Complete experimental toolbox for alignment-free quantum communication – Supplementary Information

Vincenzo D'Ambrosio,[1] Eleonora Nagali,[1] Stephen P. Walborn,[2] Leandro Aolita,[3] Sergei Slussarenko,[4] Lorenzo Marrucci,[4,5] and Fabio Sciarrino[1]

[1]*Dipartimento di Fisica, Sapienza Università di Roma, Roma 00185, Italy*
[2]*Instituto de Física, Universidade Federal do Rio de Janeiro, Rio de Janeiro, RJ 21941-972, Brazil*
[3]*ICFO-Institut de Ciències Fotòniques, Av. Carl Friedrich Gauss 3, 08860 Castelldefels (Barcelona), Spain*
[4]*Dipartimento di Scienze Fisiche, Università di Napoli "Federico II", Compl. Univ. di Monte S. Angelo, 80126 Napoli, Italy*
[5]*CNR-SPIN, Complesso Universitario di Monte S. Angelo, 80126 Napoli, Italy*

Supplementary Discussion

Review of previous results on alignment-free quantum communication. We begin by considering prepare-and-measure quantum-key distribution protocols: In Ref. 43, an ingenious technique was proposed based on circularly polarized single-photon states. This scheme (from now on called the LSRO10 scheme) is suitable for unknown, and possibly misaligned, relative transverse-axis orientations. However, to bound the knowledge of potential eavesdroppers, a tomographically-complete set of correlations between sender preparations and receiver measurements must be determined[50]. If the relative misalignment varies in an uncontrolled fashion during the signal-acquisition process, the necessary correlations are smeared out and therefore no security can be guaranteed. For this reason, the scheme is applicable if the misalignment angle θ varies at a slow rate over a time long enough to collect enough signals to overcome finite-sized key effects.

This has been quantitatively studied in Ref. 51, accounting for realistic conditions as non-perfect classical post-processing, quantum-bit error rates of 5%, and for θ varying both at constant speed or in a random walk. The authors found for instance that, for secret-key fractions of $r \approx 5\%$, the LSRO10 scheme requires about 10^7 signals, and this holds only if θ varies at most 10^{-10} (for constant rotation) and 10^{-5} (for random-walk rotation) degrees from signal to signal uninterruptedly throughout the entire signal collection. Our scheme instead allows a BB84 implementation which does not suffer from such restriction, as it is immune to arbitrary variations of θ.

Considering now non-locality tests, recently interesting alignment-free approaches to extract non-local correlations have been put forward (Refs. 45,46). They are based on the fact that, even for randomly chosen settings, there is always a finite probability of observing non-locality[44]. However these approaches require that θ stays fixed throughout the data exchange session.

Misalignment-immune quantum communication, for the restricted case of a single logical qubit, has been previously demonstrated in Ref. 13. This experiment used four physical qubits realized with the polarization and time-bin degrees of an entangled-photon pair, to encode a logical one. That is, it required a parametric down-conversion setup plus a complex interferometer to encode a single logical qubit. The main disadvantage of this approach is that, since two photons are used in the encoding, the sensitivity to photon losses increases quadratically. For example, in a scenario of satellite-to-earth quantum communication, losses may typically be greater than 10^{-9} per photon (see Ref. 5). Thus, two-photon encodings must overcome losses of around 10^{-18}. In addition to losses, the state preparation in the approach of Ref. 13 is probabilistic, so that only about 1/3 of the pairs produced are actually used. Moreover, an interferometric setup is sensible to optical-path fluctuations and requires thus non-trivial compensations in a hypothetical distant moving station.

Advantages and limitations of the q-plate device. Let us now briefly discuss the advantages of the q-plate over other methods for OAM manipulation. In principle the q-plate used in our work for converting the polarization encoding of qubits into the hybrid rotation-invariant one could be replaced with a complex arrangement of standard polarization and OAM generation/measurement devices. However the latter would be significantly less efficient (for example, spatial light modulators typically cannot exceed 40-45% of efficiency when used for measuring an OAM-encoded qubit in a given basis) and more difficult to align. In addition these standard methods would only allow one to generate and measure the hybrid qubit locally (unless a very complex interferometric layout is adopted), while the q-plates may be used to transmit (without shared reference frame) unknown qubits coming from external remote sources and encoded in polarization. Or, at the receiver site, the q-plate allows one to use the received qubit in further quantum processing based on polarization encoding, without actually measuring it.

Current q-plates have a radius of few millimeters, but q-plates having a radius as large as few meters (e.g., for long-distance communication) should be practically realizable with current liquid crystal display technology or using liquid-crystal polymer films[52]. One important practical issue is the actual size of the central defect, which ideally

should be pointlike, but in practice always has a finite extension. This size is important for the proper working of the encoding/decoding units, in particular when the beam is displaced (or the two units' optical axes are not well aligned). Indeed, we believe that the decrease in average communication fidelity as a function of the beam displacement that we have observed (see Fig. 4 of the main article), which is not expected on the basis of our theory for ideal q-plates, is actually due to imperfections in our q-plate devices. In particular, the central defect of our q-plates with $q = 1/2$ has an extension of about 100 μm. This introduces a small component of light that is not properly decoded in the measurement stage and therefore gives rise to some qubit alteration. This effect is usually negligible in the case of well-aligned beams because the defect coincides with the beam vortex, so there is almost no light being affected. This is however clearly not a fundamental limitation, and we are confident that this problem will be strongly reduced by using light beams with a larger waist and by perfecting the manufacturing process of the q-plate. We notice that a similar sensitivity to the size of the q-plate central defect is found in their recently demonstrated coronography applications, e.g. in connection with the search for extra-solar planets[53,54].

Supplementary Methods

Effect of parallel beam displacement. The effect of beam translation for a Laguerre-Gauss (LG) beam with initial $p = 0$ and $m = 1$ was treated in Ref. 42 [equations (4)-(7)]. We generalize here the reported result to the case of initial $p = 0$ and $m = \pm 1$, obtaining the following expression for the translated beam in polar coordinates ρ, φ:

$$E(\rho,\varphi) = \frac{A}{w_0}\left(\rho e^{\pm i\varphi} - \delta e^{\pm i\theta}\right) e^{-\frac{\rho^2+\delta^2}{w_0^2}} \sum_{m=-\infty}^{+\infty} I_m\left(\frac{2\rho\delta}{w_0^2}\right) e^{im(\varphi-\theta)} \tag{S1}$$

where δ and θ are the polar coordinates of the displacement vector in the plane orthogonal to the beam axis z, w_0 is the beam waist, A a normalization constant, and I_m are the modified Bessel functions of the first kind.

By projection of the latter expression on a LG mode with $p' = 0$ and $m' = m = \pm 1$, we obtain the following transformation coefficients:

$$C_{m,m';0,0} = \frac{2\pi A^2}{w_0^2}\int_0^\infty \left\{\rho^2 e^{-\frac{2\rho^2+\delta^2}{w_0^2}}\left[\rho I_0\left(\frac{2\rho\delta}{w_0^2}\right) - \delta I_1\left(\frac{2\rho\delta}{w_0^2}\right)\right]\right\} d\rho \tag{S2}$$

which are independent of the sign of $m = m'$ and hence satisfy Eq. (17) of the main article. A similar, though more complex, analysis can be carried out for arbitrary p and p'.

Beam tilting. We generalize the results given in Ref. 42 [equations (11)-(13)], obtaining the following expression for the transformation coefficients representing the effect of beam tilt on LG beam having $p = p' = 0$ and $m = m' = \pm 1$:

$$C_{m,m';0,0} = \frac{2\pi A^2}{w_0^2}\int_0^\infty \rho^3 e^{-\frac{2\rho^2}{w_0^2}} J_0(\alpha\rho) d\rho \tag{S3}$$

where $\alpha = k\sin\gamma$, with k the beam wavenumber and γ the tilt angle. The tilt azimuthal angle η is irrelevant here, and Eq. (17) of the main article is satisfied.

Combination of beam tilt and displacement. We now generalize the results given in Ref. 42 [equations (14)-(17)], obtaining the following expression for the transformation coefficients representing the combined effect of beam tilt and displacement on LG beam having $p = p' = 0$ and $m = m' = \pm 1$:

$$C_{m,m';0,0} = \frac{2\pi A^2}{w_0^2}\int_0^\infty \rho^2 e^{-\frac{2\rho^2+\delta^2}{w_0^2}} \left[\rho S_0(\rho) - \delta S_1(\rho)\right] d\rho \tag{S4}$$

where

$$S_0(\rho) = \sum_{n=-\infty}^{+\infty} I_{|n|}\left(\frac{2\rho\delta}{w_0^2}\right) J_n(\alpha\rho) e^{in(\theta-\eta+\pi/2)} \tag{S5}$$

and

$$S_1(\rho) = \sum_{n=-\infty}^{+\infty} I_{|n-m|}\left(\frac{2\rho\delta}{w_0^2}\right) J_n(\alpha\rho) e^{in(\theta-\eta+\pi/2)} \tag{S6}$$

On inspection, we find that this result satisfies Eq. (17) of the main article if $\theta = \eta$ (or $\theta = \eta \pm \pi$), i.e. tilt and displacement occur in the same (or opposite) azimuthal direction. This is consistent with the general analysis based on the mirror symmetry of the transformation, which is broken if $\theta \neq \eta$ and $\theta \neq \eta \pm \pi$.

Supplementary References

[50] Le, T. P., Sheridan, L. & Scarani, V. Tomographic quantum cryptography protocols are reference frame independent. Preprint at http://arxiv.org/abs/1109.2510v3 (2011).

[51] Sheridan, L., Le, T. P. & Scarani, V. Finite-key security against coherent attacks in quantum key distribution. *New. J. Phys.* **12**, 123019 (2010).

[52] Nersisyan, S., Tabiryan, N., Steeves, D. M. & Kimball, B. R. Fabrication of liquid crystal polymer axial waveplates for UV-IR wavelengths. *Opt. Express* **17**, 11926–11934 (2009).

[53] Mawet, D. *et al.* Optical vectorial vortex coronagraphs using liquid crystal polymers: theory, manufacturing and laboratory demonstration. *Opt. Express* **17**, 1902-1918 (2009).

[54] Serabyn, E., Mawet, D. & Burruss, R. An image of an exoplanet separated by two diffraction beamwidths from a star *Nature* **464**, 1018–1020 (2010).