# Quantum optics lab report — part 2

Jacopo Tissino

2020-10-25

**Abstract**

We use an optical bench set up for the generation and measurement of polarization-entangled photon pairs in order to first violate the Bell inequalities with $|S| \approx 2.60 \pm 0.02$, and then to build a prototype for an entanglement-based Quantum Key Distribution protocol [BBM92], achieving a shared key rate of the order of 100 bits/s.

## 1 Experimental setup

We give a short description of the experimental apparatus, neglecting all mirrors, lenses, irises and in general devices needed in order to direct, select and concentrate the light beam.

A blue "pump" laser emits light with wavelength $\lambda = 405\,\text{nm}$ continuously. The light from this laser is initially horizontally polarized; it passes through a half-wave plate which achieves a linear polarization at 45° from the horizontal: a state proportional to $|H\rangle + |V\rangle$, where $H$ and $V$ denote the horizontal and vertical linear polarizations respectively.

The light then impinges upon a pair of parametric fluorescence crystals with optical axes orthogonal to each other and to the propagation direction; a fraction $10^{-8} \div 10^{-7}$ of the times an incoming photon from the pump is turned into a pair of photons with $\lambda = 810\,\text{nm}$ and with propagation directions of around 4° from the original beam.

The polarizations of these two photons are entangled: their state is

$$\frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle)\,, \tag{1}$$

where $|H\rangle$ or $|V\rangle$ denotes the horizontal or vertical polarization of a photon.

These two photons then each pass through a half-wave plate and a Polarizing Beam Splitter: this pair of components selects a (linear) polarization to project the state along, since the half-wave plate rotates the polarization by a certain angle, while the PBS transmits only photons with a certain polarization (say, $H$). The reflected photons are discarded in this setup.

In order to measure along the polarization $\cos\theta\,|H\rangle + \sin\theta\,|V\rangle$ we must rotate the polarization of the photons by an angle $\theta$, which is achieved by rotating the half-wave plate by an angle $\theta/2$.

The half-wave plate at an angle $\varphi$ can be modelled as the quantum gate

$$\begin{bmatrix} \cos(2\varphi) & \sin(2\varphi) \\ -\sin(2\varphi) & \cos(2\varphi) \end{bmatrix} \tag{2}$$

in the single-photon polarization space with basis $\{|H\rangle, |V\rangle\}$.

After the PBS, the photons reach a single-photon detector, which measures their arrival time with a jitter of approximately 1 ns, a quantum efficiency (probability that a specific photon is detected) of approximately 50 %, and a dark count of approximately 100 Hz.

## 2 Bell test

A Bell test allows us to experimentally violate a classical inequality, showing that a theory with classical probability (and possibly hidden variables) cannot describe a quantum system — or, at least, entanglement in the polarizations of photons.

The two photons can be measured in two different bases (denoted as $x = 0$ and $x = 1$ for the first photon, $y = 0$ and $y = 1$ for the second) and can yield two different outcomes, which we associate to the values $+1$ and $-1$ when computing expectation values.[1] We can then define

$$S = \langle 00 \rangle + \langle 01 \rangle + \langle 10 \rangle - \langle 11 \rangle \ , \tag{3}$$

where by $\langle ij \rangle$ we mean the expectation value of the tensor product of the two bases: $\langle x = i \otimes y = j \rangle$.

Classically, it can be shown [Cla+69] that $|S| \leq 2$, while a quantum system can theoretically achieve $|S| = 2\sqrt{2} \approx 2.82$.

The two bases[2] are chosen for the first photon to be the ones corresponding to the maximum quantum violation of the inequalities: the first is $\{|H\rangle, |V\rangle\}$, while the second is $\{|D\rangle, |A\rangle\}$, where the states $|A\rangle$ and $|D\rangle$ are defined as $(|H\rangle \pm |V\rangle)/\sqrt{2}$. For the second photon the bases are the same but rotated around the propagation direction by an angle $\pi/8$.

Measurements are performed by selecting one of these four vectors for each of the photons (so, performing $4^2$ measurements for all the combinations) through a half-wave plate and counting the number of photons being detected after it per unit time.

The detection numbers are turned into expectation values by estimating probabilities through their corresponding relative frequencies, and then computing $\langle x \rangle = \sum_i x_i \mathbb{P}(x_i)$.

Experimentally, with this method we achieved $|S| = 2.597 \pm 0.015$.

An explanation of how the data was analyzed, going from the list of the arrival times to the Bell inequality violation, can be found in a Jupyter notebook at https://github.com/jacopok/quantum_optics/blob/master/bell_test/report_bell_test.ipynb.

The code for the analysis can be found in the folder https://github.com/jacopok/quantum_optics/tree/master/bell_test.

[1] We denote these, instead, as 0 and 1 when writing results in matrix notation, for consistency with the indexing of vectors.

[2] They are not bases for the full two-photon Hilbert space, their span only consists of the linear polarizations, which is enough for our purposes.

## 3 Quantum Key Distribution

With the same experimental setup as the Bell test, we were able to implement a Quantum Key Distribution entanglement-based scheme, first described by Bennett, Brassard, and Mermin [BBM92].

The two conventional communicators Alice and Bob can achieve a shared secret key by receiving entangled qubits. Two bases are agreed upon, we use the same ones which were used in the Bell inequalities case ($H - V$ and $D - A$). They measure each qubit in a randomly-chosen basis, half of the time on average they will happen to choose the same one. They can later disclose which bases were used; the results of the measurements in a shared basis then will be a shared key.

This shared key can then be used in order to encrypt a message bit-by-bit using a logical XOR gate: as long as the key is secret and longer than the message this is fully secure.

In order to be sure that the qubits have not been tampered with a certain fraction of them should be periodically analyzed publicly: if they manage to retain entanglement (which can be verified, for example, by checking for the violation of Bell inequalities) then they are safe.

We measured the rate of key transfer which can be achieved by our experimental setup. The state we use is the same as in (1), and it can also be written as

$$\frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle) = \frac{1}{\sqrt{2}}(|AA\rangle + |DD\rangle)\,. \tag{4}$$

The key rate is constrained by errors, which can be quantified through the Quantum Bit Error Rate: the probability of detecting $HV$, $AD$ and such should be zero ideally, but because of various sources of noise this is not so. Then, for the $H - V$ basis we define

$$\mathrm{QBER}(HV) = \mathbb{P}(HV) + \mathbb{P}(VH)\,, \tag{5}$$

and similarly for $A - D$. This is computed, as usual, as favorable events versus total events, where the "total events" only refer to that specific basis: for example,

$$\mathbb{P}(HV) = \frac{N_{HV}}{N_{HH} + N_{VV} + N_{HV} + N_{VH}}\,. \tag{6}$$

The fraction of usable qubits is then calculated as

$$r = 1 - h(\mathrm{QBER}(HV)) - h(\mathrm{QBER}(AD))\,, \tag{7}$$

where the function $h$ comes from considerations about the mutual information of Alice and Bob; it is given by

$$h(p) = -\big(p \log_2 p + (1-p)\log_2(1-p)\big)\,. \tag{8}$$

With our experiment we find $r \approx 0.72 \pm 0.01$.

The rate in bits per second is further halved because of the random choice of basis of Alice and Bob. With this consideration, we find a key rate of approximately 125 Hz (or bits per second); this will be further reduced because of the requirement to reserve a fraction of the qubits for entanglement verification.

A Jupyter notebook summarizing the results and analysis can be found at https://github.com/jacopok/quantum_optics/blob/master/QKD/report_QKD.ipynb.

The full code for the analysis is in the folder https://github.com/jacopok/quantum_optics/tree/master/QKD.

Considering the relative simplicity of the experimental setup — it is a table-top experiment, after all — this key rate is not bad, it would be enough for somewhat slow fully secure text-based communication, at about 10 letters a second.

## References


[BBM92] Charles H. Bennett, Gilles Brassard, and N. David Mermin. "Quantum Cryptography without Bell's Theorem". In: *Physical Review Letters* 68.5 (Feb. 3, 1992), pp. 557–559. DOI: 10.1103/PhysRevLett.68.557. URL: https://link.aps.org/doi/10.1103/PhysRevLett.68.557 (visited on 10/21/2020) (cit. on pp. 1, 3).

[Cla+69] John F. Clauser et al. "Proposed Experiment to Test Local Hidden-Variable Theories". In: *Physical Review Letters* 23.15 (Oct. 13, 1969), pp. 880–884. DOI: 10.1103/PhysRevLett.23.880. URL: https://link.aps.org/doi/10.1103/PhysRevLett.23.880 (visited on 10/25/2020) (cit. on p. 2).