different from what we expected:

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \neq \frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|1\rangle$$

III. Quantum information

In "classical" information theory Shannon's entropy is defined as the measure of information of a memory-less stationary source, for which we know the probability $P(X)$ of a set of symbols {X}:

$$H(X) = -\sum_X P(X)\log_2 P(X)$$

To describe a set of quantum states $\{\psi\}$, probability distributions are replaced by density operators. The natural extension of the Shannon's entropy is the Von Neumann entropy, defined as:

$$S(\rho) = -tr(\rho\log\rho) = -\sum_\psi \lambda_\psi \log\lambda_\psi$$

Where λ_ψ are the eigenvalues of the density operator ρ. We can easily verify that if the states of the alphabet are orthogonal (e.g. $\{X\} = \{|0\rangle, |1\rangle\}$), the Von Neumann entropy coincides with Shannon's entropy:

$$\rho = p|0\rangle\langle 0| + (1-p)|1\rangle\langle 1| = \begin{bmatrix} p & 0 \\ 0 & 1-p \end{bmatrix}$$

$$\Rightarrow S(\rho) = -p\log_2 p - (1-p)\log_2(1-p) = \log_2\frac{(1-p)^{p-1}}{p^p}$$

That coincides with Shannon's entropy of a binary source. Suppose the dimension d of the space vector C^d can be considered as the number of symbols in a classical alphabet. In that case, the Von Neumann entropy is upper bounded by:

$$S(\rho) \leq log_2(d)$$

And in general, for an ensemble of non-orthogonal pure quantum states (in this case ρ is not hermitian) we have:

$$S(\rho) \leq H(X)$$

It is possible to verify that the single pure state i of the ensemble has the property $S(\rho_i) = 0$[3]. In the most general case, when an ensemble of mixed states describes our system, we have the following upper bound:

$$S(\rho) \leq \sum_i p_i S(\rho_i) + H(X)$$

that is held with equality only when the states ρ_i have orthogonal support. If we rewrite the last expressions as follows:

$$S(\rho) - \sum_i p_i S(\rho_i) \leq H(X)$$

We can identify a quantity:

$$\chi(\rho_i) = S(\rho) - \sum_i p_i S(\rho_i)$$

that is the Holevo information of our ensemble. This quantity can be regarded as a generalization of the Von Neumann entropy when we send messages constructed from an alphabet of non-orthogonal mixed states. It will play an important role when we will describe the Holevo's bound.

When we use non-orthogonal states, a new "quantum" problem arises. Suppose that our source can only send symbols from an ensemble of two non-orthogonal states e.g. $\{|0\rangle, \frac{|0\rangle+|1\rangle}{\sqrt{2}}\}$ and we want to measure them with a set E of POVM elements. We can define[1]:

$$E_1 = \frac{\sqrt{2}}{1+\sqrt{2}}|1\rangle\langle 1|,$$

$$E_2 = \frac{\sqrt{2}}{1+\sqrt{2}}\frac{(|0\rangle - |1\rangle)(\langle 0| - \langle 1|)}{2}$$

such that we always have state $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ when we measure E_1 and state $|0\rangle$ when we measure E_2. However the set $\{E_1, E_2\}$ does not satisfy completeness relation $\sum_m E_m = I$, which is only satisfied by adding a third operator $E_3 = I - E_1 - E_2$, that gives no information about the identity of the measured the state:

$$\langle\psi_i| E_3 |\psi_i\rangle \neq 0, 1$$

That means that if we use non-orthogonal states we don't have perfect reliability. This is the accessible information problem, and can be seen as a direct consequence of the no-cloning theorem. This is never seen in classical information theory, since its symbols are always pure orthogonal states. To quantify how can we know about the accessible information, we can use another classical information theory concept known as mutual information:

$$I(X,Y) = H(X) - H(X|Y)$$

This is a measurement of the degree of correlation between two random variables, in our case the state measured is Y and the state sent is X. In classical noiseless channels, the mutual information is always equal to the Shannon entropy of the source, since there isn't a problem with accessible information. We expect that in quantum information this inequality holds:

$$I(X,Y) \leq H(X)$$

and is satisfied with equality when the quantum system can only find itself in orthogonal states. In the next chapter, we wish to connect the Holevo quantity and the mutual information to get more general results.

IV. Holevo's bound

The Holevo's bound is one of the most important results in quantum information theory. Suppose that one actor has prepared a quantum state with density operator ρ_X choosing over n different possible states with probability p_x $x \in [0,n]$. A second actor has then measured this state with a POVM set $E_y = E_0, ..., E_y$ with measure outcome Y. The Holevo's bound states that for such measurement:

$$I(X,Y) \leq S(\rho) - \sum_x p_x S(\rho_x) = \chi$$

where $\rho = \sum_x p_x \rho_x$ and χ is the Holevo χ quantity[1].

Using Holevo bound and the results from the previous chapter, we can relate the mutual information of a quantum source described by an alphabet of mixed states with Shannon's entropy of that source:

$$I(X,Y) \leq \chi(\rho_i) \leq H(X)$$

This means that the mutual information is strictly less than $H(X)$ when ρ_i doesn't have orthogonal support, or in other words, when the mixed states of the alphabet are not orthogonal. This is the generalization of what was shown in the previous chapter for the simplified case of a quantum system with an alphabet of non-orthogonal pure states.

To show the importance of the orthogonality of the mixed states, let's switch for a moment to a 3-dimensional Hilbert space. Suppose we take ρ_i from the ensemble of pure orthogonal states $X = \{|0\rangle, |1\rangle, |2\rangle\}$. We choose $\rho_1 = q\,|0\rangle\langle 0| + (1-q)\,|1\rangle\langle 1|$ and $\rho_2 = p\,|1\rangle\langle 1| + (1-p)\,|2\rangle\langle 2|$ to be the mixed states of our system. The density operator of the system is $\rho = \frac{1}{2}\rho_1 + \frac{1}{2}\rho_2$, so the Holevo quantity is upper bounded by the binary entropy: H(X) = 1. When $q = 1$ or $p = 0$, the mixed states are orthogonal, so we expect the Holevo quantity to be independent of respectively p or q. We compute the Von Neumann entropies for this system:

$$\rho_1 = \begin{bmatrix} q & 0 & 0 \\ 0 & 1-q & 0 \\ 0 & 0 & 0 \end{bmatrix} \Rightarrow S(\rho_1) = H_2(q);$$

$$\rho_2 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & p & 0 \\ 0 & 0 & 1-p \end{bmatrix} \Rightarrow S(\rho_2) = H_2(p);$$

$$\rho = \frac{1}{2}\begin{bmatrix} q & 0 & 0 \\ 0 & (1-q)+p & 0 \\ 0 & 0 & 1-p \end{bmatrix}$$

$$\Rightarrow S(\rho) = -\frac{1}{2}[q\log(\frac{q}{2}) + (1-p)\log(\frac{1-p}{2}) + (1-q+p)\log(\frac{1-q+p}{2})]$$

$$= 1 + \frac{1}{2}(H_2(p) + H_2(q) + \log\frac{p^p(1-q)^{1-q}}{(1-q+p)^{1-q+p}})$$

We can finally write the Holevo quantity χ:

$$\chi(q,p) = S(\rho) - \sum_i p_i S(\rho_i) = 1 + \frac{1}{2}\log\frac{p^p(1-q)^{1-q}}{(1-q+p)^{1-q+p}}$$

$$\Rightarrow \chi(q,p) = 1 + G(q,p) \leq H(X) = 1$$

And as we expected:

$$G(1,p) = G(q,0) = \log_2 1 = 0 \Rightarrow \chi = 1 = H(X)$$

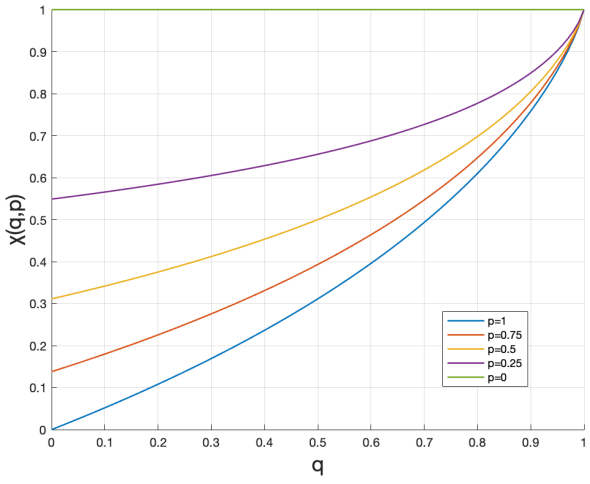

Figure 1: Holevo quantity χ as function of q and p.

If p it's set and we increase q, the Holevo quantity increases because the mixed states approach the orthogonality condition. The mutual information of this quantum system is upper bounded by:

$$I(X,Y) \leq 1$$

If we choose a proper POVM set and two orthogonal mixed states, we can achieve $I(X,Y) = 1$. Suppose to pick the

particular case $\{X\} = \{\frac{1}{2}(|0\rangle + |1\rangle), |2\rangle\} = \{|\psi_1\rangle, |\psi_2\rangle\}$, we can calculate the POVM as:

$$\langle\psi_1| E_1 |\psi_1\rangle = 1 \Rightarrow E_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

$$\langle\psi_2| E_2 |\psi_2\rangle = 1 \Rightarrow E_2 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Where the completeness relation has been used to maximize the mutual information:

$$\sum_m E_m = E_1 + E_2 = I$$

We have found that optimal measurement determined by the ensemble has the property:

$$p(m) = \delta_{m,x}$$

Where $\delta_{m,x}$ is the Kronecker delta. We can now better define the concept of accessible information as the maximization of the mutual information over all the sets $\{E_m\}$ of possible POVM measurements [4]:

$$I_{acc} = \max_{\{E_m\}} I(X, Y)$$

We have seen that orthogonal states are perfectly distinguishable, however it's not possible to maximize the mutual information in this way when the mixed states are non-orthogonal ($\chi < H(X)$). If we use an alphabet of pure states (to simplify the expression of χ), we expect that:

$$I(X, Y) \leq \chi = S(\rho) < H(X)$$

Furthermore, it's also more complicated to guess what is the optimal POVM measurement. In some cases we can exploit symmetries, for example, if we take an ensemble of pure states which have a three-fold symmetry e.g.:

$$\{\psi_i\} = \{\cos(\frac{2\pi}{3} * n) |0\rangle + \sin(\frac{2\pi}{3} * n) |1\rangle\} =$$

$$\{|0\rangle, -\frac{1}{2} |0\rangle + \frac{\sqrt{3}}{2} |1\rangle, -\frac{1}{2} |0\rangle + -\frac{\sqrt{3}}{2} |1\rangle\}$$

with n=0,1,2 and the same a priori probabilities, it is possible to construct an optimal POVM with the same symmetry, that achieves[5]:

$$I_{acc} \simeq 0.58496 < S(\rho) = 1$$

We could try and group states in a similar way to classical information theory:

$$|\psi\rangle = |\psi_i\rangle_1 |\psi_i\rangle_2 ... |\psi_i\rangle_m$$

In this way, we would have 3^m possible "codewords". However, it is possible to demonstrate that the accessible information doesn't change. A better strategy is the Peres-Wootters method [6]: instead of using all the 3^m codewords built before, we just use three codewords formed by repeating m times one of the three pure states of the ensemble, e.g. for the first state:

$$|\psi_1\rangle = |0\rangle_1 |0\rangle_2 ... |0\rangle_m$$

In this way the three new states $|\psi_i\rangle$ are more distinguishable; for the case m = 2 we have an improvement of the Von Neumann entropy:

$$S(\rho)_m = S(\rho)_2 = 1.5 < H(X) = \log_2 3$$

We can say that they are more distinguishable because the inner product with the other states is more orthogonal increasing m, in other words:

$$\langle\psi_i| |\psi_j\rangle_m > \langle\psi_i| |\psi_j\rangle_{m+1}, i \neq j$$

In fact for the $m = 2$ case, we improve the maximum mutual information:

$$I_{acc,m=2} = 1.36907 > 0.58496$$

The most fundamental concept that the Peres-Wooters method highlights is that it's better to group qubits to create an alphabet with just the more distinguishable letters. Furthermore, we want to measure these states using a POVM constructed by a procedure called PGM ("pretty good measurements")[5], which gives the maximization of the mutual information.

We can also extend this method to an ensemble of non-orthogonal mixed states, saying that when $m \to \infty$ the accessible information tends to the Holevo's quantity:

$$I_{acc,m\to\infty} \to \chi(\rho_i)$$

We can say, from what we have shown in this paragraph, that the accessible information plays a role similar to the capacity of a channel in classical information theory: it tells us how many "classical" bits of information can be reliably transmitted over the channel. In order to have a good accessible information, we can maximize the Holevo's quantity by using longer codewords and by choosing the optimal POVM set of the system.

V. Discrete-Variable QKD

One of the most important applications of quantum information theory and cryptography is Quantum Key Distribution: a secret key is exchanged through a quantum communication channel using quantum states, and then it can be used as a one-time pad key in a cryptosystem[7]. The BB84 protocol is the first QKD protocol ever proposed, and it was made by Charles H. Bennett and Gilles Brassard in 1984 [8], [9]. It exploits the polarization of photons, a continuous parameter that can be regarded quantistically as the photon spin[10], a vector in a 2-dimensional Hilbert space, hence a qubit. In classical communication, channel messages can be secretly monitored by an eavesdropper without the knowledge of the sender or the receiver; in QKD when the qubits are intercepted, the no-cloning theorem assures that they can only be measured by perturbing their state, so the receiver may notice that someone was eavesdropping the channel by receiving unexpected results. At first, without considering eavesdropping, the protocol works as follows: a sender (Alice) prepares with equal probabilities a photon in a rectilinear polarization (state $|0\rangle$ or $|1\rangle$) or in a diagonal polarization (state $\frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle$

or $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$) and sends it to the receiver (Bob). The different states of a polarization basis encode bit 0 or bit 1. We define as the efficiency of retrieving the secret key the capacity of the channel, which in the case of fixed source probabilities is just the mutual information. Our quantum system can be described by the matrix:

$$\rho = \begin{bmatrix} 3/4 & 0 \\ 0 & 1/4 \end{bmatrix}$$

Which gives $I_{acc} = \chi = 0.3113$ [bits/channel use]. This means that on average we have to use the channel $1/I_{acc} \simeq 3.21$ times to get a bit of the secret key. However, this is not the actual functioning mechanism of QKD. After having received all the qubits, Alice and Bob communicate over an ordinary non-quantum channel to compare the polarization basis used to send and receive the message. This operation is called basis *reconciliation*, and when the same basis is used, Bob can keep the content of the qubit; otherwise, the received bit must be discarded. Following this procedure, the newly generated secret key is referred to as the *sifted* key. The protocol can be modeled by a binary erasure channel with source probabilities $P(X_1) = P(X_2) = 0.5$, and conditional probabilities $P(y = 0|x = 0) = P(1|1) = P(e|0) = P(e|1) = 0.5$ and $P(1|0) = P(0|1) = 0$:

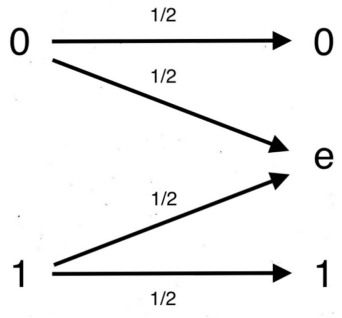

Figure 2: BB84 channel model (withouth eavesdropping).

The mutual information of this channel is $I(X,Y)_{BB84} = 0.5$, which means that the public discussion between Alice and Bob has improved the efficiency of the channel. The channel has the following probability matrix:

$$\underline{\mathrm{P}}_{BB84} = \begin{bmatrix} 1/2 & 0 & 1/2 \\ 0 & 1/2 & 1/2 \end{bmatrix}$$

In this way we get a bit every 2 channel uses, as expected by the protocol. A more generalized version of this protocol, called the six-state protocol, adds the circular polarization to the possible basis. The circular basis introduces two more states: $\frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle$ and $\frac{1}{\sqrt{2}}|0\rangle - \frac{i}{\sqrt{2}}|1\rangle$, and the channel assumes the following probability matrix:

$$\underline{\mathrm{P}}_{ssp} = \begin{bmatrix} 1/3 & 0 & 2/3 \\ 0 & 1/3 & 2/3 \end{bmatrix}$$

With source probabilities $P(X_i) = 1/2$, and channel model as in figure 3

This protocol achieves a lower mutual information:

$$I(X,Y)_{SSP} = 1/3$$

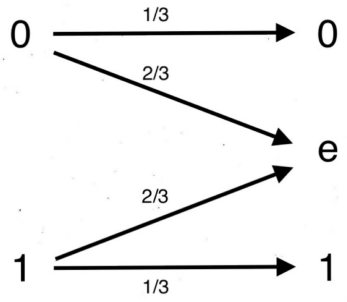

Figure 3: Six-state protocol channel model (withouth eavesdropping).

We receive, on average, a bit for the secret key every 3 channel uses, which is worse than the BB84 protocol. However, as we will see in the following examples, the SSP trades it off for better resilience against eavesdropping.

VI. Discrete-Variable QKD with eavesdropping

Ideally, the sifted keys obtained by Alice and Bob should be the same, but in a real scenario we also have to consider the presence of an eavesdropper (Eve) and its effect on the channel capacity. It is a difficult task to bring together information theory and quantum mechanics, because they can be combined in several ways, depending on the protocol used and on the way the eavesdropping is performed. Therefore, we focus on a specific type of *individual* attacks: the intercept-resend. Eve's task is to intercept all photons individually, to measure them, and to re-send them in the same state they were obtained. The intrusion of Eve can be noticed only when Bob chooses the same polarization basis as Alice, because otherwise the bit is discarded *a priori*. When Eve re-sends a photon with the same basis as Alice and Bob, but in a different state, the bit received is flipped, and Bob notices the presence of the eavesdropper. For the BB84, we can implement the presence of Eve using the following channel model (source probabilities $P(X_i) = 1/2$):

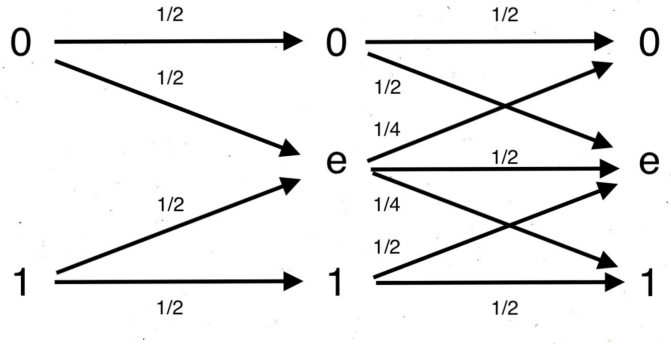

Figure 4: BB84 channel model (intercept-resend attack).

We can calculate a quantity called Quantum Bit Error Rate (QBER), which is defined as the number of the wrong (flipped)

bits of the sifted key over the length of the sifted key:

$$QBER_{BB84} = \frac{P(y=1|x=0)}{P(y=0|x=0)+P(y=1|x=0)} =$$

$$= \frac{1/8}{(1/4+1/8)+1/8} = 1/4 = 25\%$$

Due to the errors, the sifted key shared between Alice and Bob is not the same anymore, so we need to apply an error correction code to have a better match between them. Furthermore, now Eve has knowledge of some bits of the secret key, so we need to apply a privacy amplification protocol to reduce its information. The information received by Eve is equal to the information of a channel without eavesdropping, so we use the result of the previous chapter: $I(X, Eve) = 0.5$. In order to calculate $I(X, Y)$, we need to define the probability matrix of the new channel model:

$$\underline{\mathrm{P}}_{BB84,X\to Y} = \begin{bmatrix} 3/8 & 1/8 & 1/2 \\ 1/8 & 3/8 & 1/2 \end{bmatrix}$$

We obtain: $I(X, Y) = 0.0944$. We also calculate $I(Eve, Y) = 0.25$, considering the channel between Eve and Bob ($P(Eve = e) = 1/2, P(Eve = 0, 1) = 1/4$):

$$\underline{\mathrm{P}}_{BB84,Eve\to Y} = \begin{bmatrix} 1/2 & 1/2 & 0 \\ 1/4 & 1/2 & 1/4 \\ 0 & 1/2 & 1/2 \end{bmatrix}$$

To verify whether we can apply error correction and privacy amplification to the sifted key, we use the Csiszár-Körner theorem[11], [12]: if $I(X, Y) \geq \min(I(X, Eve), I(Eve, Y)) \Rightarrow$ a secret key can be obtained. In our case $I(X, Y)$ is lower than the other two mutual informations, however, we have to consider that Eve isn't always present in the channel, so the real capacity is an average between the channel with and without eavesdropping. We define a new variable μ, as how many photons are intercepted by Eve over the number of photons sent by Alice. We calculate the minimum μ for which the Csiszár-Körner theorem is fulfilled (how much Eve can interfere), taking as lower bound $I(Eve, Y) = 0.25 < I(X, Eve)$:

$$I(X,Y)_{no,Eve}(1-\mu) + I(X,Y)_{Eve} \cdot \mu \geq I(Eve, Y)$$

$$0.5(1-\mu) + 0.0944\mu \geq 0.25$$

$$\Rightarrow \mu_{BB84} \leq 0.6164$$

Therefore, the maximum QBER tolerated by the BB84 is:

$$QBER_{MAX,BB84} = QBER_{BB84} \cdot \mu = (25\%) \cdot 0.6164 \simeq 15.4\%$$

Which is analogous to the result obtained by Gisin et al. [11].

The same procedure can be applied to analyze the six-state protocol, which has the following channel model and probability matrix:

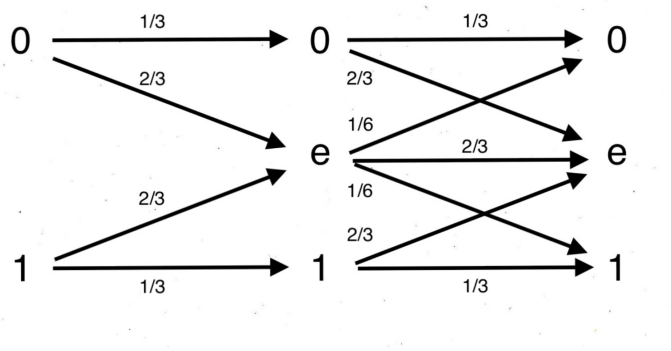

Figure 5: six-state protocol channel model (intercept-resend attack).

$$\underline{\mathrm{P}}_{SSP,X\to Y} = \begin{bmatrix} 2/9 & 2/3 & 1/9 \\ 1/9 & 2/3 & 2/9 \end{bmatrix}$$

We obtain $I(X, Y) = 0.0272$ (source probabilities $P(X_i) = 1/2$) and a QBER:

$$QBER_{ssp} = \frac{2/18}{(1/9+2/18)+2/18} = 1/3 = 33.3\%$$

The maximum QBER for the six-state protocol is found applying again the Csiszár-Körner theorem. As a first step, we calculate the other mutual information: $I(X, Eve) = 1/3$, it is the same as a channel without eavesdropping, and $I(Eve, Y) \simeq 0.1111$ is obtained using the following probability matrix (Eve probabilities $P(Eve = e) = 2/3$, $P(Eve = 0, 1) = 1/6$):

$$\underline{\mathrm{P}}_{SSP,Eve\to Y} = \begin{bmatrix} 1/3 & 2/3 & 0 \\ 1/6 & 2/3 & 1/6 \\ 0 & 2/3 & 1/3 \end{bmatrix}$$

Applying the theorem, we find:

$$(1/3)(1-\mu) + 0.0272\mu \geq 0.1111$$

$$\Rightarrow \mu_{ssp} \leq 0.7259$$

$$\Rightarrow QBER_{MAX,ssp} = (33.3\%) \cdot 0.7259 \simeq 24.2\%$$

This is a higher value than the maximum QBER of BB84, so we have quantitatively demonstrated that the six-state protocol is more resilient against intercept-resend attacks.

VII. Continuous-Variable QKD

As we have shown in the previous paragraph for the specific case of intercept-resend attack, discrete-variable QKD is not hard to analyze in terms of capacity and QBER. However, it is not an easy task to realize an experimental implementation of this category of protocols, because they require single-photon sources (usually approximated with weakly coherent beams) and single-photon detectors. Alternatively, it is possible to use continuous variables of the quantized electromagnetic field,

such as its amplitude and phase, to encode the information. In this case, we just need to produce coherent states of light and to use homodyne detection, which is easier and more efficient than the DV-QKD setup. In this new setting, the concept of qubit, or more in general, qudit, loses significance, and we use the analogue concept of qumode, a quantum state in an infinite Hilbert space. Each mode of this space can be described by the quadrature field operators, $\hat{q}$ and $\hat{p}$. These two operators don't commute, and using the (generalized) Heisenberg uncertainty principle we get a relationship for their variances [13], [14]:

$$\sigma_q^2 \sigma_p^2 \geq N_0$$

Where N_0 is the shot noise level. This means that we can't measure with the same probability both quadratures with arbitrary precision. This result changes the points of the p-q plane of a coherent state into circles:

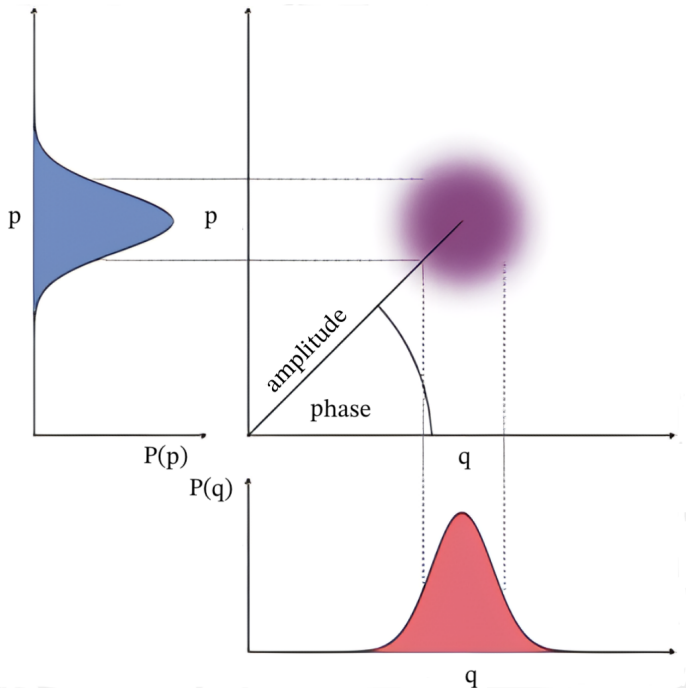

Figure 6: Coherent state with Gaussian Wigner function [13].

Each quantum state can be described by a quasi-probability distribution (Wigner function) which is analogous to the density operator used for qudit systems. Coherent states of light are Gaussian states, this means that they have a Gaussian Wigner function. We're particularly interested in these states because it is known how to generate them with lasers. Morover, also Fock states, which are light pulses in a state with an exact number of photons, are Gaussian states[13], and as it will be shown in the next paragraph, Gaussian modulated Fock states set the maximum capacity obtainable in Bosonic Gaussian channels. The simplest CV-QKD protocol that exploits coherent states is the GG02 [15], and it resembles in some features the BB84 protocol: Alice prepares a finite number of coherent states $|q + ip\rangle$, picking them from a complex Gaussian probability distribution with zero mean and variance V. The states are sent to Bob, which measures randomly one of the quadratures with homodyne detection. The measurement is optimal, which means that the variance added is just equal to the (intrinsic) shot-noise N_0. We can also consider other noise parameters such as transmission efficiency τ and excess noise ξ (channel noise), and quantum efficiency η and electric noise v_{el} (non-ideal detection noise). The Gaussian variable received by Bob is the sum of one of the variables sent by Alice, X_A, with the Gaussian noise variable X_N with variance $V_N = N_0 + \eta\tau\xi + v_{el}$ and zero mean [16]:

$$X_B = \sqrt{\eta\tau}(X_A + X_N)$$

With variance:

$$V_B = \eta\tau V_A + V_N$$

Using a classical public channel, Bob informs Alice about which quadrature was measured, and about half of the key is discarded. The steps remaining consist in the usual post-processing. It includes, similarly to DV-QKD, error correction, parameter estimation and privacy amplification.

To simplify the analysis of the protocol in terms of key extraction, information rate and QBER, it's convenient to use a discrete modulation of coherent states. In the last paragraph, we will show an implementation of of the GG02 protocol, using a discrete alphabet of symbols-states whose constallation is shaped on a Gaussian distribution [17].

VIII. Holevo's and Shannon's bound in Optical Communications

In this paragraph we want to show that it's possible to improve the capacity of a channel by switching from a classical encoding of information to a quantum one. So far we have seen that it's not possible to overcome the Shannon's entropy of memory-less stationary source. In real-case scenarios a communication channel is never lossless, and noise modifies the maximum amount of information per channel use that can be reliably communicated. An usual channel model used in optical communication is the AWGN (Additive White Gaussian Noise) channel, in which the noise is considered independent from the input of the channel. Its capacity is computed by finding the maximum of the mutual information all over the possible input distributions, which in the classical case is demonstrated to be also a Gaussian distribution:

$$C = \max_{\{P(X)\}} I(X,Y) = \frac{1}{2}\log(1 + SNR)$$

The SNR is the signal to noise ratio, the average power of the input signal over the average power of the noise. It is possible to use this model to calculate the capacity of an optical communication channel that uses a linearly polarized optical signal in two-quadrature encoding[18], [19] and homodyne detection:

$$C_{S2} = \log(1 + \frac{n_s}{n_n + 1})$$

This capacity is in function of the average received signal photon number (n_s) and the mean number of excess noise photons (n_n) per temporal slot. This approach is semi-classical and doesn't use quantum states to encode the information. However it possible to demonstrate that the same result holds

for coherent states of light, which are the quantum counterpart of the semi-classical approach[20]. Otherwise, it is possible to encode the information in quantum (Fock) states of light containing an average number $\bar{n} = n_s$ of photons with probability p_n. In this case, the mutual information of the channel in absence of excess noise, and using an ideal photodetector is [19]:

$$I(x, y) = -\sum_{n}^{\infty} p_n \log(p_n)$$

Which only needs to be optimized with the physical constraint of conservation of average power (otherwise the best probability would be all equal probabilities, which is physically impossible): $\sum_n^{\infty} np_n = n_s$, to obtain the capacity (or accessible information):

$$C_F = (n_s + 1)\log(n_s + 1) - n_s \log(n_s)$$

that is an higher capacity than C_{S2}. The ensemble of Fock states can be rewritten in the formalism of the previous chapters using the density operator:

$$\rho = \begin{bmatrix} p_1 & 0 & \dots & 0 \\ 0 & p_2 & & \\ \vdots & & \ddots & \\ 0 & & & p_n \end{bmatrix}$$

If we now consider Gaussian noise, after propagating through the channel the quantum states will not be orthogonal pure states, but more general non-orthogonal mixed states, depending on the noise and on the input distribution. The minimum Holevo's quantity at the output of a Bosonic Gaussian Channel (quantum version of AWGN) is achieved by Gaussian input states [21]. If we say that we can perform the best possible measure, the accessible information is equal to the Holevo's quantity, and the following formula is found:

$$\chi = C_H = C_F(n_s + n_n) - C_F(n_s)$$

Comparing this result with the classical capacity, we notice that $C_H \gg C_{S2}$ only when the excess noise is very low (in that case $C_H \simeq C_F$) and the average number of photons is not high enough (in that case $C_H \simeq C_{S2}$). However, it has not yet been found the right optical detection scheme for which the accessible information is equal to the Holevo's bound. We can conclude that, in non-ideal/real case scenarios, we don't get a higher capacity with Fock states, especially when the mean number of photons (n_s) is high enough.

IX. GG02 Channel Model and Simulations

In practice, to implement the GG02 protocol, the input and output constellations are usually discretized. Although this does not impact the security capabilities of the protocol[22],using a lower cardinality constellation intrinsically limits the information (bit) rate of the protocol. Following the example of[17], we sought to investigate the information rate of the GG02 protocol using high-cardinality QAM constellations, simulating the various distortion effects of the optical channel and receiver. As for the input probability distribution, we follow the work of Roumestan et al.[17]; each symbol has probability:

$$P_X(p + iq) = \frac{e^{-v(p^2+q^2)}}{\sum_{p,q} e^{-v(p^2+q^2)}}$$

where p and q are, respectively, the in-phase and in-quadrature components of the symbol.

Various effects can disturb an optical signal that is propagating through a fiber. Attenuation, due to scattering and absorption, weakens the propagating signal, and dispersion broadens the pulse width. The last effect can cause inter-symbol interference after a certain distance, meaning that the receiver will no longer correctly distinguish the symbols because they are overlapped: consequently, we obtain a higher bit

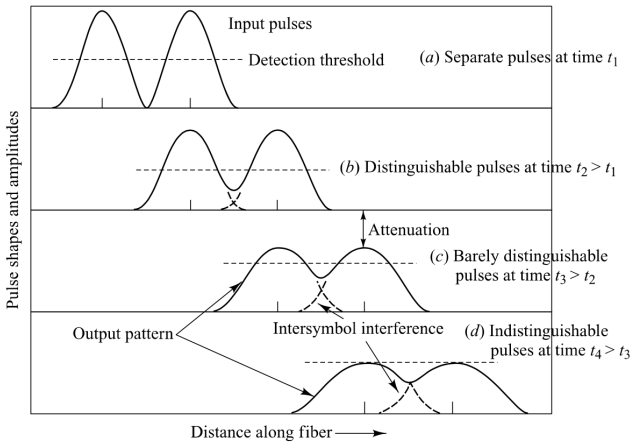

Figure 7: Example of the effect of chromatic dispersion on two consecutive symbol[23].

error rate and a worse capacity. Chromatic dispersion results from the group velocity being a function of the wavelength, so the distortion increases with a large spectral band of the light source. In general, it is the sum of two effects, waveguide dispersion and material dispersion; the first one is the consequence of shorter wavelengths being more confined in the fiber core, so their effective refractive index is more similar to the index of the core, thus changing the beta; material dispersion is caused by the refractive index of the material being a function of the wavelength. To analyze the effects of dispersion, we can model our propagation constant by expanding it with a Taylor series [23]:

$$\beta \simeq \beta_0(w_0) + \beta_1(\omega - \omega_0) + \frac{1}{2}\beta_2(\omega - \omega_0)^2$$

The factor $\beta_2 = \frac{\partial^2 \beta}{\partial \omega^2}$ is the group velocity dispersion (GVD) and it is related to the dispersion:

$$D = -\frac{2\pi c}{\lambda^2}\beta_2$$

which is the result of both the material and the waveguide dispersion.

Chromatic dispersion is one of the main limiting factors in optical communication systems, and it has to be taken

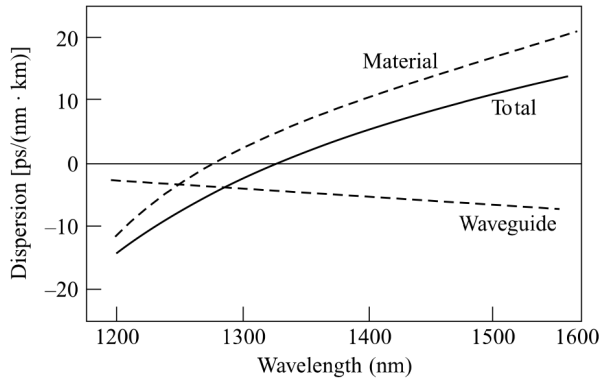

Figure 8: D as function of the wavelength. For a standard mono-mode fiber operating in the C band (1550 nm) D is equal to 17 ps/(nm*km) [23], [24].

into account, either at the physical level using dispersion compensating systems such as fiber gratings and special *dispersion-compensating fiber*, using standard single-mode fibers in the O-band, or by compensating it with digital signal processing.

Another relevant source of noise inside an optical channel originates from the use of optical amplifiers: usually made with erbium-doped glass, they act as a source of non-coherent light, reducing the SNR and changing the statistics of the photo-counting at the receiver from a Poissonian to a Laguerre-Gauss distribution[25]. However, as mentioned in the previous paragraph, we have chosen not to include optical amplifiers within our model. The reason is that the increase in noise that amplifiers introduce is not compatible with the high-cardinality constellation we want to obtain, and it would limit the maximum length of the optical channel. Furthermore, even if non-linear effects are relevant in coherent detection systems[24], we have not included them in our model.

Another aspect that must be taken into account in coherent detection systems is phase noise. Generally, coherent detection is influenced by three factors: phase noise in the local laser, polarization mismatch between the signal and the local laser, and multimode interference. Polarization mismatch becomes relevant only for very high bit rates in long-haul links and can be managed using *polarization diversity receivers*, and multimode interference can be avoided by a correct design of the receiver apparatus[26] or using a single-mode fiber, as in our case. Phase noise[27], on the other hand, is an intrinsic property of whatever laser may be used in our system [28], and as such it has to be included in the simulation of a coherent detection scheme. Starting from the linewidth Δf and the power spectral density D_{PSD} of the laser being taken into account, we modeled the phase noise of the local laser with a Lorentzian power spectral density $S(f) \propto \frac{1}{f^2}$[29].

$$S(f) = \frac{A^2 D_{PSD}}{2\pi} \frac{\Delta f}{\Delta f^2 + f^2}$$

The time samples of the phase jitter are then obtained filtering a Gaussian white noise and cumulating the result in the "phase" domain to obtain the random walk.

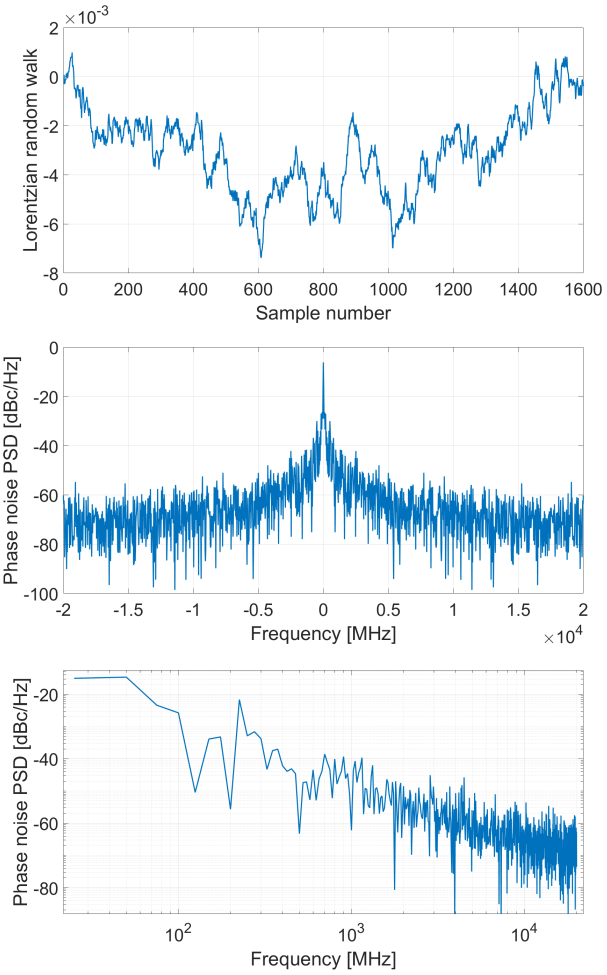

Figure 9: Example of a Lorentzian random walk and its power spectral density in dBc/Hz, with linear and logarithmic frequency axis, obtained by filtering a white Gaussian noise (linewidth 1 kHz).

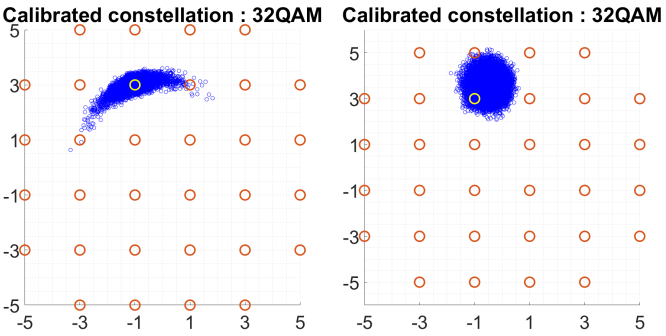

Figure 10: Example of the effect of phase noise (left) and dispersion (right) on the received symbols after gain adjustment, 32-QAM. In yellow the original transmitted symbol.

In our simulations, a G.652[30] fiber has been considered, working with a carrier wavelength at $1550\,\mathrm{nm}$ with a symbol rate of $29\,\mathrm{GHz}$, root raised cosine pulse shaping at the transmitter and respective matched filter at the receiver, with roll off factor $\gamma = 0.2$ and 16 symbol span.

A. Quantum limited mutual information

To approach these effects gradually, we begin our simulations considering propagation without dispersion, phase noise and attenuation, and an ideal detector without dark counts and electrical noise ($\tau = 1, \eta = 1, \xi = 0, v_e = 0$). The relevant effect that remains in this case is the quantum limited shot noise due to the Poissonian photocounting statistics [24]:

$$X_B = X_A + X_N$$

$$V_B = V_A + N_0$$

From the simulation, we obtain the following information rate and QBER of figure 11:

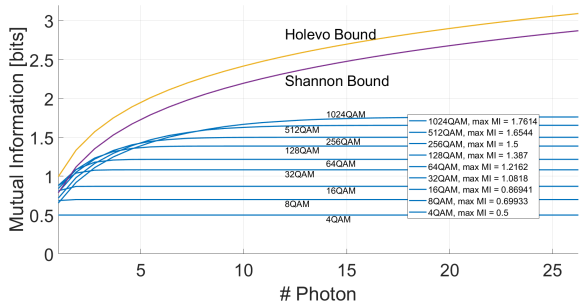

Figure 11: Mutual Information of the various modulation format up to 1024 QAM (quantum limited case).

We immediately notice from these graphs that the discretization of the Gaussian constellation has had a severe impact on the information rate of the protocol. The rate is now constrained for high values of SNR (high number of photons), therefore it tends to saturate to a constant value. Moreover, the rates shown in our graphs are halved due to the fact that on average the protocol discards half of the photons/bits to construct the sifted key. We can increase the rate with a higher number of symbols in the QAM modulation, but this also involves a higher QBER. For all types of modulation formats, the QBER tends to reach zero as the number of photons is large enough. Furthermore, we have included in the first graph the curve given by the Fock states to give an idea of the ultimate (quantum) limit that is possible to reach. Since we are encoding the information in coherent states, our ideal curve is the Shannon curve, obtained with a continuous Gaussian input. To retrieve the bits at the output, we use a hard decoding technique. This type of decoding has been used to simplify the complexity of the system, so as to avoid the use of error correction and privacy amplification. However, the use of this approach increase the error rate of high cardinality constellation formats, which saturates the value of the information rate even with an high number of photons (high input power). This phenomenon can be observed directly on the graph by noticing that the amount of mutual information added when increasing the number of symbols tends to smaller values at each step.

B. Effect of phase noise on mutual information

The phase stability of the local oscillator is of paramount importance in coherent detection, since any error on the phase of the interfering laser will add to the phase of the detected symbol, increasing QBER. In our simulation the phase noise was applied only to the local oscillator at the receiver side. The noise samples were created starting with samples of Gaussian white noise with variance 1 and filtering them with a filter with response $|H_c| = \sqrt{S(f)}$ and random phase generated with Gaussian distributed sample of variance D_{PSD}. In 12 it is reported the result of the mutual information for a local oscillator with linewidth $\Delta f = 1\,\mathrm{kHz}$ and $D_{PSD} = -80\,\mathrm{dBc}$.

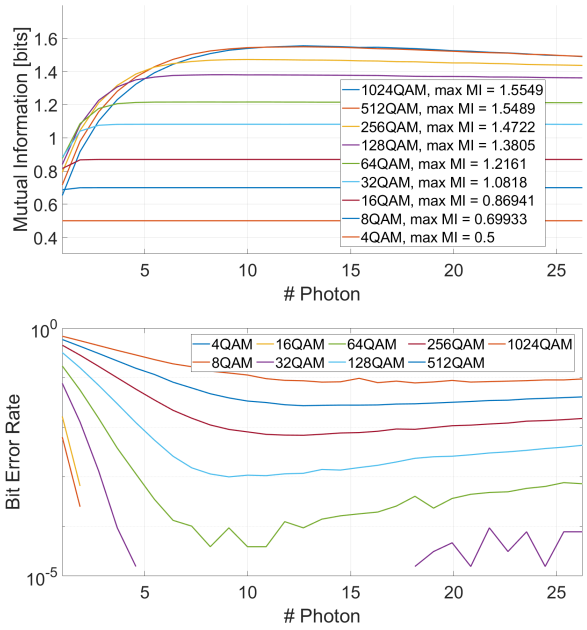

Figure 12: Mutual Information and (Quantum) Bit Error Rate with phase noise at $1\,\mathrm{kHz}$ and $-80\,\mathrm{dBc}$.

We can note an important phenomena that appears for higher cardinality modulation schemes: the QBER seems to increase with the number of photons. This happens because during the simulations the power of the local oscillator is increased, while the signal power remains constant, hence the PSD of the noise process is also increasing with the number of photons. This choice was made because in a real application it is safer and more costly-effective to increase the power of the local laser than the source signal, since non-linear effect could easily incur at the transmitter side, having to compensate for transmission absorption. However, phase noise imposes a limit on the gain mechanism of coherent detection, and in turn limits the length of the optical link in order to maintain a certain optical SNR. Considering a laser with worse performance (e.g. $\Delta f = 10\,\mathrm{kHz}$, $D_{PSD} = -70\,\mathrm{dBc}$) it is possible to appreciate the limiting effect of phase noise even for lower cardinalities.

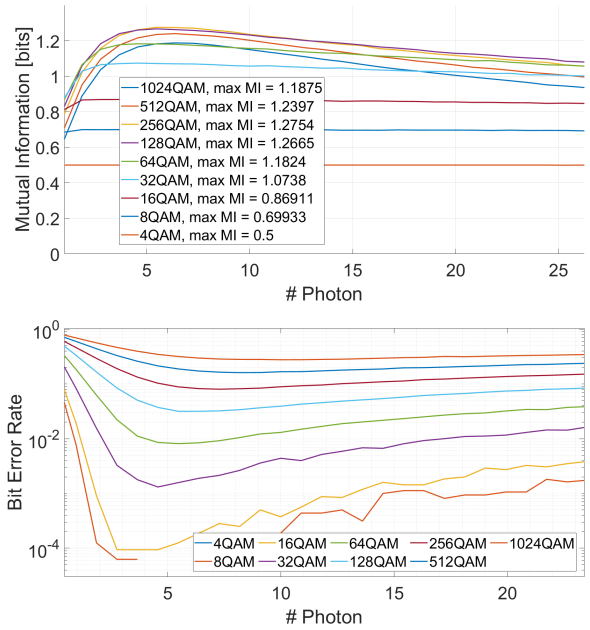

Figure 13: Mutual Information and QBER with phase noise at $10\,\mathrm{kHz}$ and $-70\,\mathrm{dBc}$.

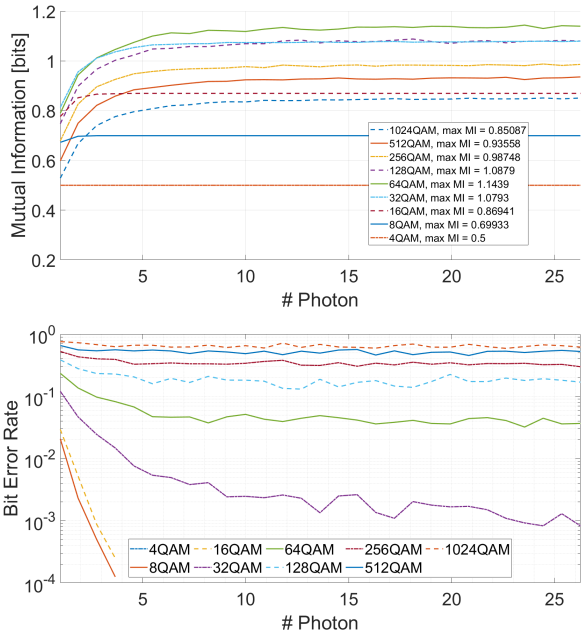

Figure 15: MI and QBER for a L_{max} long link with dispersion of $17\,\mathrm{ps/(km\,nm)}$. The mutual information does not increase monotonically with the size of the modulation constellation, but it peaks at 64-QAM and then decreases.

C. *Effect of dispersion on mutual information*

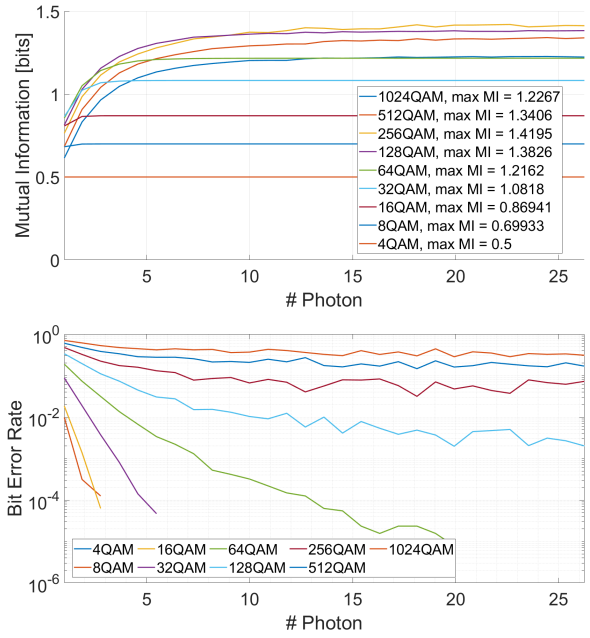

Figure 14: Mutual Information and QBER with dispersion at $17\,\mathrm{ps/(km\,nm)}$ and $L_{max}/2$.

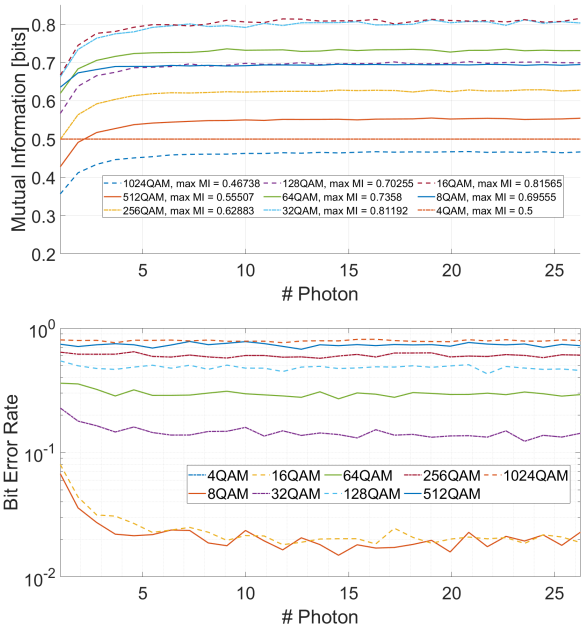

Figure 16: MI and QBER for a $2L_{max}$ long link with dispersion of $17\,\mathrm{ps/(km\,nm)}$. The maximum MI is obtained for the 16-32 QAM formats.

In this section we analyze the effect of dispersion on QBER and mutual information, due to generated intersymbol interference. To simulate these effects a phase filter has been generated considering only the second order dispersion, with β equal:

$$\beta = D\lambda_0^2 f^2 \frac{\pi}{c}$$

D is usually expressed in $[\mathrm{ps/(km\,nm)}]$ and in the case of the G.602 fiber at $1550\,\mathrm{nm}$ is equal to $17\,\mathrm{ps/(km\,nm)}$[30] To estimate the length of the link at which the dispersion effects begins to impact the mutual information we consider the following inequality:

$$B\Delta T < 1$$

where $\Delta T = DL\Delta\lambda$ is the time dilation induced by dispersion

to the symbols[26]. We then obtain

$$L_{max} = \frac{c}{4D\lambda_0^2 B^2}$$

In figures 14, 15, 16, 17 the MI and QBER are reported for a link length of $L_{max}/2$, L_{max}, $L_{max} \cdot 2$, $L_{max} \cdot 5$ respectively.

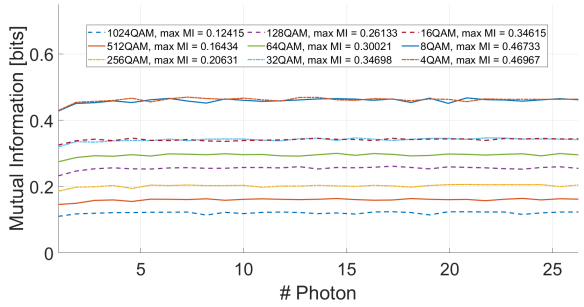

Figure 17: MI for a $5L_{max}$ long link with dispersion of $17\,\mathrm{ps}/(\mathrm{km\,nm})$. The effect of dispersion can be seen also for lower cardinality constellations.

As the signals propagate in the fiber, the accumulated chromatic dispersion degrades the information rates of the various modulation formats. The maximum mutual information tends to shift to lower constellations as we use longer fibers. This shift is a direct consequence of intersymbol interference, since now the SNR is too low to reliably recognize the symbols of high cardinality constellations.

D. Combined effect of phase noise and dispersion

In order to get more reliable results, we add both phase noise and dispersion to our simulation. The results are reported in figure 18. The dominant contribution to the degradation

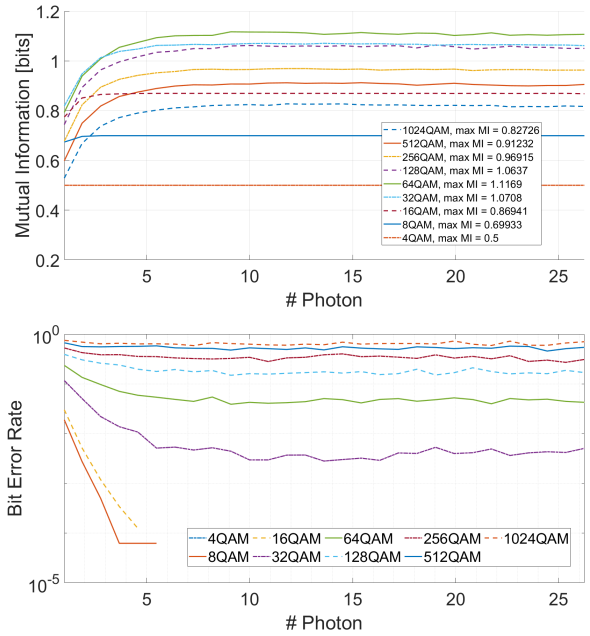

Figure 18: MI and QBER for a L_{max} long link with dispersion of $17\,\mathrm{ps}/(\mathrm{km\,nm})$ and phase noise at $1\,\mathrm{kHz}$ and $-80\,\mathrm{dBc}$.

of mutual information is still the chromatic dispersion; the comparison between figures 15 and 18 shows that only constellations with a high cardinality are significantly impacted by phase noise.

Modulation	Quantum lim.	Phase Noise	Dispersion	PN+Disp
4-QAM	0.5	0.5	0.5	0.5
8-QAM	0.699	0.699	0.699	0.699
16-QAM	0.869	0.869	0.869	0.869
32-QAM	1.082	1.082	1.079	1.07
64-QAM	1.216	1.216	1.144	1.117
128-QAM	1.387	1.38	1.088	1.064
256-QAM	1.5	1.472	0.987	0.969
512-QAM	1.654	1.549	0.936	0.912
1024-QAM	1.761	1.555	0.850	0.827

Table I: Comparison of the maximum mutual Information of the QAM formats for the quantum limited case, only phase noise $1\,\mathrm{kHz}$ $-80\,\mathrm{dBc}$ case, only dispersion $17\,\mathrm{ps\,km^{-1}\,nm^{-1}}$ and $L = L_{max}$ case and dispersion plus phase noise case. Highlighted in blue the maximum capacity for each column.

X. Conclusions and Future Developments

In this analysis, we demonstrated the superior channel capacity of CV-QKD over that of DV-QKD: the information rate of the BB84 protocol can be reached with the use of the GG02 protocol through a straightforward 4-QAM. A further step to improve the results of our analysis could be to enrich the CV-QKD channel simulation by adding more distorting effects such as polarization dispersion, non-linear effects, the presence of different carrier frequencies, electronic noise and dark currents. In addition, different modulation schemes, error correction codes, privacy amplification and soft decoding techniques could be implemented and tested to verify whether there is an improvement in channel capacity. Another aspect that needs to be investigated in the context of QKD is the integration of these protocols into the existing optical network. A recent paper by Alessandro Gagliano et al.[31] has already demonstrated the possibility and requirements for coexistence between the BB84 protocol and other PON standards. We argue that integration of GG02 into existing networks would require less effort, since the use of coherent states for transmission is already well established for other classical communication protocols, but a similar work should be conducted with the GG02 to verify our statement. Experimental work could also be conducted starting from the recent work of Yoann Piétri et al. [32] which describes the realization of an integrated receiver in silicon photonics for a variant of the GG02 protocol.

The source code used for the simulations of this report can be found at https://github.com/robscardi/Quantum_Information_theory_project.

References

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, Dec. 9, 2010, ISBN: 978-0-511-97666-7.

[2] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, Oct. 1982, ISSN: 1476-4687.

[3] Steven J. van Enk, "Mixed and pure states," notes of the course of quantum mechanics, University of Oregon, Apr. 9, 2009. [Online]. Available: https://pages.uoregon.edu/svanenk/solutions/Mixed_states.pdf.

[4] R. O'Donnell and J. Wright, "Lecture 18: Quantum Information Theory and Holevo's Bound," Carnegie Mellon University. [Online]. Available: https://www.cs.cmu.edu/~odonnell/quantum15/QuantumComputationScribeNotesByRyanODonnellAndJohnWright.pdf.

[5] John Preskill, "Quantum Information Theory," notes of the course of quantum computation, California Institute of Technology, [Online]. Available: http://theory.caltech.edu/~preskill/ph229/notes/chap5.pdf.

[6] A. Peres and W. K. Wootters, "Optimal detection of quantum information," *Physical Review Letters*, vol. 66, no. 9, pp. 1119–1122, Mar. 4, 1991.

[7] A. Singh, K. Dev, H. Siljak, H. D. Joshi, and M. Magarini, "Quantum Internet—Applications, Functionalities, Enabling Technologies, Challenges, and Research Directions," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2218–2247, 2021, ISSN: 1553-877X.

[8] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, pp. 7–11, Dec. 2014, ISSN: 03043975.

[9] Gilles Brassard, *Modern Cryptology* (Lecture Notes in Computer Science). Springer New York, 1988, vol. 325, ISBN: 978-0-387-96842-1.

[10] A. Luis and A. Rodil, "Polarization versus photon spin," *Optics Express*, vol. 22, no. 2, pp. 569–1575, 2014.

[11] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum Cryptography," *Reviews of Modern Physics*, vol. 74, no. 1, pp. 145–195, Mar. 8, 2002, ISSN: 0034-6861, 1539-0756. arXiv: quant-ph/0101098.

[12] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978, ISSN: 1557-9654.

[13] R. Wolf, *Quantum Key Distribution: An Introduction with Exercises* (Lecture Notes in Physics). Cham: Springer International Publishing, 2021, vol. 988, ISBN: 978-3-030-73990-4 978-3-030-73991-1.

[14] D. J. Griffiths and D. F. Schroeter, *Introduction to Quantum Mechanics*, 3rd ed. Cambridge University Press, Aug. 16, 2018, ISBN: 978-1-316-99543-3 978-1-107-18963-8.

[15] F. Grosshans and P. Grangier, "Continuous Variable Quantum Cryptography Using Coherent States," *Physical Review Letters*, vol. 88, no. 5, p. 057 902, Jan. 16, 2002.

[16] P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier, "Analysis of imperfections in practical continuous-variable quantum key distribution," *Physical Review A*, vol. 86, no. 3, p. 032 309, Sep. 10, 2012.

[17] F. Roumestan, A. Ghazisaeidi, J. Renaudier, P. Brindel, E. Diamanti, and P. Grangier, "Demonstration of Probabilistic Constellation Shaping for Continuous Variable Quantum Key Distribution," in *2021 Optical Fiber Communications Conference and Exhibition (OFC)*, Jun. 2021, pp. 1–3.

[18] K. Banaszek, L. Kunz, M. Jachura, and M. Jarzyna, "Quantum Limits in Optical Communications," *Journal of Lightwave Technology*, vol. 38, no. 10, pp. 2741–2754, May 2020, ISSN: 1558-2213.

[19] J. P. Gordon, "Quantum Effects in Communications Systems," *Proceedings of the IRE*, vol. 50, no. 9, pp. 1898–1908, Sep. 1962, ISSN: 2162-6634.

[20] E. C. G. Sudarshan, "Equivalence of Semiclassical and Quantum Mechanical Descriptions of Statistical Light Beams," *Physical Review Letters*, vol. 10, no. 7, pp. 277–279, Apr. 1, 1963, ISSN: 0031-9007.

[21] V. Giovannetti, R. García-Patrón, N. J. Cerf, and A. S. Holevo, "Ultimate classical communication rates of quantum optical channels," *Nature Photonics*, vol. 8, no. 10, pp. 796–800, Oct. 2014, ISSN: 1749-4885, 1749-4893.

[22] S. Ghorai, P. Grangier, E. Diamanti, and A. Leverrier, "Asymptotic security of continuous-variable quantum key distribution with a discrete modulation," *Physical Review X*, vol. 9, no. 2, p. 021 059, Jun. 25, 2019, ISSN: 2160-3308. arXiv: 1902.01317 [quant-ph].

[23] G. Keiser, "Optical Signal Attenuation and Dispersion," in *Fiber Optic Communications*, G. Keiser, Ed., Singapore: Springer, 2021, pp. 93–145, ISBN: 978-981-334-665-9.

[24] R.-J. Essiambre, G. Kramer, P. J. Winzer, G. J. Foschini, and B. Goebel, "Capacity Limits of Optical Fiber Networks," *Journal of Lightwave Technology*, vol. 28, no. 4, pp. 662–701, Feb. 2010, ISSN: 1558-2213.

[25] M. Martinelli and P. Martinelli, "Laguerre Mathematics in Optical Communications," *Optics and Photonics News*, vol. 19, no. 2, p. 30, Feb. 1, 2008, ISSN: 1047-6938, 1541-3721.

[26] G. P. Agrawal, *Fiber-Optic Communication Systems* (Wiley Series in Microwave and Optical Engineering), 3. ed. New York, NY: Wiley-Interscience, 2002, ISBN: 9780471221142 9786610556304.

[27] R. Paschotta, A. Schlatter, S. Zeller, H. Telle, and U. Keller, "Optical phase noise and carrier-envelope offset noise of mode-locked lasers," *Applied Physics B*, vol. 82, no. 2, pp. 265–273, Feb. 1, 2006, ISSN: 1432-0649.

[28] O. Svelto, *Principles of Lasers*. Boston, MA: Springer US, 2010, ISBN: 978-1-4419-1301-2 978-1-4419-1302-9.

[29] K. Kundert, "Introduction to RF simulation and its application," *IEEE Journal of Solid-State Circuits*, vol. 34, no. 9, pp. 1298–1319, Sep. 1999, ISSN: 1558-173X.

[30] "Recommendation ITU-T G.652, Characteristics of a single-mode optical fibre and cable," International Telecommunication Union, Aug. 2024.

[31] A. Gagliano, A. Gatto, P. Boffi, P. Martelli, and P. Parolari, "Quantum Key Distribution Spectral Allocation and Performance in Coexistence With Passive Optical Network Standards," *IEEE Transactions on Communications*, vol. 73, no. 1, pp. 510–523, Jan. 2025, ISSN: 1558-0857.

[32] Y. Piétri, L. Trigo Vidarte, M. Schiavon, *et al.*, "Experimental demonstration of continuous-variable quantum key distribution with a silicon photonics integrated receiver," *Optica Quantum*, vol. 2, no. 6, p. 428, Dec. 25, 2024, ISSN: 2837-6714.