Deliverable Report

Deliverable No: D6.1

Deliverable Title: Devices for misalignment free quantum communication (encoding, decoding and manipulation)

Grant Agreement number: 255914

Project acronym: PHORBITECH

Project title: A Toolbox for Photon Orbital Angular Momentum Technology

Project website address: www.phorbitech.eu

Name, title and organisation of the scientific representative of deliverable's lead beneficiary (task leader):

Dr. Fabio Sciarrino
Sapienza Università di Roma (UROM)
Roma, Italy

Deliverable table

Deliverable no.	D6.1
Deliverable name	Devices for misalignment free quantum communication (encoding, decoding and manipulation)
WP no.	6
Lead beneficiary no.	2 (UROM)
Nature	P
Dissemination level	PU
Delivery date from Annex I	Month 27
Actual delivery date	30 September 2012

D6.1) Devices for misalignment free quantum communication (encoding, decoding and manipulation): Prototypes of devices allowing for the encoding and decoding of the quantum information in rotation-invariant states of the photons and for their manipulation, and demonstration of basic quantum communication tasks. [*Excerpt from the Annex describing the deliverables of WP6, page 30]*

Notice on the delivery time: this deliverable was initially scheduled for month 27 of the project, but all the main objectives have been achieved and the scientific results have been published in a article appeared in Nature Communication (Ref. [1]). Accordingly, we prefer to anticipate the delivery in order to focus on more advanced scientific tasks in the third year of the projects.

Quantum communication employs the counter-intuitive features of quantum physics for tasks that are impossible in the classical world. It is crucial for testing the foundations of quantum theory and promises to revolutionize information and communication technologies. However, to execute even the simplest quantum transmission, one must establish, and maintain, a shared reference frame. This introduces a considerable overhead in resources, particularly if the parties are in motion or rotating relative to each other.

UNAP, URIO and UROM have experimentally shown how to circumvent this problem with the transmission of quantum information encoded in rotationally invariant states of single photons.

The PHORBITECH consortium has experimentally demonstrated a complete toolbox for the efficient encoding and decoding of quantum information in such photonic qubits, suitable for alignment-free quantum communication. The core of our toolbox is the 'q-plate' device developed by UNAP, that maps polarization-encoded qubits into qubits encoded in hybrid polarization-OAM states of the same photon that are invariant under arbitrary rotations around the propagation direction, and vice versa: Figure 1-a,b. In other words, the q-plate acts as a universal encoder/decoder, where 'universal' refers to the fact that it works for any qubit state. The q-plate used in the present work is the result of a very recent technological advance allowing for the manufacture of electrically tunable devices with topological charge $q = 1/2$ reported within the first year of PHORBITECH. The application reported here corresponds to the first time such devices are exploited in the quantum regime. In addition, the toolbox requires no interferometric stability and can be set entirely in a robust and compact unit that could easily be mounted in a small satellite, for instance. Furthermore, the present universal-decoder set-up features a built-in filtering mechanism that maps a wide class of physical errors into losses instead of logical errors. UROM developed a compact toolbox with qplates, devices for the manipulation of the polarization (waveplates and polarizers) and single mode couplers: Figure 1: c-d-e.

By developing this complete toolbox for the efficient encoding and decoding of quantum information in such photonic qubits, we demonstrate the feasibility of alignment-free quantum key-distribution, and perform proof-of-principle demonstrations of alignment-free entanglement distribution and Bell-inequality violation. The scheme should find applications in fundamental tests of quantum mechanics and satellite-based quantum communication.

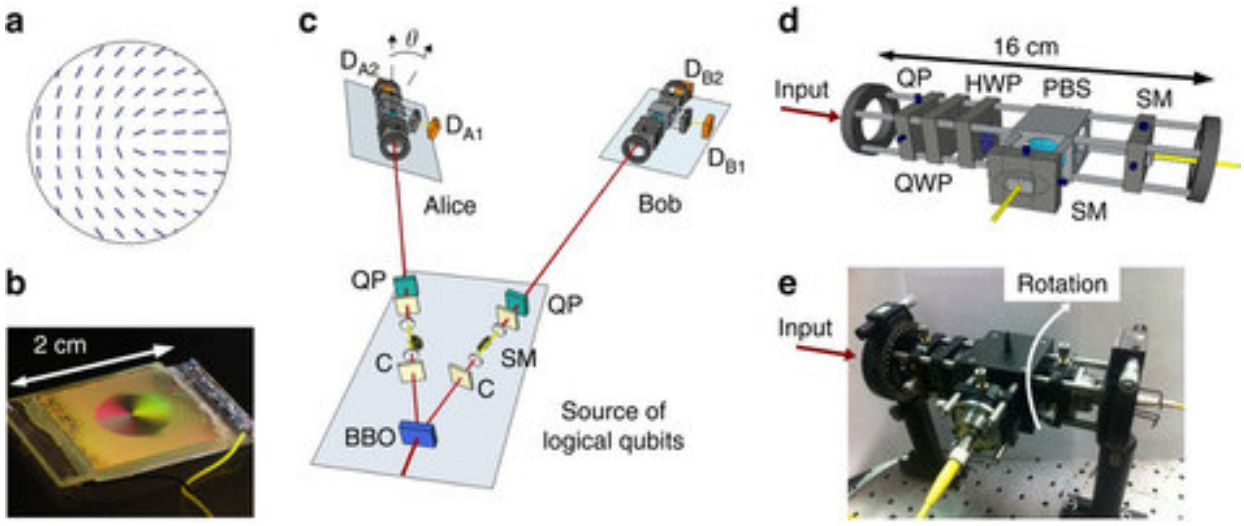

Figure 1. Toolbox for experimental alignment-free quantum communication.
(a, b) The liquid crystal q-plate with topological charge q=1/2 works as a universal logical-qubit encoder/decoder. Panel (a) shows the q-plate optical axis pattern, whereas panel (b) is a photo of the device seen through crossed polarizers, under oblique illumination; different colours result from different optical axis orientations. The q-plate birefringent retardation is electrically tuned. **(c)** Experimental set-up, in the configuration used to generate entangled rotationally invariant photon pairs and to perform a misalignment-immune demonstration of non-locality. Reference-frame misalignments are implemented by physically rotating Alice's entire measurement station around the optical axis by an angle θ. For the alignment-free BB84 QKD test, the entangled-photon source, together with Bob's measurement station, is taken as the transmitting party, and Bob's photon is used to herald the transmission of the other photon to Alice. The communication distance was 60 cm. **(d)** Schematics of the rotating device for measuring rotationally invariant qubits in arbitrary reference frames. **(e)** Photo of the actual measurement device. QP, q-plate; C, walk-off compensation crystals; SM, single-mode fibres; D, single photon detectors; HWP, half-wave plate; QWP, quarter-wave plate.

As further step, UNAP and UROM have designed a q-plate with an innovative geometry able to perform a unitary transformation (a rotation) of a qubit encoded in the hybrid polarization-OAM Hilbert space. The rotation in the hybrid encoding space can be written as follows:

$$QP[\delta]|Rl\rangle = \cos\left(\frac{\delta}{2}\right)|Rl\rangle + \sin\left(\frac{\delta}{2}\right)|Lr\rangle$$

$$QP[\delta]|Lr\rangle = -\sin\left(\frac{\delta}{2}\right)|Rl\rangle + \cos\left(\frac{\delta}{2}\right)|Lr\rangle$$

The geometry of a q-plate with q = 1 and $\alpha_0 = \pi/4$ is showed in Figure 2. The retardation δ of the q-plate (and the induced angle of logical rotation) can be controlled in different ways (pressure, temperature, electric field). Among them, the most practical is certainly the application of a tunable electric field (B. Piccirillo, V. D'Ambrosio, S. Slussarenko, L. Marrucci, E. Santamato, Appl. Phys. Lett. 97, 241104 (2010)) via a common generator. This technology would allow to operate the logical rotations acting only on a knob. The new q-plate has recently been fabricated by UNAP.

UROM and UNAP have characterized the q-plate retrieving the retardation δ from a measurement of the conversion efficiency versus the applied voltage. Presently we are adopting the same setup of the alignment free experiment to a polarization tomography to reconstruct the state for different values of δ [2]. The final results will be reported within deliverable D6.2.

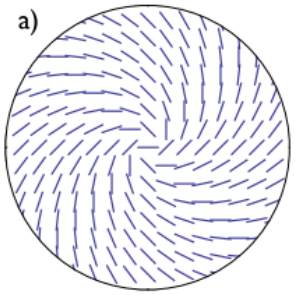

Figure 2. Q-plate geometry for the logical rotation of rotational invariant qubits

It is worth mentioning here also another scientific result obtained by UNIVBRIS (Jeremy O'Brien, in collaboration with other non-PHORBITECH researchers), on the guaranteed violation of a Bell inequality without aligned reference frames or calibrated devices [3]. Bell tests — the experimental demonstration of a Bell inequality violation — are central to understanding the foundations of quantum mechanics, and are a powerful diagnostic tool for the development of quantum technologies. To date, Bell tests have relied on careful calibration of measurement devices and alignment of a shared reference frame between two parties — both technically demanding tasks. The UNIVBRIS team has shown that neither of these operations are necessary, violating Bell inequalities (i) with certainty using unaligned, but calibrated, measurement devices, and (ii) with near-certainty using uncalibrated and unaligned devices. They demonstrated generic quantum nonlocality with randomly chosen measurements on a single state of two photons, implemented using a reconfigurable integrated optical waveguide circuit. The observed results demonstrate the robustness of these schemes to imperfections and statistical noise. Although not originally planned in PHORBITECH workplan, this result is consistent with the general goals of WP6.

References (publications related with this deliverable):

[1] "Complete experimental toolbox for alignment-free quantum communication", V. D'Ambrosio, E. Nagali, S.P. Walborn, L. Aolita, S. Slussarenko, L. Marrucci, F. Sciarrino, *Nature Communications* **3**, 961 (2012).

[2] "Logical rotation of rotational-invariant qubits through q-plates", V. D'Ambrosio, L. Marrucci, F. Sciarrino, S. Slussarenko (manuscript in preparation).

[3] "Guaranteed violation of a Bell inequality without aligned reference frames or calibrated devices", P. T. Vértesi, Y.-Cherng Liang, C. Branciard, N. Brunner, and J.L. O'Brien, *Scientific Reports* **2**, 470 doi:10.1038/srep00470 (2012).

PHORBITECH contribution to this deliverable:
The UROM-URIO-UNAP collaboration work reported in this deliverable report, corresponding to the development of the protoype, has been mainly supported by PHORBITECH, with some minor contribution coming from other funds (HYTEQ) for some lab equipment purchase. All UROM-UNAP-URIO involved researchers have been supported by PHORBITECH. The only person external to PHORBITECH in this work was Leandro Aolita, from ICFO, who contributed to some theoretical aspects of the work. The UNIVBRIS work has been supported by PHORBITECH in a fraction of the time of Jeremy O'Brien.

PHORBITECH contributors to this deliverable:
UROM: Eleonora Nagali, Vincenzo D'Ambrosio, Sandro Giacomini, Giorgio Milani, Fabio Sciarrino
UNAP: Sergei Slussarenko, Lorenzo Marrucci
URIO: Stephen P. Walborn
UNIVBRIS: Jeremy O'Brien

PROTOTYPE VALIDATION. The quality of the toolbox prototype for alignment-free quantum communication (that is, the encoder and decoder devices) has been assessed by the PHORBITECH steering committee in its meeting held in Leiden on September 13, 2012, after a detailed presentation of the device features and performances. The committee unanimously judged that the prototype performances meet fully the target goals set in the proposal (the members of the committee who are directly involved in this work did not participate in this final assessment). Particularly promising is the unanticipated robustness of the communication scheme against various beam perturbations.

Publications included with this report:
1. "Complete experimental toolbox for alignment-free quantum communication", V. D'Ambrosio, E. Nagali, S.P. Walborn, L. Aolita, S. Slussarenko, L. Marrucci, F. Sciarrino, *Nature Communications* **3**, 961 (2012).
2. "Guaranteed violation of a Bell inequality without aligned reference frames or calibrated devices", P. T. Vértesi, Y.-Cherng Liang, C. Branciard, N. Brunner, and J. L. O'Brien, *Scientific Reports* **2**, 470 (2012) doi:10.1038/srep00470.

nature COMMUNICATIONS

OPEN

ARTICLE

Received 30 Apr 2012 | Accepted 13 Jun 2012 | Published 17 Jul 2012

DOI: 10.1038/ncomms1951

Complete experimental toolbox for alignment-free quantum communication

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

Quantum communication employs the counter-intuitive features of quantum physics for tasks that are impossible in the classical world. It is crucial for testing the foundations of quantum theory and promises to revolutionize information and communication technologies. However, to execute even the simplest quantum transmission, one must establish, and maintain, a shared reference frame. This introduces a considerable overhead in resources, particularly if the parties are in motion or rotating relative to each other. Here we experimentally show how to circumvent this problem with the transmission of quantum information encoded in rotationally invariant states of single photons. By developing a complete toolbox for the efficient encoding and decoding of quantum information in such photonic qubits, we demonstrate the feasibility of alignment-free quantum key-distribution, and perform proof-of-principle demonstrations of alignment-free entanglement distribution and Bell-inequality violation. The scheme should find applications in fundamental tests of quantum mechanics and satellite-based quantum communication.

[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, Mediterranean Technology Park, 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. Correspondence and requests for materials should be addressed to F.S. (email: fabio.sciarrino@uniroma1.it).

Current implementations of quantum communication (QC) use photons as the carriers of qubits (quantum bits), the basic units of quantum information. This is due to the fact that photons, known as so-called 'flying qubits', are easy to transport from one location to another[1]. Photonic free-space QC has been demonstrated for distances of hundreds of kilometers[2], a progress that could soon lead to satellite-based long-distance QC[3–6]. However, standard approaches to QC, for example, the one based on encoding qubits into the polarization of photons, require that all users involved have knowledge of a shared reference frame. For instance, in the bipartite scenario, the emitter and receiver, conventionally called Alice and Bob, must initially align their local horizontal (H) and vertical (V) transverse axes, and then keep them aligned throughout the transmission (Fig. 1a). This, in turn, requires the exchange of a large (strictly speaking, infinite) amount of classical information. This represents, in general, an extra technical overhead, which can impose serious obstacles in the particular situations where the users are very far apart from each other, the misalignment between their frames varies in time, or the number of users is large, for example[7,8]. In general, the lack of a shared reference frame inhibits faithful QC, because it is equivalent to an unknown relative rotation, therefore introducing noise into the quantum channel[8].

A possible solution to this problem is to exploit multi-qubit entangled states that are invariant under single-qubit rotations acting collectively on all the qubits (see refs 9–13 and references therein). These constitute particular instances of decoherence-free subspaces, originally introduced in the context of fault-tolerant quantum computing[14–17]. The idea is thus to encode logical qubits into rotationally invariant states of multiple physical qubits. These can, in principle, be realized with multiple photons[10–12]. However, the efficient production and detection of multi-photon states is a technological challenge, they are more susceptible to losses, and the requirement that multiple photons are subject to exactly the same rotation is very seldom perfectly satisfied.

A more efficient way to circumvent misalignments is provided by exploiting multiple degrees of freedom of single photons[18]. In particular, the polarization and transverse spatial modes stand out for this purpose (Fig. 1b). Just as the circular polarization states are eigenstates of the spin angular momentum (SAM) of light, the helical-wavefront Laguerre-Gaussian modes are eigenmodes of its orbital angular momentum (OAM). The OAM degree of freedom is attracting a growing interest for applications in both classical and quantum photonics[19–22]. The peculiarity of the SAM and (first order) OAM eigenstates together is that, as they are defined with respect to the same reference frame, they suffer exactly the same transformation under coordinate rotation. Therefore, they satisfy the collective rotation requirement exactly, constituting an ideal pair to carry rotationally invariant hybrid qubits (see Fig. 1c).

Here we experimentally demonstrate a complete toolbox for the efficient encoding and decoding of quantum information in such photonic qubits, suitable for alignment-free QC. The core of our toolbox is a liquid crystal device, named 'q-plate'[22,23], that maps polarization-encoded qubits into qubits encoded in hybrid polarization-OAM states of the same photon that are invariant under arbitrary rotations around the propagation direction, and *vice versa*. In other words, the q-plate acts as a universal encoder/decoder, where 'universal' refers to the fact that it works for any qubit state. The q-plate used in the present work is the result of a very recent technological advance allowing for the manufacture of electrically tunable devices with topological charge $q = 1/2$ (ref. 24). This is the first time such devices are exploited in the quantum regime. In addition, the toolbox requires no interferometric stability as in previous proposals[18,25], and can be set entirely in a robust and compact unit that could easily be mounted in a small satellite, for instance. Furthermore, our universal-decoder set-up features a built-in filtering mechanism that maps a wide class of physical errors into losses instead of logical errors. We show that, owing to this mechanism, the scheme is robust also against misalignments around axes other than the propagation direction, as well as against other spatial perturbations. We demonstrate the potential of our method by performing a proof-of-principle misalignment-immune implementation of the single-photon Bennett–Brassard (BB84) quantum key-distribution (QKD) protocol[26], entanglement distribution, and the violation of the Clauser-Horne-Shimony-Holt (CHSH) Bell inequality[27].

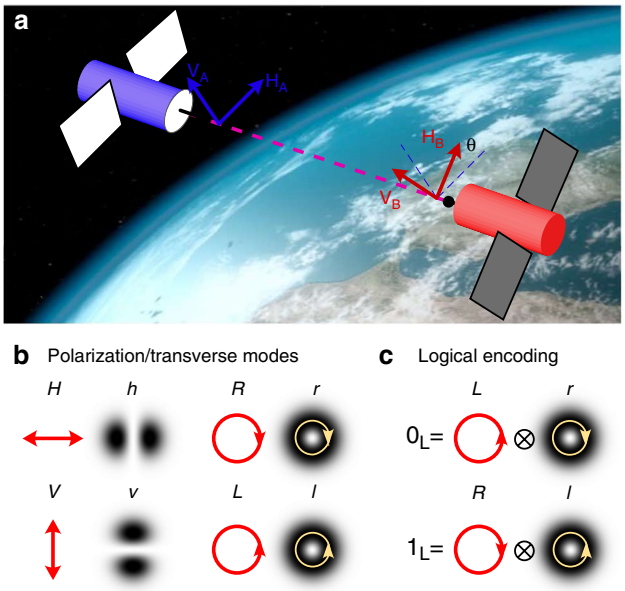

Figure 1 | Misalignment-immune single-photon qubits. (**a**) Alice and Bob, here depicted as satellites, need to carefully control the relative orientation between their horizontal (H) and vertical (V) axes to faithfully implement QC in free-space. Unknown misalignments around the propagation axis manifest as rotations of the transmitted qubits by unknown angles θ in the $H-V$ plane. (**b**) Qubits can be equivalently encoded in both polarization and transverse modes: H/V denote horizontal/vertical linear polarizations, L/R left/right circular polarizations, h/v horizontal/vertical first-order Hermite-Gauss modes, and l/r left- and right-handed first-order Laguerre-Gauss modes. The L/R polarizations are eigenstates with eigenvalues $\pm\hbar$ of the SAM, whereas the l/r modes are the equivalent eigenstates of the OAM. (**c**) By combining SAM and OAM eigenstates of opposite handedness, two null-eigenvalue eigenstates of the total angular momentum arise. Both these hybrid states are invariant under rotations around the propagation axis, and can therefore encode misalignment-immune logical qubit states, called 0_L and 1_L.

Results

Hybrid logical qubit encoding. Our logical qubit basis is defined by the hybrid polarization-OAM single-photon states

$$|1\rangle_L = |R\rangle_p |l\rangle_o \qquad |0\rangle_L = |L\rangle_p |r\rangle_o. \tag{1}$$

Subscript 'p' denotes the polarization Hilbert space, spanned by the left- and right-handed circular polarization states $|L\rangle_p$ and $|R\rangle_p$, respectively, which are eigenstates of the SAM operator S_p^z along the propagation direction (z axis) of respective eigenvalues $s_p^z = \hbar$ and $s_p^z = -\hbar$. In turn, subscript 'o' stands for the OAM bidimensional subspace spanned by the left- and right-handed first-order Laguerre-Gauss modes $|l\rangle_o$ and $|r\rangle_o$, eigenstates of the OAM operator S_o^z of respective eigenvalues $s_o^z = \hbar$ and $s_o^z = -\hbar$. Finally, subscript L refers

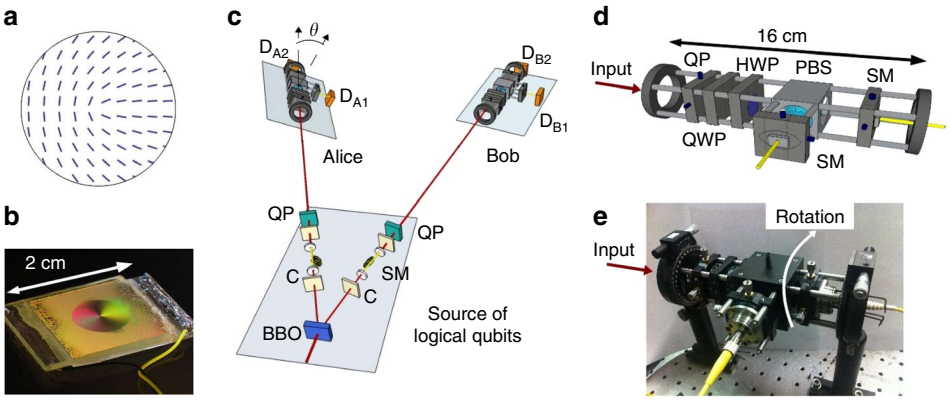

Figure 2 | Toolbox for experimental alignment-free quantum communication. (**a**, **b**) The liquid crystal q-plate with topological charge $q=1/2$ works as a universal logical-qubit encoder/decoder. Panel (**a**) shows the q-plate optical axis pattern, whereas panel (**b**) is a photo of the device seen through crossed polarizers, under oblique illumination; different colours result from different optical axis orientations. The q-plate birefringent retardation is electrically tuned. (**c**) Experimental set-up, in the configuration used to generate entangled rotationally invariant photon pairs and to perform a misalignment-immune demonstration of non-locality. Reference-frame misalignments are implemented by physically rotating Alice's entire measurement station around the optical axis by an angle θ. For the alignment-free BB84 QKD test, the entangled-photon source, together with Bob's measurement station, is taken as the transmitting party, and Bob's photon is used to herald the transmission of the other photon to Alice. The communication distance was 60 cm. (**d**) Schematics of the rotating device for measuring rotationally invariant qubits in arbitrary reference frames. (**e**) Photo of the actual measurement device. QP, q-plate; C, walk-off compensation crystals; SM, single-mode fibres; D, single photon detectors; HWP, half-wave plate; QWP, quarter-wave plate.

to the logical subspace of zero total angular momentum along z. The latter is spanned by the two hybrid states (1), null-eigenvalue eigenstates of the total SAM + OAM operator $S_p^z + S_o^z$. Because the total angular momentum operator is the generator of state rotations, states (1) are both invariant under arbitrary rotations around the z axis (on this issue, see also ref. 28). More specifically, in a physical rotation about the z axis by any angle θ, the circular polarization states and OAM eigenmodes acquire equivalent phase factors on their own: $|L/R\rangle_p \to e^{\mp i\theta}|L/R\rangle_p$ and $|l/r\rangle_o \to e^{\mp i\theta}|l/r\rangle_o$. However, for tensor-product combinations with opposite handedness as (1), the individual phases cancel each other and the composite states remain intact. As a consequence, because of linearity, any coherent superposition (or incoherent mixture) of the two logical states, that is, the entire logical subspace, is also immune to all possible reference-frame misalignments during the entire QC session.

Universal encoder/decoder. The experimental set-up used to encode and decode arbitrary hybrid qubit states in the logical basis (1) is shown in Fig. 2. The q-plates are liquid crystal devices that produce a spin-orbit coupling of the polarization and OAM contributions to the total angular momentum of photons[23,22]. The q-plate is a birefringent slab having a uniform optical retardation δ and a suitably patterned transverse optical axis, with a topological singularity of charge q at its centre. A 'tuned' q-plate with $\delta=\pi$ transfers quanta of angular momentum between the SAM and the OAM. Specifically, each photon suffers a variation in its OAM by an amount $\Delta = s_p^z 2q$ determined by the charge q and the SAM s_p^z of the input polarization. q-plates with $q=1$ have been recently used to demonstrate interesting spin-OAM quantum information manipulations[29–33].

A tuned q-plate with topological charge $q=1/2$ gives rise to the following transformations:

$$\begin{aligned} |R\rangle_p|0\rangle_o &\xrightarrow{q\text{-plate}} |L\rangle_p|r\rangle_o = |0\rangle_L \\ |L\rangle_p|0\rangle_o &\xrightarrow{q\text{-plate}} |R\rangle_p|l\rangle_o = |1\rangle_L, \end{aligned} \tag{2}$$

where $|0\rangle_o$ denotes a zero-OAM state, such as the fundamental Gaussian mode (TEM_{00}). We note that the radial profile of the $|l\rangle_o$ and $|r\rangle_o$ states generated by the q-plate is not exactly Laguerre-Gauss (see Methods for more details), but this does not affect their pure OAM-eigenstate rotational behaviour[22]. Indeed, the q-plate is ideally a unitary device (our q-plate was uncoated and had a transmission efficiency of about 85%), but the induced radial-mode effects (see Methods) may introduce about 40% of total additional losses in the final recoupling to the single-mode fibre before detection. Consider then a generic polarization-encoded qubit $|\psi\rangle_p = \alpha|R\rangle_p + \beta|L\rangle_p$ prepared in the TEM_{00} spatial mode. From transformations (2), sending the qubit through the q-plate yields

$$|\psi\rangle_p|0\rangle_o \xrightarrow{q\text{-plate}} \alpha|0\rangle_L + \beta|1\rangle_L = |\psi\rangle_L. \tag{3}$$

That is, the qubit is now encoded into the desired rotationally invariant space spanned by logical basis (1). Remarkably, the same q-plate device works also as a universal decoder, transferring generic rotationally invariant qubits to their polarization-encoded counterparts. Explicitly, by injecting $|\psi\rangle_L$ into the q-plate, one obtains

$$|\psi\rangle_L \xrightarrow{q\text{-plate}} (\alpha|R\rangle_p + \beta|L\rangle_p)|0\rangle_o = |\psi\rangle_p|0\rangle_o, \tag{4}$$

that can then be coupled into a single-mode fibre and analysed in polarization using standard methods. The measurement device is sketched in Fig. 2d. Again from the linearity of quantum mechanics, the encoding and decoding transformations (3) and (4) hold, even if the polarization state is part of some larger entangled state. In addition, an outstanding feature of the q-plate is that it realizes the polarization-transverse-mode coupling in a single compact device that requires no interferometric stability, therefore providing the scheme with a built-in robustness.

Our first step was to experimentally verify that the encoding/decoding apparatus works properly in the case of stationary aligned reference frames. We prepared the input photon in one of the polarization states $|H\rangle$, $|V\rangle$, $|R\rangle$, $|L\rangle$, or $|\pm\rangle = (|H\rangle \pm |V\rangle)/\sqrt{2}$.

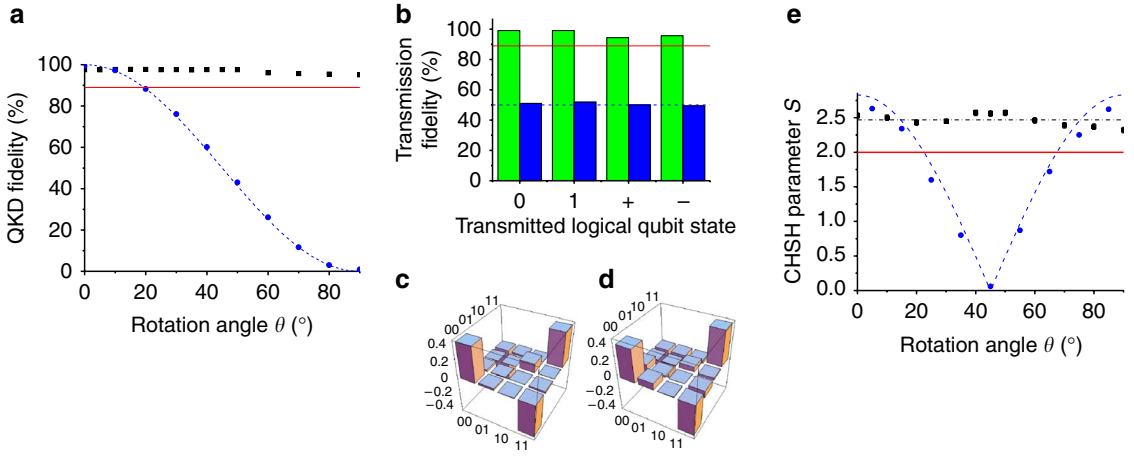

Figure 3 | Experimental results of alignment-free QC tests. (**a**, **b**) Measured fidelity of qubits encoded in the rotationally invariant polarization-OAM space, in a test of the BB84 quantum key distribution protocol, compared with that of standard polarization-encoded qubits. Panel (**a**) shows the fidelity F_{QKD} (black square dots) averaged over the four hybrid qubit states used in the protocol, as a function of the misalignment angle θ between the transmission and detection reference frames. Panel (**b**) shows the individual fidelity of each of the four states (green bars) observed over the whole QC session including all the different rotation angles probed. The latter accounts for the general situation where the misalignment could vary randomly between transmitted photons. In both panels, the blue dots/bars and dashed lines give, respectively, the measured and theoretically calculated fidelity for the standard case of polarization encoding. The red line delineates the QKD security threshold. (**c**, **d**) Quantum state tomography of the entangled state of hybrid qubits distributed between Alice and Bob, for the case of aligned reference frames (**c**) and for a misalignment of $\theta = 45°$ (**d**). In both cases, only the real part of the density matrices is shown, as the imaginary part is negligible. (**e**) CHSH parameter S (black squares) in experimental non-locality tests on photon pairs entangled in the rotationally invariant qubit space, as a function of the relative misalignment θ between Alice's and Bob's frames. The red line is the local-hidden-variable bound. The blue dots represent the measured values of S for the bare polarization-entangled states without the logical protection, whereas the blue dashed line is the theoretically calculated maximal CHSH parameter that would be obtained with pure maximally entangled polarization states. The black dot-dashed line, in turn, represents the overall CHSH value S of the entire test, taking into account all the experimental runs with different θ. Error bars result from Poissonian statistics. When not visible, the error bar is smaller than the symbol.

The qubit was then mapped by a first q-plate into the rotationally invariant encoding, transmitted through free space to the measurement stage, then decoded back to polarization by a second q-plate, and finally analysed in polarization using a set of wave plates and a polarizing beam splitter (PBS). The full experimental apparatus is described in the Methods. The average measured fidelity with the input states was $F = (98 \pm 1)\%$, indicating that the devices work nearly perfectly.

Alignment-free quantum key distribution. To experimentally demonstrate that the present QC set-up works well for arbitrary relative alignment of Alice and Bob's transverse reference frames, we mounted the q-plate, waveplates, PBS and optical fibre couplers in a compact and robust detection stage that can be freely rotated by any angle θ around the light propagation axis, as shown in Fig. 2d,e. Then, using heralded single photons, and for different angles θ, we encoded, transmitted and decoded, the four hybrid-qubit states required for the BB84 QKD protocol[26]: $|0\rangle_L, |1\rangle_L$, and $|\pm\rangle_L = (|0\rangle_L \pm |1\rangle_L)/\sqrt{2}$. We quantified the potential of our set-up for QKD by measuring the fidelities of the states prepared and measured with the ideal ones, as well as the qubit-error rates[34] $\varepsilon_{0_L/1_L}$ and $\varepsilon_{+_L/-_L}$ for the logical bases $\{|0\rangle_L, |1\rangle_L\}$ and $\{|+\rangle_L, |-\rangle_L\}$, respectively. The experimental results are reported in Fig. 3a,b.

Figure 3a shows the average fidelity F_{QKD} over the four states, as a function of θ. F_{QKD} is constantly above the value $F_T = 89\%$, which corresponds to the well-known Shor-Preskill security proof threshold[35]. Above this, under the usual assumptions that Alice's source emits (logical) qubits, Bob's detectors perform (logical) qubit measurements, and there is no basis-dependent flaw in Alice's and Bob's systems[36], unconditional security can be guaranteed. In contrast, the fidelity attained using polarization-encoded qubits falls below the security bound for angles $\theta > 20°$, even in the ideal noiseless case (blue dashed line). Figure 3b, in turn, shows the fidelity for each state, obtained by uniformly mixing the data over all measured angles θ. Again, all the individual-state fidelities are consistently larger than the security threshold. Indeed, the measured qubit-error rates, estimated as $1 - F$, were $\varepsilon_{0_L/1_L} = (0.65 \pm 0.09)\%$ and $\varepsilon_{+_L/-_L} = (4.1 \pm 0.2)\%$, from which we expect a high secret-key fraction $r = (70 \pm 1)\%$ (ref. 34).

Alignment-free entanglement distribution. To test entanglement distribution, the photon pair is prepared in the polarization entangled state $|\phi^-\rangle_p^{AB} = (1/\sqrt{2})(|R\rangle_p^A |R\rangle_p^B - |L\rangle_p^A |L\rangle_p^B)$, where the superscripts A and B refer to Alice's and Bob's photons, respectively. The photons are coupled into single-mode fibres that select only states with zero OAM (TEM_{00} mode). A q-plate at the output of each fibre transforms the polarization-entangled state to the rotationally invariant entangled state:

$$|\phi^-\rangle_p^{AB} \xrightarrow{q\text{-plates}} \rightarrow \frac{1}{\sqrt{2}}(|0\rangle_L^A |0\rangle_L^B - |1\rangle_L^A |1\rangle_L^B) = |\phi^-\rangle_L^{AB}. \qquad (5)$$

To verify the generation of hybrid entanglement, we performed quantum state tomography of the experimental density matrix ρ_L^{AB} measured without misalignment ($\theta = 0$). The tomographically reconstructed matrix, in the basis $\{|0\rangle_L^A |0\rangle_L^B, |0\rangle_L^A |1\rangle_L^B, |1\rangle_L^A |0\rangle_L^B, |1\rangle_L^A |1\rangle_L^B\}$, is shown in Fig. 3c. The fidelity with the experimental polarization entangled state ρ_p^{AB} input to the encoder is $F_0(\rho_L^{AB}, \rho_p^{AB}) = (93 \pm 1)\%$, while the entanglement of ρ_L^{AB}, as given by the concurrence, is $C = (0.85 \pm 0.03)$. As a first test on the rotational invariance of the state produced, we repeated the tomographic reconstruction with Alice's measurement stage rotated by $\theta = 45°$. The corresponding reconstruction is shown in Fig. 3d. The fidelity with ρ_p^{AB} is $F_{45}(\rho_L^{AB}, \rho_p^{AB}) = (96 \pm 1)\%$, and the concurrence is $C = (0.84 \pm 0.03)$, consistent with the case $\theta = 0$. This indicates that our entanglement

distribution scheme is immune to relative misalignments of Alice and Bob.

Alignment-free quantum non-locality. With the hybrid entangled state (5), we performed a violation of the CHSH inequality $S=|E(a_0,b_0)+E(a_1,b_0)+E(a_0,b_1)-E(a_1,b_1)|\leq 2$ in an alignment-free setting. In the inequality, a_x and b_y, with possible values 0 or 1, are the outcomes of Alice's and Bob's measurement settings x and y, respectively, with x and y equal to 0 or 1. Correlators $E(a_x,b_y)=\langle(-1)^{a_x+b_y}\rangle$, with $\langle\rangle$ the statistical average, quantify the fraction of events where Alice's and Bob's outcomes are observed to coincide. Any local-hidden-variable model satisfies the inequality[27]. For the rotationally invariant quantum violation of the inequality we chose the following hybrid measurement bases: $\{|0\rangle_L,|1_L\rangle\}$ and $\{|+\rangle_L,|-\rangle_L\}$, corresponding to Alice's settings $x=0$ and $x=1$, respectively, and $\{\cos(\pi/8)|0\rangle_L+\sin(\pi/8)|1\rangle_L,-\sin(\pi/8)|0\rangle_L+\cos(\pi/8)|1\rangle_L\}$ and $\{\sin(\pi/8)|0\rangle_L+\cos(\pi/8)|1\rangle_L,-\cos(\pi/8)|0\rangle_L+\sin(\pi/8)|1\rangle_L\}$, corresponding to Bob's settings $y=0$ and $y=1$, respectively. Figure 3e reports the measured CHSH parameter S versus the rotation angle θ of Alice's measurement frame. The figure shows that the local-hidden-variable bound is violated for all angles, in striking contrast with the experimental polarization state ρ_p^{AB} (blue circles), or even with the ideal maximally entangled polarization state $|\phi^-\rangle_p^{AB}$ (blue dashed line). For the logically encoded states, we mixed the data of all different values of θ to test the violation's immunity to arbitrarily varying frame orientation, obtaining a value of $S=(2.47\pm0.01)>2$. This alignment-free extraction of non-local correlations reconfirms the rotational invariance of the quantum resources created here.

Robustness of rotational-invariant hybrid qubits. A remarkable feature of our polarization-OAM hybrid-encoding QC scheme is that it turns out to be robust against the spatial-mode perturbations arising in beam misalignments around axes other than the optical one and atmospheric turbulence effects. Such robustness appears at first glance counterintuitive, because the encoding involves the use of OAM, which is quite sensitive to all the above-mentioned spatial perturbations[37,38] (although significant progresses in pure OAM-based classical and quantum communication through the atmosphere have been recently reported[39–41]). The main reason for such robustness is that the OAM spread induced by spatial-mode perturbations is neutralized by the polarization degree of freedom, which is in contrast very robust against those spatial-mode perturbations. This allows one to filter out, in the receiving unit, most components of the state that would otherwise decrease the fidelities. That is, the particular decoding set-up used intrinsically implements an effective quantum error-correction procedure that discards (but does not correct) all states outside the logical subspace.

Indeed, spatial-mode perturbations will alter a generic hybrid qubit $\alpha|R\rangle_p|l\rangle_o+\beta|L\rangle_p|r\rangle_o$, transforming it into the following state:

$$\sum_m[C_{+1,m}\alpha|R\rangle_p|m\rangle_o+C_{-1,m}\beta|L\rangle_p|m\rangle_o], \quad (6)$$

where $|m\rangle_o$ denotes a generic mode with OAM eigenvalue $m\hbar$ and $C_{m,m'}$ are the probability amplitudes for the photon OAM to be shifted from $m\hbar$ to $m'\hbar$, owing to the perturbation. However, in the decoding unit, the photon undergoes another q-plate transformation

$$\xrightarrow{q\text{-plate}}\sum_m[C_{+1,m}\alpha|L\rangle_p|m-1\rangle_o+C_{-1,m}\beta|R\rangle_p|m+1\rangle_o], \quad (7)$$

followed by a projection onto an $m=0$ Gaussian spatial mode (for example, by coupling it into a single-mode fibre), which leads to the following final state:

$$[C_{+1,+1}\alpha|L\rangle_p+C_{-1,-1}\beta|R\rangle_p]|0\rangle_o. \quad (8)$$

Therefore, if the spatial-mode perturbation satisfies the condition

$$C_{+1,+1}=C_{-1,-1}, \quad (9)$$

the final polarization-encoded qubit will be identical to the initial one, except for a global phase and amplitude, and the communication fidelity will be preserved (in this simple analysis, we did not consider the radial modes; see Methods for a complete theory).

In particular, every beam transformation that is mirror-symmetric with respect to a plane containing the initial beam axis will be symmetrical in the sign of OAM and hence will satisfy equation (9). For example, beam parallel displacements, tilts, elliptical deformations, or aperturings with a circular iris (even if off centre) or a half-plane mask (knife-edge), all have this symmetry. An axial misalignment, that is, a misalignment around an axis other than the optical one, between the transmitting and receiving communication units is equivalent to a beam translation and/or tilt, with both contained in the same plane, and can be treated analogously. Only symmetry-breaking combinations of two or more of the above effects may affect the fidelity. For example, a beam tilt combined with a beam displacement along a different plane will break the mirror symmetry and hence might introduce some degree of qubit alteration. (See Supplementary Methods for an explicit analysis of these beam-misalignment perturbations.[42]) Also, the main optical effects arising from atmospheric turbulence, such as beam wandering and spreading are mirror-symmetric, so that the extent of qubit alteration is expected to be much less significant in our communication scheme than in the case of pure OAM communication.

Another important class of transformations that satisfies equation (9) is that mathematically defined by pure multiplicative factors acting on the optical field, for example, the transformations arising from crossing any arbitrary inhomogeneous medium that is thin as compared with the Rayleigh length. It is easy to verify that these will be described by coefficients $C_{m,m'}$ that depend on the difference $m-m'$ and on the absolute values $|m|$ and $|m'|$, so that equation (9) is automatically satisfied. Weak turbulence, introducing only pure phase wavefront distortions, falls within this class of transformations and is therefore predicted to leave the qubit fidelity intact[37]. If we now consider the fact that light propagation in homogeneous media leaves the various OAM components constant, we conclude that equation (9) is satisfied even if the turbulent medium is followed and/or preceded by a long-distance free-space propagation, as in the case of earth to satellite (and *vice versa*) communication through the atmosphere.

Experimental tests of rotational-invariant qubit robustness. As a first test, we considered transmission through two types of transverse apertures: a half-plane movable obstruction (knife) covering a variable fraction of the transverse mode, and an iris (or pinhole) with variable radius. We have measured the state transmission fidelity F for different input states, at both aligned and 45°-rotated measurement stages, with respect to the transmitting unit, and for an increasing disturbance due to the obstruction. The experimental set-up used for this test is illustrated in Fig. 4a. We encoded different polarization qubits using two wave plates and mapped them into the hybrid encoding using a q-plate. For the purpose of comparison, we also switched to a pure-OAM encoding by inserting a fixed linear polarizer after the q-plate, so as to erase the polarization content of the qubit. Then, the photon was sent through the obstruction and to the receiving unit, and the communication fidelity was measured as a function of the obstruction transmittance, by varying the aperture of the pinhole or the transverse position of the knife. Thus, the

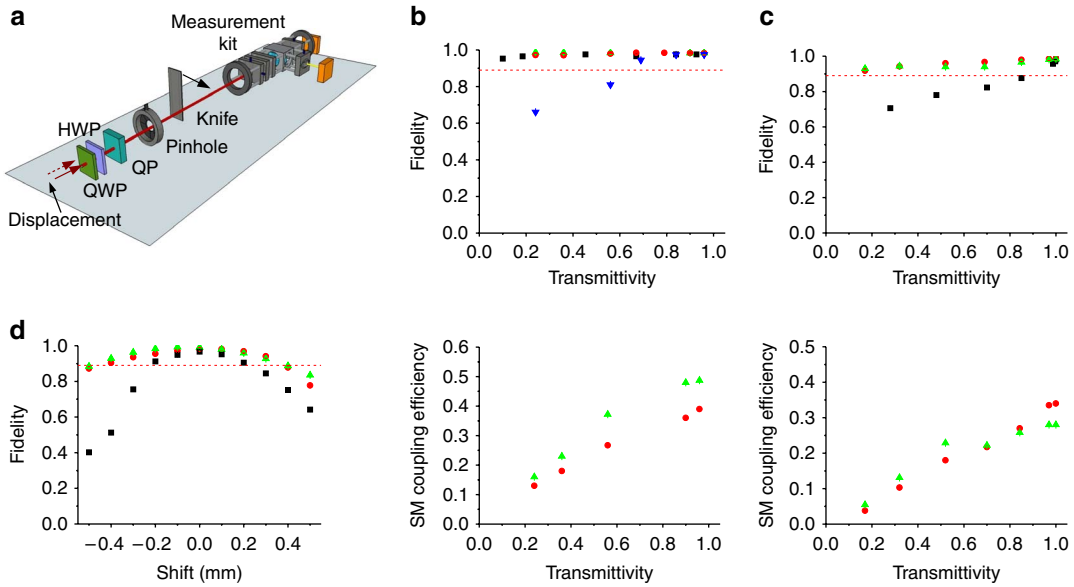

Figure 4 | Experimental results for rotational-invariant qubit robustness. (**a**) Experimental set-up adopted for the tests on the resistance of the rotational invariant hybrid photonic qubits to spatial-mode perturbations. In the schematics, we reported both the circular aperture (pinhole) and the half-plane obstruction (a movable knife-edge) that can alter the transmission of the qubits. Displaced beam is represented by a dashed red arrow. QP, *q*-plate; HWP, half-wave plate; QWP, quarter-wave plate. (**b**, **c**) Experimental resistance of rotational invariant hybrid qubits to beam perturbations, compared with the case of pure OAM qubits. Panel (**b**) refers to the case of circular aperture. Average fidelity of pure OAM qubits (black squares), hybrid qubits for a measurement stage rotated at an angle $\theta = 0°$ (green triangles) and at an angle $\theta = 45°$ (red circles) with respect to the transmitting unit. The blue triangles refer to the pure OAM qubits case, when the circular aperture is displaced off the beam axis by 5% of the beam waist (the hybrid qubit behaviour in the latter case was essentially indistinguishable from the centred aperture case). The transmission efficiency is determined by single-mode (SM) fibre-coupling efficiency after a circular aperture of varying radius, in the case of hybrid qubits only. Panel (**c**) refers to half-plane aperture. Average fidelities for hybrid qubits at $\theta = 0°$ (green triangles) and $\theta = 45°$ (red circles). Black squares are the corresponding results for pure OAM qubits. SM coupling efficiency after a movable half-plane aperture. (**d**) Experimental resistance of hybrid qubits (green triangles represent the case $\theta = 0°$ and red circles $\theta = 45°$) to a beam displacement, compared with the case of pure OAM encoding (black squares). In all panels, the red dashed line delineates the QKD security treshold. The beam waist in our experiment is $w_0 = (1.0 \pm 0.1)$mm. Uncertainties are smaller than the symbols.

lowest transmittivity corresponds to a tiny aperture of the pinhole (0.2 times the beam size), or to the almost complete coverage of the beam. All reported experimental fidelities were obtained by averaging over the six eigenstates of three mutually unbiased bases, therefore providing a good representative of the average fidelity over any input qubit state. The experimental results are reported in Fig. 4b,c. It is seen that the average fidelity of hybrid qubits is independent both of the transmittivity of the aperture and of the rotation angle of the measurement kit, with a global average of $F = (98 \pm 1)\%$ for the case of iris and $F = (96 \pm 1)\%$ for the knife. Moreover, in the former case the fidelity is not affected by the displacement of the pinhole off the beam axis. For comparison, we tested the resistance of qubits encoded only in the two-dimensional OAM subspace $o_1 = \{|+1\rangle, |-1\rangle\}$, that is, the same subspace used for the hybrid encoding. In this case, the fidelity remains high ($F = (97 \pm 1)\%$) only when the cylindrical symmetry of the modes is not perturbed, as for the centred iris, although for all other cases (non-centred iris or knife), the fidelity drops rapidly with decreasing transmission.

As a second test, we performed a communication run while changing the angle of the measurement kit without reoptimizing the alignment of the single-mode fibre. This corresponds to introducing small uncontrolled tilt and displacements in the beam during the measurement. We found that the system preserves a good QC fidelity (that is, above the security threshold) for rotations up to 30°. Above this angle, it was necessary to slightly readjust the single-mode fibre alignment to restore a high fidelity.

Finally, we tested the communication fidelity dependence on a controlled beam displacement, for two fixed angles of the measurement stage. Fig. 4d shows the behaviour of the average communication fidelity as a function of the beam displacement. The hybrid-qubit fidelity decreases with the displacement, but much slower than that of pure OAM encoding (see also the Supplementary Discussion).

Discussion

QC has a fundamental role in the modern view of quantum physics and opens the possibility of a variety of technological applications. Uncontrolled reference-frame misalignments limit QC, as they turn the transmitted quantum messages into noisy, classical ones. Here we report the development of a robust and compact toolbox for the efficient encoding and decoding of quantum information into single-photon states that are invariant under arbitrary rotations around the optical axis. With this, all concerns on relative axis-orientation during quantum transmissions reduce simply to the basic requirement of establishing an optical link.

Rotational invariance is achieved by exploiting decoherence-free subspaces spanned by hybrid polarization-OAM-entangled states. We experimentally showed the efficacy of these states through the feasibility demonstration of a cryptographic-key distribution protocol, distribution of entanglement, and violation of a Bell inequality, all in alignment-free settings. Importantly, as far as cryptographic security is concerned, our scheme does not introduce loopholes other than those already present in any photonic experiment with conventional encodings. We also emphasize that, even though the states used are themselves invariant only under rotations about the propagation axis, the scheme resists misalignments around other directions too. This is due to a filtering mechanism intrinsic to our universal-decoder set-up, which maps errors originating from beam

rotations around axes other than the optical link, as well as other spatial perturbations, into signal losses instead of infidelity.

Recently, interesting alignment-free approaches for QKD[43] and to extract non-local correlations[44–46] have been put forward. These, however, require that the relative axis orientations, though unknown, stay approximately static throughout the quantum data exchange session (see Supplementary Discussion for details). Remarkably, in contrast, our rotational-invariance protection works even if the relative orientations vary arbitrarily from measurement to measurement. Moreover, another important feature of the present scheme is that it does not restrict to non-locality and QKD but enables also fully general QC protocols, all misalignment-immune[18]. These include, for instance, quantum teleportation, dense coding, and entanglement swapping, the main ingredient of quantum repeaters.

Finally, our scheme should find applications in the forthcoming experiments on long-distance satellite-based QC[3–6]. There, apart from misalignments, other issues may impose serious obstacles too, such as precise satellite laser-tracking, collection efficiencies, or finite-size effects (for QKD). However, immunity against arbitrarily varying transverse relative orientations not only solves for misalignments but also relaxes requirements on the repetition rates needed to overcome finite-size effects (see Supplementary Discussion).

Methods

Experimental apparatus. The input photon pairs are generated via spontaneous parametric fluorescence in a β-barium borate (BBO) crystal cut for type-II phase matching, pumped by the second harmonic of a Ti:sapphire mode-locked laser beam with a 76-MHz repetition rate. The generated photons have wavelength $\lambda = 795$ nm and spectral bandwidth $\Delta\lambda = 3$ nm, as determined by two interference filters. The spatial and temporal walk-off is compensated by inserting a $\lambda/2$ wave plate and a 0.75-mm thick BBO crystal on each output mode[47]. The detected coincidence rate of the source is 8 kHz. The photons are delivered to the set-up via single-mode fibres, to define their transverse spatial mode to a pure TEM_{00}, corresponding to OAM $m = 0$. After the fibre output, two wave plates compensate the polarization rotation introduced by the fibre. The polarization-encoded photonic states are transformed into rotationally invariant hybrid states by q-plates with topological charge $q = 1/2$. The average conversion efficiency of all the q-plates employed in the experiment has been optimized to $(94 \pm 2)\%$ by controlling the electric field applied to the device[48,49]. For the analysis of experimental data, we referred to the coincidence counts between detectors $[D_{A1}, D_{B1}]$ and $[D_{A2}, D_{B2}]$ shown in Fig. 2, collected by a coincidence circuit with a gate of 3 ns. Typical coincidence rates were 30 Hz for the CHSH experiment and 300 Hz for the BB84 one.

Theory of q-plate encoding/decoding with radial modes. To fully describe the optical action of the q-plate, we need to consider both the azimuthal quantum number m, corresponding to the OAM eigenvalue in units of $\hbar$, and a radial quantum number p. These two numbers can be defined, for example, as in the case of Laguerre-Gauss beams, although this is not the only possible choice and our treatment is general in this respect. We denote with $|P, m, p\rangle$ the photon quantum state, including the spatial mode defined by m and p and the polarization state P (for example, L, R, H or V). The q-plate transformation laws are as follows:

$$\begin{aligned} |L,m,p\rangle &\rightarrow \sum_{p'} Q_{|m|,|m+1|;p,p'} |R,m+1,p'\rangle \\ |R,m,p\rangle &\rightarrow \sum_{p'} Q_{|m|,|m-1|;p,p'} |L,m-1,p'\rangle \end{aligned} \tag{10}$$

where $Q_{m,m';p,p'}$ are coefficients that do not depend on the sign of m and m', owing to the mirror symmetry of the q-plate pattern. These coefficients can be also given explicit analytical expressions in a given radial basis (for example, the Laguerre-Gauss one), but these expressions are not needed for our purposes here. Let us now consider a generic input polarization-encoded qubit photon in a Gaussian mode TEM_{00} ($m = 0$, $p = 0$):

$$|\psi\rangle_{\mathrm{P}} = \alpha |R,0,0\rangle + \beta |L,0,0\rangle. \tag{11}$$

After the q-plate, this photon is converted into the following rotation-invariant hybrid state (corresponding to the logical qubit):

$$|\psi\rangle_{\mathrm{L}} = \sum_{p} Q_{0,1;0,p} \left(\alpha |L,-1,p\rangle + \beta |R,+1,p\rangle\right). \tag{12}$$

This generalizes the transformation (3), by including also the radial modes. In free-space propagation, the different spatial modes will acquire Gouy phase factors $G_{|m|,p}$ that depend only on the absolute value of m (see, for example, ref. 30). The final decoding procedure is based on a second q-plate followed by a spatial filtering into an output TEM_{00} mode (that is, $m = 0$, $p = 0$; but the output radial basis need not be the same as the input one, as a different beam radius can be defined). This spatial filtering can, for example, be implemented by coupling into a single-mode fibre. This leads to the output polarization-encoded state $|\psi'\rangle_P = \eta |\psi\rangle_P$, where

$$\eta = \sum_{p,p'} Q_{0,1;0,p} G_{1,p} Q_{1,0;p',0}. \tag{13}$$

Therefore $|\eta|^2$ gives the quantum efficiency of the encoding/decoding process. After decoding, this output state is ready for detection or for further quantum processing.

Effect of spatial-mode perturbations during propagation. Let us now consider the action of generic spatial-mode perturbation acting on the photons during propagation, as defined by the following transformation laws:

$$|P,m,p\rangle \rightarrow \sum_{p',m'} C_{m,m';p,p'} |P,m',p'\rangle \tag{14}$$

where $C_{m,m';p,p'}$ are suitable complex-valued coefficients (when ignoring the radial modes, they correspond to the $C_{m,m'}$ coefficients used in equation (6)). We assume here that the perturbation does not affect the polarization state. The Gouy phase factors describing free-space propagation can be included in (14) without loss of generality. Let us now consider the effect of the perturbation (14) on the encoded qubit (12), which is transformed into the following state:

$$\begin{aligned} |\psi'\rangle_{\mathrm{L}} = \sum_{p,m,p'} Q_{0,1;0,p} \Big(&\alpha C_{-1,m;p,p'} |L,m,p'\rangle \\ &+ \beta C_{+1,m;p,p'} |R,m,p'\rangle\Big). \end{aligned} \tag{15}$$

Next, we apply again to this perturbed state, the transformations used in the decoding unit (q-plate and TEM_{00} filtering), obtaining the following final state

$$\begin{aligned} |\psi'\rangle_{\mathrm{P}} = &\sum_{p,p'} Q_{0,1;0,p} Q_{1,0;p',0} \\ &\times \left(\alpha C_{-1,-1;p,p'} |R,0,0\rangle + \beta C_{+1,+1;p,p'} |L,0,0\rangle\right). \end{aligned} \tag{16}$$

The latter equation shows that the qubit state will be unaffected, except for a global amplitude and phase factor, if and only if the following equality holds true:

$$C_{-1,-1;p,p'} = C_{+1,+1;p,p'}, \tag{17}$$

for all values of the radial indices p, p', thus generalizing equation (9). In other words, any spatial-mode perturbation that satisfies equation (17) will not alter the qubit transmission fidelity, although it may affect the transmission efficiency by increasing the photon losses. Explicit examples of spatial transformations arising in typical beam misalignment effects, such as beam translations and/or tilting, are considered in the Supplementary Methods.

References

1. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74,** 145–195 (2002).
2. Ursin, R. *et al.* Entanglement-based quantum communication over 144 km. *Nat. Phys.* **3,** 481–486 (2007).
3. Rarity, J. G., Tapster, P. R., Gorman, P. M. & Knight, P. Ground to satellite secure key exchange using quantum cryptography. *New J. Phys.* **4,** 82 (2002).
4. Aspelmeyer, M. *et al.* Long-distance free-space distribution of quantum entanglement. *Science* **301,** 621–623 (2003).
5. Villoresi, P. *et al.* Experimental verification of the feasibility of a quantum channel between Space and Earth. *New J. Phys.* **10,** 033038 (2008).
6. Bonato, C., Tomaello, A., Da Deppo, V., Naletto, G. & Villoresi, P. Feasibility of satellite quantum key distribution. *New J. Phys.* **11,** 045017 (2009).
7. Peres, A. & Scudo, P. F. Entangled quantum states as direction indicators. *Phys. Rev. Lett.* **86,** 4160–4162 (2001).
8. Bartlett, S. D., Rudolph, T. & Spekkens, R. W. Reference frames, superselection rules, and quantum information. *Rev. Mod. Phys.* **79,** 555–609 (2007).
9. Cabello, A. Bell's theorem without inequalities and without alignments. *Phys. Rev. Lett.* **91,** 230403 (2003).
10. Walton, Z. D., Abouraddy, A. F., Sergienko, A. V., Saleh, B. E. A. & Teich, M. C. Decoherence-free subspaces in quantum key distribution. *Phys. Rev. Lett.* **91,** 087901 (2003).

11. Boileau, J. C., Gottesman, D., Laflamme, R., Poulin, D. & Spekkens, R. W. Robust polarization-based quantum key distribution over a collective-noise channel. *Phys. Rev. Lett.* **92,** 017901 (2004).
12. Bourennane, M. *et al.* Decoherence-free quantum information processing with four-photon entangled states. *Phys. Rev. Lett.* **92,** 107901 (2004).
13. Chen, T.- Y. *et al.* Experimental quantum communication without a shared reference frame. *Phys. Rev. Lett.* 96, 150504 (2006).
14. Palma, G. M., Suominen, K. A. & Ekert, A. K. Quantum Computers and Dissipation. *Proc. R. Soc. Lond. Ser. A* **452,** 567–584 (1996).
15. Barenco, A. *et al.* Stabilisation of Quantum Computers by Symmetrisation. *SIAM J. Comp.* **26,** 1541–1557 (1997).
16. Zanardi, P. & Rasetti, M. Noiseless Quantum Codes. *Phys. Rev. Lett.* **79,** 3306–3309 (1997).
17. Lidar, D. A., Chuang, I. L. & Whaley, K. B. Decoherence-Free Subspaces for Quantum Computation. *Phys. Rev. Lett.* **81,** 2594–2597 (1998).
18. Aolita, L. & Walborn, S. P. Quantum communication without alignment using multiple-qubit single-photon states. *Phys. Rev. Lett.* **98,** 100501 (2007).
19. Molina-Terriza, G., Torres, J. P. & Torner, L. Twisted photons. *Nat. Phys.* **3,** 305–310 (2008).
20. Franke-Arnold, S., Allen, L. & Padgett, M. Advances in optical angular momentum. *Laser & Photon. Rev.* **2,** 299–313 (2008).
21. Stütz, M., Gröblacher, S., Jennewein, T. & Zeilinger, A. How to create and detect N-dimensional entangled photons with an active phase hologram. *Appl. Phys. Lett.* **90,** 261114 (2007).
22. Marrucci, L. *et al.* Spin-to-orbital conversion of the angular momentum of light and its classical and quantum applications. *J. Optics* **13,** 064001 (2011).
23. Marrucci, L., Manzo, C. & Paparo, D. Optical spin-to-orbital angular momentum conversion in inhomogeneous anisotropic media. *Phys. Rev. Lett.* **96,** 163905 (2006).
24. Slussarenko, S. *et al.* Tunable liquid crystal q-plates with arbitrary topological charge. *Opt. Express* **19,** 4085–4090 (2011).
25. Souza, C. E. R. *et al.* Quantum key distribution without a shared reference frame. *Phys. Rev. A* **77,** 032345 (2008).
26. Bennett, C. H. & Brassard, G. Quantum cryptography: Public-key distribution and coin tossing. in *Proceedings of the International Conference on Computer Systems and Signal Processing, Bangalore, India* 175 (IEEE, New York, 1984).
27. Clauser, J. F., Horne, M. A., Shimony, A. & Holt, R. A. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.* **23,** 880–884 (1969).
28. Holleczek, A., Aiello, A., Gabriel, C., Marquardt, C. & Leuchs, G. Classical and quantum properties of cylindrically polarized states of light. *Opt. Express* **19,** 9714–9736 (2011).
29. Nagali, E. *et al.* Quantum information transfer from spin to orbital angular momentum of photons. *Phys. Rev. Lett.* **103,** 013601 (2009).
30. Nagali, E. *et al.* Polarization control of single photon quantum orbital angular momentum states. *Opt. Express* **17,** 18745–18759 (2009).
31. Nagali, E. *et al.* Optimal quantum cloning of orbital angular momentum photon qubits via hong-ou-mandel coalescence. *Nat. Photon.* **3,** 720–723 (2009).
32. Nagali, E. *et al.* Experimental generation and characterization of single-photon hybrid ququarts based on polarization and orbital angular momentum encoding. *Phys. Rev. A* **81,** 052317 (2010).
33. Nagali, E. *et al.* Experimental optimal cloning of four-dimensional quantum states of photons. *Phys. Rev. Lett.* **105,** 73602 (2010).
34. Scarani, V. *et al.* The security of practical quantum key distribution. *Rev. Mod. Phys.* **81,** 1301–1350 (2009).
35. Shor, P. W. & Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **85,** 441–444 (2000).
36. Gottesman, D., Lo, H.- K., Lütkenhaus, N. & Preskill, J. Security of quantum key distribution with imperfect devices. *Quant Inf. Comput.* **5,** 325–360 (2004).
37. Paterson, C. Atmospheric turbulence and orbital angular momentum of single photons for optical communication. *Phys. Rev. Lett.* **94,** 153901 (2005).
38. Giovannini, D., Nagali, E., Marrucci, L. & Sciarrino, F. Resilience of orbital-angular-momentum photonic qubits and effects on hybrid entanglement. *Phys. Rev. A* **83,** 042338 (2011).
39. Djordjevic, I. B. Deep-space and near-earth optical communications by coded orbital angular momentum (OAM) modulation. *Opt. Express* **19,** 14277–14289 (2011).
40. Zhao, S. M., Leach, J., Gong, L. Y., Ding, J. & Zheng, B. Y. Aberration corrections for free-space optical communications in atmosphere turbulence using orbital angular momentum states. *Opt. Express* **20,** 452–461 (2012).
41. Pors, B.- J., Monken, C. H., Eliel, E. R. & Woerdman, J. P. Transport of orbital-angular-momentum entanglement through a turbulent atmosphere *Opt. Express* **19,** 6671–6683 (2011).
42. Vasnetsov, M. V., Pasko, V. A. & Soskin, M. S. Analysis of orbital angular momentum of a misaligned optical beam. *New J. Phys.* **7,** 46 (2005).
43. Laing, A., Scarani, V., Rarity, J. G. & O'Brien, J. L. Reference-frame-independent quantum key distribution. *Phys. Rev. A* **82,** 012304 (2010).
44. Liang, Y.- C., Harrigan, N., Bartlett, S. & Rudolph, T. Nonclassical correlations from randomly chosen local measurements. *Phys. Rev. Lett.* **104,** 050401 (2011).
45. Wallman, J. J. & Bartlett, S. D. Observers can always generate nonlocal correlations without aligning measurements by covering all their bases. *Phys. Rev. A* **85,** 024101 (2012).
46. Shadbolt, P. *et al.* Guaranteed violation of a Bell inequality without aligned reference frames or calibrated devices. Preprint at http://arxiv.org/abs/1111.1853 (2011).
47. Kwiat, P. G. *et al.* New high-intensity source of polarization-entangled photon pairs. *Phys. Rev. Lett.* **75,** 4337–4341 (1995).
48. Piccirillo, B., D'Ambrosio, V., Slussarenko, S., Marrucci, L. & Santamato, E. Photon spin-to-orbital angular momentum conversion via an electrically tunable q-plate. *Appl. Phys. Lett.* **97,** 241104 (2010).
49. D'Ambrosio, V. *et al.* Deterministic qubit transfer between orbital and spin angular momentum of single photons. *Opt. Lett.* **37,** 172–174 (2012).

Acknowledgements

This work was supported by the FET-Open Program, within the 7th Framework Programme of the European Commission under Grant No. 255914, PHORBITECH, FIRB-Futuro in Ricerca (HYTEQ), the Brazilian funding agencies FAPERJ, CNPq and the INCT-Informação Quântica, and the Spanish Juan de la Cierva foundation.

Author contributions

V.D., E.N., L.A., S.W., L.M. and F.S. jointly conceived the misalignment-free scheme, the underlying theory, the experimental layout and methodology. S.S. and L.M. fabricated the *q*-plates. V.D., E.N. and F.S. performed the experiments. All authors discussed the results and participated in the manuscript preparation.

Additional information

Supplementary information accompanies this paper at http://www.nature.com/naturecommunications

Competing financial interests: The authors declare no competing financial interests.

Reprints and permission information is available online at http://npg.nature.com/reprintsandpermissions/

How to cite this article: D'Ambrosio, V. *et al.* Complete experimental toolbox for alignment-free quantum communication. *Nat. Commun.* 3:961 doi: 10.1038/ncomms1951 (2012).

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).

SCIENTIFIC REPORTS

OPEN

SUBJECT AREAS:
QUANTUM PHYSICS
QUANTUM OPTICS
GENERAL PHYSICS
NANOPHOTONICS

Received
22 May 2012

Accepted
12 June 2012

Published
25 June 2012

Correspondence and requests for materials should be addressed to N.B. (n.brunner@bristol.ac.uk)

Guaranteed violation of a Bell inequality without aligned reference frames or calibrated devices

Peter Shadbolt[1], Tamás Vértesi[2], Yeong-Cherng Liang[3], Cyril Branciard[4], Nicolas Brunner[5] & Jeremy L. O'Brien[6]

[1]Centre for Quantum Photonics, H. H. Wills Physics Laboratory & Department of Electrical and Electronic Engineering, University of Bristol, Merchant Venturers Building, Woodland Road, Bristol, BS8 1UB, United Kingdom, [2]Institute of Nuclear Research of the Hungarian Academy of Sciences, H-4001 Debrecen, P.O. Box 51, Hungary, [3]Group of Applied Physics, University of Geneva, CH-1211 Geneva 4, Switzerland, [4]School of Mathematics and Physics, The University of Queensland, St Lucia, QLD 4072, Australia, [5]H.H. Wills Physics Laboratory, University of Bristol, Tyndall Avenue, Bristol, BS8 1TL, United Kingdom, [6]Centre for Quantum Photonics, H. H. Wills Physics Laboratory & Department of Electrical and Electronic Engineering, University of Bristol, Merchant Venturers Building, Woodland Road, Bristol, BS8 1UB, UK.

Bell tests — the experimental demonstration of a Bell inequality violation — are central to understanding the foundations of quantum mechanics, and are a powerful diagnostic tool for the development of quantum technologies. To date, Bell tests have relied on careful calibration of measurement devices and alignment of a shared reference frame between two parties — both technically demanding tasks. We show that neither of these operations are necessary, violating Bell inequalities (i) with certainty using unaligned, but calibrated, measurement devices, and (ii) with near-certainty using uncalibrated and unaligned devices. We demonstrate generic quantum nonlocality with randomly chosen measurements on a singlet state of two photons, implemented using a reconfigurable integrated optical waveguide circuit. The observed results demonstrate the robustness of our schemes to imperfections and statistical noise. This approach is likely to have important applications both in fundamental science and quantum technologies, including device-independent quantum key distribution.

Nonlocality is arguably among the most striking aspects of quantum mechanics, defying our intuition about space and time in a dramatic way[1]. Although this feature was initially regarded as evidence of the incompleteness of the theory[2], there is today overwhelming experimental evidence that nature is indeed nonlocal[3]. Moreover, nonlocality plays a central role in quantum information science, where it proves to be a powerful resource, allowing, for instance, for the reduction of communication complexity[4] and for device-independent information processing[5–8].

In a quantum Bell test, two (or more) parties perform local measurements on an entangled quantum state, Fig. 1(a). After accumulating enough data, both parties can compute their joint statistics and assess the presence of nonlocality by checking for the violation of a Bell inequality. Although entanglement is necessary for obtaining nonlocality it is not sufficient. First, there exist some mixed entangled states that can provably not violate any Bell inequality since they admit a local model[9,10]. Second, even for sufficiently entangled states, one needs judiciously chosen measurement settings[11]. Thus although nonlocality reveals the presence of entanglement in a device-independent way, that is, irrespectively of the detailed functioning of the measurement devices, one generally considers carefully calibrated and aligned measuring devices in order to obtain a Bell inequality violation. This in general amounts to having the distant parties share a common reference frame and well calibrated devices.

Although this assumption is typically made implicitly in theoretical works, establishing a common reference frame, as well as aligning and calibrating measurement devices in experimental situations are never trivial issues. For instance, in the context of quantum communications via optical fibres, unavoidable small temperature changes induce strong rotations of the polarisation of photons in the fibre. This makes it challenging to maintain a good alignment, which in turn severely hinders the performance of quantum communication protocols in optical fibres[12]. Also, in the field of satellite based quantum communications[13,14], the alignment of a reference frame represents a key issue given the fast motion of the satellite and the short amount of time available for completing the protocol—in certain cases there simply might not be enough time to align a reference frame.

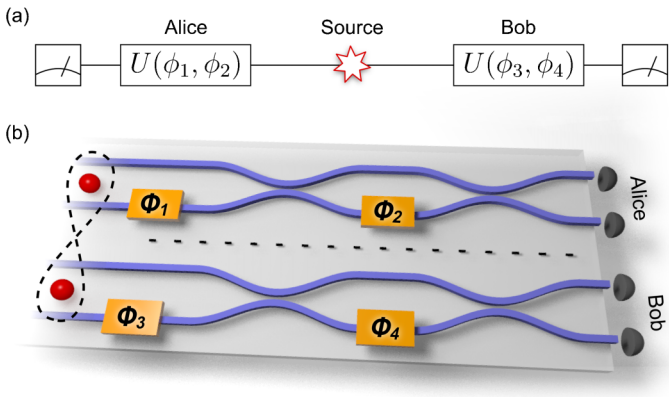

Figure 1 | Bell violations with random measurements. (a) Schematic representation of a Bell test. (b) Schematic of the integrated waveguide chip used to implement the new schemes described here. Alice and Bob's measurement circuits consist of waveguides to encode photonic qubits, directional couplers that implement Hadamard-like operations, thermal phase shifters to implement arbitrary measurements, and detectors.

Finally, in integrated optical waveguide chips, the calibration of phase shifters is a cumbersome and time-consuming operation. As the complexity of such devices is increased, this calibration procedure will become increasingly challenging.

It is therefore an interesting and important question whether the requirements of having a shared reference frame and calibrated devices can be dispensed with in nonlocality tests. It was recently shown[15] that, for Bell tests performed in the absence of a shared reference frame, i.e., using randomly chosen measurement settings, the probability of obtaining quantum nonlocality can be significant. For instance, considering the simple Clauser-Horne-Shimony-Holt (CHSH) scenario[16], randomly chosen measurements on the singlet state lead to a violation of the CHSH inequality with probability of $\sim$ 28%; moreover this probability can be increased to $\sim$ 42% by considering mutually unbiased measurement bases. The generalisation of these results to the multipartite case were considered in Refs. [15, 17], as well as schemes based on decoherence-free subspaces[18]. Although these works demonstrate that nonlocality can be a relatively common feature of entangled quantum states and random measurements, it is of fundamental interest and practical importance to establish whether Bell inequality violation can be ubiquitous.

Here we demonstrate that nonlocality is in fact a far more generic feature than previously thought, violating CHSH inequalities without a shared frame of reference, and even with uncalibrated devices, with near-certainty. We first show that whenever two parties perform three mutually unbiased (but randomly chosen) measurements on a maximally entangled qubit pair, they obtain a Bell inequality violation with certainty—a scheme that requires no common reference frame between the parties, but only a local calibration of each measuring device. We further show that when all measurements are chosen at random (*i.e.*, calibration of the devices is not necessary anymore), although Bell violation is not obtained with certainty, the probability of obtaining nonlocality rapidly increases towards one as the number of different local measurements increases. We perform these random measurements on the singlet state of two photons using a reconfigurable integrated waveguide circuit, based on voltage-controlled phase shifters. The data confirm the near-unit probability of violating an inequality as well as the robustness of the scheme to experimental imperfections—in particular the non-unit visibility of the entangled state—and statistical uncertainty. These new schemes exhibit a surprising robustness of the observation of nonlocality that is likely to find important applications in diagnostics of quantum devices (*e.g.* removing the need to calibrate the reconfigurable circuits used here) and quantum information protocols, including device-independent quantum key distribution[5] and other protocols based on quantum nonlocality[6–8] and quantum steering[19].

Results

Bell test using random measurement triads. Two distant parties, Alice and Bob, share a Bell state. Here we will focus on the singlet state

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B\right), \tag{1}$$

though all our results can be adapted to hold for any two-qubit maximally entangled state. Let us consider a Bell scenario in which each party can perform 3 possible qubit measurements labelled by the Bloch vectors $\vec{a}_x$ and $\vec{b}_y$ ($x, y = 1, 2, 3$), and where each measurement gives outcomes ± 1. After sufficiently many runs of the experiment, the average value of the product of the measurement outcomes, i.e. the correlators $E_{xy} = -\vec{a}_x \cdot \vec{b}_y$, can be estimated from the experimental data. In this scenario, it is known that all local measurement statistics must satisfy the CHSH inequalities:

$$CHSH = \left|E_{xy} + E_{xy'} + E_{x'y} - E_{x'y'}\right| \leq 2, \tag{2}$$

and their equivalent forms where the negative sign is permuted to the other terms and for different pairs x, x' and y, y'; there are, in total, 36 such inequalities.

Interestingly, it turns out that whenever the measurement settings are mutually unbiased, i.e. $\vec{a}_x \cdot \vec{a}_{x'} = \delta_{x,x'}$ and $\vec{b}_y \cdot \vec{b}_{y'} = \delta_{y,y'}$ (orthogonal measurement triads, from now on simply referred to as measurement triads), then at least one of the above CHSH inequalities *must be violated* — except for the case where the measurement triads are perfectly aligned, i.e. for each x, there is a y such that $\vec{a}_x = \pm \vec{b}_y$. Therefore, a generic random choice of unbiased measurement settings — where the probability that Alice and Bob's settings are perfectly aligned is zero (for instance if they share no common reference frame) — will *always* lead to the violation of a CHSH inequality.

Proof. Assume that $\{\vec{a}_x\}$ and $\{\vec{b}_y\}$ are orthonormal bases. Since the correlators of the singlet state have the simple scalar product form $E_{xy} = -\vec{a}_x \cdot \vec{b}_y$, the matrix

$$\varepsilon = \begin{pmatrix} E_{11} & E_{12} & E_{13} \\ E_{21} & E_{22} & E_{23} \\ E_{31} & E_{32} & E_{33} \end{pmatrix} \tag{3}$$

contains (in each column) the coordinates of the three vectors $-\vec{b}_y$, written in the basis $\{\vec{a}_x\}$.

By possibly permuting rows and/or columns, and by possibly changing their signs (which corresponds to relabelling Alice and Bob's settings and outcomes), we can assume, without loss of generality, that $E_{11}, E_{22} > 0$ and that $E_{33} > 0$ is the largest element (in absolute value) in the matrix $\mathcal{E}$. Noting that $\vec{b}_3 = \pm \vec{b}_1 \times \vec{b}_2$ and therefore $|E_{33}| = |E_{11}E_{22} - E_{12}E_{21}|$, these assumptions actually imply $E_{33} = E_{11}E_{22} - E_{12}E_{21} \geq E_{11}, E_{22}, |E_{12}|, |E_{21}|$ and $E_{12}E_{21} \leq 0$; we will assume that $E_{12} \leq 0$ and $E_{21} \geq 0$ (one can multiply both the $x = 2$ row and the $y = 2$ column by -1 if this is not the case).

With these assumptions, $(E_{11} + E_{21})\max[-E_{12}, E_{22}] \geq E_{11}E_{22} - E_{12}E_{21} = E_{33} \geq \max[-E_{12}, E_{22}]$, and by dividing by $\max[-E_{12}, E_{22}] > 0$, we get $E_{11} + E_{21} \geq 1$. One can show in a similar way that $-E_{12} + E_{22} \geq 1$. Adding these last two inequalities, we obtain

$$E_{11} + E_{21} - E_{12} + E_{22} \geq 2. \tag{4}$$

Since $\mathcal{E}$ is an orthogonal matrix, one can check that equality is obtained above (which requires that both $E_{11} + E_{21} = 1$ and $-E_{12} + E_{22} = 1$) if and only if $\vec{a}_1 = \vec{b}_1$, $\vec{a}_2 = \vec{b}_2$ and

$\vec{a}_3 = \vec{b}_3$. (See Supplementary Information for details) Therefore, if the two sets of mutually unbiased measurement settings $\{\vec{a}_x\}$ and $\{\vec{b}_y\}$ are not aligned, then inequality (4) is strict: a CHSH inequality is violated. Numerical evidence suggests that the above construction always gives the largest CHSH violation obtainable from the correlations (3).

While the above result shows that a random choice of measurement triads will lead to nonlocality with certainty, we still need to know how these CHSH violations are distributed; that is, whether the typical violations will be rather small or large. This is crucial especially for experimental implementations, since in practise, various sources of imperfections will reduce the strength of the observed correlations. Here we consider two main sources of imperfections: limited visibility of the entangled state, and finite statistics.

First, the preparation of a pure singlet state is impossible experimentally due to noise. In the experiment described here, limited visibility mainly originates from imperfect operation of the photon source and detectors. It is thus desirable to understand the effect of such experimental noise, which can be modelled by a Werner state with limited visibility V:

$$|\Psi^-\rangle \rightarrow \rho_V = V|\Psi^-\rangle\langle\Psi^-| + (1-V)\frac{1}{4}. \qquad (5)$$

This, in turn, results in the decrease of the strength of correlations by a factor V. In particular, when $V \leq 1/\sqrt{2}$, the state (5) ceases to violate the CHSH inequality. States ρ_V are known as Werner states[9].

Second, in any experiment the correlations are estimated from a finite set of data, resulting in an experimental uncertainty. To take into account this finite-size effect, we will consider a shifted classical bound $\mathcal{L} \geq 2$ of the CHSH expression (2) such that an observed correlation is only considered to give a conclusive demonstration of nonlocality if CHSH $> \mathcal{L}$. Thus, if the CHSH value is estimated experimentally up to a precision of δ, then considering a shifted classical bound of $\mathcal{L} = 2 + \delta$ ensures that only statistically significant Bell violations are considered.

We have estimated numerically the distribution of the CHSH violations (the maximum of the left-hand-side of (2) over all x, x', y, y') for uniformly random measurement triads on the singlet state (see Fig. 2). Interestingly, typical violations are quite large; the average CHSH value is ~ 2.6, while only $\sim 0.3\%$ of the violations are below 2.2. Thus this phenomenon of generic nonlocality is very robust against the effect of finite statistics and of limited visibility, even in the case where both are combined. For instance, even after raising the cutoff to $\mathcal{L} = 2.1$ and decreasing the singlet visibility to $V = 0.9$, our numerical simulation shows that the probability of violation is still greater than 98.2% (see Fig 2).

Bell tests using completely random measurements. Although performing unbiased measurements does not require the spatially separated parties to share a common reference frame, it still requires each party to have good control of the local measurement device. Clearly, local alignment errors (that is, if the measurements are not exactly unbiased) will reduce the probability of obtaining nonlocality. In practise the difficulty of correctly aligning the local measurement settings depends on the type of encoding that is used. For instance, using the polarisation of photons, it is rather simple to generate locally a measurement triad, using wave-plates. However, for other types of encoding, generating unbiased measurements might be much more complicated (see experimental part below).

This leads us to investigate next the case where all measurement directions $\{\vec{a}_x, \vec{b}_y\}$ are chosen randomly and independently. For simplicity, we will focus here on the case where all measurements are chosen according to a uniform distribution on the Bloch sphere. Although this represents a particular choice of distribution, we believe that most random distributions that will naturally arise in an experiment will lead to qualitatively similar results, as indicated by our experimental results.

We thus now consider a Bell test in which Alice and Bob share a singlet, and each party can use m possible measurement settings, all chosen randomly and uniformly on the Bloch sphere. We estimated numerically the probability of getting a Bell violation as a function of the visibility V [of the state (5)] for $m = 2,\ldots,8$; see Fig. 2. Note that for $m \geq 4$, additional Bell inequalities appear[20]; we have checked however, that ignoring these inequalities and considering only CHSH leads to the same results up to a very good approximation. Fig. 2 clearly shows that the chance of finding a nonlocal correlation

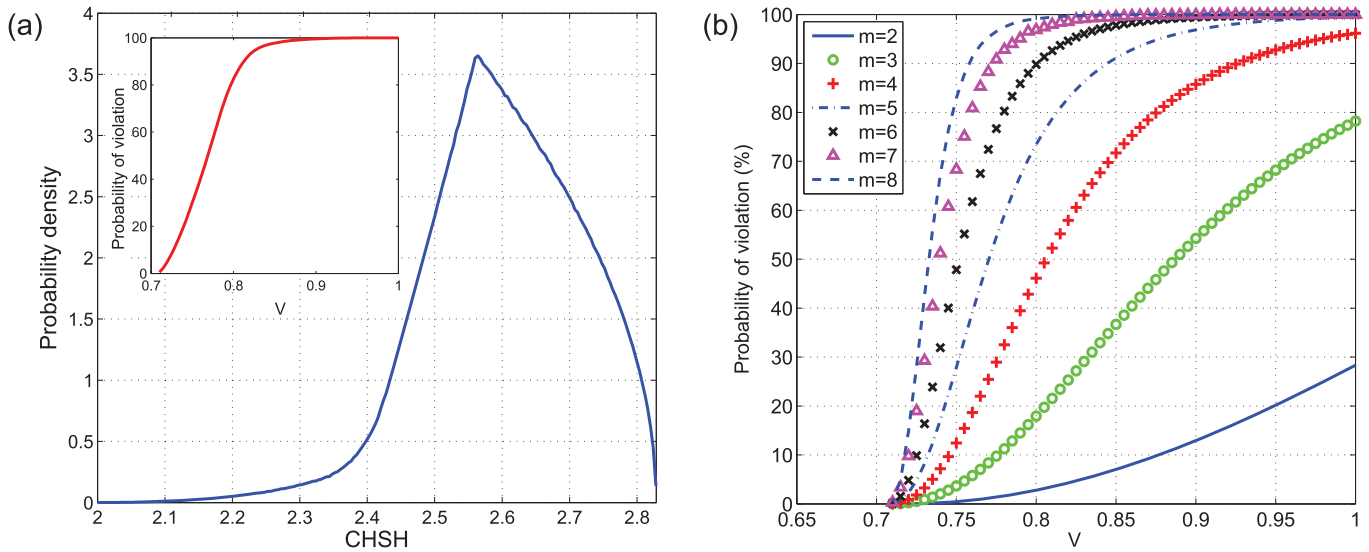

Figure 2 | (a) Bell tests using random measurement triads (theory). Distribution of the (maximum) CHSH violations for uniformly random measurement triads on a singlet state. The inset shows the probability of obtaining a CHSH violation as a function of the visibility V of the Werner state; this probability is obtained by integrating the distribution of CHSH violations (main graph) over the interval $[2/V, 2\sqrt{2}]$. (b) **Bell tests using completely random measurements (theory).** Plot of the probability of Bell violation as a function of the visibility V of the Werner state, for different numbers m of (completely random) measurements per party.

rapidly increases with the number of settings m. Intuitively, this is because when choosing an increasing number of measurements at random, the probability that at least one set of four measurements (2 for Alice and 2 for Bob) violates the CHSH inequality increases rapidly. For example, with $m = 3$ settings, this probability is 78.2% but with $m = 4$, it is already 96.2%, and for $m = 5$ it becomes 99.5%. Also, as with the case of unbiased measurements, the probability of violation turns out to be highly robust against depolarising noise; for instance, for $V = 0.9$ and $m \geq 5$, there is still at least 96.9% chance of finding a subset $\left\{\vec{a}_x, \vec{a}_{x'}, \vec{b}_y, \vec{b}_{y'}\right\}$ among our randomly chosen measurements that gives nonlocal correlations.

Measurement devices. We use the device shown in Fig. 1(b) to implement Alice and Bob's random measurements on an entangled state of two photons. This device is a reconfigurable quantum photonic chip, in which qubits are encoded using path or dual-rail encoding[25]. The path encoded singlet state is generated from two unentangled photons using an integrated waveguide implementation[21,22] of a nondeterministic CNOT gate[23], an architecture which also enables deliberate introduction of mixture. This state is then shared between Alice and Bob who each have a Mach-Zehnder (MZ) interferometer, consisting of two directional couplers (equivalent to beamsplitters) and variable phase shifters ($\phi_{1,2}$ and $\phi_{3,4}$) and single photon detectors. This enables Alice and Bob to independently make a projective measurement in any basis by setting their phase shifters to the required values[24,25]. The first phase-shifters ($\phi_{1,3}$) implement rotations around the Z axis of the Bloch sphere ($R_Z(\phi) = e^{-i\phi\sigma_Z/2}$); since each directional coupler implements a Hadamard-like operation ($H' = e^{i\pi/2}e^{-i\pi\sigma_Z/4}He^{-i\pi\sigma_Z/4}$, where H is the usual Hadamard gate), the second phase shifters ($\phi_{2,4}$) implement rotations around the Y axis ($R_Y(\phi) = e^{-i\phi\sigma_Y/2}$). Overall, each MZ interferometer implements the unitary transformation $U(\phi_{1,3}, \phi_{2,4}) = R_Y(\phi_{2,4})R_Z(\phi_{1,3})$, which enables projective measurement in any qubit basis when combined with a final measurement in the logical (Z) basis using avalanche photodiode single photon detectors (APDs).

Each thermal phase shifter is implemented as a resistive element, lithographically patterned onto the surface of the waveguide cladding. Applying a voltage v to the heater has the effect of locally heating the waveguide, thereby inducing a small change in refractive index n ($dn/dT \approx 1 \times 10^{-5}K$) which manifests as a phase shift in the MZ interferometer. There is a nonlinear relationship between the voltage applied and the resulting phase shift $\phi(v)$, which is generally well approximated by a quadratic relation of the form

$$\phi(v) = \alpha + \beta v^2. \tag{6}$$

In general, each heater must be characterised individually — a procedure which is both cumbersome and timeconsuming. The function $\phi(v)$ is estimated by measuring single-photon interference fringes from each heater. The parameter α can take any value between 0 and 2π depending on the fabrication of the heater, while typically $\beta \sim 0.15\frac{\text{rad}}{V^2}$ [24,25]. For any desired phase, the correct voltage can then be determined.

In the experiments described here, heater calibration is necessary both for state tomography, and for implementing random measurement triads. In contrast, this calibration can be dispensed with entirely when implementing completely random measurements. Thus, in this case we simply choose random voltages from a uniform distribution, in the range [0V, 7V], which is adequate to address phases in the range $0 \leq \phi \leq 2\pi$—*i.e.* no a priori calibration of Alice and Bob's devices is necessary. Clearly this represents a significant advantage for our device.

Experimental violations with random measurement triads. We first investigate the situation in which Alice and Bob both use 3 orthogonal measurements. We generate randomly chosen measurement triads using a pseudo-random number generator. Having calibrated the phase/voltage relationship of the phase shifters, we then apply the corresponding voltages on the chip. For each pair of measurement settings, the two-photon coincidence counts between all 4 combinations of APDs ($C_{00}, C_{01}, C_{10}, C_{11}$) are then measured for a fixed amount of time—the typical rate of simultaneous photon detection coincidences is $\sim$ 1 kHz. From these data we compute

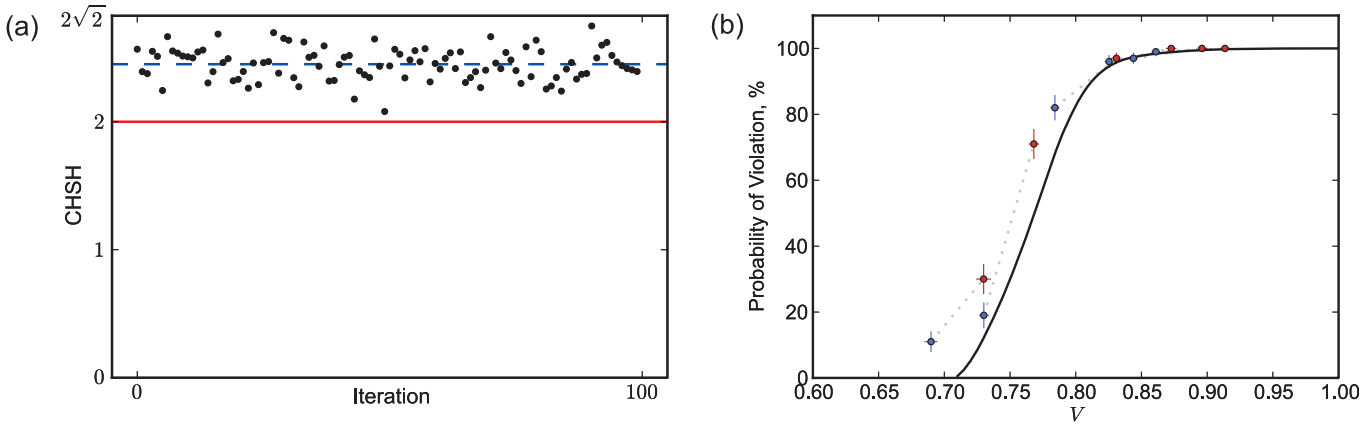

Figure 3 | Bell tests requiring no shared reference frame. Here we perform Bell tests on a two-qubit Bell state, using randomly chosen measurement triads. Thus our experiment requires effectively no common reference frame between Alice and Bob. (a) 100 successive Bell tests; in each iteration, both Alice and Bob use a randomly-chosen measurement triad. For each iteration, the maximal CHSH value is plotted (black points). In all iterations, we get a CHSH violation; the red line indicates the local bound (CHSH=2). The smallest CHSH value is $\sim$ 2.1, while the mean CHSH value (dashed line) is $\sim$ 2.45. This leads to an estimate of the visibility of $V = \frac{2.45}{2.6} \simeq 0.942$, to be compared with 0.913 ± 0.004 obtained by maximum likelihood quantum state tomography[28]. (See Supplementary Information for further discussion of this slight discrepancy.) Error bars, which are too small to draw, were estimated using a Monte Carlo technique, assuming Poissonian photon statistics. (b) The experiment of (a) is repeated for Bell states with reduced visibility, illustrating the robustness of the scheme. Each point shows the probability of CHSH violation estimated using 100 trials. Uncertainty in probability is estimated as the standard error. Visibility for each point is estimated by maximum-likelihood quantum state tomography, where the error bar is calculated using a Monte Carlo approach, again assuming Poissonian statistics. Red points show data corrected for accidental coincidences (see Methods), the corresponding uncorrected data is shown in blue. The black line shows the theoretical curve from Fig. 2 (inset). Further discussion of the slight discrepancy between experimental and theoretical probabilities of CHSH violation is provided in the Supplementary Information.

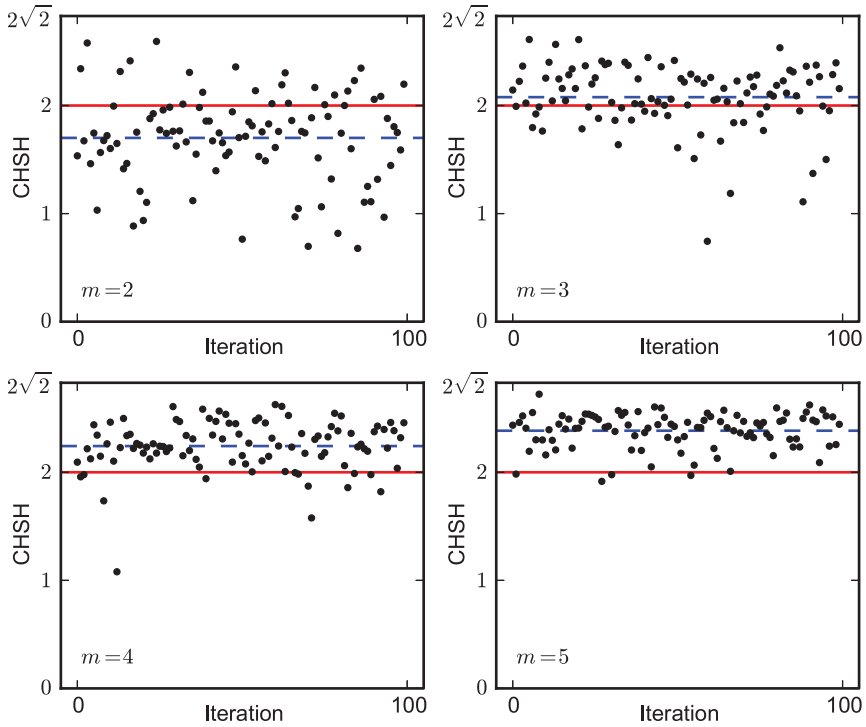

Figure 4 | Experimental Bell tests using uncalibrated devices. We perform Bell tests on a two-qubit Bell state, using uncalibrated measurement interferometers, that is, using randomly-chosen voltages. For $m = 2, 3, 4, 5$ local measurement settings, we perform 100 trials (for each value of m). As the number of measurement settings m increases, the probability of obtaining a Bell violation rapidly approaches one. For $m \geq 3$, the average CHSH value (dashed line) is above the local bound of CHSH=2 (red line). Error bars, which are too small to draw, were estimated by a Monte Carlo technique, assuming Poissonian statistics. Data has been corrected for accidentals (see Methods).

the maximal CHSH value as detailed above. This entire procedure is then repeated 100 times. The results are presented in Fig. 3a, where accidental coincidences, arising primarily from photons originating from different down-conversion events, which are measured throughout the experiment, have been subtracted from the data (the raw data, as well as more details on accidental events, can be found in the Methods). Remarkably, all 100 trials lead to a clear CHSH violation; the average CHSH value we observe is $\sim$ 2.45, while the smallest measured value is $\sim$ 2.10.

We next investigate the effect of decreasing the visibility of the singlet state: By deliberately introducing a temporal delay between the two photons arriving at the CNOT gate, we can increase the degree of distinguishability between the two photons. Since the photonic CNOT circuit relies on quantum interference[26] a finite degree of distinguishability between the photons results in this circuit implementing an incoherent mixture of the CNOT operation and the identity operation[27]. By gradually increasing the delay we can create states ρ_V with decreasing visibilities. For each case, the protocol described above is repeated, which allows us to estimate the average CHSH value (over 100 trials). For each case we also estimate the visibility via maximum likelihood quantum state tomography. Figure 3b clearly demonstrates the robustness of our scheme, in good agreement with theoretical predictions: a considerable amount of mixture must be introduced in order to significantly reduce the probability of obtaining a CHSH violation.

Together these results show that large Bell violations can be obtained without a shared reference frame even in the presence of considerable mixture.

Experimental violations with completely random measurements. We now investigate the case where all measurements are chosen at random. The procedure is similar to the first experiment, but we now apply voltages chosen randomly from a uniform distribution, and independently for each measurement setting. Thus our experiment requires no calibration of the measurement MZ interferometers (*i.e.* the characterisation of the phase-voltage relation), which is generally a cumbersome task. By increasing the number of measurements performed by each party (m = 2, 3, 4, 5), we obtain CHSH violations with a rapidly increasing probability, see Fig. 4. For m = 5, we find 95 out of 100 trials lead to a CHSH violation. The visibility V of the state used for this experiment was measured using state tomography to be 0.869 $\pm$ 0.003, clearly demonstrating that robust

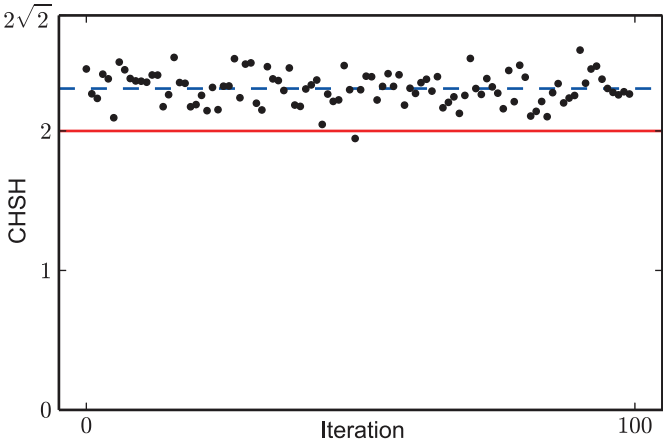

Figure 5 | Raw data of experimental Bell tests requiring no shared reference frame. This figure shows the raw data, without correcting for accidental coincidences, of Fig. 4a. Here the average CHSH value is 2.30 (dashed line), leading to an estimate of the visibility of $V = \frac{2.3}{2.6} \simeq 0.885$, while the estimate from quantum state tomography is $V = 0.861 \pm 0.003$ (see Supplementary Information). Error bars, which are too small to draw, were estimated using a Monte-Carlo technique, assuming Poissonian photon statistics.

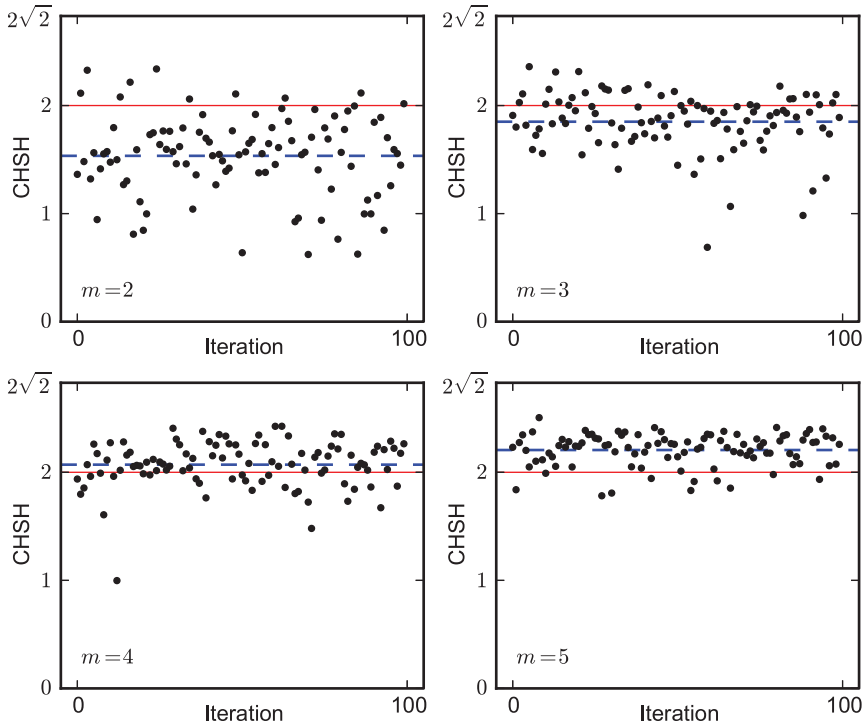

Figure 6 | Raw data of experimental Bell tests using uncalibrated measurement interferometers (random voltages). This figure shows the raw data, without correcting for accidental coincidences, of Fig. 5. Error bars, which are too small to draw, are estimated by a Monte Carlo technique, assuming Poissonian statistics. The visibility V of the state used for this experiment was measured using state tomography to be 0.804 ± 0.003.

violation of Bell inequalities is possible for completely random measurements.

It is interesting to note that the relation between the phase and the applied voltage is typically quadratic, see Eq. (6). Thus, by choosing voltages from a uniform distribution, the corresponding phase distribution is clearly biased. Our experimental results indicate that this bias has only a minor effect on the probability of obtaining nonlocality.

Discussion

Bell tests provide one of the most important paths to gaining insight into the fundamental nature of quantum physics. The fact that they can be robustly realised without the need for a shared reference frame or calibrated devices promises to provide new fundamental insight. In the future it would be interesting to investigate these ideas in the context of other Bell tests, for instance considering other entangled states or in the multipartite situation (see[29] for recent progress in this direction), as well as in the context of quantum reference frames[30,31].

The ability to violate Bell inequalities with a completely uncalibrated device, as was demonstrated here, has important application for the technological development of quantum information science and technology: Bell violations provide an unambiguous signature of quantum operation and the ability to perform such diagnostics without the need to first perform cumbersome calibration of devices should enable a significant saving in all physical platforms. These ideas could be particularly helpful for the characterisation of entanglement sources without the need for calibrated and aligned measurement devices. They could also be relevant to quantum communications experiments based on optical fibres or earth-satellite links, in which the alignment of a reference frame is cumbersome.

Finally Bell violations underpin many quantum information protocols, and therefore, the ability to realise them with dramatically simplified device requirements holds considerable promise for simplifying the protocols themselves. For example, device-independent quantum key distribution[5] allows two parties to exchange a cryptographic key and, by checking for the violation of a Bell inequality, to guarantee its security without having a detailed knowledge of the devices used in the protocol. Such schemes, however, do typically require precise control of the apparatus in order to obtain a sufficiently large violation. In other words, although a Bell inequality violation is an assessment of entanglement that is device-independent, one usually needs carefully calibrated devices to obtain such a violation. The ability to violate Bell inequalities without these requirements could dramatically simplify these communication tasks. The implementation of protocols based on quantum steering[19] may also be simplified by removing calibration requirements.

Note added. While completing this manuscript, we became aware of an independent proof of our theoretical result on Bell tests with randomly chosen measurement triads, obtained by Wallman and Bartlett[29], after one of us mentioned numerical evidence of this result to them.

Methods

Photon counting and accidentals. In our experiments, we postselect on successful operation of the linear-optical CNOT gate by counting coincidence events, that is, by measuring the rate of coincidental detection of photon pairs. Single photons are first detected using silicon avalanche photodiodes (APDs). Coincidences are then counted using a Field-Programmable Gate Array (FPGA) with a time window of ~ 5 ns. We refer to these coincidence events as $\{t_0^A, t_0^B\}$.

Accidental coincidences have two main contributions: first, from photons originating from different down-conversion events arriving at the detectors within the time window; second, due to dark counts in the detectors. Here we directly measure the (dynamic) rate of accidental coincidences in real time, for the full duration of all the experiments described here. To do so, for each pair of detectors we measure a second coincidence count rate, namely $\{t_0^A, t_1^B\}$, with $|t_1 - t_0| = 30$ ns. In order to do this, we first split (duplicate) the electrical TTL pulse from each detector into two BNC cables. An electrical delay of 30 ns is introduced into one channel, and coincidences (i.e. at $\{t_0^A, t_1^B\}$) are then counted directly. Finally we obtain the corrected coincidence counts by subtracting coincidence counts at $\{t_0^A, t_1^B\}$ from the raw coincidence counts at $\{t_0^A, t_0^B\}$.

All experimental results presented in the main text have been corrected for accidentals. Here we provide the raw data. Fig. 5 presents the raw data for Fig. 3(a) while Fig. 6 presents the raw data for Fig. 4. Notably, in Fig. 5, corresponding to the case of randomly chosen triads, all but one of the hundred trials feature a CHSH violation. The average violation is now ~ 2.3.

1. Bell, J. S. On the Einstein Podolsky Rosen paradox. *Physics (Long Island City, N.Y.)* **1**, 195200 (1964).
2. Einstein, A., Podolsky, B. & Rosen, N. Can quantum–mechanical description of reality be considered complete? *Phys. Rev.* **47**, 777–780 (1935).
3. Aspect, A. Bell's inequality test: more ideal than ever. *Nature* **398**, 189190 (1999).
4. Buhrman, H., Cleve, R., Massar, S. & Wolf, R. Nonlocality and communication complexity. *Rev. Mod. Phys.* **82**, 665 (2010).
5. Acín, A. *et al.* Device–independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.* **98**, 230501 (2007).
6. Pironio, S. *et al.* Random numbers certified by Bells theorem. *Nature* **464**, 1021 (2010).
7. Colbeck, R. & Kent, A. Private randomness expansion with untrusted devices. *J. Phys. A* **44**, 095305 (2011).
8. Rabelo, R., Ho, M., Cavalcanti, D., Brunner, N. & Scarani, V. Device–independent certification of entangled measurements. *Phys. Rev. Lett.* **107**, 050502 (2011).
9. Werner, R. F. Quantum states with Einstein–Podolsky–Rosen correlations admitting a hidden–variable model. *Phys. Rev. A* **40**, 4277 (1989).
10. Barrett, J. Nonsequential positive-operator-valued measurements on entangled mixed states do not always violate a Bell inequality. *Phys. Rev. A* **65**, 042302 (2002).
11. Liang, Y.–C. & Doherty, A. Bounds on Quantum Correlations in Bell Inequality Experiments. *Phys. Rev. A* **75**, 042103 (2007).
12. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145195 (2002).
13. Ursin, R. *et al.* Space–QUEST: Experiments with quantum entanglement in space. *IAC Proceedings* A2.1.3 (2008).
14. Laing, A., Scarani, V., Rarity, J. G. & O'Brien, J. L. Reference frame independent quantum key distribution. *Phys. Rev. A* **82**, 012304 (2010).
15. Liang, Y.–C., Harrigan, N., Bartlett, S. D., & Rudolph, T. G. Nonclassical Correlations from Randomly Chosen Local Measurements. *Phys. Rev. Lett.* **104**, 050401 (2010).
16. Clauser, J. F., Horne, M. A., Shimony, A. & Holt, R. A. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.* **23**, 880884 (1969).
17. Wallman, J. J., Liang, Y.–C. & Bartlett, S. D. Generating nonclassical correlations without fully aligning measurements. *Phys. Rev. A* **83**, 022110 (2011).
18. Cabello, A. Bell's Theorem without Inequalities and without Alignments. *Phys. Rev. Lett.* **91**, 230403 (2003).
19. Branciard, C., Cavalcanti, E. G., Walborn, S. P., Scarani, V. & Wiseman, H. M. One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering. *Phys. Rev. A* **85**, 010301(R) (2012).
20. Gisin, N. Bell inequalities: many questions, a few answers. arXiv:quant–ph/0702021.
21. Politi, A., Cryan, M. J., Rarity, J. G., Yu, S. & O'Brien, J. L. Silica-on-silicon waveguide quantum circuits. *Science* **320**, 646649 (2008).
22. Politi, A., Matthews, J. C. F. & O'Brien, J. L. Shor's quantum factoring algorithm on a photonic chip. *Science* **325**, 1221 (2009).
23. O'Brien, J. L. *et al.* Demonstration of an all-optical quantum controlled-NOT gate. *Nature* **426**, 264267 (2003).
24. Shadbolt, P. J. *et al.* Generating, manipulating and measuring entanglement and mixture with a reconfigurable photonic circuit. *Nature Photon.* **6**, 4549 (2012).
25. Matthews, J. C. F., Politi, A., Stefanov, A. & O'Brien, J. L. Manipulation of multiphoton entanglement in waveguide quantum circuits. *Nature Photon.* **3**, 346350 (2009).
26. Hong, C. K., Ou, Z. Y. & Mandel, L. Measurement of subpicosecond time intervals between two photons by interference. *Phys. Rev. Lett.* **59**, 20442046 (1987).
27. O'Brien, J. L. *et al.* Quantum process tomography of a controlled-not gate. *Phys. Rev. Lett.* **93**, 080502 (2004).
28. James, D. F. V., Kwiat, P. G., Munro, W. J. & White, A. G. *Phys. Rev. A* **64**, 052312 (2001).
29. Wallman, J. J. & Bartlett, S. D. Observers can always generate nonlocal correlations without aligning measurements by covering all their bases. *Phys. Rev. A* **85**, 024101 (2012).
30. Bartlett, S. D, Rudolph, T. & Spekkens, R.W. Reference frames, superselection rules, and quantum information. *Rev. Mod. Phys.* **79**, 555 (2007).
31. Costa, F., Harrigan, N., Rudolph, T. & Brukner, Č. *New J. Phys.* **11**, 123007 (2009).

Acknowledgements

We acknowledge useful discussions with Jonathan Allcock, Nicolas Gisin and Joel Wallman. We acknowledge financial support from the UK EPSRC, ERC, QUANTIP, the EU DIPIQ, PHORBITECH, Nokia, NSQI, the Hungarian National Research Fund OTKA (PD101461), the Swiss NCCR "Quantum Photonics", and the European ERC-AG QORE. J.L.O'B. acknowledges a Royal Society Wolfson Merit Award.

Author contributions

TV, YCL, CB and NB developed the theory. PS, NB and JO designed the experiments. PS performed the experiments and data analysis. All authors contributed to the preparation of the manuscript.

Additional information

Supplementary information accompanies this paper at http://www.nature.com/scientificreports

Competing financial interests: The authors declare no competing financial interests.

How to cite this article: Shadbolt, P. *et al.* Guaranteed violation of a Bell inequality without aligned reference frames or calibrated devices. *Sci. Rep.* **2**, 470; DOI:10.1038/srep00470 (2012).