Classical Capacity of a Bayesian Inference Quantum Channel Employing Photon Counting Detectors

F. Daneshgaran  
ECE Department,  
California State University,  
Los Angeles, California, US  
+1 323 3434480  
fdanesh@calstatela.edu

M.T. Delgado, M. Mondin, I. Bari  
Dipartimento di Elettronica  
Politecnico di Torino  
C.so Duca degli Abruzzi, 24, 10129 Torino, Italy  
+39 011 0904023  
{marina.mondin,maria.delgadoalizo,inar.bari}@polito.it

ABSTRACT
Recently we investigated the potential improvements in key transmission rate in a Quantum Key Distribution (QKD) scheme whereby photon-counting detectors are used at the receiver. To take full advantage of such detectors, soft information is generated in the form of Log-Likelihood Ratios (LLRs) using a Bayesian estimator of phase of the signal pulse which is used to carry the information. We achieved significant reduction in the residual Bit Error Rate (BER) and Frame Error Rate (FER) using LDPC codes in the information reconciliation process. In this paper we explore the limits of the achievable performance gains when using photon counting detectors as compared to the case when such detectors are not available. To this end, we find the classical capacity of the Bayesian inference channel clearly showing the potential gains that photon counting detectors can provide in the context of a realistic cost-effective scheme from an implementation point of view. While there are binary communication schemes that can achieve a higher capacity for a given mean photon count at the receiver compared to the scheme presented here (e.g., the Dolinar receiver), most such schemes are complex and at times unrealistic from an implementation point of view.

Keywords  
QKD, soft-metric, information reconciliation, LDPC codes, Bayesian estimator, quantum channel capacity

1. INTRODUCTION
Quantum Key Distribution (QKD) has recently emerged as one of the key application areas of the quantum theory, promising unconditional security founded on the laws of quantum-mechanics. The most common architectures for QKD employ the quantum states of light as the carriers of information. From an implementation point of view, the ideal scenario for QKD would be to have an on-demand, fast single photon source and perfect single photon detectors. Improvements in device fabrication technology allow one to approach these ideals, but no commercial single-photon sources are available yet. Most practical schemes today employ very weak laser sources with small mean photon count as the source and non-photon number discriminating detectors with acceptable dark count rates and detector dead-times at the receiver. A step forward in the evolution of such schemes would be to employ photon counting detectors at the receiver. This article focuses on such a paradigm.

Given that one could use photon-counting detectors at the receiver, the question arises as to how such a detector may be employed to improve the system performance. The key performance metric is obviously the achievable secret key rate, which is linked to the capacity of the corresponding quantum channel, and to the achievable residual Bit Error Rate (BER) on such a channel. From a telecom-communication point of view, the presence of a photon counting detector provides the possibility of generating at the receiver a soft-metric (as opposed to a hard metric which essentially indicates the presence or an absence of a signal) that may be exploited in the information reconciliation phase of the QKD process to improve performance. Recently, a Bayesian inference technique [1] that allows for the generation of a soft metric in the form of a Log Likelihood Ratio (LLR) suitable for soft information processing for data detection has been proposed, as shown in section 2. In what follows, the potential improvements that may be obtained in terms of classical capacity in a QKD scheme using the photon-counting detectors based scheme proposed in [1] will be investigated.

In particular, the paper is organized as follows: the considered system is described in section 2, where the corresponding channel model and LLR metric are also defined. The associated quantum channel capacity is derived in section 3, while the achievable residual BER in presence of LDPC coding within a QKD information reconciliation scheme are shown in section 4.

2. THE CONSIDERED SYSTEM
In the considered scheme [1], shown in Figure 1, the information bit “k” is encoded as k=0,1 by applying the unitary transformation $U(\phi_k)$ to the polarization degree of freedom of a coherent state $|\alpha\rangle$, which is assumed to be initially in the polarization state $|+\rangle = \frac{|H\rangle + |V\rangle}{\sqrt{2}}$. This technique is based on the use of a Phase Beam Splitter (PBS) and two photon counters. The scheme allows one to map the discrete bit value “k” to an optical polarization qubit, but at the detection stage can produce a discrete set of real numbers, either in the form of Log-Likelihood Ratios (LLR), or in the form of output phase values, which can be used for soft information processing. A possible experimental setup is shown in Figure 1, where the polarization degree of freedom $\varphi_{in}$ of a coherent state $|\alpha\rangle$ is associated to the information bit “k” according to the following encoding rule:

$$
\begin{align*}
&k \rightarrow \varphi_{in} \\
&0 \rightarrow \pi/4 \\
&1 \rightarrow 3\pi/4
\end{align*}
$$
showing a phase shift of $\pi/2$ of the qubit associated with $k=1$ relative to the qubit associated with $k=0$.

The transformation $U(\phi) = \exp\left(-\frac{\phi}{2}\sigma_3\right)$ is then applied, where $\sigma_3$ is the Pauli rotation matrix. This kind of transformation can be realized by means of a potassium dihydrogen phosphate (KDP) crystal driven by a high voltage generator and corresponds to change of the polarization from linear to elliptical.

At the detection stage a measurement of the phase shift of the qubit should be performed. This can be implemented as depicted in Figure 1 by using a Half-Wave Plate (HWP) placed in front of a Polarizing Beam Splitter (PBS) with two photon-counters providing the number of photons in the reflected and transmitted beams, denoted as $n_0$ and $n_1$ respectively. Let $n = n_0 + n_1$ denote the total number of detected photons. We assume this is also the total number of transmitted photons (in the hypothesis that no photon is lost), which is a Poisson distributed random variable with mean value $E[n] = N_c = |\alpha|^2$.

From the knowledge of the photon counts $n_0$ and $n_1$, the actual value of the phase shift can be obtained by using the Bayesian estimator [2]

$$\varphi_{est} = \int_0^\pi \varphi p_\theta(\varphi | n_0, n) d\varphi = E(\varphi | n_0, n),$$

where,

$$p_\theta(\varphi | n_0, n) = \frac{p(\varphi = 0 | \varphi)^{n_0} p(\varphi = 1 | \varphi)^{n_1}}{N} \frac{1}{N} p(0 | \varphi)^{n_0} p(1 | \varphi)^{n-n_0}$$

is the probability density function of the received phase shift given the fact that $n = n_0 + n_1$ photons have been received and $n_0$ photons have been counted at the “$k=0$” output of the PBS, and $N$ is a normalization factor such that

$$\int_0^\pi p_\theta(\varphi | n_0, n) d\varphi = 1.$$

These scenario generates the equivalent quantum channel model with binary input (the random variable $k$), and multilevel output (the couple of random variables $\{n_0, n_1\}$) shown in Figure 2, which will be discussed in what follows.

### 2.1 Evaluation of the Log-Likelihood Ratios

In soft-decoding algorithms, Log-Likelihood-Ratios are typically required, which in our case can be defined as:

$$LLR(n_0, n_1) = \log \frac{p(1 | n_0, n_1)}{p(0 | n_0, n_1)}$$

where,

$$p(k | n_0, n_1) = p(\phi_k | n_0, n_1) \quad k = 0, 1$$

is the probability that the transmitted bit was "$k" given the measurement pair $\{n_0, n_1\}$. Using Bayes' Theorem, equation (1) can be rewritten as:

$$LLR(n_0, n_1) = \log \frac{p((n_0, n_1) | 11)}{p((n_0, n_1) | 00)}$$

Since coherent states are being used, the number of photons $n_0$ and $n_1$ measured at the two detectors are uncorrelated and, in particular, are distributed according to a Poisson statistic. Given $\phi_k$, the average number $N_k^{(h)}$ of detected photons at the detector "h" is given by the expression [1]:

$$N_k^{(h)} = N_c p(h | \phi_k) \quad h, k = 0, 1$$

where $N_c = |\alpha|^2$ is the average number of photons of the input coherent state, and

$$p(0 | \phi_k) = \frac{1}{2} \left(1 + e^{-\Delta^2} \cos(\phi_k)\right)$$

$$p(1 | \phi_k) = \frac{1}{2} \left(1 - e^{-\Delta^2} \cos(\phi_k)\right)$$

where, to make the analysis more general, it is assumed that during propagation, the qubit undergoes a phase diffusion process whose amplitude is characterized by the parameter $\Delta$ (the feasibility of this scheme and its experimental demonstration have been thoroughly investigated in [3]).

We have therefore:

$$p([n_0, n_1] | k) = \mathcal{P}(n_0, N_k^{(0)}) \mathcal{P}(n_1, N_k^{(1)})$$

where,

$$\mathcal{P}(1, N) = \frac{e^{-N} N!}{l!}$$

is the Poisson probability distribution. Then, substituting equation (6) into equation (3) the following expression for the LLR can be easily obtained [4]:

$$LLR(n_0, n_1) = \left(n_1 - n_0\right) \log \frac{p_0}{p_1}$$

$$p_0 = P(0 | \varphi_0) = P(1 | \varphi_1) = \frac{1}{2} \left(1 + e^{-\Delta} \cos\left(\frac{\pi}{4}\right)\right)$$

Figure 1. A possible experimental setup to generate soft information in QKD applications.
\[ p_{ij} = P(1|\varphi_i) = P(0|\varphi_i) = \frac{1}{2} \left( 1 - e^{-\xi} \cos \left( \frac{\pi}{4} \right) \right) = 1 - p_d \]

The system described up to this point can be modeled as a Discrete Memoryless Channel (DMC), and more precisely a Binary Input Multiple Output (BIMO) channel, with binary input \( k \) and \( n + 1 = n_0 + n_1 \) + 1 outputs \((n_0, n_1)\) (where \( n \) is a random variable) as shown in Figure 2. The capacity of this channel is evaluated in the next section.

\begin{figure}[h]
\centering
\include{bimo_channel_model}
\caption{BIMO channel model of the considered system.}
\end{figure}

### 3. CAPACITY EVALUATION

The quantum channel in d-dimensions is often modeled as a completely positive trace preserving map \( \Psi \). The most common channel model is the depolarizing channel which depends on one parameter \( \lambda \) mapping a mixed state in \( \mathbb{C}^{d^2} \) into:

\[ \rho \rightarrow \lambda \rho + \frac{1-\lambda}{d} I \]

Where, \( I \) is the dxd identity matrix. For a general quantum channel, let \( \varepsilon \) denote the ensemble of input states, and M the measurement or a Positive Operator Valued Measure (POVM) \( \{E_j\} \) at the channel output. The input state ensemble, channel and measurement together define a classical noisy channel with probability transitions:

\[ p_{hm} = Tr[\Psi(\rho_n)E_m] \]

Defining the probabilities over the input state, which we will denote as \( X \), a natural definition of classical capacity of the quantum channel would be:

\[ C_{shan}(\Psi) = \sup_{\varepsilon,M} I(X;Y) \]

where \( I(X;Y) \) is the Shannon mutual information. The complication in defining capacity of the quantum channel in contrasts with the classical channel really arises in connection with purely quantum mechanical effects which have no analogue in the classical domain, i.e., entanglement. In particular, in general it is reasonable to assume (which is in fact shown to be true) that the capacity of parallel copies of a quantum channel with entangled inputs may be larger than the sum capacity of each channel treated separately. It turns out that for the most common channel model, namely the depolarizing channel, entanglement buys nothing.

We note that the closest analogue of the binary communication scheme proposed here is Binary Phase Shift Keying (BPSK) using coherent states. It is well known that for such a scheme the Dolinar receiver achieves nearly optimal results with capacity:

\[ C_{BPSK-Dolinar} = 1 - H_2 \left( 0.5(1 - \sqrt{1 - e^{-4N_{c}}}) \right) \]

where, \( H_2(\cdot) \) is the binary Entropy function. This capacity is close to the ultimate capacity obtained using an as yet unknown optimal receiver:

\[ C_{BPSK-ultimate} = 1 - H_2(0.5(1 + e^{-2N_{c}})) \]

The Dolinar receiver requires a complicated feedback system for its implementation. Hence, while its capacity for a given \( N_{c} \) is greater than what is reported here, there is significant difference in the level of the complexity of the receiver.

Our discussion thus far has been general and focused on quantum channels as trace-preserving maps. We have a much more humble pursuit in this article that is modeling an experimental setup using realistic off-the-shelf components and a particular method of communicating the quantum states, and specifically calculating the traditional Shannon capacity of the link viewed as a probabilistic transition mechanism that maps input bits into possibly multi-level signals used for detection. In this sense, we model our channel as a Binary Input Multilevel Output (BIMO) DMC, and our goal is to contrast the capacity of a system employing photon counting detectors to that of the equivalent Binary Symmetric Channel (BSC) resulting from reducing the photon counts into presence or absence of signals (i.e., hard decoding).

As noted earlier, the sufficient statistic for detection with photon counting detectors is the count difference of detector 1 and 0, i.e., \((n_1-n_0)\). Since each variable is an independent Poisson random variable, the difference \((n_1-n_0)\) is Skellam distributed:

\[ n_1 - \text{Poisson}, \mu_1 = N^{(1)}_k \]
\[ n_0 - \text{Poisson}, \mu_0 = N^{(0)}_k \]

\[ P(n_1 - n_0 = m|\varphi_k) = e^{-\left((N^{(1)}_k + N^{(0)}_k)\right)} \left(\frac{N^{(1)}_k}{N^{(0)}_k}\right)^m \left(2\sqrt{(N^{(1)}_k \cdot N^{(0)}_k)}\right) \]

where, \( k = 0 \ or \ 1 \), and \( I_{m}(\cdot) \) is the modified Bessel function of the first kind and order \( |m| \). Note that \( m \) itself is an integer that can be positive or negative. Plugging known values of the parameters, we get:

\[ N^{(0)}_k + N^{(1)}_k = N_{c} \]
\[ N^{(1)}_k \cdot N^{(0)}_k = \frac{p(1|\varphi_k)}{p(0|\varphi_k)} \]

Specializing to the case “zero is transmitted and is mapped to \( \varphi_0 \)” we get:

\[ P(n_1 - n_0 = m|\varphi_0) = e^{N_{c}} \left(\frac{\sqrt{2} - e^{-N_{c}}}{\sqrt{2} + e^{-N_{c}}}\right) I_{m(\sqrt{N_{c}})} \left(1 - \frac{e^{-2N_{c}}}{2}\right) \]

and similarly for the case “one is transmitted and is mapped to \( \varphi_1 \)”:

\[ P(n_1 - n_0 = m|\varphi_1) = e^{N_{c}} \left(\frac{\sqrt{2} + e^{-N_{c}}}{\sqrt{2} - e^{-N_{c}}}\right) I_{m(\sqrt{N_{c}})} \left(1 - \frac{e^{-2N_{c}}}{2}\right) \]
Let $X$ be the random variable associated with the transmitted phase and $Y$ be the channel output which is our sufficient statistic ($n_1 - n_0$). Then, the formulas above give us the channel transition probabilities for our DMC. Using the classic definition of mutual information:

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

and noting that the input is binary with $p(X = 0) = p(\varphi_0) = p$, after some manipulation we have:

$$p(X = 0|Y = m) = \frac{p}{p(1 - \alpha^m) + \alpha^m}$$

$$p(X = 1|Y = m) = \frac{(1 - p)\alpha^m}{p(1 - \alpha^m) + \alpha^m}$$

where,

$$\alpha = (\sqrt{2} + e^{-\Delta^2})/(\sqrt{2} - e^{-\Delta^2})$$

Finally, the conditional entropy based on two parameters, $p$ and $\Delta$ can be written as:

$$H(X|Y) = -e^{-N_c} \sum_m p \left( \frac{1}{\alpha^m} \right)^{l_{|m|}} \left( \frac{N_c}{1 - e^{-\Delta^2}/2} \right) \log(p(X = 0|Y = m))$$

$$-e^{-N_c} \sum_m (1 - p)\alpha^m l_{|m|} \left( \frac{N_c}{1 - e^{-\Delta^2}/2} \right) \log(p(X = 1|Y = m))$$

While our BIMO DMC is neither symmetric nor weakly symmetric, it is not difficult to show that the maximizing input probability distribution is uniform. Hence, $p=0.5$ maximizes the mutual information leading to channel capacity. To compare the capacity of the link employing photon counting detector to that of a simple detector signaling the presence or absence of signal, we need to specify how such a detector behaves. It is logical to assume that cross-over probability of the BSC channel associated with such a receiver can be obtained via:

$$p_{\text{BSC}} = \sum_{m=1}^{\infty} p(n_1 - n_0 = m|\varphi_0) + \frac{1}{2} p(n_1 - n_0 = 0|\varphi_0)$$

Notice that when $(n_1 - n_0) = 0$ (which for low values of $N_c$ happens often), the detector chooses at random between $k=0$ and $k=1$.

Figure 3 depicts the capacity of our BIMO DMC and its comparison to the equivalent Binary Symmetric Channel (BSC) channel in case of hard decision decoding as a function of the mean photon count in the case the phase diffusion parameter is zero.

Figure 4 depicts the capacity of our BIMO DMC and its comparison to the equivalent BSC in case of hard decision decoding as a function of the phase diffusion parameter $\Delta$ for three different values of $N_c$.

It can be observed that the considered BIMO DMC channel offers a capacity improvement over the equivalent BSC. This improvement could lead to a BER improvement when comparing the two channels in presence of an error correction code. This is investigated in the next section.

4. SIMULATION RESULTS

In this section the performance obtainable with the scheme of Figure 1 when employed within a QKD system performing information reconciliation based on forward error correction (FEC) is presented. In the hypothesis that the system is properly designed, we will neglect the presence of eavesdropping. Furthermore, we assume that...
the information bits are transmitted on a private quantum channel modelled as in Figure 2, while the additional redundancy bits are transmitted on a public channel, modelled as an Additive White Gaussian Noise (AWGN) channel, as shown in Figure 5. A block of \( n_q \) information bits plus the corresponding \( r \) redundancy bits generate one codeword of a block FEC code with rate \( R_c = n_q / (n_q + r) \).

In order to assess the potential gains that can be obtained using the soft-metric of equation (8) in the information reconciliation phase, we have conducted simulation studies using FEC coding with Low Density Parity Check (LDPC) codes simulated over the composite channel of Figure 5 with three different secure quantum channel models, all with the same equivalent uncoded Quantum Bit Error Rate (QBER) observed on the quantum channel. Figure 6, depicts three sets of simulation results. Each pair of curves is associated with a residual Bit Error Rate (BER) and Frame Error Rate (FER) curves. The LDPC code used for information reconciliation is one with \( n_q = 252, r = 156 \) and code rate \( R_c = 0.61 \). The black pair (labeled “Quantum BSC”) is for the reference system used for comparison whereby the quantum channel is modeled as an equivalent BSC with transition probability QBER (i.e., inherently there is no soft metric at the receiver and the only LLR available is from the knowledge of the QBER [4]). The blue pair represents an idealistic model whereby we have assumed that the quantum channel did not exist at all and the information transmitted over the quantum channel was presumed to pass through a fictitious AWGN channel with an SNR that would yield the observed QBER if Binary Phase Shift Keying (BPSK) were used for data transmission (curves labeled as “Quantum AWGN”).

![Quantum Channel Diagram](image)

**Figure 5.** The composite channel (composed of the parallel secure and public channels) linking transmitter and receiver in QKD applications.

The red pair (curves labeled “Quantum Bayesian est.”) is the core results and is associated with the use of a quantum channel modeled as a BIMO DMC with equivalent bit error rate QBER and LLR metrics generated via photon counting according to equation (8). The public AWGN channel of Figure 5 is modeled as practically ideal in all three cases (with signal to noise ratio of 20 dB).

As is evident from the results there is significant reduction in BER and FER for QBER values below 0.15 allowing significantly larger portion of the data to be kept during further reconciliation, data sifting and privacy amplification phases of the protocol. For instance at QBER=0.05, there is more than two orders of magnitude improvement in BER and FER when comparing the proposed soft-metric processing versus the reference protocol whereby the quantum channel is a BSC.

![Figure 6: BER and FER Simulation Results](image)

**Figure 6.** BER and FER simulation results for a LDPC code with \( n_q = 252, r = 156 \) and code rate \( R_c = 0.61 \) obtained with the composite scheme of Figure 5 and different models of the private quantum channel: BSC (black curves), AWGN (blue curves) and BIMO DMC with Bayesian estimation (red curves).

Notice that the parameter QBER in Figure 6 is actually the equivalent transition probability \( p_{BSC} \) of the (equivalent) secure quantum channel, previously defined. In the case of the BIMO DMC, values of \( N_r \) ranging from 2 to 7 have been considered to obtained the consider values of \( p_{BSC} \).

5. REFERENCES


