Experimental data used for key extraction

In this section we report the experimental data used to extract the secure key in the QKD protocol. Decoy state method has been developed \[1, 2\] to avoid photon number splitting attacks on qubits generated by attenuated laser pulses. The transmitter randomly changes the mean photon number of the sent pulses between three values: \(\mu\), the signal state, and two other decoy values, \(\nu\) and zero (corresponding to sending empty pulses). The bits obtained with \(\mu\) are used to build the final key, while other pulses are used to bound Eve’s knowledge on the key.

In the infinite key-length limit, the secret key rate, defined as the number of secure over sifted bits, is given by \[1, 2\]

\[
r = \frac{Q^2_{\mu}}{Q^2_{\mu}} [1 - h_2(e^U_1)] - \text{leak}_{EC} + \frac{Q_0}{Q_{\mu}} \]

(1)

where \(Q_{\mu}\) is the total gain (the fraction of detected bits over the sent bits), \(Q^2_{\mu}\) the lower bound of the gain of the one-photon states, \(Q_0\) the gain of the vacuum states, \(E_{\mu}\) the total quantum bit error rate (QBER), \(e^U_1\) the upper bound of errors of the one-photon states, \(h_2\) the binary entropy \(h_2(x) = -x \log_2 x - (1 - x) \log_2 (1 - x)\). The term \(\text{leak}_{EC}\) represent the fraction of revealed bits during the classical error correction protocol, whose efficiency, given by \(f(E_{\mu}) = \frac{\text{leak}_{EC}}{h_2(E_{\mu})}\), is below 1.05.

By the decoy state method it is possible to estimate the parameters \(Q^2_{\mu}\), \(Q_0\) and \(e^U_1\) by the decoy data as

\[
Q^2_{\mu} = \frac{\mu^2 e^{-\mu}}{\mu - \nu^2} \left( Q_\nu e^{\nu} - Q_{\nu} e^{\nu} \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0 \right)
\]

(2)

and

\[
e^U_1 = \frac{E_\nu Q_\nu e^{\nu} - c_0 Y_0}{Q^2_{\mu} e^{\mu}}, \quad Q_0 = e^{-\mu} Y_0.
\]

(3)

In the previous expression \(Q_{\nu}\) and \(E_{\nu}\) are the total gain and the QBER of decoy states \(\nu\) respectively, while \(Y_0\) is the dark rate at the receiver. The parameters \(\mu\) and \(\nu\) represent the measured value of signal and decoy mean photon number per pulse at the transmitter, respectively given by \(\mu = 0.623 \pm 0.002\) and \(\nu = 0.165 \pm 0.001\).

In table I we show the experimental measured parameters \(Q_{\mu}, E_{\mu}, Q_{\nu}, E_{\nu}\) and \(Y_0\) used to estimate the secure key rate. The measured \(Q_{\mu}\) are compatible with the the measured transmission of the channel \(\eta_{\text{ch}} \sim 10\%\), the coupling efficiency into single mode fiber \(\eta_c \sim 25\%–35\%\), the detection efficiency \(\eta_d \sim 60\%\) since \(Q_{\mu} \simeq \mu \eta_{\text{ch}} \eta_c \eta_d\).

<table>
<thead>
<tr>
<th>(\theta)</th>
<th>(Q_{\mu})</th>
<th>(E_{\mu}(%))</th>
<th>(Q_{\nu})</th>
<th>(E_{\nu}(%))</th>
<th>(Y_0)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0°</td>
<td>1.43 \times 10^{-2}</td>
<td>3.81</td>
<td>4.77 \times 10^{-3}</td>
<td>7.63</td>
<td>3.77 \times 10^{-4}</td>
</tr>
<tr>
<td>15°</td>
<td>1.30 \times 10^{-2}</td>
<td>6.88</td>
<td>4.12 \times 10^{-3}</td>
<td>8.67</td>
<td>2.55 \times 10^{-4}</td>
</tr>
<tr>
<td>45°</td>
<td>1.11 \times 10^{-2}</td>
<td>4.16</td>
<td>2.77 \times 10^{-3}</td>
<td>4.47</td>
<td>6.63 \times 10^{-5}</td>
</tr>
<tr>
<td>60°</td>
<td>0.85 \times 10^{-2}</td>
<td>5.84</td>
<td>2.34 \times 10^{-3}</td>
<td>6.23</td>
<td>1.13 \times 10^{-4}</td>
</tr>
</tbody>
</table>

TABLE I. Experimental values of the signal and decoy gains, \(Q_{\mu}\) and \(Q_{\nu}\) and corresponding QBER \(E_{\mu}\) and \(E_{\nu}\) for different rotation angles \(\theta\). We also report the background rate \(Y_0\).
Analysis of the turbulence

In this section we investigate the effects of the turbulence on the OAM propagation. We recorded the intensity pattern at the receiver for 30 seconds at a frame rate of 4.95fps, obtaining 177 frames. We show in figure 1 some of the recorded frames. In Supplementary Material we show the full recorded video.

![Intensity pattern recorded at the receiver at different times. The delay between images is 10s.](image1)

In case of weak turbulence, the main effect on the beam propagation is the so called beam wandering, corresponding to a movement of the intensity centroids at the receiver plane. In order to evaluate the turbulence parameters, we calculated the centroid positions in each frame. Their positions and they corresponding distributions in the X and Y axis are reported in fig. 2.

In weak turbulence condition, the standard deviation $\sigma_m$ of the displacement of the centroids is related to the Fried parameter (or Fried’s coherence length) $r_0$ according to the relation given by Fante [3]:

$$\sigma_m^2 = \frac{4L^2}{k^2 r_0^2}$$

where $L$ is the path length and $k = \frac{2\pi}{\lambda}$ the wavevector of the optical beam. We extended the previous equation for OAM beam since the turbulence is weak and its main effect on the beam propagation is beam wandering.

![Centroids position and their distributions in the X and Y axis.](image2)

In our case, the measured average value is $\sigma_m = 0.33mm$, and the corresponding estimate for $r_0$ is

$$r_0 = \frac{2L}{k\sigma_m} \simeq 17cm.$$  

Since the beam radius $r \simeq 1.5cm$ is much smaller than $r_0$ the effects of the phase aberrations are weak and the OAM scattering is small [4]. Indeed, the chief ray of the beam is moving of the order of a millimeter in the transverse plane of the receiver, with a limited increase of losses. In these conditions we can also exclude the generation of OAM states which is predicted for stronger turbulence in [5] (see also references therein and [6]).

The Fried parameter can be related to the atmospheric turbulence strength $C_n^2$ by the following equation

$$r_0 = [0.423k^2 \int C_n^2(z)dz]^{-3/5}.$$  

By assuming that the $C_n^2$ coefficient is constant along the path $C_n^2(z) = C_n^2$ we can obtain

$$C_n^2 = \frac{r_0^{-5/3}}{0.432 \frac{k^2 L}{k^2 L}} \simeq 4 \cdot 10^{-15} m^{-2/3},$$
indeed corresponding to weak turbulence.

**Secure distance Analysis**

By using the data of our experiment we can estimate the maximum distance for the secure key generation. We consider the dark count of the (free-running) detectors equal to 100Hz (a typical condition achievable in dark condition). Since the duration of our qubits is 50ns, it is possible to estimate the dark rate as $Y_0 = 5 \cdot 10^{-6}$. By considering a typical channel QBER of $E_{ch} = 2\%$, we can predict the error rate in the signal and decoy transmission as

$$E_\mu^* = \frac{1}{2} \frac{Y_0}{Q_\mu} + E_{ch}(1 - \frac{Y_0}{Q_\mu}), \quad E_\nu^* = \frac{1}{2} \frac{Y_0}{Q_\nu} + E_{ch}(1 - \frac{Y_0}{Q_\nu}) \quad (8)$$

with $Q_\nu = \frac{\nu}{\mu} Q_\mu$. We here remember that, due to our polarization-OAM encoding, turbulence will affect the losses and not the QBER.

By using equations (1) with $f(E_\mu) = 1.05$, $\mu = 0.623$ and $\nu = 0.165$, we can estimate the QBERs $E_\mu$, $E_\nu$ and the key rate $r$ in function of the signal gain $Q_\mu$. The result are shown in fig. 3. Positive rates are obtained up to a gain of $G_\mu^* \simeq 10^{-4}$. Since we measured a gain of $G_\mu = 1.2 \cdot 10^{-2}$, our system could tolerate losses that are two order of magnitude larger.

We estimate that positive rate could be achieved up to few kilometers. Indeed, by using a suitable collecting telescope (with diameter of the order of 30cm) it is possible to reduce the losses due to beam clipping in the few km scale. Concerning turbulence effects, with the atmospheric turbulence strength equal to the value we measured $C_n^2 \simeq 4 \cdot 10^{-15} m^{-2/3}$, the Fried parameter $r_0$ becomes of the order of the beam radius for distance larger than 1km. In this case, as predicted by Paterson [4], the scattering between OAM modes become influent and this translates for our encoding into additional losses lowering the transmission by a factor of 0.1. Longer links will produce larger losses according to [4].

---

* Current address: Centre for Quantum Dynamics, Griffith University, Brisbane 4111, Australia