Supplementary Information of: Free-space quantum key distribution by rotation-invariant twisted photons

Giuseppe Vallone,[1] Vincenzo D'Ambrosio,[2] Anna Sponselli,[3] Sergei Slussarenko,[4,*] Lorenzo Marrucci,[4] Fabio Sciarrino,[2,5] and Paolo Villoresi[1]

[1] *Dipartimento di Ingegneria dell'Informazione, Università di Padova, I-35131 Padova, Italy*
[2] *Dipartimento di Fisica, Sapienza Università di Roma, I-00185 Roma, Italy*
[3] *Dipartimento di Fisica e Astronomia, Università di Padova, I-35131 Padova, Italy*
[4] *Dipartimento di Fisica, Università di Napoli Federico II and CNR - SPIN, Napoli.*
[5] *Istituto Nazionale di Ottica (INO-CNR), Largo E. Fermi 6, I-50125 Firenze, Italy*

(ΩDated: July 1, 2014)

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: μ, the signal state, and two other decoy values, ν and zero (corresponding to sending empty pulses). The bits obtained with μ 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]

$$r = \frac{Q_1^L}{Q_\mu}[1 - h_2(e_1^U)] - \text{leak}_{EC} + \frac{Q_0}{Q_\mu} \tag{1}$$

where Q_μ is the total gain (the fraction of detected bits over the sent bits), Q_1^L the lower bound of the gain of the one-photon states, Q_0 the gain of the vacuum states, E_μ the total quantum bit error rate (QBER), e_1^U 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 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_1^L, Q_0 and e_1^U by the decoy data as

$$Q_1^L = \frac{\mu^2 e^{-\mu}}{\mu\nu - \nu^2}\left(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0\right) \tag{2}$$

and

$$e_1^U = \frac{E_\nu Q_\nu e^\nu - e_0 Y_0}{Q_1^L \frac{\nu}{\mu} e^\mu}\,, \quad Q_0 = e^{-\mu} Y_0\,. \tag{3}$$

In the previous expression Q_ν and E_ν are the total gain and the QBER of decoy states ν respectively, while Y_0 is the dark rate at the receiver. The parameters μ and ν 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_μ, E_μ, Q_ν, E_ν and Y_0 used to estimate the secure key rate. The measured Q_μ are compatible with the the measured transmission of the channel $\eta_{\rm ch} \sim 10\%$, the coupling efficiency into single mode fiber $\eta_{\rm c} \sim 25\%$–35%, the detection efficiency $\eta_{\rm d} \sim 60\%$ since $Q_\mu \simeq \mu\eta_{\rm ch}\eta_{\rm c}\eta_{\rm d}$.

θ	Q_μ	$E_\mu(\%)$	Q_ν	$E_\nu(\%)$	Y_0
$0°$	1.43×10^{-2}	3.81	4.77×10^{-3}	7.63	3.77×10^{-4}
$15°$	1.30×10^{-2}	6.88	4.12×10^{-3}	8.67	2.55×10^{-4}
$45°$	1.11×10^{-2}	4.16	2.77×10^{-3}	4.47	6.63×10^{-5}
$60°$	0.85×10^{-2}	5.84	2.34×10^{-3}	6.23	1.13×10^{-4}

TABLE I. Experimental values of the signal and decoy gains, Q_μ and Q_ν and corresponding QBER E_μ and E_ν for different rotation angles θ. 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.

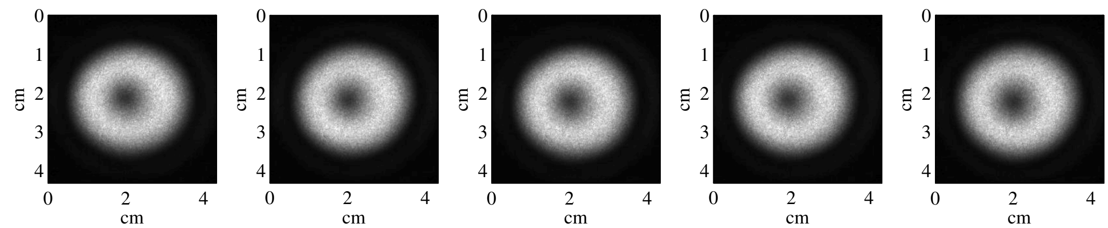

FIG. 1. Intensity pattern recorded at the receiver at different times. The delay between images is 10s.

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 σ_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]:

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

where L is the path length and $k = 2\pi/\lambda$ 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.

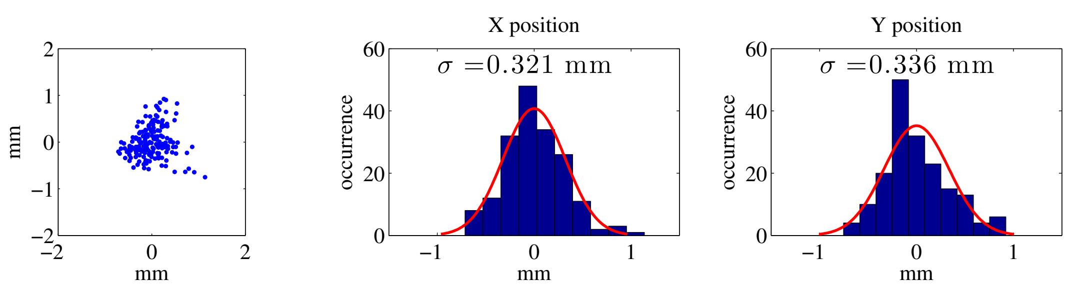

FIG. 2. Centroids position and their distributions in the X and Y axis.

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

$$r_0 = \frac{2L}{k\sigma_m} \simeq 17cm\,. \tag{5}$$

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

$$r_0 = [0.423k^2 \int C_n^2(z)dz]^{-3/5}\,. \tag{6}$$

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

$$C_n^2 = \frac{r_0^{-5/3}}{0.432\,k^2\,L} \simeq 4\cdot 10^{-15} m^{-2/3}\,, \tag{7}$$

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 $E_{\rm ch} = 2\%$, we can predict the error rate in the signal and decoy transmission as

$$E^*_\mu = \frac{1}{2}\frac{Y_0}{Q_\mu} + E_{\rm ch}(1 - \frac{Y_0}{Q_\mu})\,, \qquad E^*_\nu = \frac{1}{2}\frac{Y_0}{Q_\nu} + E_{\rm ch}(1 - \frac{Y_0}{Q_\nu}) \tag{8}$$

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_μ, E_ν and the key rate r in function of the signal gain Q_μ. The result are shown in fig. 3. Positive rates are obtained up to a gain

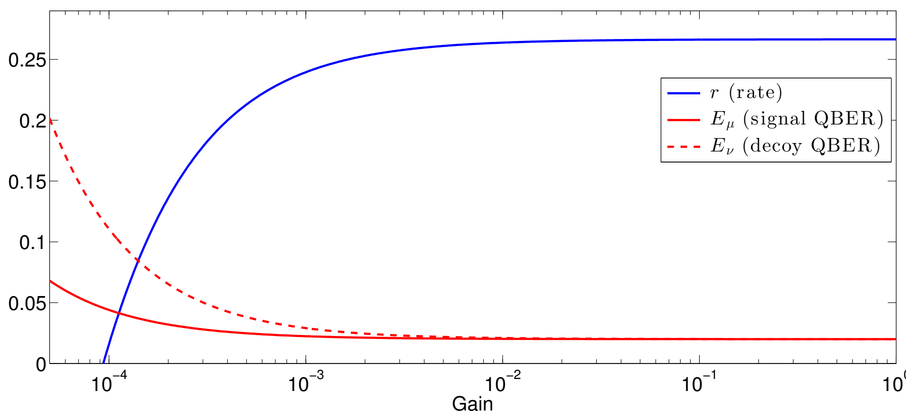

FIG. 3. Expected rate and QBER in function of the gain Q_μ.

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

[1] W.-Y. Hwang, Phys. Rev. Lett. **91**, 57901 (2003).
[2] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).
[3] R. L. Fante, Proceedings of the IEEE **63**, 1669 (1975).
[4] C. Paterson, Phys. Rev. Lett. **94**, 153901 (2005).
[5] D. W. Oesch, D. J. Sanchez, A. L. Gallegos, J. M. Holzman, T. J. Brennan, J. C. Smith, W. J. Gibson, T. C. Farrell, and P. R. Kelly, Optics Express **21**, 5440 (2013).
[6] M. Malik, M. O'Sullivan, B. Rodenburg, M. Mirhosseini, J. Leach, M. P. J. Lavery, M. J. Padgett, and R. W. Boyd, Opt. Exp. **20**, 13195 (2012).