Quantum Optics Lab report

Alessandro Lovo

July 18, 2020

Abstract

In this report, using the same experimental apparatus, three experiments regarding the quantum entanglement of photons will be performed: Entangled Quantum Key Distribution, Bell Inequality Violation and Quantum Tomography.

1 Experimental apparatus

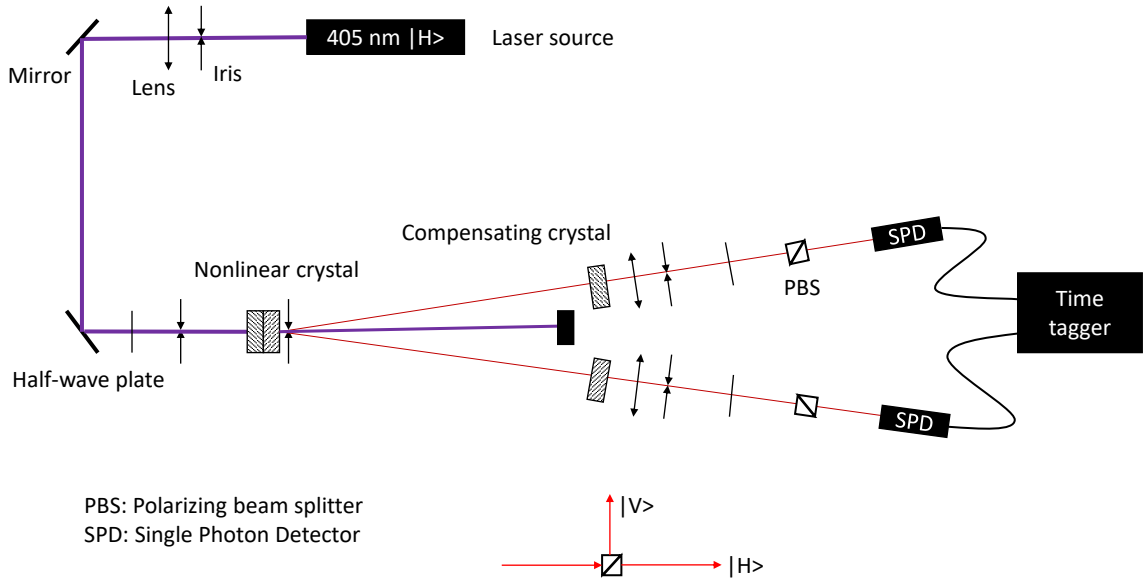

Figure 1: Schematics of the experimental apparatus.

The schematics of the experimental apparatus are reported in fig 1: the source is a 405 nm laser whose beam is focused onto a nonlinear type II crystal obtained by sticking together two type I crystals with perpendicular optical axes. The laser emits light horizontally polarized ($|H\rangle$) and the two nonlinear crystals have a small chance ($\sim 10^{-7}$) of converting a photon into a pair of photons: if $|V\rangle$ is the vertical polarization, the conversion reads as:

$$|H\rangle \xrightarrow{\text{crystal 1}} |VV\rangle \quad |V\rangle \xrightarrow{\text{crystal 2}} |HH\rangle$$

Using the first half-wave plate the polarization of the beam is rotated to the diagonal state $|D\rangle = \frac{|H\rangle+|V\rangle}{\sqrt{2}}$, so when it impinges on the two crystals the exiting pair is in the entangled state $|\phi^+\rangle = \frac{|HH\rangle+|VV\rangle}{\sqrt{2}}$. However since the conversion is due to two type I crystals in order to not be able to distinguish which one did the conversion, two compensating crystals are introduced on the optical

path. After some focusing the two beams hit the measuring device: a half-wave plate, a polarizing beam splitter (PBS) and a single photon detector (SPD). By tuning the angle α of the half-wave plate it is possible to measure any linear polarization $|\theta\rangle = \cos\theta\,|H\rangle + \sin\theta\,|V\rangle$ with the simple relation $\theta = 2\alpha$. The signals of the SPDs are sent to a time tagger in order to be able to do an a-posteriori coincidence analysis.

Coincidence analysis The raw data of an acquisition consist of a list of timetags corresponding to the clicks of each of the two detectors expressed in timesteps of the time tagger $\tau = 80.955\,\text{ps}$. To extract the coincidences from it, first a histogram of the time differences between the two detectors is plotted and fitted with a gaussian with centroid μ and dispersion σ (fig 2). At this point one can set a threshold $thr_c = 2\sigma$ for accepting coincidences, namely the number of coincidences N is simply the number of points in the histogram for which $|\Delta t/\tau - \mu| < thr_c$. To this value can be then assosciated a poissonian error $\sigma(N) = \sqrt{N}$.

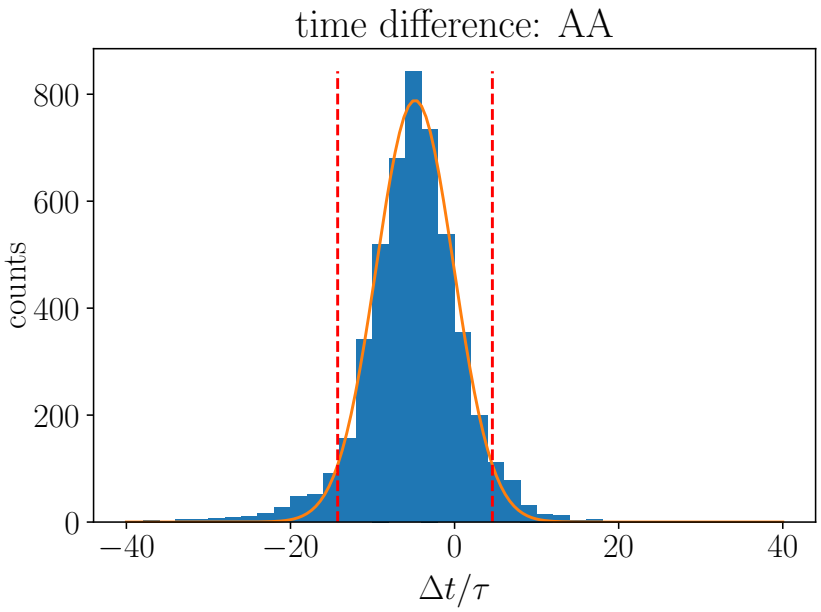

Figure 2: Example of histogram of the time differences between the two detectors; here both photons are measured in the state $|A\rangle = \left|-\pi/4\right\rangle$. The red lines are drawn at thr_c.

2 Entangled Quantum Key Distribution

Following the protocol BBM92 Alice and Bob share a source of entangled photons (in our experiment Alice and Bob can be considered as the two measuring devices measuring the photon pairs) and will end up with a random secret shared key. The protocol can be summarized as follows:

1. *Quantum Communication* For each photon they receive, Alice and Bob randomly and independently choose in which base to measure the polarization:

$$\mathcal{B}_1 = \{|H\rangle, |V\rangle\} \quad \text{or} \quad \mathcal{B}_2 = \left\{|D\rangle = \left|\pi/4\right\rangle, |A\rangle = \left|-\pi/4\right\rangle\right\}.$$

   Since the state of the pair is $\left|\phi^+\right\rangle = \frac{|HH\rangle+|VV\rangle}{\sqrt{2}} = \frac{|DD\rangle+|AA\rangle}{\sqrt{2}}$ for each measurement they have a 50% chance of obtaining either result: result that can be coded, for example, as 0 if it is first element of the base and 1 if it is the second.

2. *Sifting* After all the measurements they communicate via a classical channel the sequence of bases used for the measurement, restricting to the data in which they both measured in the same base. So on average the lenght of the key halves.

3. *Parameter Estimation* Alice and Bob communicate to each other the results of the measurements of a portion (for example $r_s = 10\%$) of the sifted key to estimate the Quantum Bit Error Rate (QBER), namely the percentage of measurements in which they obtained a different result. The Qber can then be used to quantify the information that an eventual Evesdroppper has on the key.

4. *Error Correction* Classical protocol at the end of which Alice and Bob have the same key, but the Evesdroppper has still information on it.

5. *Privacy Amplification* Other classical protocol that allows Alice and Bob to extract from their shared key a shorter one on which the Evesdroppper has no information at all. With this step the lenght of the key gets multiplied by the secret key rate

$$r = 1 - h_2(QBER[\mathcal{B}_1]) - h_2(QBER[\mathcal{B}_2])$$

where

$$h_2(x) = -x \log_2 x - (1-x) \log_2 (1-x)$$

is the Shannon entropy. Clearly as the QBER increases, r decreases and when $r < 0$ it is impossible to extract a secure key. The relationship between r and the QBER is plotted in fig 3. If one considers also the losses in key lenght due to sifting and parameter estimation the ratio between number of bits in the final key and number of pair of photons measured is $\frac{1}{2}(1 - r_s)r$.

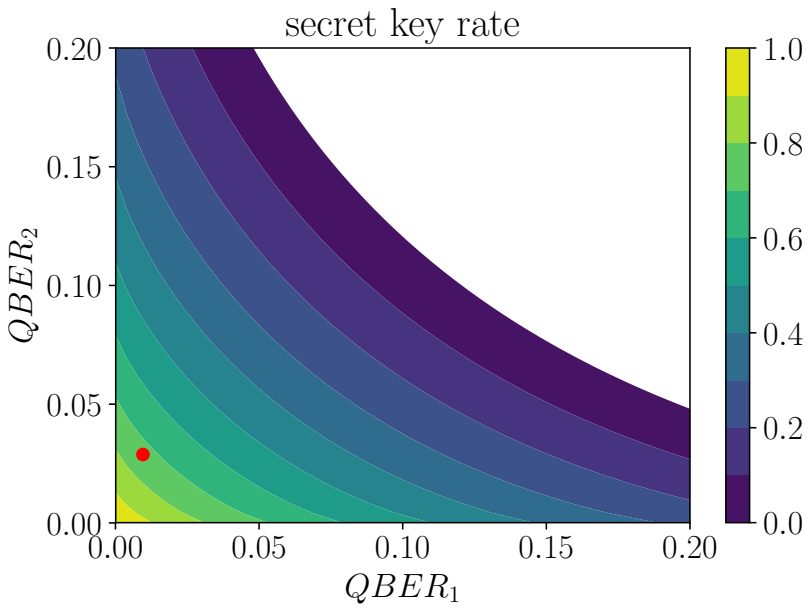

Figure 3: Secret key rate as a function of the QBER in the tw bases. The red dot represents the experimental point found later.

2.1 Experimental data

In the experiment we performed the focus is on the computation of the QBER and subsequently the estimation of the secret key rate. To do so we rotated the two half-wave plates in order to measure the pair of photons in the states reported in tab 1 acquiring for each configuration a dataset of around 15 s. In order to have a correct normalization, all datasets have been cropped in order to have the same temporal lenght of the shortest one: 14.016 s.

Configuration	Coincidences
AA	4440 ± 70
AD	140 ± 10
DA	120 ± 10
DD	4270 ± 70
HH	4390 ± 70
HV	21 ± 4
VH	64 ± 8
VV	4410 ± 70

Table 1: Number of coincidences

From these data it is then possible to compute the two QBERs and hence the secret key rate. If N_{HH} is the number of coincidences measured in configuration HH one gets the following:

$$QBER[\mathcal{B}_1] = \frac{N_{HV} + N_{VH}}{N_{HH} + N_{HV} + N_{VH} + N_{VV}} = 0.010 \pm 0.001$$
$$QBER[\mathcal{B}_2] = \frac{N_{DA} + N_{AD}}{N_{DD} + N_{DA} + N_{AD} + N_{AA}} = 0.029 \pm 0.002$$
$$r = 1 - h_2(QBER[\mathcal{B}_1]) - h_2(QBER[\mathcal{B}_2]) = 0.73 \pm 0.01$$