LDPD Coding for QKD at Higher Photon Flux Levels Based on Spatial Entanglement of Twin beams in PDC

Fred Daneshgaran\textsuperscript{a}, Marina Mondin\textsuperscript{b}, Inam Bari\textsuperscript{b}

\textsuperscript{a} Elec. & Comp. Engr. Dept., California State Univ., 5151 State University Dr., 90032 Los Angeles, USA.
\textsuperscript{b} Dip. di Elettronica e Telecom., Politecnico di Torino, C.so Duca degli Abruzzi 24, 10129 Torino, Italy.
E-mail: fdanesh@calstatela.edu, mondin.marina@polito.it

Abstract.

Twin beams generated by Parametric Down Conversion (PDC) exhibit quantum correlations that has been effectively used as a tool for many applications including calibration of single photon detectors. By now, detection of multi-mode spatial correlations is a mature field and in principle, only depends on the transmission and detection efficiency of the devices and the channel. In \cite{2, 4, 5}, the authors utilized their know-how on almost perfect selection of modes of pairwise correlated entangled beams and the optimization of the noise reduction to below the shot-noise level, for absolute calibration of Charge Coupled Device (CCD) cameras. The same basic principle is currently being considered by the same authors for possible use in Quantum Key Distribution (QKD) \cite{3, 1}. The main advantage in such an approach would be the ability to work with much higher photon fluxes than that of a single photon regime that is theoretically required for discrete variable QKD applications (in practice, very weak laser pulses with mean photon count below one are used). The natural setup of quantization of CCD detection area and subsequent measurement of the correlation statistic needed to detect the presence of the eavesdropper Eve, leads to a QKD channel model that is a Discrete Memoryless Channel (DMC) with a number of inputs and outputs that can be more than two (i.e., the channel is a multi-level DMC).

This paper investigates the use of Low Density Parity Check (LDPC) codes for information reconciliation on the effective parallel channels associated with the multi-level DMC. The performance of such codes are shown to be close to the theoretical limits.

Keywords: Quantum Key Distribution, Quantum Correlation, Polar Codes, Multi-level DMC

1. Introduction

Parametric Down Conversion (PDC) is an effective means of producing entangled photons. The state produced by spontaneous PDC exhibits perfect momentum phase matching for plane wave pump field. The state of a single bipartite transverse mode near degeneracy can be written as:

\[ |\psi(\vec{q})\rangle = \sum_n C_{i,\vec{q}}(n) |n\rangle_{i,\vec{q}} |n\rangle_{s,-\vec{q}}, \]  

where, \( i \) stands for the idler and \( s \) stands for the signal beams. The two modes in equation (1) are entangled in the number of photons in each pair of modes \( \pm \vec{q} \). Imaging the beams in the far field of a thin lens of focal length \( f \) in a \( f-f \) arrangement as depicted in Figure 1, leads to an association of each

\footnote{This work has been supported by NATO SfP Project 984397 entitled “SfP - Secure Quantum Communications”}
Figure 1. General block diagram of the experimental setup from [4].

mode to a unique position in the focal plane via the mapping:

$$\frac{2c f}{\omega_p} \vec{q} \rightarrow \vec{x}$$

Hence, a perfect correlation should be detected in the photon numbers $N_{i,\vec{x}}$ and $N_{s,-\vec{x}}$ where the center of symmetry relative to which the symmetric positions are identified is the pump detection plane interception point. In reality, the pump field is not a perfect plane wave, rather a Gaussian beam with spatial waist $w_p$ inducing an uncertainty in the relative propagation direction of the twin photons on the order of the angular beam-width of the pump. This uncertainty is the coherence area of the process roughly corresponding to the transverse size of the mode in the far field and is given by:

$$A_{coh} \sim \left[ \frac{2\pi cf}{\omega_p w_p} \right]^2$$

The number of spatial modes observed over a detection area that is usually taken to be much larger than the coherence area is given by $M_{spatial} = A_{det,j}/A_{coh}$, where $j = i$ or $s$. Similarly, it is assumed that the detection time is much larger than the coherence time hence the number of temporal modes $M_t = T_{det}/T_{coh}$ is much larger than one. The total number of modes in the detection region is $M_{tot} = M_{spatial}M_t$. The different modes in a single region are independent and thus the statistics of the detected photons is multi-thermal with mean value $\langle N_j \rangle = M_{tot}\eta_j \mu$, where, $j = i$ or $s$, $\mu$ is the number of photons per mode, and $\eta_j$ is the overall efficiency. The variance of the number of detected photons is given by:

$$\langle \delta^2 N_j \rangle = \langle N_j \rangle \left( 1 + \frac{\langle N_j \rangle}{M_{tot}} \right) = \langle N_j \rangle (1 + E) = M_{tot}\eta_j \mu(1 + \eta_j \mu)$$

where $E$ is the excess noise defined as fluctuations that exceed the Shot Noise Limit (SNL). The covariance between the signal and idler photon numbers is given by:

$$\langle \delta N_i \delta N_s \rangle = M_{tot}\eta_i \eta_s \mu(1 + \mu).$$

The correlation statistic between signal and idler is measured in terms of the fluctuations of the difference $N_- = N_s - N_i$ normalized to the corresponding level of shot noise:

$$\sigma = \frac{\langle \delta^2 N_- \rangle}{\langle N_i + N_s \rangle} = 1 - \eta_+ + \frac{\eta_+^2}{4\eta_+} \left( \eta_+ + \frac{\langle N_s + N_i \rangle}{M_{tot}} \right),$$

where $\eta_+$ and $\eta_-$ are the overall efficiencies of the signal and idler respectively.
where, $\eta_+ = (\eta_s + \eta_i)/2$ and $\eta_- = \eta_s - \eta_i$. If the losses are perfectly balanced, $\eta_s = \eta_i = \eta$ and we get $\sigma = 1 - \eta$ depending only on the quantum efficiency. In the ideal case of perfect efficiency, indeed, $\sigma \to 0$ while for classical states of light the degree of correlation is bounded by $\sigma \geq 1$ with the lower limit achieved by coherent beams leading to $\sigma = 1$.

The basic requirement on the size of the detection area is that the number of speckles in the region far exceeds the number on the perimeter. A pictorial representation of this is depicted in Figure 2. The core idea of using the spatial entanglement of twin beams for Quantum key Distribution (QKD) stems from the fact that the correlation statistic generated on two symmetric regions in the CCD focal plane must exhibit a $\sigma < 1$. Eavesdropping by Eve will lead to increase in $\sigma$ above one and is therefore detectable. Indeed, the extent of interference by Eve may be measured by how much $\sigma$ has increased beyond its expected value. Depending on the extent of this interference, the parties can decide to either continue generating a random key or halt the process all together. Note that under ideal circumstances $\sigma \to 0$ while practically, it is always above zero but hopefully sufficiently below one to allow for secure communication to take place. This is pictorially depicted in Figure 3. In reality, one cannot assert that eavesdropping will always lead to $\sigma > 1$. Even in the simplest situation, Eve can always reduce the level of eavesdropping for having $\sigma < 1$, but then again the information she acquires will be very small as well.

Eventually, disposing of ideal technologies, Eve can measure a certain number $N$ of photons and reproduce it by a squeezed source in the photon number even post selected (e.g., a PDC sources), sending to Bob the signal only when she observes $N$ Photons in the heralding channel. However, if one could detect quantum correlations in the near field and in the far field, this would correspond to having two conjugated bases. In this case, only entanglement should provide strict correlation at the same time in the two measurements, a situation that cannot be reproduced by Eve.

The process of generating a random key based on this core concept is as follows:

- Alice generates the twin beams via PDC and images one of the two beams on its CCD array and launches the second beam towards Bob;
- both Alice and Bob are assumed to have achieved timing synchronization so they know the start and end time of each firing of the laser pulses;

Figure 2. A detection region identified as a square on the upper right corner whereby the condition that the number of speckles in the region is much larger than that on the perimeter is satisfied.
Correlation Statistic
Normal light
Entangled light
Increase if intercepted by Eve

Figure 3. Pictorial representation of the impact of eavesdropping by Eve on the measured correlation statistic.

- the CCD detection area is partitioned into a number of smaller detection areas we call super-pixels, say four equal sized regions, satisfying our basic requirement that the detection area be much larger than the coherence area of the spatial modes;
- Alice and Bob make measurements on one reference quadrant (Alice and Bob’s reference quadrants are at symmetric positions). Alice sends Bob her measurement results that Bob uses to estimate $\sigma$ based on his a-priori knowledge of system level parameters and experimental setup uncertainties. Bob repeats the same process on a different set of measurement so that Alice can obtain a similar statistic. If the measured $\sigma$ is acceptable by both parties, they continue with the protocol;
- assuming the measurements made on the reference quadrant in the previous step indicated that impact of eavesdropping by Eve is tolerable, Alice and Bob make measurements of the number of the detected photons in the other quadrants. A pair of quadrants, one at Alice and one at Bob, that are in symmetric regions of their CCDs focal plane represent a quantum channel between the two parties. In our example, three of the four quadrants would be used and constitute three parallel quantum channels that can be used to generate random keys;
- for each of the quantum channels described in the previous step, Alice and Bob make a measurement of the number of their detected photons and use binning and associate a unique label to their measurement. Ideally, for each quantum channel, Alice and Bob obtain an identical sequence of labels in their measurement that constitute a secret key. In practice, fluctuations in the number of measured photons lead to discrepancies and the label sequence at Alice and Bob don’t match perfectly, hence requiring Information Reconciliation (IR) and privacy amplification to lead to distilled keys that can be used for cryptography.

2. Development of the Channel Model
The aim of this section is to outline in detail the process for generating the binary or multilevel DMC channel model for each of the parallel quantum channels described in the previous section. To this end, we need a detailed knowledge of the photon statistics in each detection area. As stated previously, the number of modes in a given detection area is very large. The number of temporal modes is dependent on the duration of the laser pulse width and the coherence time and is reported to be 5000 in [4]. The number of spatial modes is dependent on the size of the detection area that carries a trade-off in terms of the degree of the determination of the Center of Symmetry (CS), requiring a small detection area, and visibility of the quantum correlation, requiring a large detection area. The determination of the center of symmetry can be done with high resolution using small pixels and then performing the experiment with larger pixels.
In the experimental setup presented in [4], the number of spatial modes is about 150. Given the large number of detected modes, the statistic of the number of detected photons in a given region is multi-thermal.

For a single mode, the thermal distribution is geometric with Probability Mass Function (PMF) $P_1(n) = (1 - \xi)\xi^n$, where, the parameter $\xi$ is related to the mean of the geometric PMF $\lambda$ via $\xi = \frac{\lambda}{1+\lambda}$. The photons in different modes are independent and therefore the PMF of the total number of detected photons in $N$ modes is the $N$-fold convolution of the geometric PMF and given by:

$$P_N(k) = \frac{(k + N - 1)!}{k!(N - 1)!} (1 - \xi)^N \xi^k.$$  

The mean and variance of the photon number in this case is given by $E[X] = N\lambda$ and $\sigma_X^2 = N\lambda(1 + \lambda)$.

In each detection region, at either Alice or Bob, the number of photons are counted and using a binning approach (i.e., multi-level quantization), the bin to which the number of detected photons belong is identified and the associated symbol is assigned as a component of a potential secret key. The Alice and Bob’s measurements on the symmetric detection regions illuminated by the entangled twin beams may either result in identical bins, leading to identical symbols, or different bins leading to two different symbols. The derivation of the channel model requires computation of the probability that a certain number of photons is detected at Alice, and another number is detected at Bob. Once this joint probability is known, the computation of the transition probabilities associated with the resulting DMC modeling the behavior of a fictitious channel we may imagine exists between Alice and Bob and causes discrepancies between their detected symbols becomes straightforward.

The problem of determination of the number of detected photons at Alice and Bob is essentially a bipartite detection problem. Let $P(n)$ denote the probability of generation of $n$ photon-pairs at the source and let $\text{Bin}(k|n, \xi)$ denote the binomial PMF:

$$\text{Bin}(k|n, \xi) = \frac{n!}{k!(n - k)!}\xi^k(1 - \xi)^{n-k},$$

then the probability of detecting $k$ photons at Alice and $m$ photons at Bob is given by:

$$P(K, m) = \sum_{n=\max(k,m)}^{\infty} P(n)\text{Bin}(k|n, \xi_A)\text{Bin}(m|n, \xi_B),$$  \hspace{1cm} (5)

where, $\xi_A$ and $\xi_B$ are related to the mean of the geometric PMF for a single mode. Substituting $P_N(n)$ for $P(n)$ in above expression we get the desired PMF of detecting $k$ photons at Alice and simultaneously $m$ photons at Bob over our detection area.

3. LDPC Coding for Information Reconciliation

Alice and Bob need to be in possession of identical sequences of symbols before they can proceed with privacy amplification and generate secure keys for encryption. Information Reconciliation (IR) is the process of eliminating discrepancies that may exist in the sequences at Alice and Bob as much as possible. This is achieved using essentially error correction coding. The process is not perfect in that there is always some residual symbol errors left leading to very low symbol and frame error rates. By selecting a very low frame error rate threshold, one can almost guarantee that the symbol sequences at Alice and Bob are identical with very high probability.

Multitude of error correction techniques are available for information reconciliation. Broadly speaking, we can classify the available techniques into

- Forward Error Correction (FEC) techniques, and
- interactive two-way coding schemes with feedback such as the CASCADE algorithm.
Fundamentally from an information theoretic point of view, there is no advantage to two-way interactive techniques (this is reinforced in light of the given symmetry of the problem formulation presented in the introduction section). Either Alice or Bob could initiate an information reconciliation protocol since their roles are perfectly interchangeable. There is a vast body of literature on FEC techniques from the digital communications field and we shall resort to the available techniques for IR.

Forward error correction is a very mature field with performance of modern coding techniques approaching the capacity of the underlying channels at extremely long block lengths. Hence, one has a vast menu of FEC techniques to employ for the problem at hand. There are however some simple criteria one could apply in making the selection of a suitable technique:

- the code must be systematic since the data block is what Alice and Bob have direct access to, albeit, with possible discrepancies. As noted in introduction, there is no channel per se between Alice and Bob. We may view the discrepancy between their symbol sequences as having been caused by a fictitious $Q$-ary DMC;
- any systematic FEC generates coded symbols that need to be communicated across a classic public channel. We assume the encoding operation is performed at Alice while decoding is performed at Bob;
- most modern decoding techniques rely on the use of soft-information processing and this is what we shall assume as well. We have however, two separate channels that lead to two different soft metrics that would need to be combined in decoding. The fictitious channel between Alice and Bob is modeled as a $Q$-ary DMC, the real channel over which the coded symbols propagate is a public channel we assume to be ideal.

As an initial simplified model we will consider a $Q$-ary DMC channel model (with $Q = 4$) as shown in Figure 4, with input alphabet $X = \{x_k\}_{k=1}^{Q} = \{00, 01, 10, 11\}$ and output alphabet $Y = \{y_k\}_{k=1}^{Q} = \{00, 01, 10, 11\}$. We associate a binary labeling to the $Q$ transmitted symbols, and denote as $p_i$ the probability of having $i$ bit errors in one transmitted $Q$-ary symbol ($i=1,2$), with the added hypothesis (justified by preliminary tests) that the probability of having one bit error per symbol is independent on the position of the error within the symbol. With reference to Figure 4 notice that, in the hypothesis of independent equally likely transmitted bits, the equivalent bit error probability (i.e. the equivalent Quantum Bit Error Rate - $QBER$) is

$$QBER = P(\text{bit error}) = p_1 + p_2.$$ (6)
The $Q$-ary channel model in Figure 4 is used to transmit the $k$ bits that compose the cryptographic key. After the transmission of the key, and once the presence of Eve has been excluded as described in Section 1, additional $r$ redundancy bits are transmitted on a parallel ideal Binary Symmetric Channel (BSC), so that the $k$ information bits together with the $r$ redundancy bits represent a $n = k + r$ bits codeword of a rate $R_c = k/n$ LDPC code. Note that the above channel model is obtained from proper binning of the photon numbers at the transmitter and receiver (i.e., the intervals used to define the channel symbols at input and output can be adjusted to get the transition probabilities that adhere to the model above). At the receiver a soft metric LDPC decoder is employed, operating according to a belief propagation strategy, with input soft metrics from the $Q$-ary channel evaluated as

$$LLR(y_i^k) = \log \left( \frac{\sum_{x \in x(0)^i} P(y_k|x)}{\sum_{x \in x(1)^i} P(y_k|x)} \right),$$

where $LLR(y_i^k)$ is the Log Likelihood Ratio (LLR) of the $i$-th bit of the received symbol $y_k$ and $x(w)^i$ are the symbols of $X$ whose $i$-th bit has weight $w$. Applying equation (7) to our channel model we obtain

$$LLR(y_i^k) = \begin{cases} 
+\log \left( \frac{1-p_1-p_2}{p_1+p_2} \right) & \text{if } y_i^k = 0 \\
-\log \left( \frac{1-p_1-p_2}{p_1+p_2} \right) & \text{if } y_i^k = 1
\end{cases} \quad (8)$$

A rate 0.8 (1000,800) LDPC code has been applied to perform IR on the scheme described so far, selecting, for the same overall $QBER$, different values of $p_1$ and $p_2$. The decoded Bit Error Rate (BER) performances shown in Figure 5 have been obtained by Montecarlo simulation, showing that the decoded BER depends on the overall $QBER$ value and not on how the error probability is distributed on the first and second bit of the $Q$-ary transmitted symbols. This proves, in practice, that with the considered binary FEC LDPC codes the use of a $Q$-ary channel is equivalent to $\log_2(Q)$ successive uses of a BSC with the same value of $QBER$.

Figure 5. BER performances of a (1000,800) binary LDPC over the $Q$-ary channel in Figure 3 for (2) $p_1 = QBER^2$, (3) $p_1 = QBER^2/2$ and (4) $p_1 = QBER/2$ as a function of $QBER$, compared with (1) a BSC with transition probability $QBER$. In (2), (3) and (4) $p_2 = QBER - p_1$. 

7
LDPC codes with different rates have then been simulated, obtaining the efficiency of the considered information reconciliation scheme. The efficiency, defined as [6]

$$
\epsilon_{IR} = \frac{1 - R_c}{H(X|Y)} = \frac{1 - R_c}{R_c H_2(QBER)}
$$

(9)
is shown in Figure 6, where the considered codeword lengths \( n \) are always smaller or equal to 1000. It can be noticed that the proposed scheme allows to achieve efficiency values better (i.e. closer to 1) than the CASCADE algorithm, with reasonable complexities, proving the effectiveness of the approach.

![Figure 6. Reconciliation efficiency with LDPC codes for different coding rates as a function of the channel quantum bit error rate QBER. The red continuous line is a graphical lower bound of the efficiency of the CASCADE IR algorithm [6].](image)

4. Conclusions
This paper offers a preliminary investigation on the use of FEC LDPC codes for information reconciliation when the underlying channel is a \( Q \)-ary DMC, for QKD applications based on higher photon flux levels with spatial entanglement of twin beams in PDC. The simulation results show that acceptable error reconciliation efficiency values can be obtained with reasonable decoding complexity.

5. Bibliography
[1] I. P. Degiovanni M. Genovese M. Gramegna A. Avella, G. Brida and P. Traina. *Phys. Rev. A*, 82:062309, 2010.
[2] M. Genovese Brida and I. Ruo Berchera. *Nature Photonics*, 4:227, 2010.
[3] I. P. Degiovanni M. Genovese P. Traina G. Brida, A. Cavanna. *Laser Physics Letters*, 9:247, 2012.
[4] M. Genovese M. L. Rastello I. Ruo-Berchera G. Brida, Ivo P. Degiovanni. *Opt. Exp.*, 18:20572, 2010.
[5] A. Gatti M.Genovese A.Meda I.Ruo-Berchera G.Brida, L. Caspani. *Phys. Rev. Lett.*, 102:213602, 2009.
[6] V. Martin J. Martinez-Mateo, D. Elkouss. *Quantum Information and Computation*, 12:07910812, 2012.