RIVISTA DEL NUOVO CIMENTO Vol. 37, N. 5 2014
DOI 10.1393/ncr/i2014-10100-0

Quantum imaging technologies

M. Malik(1)(2)(*) and R. W. Boyd(1)(3)

(1) *The Institute of Optics, University of Rochester - Rochester, New York 14627, USA*
(2) *Institute for Quantum Optics and Quantum Information (IQOQI) Austrian Academy of Sciences - Boltzmanngasse 3, A-1090, Austria*
(3) *Department of Physics, University of Ottawa - Ottawa, ON K1N 6N5 Canada*

ricevuto il 7 Aprile 2014

Summary. — Over the past three decades, quantum mechanics has allowed the development of technologies that provide unconditionally secure communication. In parallel, the quantum nature of the transverse electromagnetic field has spawned the field of quantum imaging that encompasses technologies such as quantum lithography, quantum ghost imaging, and high-dimensional quantum key distribution (QKD). The emergence of such quantum technologies also highlights the need for the development of accurate and efficient methods of measuring and characterizing the elusive quantum state itself. In this paper, we describe new technologies that use the quantum properties of light for security. The first of these is a technique that extends the principles behind QKD to the field of imaging and optical ranging. By applying the polarization-based BB84 protocol to individual photons in an active imaging system, we obtained images that are secure against any intercept-resend jamming attacks. The second technology presented in this article is based on an extension of quantum ghost imaging, a technique that uses position-momentum entangled photons to create an image of an object without directly obtaining any spatial information from it. We used a holographic filtering technique to build a quantum ghost image identification system that uses a few pairs of photons to identify an object from a set of known objects. The third technology addressed in this document is a high-dimensional QKD system that uses orbital-angular-momentum (OAM) modes of light for encoding. Moving to a high-dimensional state space in QKD allows one to impress more information on each photon, as well as introduce higher levels of security. We discuss the development of two OAM-QKD protocols based on the BB84 and Ekert protocols of QKD. The fourth and final technology presented in this article is a relatively new technique called direct measurement that uses sequential weak and strong measurements to characterize a quantum state. We use this technique to characterize the quantum state of a photon with a dimensionality of $d = 27$, and measure its rotation in the natural basis of OAM.

PACS 01.30.Rr – Surveys and tutorial papers; resource letters.
PACS 42.50.Ex – Optical implementations of quantum information processing and transfer.
PACS 42.50.Tx – Optical angular momentum and its quantum aspects.
PACS 42.50.-p – Quantum optics.

(*) E-mail: mehul.malik@univie.ac.at

1. Key concepts

1˙1. *Introduction* – Here we introduce certain key concepts that are essential to understanding current research in quantum information and especially the experiments that are described in later sections. While the field of quantum mechanics (QM) is vast, there are certain ideas that underlie almost all quantum technologies today. For example, the quantum no-cloning theorem [1] states that one cannot create a perfect copy of an arbitrary single quantum state. This seemingly simple theorem has led to applications such as quantum cryptography [2], which offers encryption with unconditional security —a feat considered impossible with classical physics. Similarly, quantum entanglement, long considered one of the "spookier" concepts in quantum mechanics, has allowed the development of quantum technologies such as quantum lithography [3,4] —the ability to

Fig. 1. – A cartoon depicting the "Schrödinger's cat" thought experiment [6].

make measurements more sensitive and lithographic patterns finer than those allowed by classical physics.

While it is important to understand the formal theory behind these concepts, it is perhaps more important to gain intuition for what really is going on in quantum mechanics. The chief difficulty in understanding or explaining QM is that of language. Modern day English (or any other language) is steeped in the language of classical mechanics. This makes sense of course, as we experience the world through our five senses, which are essentially classical detectors. It would be absurd to describe the iconic apple that supposedly fell on Newton's head in terms of the apple's wave function. How do we, then, go about trying to explain the highly counterintuitive aspects of QM using our everyday Newtonian language?

In the beginning of book VII of Plato's *The Republic* [5], Socrates describes a cave whose inhabitants are chained and forced to look upon a wall since they were born, not knowing anything else. Behind them, a fire burns and casts shadows of objects moving in front of it upon the cave wall. These people, having been forced to gaze only at the wall, can see just these shadows, and not the objects themselves or the fire. Plato uses this allegory to describe the nature of the philosopher as a person who has been freed from these chains and can see the true nature of reality. One could argue that the quantum mechanical world is like Plato's cave. Limited by our classical senses, we can only see the "classical" shadows of the wave function. The quantum physicist then rises as the freed philosopher, empowered to see the "true nature" of reality!

The broad and fantastical imagery of Plato's cave allegory allows one to visualize the divide between the classical and quantum world using classical language. However, it is perhaps too broad to describe individual concepts in QM. In order to do that, one needs a metaphor for a quantum state itself. In 1935, Erwin Schrödinger proposed a thought experiment that has come to be called "Schrödinger's cat". In it, Schrödinger describes a cat that has been put in a box that contains a tiny amount of radioactive substance that has an equal probability of decaying and not decaying. If it decays, it sets off a geiger counter that triggers a hammer that breaks a vial of poison that kills the cat (see fig. 1). If the box is closed, the tiny amount of radioactive substance can be expressed for a certain instant in time as simultaneously being in a state of decay and not having decayed, putting the cat in a similar state of being alive and dead. On one hand, this thought experiment raises many deeper issues in QM such as the macroscopic limits of superposition and the role of the observer in collapsing the wave function. On

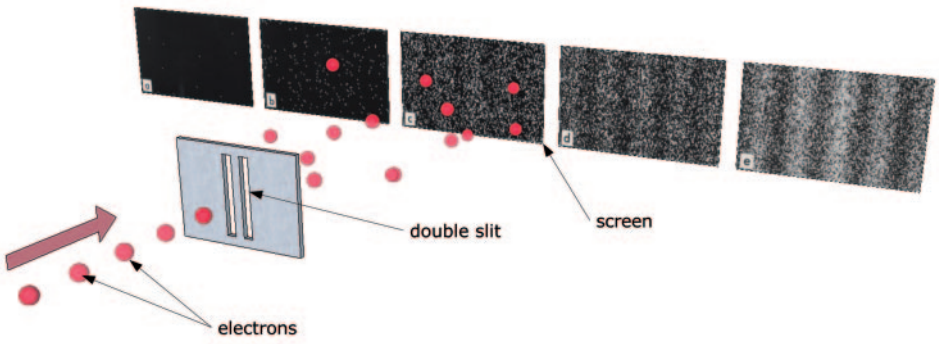

Fig. 2. – A schematic of Young's double-slit experiment performed with electrons. Plates (a)-(e) show the buildup of an interference pattern at the single electron level. Thus, each electron only interferes with itself.

the other hand, it is extremely useful for illustrating many fundamental concepts in QM using a simple, visual metaphor. Throughout this section, we will refer to Schrödinger's cat whenever possible in an effort to provide some intuition for the topic at hand.

1˙2. *Superposition and no-cloning.* – Schrödinger's cat is an archetypal metaphor for quantum superposition. In the language of quantum mechanics, the state of the cat is written as

$$|\text{cat}\rangle = \frac{1}{\sqrt{2}}\big[|\text{dead}\rangle + |\text{alive}\rangle\big]. \tag{1}$$

The act of opening the box constitutes a measurement, which *collapses* the wave function of the cat into one of the two states, dead or alive. Here we are using language associated with the Copenhagen interpretation of quantum mechanics, which describes reality in terms of probabilities associated with observations or measurements. While Schrödinger's cat lies in the domain of *gedankenexperiments*, realistic proposals have been made to put small living objects such as viruses into a quantum superposition [7]. Perhaps the simplest real world example of superposition is found in Young's famous double-slit experiment when applied to particles. Many electrons are fired one at a time through a set of narrow slits. The resulting pattern measured on a screen on the other side of the slits shows distinct peaks and valleys (fig. 2). Care is taken to ensure that only one electron is present in the setup at any given time. How, then, can each electron independently know where to land in order to create an interference pattern usually associated with waves?

The answer lies in interpreting each electron as being in a probabilistic mixture of going through both slits at the same time. To paraphrase Dirac, "each electron only interferes with itself". This experiment was the first to illustrate the principle of wave-particle duality, which states that all matter has a wavelength equal to h/p, where h is Planck's constant and p the momentum of any particle. Thus, one can see how particles with a very small mass (such as electrons) would have a measurable wavelength. The double-slit experiment has been performed with molecules as large as buckyballs (with a diameter of about 0.7 nm), steadily bringing the idea of quantum superposition into the macroscopic domain.

Current technology allows us to perform Young's double-slit experiment with light as originally intended, but at the single photon level. As expected, one sees the familiar buildup of interference fringes on an electron-multiplying CCD camera, one photon at a time (as seen for electrons in fig. 2). Besides being in a superposition of two slits or positions, photons can be easily put into many other types of superpositions. For this reason, they form the building blocks for many proof-of-principle experiments in quantum optics and quantum information. Perhaps the simplest quantum superposition of a photon is that of polarization, where the state of the photon is written as

$$|\psi\rangle = \frac{1}{\sqrt{2}}\big[a|H\rangle + b|V\rangle\big], \tag{2}$$

where $|H\rangle$ and $|V\rangle$ refer to the horizontal and vertical quantum states of polarization. The coefficients a and b are, in general, complex coefficients of probability known as probability amplitudes. This type of superposition state is known as a *qubit*, as it serves as a fundamental unit of quantum information. Just like a classical bit can have a value 0 or 1, a qubit can be in a superposition of 0 *and* 1. The modulus-squares of the probability amplitudes $|a|^2$ and $|b|^2$ dictate the probability of finding the photon in either state $|H\rangle$ or $|V\rangle$. The relative phase between a and b governs the phase relationship between the H and V components, which can be interpreted as a measure of the ellipticity of polarization. A diagonally or anti-diagonally polarized photon can be written as superposition of horizontally and vertically polarized states as

$$|D\rangle = \frac{1}{\sqrt{2}}\big[|H\rangle + |V\rangle\big], \tag{3}$$
$$|A\rangle = \frac{1}{\sqrt{2}}\big[|H\rangle - |V\rangle\big].$$

Thus, in this case, the coefficients a and b are unity, except for state $|A\rangle$, where the coefficient of $|V\rangle$ has a minus sign. The states $|D\rangle$ and $|A\rangle$ are "mutually unbiased" with respect to the $|H\rangle$ and $|V\rangle$ states, as measuring one of them in the H/V basis is equally likely to give an outcome of H and V. Throughout this article, we will deal with superpositions of other properties of a photon, such as its position, momentum, and orbital angular momentum.

The no-cloning theorem, postulated by Wootters and Zurek in 1982 [1], states that one cannot create a perfect copy of an arbitrary quantum state. When applied to our metaphor of Schrödinger's cat, this means that one cannot create a second "cat superposition" that is identical to the first, without opening the box and destroying the first superposition. In their simple proof, Wootters and Zurek used an example of a device that perfectly clones a polarization qubit. In order to do so, they assume the device can independently clone a $|H\rangle$ photon as well as a $|V\rangle$ photon. However, when an arbitrary superposition state such as that shown in eq. (2) is fed into this device, it creates a two-photon state that, in general, cannot be a replica of the original. Despite its simplicity, the ramifications of the quantum no-cloning theorem were huge. Just two years later, Bennett and Brassard applied this theorem to create the field of quantum cryptography [2]. If one cannot perfectly clone a quantum state, then why not use it to securely send information? In this manner, two parties using quantum states for communication could detect any tampering, as an eavesdropper could not create copies of their communication states without introducing some error in the protocol.

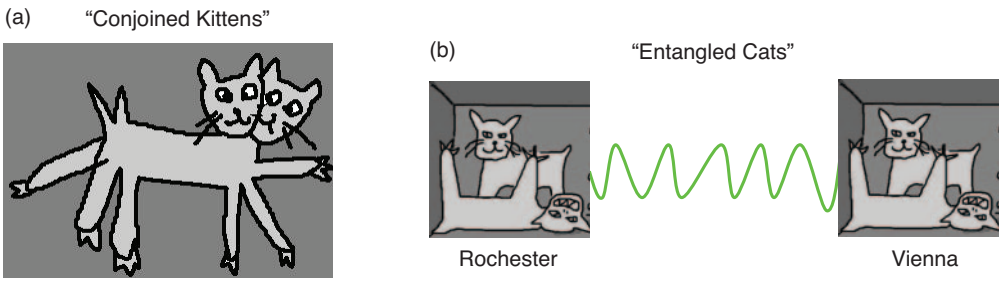

Fig. 3. – (a) A pair of conjoined kittens are separated by skilled veterinarians at birth and grow up to strangely feel each others pain. (b) When put into identical Schrödinger boxes, these cats constitute an entangled state. When one cat is measured to be alive, one knows immediately that the other cat is alive (and vice-versa), no matter how far apart they are.

1˙3. *Entanglement*. – Since it was first proposed in a seminal paper by Schrödinger in 1935 [8], the phenomenon of entanglement has captured the imaginations of physicists and philosophers alike, and has made itself manifest as one of the most counterintuitive aspects of quantum mechanics. We can use a variation of the Schrödinger's cat metaphor to illustrate the concept of entanglement. Imagine the freak occurrence of a birth of a pair of conjoined kittens (fig. 3(a)). These kittens are separated at birth by the finest veterinarians in the land. However, due to some unexplained unnatural phenomenon, the kittens grow up to share each others feelings and pain. Now, imagine putting both of these cats into identical Schrödinger boxes. One box is kept in Rochester, while the other is sent to Vienna (fig. 3(b)). If the Rochester box is opened and the cat is found to be alive, we know instantly that the cat in the Vienna box is also alive (and vice versa)! The state of the cats can be written as

$$|\text{cats}\rangle = \frac{1}{\sqrt{2}}\big[|\text{dead}\rangle_R|\text{dead}\rangle_V + |\text{alive}\rangle_R|\text{alive}\rangle_V\big]. \tag{4}$$

This state indicates the cats share a highly correlated, or entangled state. By measuring the state of one of the cats, one non-locally collapses the state of the other cat. It is crucial to point out that this non-local relationship is not causal, *i.e.*, one cannot kill the Vienna cat by shooting the Rochester cat. Only the different outcomes of measurement are perfectly correlated.

Of course, it is not realistic to imagine such a situation in real life. However, the phenomenon of entanglement is readily seen in the laboratory setting in the form of entangled photons. The strong correlations found in entangled photons have allowed great headway in experimental quantum mechanics, facilitating experiments ranging from the most fundamental to the very applied. Polarization-entangled photons have been used to obtain some of the most exacting experimental violations of Bell's inequality [9-11]. Time-energy entangled photons have found large application in various non-classical techniques such as quantum cryptography [12] and quantum teleportation [13]. The strong spatial correlations found in position-momentum entangled photons have given rise to the field of quantum imaging and have allowed the development of techniques such as quantum lithography [3, 14] and ghost imaging [15].

In direct analogy with the above entangled Schrödinger cats state, one can entangle

a pair of photons in their polarization to create the state

$$|\psi\rangle = \frac{1}{\sqrt{2}}\Big[|H\rangle_1|H\rangle_2 + e^{i\phi}|V\rangle_1|V\rangle_2\Big], \tag{5}$$

where ϕ is the phase between the H and V states. If one were to measure the polarization of one these photons to be horizontal, one would know immediately that the polarization of the other is horizontal, and vice versa. Interestingly, when $\phi = 0$ or some multiple of 2π, this state can be written in the diagonal-anti-diagonal (D/A) basis by substituting eqs. (3) into the above equation and simplifying to

$$|\psi\rangle = \frac{1}{\sqrt{2}}\Big[|D\rangle_1|D\rangle_2 + |A\rangle_1|A\rangle_2\Big]. \tag{6}$$

The correlations seen in H and V polarizations are perfectly preserved in the mutually unbiased basis of D and A polarization. This aspect of entanglement is crucial for distinguishing it from classically correlated states. Photons similarly entangled in position will retain these correlations when observed in the conjugate basis of momentum. However, in this case the correlations are opposite, *i.e.* position-entangled photons are anti-correlated in momentum. In the momentum representation, the state of position-momentum entangled photons is written as [16, 17]

$$|\psi\rangle = \int\int \mathrm{d}\mathbf{q}_1 \mathrm{d}\mathbf{q}_2 \Phi(\mathbf{q}_1, \mathbf{q}_2)|\mathbf{q}_1\rangle_1|\mathbf{q}_2\rangle_2, \tag{7}$$

where the vector $\mathbf{q}_i$ is the transverse component of the wave vector $\mathbf{k}_i$, and $|q_i\rangle$ represents the state of a single photon in momentum space (*i.e.* a plane wave mode). This definition uses the paraxial approximation $|\mathbf{q}| \ll |\mathbf{k}|$ and the normalized function $\Phi(\mathbf{q}_1, \mathbf{q}_2)$ is defined as

$$\Phi(\mathbf{q}_1, \mathbf{q}_2) = \frac{1}{\pi}\sqrt{\frac{2L}{K}}v(\mathbf{q}_1 + \mathbf{q}_2)\gamma(\mathbf{q}_1 - \mathbf{q}_2). \tag{8}$$

Here, $\gamma(\mathbf{q})$ is a phase-matching function and $\mathbf{v}(\mathbf{q})$ is the angular spectrum of the pump beam. For a pump beam with a narrow angular spectrum, this function is large only when the argument is zero, *i.e.* $\mathbf{q}_1 = -\mathbf{q}_2$. This describes a state strongly anti-correlated in momentum. The same state can be written in position space, which we do later in sect. **4**.

Another property of photons that can be entangled is their orbital angular momentum (OAM). While the topic of OAM is discussed in detail in the next section, it is worth mentioning some key points here. Just as momentum entanglement manifests as momentum anti-correlations, OAM entangled photons also exhibit OAM anti-correlations. The state of these photons is written as

$$|\psi\rangle = \sum_{\ell} c_\ell |\ell\rangle|-\ell\rangle. \tag{9}$$

As OAM exists in a discrete, infinite-dimensional space, the entangled state is written in a simpler form as a sum over all possible ℓ modes. The range of ℓ modes in an OAM-

entangled state usually depends on experimental considerations such as aperture sizes and the pump beam waist.

Entangled photons are readily produced via the process of spontaneous parametric down-conversion (SPDC). In this process, one photon conventionally known as the *pump* (p) is annihilated in a second-order ($\chi^{(2)}$) nonlinear crystal and two photons are created, known as the *signal* (s) and *idler* (i) photons. This process is governed by the conservation of energy and momentum, and the frequencies and wave vectors of the photons involved are related as follows:

$$\omega_p = \omega_s + \omega_i, \tag{10}$$

$$\mathbf{k}_p = \mathbf{k}_s + \mathbf{k}_i.$$

Entanglement will play a strong role in sects. **3** and **4**, where we utilize it for techniques such as quantum-secured surveillance and quantum ghost image identification.

1˙4. *Orbital Angular Momentum.* – It is well known that light carries both spin and orbital angular momentum (OAM). The spin angular momentum of light is associated with its circular polarization. Such circularly polarized light was shown to exert a torque on a suspended wave plate by Beth in 1936 [18]. In the language of quantum mechanics, each circularly polarized photon carries a spin angular momentum of $\hbar$. Subsequently, Allen *et al.* extended this idea to OAM and showed that light also carries an angular momentum of $\ell\hbar$, where ℓ is the azimuthal mode index of the Laguerre-Gaussian mode solution to the paraxial wave equation [19].

By making a paraxial approximation to the Helmholtz equation $(\Delta^2 + k^2)E(k) = 0$, we can write the paraxial wave equation

$$\left(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + 2ik\frac{\partial}{\partial z}\right)E(x, y, z) = 0. \tag{11}$$

This equation is satisfied by the cylindrically symmetric Laguerre-Gaussian modes, whose normalized amplitude is described as

$$\begin{aligned} LG_\ell^p(\rho, \theta, z) = {} & \sqrt{\frac{2p!}{\pi(|\ell| + p)!}}\frac{1}{w(z)}\left[\frac{\sqrt{2}\rho}{w(z)}\right]^{|\ell|} L_p^\ell\left[\frac{2\rho^2}{w^2(z)}\right] \\ & \times \exp\left[-\frac{\rho^2}{w^2(z)}\right]\exp\left[-\frac{ik^2\rho^2 z}{2(z^2 + z_R^2)}\right] \\ & \times \exp\left[i(2p + |\ell| + 1)\tan^{-1}\left(\frac{z}{z_R}\right)\right]e^{i\ell\theta}, \end{aligned} \tag{12}$$

where z_R is the Rayleigh range, $w(z)$ is the beam radius, k is the wave vector magnitude, and L_p^ℓ is the associated Laguerre polynomial. The quantities ℓ and p are the azimuthal and radial quantum numbers respectively. Allen *et al.* showed that each photon in such a Laguerre-Gaussian beam carries a well defined OAM of $\ell\hbar$ in vacuum.

The ramifications of the quantized nature of OAM modes are huge. Theoretically, OAM modes reside in a discrete, infinite-dimensional Hilbert space. The dimensionality of this space is only limited by the physical size of apertures. The quantum nature of the spin angular momentum, or polarization, has allowed the use of photons as carriers

of quantum information, or *qubits*. The ability to use the OAM of photons for encoding quantum information opens up the potential to encode vastly more amounts of information per photon. Further, it also provides increased security in quantum information protocols. These key points are discussed further in sect. **5**. Photons carrying more than two bits of quantum information are referred to as *qudits*, where d refers to the dimensionality of the Hilbert space.

In this article, we will focus on pure vortex modes, which are OAM modes with a spatially uniform amplitude. This allows for a simpler theoretical treatment, and lets one use the full aperture of the transmitter. Vortex modes can be written as

$$\Psi_\ell = A_0 W(r/R) \exp(i\ell\theta), \tag{13}$$

where A_0 is the spatially uniform field amplitude, $W(x)$ is an aperture function such that $W(x) = 1$ for $|x| \leq 1$ and zero otherwise, r and θ are the radial and azimuthal coordinates, and ℓ is the azimuthal quantum number. The radial quantum number p is zero in these modes. This allows us to isolate the azimuthal phase dependance for further study. The wavefronts of five vortex modes ($\ell = 0, \pm 1, \pm 2$) are shown in fig. 4. The helical nature of the phase fronts is apparent in this figure, and shows why they are referred to as *vortex* modes. Figure 4 also shows X-Y cross-sections of the phase profiles. These cross-sections clearly show how the phase winds ℓ times from 0 to 2π in the azimuthal direction for a mode with azimuthal quantum number ℓ. There is a phase singularity at the very center of these modes, which results in the intensity having a null at the center. This is the reason that these modes are sometimes referred to as "donut" modes. Throughout this article, a reference to an "OAM mode" implies a vortex mode as defined above.

As the set of OAM modes is complete and orthonormal, one can express any spatial mode with rotational symmetry in terms of its component OAM modes. Another set of orthonormal modes can be formed by taking a finite number of OAM modes $N = 2L + 1$ and adding them coherently according to the relationship

$$\Theta_n = \frac{1}{\sqrt{2L+1}} \sum_{\ell=-L}^{L} \Psi_\ell \exp\left(\frac{i2\pi n\ell}{2L+1}\right). \tag{14}$$

This second set modes is called the angular position, or ANG basis. These modes are so named because their intensity profile looks like an angular slice that moves around the center of the beam as one changes the relative phases of the component OAM modes. It is important to note that the number of ANG modes in the basis will be equal to the number of OAM modes used to form the basis. As an example, we show simulated intensity and phase for the set of five ANG modes composed of the OAM modes with $\ell = 0, \pm 1, \pm 2$ in fig. 5. These modes are given by the formula

$$\Theta_n = \frac{1}{\sqrt{5}} \sum_{\ell=-2}^{2} \Psi_\ell \exp\left(\frac{i2\pi n\ell}{5}\right), \tag{15}$$

which is simply a special case of eq. (14). As the set of ANG modes is composed of an equal superposition of OAM modes, they form a basis that is mutually unbiased (*i.e.* a MUB) with respect to the OAM basis. This point is important for application in quantum key distribution and will be discussed in the next section.

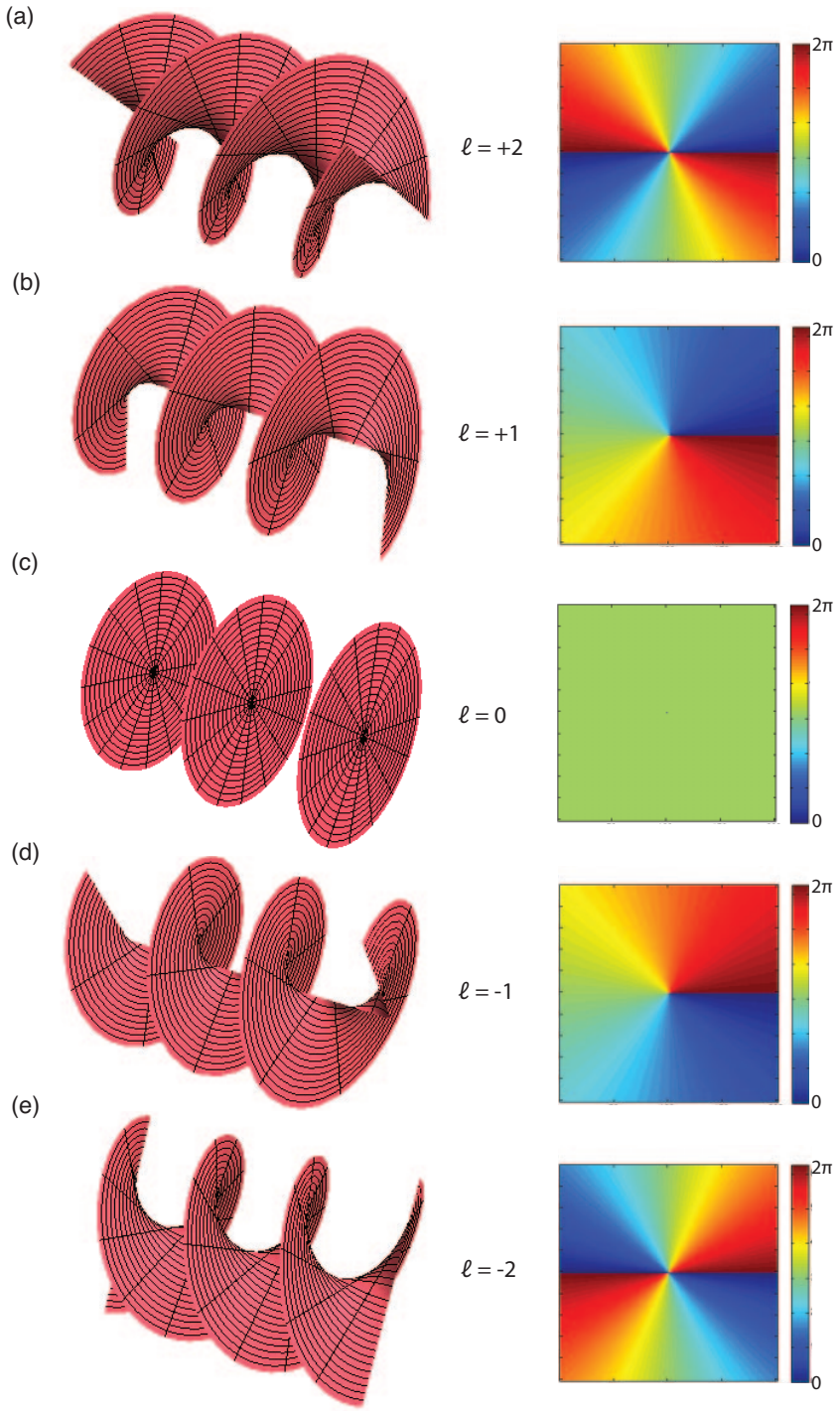

Fig. 4. – The wavefronts and transverse phase structure of five vortex modes with azimuthal quantum numbers: (a) $\ell = +2$, (b) $\ell = +1$, (c) $\ell = 0$, (d) $\ell = -1$, and (e) $\ell = -2$.

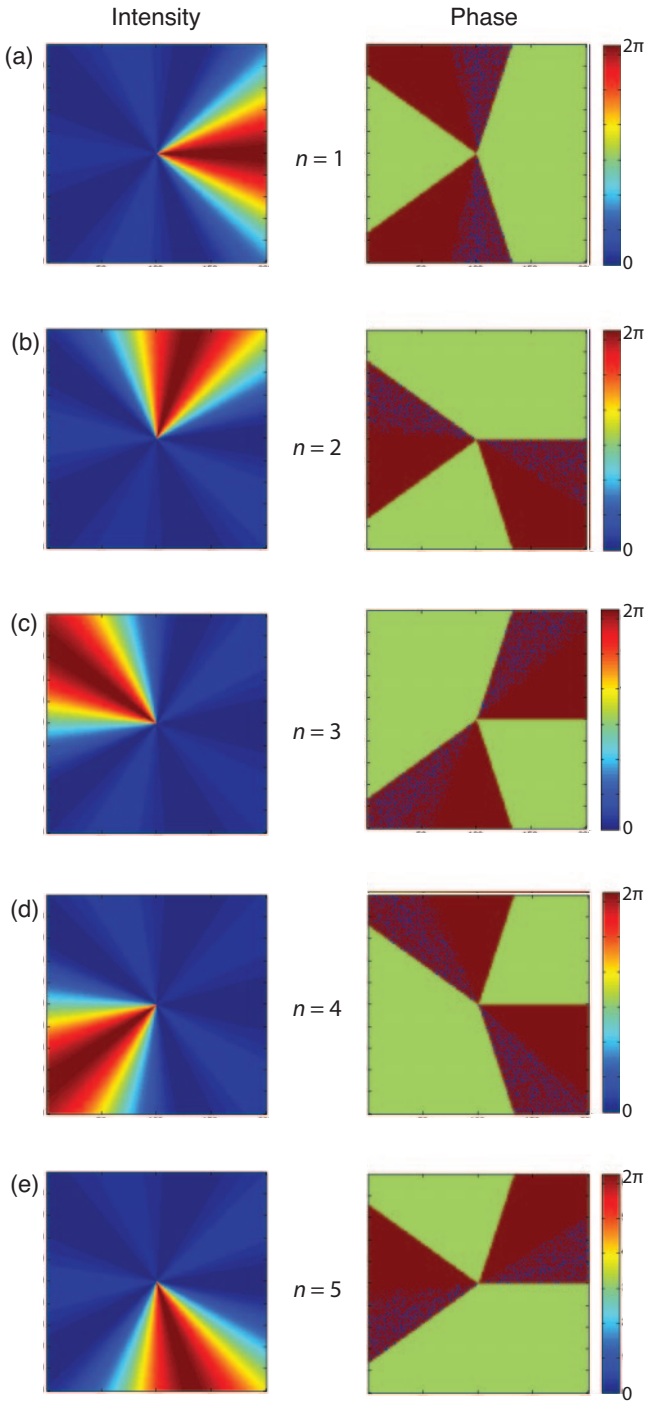

Fig. 5. – Simulated intensity and phase for the set of five angular position (ANG) modes composed of OAM modes with $\ell = 0, \pm 1, \pm 2$.

1˙5. *Weak values*. – Weak values were first introduced in a seminal paper by Aharanov, Albert, and Vaidman in 1988 [20]. In general, weak values are complex numbers that one can assign to the powers of a quantum observable operator $\hat{A}$ using two states: an initial, preparation state $|i\rangle$, and a final, post-selection state $|f\rangle$. The n-th order weak value of $\hat{A}$ has the form

$$A_w^n = \frac{\langle f|\hat{A}^n|i\rangle}{\langle f|i\rangle}\,, \tag{16}$$

where the order n corresponds to the power of $\hat{A}$ that appears in the expression.

Weak values have long been considered an abstract concept. However, since their introduction 25 years ago, they have gradually transitioned from a theoretical curiosity to a practical laboratory tool. In a recent review, we show how these peculiar complex expressions appear naturally in laboratory measurements [21]. In order to do so, we derive them in terms of measurable detection probabilities.

In a standard prepare-and-measure experiment, the probability of detecting an event is given by $P = |\langle f|i\rangle|^2$ where $|i\rangle$ corresponds to the initial and $|f\rangle$ to the final state. If we introduce an intermediate unitary interaction $\hat{U}(\epsilon) = \exp(-i\epsilon\hat{A})$ that modifies the initial state, the detection probability also changes to $P_\epsilon = |\langle f|i'\rangle|^2 = |\langle f|\hat{U}(\epsilon)|i\rangle|^2$. If ϵ is small enough, we can consider $\hat{U}(\epsilon)$ to be "weak". In this case, the operator $\hat{U}$ can be expanded in a Taylor series. The detection probability above can then be written as (shown here to first order):

$$\begin{aligned} P_\epsilon &= |\langle f|\hat{U}(\epsilon)|i\rangle|^2 = |\langle f|(1 - i\epsilon\hat{A} + \ldots)|i\rangle|^2 \\ &= P + 2\epsilon\,\mathrm{Im}\langle i|f\rangle\langle f|\hat{A}|i\rangle + O(\epsilon^2). \end{aligned} \tag{17}$$

Assuming $|i\rangle$ and $|f\rangle$ are not orthogonal (*i.e.* $P \neq 0$), we can divide both sides of the previous equation by P to obtain

$$\frac{P_\epsilon}{P} = 1 + 2\epsilon\,\mathrm{Im}\,A_w - \epsilon^2\left[\mathrm{Re}\,A_w^2 - |A_w|^2\right] + O(\epsilon^3), \tag{18}$$

where A_w is the first-order weak value and A_w^2 is the second-order weak value as defined above in eq. (16). Here, we arrive at our operational definition: weak values characterize the relative correction to a detection probability $|\langle f|i\rangle|^2$ due to a small intermediate perturbation $\hat{U}(\epsilon)$ that results in a modified detection probability $|\langle f|\hat{U}(\epsilon)|i\rangle|^2$. When the higher order terms in the expansion given in eq. (18) can be neglected, one has a linear relationship between the probability correction and the first order weak value, which we call the *weak interaction regime*. The conditions under which the higher order terms cannot be neglected are discussed in detail in ref. [21].

In general, weak values are complex quantities. In order to measure a weak value, one has to measure both its real and imaginary parts. In most laboratory measurements of the weak value, one uses a coupled system of observables in order to do so. Such a system is composed of two parts —a "system" observable, whose weak value we are interested in measuring, and a "pointer" observable, which provides us with information about the system observable. For example, in the experiment of Ritchie *et al.* [22], the authors use a coupled system of photon polarization and position. This system is illustrated in fig. 6 by an experimental setup where the polarization of a photon is weakly coupled to its

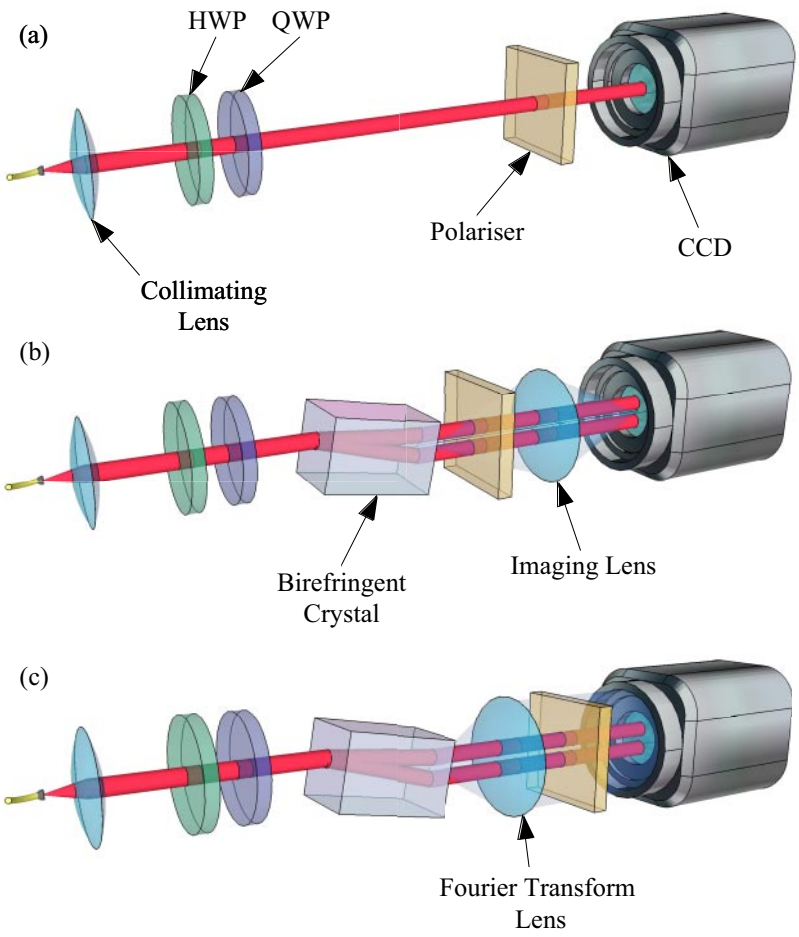

Fig. 6. – An experiment illustrating how weak values are measured by using a coupled system of two observables. (a) A collimated Gaussian beam from a single mode fiber (SMF) is prepared in an initial polarization state by a quarter-wave plate (QWP) and half-wave plate (HWP). A polarizer is used for post-selection into a final polarization state. A CCD is used for measuring the position-dependent beam intensity. (b) A birefringent crystal inserted between the wave plates and polarizer displaces the beams by a small amount. A lens is used for imaging the output face of the crystal onto the CCD in order to measure the real part of the polarization weak value. (c) A lens is used for imaging the far-field of the crystal face onto the CCD in order to measure the imaginary part of the polarization weak value (figure redrawn from ref. [21]).

position by a thin birefringent crystal. In this setup, the polarization state is prepared by a half-wave and quarter-wave plate, and post-selected by a polarizer. The position state is prepared in a gaussian mode by collimating light from a fiber, and post-selected by either imaging or Fourier-transforming the mode onto a CCD detector. The real and imaginary parts of the polarization weak value are obtained by making appropriate post-selections on the photon position or momentum, which result in the real or imaginary parts of the polarization weak value being isolated.

Such a system is described by a symmetric combination of the real and imaginary parts of the weak values of polarization (S_w) and momentum (p_w):

$$\frac{P_\epsilon}{P} - 1 \approx \frac{2\epsilon}{\hbar} \left[\mathrm{Re}\, S_w \,\mathrm{Im}\, p_w + \mathrm{Im}\, S_w \,\mathrm{Re}\, p_w\right]. \tag{19}$$

Here, the real and imaginary parts of the polarization weak value are isolated by using two experimental configurations. In one configuration, a post-selection of the photon position is performed such that the momentum weak value is purely imaginary. This corresponds to imaging the crystal face onto the detector, as shown in fig. 6(b). In this case, the real part of the momentum weak value in eq. (19) goes to zero, which effectively isolates the real part of the polarization weak value. In the second configuration, a post-selection of the photon momentum is performed, which results in the momentum weak value being purely real. This corresponds to looking at the far-field of the crystal face with a Fourier-transform lens, as shown in fig. 6(c). In this case, the imaginary part of the momentum weak value in eq. (19) goes to zero, which effectively isolates the imaginary part of the polarization weak value. This example is analyzed in more detail in ref. [21].

In this manner, any system of two coupled observables can be used to measure the weak value of one of the observables. For example, by making appropriate post-selections on the polarization degree of freedom, one could isolate and measure the real and imaginary parts of the momentum weak value. This is indeed the technique used in the direct measurement method that is explained in sect. **2**˙4.

2. – Quantum technologies today

2˙1. *Introduction.* – The Heisenberg uncertainty principle lies at the heart of most modern quantum technologies. The ultimate limits of measurement precision are set by this principle and have been reached through the use of quantum resources such as entanglement and squeezed light [23, 3, 24]. The uncertainty principle also bounds the probability of simultaneously measuring two complementary observables, such as position and momentum. By extending this idea to discrete properties of a photon such as its polarization, the field of quantum secure communication was developed [2, 12]. Quantum concepts such as superposition and entanglement have expanded the fields of information theory and computing to remarkable frontiers [25, 26]. Clearly, quantum mechanics has had a profound impact on modern technology. However, most of these technologies still live in the domain of proof-of-principle experiments on the lab bench. Given the rate of technological progress today, it will not be long before we see technologies such as practical quantum computing and long-distance quantum communication become a reality. In this section, we briefly describe three quantum technologies that form the backbone of this article —quantum key distribution, quantum ghost imaging, and direct measurement.

2˙2. *Quantum key distribution.* – Quantum key distribution (QKD) was first proposed by Bennett and Brassard in 1984 as a method by which two parties, Alice and Bob, could share a random string of bits with one another with unconditional security [2, 27]. A third party, Eve, with the intention of eavesdropping on Alice and Bob's communication channel, would be unable to do so without introducing a certain amount of statistical error in the channel. This is best illustrated by the use of a simple example. Let us say Alice wants to convey a bit value of 1 or 0 to Bob. She will then choose at least

two mutually unbiased bases in which to represent this bit value. For polarization, two such bases are the horizontal-vertical (H/V) basis and the diagonal-anti-diagonal (D/A) basis. These are known as "mutually unbiased bases" (MUBs) because one can express each state in one basis as an equally weighted sum of the states in the other. We can invert eqs. (3) from sect. **1** to write states in the H/V basis as a sum of states in the D/A basis:

$$|V\rangle = \frac{1}{\sqrt{2}}\big[|D\rangle - |A\rangle\big], \tag{20}$$
$$|H\rangle = \frac{1}{\sqrt{2}}\big[|D\rangle + |A\rangle\big].$$

Let us say Alice picks the H/V basis for encoding. Then, state $|H\rangle$ corresponds to 0 and state $|V\rangle$ corresponds to 1. Alice sends a bit value of 0 encoded as an $|H\rangle$ state. If Eve intercepts the communication channel and measures this state in the correct H/V basis, she will obtain the correct bit value. However, if she measures the state in the incorrect D/A basis, she will have an error half the time. This is because when measuring an $|H\rangle$ state in the D/A basis, Eve has an equal probability of measuring a $|D\rangle$ or an $|A\rangle$ state, which in turn correspond to 0 or 1. This results in an error of 50% when Eve measures in the wrong basis. Combined with the 50% chance of Eve picking the wrong basis leads to a total error probability of 25%.

For the protocol to work, Alice randomly picks between the H/V and D/A bases for encoding. She then transmits these states to Bob. Bob measures these states in the same manner as Eve, by also randomly picking between the H/V and D/A bases. Just like Eve, Bob will also get an error with 25% probability. To remove these errors, Alice shares her basis choices through a public channel *after* Bob has made all his measurements. Bob then discards all the measurements that he made where his basis choice did not match Alice's. This procedure is known as "sifting".

After the sifting procedure, Alice and Bob ideally share an error-free string of bits. Now let us reinsert Eve, who intercepts and resends all of Alice's states to Bob. Like Bob, Eve also measures these states by randomly picking between the H/V and D/A bases. Again, like Bob, Eve gets an error rate of 25%. She then resends her measured states to Bob in the basis she measured them in. By doing so, she introduces errors than cannot be removed by the sifting process. For example, after sifting, Alice and Bob both have a bit value measured in the H/V basis. If Eve also measured and resent that bit in the H/V basis, she would have introduced no error. However, if she measured and resent that bit in the D/A basis, she would have introduced an error half the time, leading to a total error rate of 25%.

Thus, Alice and Bob can determine if Eve had intercepted and resent their states by sacrificing a small part of the key and checking the error rate. If they obtain an error rate less than 25%, they can assume their protocol was secure. If they obtain an error rate greater than or equal to 25%, they assume an eavesdropper was present and abandon the protocol. In this manner, Alice and Bob can generate a secure key using the method of QKD.

The intercept-resend attack explained above is illustrated by means of a table in fig. 7. All possible outcomes (post-sifting) are shown for the case when Alice picks an $|H\rangle$ photon to encode a 0. The cases where Bob has an error, *i.e.* he registers a $|V\rangle$ photon, are shown as purple cells. These occur with a probability of $0.125 + 0.125 = 0.25$. It is clear from

Alice's Basis	Alice Prepares	Eve's Basis	Eve Measures	Bob's Basis	Bob receives	Occurrence Probability
HV	H (0)	HV	H (0)	HV	H (0)	0.5
HV	H (0)	DA	D (0)	HV	H (0)	0.125
HV	H (0)	DA	A (1)	HV	H (0)	0.125
HV	H (0)	DA	D (0)	HV	V (1)	0.125
HV	H (0)	DA	A (1)	HV	V (1)	0.125

Probability that Eve introduces an error using intercept-resend:
1. Alice sends a state (H) in the HV basis.
2. Eve intercepts and measures randomly in either the HV or the DA basis.
3. Eve resends the state she measured.
4. Bob always measures in the same basis as Alice (after sifting)
5. Bob measures the wrong symbol (V) with a 0.125+0.125=0.25 probability.

Fig. 7. – A table showing the different possible outcomes in an intercept-resend eavesdropping attack when Alice and Bob use a 4 state, 2 MUB protocol. As shown, Eve introduces a 25% error between Alice and Bob after the sifting procedure (*i.e.* Alice and Bob discard all mismatched basis measurements).

this table that an intercept-resend eavesdropping attack by Eve will introduce an error of 25% between Alice and Bob.

The two main protocols used to perform QKD are known as the BB84 protocol [2] and the Ekert protocol [12], named after their founders Charles Bennett, Gilles Brassard, and Artur Ekert. The procedure described above is known as the BB84 protocol and relies on the impossibility of cloning single photons for security [1]. Recent work has cleverly extended this protocol for use with weak coherent pulses which are susceptible to a photon number splitting eavesdropping attack. In this extension known as the decoy state protocol, Alice randomly modulates the mean photon number of her pulses and later shares this information with Bob [28]. The decoy state protocol is discussed further in sect. **5**. The second main QKD protocol invented by Artur Ekert relies on the quantum correlations in entanglement for security. Alice and Bob initially share correlated photons from a common entanglement source. Any eavesdropper intercepting and resending either Alice or Bob's photons disturbs the fragile entanglement, which introduces errors as before. This loss of entanglement can also be checked via other means such as a test of Bell's inequalities [10] and entanglement witnesses [29]. Schematics for both these protocols are shown in fig. 8.

The security analysis in the Ekert protocol is identical to that of BB84. The main difference appears in the passive selection of states by Alice *and* Bob and the location of the source. In BB84, the source is located at Alice and she actively picks states to send to Bob. In Ekert, both Alice and Bob make passive measurements in their chosen measurement bases. In addition, the source of entangled photons can be spatially separated from both Alice and Bob. The lack of active preparation can be considered a technological advantage of Ekert over BB84, especially since entangled sources are available rather easily today.

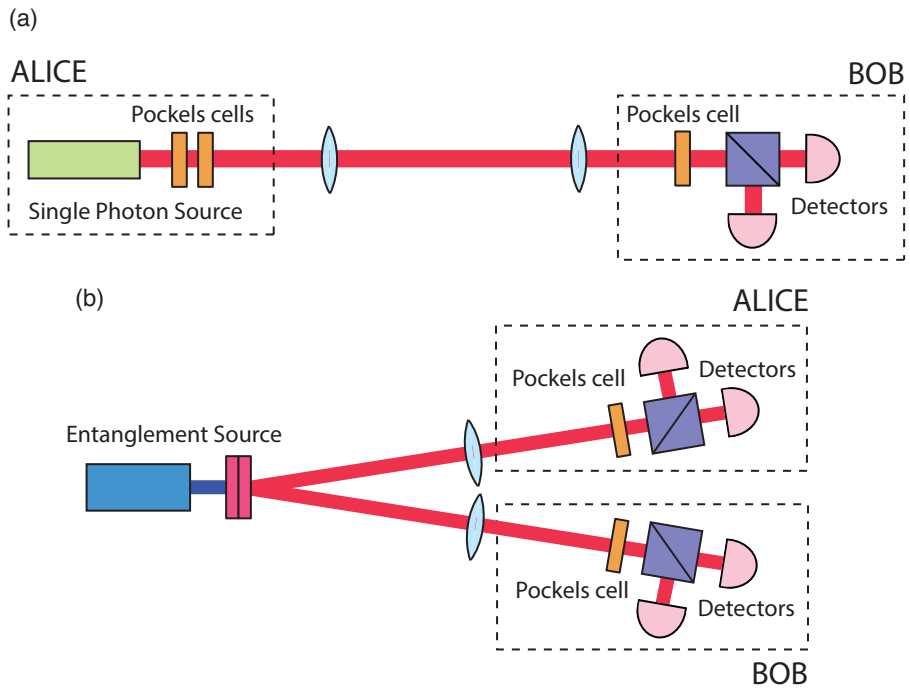

Fig. 8. – Schematics for (a) prepare and measure BB84 QKD protocol and (b) entanglement-based Ekert QKD protocol.

2˙3. *Quantum ghost imaging.* – Ghost imaging, also known as coincidence imaging, was first implemented with position-momentum entangled photons [15, 30]. The strong position and momentum correlations shared by such photons allow one to perform imaging without a spatially resolving detector. This process is depicted in fig. 9(a). The entangled photons are generated by pumping a β-Barium Borate (BBO) crystal with a pump laser (not shown). The entangled signal and idler photons generated in the type II downconversion process are orthogonally polarized, and can be separated with a polarizing beamsplitter (PBS). The crystal face is imaged both onto an object and onto a "ghost" image plane through the PBS. The signal photon, as it has come to be called, is then allowed to fall onto a spatially non-resolving bucket detector. As its name implies, the bucket detector collects all the signal photons that make it past the object. The idler photons, on the other hand, are imaged from the ghost image plane onto a spatially resolving detector (CCD). A sharp image is obtained in the coincidence counts of the CCD and the bucket detector. The term "ghost image" was coined for this phenomenon based on the fact that the image was formed without directly obtaining any spatially resolved image information from the object itself [15].

It was soon shown that ghost imaging relied solely on the spatial correlations of the two light fields. The same effect was reproduced by using randomly but synchronously directed twin beams of classical light [31]. A benefit of using entangled photons was found to be that imaging could be performed both in the near and far fields, without having to change the source [32, 33]. This is a direct consequence of the fact that entangled photons have strong correlations in both position and momentum, which correspond to

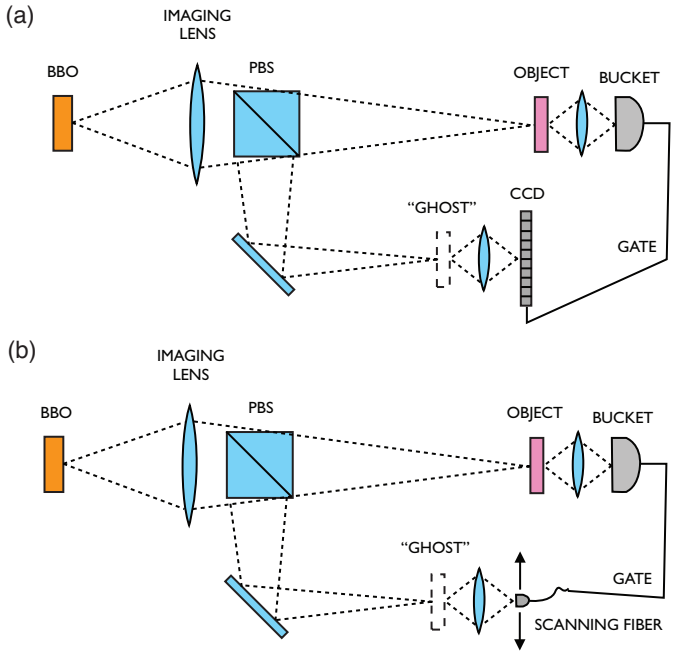

Fig. 9. – (a) An ideal quantum ghost imaging scheme that uses a CCD gated by a bucket detector for creating a "ghost" image of an object without directly gaining any spatial information from it. (b) In reality, CCDs that can detect single photons are not commonplace. Hence, a scanning fiber tip is used in place.

correlations in the near and far fields respectively. In the case of ghost imaging with an entangled source, the choice of whether to measure in the image plane or the diffraction pattern is left to the observer, instead of being determined by the source. Subsequently, even this property of ghost imaging with an entangled source was mimicked by using a pseudothermal source [34]. The twin speckle patterns created by shining an intense beam of light through a ground glass plate and a beamsplitter were found to have strong spatial correlations in both the near and far fields [32].

In practice, both the quantum and thermal ghost imaging methods require the use of many single-photon pairs or random speckle patterns to obtain an image. Also, long processing times are needed for scanning an avalanche photodiode in the quantum case [15] (fig. 9(b)) or averaging many speckle patterns on a CCD camera in the thermal case [34]. These requirements have made the practical applicability of such schemes difficult. Due in part to this, ghost imaging has steadily inhabited the domain of proof-of-principle experiments. Studies of ghost imaging through turbulence [35, 36] and ghost imaging experiments using compressive sensing [37-39] have been performed. More recent efforts to exploit the quantum correlations of spatially entangled photons have led to new techniques for sub-shot-noise imaging [40]. A very recent experiment was able to use induced coherence between entangled photons from two separate sources in order to image an object with photons that never interacted with it [41]. It is clear that the field of quantum imaging still has many new insights to offer and unexplored ideas yet to be discovered. In sect. **4**, we extend the ghost imaging technique described in this section into a ghost

image identification scheme. Instead of using a scanning fiber tip to measure the image, we use a hologram as an "image sorter". In this manner, a known set of objects can identified by a pair of entangled photons, one of which interacts with the object and the other with the image sorting hologram. This technique is much faster than building a ghost image pixel by pixel, and maximizes the amount of image information carried by each photon.

2˙4. *Direct measurement.* – Weak values first aroused interest in the context of amplifying a small detector signal. By making an appropriate post-selection, the weak value can be made very large, which allows an experimenter to easily estimate the unknown small parameter ϵ. However, this amplification is achieved at the cost of a large loss due to the post-selection process. Due to this, the benefits of weak value amplification as compared to standard statistical techniques have been studied in detail [42, 43]. More recently, weak values have been used in an alternative technique for measuring a quantum state. Conventionally, a quantum state is measured through the indirect process of quantum tomography [44]. Like its classical counterpart, quantum tomography involves making a series of projective measurements in different bases of a quantum state. This process is indirect in that it involves a time consuming post-processing step where the density matrix of the state must be globally reconstructed through a numerical search over the many allowed alternatives. Due to this, tomography is prohibitive for measuring high-dimensional multipartite quantum states such as those of orbital angular momentum.

Recent work has shown that a quantum state can be expanded into sums and products of complex weak values, which are proportional to the probability amplitudes of the state [45-47]. As these weak values are measurable quantities, a quantum state can thus be determined directly without the need for the complicated post-processing step involved in tomography. A particularly notable application of such an expansion is the direct determination of the complex components of a pure quantum state $|\psi\rangle$ expanded in a particular measurement basis $\{|a\rangle\}$ [45-47]. This is accomplished by the insertion of the identity and multiplication by a strategically chosen constant factor $c = \langle b|a\rangle/\langle b|\psi\rangle$, where the auxilliary state $|b\rangle$ must be unbiased with respect to the entire basis $\{|a\rangle\}$ such that $\langle b|a\rangle$ is a constant for all a. With this choice we have

$$c|\psi\rangle = c\sum_a |a\rangle\langle a|\psi\rangle = \sum_a |a\rangle \frac{\langle b|a\rangle\langle a|\psi\rangle}{\langle b|\psi\rangle}\,. \tag{21}$$

That is, each scaled complex component $c\langle a|\psi\rangle$ of the state $|\psi\rangle$ can be directly measured as a complex weak value of the projection operator $\hat{\Pi}_a = |a\rangle\langle a|$ using the unbiased auxilliary state $|b\rangle$ as a post-selection. After determining these complex components experimentally, the state can be renormalized to eliminate the constant c up to a global phase. For mixed states, one can additionally vary the auxilliary state $|b\rangle$ within a mutually unbiased basis to determine the Dirac distribution for the state directly using the same technique [46, 47].

We can use our previous example of a polarized beam going through a birefringent crystal (fig. 6) to illustrate this idea. We showed earlier how we can isolate and measure both the real and imaginary parts of the polarization weak value S_w in this experiment. In order to apply our setup to characterize the polarization quantum state, we must perform the post-selection in a basis mutually unbiased with respect to the weak measurement basis. Specifically, as the birefringent crystal in our example performs a weak

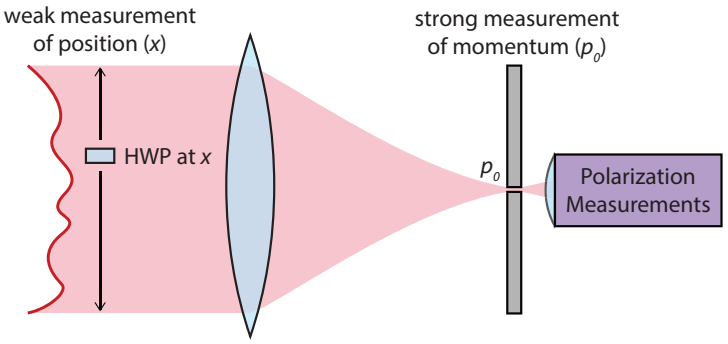

Fig. 10. – A schematic outlining the direct measurement experiment of Lundeen *et al.* [45] where the authors measured the wave function in the position basis by using polarization as a pointer.

measurement in the H/V basis, we must orient the post-selecting polarizer in the D/A basis (which is mutually unbiased with respect to the H/V basis). This is the exact procedure used in the polarization state characterization experiment of ref. [47] and discussed in further detail in ref. [21].

In the pioneering experiment of Lundeen *et al.* [45], the authors first used this technique to measure the wave function of an ensemble of identically prepared photons in the position basis. Following the theoretical treatment above, one can expand the wave function $|\Psi\rangle$ in the position basis in terms of weak values. By inserting the identity $|x\rangle\langle x|$ and multiplying by a constant factor $c = \langle p\,|x\,\rangle\,/\,\langle p\,|\Psi\,\rangle$, one can write the wave function as

$$c|\Psi\rangle = c\int \mathrm{d}x|x\rangle\langle x|\Psi\rangle = \int \mathrm{d}x|x\rangle\frac{\langle p|x\rangle\langle x|\Psi\rangle}{\langle p|\Psi\rangle} = \int \mathrm{d}x\,\langle\pi_x\rangle_{\mathrm{W}}\,|x\rangle. \tag{22}$$

In this manner, the wave function at a particular position x is found to be proportional to the weak value at that position

$$c\Psi(x) = \langle\pi_x\rangle_{\mathrm{W}}\,. \tag{23}$$

In order to measure the position weak value, Lundeen *et al.* used polarization as a pointer. As explained in sect. **1**˙5, the weak value of a particular observable can be measured by coupling that observable to a pointer observable. As shown in fig. 10, the authors performed a weak measurement of the position x of a photon by rotating the polarization at x by a small angle with a sliver of half-wave plate (HWP). A strong measurement of the conjugate variable of momentum was performed by Fourier-transforming with a lens and post-selecting value $p = 0$ of momentum. By measuring the rotation of the polarization vector in the linear and circular polarization bases, the authors were able to measure the real and imaginary parts of the position weak value. From this, they obtained the real and imaginary parts of the wave function, which then gave them the amplitude and phase as a function of x. They verified this measurement by comparing it to a regular measurement with a Shack-Hartmann wavefront sensor. We use this direct measurement technique in sect. **6** to measure the wave function of a high-dimensional quantum state in the OAM basis.

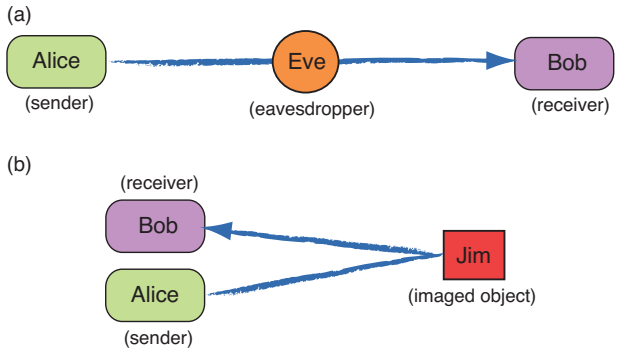

Fig. 11. – A sketch comparing the (a) quantum key distribution and (b) quantum-secured imaging protocols. (Figure redrawn from ref. [50], © 2012 American Institute of Physics.)

The primary benefit of this tomographic approach is that minimal post-processing is required to construct the state from the experimental data. The real and imaginary parts of each state component directly appear in the linear response of the measurement device up to appropriate scaling factors. The downside of this approach is that the auxiliary state $|b\rangle$ must be chosen carefully so that the denominator $\langle b|\psi\rangle$ or $\langle p|\Psi\rangle$ (and hence the detection probability) does not become too small and break the weak interaction approximation used to determine the weak values [48]. This restriction limits the generality of the technique for faithfully determining a truly unknown $|\psi\rangle$. For a more comprehensive review of recent work on this topic, see ref. [21].

3. – Quantum-secured surveillance

3˙1. *Quantum-Secured Imaging*. – Active imaging systems such as radar and lidar are susceptible to intelligent jamming attacks, where the light used for querying an object is intercepted and resent. In this manner, an object can send false information to the receiver belying its true position or velocity, or even creating a false target [49]. In this section, we show how one can detect such jamming attacks by using quantum states of light modulated in polarization. The BB84 protocol of quantum key distribution (QKD) uses such quantum states to generate a random key with unconditional security [2]. By randomly modulating the polarization of single photons in two mutually unbiased polarization bases, the sender (Alice) can send a stream of 1s and 0s to the receiver (Bob). Any eavesdropper trying to gain information about the polarization of a photon will have to perform a measurement, thus unalterably changing the polarization state and introducing errors that Alice and Bob can detect. In this manner, the eavesdropper will reveal herself (fig. 11a).

We extend this idea to an imaging system, where the object to be imaged now plays the role of the eavesdropper. Alice and Bob constitute the imaging system, and are hence located in the same place (fig. 11b). If the object intercepts and resends any of the imaging photons, it will introduce errors in the polarization encoding that can be detected by Alice and Bob. In a two-dimensional polarization-based QKD system, the minimum error introduced by an eavesdropper using an intercept-resend attack is equal to 25%. We apply this same error bound to our imaging system. As shown in fig. 12, a HeNe laser is intensity modulated by an acousto-optic modulator (AOM) to create pulses

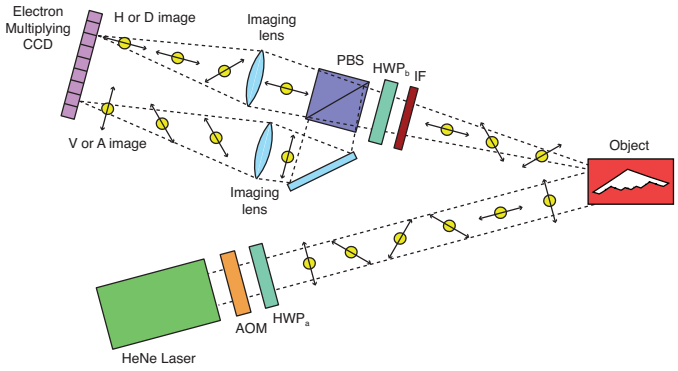

Fig. 12. – Schematic of our quantum-secured imaging experiment. An object is securely imaged with single-photon pulses modulated in polarization. Security is verified by measuring the error between sent and received polarizations. (Figure redrawn from ref. [50], © 2012 American Institute of Physics.)

with less than one detected photon on average. A half-wave plate ($\mathrm{HWP_a}$) mounted on a motorized rotation stage randomly switches the polarization state of the photon among horizontal, vertical, diagonal, and anti-diagonal ($|H\rangle$, $|V\rangle$, $|D\rangle$, and $|A\rangle$). The single-photon pulses are incident on the object, which consists of a stealth aircraft silhouette on a mirror. They are then specularly reflected from the object towards our detection system. In fig. 12, a non-zero reflectance angle is shown for clarity. An interference filter (IF) is used to eliminate the background. A second rotating half-wave plate ($\mathrm{HWP_b}$) and a polarizing beam-splitter (PBS) perform a polarization measurement in either the horizontal-vertical (H/V) or diagonal-anti-diagonal (D/A) basis. Two lenses are used after the PBS to create four images corresponding to the four measured polarizations on an electron-multiplying CCD camera (EMCCD), which serves as a spatial single-photon detector.

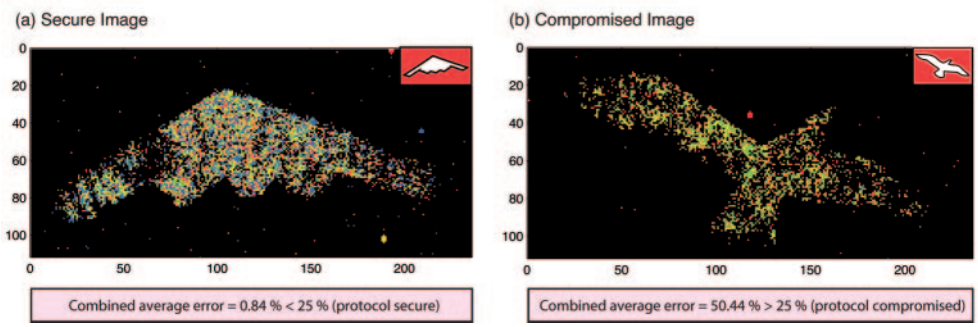

Fig. 13. – Laboratory demonstration of quantum-secured imaging. (a) When there is no jamming attack, the received image faithfully reproduces the actual object, which is shown in the inset. (b) In the presence of an intercept-resend jamming attack, the received image is the "spoof" image of a bird. However, the imaging system can always detect the presence of the jamming attack, because of the large error rate in the received polarization. In (a) the error rate is 0.84%, while in (b) it is 50.44%. A detected error rate of $> 25\%$ indicates that the image received has been compromised. (Figure redrawn from ref. [50], © 2012 American Institute of Physics.)

Figure 13(a) and (b) show two images formed using this system. The first image of a stealth aircraft has a measured polarization error of 0.84%. This means that 0.84% of the time in the image, the measured polarization of a received photon was different from the photon polarization sent. Since this is less than the error bound of 25%, this image can be considered secure. The second image shows results from a simulated intercept-resend attack where the object simply blocked all the incoming photons, and resent photons in state $|H\rangle$ with modified information indicating the image of a bird. The polarization error measured in this case is 50.44%, which is very close to the expected value of 50%. Since this is greater than the error bound of 25%, it indicates that the object was actively jamming the imaging system.

3˙2. *Quantum-secured LIDAR.* – We can apply this quantum-secured protocol to a lidar system that uses the time-of-flight information of a light pulse to measure the velocity of a moving object. In ref. [50], we propose such a system based on the Ekert protocol of QKD. In our system, one photon from an entangled pair is kept locally. The second photon travels to the object and back. Any intercept-resend attack by the object can be detected by testing the presence of entanglement in the system via a test of Bell's inequalities. The loss of entanglement would indicate that the lidar system system is being actively jammed. This lidar system is discussed in more detail in ref. [50]. While our quantum-secured protocols are certainly limited by cloaking techniques that do not modify the polarization state of a photon, they can be easily integrated into modern optical ranging systems given the current state of QKD technology.

4. – Quantum ghost image identification

4˙1. *Introduction.* – Holograms are a hallmark of science fiction movies, often used to instill a sense of futuristic reality where one can create three-dimensional objects made entirely of light. While realistic 3D holograms are indeed a technology of the future, simpler holograms are more commonplace than one may think. For example, holograms are used as security marks on identity and credit cards. Holograms are also used for recording large amounts of information onto a medium. A simple hologram can be formed by interfering two mutually coherent waveforms, which can be written in terms of their amplitude and phase as [51]

$$A(x,y) = |A(x,y)|e^{i\phi_A(x,y)}, \qquad R(x,y) = |R(x,y)|e^{i\phi_R(x,y)}. \tag{24}$$

Here, A is an arbitrary unknown field and R is a known reference field. In the developing process, the interference pattern written onto the hologram is given by the intensity $I(x,y) = |A(x,y) + R(x,y)|^2$ as follows:

$$\begin{aligned} I(x,y) &= |A(x,y)|^2 + |R(x,y)|^2 + A(x,y)^\dagger R(x,y) + A(x,y)R(x,y)^\dagger \\ &= |A(x,y)|^2 + |R(x,y)|^2 + 2|A(x,y)||R(x,y)| \cos\left[\phi_R(x,y) - \phi_A(x,y)\right]. \end{aligned} \tag{25}$$

Here, the first two terms depend only on the intensities of each field while the third term depends on their relative phases. In this manner, a hologram stores information about both, the amplitude and the phase of the unknown waveform A. By sending the reference waveform R through the developed hologram, the unknown waveform A can

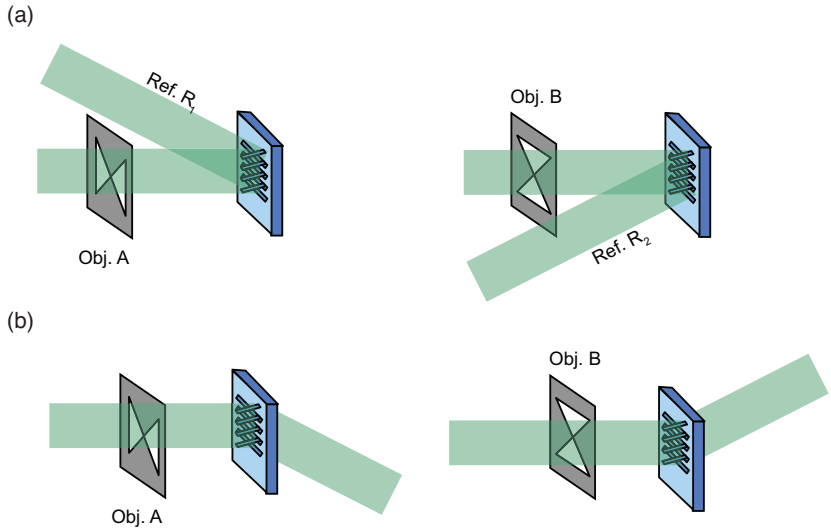

Fig. 14. – A cartoon showing (a) the construction and (b) the operation of a two-object multiplexed hologram as an image sorter.

be reconstructed. In fact, we use this technique in sect. **5** to create fields with a helical phase structure, also known as orbital angular momentum modes.

4˙2. *Holograms as image sorters.* – The wavefront reconstruction process described above can be employed in reverse. Instead of recreating the waveform A by sending reference R into the hologram, one can send waveform A into the hologram to recreate reference R. In this manner, a hologram can be used to "identify" an image from a set of images. The resulting output can be written as a product of the original waveform with the transmission function given by the intensity of the hologram

$$A(x,y)I(x,y) = A(x,y)|A(x,y)|^2 + A(x,y)|R(x,y)|^2 + |A(x,y)|^2 R(x,y) + A^2(x,y)R(x,y)^\dagger \tag{26}$$

If a plane wave is used as the reference beam, the first two terms in the above equation are simply an attenuated version of the original unknown waveform propagating in the normal direction. We refer to this as the "zero-order" output from the hologram. The third term gives us the recreated reference beam R, which also carries the intensity distribution of the original waveform $|A|^2$. The fourth term refers to a virtual reference beam $R^\dagger$. A similar hologram can be constructed for two arbitrary fields A and B, with two difference reference fields R_1 and R_2. Such a hologram is referred to as a *multiplexed* hologram, and can be used an image sorter for distinguishing two images for each other.

A cartoon showing the construction and operation of such a multiplexed hologram is shown in fig. 14(a) and (b). First, the holographic material is exposed with an interference pattern formed by interfering field A originating from object A with a reference plane wave R_1. Then, this procedure is repeated for object B with a reference plane wave R_2 from a different direction (fig. 14(a)). The hologram is then fixed (or developed) to make the interference pattern permanent. This multiplexed hologram then acts as an image

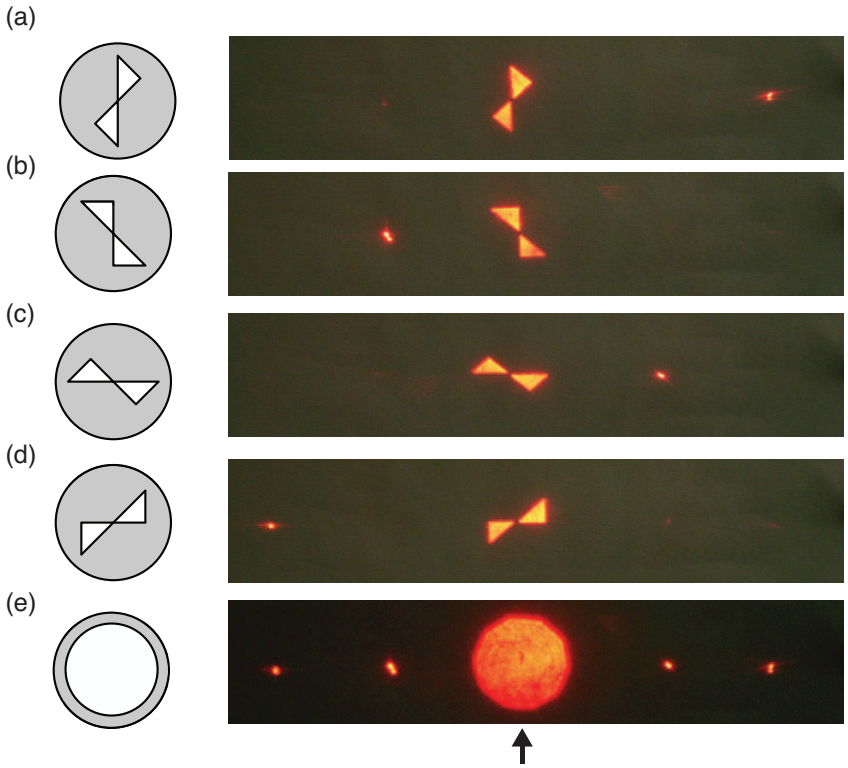

Fig. 15. – CCD images showing the output from a four-object multiplexed hologram sorting objects (a)-(d). Panel (e) shows the output when a collimated field is sent into the hologram. Notice that a strong zero-order field (indicated by the vertical black arrow) is present in all cases.

sorter, converting a field from object A into reference R_1 and one from object B into reference R_2 (fig. 14(b)). The output from such a hologram made for 4 different objects is shown in fig. 15. CCD images of the output for each object (a-d) show a strong zero-order output in the normal direction (indicated by a black arrow), and a strong diffracted component in the direction of the original plane wave associated with object (a-d). In fig. 15(e), the output obtained when a collimated beam with uniform amplitude is input into the hologram is shown. As can be seen, all four diffracted orders are present, as image information for all four objects is present in the input. While these images show the hologram operating at high light levels, we use the same hologram in the next section to perform ghost image identification with single photons. Many of these predictions have been verified in recent publications [52, 53].

4˙3. *Ghost image identification with correlated photons.* – In this section, we describe a quantum ghost imaging scheme that uses the aforementioned holographic filtering technique to identify an object from a large basis set of objects [53]. As a proof-of-principle experiment, we demonstrate this method for both a set of two and a set of four spatially non-overlapping objects. We do so by replacing the CCD in the idler arm of the standard ghost imaging setup described in sect. **2˙3** with a holographic sorter. The ghost image

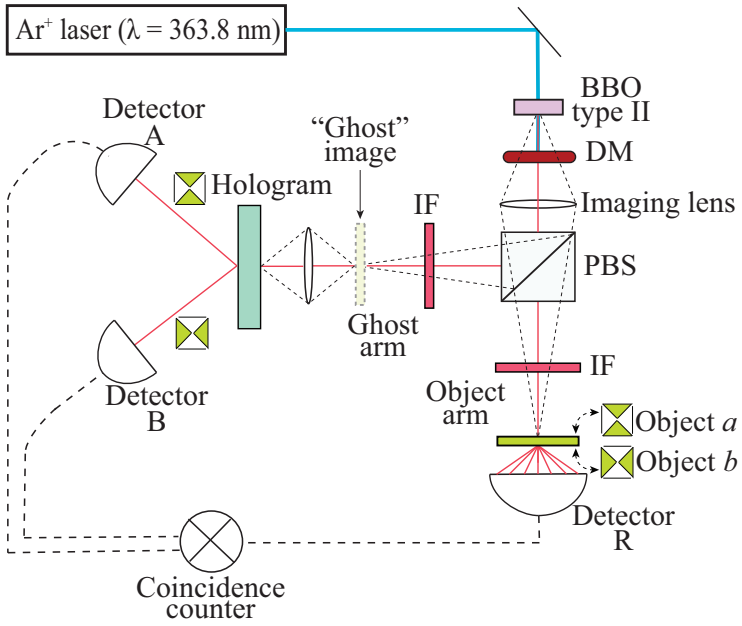

Fig. 16. – Experimental setup for quantum ghost image identification. DM is a dichroic mirror for blocking the pump laser; IF is an interference filter with 10 nm bandwidth, centered at 727.6 nm. The dotted lines indicate the imaging process for a point object. (Figure adapted from ref. [53].)

is obtained from the coincidence counts of the bucket detector and the beams diffracted by the hologram. In this manner, we are able to determine which object from our pre-established set is in the signal arm without directly acquiring any spatial information about it. In our analysis, we change the naming system by referring to the signal arm as the "object" arm and the idler arm as the "ghost" arm. The object arm is the path taken by the object photon and contains the object followed by the bucket detector. The ghost arm is the path taken by the ghost photon and contains a holographic sorter and single-photon detectors (fig. 16).

Let us first describe the two-object case. The measurement in the object arm is carried out by the object-bucket detector combination. The object photon is either transmitted into the bucket detector, labelled R in fig. 16, or is blocked by the object. The measurement in the ghost arm is carried out by the hologram-detectors combination. The ghost photon is diffracted into either detector A or B. If object a is present in the object arm and transmits an object photon into bucket detector R, the corresponding ghost photon will always be diffracted by the hologram into detector A. This is due to the strong position correlations between the two photons. A similar explanation holds for object b.

Our experimental setup for the two-object case is sketched in fig. 16. The holographic sorter is created by multiplexing the two spatially non-overlapping objects a and b with reference beams incident at different angles. It is recorded with a collimated HeNe laser at 633 nm on a silver-halide plate. The entangled photon pairs are created by degenerate SPDC in a collinear type-II phase matched BBO crystal pumped by a cw beam from an

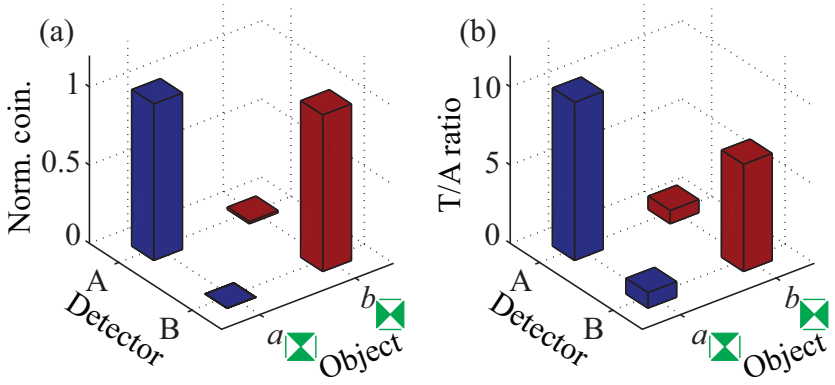

Fig. 17. – Image-identification results for the two-object case. (a) Data for each object-detector combination is normalized by the maximum coincidence count for the corresponding object. (b) T/A ratio is calculated by dividing the total coincidences by the accidental coincidences for each object-detector combination. (Figure adapted from ref. [53].)

argon-ion laser operating at a wavelength of 363.8 nm. The pump beam is well collimated with a divergence of less than 0.31 mrad and a beam waist of 3 mm. A dichroic mirror placed after the crystal blocks the pump laser light. A polarizing beam splitter separates the object photon from the ghost photon. The distance between the crystal and the object (and the ghost image plane) is 45 cm. The imaging condition is met by placing a 10-cm-focal-length lens 15 cm after the crystal. The ghost image plane then acts as a "virtual object" for the hologram. This imaging process is illustrated in fig. 16 with dotted lines for a point object at the crystal. In the unfolded or Klyshko interpretation of the setup [30], one can understand the object as being imaged onto the crystal face, which is then imaged onto the ghost image plane, and consequently imaged onto the hologram. A more detailed theoretical analysis of the imaging process for entangled two-photon fields can be found in ref. [54]. Perkin-Elmer avalanche photodiodes and a coincidence circuit with a window of approximately 12 ns are used for the detection.

When a coincidence count correctly identifies the object, we refer to it as a true case (A-a or B-b), and the opposite as a false case (A-b or B-a). The normalized experimental results for each object are graphed in fig. 17(a). The data for each detector are normalized by the number of coincidence counts recorded by that detector for a true case. It is clear from this figure that our experimental system has high contrast between true and false cases. The ratio between total and accidental coincidence counts (T/A ratio) for each object-detector combination serves as a measure of the system fidelity [52] and is graphed in fig. 17(b).

We repeat this experiment for an object space of four objects. An angularly multiplexed hologram was created for the four spatially non-overlapping objects shown in fig. 18(c) using the same method as before. The image sorting operation of this hologram at high light levels is discussed in the previous section. The normalized coincidence counts and the T/A ratios for each object-coincidence combination are plotted in fig. 18.

Ghost image identification using a holographic sorter clearly has many advantages over other ghost imaging schemes. First, a hologram provides an all-optical method of sorting images that can overcome the limitations of slow CCD frame rates [55]. Second,

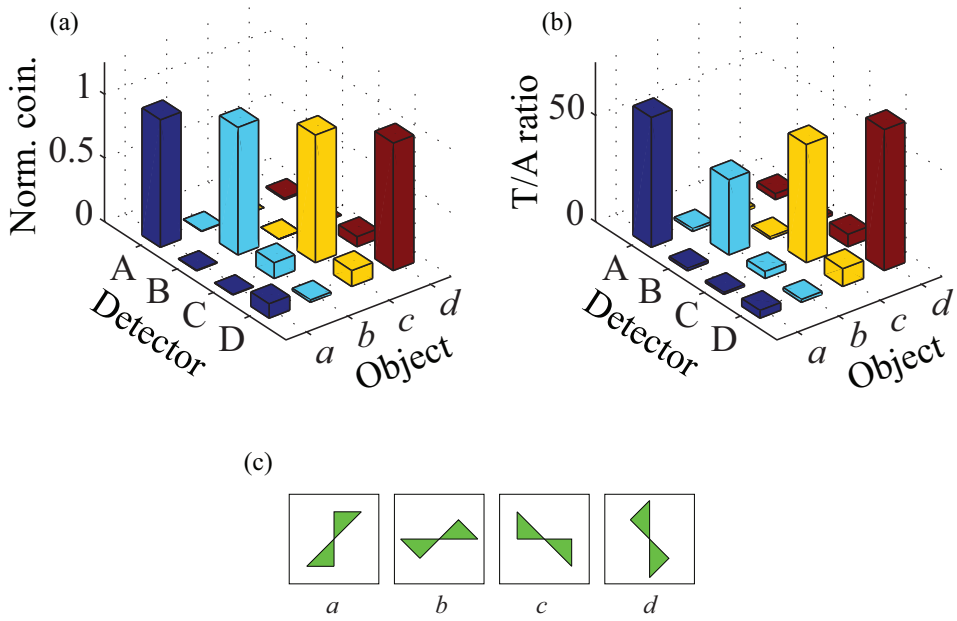

Fig. 18. – (a) and (b) Graphs of ghost-image-identification results for the four-object case. (c) The four spatially non-overlapping objects used in our experiment. (Figure adapted from ref. [53].)

distinguishing among objects of a known set is much faster than building an image pixel by pixel. This approach has practical applications in situations where the objects to be distinguished fall into a relatively small class of objects. Third, an advantage of using quantum ghost image identification appears in the applicability of this method when extremely low light levels are required. One can classify this as a type of "stealth imaging", where a minimum number of photons is used in order to avoid optical eavesdropping or letting the object become aware of its detection. The small number of photons used in quantum ghost image identification make it an excellent candidate for such imaging schemes. When combined with the quantum-secured imaging technique that is discussed in sect. **3**, quantum ghost image identification could prove especially valuable for securely identifying an object while economizing the number of photons used.

Matched filters have been used for pattern recognition for many years [56]. Highly overlapping objects can be sorted with a high confidence factor using matched filters made with holograms [51]. While our experiment addresses only non-overlapping amplitude objects, in principle it is possible to construct matched filters that distinguish among complicated and overlapping objects. However, the efficiency of the identification process is reduced for such sets of objects, and more than one photon pair is needed to distinguish unambiguously among them [57].

In conclusion, we have shown that it is possible to discriminate among non-overlapping objects using a small number of correlated photon pairs, without gaining any spatially resolved information about the objects themselves. Although we have performed this experiment for object spaces of two and four objects, it is possible to expand the size of the object space markedly. Multiplexed holograms have been designed to store as many

as 10000 images [58]. However, as the object space increases, limitations on coincidence counts will be imposed by large crosstalk and low diffraction efficiency. The possibility of using thick holograms to remedy such problems is a topic worth exploring in the future.

5. – High-dimensional quantum key distribution

5˙1. *Introduction*. – Since Bennett and Brassard introduced the first quantum key distribution (QKD) protocol in 1984 [2], the field of QKD has rapidly developed to the extent that QKD systems are commercially available today. Secure transmission of a quantum key has been performed over 148.7 km of fiber [59] as well as over 144 km of free space [60]. One of the limiting aspects of these key distribution systems is that they use the polarization degree of freedom of the photon to encode information [59, 60]. The use of polarization encoding limits the maximum amount of information that can be encoded on each photon to one bit. In addition, it places a low bound on the amount of error an eavesdropper can introduce without compromising the security of the transmission [61]. Because of these limitations, there has been great interest in exploring other ways to encode information on a photon that would allow for higher data transmission rates and increased security [62, 63].

In this section, we report results on the use of orbital angular momentum (OAM) modes of a photon in QKD. The motivation for doing so is that OAM modes span a discrete, infinite-dimensional basis. Hence, there is no limit to how much information one can send per photon in such a system. The large dimensionality of this protocol also provides a much higher level of security than the two-state approach [61]. However, in a practical communication system using OAM modes, the maximum number of modes that can be used is limited by the size of the limiting aperture in the system. This occurs because the radius of an OAM mode increases with the mode number. In this section, we discuss the advantages of increasing the dimensionality of the Hilbert space for a QKD system in detail. Then, we explain how we use holograms to generate the high-dimensional modes we use in our system. A significant part of any quantum communication system is the efficient sorting of single photons carrying information. we describe the approach we use to sort photons carrying OAM. Finally, we describe two high-dimensional QKD systems that use OAM modes for encoding, which we are currently in the process of building. Since our system uses spatial modes, it is highly susceptible to turbulence. Recently, there have been several theoretical studies on how atmospheric turbulence affects OAM modes [64-68]. In addition, many recent experiments have been performed that study the effects of atmospheric turbulence on the channel capacity of an OAM communication channel at high light levels [69-71].

5˙2. *Advantages of high dimensionality*

5˙2.1. Channel capacity of an ideal channel. The amount of information that can be carried by a channel is related to the concept of entropy. Generally, entropy is understood as a measure of disorder in a system. For example, in the context of thermodynamics, the entropy of a glass of ice water increases as its reaches room temperature and the ice melts. Similarly, in information theory, entropy is understood as a measure of randomness of a variable. First applied to the field of communication systems by Claude E. Shannon [72, 73], the *Shannon entropy* of a random variable can be thought of as a measure of its uncertainty *before* we learn its value. Another way of understanding this is in terms of the information gained *after* learning the value of the variable. The

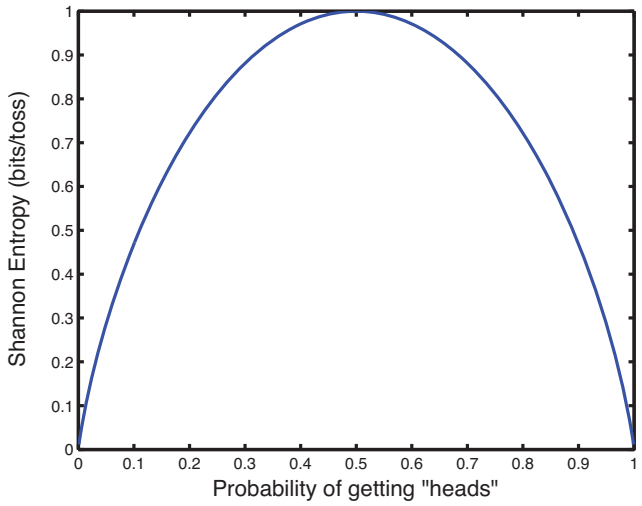

Fig. 19. – Shannon entropy of a coin toss as a function of fairness.

Shannon Entropy is defined as

$$H(X) = H(p_1, \ldots, p_N) = -\sum_n p_n \log_2(p_n), \tag{27}$$

where p_n is the probability of the n-th outcome of the variable X. A simple example is a coin toss. A fair coin has equal probability of resulting in a "heads" or "tails" outcome. This results in a maximum entropy of 1 as follows:

$$H(X) = H(p_{\text{heads}}, p_{\text{tails}}) = -(0.5 \times \log_2(0.5) + 0.5 \times \log_2(0.5)) = 1\,\text{bit}. \tag{28}$$

If the coin we are using is unfair such that it has a 3/4 probability of resulting in "heads" and 1/4 probability of resulting in "tails", its Shannon entropy is reduced to 0.81 as follows:

$$H(X) = -(0.75 \times \log_2(0.75) + 0.25 \times \log_2(0.25)) = 0.8113\,\text{bit}. \tag{29}$$

The plot in fig. 19 shows the entropy of a coin toss as a function of the fairness of the coin (the probability of getting "heads"). A fair coin has a 0.5 probability of getting "heads" in a toss. In the limits of a completely unfair coin, the entropy goes to zero. This makes sense if you think of the entropy in terms of the *information gained*. If the coin toss always results in the same outcome, no net information is gained. Another way of understanding this definition of entropy is in terms of the resources needed to store information. For a 50-50 fair coin, we need at least 1 bit per toss to store this information. For an unfair coin as shown in eq. (3), we need at least 0.8113 bit per toss to store the information.

Now lets extend this idea to a communication channel. Imagine a channel where the sender encodes a message by picking "heads" or "tails" on a coin and then sending the

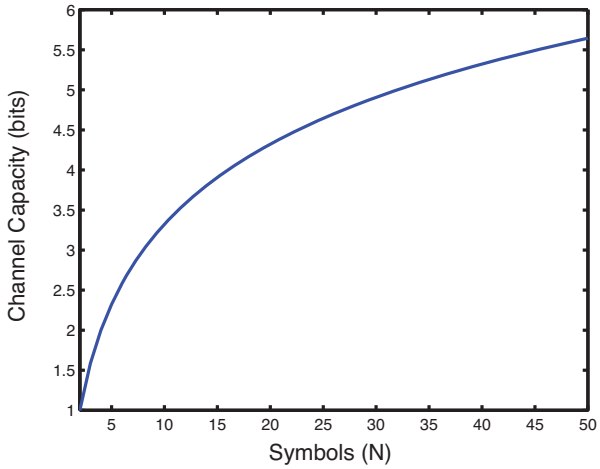

Fig. 20. – Channel capacity of a communication channel as a function of the number of symbols N.

coin to the receiver. A completely random message can be thought of as the result of many tosses of a fair coin. A communication channel employing such a 2-symbol encoding can then at most carry 1 bit of information. If the channel is biased towards one result (*i.e.* the coin is unfair), the amount of information that can be carried by this channel is reduced from 1 bit. For now, lets consider an ideal channel that employs an N-symbol encoding, with each symbol being equally likely to occur ($p_n = 1/N$). The maximum amount of information that such a channel can carry is given by simplifying eq. (27):

$$H(X) = -\sum_N \frac{1}{N} \log_2 \left(\frac{1}{N}\right) = \log_2(N). \tag{30}$$

As shown in fig. 20, the channel capacity increases logarithmically as a function of the number of symbols, or the channel dimension, N. As mentioned in the introduction above, QKD systems conventionally use the polarization degree of freedom of a photon for encoding. Polarization is inherently a two-dimensional state space, as there are only two orthogonal polarizations in any given polarization basis (for *e.g.*, horizontal and vertical, or left-circular and right-circular). For polarization, the maximum channel capacity is then limited to $\log_2(2) = 1$ bit/photon. However, for an OAM-based QKD system employing 25 OAM modes, the channel capacity is increased to $\log_2(25) = 4.64$ bits/photon, which is almost 5 times the capacity of the polarization-based system!

5˙2.2. Enhanced security in QKD. As explained in sect. **2**, a QKD link between two parties (Alice and Bob) is susceptible to eavesdropping. However, due to the quantum no-cloning theorem [1], an eavesdropper (Eve) cannot perfectly replicate a quantum system without destroying it. Thus, an eavesdropper using the simplest form of eavesdropping —intercept and resend— will introduce statistical errors in the channel that can be measured by Alice and Bob. For this reason, Alice and Bob must attribute all errors in their channel to Eve. If their measured error rate is equal to or higher than that

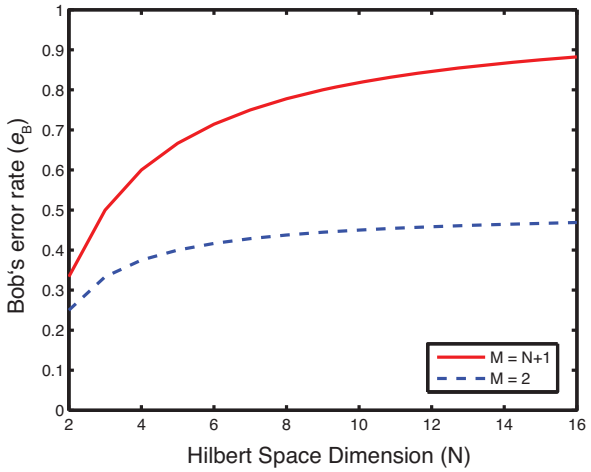

Fig. 21. – Bob's allowed error rate for an intercept-resend eavesdropping attack as a function of system dimension N for $M = 2$ MUBs (dashed blue line) and the maximum of $M = N + 1$ MUBs (solid red line).

expected from an eavesdropper using a known method of eavesdropping, their protocol is no longer secure and they must abandon it.

In sect. **3**, we discuss the error bound for a polarization-based quantum-secured imaging system in detail ($e_B < 25\%$). Similarly in polarization-based QKD, if Alice and Bob measure an error rate greater than or equal to 25%, they must abandon their protocol. However, it is important to note that this error rate was derived for a QKD system using two mutually unbiased bases (MUBs). In general, the maximum number of MUBs in an N-dimensional QKD system is equal to $N + 1$, for when N is a prime number [74]. For the polarization-based implementation of the BB84 protocol [2], N is equal to 2 and there are three available MUBs —the horizontal-vertical (HV) basis, the diagonal-anti-diagonal (DA) basis, and the left-circular-right-circular (LR) basis. A polarization-based QKD system can use all three MUBs for encoding. Such a protocol is referred to as the "six-state protocol" [75]. The use of three instead of two MUBs has two effects. First, the data rate drops by 50%. This is because Alice and Bob will now prepare and measure in the same MUB only 1/3 of the time (as opposed to 1/2 the time) and will discard 2/3 of the data in the sifting process. Second, the error bound increases from 25% to 33%. This is because Eve has a higher probability of measuring in the wrong MUB now that there are three MUBs, and hence has a higher probability of introducing errors in the transmission.

In general, the error bound for an intercept-resend attack in an N-dimensional system with M MUBs in given by [61]

$$e_B(N, M) = \left(1 - \frac{1}{M}\right)\left(1 - \frac{1}{N}\right). \tag{31}$$

Using this equation, we plot the error bound for an intercept-resend eavesdropping attack as a function of system dimension for $M = 2$ MUBs (dashed blue line) and the maximum of $M = N + 1$ MUBs (solid red line) in fig. 21. It is clear that the allowed error rate

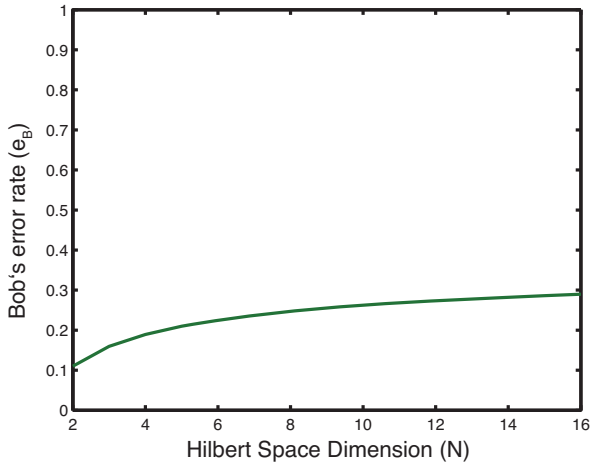

Fig. 22. – Bob's allowed error rate for finite coherent eavesdropping attacks as a function of system dimension N. The allowed error rate is independent of the number of MUBs used.

goes up markedly with system dimension. For very large N, the error rate goes to 0.5 and 1.0 asymptotically for these two cases. Clearly, using more MUBs is beneficial for security, but has an adverse effect on data rates.

While the allowed error rate can be quite high for intercept-resend attacks on high-dimensional QKD systems, a stricter bound is imposed on the error rate in the case of finite coherent eavesdropping attacks. In these attacks, Eve coherently manipulates a finite number of qudits in order to gain information about the key [76]. While the details of such attacks are outside the scope of this article, the error introduced by them on a QKD system follows the inequality [61]

$$(1 - e_{\mathrm{B}}) \log(e_{\mathrm{B}}) + e_{\mathrm{B}} \log\left(\frac{e_{\mathrm{B}}}{N-1}\right) > -\frac{1}{2}\log(N). \tag{32}$$

Notice that in contrast with intercept-resend attacks, the error rate for coherent attacks depends only on system dimension N and is independent of the number of MUBs, M. This equation can be numerically solved to produce values of the error bound e_{B} as a function of system dimension N. We used the "FindInstance" function in Mathematica to find values of the error bound, which are plotted in fig. 22. As can be seen, the allowed error rate for coherent attacks is indeed much stricter than that allowed for intercept-resend attacks. However, even in this case, there is a clear increase in the allowed error rate for larger system dimensions, N. For example, the allowed error rate for 16 modes is equal to 0.29, as opposed to 0.11 for 2 modes. This serves as ample motivation for using a high-dimensional encoding scheme for QKD such as that of OAM.

5˙3. *Generating OAM and ANG modes.* – Since OAM modes have a helical phase, a straightforward way of generating beams carrying OAM is by using a phase plate whose optical thickness varies in a similar fashion. These so called "spiral phase plates" are commercially available today but are quite expensive, costing upwards of a thousand dollars per plate. This is because of the high precision required to manufacture them. In

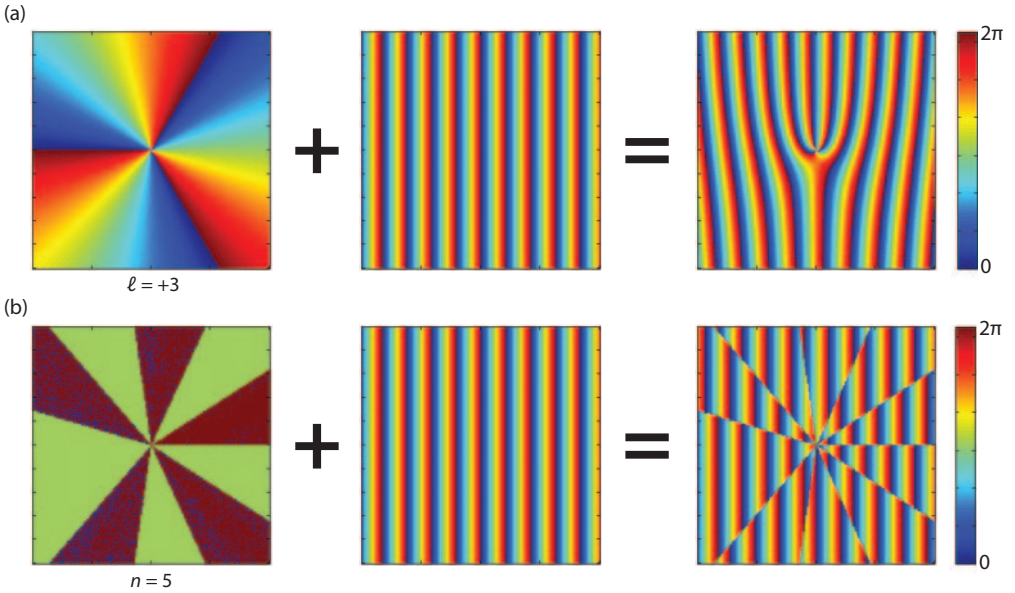

Fig. 23. – Phase profiles showing the addition of (a) an OAM mode with $\ell = +3$ with a plane wave mode generating a forked hologram and (b) an ANG mode with $n = 5$ ($N = 11$) with the same plane wave mode generating an ANG hologram. Holograms like these are implemented on spatial light modulators (SLMs) to generate arbitrary superpositions of OAM and ANG modes.

order to create an $\ell = \pm 1$ spiral phase plate, for example, one must create a refractive index variation in glass that varies as $\lambda\theta/\pi$, where θ is the azimuthal position. Due to this manufacturing difficulty, there has been increased interest in the development of other techniques for generating OAM modes. Here we describe the technique of holography, which is the one we use in our lab.

As explained in sect. **4**, a hologram is formed by interfering two wavefronts. One of these wavefronts is usually a plane wave incident at a particular angle, and is conventionally referred to as the reference beam. The second wavefront can take on any structure. The interference pattern between these two wavefronts is written onto a holographic material, which is then developed to form a permanent hologram. In sect. **4**, we used such a hologram as an image sorter. In this process, the second (more complicated) wavefront is sent through the developed hologram, producing a wavefront propagating in the direction of the original reference beam. One can easily flip this procedure around and use the same hologram to create the second complicated wavefront. This is carried out by sending a plane wave at the exact angle of the original reference beam, which interferes with the hologram to create the original, complicated wavefront.

In this manner, we can create a hologram that can be used for generating an arbitrary superposition of OAM modes. In fig. 23(a), we show the phase profiles of an $\ell = +3$ OAM mode, a plane wave, and the their sum (mod 2π). The OAM mode phase winds around the center of the beam with three 2π jumps, as expected. The phase of the plane wave mode resembles a linear grating. The combined phase shows a peculiar phase structure at its center. This is commonly referred to as a "forked" hologram. First proposed in 1992 [77], it is a standard method for generating beams with phase singularities or OAM

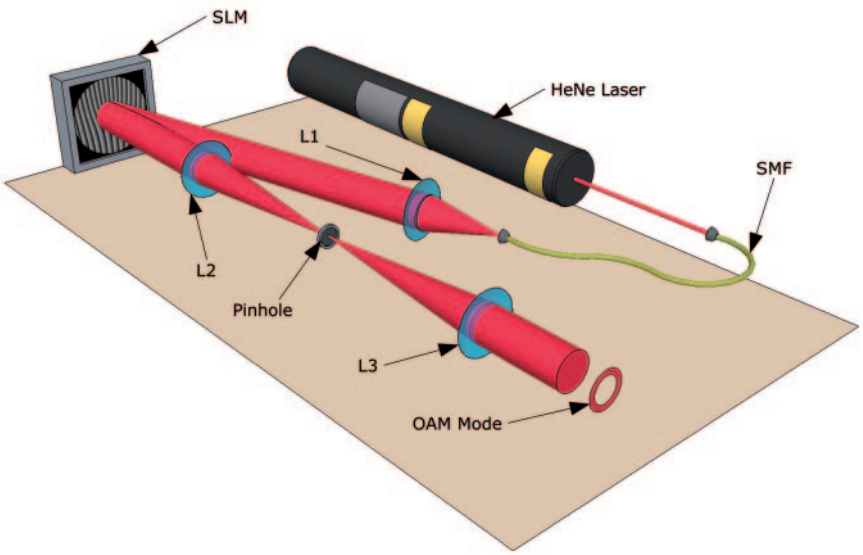

Fig. 24. – System used for generating an arbitrary superposition of OAM modes. A spatially filtered and collimated HeNe laser beam is incident on a "forked" diffraction hologram implemented on an SLM. A $4f$ system of lenses (L2 and L3) along with a pinhole is used to remove background noise from the SLM. The OAM mode is obtained in the image plane of the SLM.

beams. The number of dislocations in the fork corresponds to the azimuthal quantum number of the OAM mode. For a negative OAM mode, the fork is upside down. When a plane wave is incident on such a hologram at the angle of the original plane wave or "blaze" of the hologram, an OAM mode with $\ell = 3$ is generated propagating normal to the hologram. A similar hologram can be used for generating angular position (ANG) modes, which are simply a complex superposition of OAM modes that resemble a wedge rotating around the center of the beam (see sect. **1** for a detailed discussion). The set of ANG modes formed by combining 11 OAM modes is given by

$$\Theta_n = \frac{1}{\sqrt{11}} \sum_{\ell=-5}^{5} \Psi_\ell \exp\left(\frac{i2\pi n\ell}{11}\right). \tag{33}$$

As can be seen above, this set is formed by coherently adding OAM modes with an azimuthal quantum number $\ell \leq \pm 5$. One should note that the coefficient for each OAM mode in this superposition is equal, which is what makes the basis of ANG modes mutually unbiased with respect to the OAM basis. Specifically, if an ANG mode photon is measured in the OAM basis, it has an equal probability to appear in any of the component OAM modes, and vice versa. A hologram used for generating an ANG mode with $n = 5$ is shown in fig. 23(b).

In our experiment, we generate OAM and ANG modes by implementing such holograms on a Holoeye PLUTO phase-only spatial light modulator (SLM) in conjunction with a $4f$ system of lenses [78, 79]. A schematic for this system is shown in fig. 24. A HeNe laser is spatially filtered through a single mode fiber (SMF) and collimated by a lens (L1). This collimated, Gaussian beam is incident on an SLM with a forked diffrac-

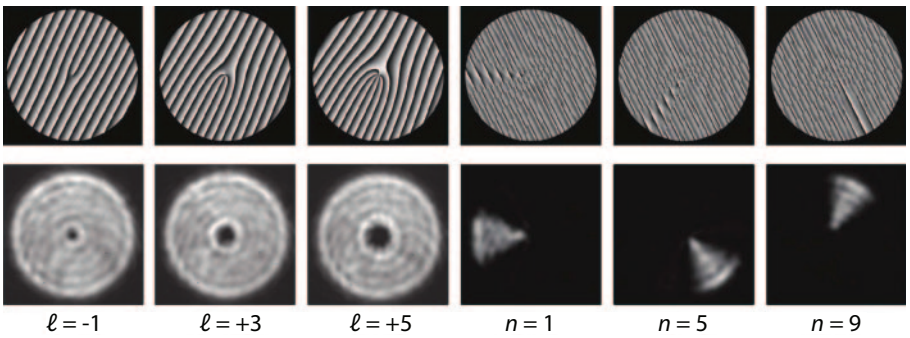

Fig. 25. – Upper row: Holograms written onto the SLM to generate OAM and ANG modes. Lower row: CCD images of the corresponding modes generated. These are OAM mode numbers $\ell = -1$, 3, and 5, and ANG mode numbers $n = 1$, 5, and 9. (Figure redrawn from [69], © 2012 The Optical Society.)

tion grating as shown in fig. 23(a). The beam diffracts off the SLM and is sent through a $4f$ system of lenses (L2 and L3) with a pinhole in between the two lenses. The purpose of this pinhole is to pick out the first diffracted order of the blazed hologram. The reason for doing so is that the zeroth order contains a lot of noise in the form of unwanted reflections from the SLM. A primary contributor to this is the periodic gap between SLM pixels, which also acts like a diffraction grating. By blazing the hologram in both x and y and picking off the first order of diffracted light in the Fourier plane, we eliminate this background noise [78]. Figure 25 shows some of the holograms we use in our setup and CCD images of the OAM and ANG modes generated by them.

5˙4. *Sorting OAM and ANG modes.* – One of the key hurdles to using OAM modes to perform QKD has been the need of a method of efficiently sorting single photons carrying OAM modes. This problem has eluded the scientific community for over a decade. A standard method for measuring the OAM content of a photon has been to project out each OAM mode. This procedure simply involves using the forked diffraction grating backwards (similar to the image sorter in sect. **4**). An OAM mode with $\ell = +2$ incident on a forked diffraction grating with $\ell = -2$ will generating a plane wave (with $\ell = 0$) traveling in a specific direction. When sent through a lens, this plane wave will produce a peak at $p = 0$. Any other OAM mode with $\ell' \neq +2$ sent through the same forked diffraction grating will *not* produce a plane wave, instead generating an OAM mode with $\ell'' = \ell' - 2$. This OAM mode, when Fourier transformed by a lens, will have a null at $p = 0$ (the Fourier transform of an OAM mode is also an OAM mode). By placing a small aperture or fiber at the focus of this lens, a forked hologram can be used to test for a particular OAM mode. However, this procedure destroys the photon under test, and is thus limited to an efficiency of $1/N$, where N is the number of OAM modes to be measured.

The first method for efficiently sorting photons carrying OAM used a set of rotated Dove prisms in the arms of a Mach-Zehnder interferometer (MZI) [80]. In this interferometric method, photons with even ℓ were obtained from one MZI port, while photons with odd ℓ were obtained from the other. By cascading such OAM "parity" checking MZIs, and cleverly inserting OAM parity shifting spiral phase plates (or holograms) between them, this method could, in principle, be used to efficiently sort single photons carrying

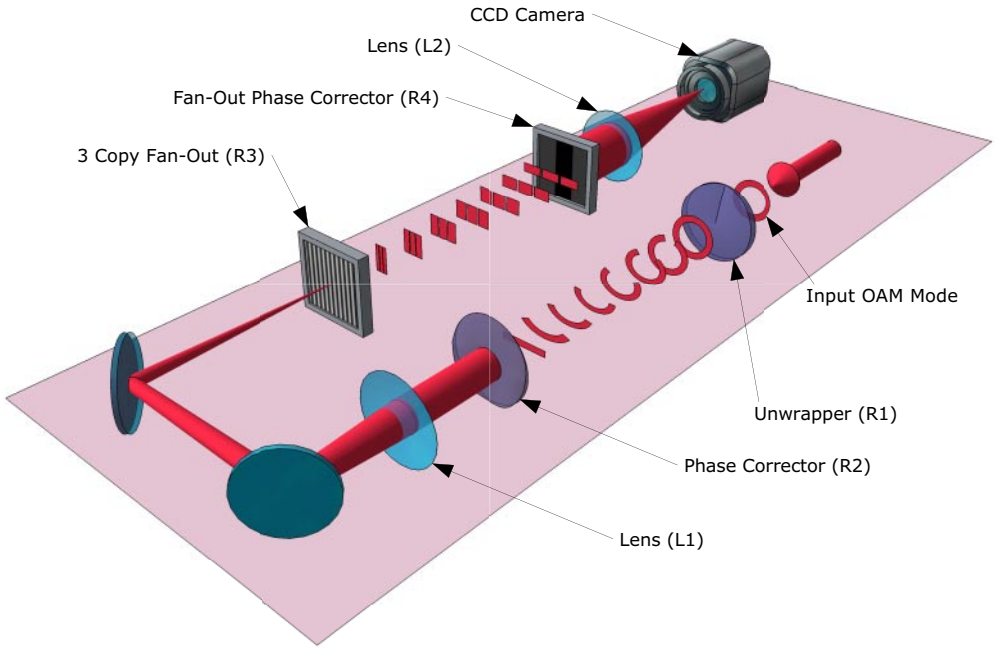

Fig. 26. – A schematic illustrating the OAM mode sorting procedure. The unwrapper element (R1) unwraps the helical phase of an input OAM mode, transforming it into a finite-sized plane wave mode with a tilt. The phase corrector element (R2) removes residual aberrations introduced during the mode transformation. A lens (L1) converts the tilted plane wave modes into somewhat spatially separated position modes. A fan-out element (R3) implemented on an SLM creates 3 adjacent copies of the finite plane wave mode, albeit with a phase offset between them. A final fan-out phase corrector element (R4) removes this phase offset between the copies. A lens (L2) then focus these larger plane wave modes into well separated position modes at the CCD camera (figure adapted from [84]).

OAM. However, the problems associated with this method are almost obvious —besides the problem of scaling to large OAM dimensions, the use of many optical components would reduce the efficiency of the method by absorption of photons.

Clearly, a more elegant solution was required, which was introduced recently by a method that uses a geometric transformation to convert an OAM mode with an azimuthal phase variation $e^{i\ell\phi}$ to a tilted plane wave mode with a position phase variation $e^{i\ell x}$ [81]. The tilt of the plane wave mode is proportional to the OAM quantum number ℓ of the OAM mode. In this manner, OAM modes can be sorted by first converting them into tilted plane waves, and then Fourier transforming the plane waves into separated position modes. Two custom refractive elements [82] are used to optically map polar coordinates (r, φ) in the input plane to rectilinear coordinates in the output plane (x, y) via the log-polar mapping $x = a(\varphi \bmod 2\pi)$ and $y = -a\ln(r/b)$. Here, a and b are scaling constants that define the size of the converted mode [83]. The first element, the *unwrapper* (R1), maps intensities according to the coordinate transformation. A second

element, the *phase corrector* (R2), corrects a residual aberration. Thus, optical waves with helical phase fronts are transformed into tilted plane waves, which can be sorted at the focus of a lens. This process is illustrated in fig. 26 for one input OAM mode.

The two custom elements used in our setup were diamond machined with a Nanotech 3 axis ultra precision lathe in combination with a Nanotech NFTS6000 fast tool servo [82]. The program used for the machining was written with DIFFSYS, which is a commercially available software. The program converted the input data given by a set of Cartesian coordinates (x, y, z) into files usable by the lathe and servo tools. The optical thickness of the first, unwrapping element can be written as a function of (x, y) as

$$Z_1(x,y) = \frac{a}{f(n-1)}\left[y\,\arctan(y/x) - x\ln(\sqrt{(x^2+y^2)}/b) + x - \frac{1}{2a}(x^2+y^2)\right]. \tag{34}$$

Here, f is the focal length of the lens integrated into both elements. This lens performs the Fourier transform operation that is required between the unwrapping and phase correcting procedures [81]. The two free parameters, a and b, dictate the size and position of the transformed beam. The optical thickness of the second, phase correcting element can be similarly written as

$$Z_2(x,y) = -\frac{ab}{f(n-1)}\left[\exp\left(-\frac{u}{a}\right)\cos\left(\frac{v}{a}\right) - \frac{1}{2ab}(u^2+v^2)\right]. \tag{35}$$

Here, u and v are spatial Cartesian coordinates in the output plane. The distance between these two elements must be exactly f, and the elements must be aligned precisely along the same optical axis. For this reason, they are mounted in a cage system with fine position and rotation controls. A schematic of the optical thickness in 3D as well as photographs of the elements used in our setup is shown in fig. 27.

While this method is substantially better at sorting OAM modes than previous methods, it is still limited to working approximately 80% of the time [82]. In other words, for a photon with OAM $\ell\hbar$, there exists an approximately 20% probability of detecting it with OAM $m\hbar$, $m \neq \ell$. This is because the "unwrapped" plane wave has a finite extent, which results in a diffraction limited spot at the focus of a lens. These spots have about 20% overlap with neighboring spots, and hence about 20% crosstalk. Clearly, this is not good enough for QKD, as any errors must be attributed to an eavesdropper. If we get an error 20% of the time, this already places a strict bound on the allowed environmental error our system can handle. Further, it reduces the benefits of going to a higher-dimensional state space.

In two recent papers [84,85], we showed that the technique of Berkhout *et al.* [81] can be combined with a holographic beam-splitting technique to sort OAM modes with only about 5% crosstalk. The principle behind our method is straightforward —by generating multiple, adjacent copies of the transformed plane wave mode, we increase its effective size. When this larger plane wave is sent through a lens, it is Fourier transformed into a smaller spot than before. More specifically, the spot size is reduced by N, where N is the number of copies. The *fan-out* element introduced in ref. [86] is a phase grating designed to diffract an incoming beam into N uniformly spaced orders, each having the same spatial profile and equal energy. For perfect beam splitting, an optical element has

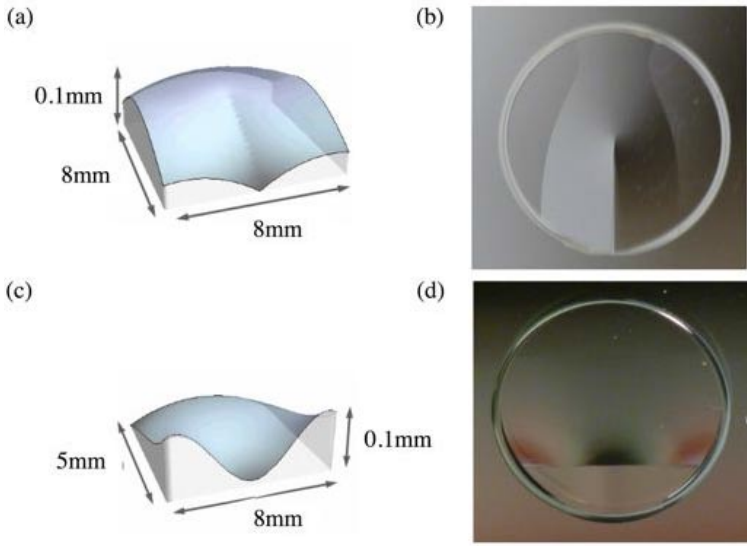

Fig. 27. – (a) and (c) Schematics showing the optical thickness of the two elements R1 and R2 as a function of position. (b) and (d) Photographs of the two elements R1 and R2 used in our setup, machined out of PMMA. (Figure redrawn from [82], © 2012 The Optical Society.)

to transform an incoming plane wave into a field distribution given by

$$U(x,y) = \sum_{m=1}^{N} A_m e^{i\phi_m} e^{-i2\pi s_m x/\lambda}, \tag{36}$$

where A_m is the amplitude, ϕ_m is the phase, and s_m is the angle of propagation of the N copies. The fan-out element (R3) is the optimal design in the family of phase-only holograms which can approximately achieve this task [87]. Generally, the fan-out element introduces a relative phase ϕ_m between the different copies. These are removed with a *phase-correcting* element (R4) in the Fourier plane of the fan-out element (fig. 26). The multiple copies are then Fourier transformed with a lens to a narrower spot than before. This process is illustrated in fig. 26 for a 3 copy fan-out. Using the specific values of A_m and ϕ_m given in refs. [86, 87], we can achieve an efficiency of more than 99% while splitting the beam into nine copies. The one-dimensional phase profiles of the 3 and 9 copy fan-out holograms are plotted in fig. 28(a) and (b) respectively.

The same fan-out procedure can be used for sorting ANG modes as well [84, 85]. In this case, the plane of the first phase correcting element (R2) is imaged onto the plane of the fan-out (R3). Figure 29 shows simulation results comparing the fan-out enhanced OAM and ANG mode sorter with the previous versions of the sorter without the fan-out [81, 82]. The decrease in the lateral size of the sorted position modes, and hence the crosstalk, is very clear. We have experimentally tested our sorting method for 25 OAM modes ($\ell = \pm 16$) and 25 ANG modes. The crosstalk matrices for both of these cases are shown in fig. 30(a) and (b). One can see how the sorting process starts to break down for OAM modes with large ℓ. For a mode number of $N = 25$, we were able to achieve a mutual information of 4.16 bits/pulse in the ANG basis and 4.18 bits/pulse in

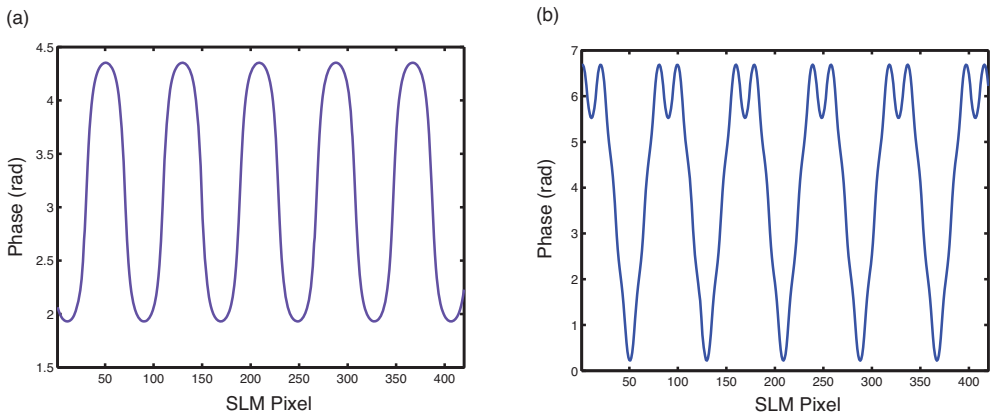

Fig. 28. – One-dimensional phase profiles of the fan-out holograms used for creating (a) 3 copies and (b) 9 copies. The profiles show a section (420 pixels) of the SLM.

the OAM basis. The ideal mutual information for 25 modes is equal to $\log_2(25) = 4.64$ bits/pulse, which goes to show how close we are to the theoretical limit. In our test, we made measurements at high light levels using a HeNe laser and a Canon 5D Mark III

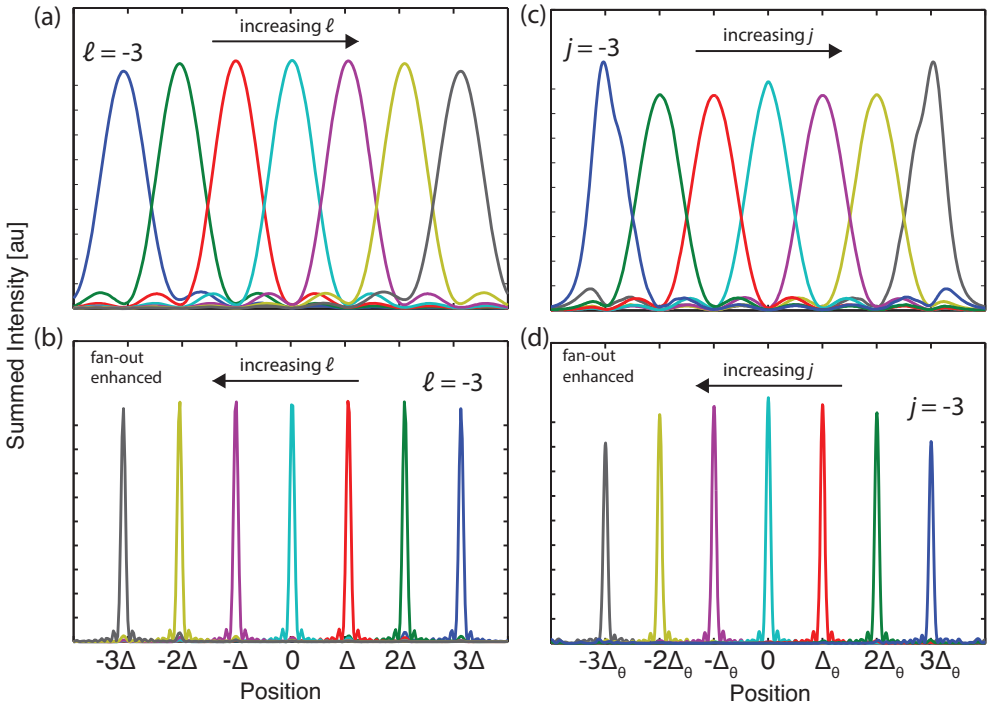

Fig. 29. – Simulation results comparing (a) the output from the OAM sorter with (b) the output from the fan-out-enhanced OAM sorter for 7 input OAM modes and comparing (c) the output from the ANG sorter with (d) the output from the fan-out-enhanced ANG sorter for 7 input ANG modes. Different colors correspond to different modes. The number of copies produced by the fan-out element is 9. (Figure redrawn from [85], © 2012 The Optical Society.)

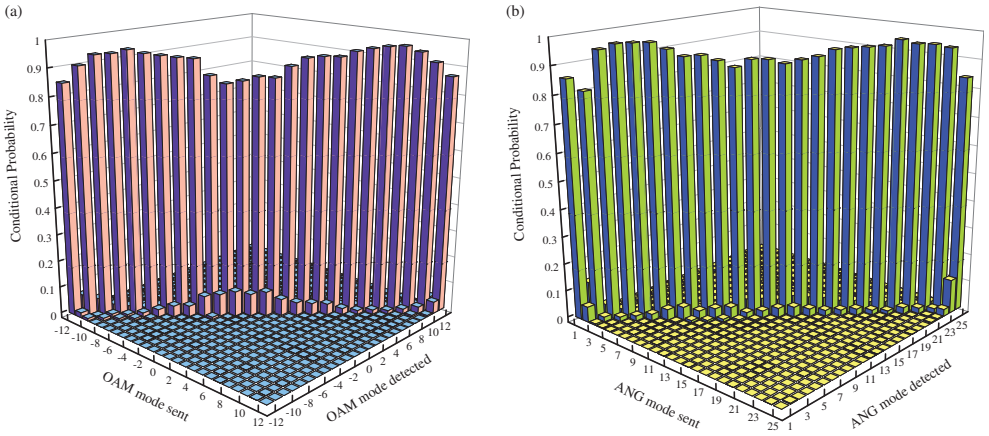

Fig. 30. – Experimental results showing the intermodal crosstalk of a fan-out enhanced OAM and ANG mode sorter. The sorter is tested for 25 OAM modes and 25 ANG modes (figure adapted from [84]).

camera. In principle, this can be extended to the single photon level with an appropriate multi-pixel single photon detector.

5˙5. *Proposed high-dimensional QKD systems.* – In this section, we describe two types of OAM-based QKD systems that could be built using the procedures for generating and sorting OAM and ANG modes explained above. The first is based on a high-dimensional version of the BB84 protocol [2], which uses two pairs of orthogonal polarization states in two mutually unbiased bases (MUBs) for encoding. The second is a high-dimensional variant of the Ekert protocol [12], which relies on the quantum correlations between two polarization-entangled photons for security. We also describe the progress we are making towards implementing the BB84-based OAM-QKD system in our lab. In the next section, we discuss the limitations of our current system.

5˙5.1. BB84 OAM-QKD with weak coherent pulses. As explained earlier in this section, using more than two dimensions for encoding in QKD also increases the number of possible MUBs one can use. Using more than two MUBs results in increased security, but a reduced key generation rate. For this reason, we are restricting ourselves to the two high-dimensional MUBs of OAM and ANG, introduced in sect. **1**. A schematic of our proposed QKD system is shown in fig. 31. We use a HeNe laser modulated by an acousto-optical modulator (AOM) as our source. By adjusting the duration of the driving pulse, we can use the AOM to carve out pulses of light containing less than one photon on average. Due to the Poissonian statistics followed by coherent states, a highly attenuated laser pulse will always contain more than one photon with some probability. This opens up such a system to eavesdropping using photon-number splitting (PNS) attacks [88]. In the simplest version of the PNS attack, an eavesdropper can insert a beam splitter into the channel and probabilistically split off a photon from pulses containing more than one photon. As all photons in the same pulse encode the same qubit, Eve can gain information about the qubit without destroying it or revealing herself. It is important to note that in general, multi-photon pulses do not necessarily undermine the security of a QKD system. However, they do limit the key generation rate, as more bits must be discarded during the privacy amplification process [89].

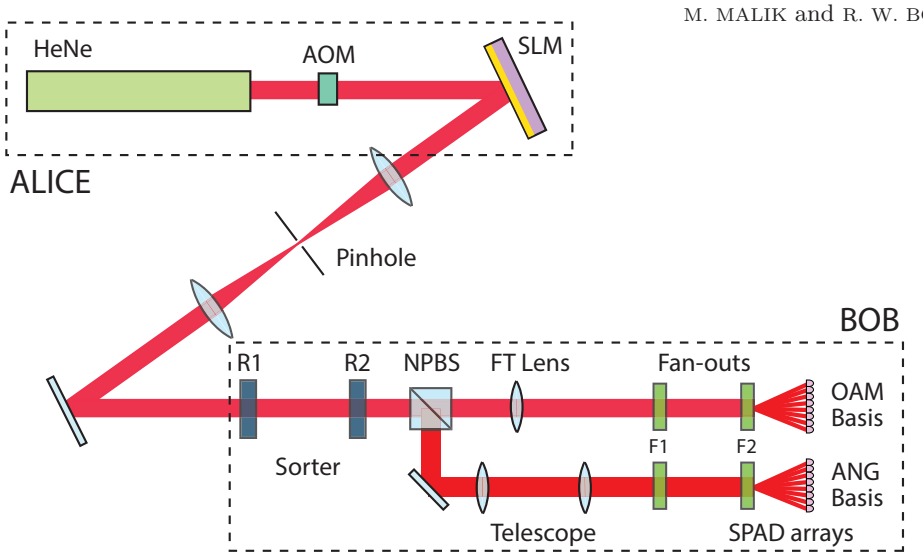

Fig. 31. – Proposed high-dimensional QKD setup using the BB84 protocol. Our source is a HeNe laser operating at 633 nm that is modulated by an acousto-optic modulator (AOM) to carve out pulses containing an average number of photons dictated by the decoy state protocol. These pulses are tailored into OAM and ANG modes by a spatial light modulator (SLM) and $4f$ system. R1 and R2 are custom refractive elements used to transform the OAM and ANG modes into plane wave modes. F1 and F2 are fan-out and phase correcting elements used to enhance the sorting process. A beam splitter (NPBS) acts as a passive basis selector between the OAM and ANG bases. The transformed modes are detected with arrays of single photon avalanche detectors (SPADs).

Recently, a variation to the BB84 protocol was proposed which uses a simple technique to counter PNS attacks. In this technique, known as the decoy state protocol [28], Alice prepares an additional set of "decoy" states by randomly varying the number of photons in each pulse. She also randomly chooses which pulses will be used as signal states and which as decoy states. Thus, both the signal and the decoy states consist of pulses containing a varying distribution of average photon number that is known to Alice. The security lies in the fact that given a single n-photon pulse, Eve has no way of knowing whether it originated as a signal or decoy. Thus, any attempt by Eve to remove photons from a pulse will occur with the same probability for a signal as well as a decoy state. However, since these two kinds of states have different photon number statistics, the effect of removing a photon is different on both. By sharing the decoy state information after the sifting process, and measuring the ratio of the number of detection events to the number of signals originally sent for each kind of state, Alice and Bob can detect any PNS attacks by Eve with a high probability. This protocol has been implemented with many different intensities of decoy states [90,91]. However, the protocol using two states —the vacuum and weak decoy state— has been shown to be optimal [92].

In our proposed QKD system, we modulate the intensities of our pulses according to this protocol. The AOM is used to carve out pulses with varying intensities. Following the AOM, a spatial light modulator (SLM), a pinhole, and a $4f$ system of lenses are used for impressing OAM or ANG mode information onto each pulse (fig. 31). The $4f$ system also images the SLM onto Bob's first detection plane at R1. Bob uses the sorting procedure explained earlier in this section to measure a pulse either in the OAM

or ANG basis. The non-polarizing beam splitter (NPBS) acts as a passive selector of Bob's measurement basis, randomly measuring pulses in either the OAM or ANG basis. The same mode transforming elements (R1 and R2) are initially used to transform both OAM and ANG modes. Following the NPBS, two sets of fan-out elements (F1 and F2) carry out the beam-copying process for each basis. For the OAM basis, the output of R2 is Fourier transformed by a lens (FT Lens) onto the fan-out element F1. For the ANG basis, the output of R2 is imaged by a telescope system onto the fan-out element F1. Following the phase-correcting elements (F2), two sets of single photon avalanche detector (SPAD) arrays are used for detecting the photon states.

After Bob completes his measurements in the OAM and ANG bases, our high-dimensional protocol follows the standard steps of the BB84 protocol. Alice and Bob share their encoding and measurement basis choices with each other over a public channel. Using this information, they sift out the states where Bob did not measure in the preparation basis used by Alice. Following this, Alice and Bob perform the procedures of error correction [93] and privacy amplification [94]. Both these procedures merit detailed discussion. However, these topics are outside the scope of this article. After privacy amplification, Alice and Bob will share a secure key with enhanced security and an increased generation rate via the use of a high-dimensional Hilbert space. An experimental implementation of such a QKD protocol that achieved 2.1 bits/photon with 7 OAM and ANG modes was recently published on the arXiv by our group [95].

5˙5.2. Ekert OAM-QKD with entangled photons. The second proposed high-dimensional QKD system is based on an extension of the Ekert protocol [12] to a high-dimensional Hilbert space. As explained in sect. **2**, the security of the Ekert protocol relies on the strong quantum correlations shared by two members of an entangled pair. An eavesdropper trying to access information in this protocol disturbs these correlations, which can be quantified through entanglement measures such as the CHSH inequality [10] or the Schmidt number [96]. Bennett and Brassard argued that the Ekert protocol was formally identical to the BB84 protocol, and thus entanglement was not necessary to perform QKD. While this is true, the Ekert protocol simply provides an alternative method to do QKD in a different architecture —the source is spatially separated from Alice and Bob. Also, a subtle yet important difference is that there is no active state preparation in the Ekert protocol. Alice and Bob simply rely on the probabilistic nature of wave function collapse to assign a bit value to their measured state. For example, a D-polarized photon encountering a polarizing beam splitter probabilistically goes into either the H or the V port. This removes certain technological requirements from Alice, as she no longer needs to employ expensive equipment such as a series of Pockels cells in order to create specific polarization states. On the contrary, of course, the Ekert protocol does require a maximally polarization-entangled state, which is fast becoming available cheaply, and is used even at the undergraduate laboratory level [97].

To perform high-dimensional OAM-based QKD with the Ekert protocol, we require a bright source of photons maximally entangled in OAM [98]. The state of OAM-entangled photons generated in spontaneous parametric downconversion (SPDC) can be written as

$$|\Psi\rangle = \sum_{\ell=-\infty}^{\infty} c_\ell |\ell\rangle_A |-\ell\rangle_B, \tag{37}$$

where ℓ is the azimuthal quantum number, c_ℓ is the probability amplitude, and A and B refer to the signal and idler photon, respectively. As can be seen, OAM-entangled

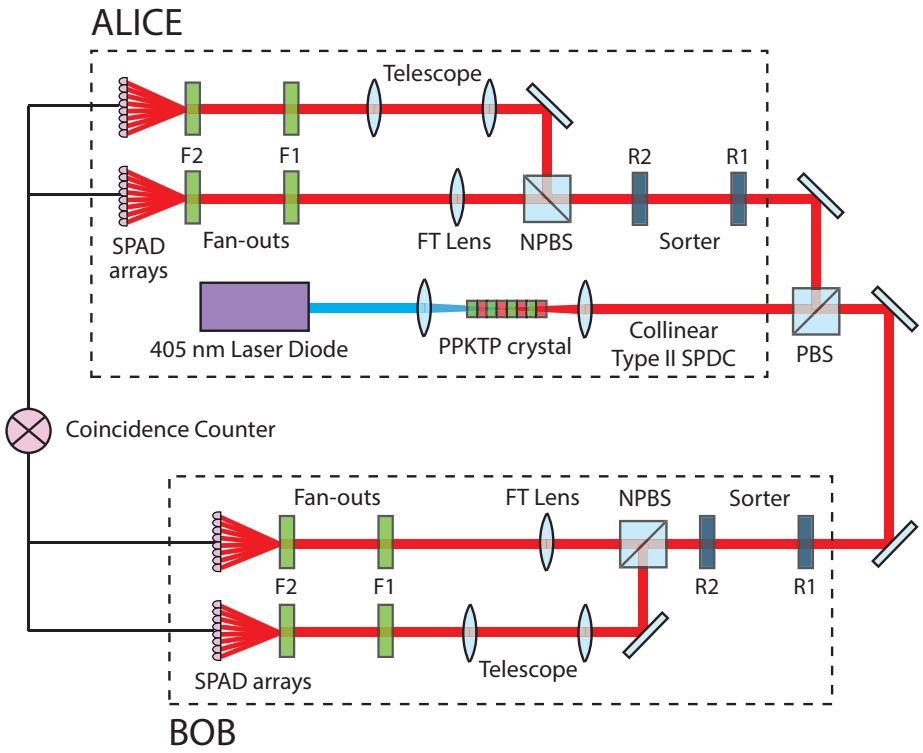

Fig. 32. – Proposed high-dimensional QKD setup using the Ekert protocol. Our source is a diode laser operating at 405 nm that pumps a periodically poled Potassium Titanyl Phosphate (PPKTP) crystal to generate type II downconverted photons at 810 nm exhibiting OAM entanglement. A polarizing beam splitter (PBS) separates the signal from the idler, directing one to Alice and the other to Bob. Alice and Bob use a similar detection setup as in the BB84 protocol (fig. 31). R1 and R2 are custom refractive elements used to transform the OAM and ANG modes into plane wave modes. F1 and F2 are fan-out and phase correcting elements used to enhance the sorting process. A beam splitter (NPBS) acts as a passive basis selector between the OAM and ANG bases. The transformed modes are detected with arrays of single photon avalanche detectors (SPADs). Alice and Bob's SPAD arrays are connected with a coincidence counting circuit to ensure that only photons from the same entangled pair result in a signal.

photons are anti-correlated in OAM. Thus, if one photon of an entangled pair is measured to have an OAM of $+3\hbar$, its entangled partner photon must have an OAM of $-3\hbar$. For any realistic SPDC source, the OAM bandwidth (spiral bandwidth) does not extend to $\pm\infty$. This is because of the physical apertures in the system and finite size of the SPDC crystal. However, considerable work has been done on tailoring the OAM spectrum for use in quantum information [99, 100]. In an experimental realization, we plan on using a periodically poled Potassium Titanyl Phosphate (PPKTP) crystal designed for degenerate, type-II, collinear SPDC. The PPKTP crystal is pumped by a laser diode at 405 nm to produced OAM-entangled photons at 810 nm. This source is based on an OAM-entanglement source used at IQOQI in Vienna [101].

The signal and idler photons are separated from one another by a polarizing beam splitter (PBS) and directed towards Alice and Bob, both of whom use a sorting procedure

similar to the one described earlier for BB84-based OAM-QKD. Following the random measurement of their respective photon in either the OAM or the ANG basis, Alice and Bob use coincidence detection to ensure that their photons originated in the same entangled pair. Thus, OAM anti-correlations and ANG correlations between these two photons will ensure that Alice and Bob measure the opposite (for the OAM basis) or the same (for the ANG basis) state at the end. Just as in polarization-entanglement-based QKD, security must be proven by testing for high-dimensional OAM-entanglement. This has been performed recently for an OAM dimensionality up to $\ell = 11$ by violating the generalized Bell-type parameter S_d by making projection measurements [99]. Interestingly, we can use our sorting method to calculate this very parameter directly. This is because the crosstalk terms (or the off-diagonal terms in the crosstalk matrix) obtained from the sorting process can be related to the measurements required to obtain S_d [102, 99]. One should keep in mind that since our sorting process is not entirely perfect (approximately 5% crosstalk), the entanglement measure will not be entirely accurate either. If the Bell-type parameter S_d is found to be greater than 2, we know that the state is still entangled in OAM and no eavesdropper is present.

5˙6. *Limitations and outlook*. – A chief limitation of our BB84 protocol-based OAM-QKD system is that an SLM is used for the generation of OAM and ANG modes. SLMs have a refresh rate of 60 Hz, which places a strict upper limit to how fast we can generate a key. For comparison, state of the art polarization-based systems have shown key generation rates exceeding 1 Mbit/s [103]. Clearly, in order to compete with polarization-based QKD, we need a faster method of generating OAM and ANG modes. A promising option is to use digital micro-mirror devices (DMDs), which are cheaply available and can operate at up to 32 kHz speeds. DMDs are binary amplitude devices that, as the name suggests, rely on tiny mirrors to turn parts of a beam on and off. Using a DMD with a $4f$ system of lenses, one can convert an arbitrary amplitude pattern into a phase pattern [104]. We have used such a device to generate OAM and ANG modes at speeds of up to 3.2 KHz [105]. We are planning to replace the SLM currently being used for OAM and ANG state preparation with this method.

Another limitation of our current system lies in our detection system. While in the previous section we have proposed the use of SPAD arrays for detecting the transformed modes, the shape of these modes creates a unique challenge for their detection. As can be seen in fig. 33, after passage through the OAM sorter, the fan-out elements and a Fourier transform lens, an OAM mode resembles a narrow line. Coupling this mode efficiently into a fiber will be a challenge and will perhaps require the use of cylindrical lenses. Optimization of the mode transformation process is also possible in order to obtain a mode that is more easily coupled into a fiber. The development of CCDs that work at the single photon level is progressing rapidly and will be key in the detection of such modes.

6. – Direct measurement of a high-dimensional quantum state

6˙1. *Introduction*. – Due in part to the no-cloning theorem [1], the measurement of a quantum state poses a unique challenge for experimentalists. Conventionally, a quantum state is measured through the indirect process of tomography [106], which requires significant post-processing times to reliably reconstruct the state [107]. For this reason, quantum tomography is an unfeasible method for measuring high-dimensional quantum states such as those of orbital angular momentum (OAM) [108]. Recently, an

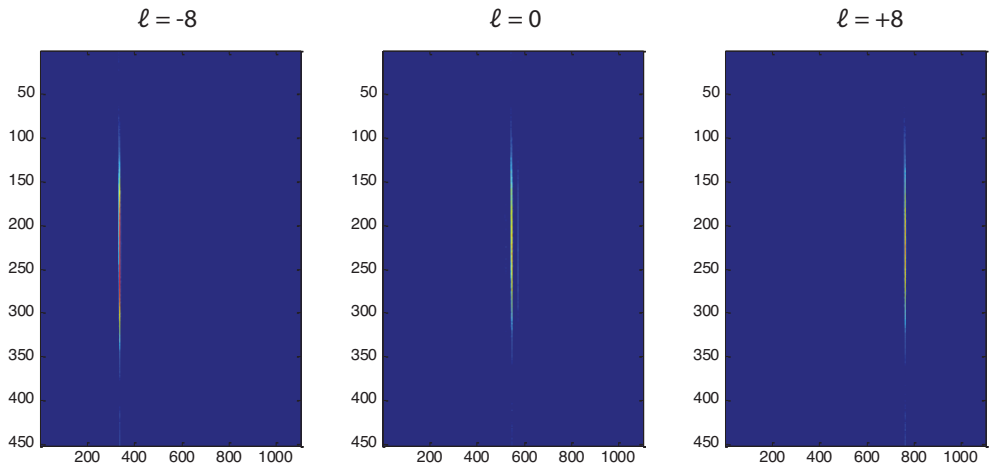

Fig. 33. – A CCD image showing the mode structure of the transformed OAM mode, after passing through the OAM sorter, the fan-out holograms, and a Fourier transform lens. Three transformed OAM modes ($\ell = -8, 0, +8$) are shown.

alternative method called "direct measurement" was proposed that utilized sequential weak and strong measurements to directly characterize a quantum state, *i.e.* without any post-processing [45]. In this section, we review a recent experiment where we use this method to characterize a high-dimensional quantum state in the discrete basis of OAM [109]. Through weak measurements of orbital angular momentum and strong measurements of angular position, we measure the probability amplitudes of a pure quantum state with a dimensionality, $d = 27$. Further, we use our method to study the relationship between the angular momentum operator and rotations of a quantum state in the natural basis of OAM [110].

The act of measuring a quantum state disturbs it irreversibly, a phenomenon referred to as *collapse* of the wave function. For example, precisely measuring the position of a single photon results in a photon with a broad superposition of momenta. Consequently, no quantum system can be fully characterized through a single measurement. An established method of characterizing a quantum state involves making a diverse set of measurements on a collection of identically prepared quantum states, followed by post-processing of the data. This process, known as quantum state tomography [106], is akin to its classical counterpart of imaging a three-dimensional object using two-dimensional projections. For a simple quantum system such as a polarization qubit, quantum tomography can be similarly visualized as making projections onto different axes of the Poincaré sphere in order to localize the state on the sphere [44]. A critical part of any real tomographic process is the analysis that follows this series of measurements —in order to obtain a physical quantum state, one must use lengthy numerical procedures to search over all the different state possibilities [111]. The time required for this post-processing step scales rather unfavorably with state dimension, and is catastrophically large for multipartite high-dimensional states [107, 108].

Photons carrying orbital angular momentum (OAM) are one such example of a high-dimensional quantum state that has come to the forefront recently [112-114]. The dis-

crete, infinite dimensionality of the OAM Hilbert space provides a larger information capacity for quantum information systems [62, 69], as well as an increased tolerance to eavesdropping in quantum key distribution [61]. Photons entangled in OAM [98,115,116] are prime candidates not only for such high capacity, high security communication systems, but also for fundamental tests of quantum mechanics [99,117]. Thus, it is essential that fast, accurate, and efficient methods for characterizing such high-dimensional states be developed. Quantum state tomography of a pair of photons entangled in OAM, each with a dimensionality of $d = 8$, was recently demonstrated —a process that took on the order of *days* to complete [108].

In sect. **2**˙4, we reviewed a novel alternative to tomography called direct measurement. In this technique, the complex probability amplitude of a pure quantum state is directly obtained as an output of the measurement apparatus, bypassing the complicated post-processing step required in quantum tomography. In the first implementation of direct measurement [45], the position of an ensemble of identically prepared photons was weakly measured, which caused a minimal disturbance to their momentum. A subsequent strong measurement of their momentum revealed all the information necessary to characterize their state in the continuous bases of position and momentum. A recent experiment extended this idea to directly measuring the two-dimensional polarization state of a laser beam [47]. Here, we apply this novel technique to characterize a photon in the discrete, infinite-dimensional space of orbital angular momentum.

6˙2. *Theoretical description of direct measurement in the OAM basis.* – In direct analogy to a photon's position and linear momentum, the angular position and OAM of a photon form a conjugate pair [118]. We can express the state of our photon as a superposition of states in the OAM or angular position basis as

$$|\Psi\rangle = \sum_{\ell} a_\ell |\ell\rangle \qquad \text{or} \qquad |\Psi\rangle = \sum_{\theta} b_\theta |\theta\rangle, \tag{38}$$

where a_ℓ and b_θ are the complex probability amplitudes in the OAM and angular position basis respectively.

By multiplying our state by a strategically chosen constant $c = \langle\theta_0\,|\ell\rangle\,/\,\langle\theta_0\,|\Psi\rangle$ and inserting the identity, we can expand our state as

$$c|\Psi\rangle = c\sum_{\ell} |\ell\rangle\,\langle\ell\,|\Psi\rangle = \sum_{\ell} |\ell\rangle \frac{\langle\theta_0\,|\ell\rangle\,\langle\ell\,|\Psi\rangle}{\langle\theta_0\,|\Psi\rangle} = \sum_{\ell} \langle\pi_\ell\rangle_{\mathrm{w}}\,|\ell\rangle. \tag{39}$$

Here we have introduced the quantity $\langle\pi_\ell\rangle_{\mathrm{w}}$, which is proportional to the probability amplitude a_ℓ from eq. (38). This quantity, known as the *weak value*, is defined as the average result of a weak measurement of a quantum state, followed by a strong measurement, or post-selection of another observable of the state [20, 21]. In general, weak values can be complex and can lie significantly outside the eigenvalue range of the observables being measured [22, 119]. In our direct measurement technique, the OAM weak value $\langle\pi_\ell\rangle_{\mathrm{w}}$ is equal to the average result obtained by making a weak measurement of a projector in the OAM basis ($\hat{\pi}_\ell = |\ell\rangle\langle\ell|$) followed by a strong measurement in the conjugate basis of angular position ($\theta = 0$). In this manner, the scaled complex probability amplitudes ca_ℓ can be directly obtained by measuring the OAM weak value $\langle\pi_\ell\rangle_{\mathrm{w}}$ for a finite set of ℓ. Following this procedure, the constant c can be eliminated by renormalizing the

state $|\Psi\rangle$.

$$|\Psi\rangle = \frac{1}{c}\sum_{\ell} \langle \pi_\ell \rangle_{\mathrm{w}} |\ell\rangle. \tag{40}$$

In order to measure such weak values, previous demonstrations of direct measurement have utilized a two-system Hamiltonian, where the system of interest is coupled to a measurement pointer [45,47]. In this manner, the real and imaginary parts of the system weak value are obtained by measuring the change in the pointer's position and momentum respectively [120]. This is well illustrated in the experiment of Salvail *et al.* [47], where the authors coupled the polarization of a laser beam to its position through the use of a birefringent crystal. By measuring the shift in the beam's position and momentum, they were able to measure its real and imaginary polarization components. In contrast, we use the polarization of the photon as a measurement pointer [45]. By coupling a photon's OAM to its polarization, we perform weak measurements of OAM by rotating the polarization of the OAM mode to be measured by a small angle. After sequential weak and strong measurements are performed, the average change in the photon's linear and circular polarization is measured, which is proportional to the real and imaginary parts of the OAM weak value.

Here we derive the relationship between the OAM weak value $\langle \pi_\ell \rangle_{\mathrm{w}}$ and expectation values of the $\hat{\sigma}_x$ and $\hat{\sigma}_y$ Pauli operators eq. (51). The von Neumann formulation can be used to describe the coupling between the OAM (system) and polarization (pointer) observables [121,120]. The product Hamiltonian describing this interaction can be written as

$$\hat{H} = -g\,\hat{\pi}_\ell \cdot \hat{S}_y = -\left(\frac{g\,\hbar}{2}\right)\hat{\pi}_\ell \cdot \hat{\sigma}_y, \tag{41}$$

where g is a constant indicating the strength of the coupling, $\hat{\pi}_\ell$ is the projection operator in the OAM basis, and $\hat{\sigma}_y$ is the Pauli spin operator in the y direction. The measurement pointer is initially in a vertical polarization state

$$|s_i\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{42}$$

and the system is in an initial state $|I\rangle$. The initial system-pointer state is modified by a unitary interaction $\hat{U} = \exp(-i\hat{H}t/\hbar)$, which can be written using the product Hamiltonian above as

$$\hat{U} = \exp\left(\frac{i\,gt\,\hat{\pi}_\ell \cdot \hat{\sigma}_y}{2}\right) = \exp\left(\frac{i\,\sin\alpha\,\hat{\pi}_\ell \cdot \hat{\sigma}_y}{2}\right) \tag{43}$$

Here we have substituted $\sin\alpha$ in place of gt as a coupling constant. This refers to the angle α by which we rotate the polarization of the OAM mode to be measured in our experiment. When α is small, the measurement is weak. In this case, we can express the operator $\hat{U}$ as a Taylor series expansion truncated to first order in $\sin\alpha$. The initial

state then evolves to

$$|\Psi(t)\rangle = \left(1 - \frac{i\hat{H}t}{\hbar} - \dots\right)|I\rangle|s_i\rangle \\ = |I\rangle|s_i\rangle + \frac{i\,\sin\alpha}{2}\hat{\pi}_\ell|I\rangle\hat{\sigma}_y|s_i\rangle. \tag{44}$$

We can express the strong measurement as a projection into a final state $|F\rangle$

$$\langle F|\hat{U}|I\rangle|s_i\rangle = \langle F\,|I\,\rangle\,|s_i\rangle + \frac{i\,\sin\alpha}{2}\langle F|\hat{\pi}_\ell|I\rangle\hat{\sigma}_y|s_i\rangle. \tag{45}$$

We can then divide by $\langle F\,|I\,\rangle$ to get the final pointer polarization state

$$|s_f\rangle = |s_i\rangle + \frac{i\,\sin\alpha}{2}\frac{\langle F|\hat{\pi}_\ell|I\rangle}{\langle F\,|I\,\rangle}\hat{\sigma}_y|s_i\rangle \\ = |s_i\rangle + \frac{i\,\sin\alpha}{2}\,\langle\pi_\ell\rangle_{\rm w}\,\hat{\sigma}_y|s_i\rangle. \tag{46}$$

Notice that the weak value $\langle\pi_\ell\rangle_{\rm w} = \langle F|\hat{\pi}_\ell|I\rangle/\langle F\,|I\,\rangle$ appears in the above equation. Using this expression for the final state of the pointer, we can calculate the expectation value of $\hat{\sigma}_x$ as follows:

$$\langle s_f|\hat{\sigma}_x|s_f\rangle = \cancel{\langle s_i|\hat{\sigma}_x|s_i\rangle} + \frac{i\,\sin\alpha}{2}\left[\,\langle\pi_\ell\rangle_{\rm w}\,\langle s_i|\hat{\sigma}_x\hat{\sigma}_y|s_i\rangle - \langle\pi_\ell\rangle_{\rm w}^{\dagger}\,\langle s_i|\hat{\sigma}_y\hat{\sigma}_x|s_i\rangle\right]. \tag{47}$$

Using the substitution $\langle\pi_\ell\rangle_{\rm w} = {\rm Re}\{\langle\pi_\ell\rangle_{\rm w}\} + i\,{\rm Im}\{\langle\pi_\ell\rangle_{\rm w}\}$ and the initial state $|s_i\rangle$ from eq. (42), the above equation can simplified further

$$\langle s_f|\hat{\sigma}_x|s_f\rangle = \frac{i\,\sin\alpha}{2}\Big[\,{\rm Re}\{\langle\pi_\ell\rangle_{\rm w}\}\langle s_i|\hat{\sigma}_x\hat{\sigma}_y - \hat{\sigma}_y\hat{\sigma}_x|s_i\rangle \\ + i\,{\rm Im}\{\langle\pi_\ell\rangle_{\rm w}\}\langle s_i|\cancel{\hat{\sigma}_x\hat{\sigma}_y + \hat{\sigma}_y\hat{\sigma}_x}|s_i\rangle\Big] \\ = -\,\sin\alpha\,{\rm Re}\{\langle\pi_\ell\rangle_{\rm w}\}\langle s_i|\hat{\sigma}_z|s_i\rangle \\ = \sin\alpha\,{\rm Re}\{\langle\pi_\ell\rangle_{\rm w}\}. \tag{48}$$

Similarly, we can calculate the expectation value of $\hat{\sigma}_y$ as follows:

$$\langle s_f|\hat{\sigma}_y|s_f\rangle = \cancel{\langle s_i|\hat{\sigma}_y|s_i\rangle} + \frac{i\,\sin\alpha}{2}\left[\,\langle\pi_\ell\rangle_{\rm w}\,\langle s_i|\hat{\sigma}_y\hat{\sigma}_y|s_i\rangle - \langle\pi_\ell\rangle_{\rm w}^{\dagger}\,\langle s_i|\hat{\sigma}_y\hat{\sigma}_y|s_i\rangle\right] \\ = \frac{i\,\sin\alpha}{2}\Big[\,{\rm Re}\{\langle\pi_\ell\rangle_{\rm w}\}\langle s_i|\cancel{\hat{\sigma}_y\hat{\sigma}_y - \hat{\sigma}_y\hat{\sigma}_y}|s_i\rangle \\ + i\,{\rm Im}\{\langle\pi_\ell\rangle_{\rm w}\}\langle s_i|\hat{\sigma}_y\hat{\sigma}_y + \hat{\sigma}_y\hat{\sigma}_y|s_i\rangle\Big] \\ = -\,\sin\alpha\,{\rm Im}\{\langle\pi_\ell\rangle_{\rm w}\}\langle s_i|\hat{\sigma}_y^2|s_i\rangle \\ = -\,\sin\alpha\,{\rm Im}\{\langle\pi_\ell\rangle_{\rm w}\}. \tag{49}$$

Thus, we see that the real and imaginary parts of the OAM weak value $\langle \pi_\ell \rangle_{\mathrm{w}}$ are proportional to the expectation values of the $\hat{\sigma}_x$ and $\hat{\sigma}_y$ Pauli operators (see eq. (51)):

$$\begin{aligned} \langle \pi_\ell \rangle_{\mathrm{w}} &= \mathrm{Re}\{\langle \pi_\ell \rangle_{\mathrm{w}}\} + i\,\mathrm{Im}\{\langle \pi_\ell \rangle_{\mathrm{w}}\} \\ &= \frac{1}{\sin\alpha}\big[\langle s_f|\hat{\sigma}_x|s_f\rangle - i\langle s_f|\hat{\sigma}_y|s_f\rangle\big]. \end{aligned} \tag{50}$$

6˙3. *Experimental weak measurement of OAM*. – In order to perform a weak measurement of OAM at the single photon level, one must first spatially separate the OAM components of the single photon. Only then can one rotate the polarization of the OAM mode to be measured by a small angle, which constitutes the weak measurement. Recently, we proposed a technique to efficiently separate the OAM components of a single photon [81, 84], which is discussed in detail in sect. **5**. Here, we implement this mode sorter technique using four phase-only elements (fig. 34, R1, R2, SLM2, and SLM3) to separate the OAM components with less than 10% overlap. The first two elements, R1 and R2, are refractive holograms made out of Poly-methyl methacrylate (PMMA) that are used to map polar coordinates (r, θ) to rectilinear coordinates (x, y) through the log-polar mapping $x = a(\theta \mod 2\pi)$ and $y = -a\ln(r/b)$ [82]. This results in the transformation of an OAM mode with azimuthal phase variation $e^{i\ell\theta}$ to a momentum mode with position phase variation $e^{i\ell x/a}$. These momentum modes are then Fourier transformed by the lens L1 to position modes. At this stage, the component OAM modes of the photon still have an overlap of about 20%. This is due to the finite size of the transformed momentum mode, which is bounded by the function $\mathrm{rect}(x/2\pi a)$. A simple way to decrease the overlap and hence the size of the position mode is to simply increase the size of the momentum mode (while maintaining the phase ramp across it). We create three adjacent copies of the momentum mode by implementing a fan-out hologram and phase-corrector on SLM2 and SLM3 [86], also previously introduced in sect. **5**. The one-dimensional phase profile of the 3 copy fan-out hologram used here is shown in fig. 28. in After passing through another lens L2, this results in well-separated OAM modes having less than 10% overlap on average with neighboring components.

In the next step, we rotate the polarization of the OAM mode to be weakly measured by an angle, $\alpha = \pi/9$. In contrast to the dynamic method used by Lundeen *et al.* [45] in which they physically moved a half-wave plate (HWP) sliver through the beam, we use a static, programmable technique. A phase-only SLM acts as a variable phase retarder with individually addressable pixels. By sandwiching such an SLM between two quarter-wave plates (QWPs) whose extraordinary axes are aligned at $\pi/4$ radians to the SLM axis, one can rotate the polarization of any part of the beam through an arbitrary angle [122]. As shown in fig. 34, we use this technique to rotate the polarization of the OAM mode to be weakly measured. Since we use SLM4 in reflection, only one quarter-wave plate (QWP0) is needed. However, QWP1 and HWP1 are used to remove any ellipticity introduced by reflection through the non-polarizing beamsplitter (NPBS). A strong measurement of angular position is performed by a $10\,\mu$m slit placed in the Fourier plane of lens L3. Since the plane of the slit is conjugate to the plane (SLM4) where the OAM modes are spatially separated, a measurement of linear position by the slit is equivalent to a measurement of angular position.

The average change in the photon's linear and circular polarization is proportional to $\mathrm{Re}\langle \pi_\ell \rangle_{\mathrm{w}}$ and $\mathrm{Im}\,\langle \pi_\ell \rangle_{\mathrm{w}}$ respectively. As shown in the previous section, for an initially

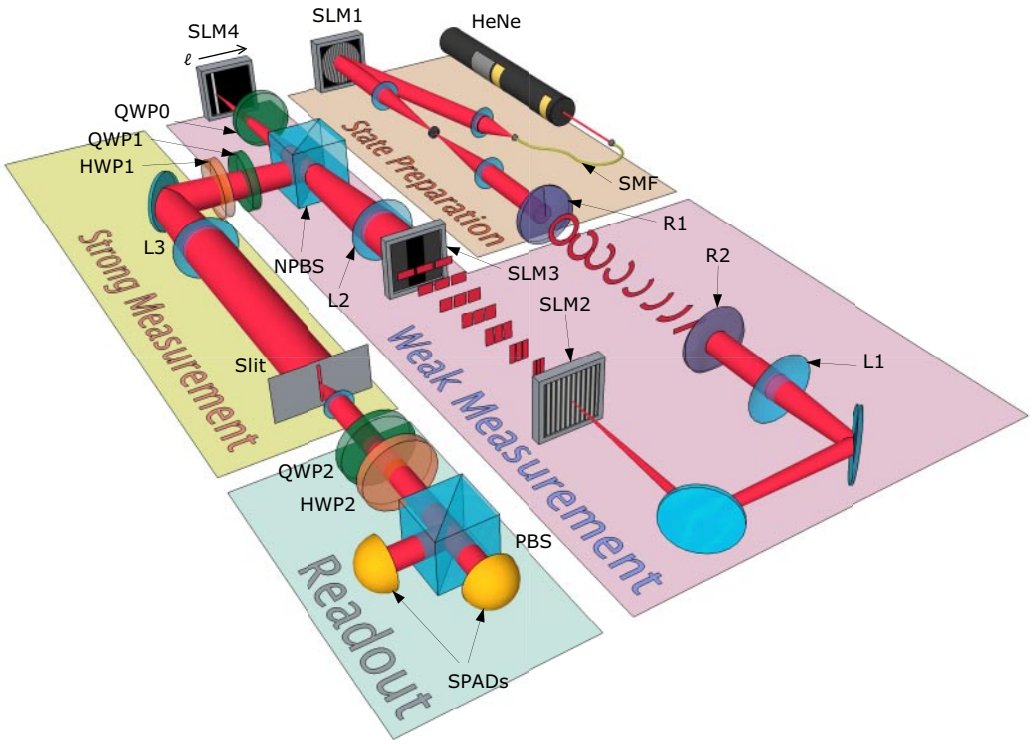

Fig. 34. – Direct measurement of a high-dimensional quantum state. State Preparation: A quantum state in an arbitrary superposition of orbital angular momentum (OAM) modes is prepared by impressing phase information onto photons from an attenuated HeNe laser. Weak Measurement: A particular OAM mode is weakly measured by rotating its polarization by a small angle. This is accomplished by first separating the component OAM modes of the photon via a geometric transformation and then performing the polarization rotation. This process is depicted in the figure for one OAM mode. Strong Measurement: The angular position of the photon is strongly measured by using a slit to post-select states with an angle $\theta = 0$. Readout: The OAM weak value $\langle \pi_\ell \rangle_{\mathrm{w}}$ is obtained by measuring the change in the photon polarization in the linear and circular polarization bases (figure adapted from ref. [109]).

vertically polarized state, the OAM weak value is given by

$$\langle \pi_\ell \rangle_{\mathrm{w}} = \frac{1}{\sin\alpha}\Big(\langle s_f|\hat{\sigma}_x|s_f\rangle - i\langle s_f|\hat{\sigma}_y|s_f\rangle\Big), \tag{51}$$

where α is the rotation angle, σ_x and σ_y are the Pauli operators in the x and y directions, and $|s_f\rangle$ is the final polarization state of the photon. In order to measure the expectation values of σ_x and σ_y, we transform to the linear and circular polarization bases with QWP2 and HWP2, and measure the two Stokes parameters with a polarizing beamsplitter (PBS) and two single-photon avalanche detectors (SPADs). In this manner, we directly obtain the scaled complex probability amplitudes ca_ℓ by scanning the weak measurement through ℓ values of ± 13. Although the OAM of a photon exists in a dis-

crete, unbounded Hilbert space, we are not able to go beyond a dimensionality of $d = 27$ as our mode transformation technique begins to break down for higher OAM modes.

6˙4. *Measuring the wave function in the OAM basis.* – To test our method, we generate single photon states by strongly attenuating a HeNe laser to the single photon level. These photons are then tailored into a high-dimensional quantum state by impressing a specific OAM distribution on them with SLM1 and a $4f$ system of lenses (fig. 34) [78]. We create a sinc-distribution of OAM using a wedge-shaped mask on the SLM. Analogous to how a rectangular aperture diffracts light into a sinc-distribution of linear momenta, a single photon diffracting through an angular aperture of width $\Delta\theta$ results in a quantum state with a sinc-distribution of OAM probability amplitudes [118]

$$a_\ell = k\,\mathrm{sinc}\left(\frac{\Delta\theta\ell}{2}\right). \tag{52}$$

The first nulls of this OAM distribution lie at OAM values $\ell = \pm 2\pi/\Delta\theta$. Using an angular aperture of width $2\pi/9$ rad (inset of fig. 35(b)), we create such an ensemble of identical single photons and perform the direct measurement procedure on them. The measured real and imaginary parts of the wave function are plotted in fig. 35(a) as a function of ℓ. From these, we calculate the probability density $|\Psi(\ell)|^2$ and the phase $\phi(\ell)$, which are plotted in figs. 35(b) and (c). The width of the sinc-squared fit to the probability density is measured to be 9.26 ± 0.21, which is very close to the value of 9 predicted from theory. The measured phase of the OAM distribution in fig. 35(c) has a tilted quadratic shape that is acquired from propagation through the system. Interestingly, π-phase jumps appear at the two minima of the sinc-squared probability density. This is because the sinc distribution of probability amplitudes in eq. (52) changes sign from positive to negative at these two points. Additionally, the phase error is large when the amplitude goes to zero. This is because the noise due to the background and detector dark counts overwhelms our signal in this regime. Theoretical fits to the phase and probability density are plotted as blue lines.

6˙5. *The angular momentum operator as a generator of rotations.* – Here, we use our technique to study the effect of rotation on a single photon carrying a range of angular momenta. Rotation of a quantum state by an angle θ_0 can be expressed by the unitary operator $\hat{U} = \exp(i\hat{L}_z\theta_0)$, where $\hat{L}_z$ is the angular momentum operator. Operating on our quantum state $|\Psi\rangle$ with $\hat{U}$, we get

$$|\Psi'\rangle = \hat{U}|\Psi\rangle = \sum_\ell k\,\mathrm{sinc}\left(\frac{\Delta\theta\ell}{2}\right)e^{i\ell\theta_0}|\ell\rangle. \tag{53}$$

Thus, the *rotation* of a state vector by an angle θ_0 manifests as an *ℓ-dependent phase* $e^{i\ell\theta_0}$ in the OAM basis. For this reason, the angular momentum operator is called the generator of rotations in quantum mechanics under the paraxial approximation [110]. In order to generate such a linear OAM-dependent phase, we create a rotated wave function by rotating our angular aperture by an angle $\theta_+ = \pi/9$ rad (inset of fig. 36(b)). Then, we perform the direct measurement procedure as explained in the previous section. The real and imaginary parts of the rotated wave function as a function of ℓ (fig. 36(a)) are measured. The probability density and phase of the wave function are calculated from these measured values and plotted in figs. 36(b) and (c). For clarity, we subtract the

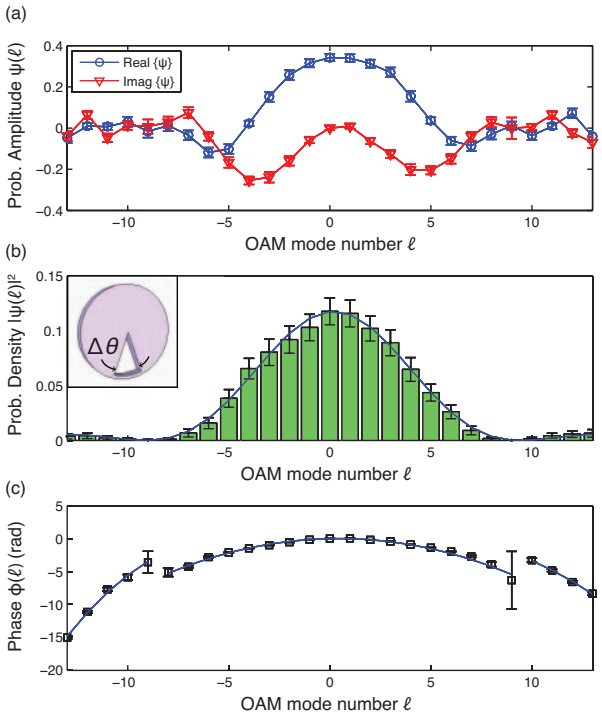

Fig. 35. – Experimental data showing direct measurement of a 27-dimensional quantum state in the OAM basis. The state is created by sending single-photons through an angular aperture of width $\Delta\theta = 2\pi/9$ rad (inset of panel (b)). (a) The measured real (blue circles) and imaginary parts (red triangles) of the wave function, (b) the calculated probability density $|\Psi(\ell)|^2$, and (c) the calculated phase $\phi(\ell)$ are plotted as functions of the OAM quantum number ℓ up to a dimensionality of $\ell = \pm 13$. π-phase jumps occur when the probability amplitude is negative (not seen in the probability density). Theoretical fits to the probability density and phase are plotted as a blue line (figure adapted from [109]).

phase of the zero rotation case (fig. 35(c)) from our measured values of phase, so the effect of rotation is clear. Barring experimental error, the amplitude does not change significantly from the unrotated case (fig. 35(b)). However, the phase of the single-photon OAM distribution exhibits a distinct ℓ-dependent phase ramp with a slope of 0.373 ± 0.007 rad/mode. This is in close agreement with theory, which predicts the phase to have a form $\phi(\ell) = \pm\pi\ell/9$, corresponding to a phase ramp with a slope of 0.35 rad/mode. Errors in slope are calculated by the process of chi-square minimization. This process is repeated for a negative rotation angle $\theta_- = -\pi/9$ rad, which results in a mostly unchanged probability density, but an ℓ-dependent phase ramp with a negative slope of -0.404 ± 0.007 rad/mode (figs. 36 (d)-(f)).

These results clearly illustrate the relationship between phase and rotation in the OAM basis in that every ℓ-component acquires a phase proportional to the azimuthal quantum number ℓ. The measured slopes in both cases are slightly larger than those expected from theory due to errors introduced in the geometrical transformation that is used to spatially separate the OAM modes. The mode sorting process is extremely

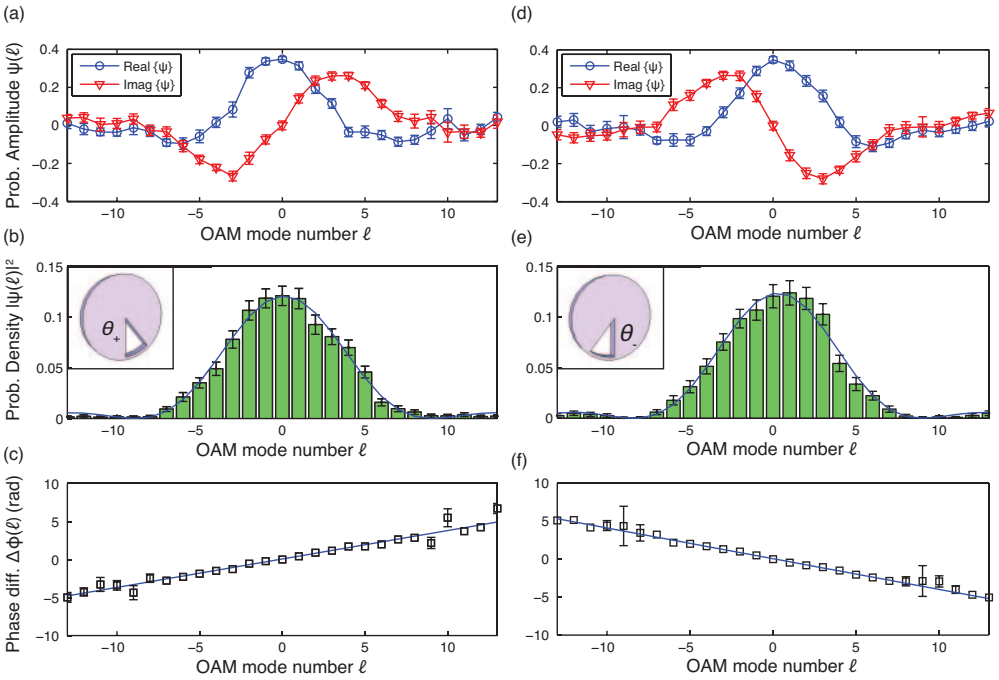

Fig. 36. – Experimental data showing the direct measurement of a high-dimensional quantum state rotated by an angle $\theta_\pm = \pm\pi/9$ rad (insets). (a) and (d) The measured real (blue circles) and imaginary parts (red triangles) of the rotated wave functions. (b) and (e) The calculated probability densities $|\Psi(\ell)_\pm|^2$. (c) and (f) The phase difference $\Delta\phi_\pm(\ell)$ between the calculated phase and the phase of the unrotated case. Theoretical fits to the probability densities and phases are plotted as blue lines. Error bars larger than the symbols are shown (figure adapted from [109]).

sensitive to misalignment, and a very small displacement of the transforming elements R1 and R2 can propagate as a phase error.

6˙6. *Summary and outlook.* – To summarize, we have measured the complex probability amplitudes that characterize the wave function in the high-dimensional bases of orbital angular momentum and angular position. Using our technique, we have also measured the effects of rotation on a quantum state in the OAM basis. The rotation manifests as an OAM mode-dependent phase and provides a clean visualization of the relationship between the angular momentum operator and rotations in quantum mechanics.

While we have directly measured pure states of OAM, this method can be extended to perform measurements of mixed, or general quantum states [46, 47]. By scanning the strong measurement of angular position as well, one can measure the Dirac distribution, which is informationally equivalent to the density matrix of a quantum state [123, 124]. Furthermore, by extending this technique to two photons, photons entangled in OAM can be measured. In this case, one would need to perform independent weak and strong measurements on each photon, followed by a two-photon coincidence-detection scheme for the polarization measurement.

Direct measurement offers distinct advantages over conventional methods of quantum state characterization such as tomography. This method does not require a global recon-

struction, a step that involves prohibitively long processing times for high-dimensional quantum states such as those of OAM. Consequently, the quantum state is more accessible in that it can be measured locally as a function of OAM quantum number ℓ, as in our experiment. These advantages may open up avenues for measuring quantum states directly in the middle of dynamically changing systems such as quantum circuits and free-space quantum communication links.

7. – Conclusions

In the immensely technological world of today, security is perhaps something we take for granted. However, security pervades through our quotidian tasks such as withdrawing money from the ATM and checking email on our smartphones. The machine gun-toting bank robbers of yesteryear have become a figment of Hollywood imagination, being replaced instead by individuals sitting behind a desk with an internet connection. The threat of cyber crimes such as identity theft and account hacking have never been more real, and nations are starting to realize that such concerns are not just limited to the individual. Large amounts of money have been spent by countries in the past for developing complex encryption algorithms that can be cracked by a sophisticated hacker.

Over the past thirty years, the simplest limitation of a quantum state has led to the development of elegant technologies that allow unconditionally secure communication. The fact that one cannot create a copy of a quantum state allows one to use it as "digital bait". A hacker who intercepts a secure quantum communication channel will disturb the delicate quantum states used in the channel, thus revealing his or her presence. The technologies reviewed in this article form part of this quantum revolution in security. We have applied ideas borrowed from quantum key distribution protocols to the field of optical imaging and surveillance. This promises a form of security for active imaging systems such as lidar that has not been seen before. Quantum ghost imaging has long been destined to the lab bench due the to impracticality of measuring an entire image at the single photon level. By extending this scheme to the identification of a set of images, we have made quantum ghost imaging easier to apply in the real world.

Quantum key distribution (QKD) is the bastion of secure quantum technologies, with commercial short-range QKD systems available today. One branch of research in this field is exploring the engineering extension of polarization-based QKD to longer and longer distances, such as ground to satellite. We have taken a parallel approach in this article, instead exploring alternative methods of encoding for QKD. QKD protocols using polarization states for encoding are limited to how much information they can send per photon, as well as how much eavesdropping error they can tolerate. By using the discrete, infinite-dimensional state space of orbital angular momentum (OAM) for encoding, we can build a QKD system that promises a vastly increased information capacity and a significantly higher tolerance to error than conventional polarization-based QKD. In this article, we have discussed the development of technologies that allow us to generate and measure single photons carrying superpositions of OAM. Further, we have explored our ability to use such states to perform communication in a real-world setting with atmospheric turbulence. The development of working OAM-based QKD systems is the next research goal in our lab, and we are making fast progress towards achieving it.

The accurate characterization of a quantum state is important for fields as diverse as information science, physical chemistry, and foundational physics. A quantum state is conventionally measured by the process of quantum state tomography. Recently, an alternative to tomography was presented that used sequential weak and strong measure-

ments in order to completely characterize a quantum state. In contrast with tomography, this "direct measurement" method does not involve a time consuming post-processing step. In this article, we have reviewed the first application of the direct measurement technique for measuring a quantum state in a discrete, high-dimensional state space such as that of OAM. This serves as a significant advance for this technique, which has been previously used to characterize a photon in the continuous basis of position-momentum and a classical beam in the two-dimensional basis of polarization. The technique of direct measurement is especially advantageous when used for measuring high-dimensional quantum states. This is because the post-processing time required for the tomography of such states is prohibitive. Our experiment serves as the first application of direct measurement that sets it clearly apart from tomography in this regard. Further, it displays the potential this technique has for measuring quantum states directly in the middle of dynamic quantum processes.

The quantum technologies presented in this article serve to advance the state of the art of research in the fields of secure quantum communication, quantum imaging, and quantum state characterization. In addition, by interfacing between these fields, they show the potential that exists for the exchange of ideas and techniques across these disciplines. It is likely that quantum technologies today are the beginning of a technological revolution that will encompass more than just security.

* * *

We would like to thank Mohammad Mirhosseini, Omar Magaña-Loaiza, Malcolm O'Sullivan, Prof. Zhimin Shi, Dr. Heedeuk Shin, Brandon Rodenberg, Prof. Anand Jha, Dr. Petros Zerom, Prof. Jonathan Leach, Dr. Martin Lavery, and Prof. Miles Padgett for their direct contributions to many of the experiments that are reviewed in this article. Additionally, we would like to thank Dr. Justin Dressel, Dr. Filippo Miatto, and Prof. Andrew Jordan for many enlightening discussions on quantum weak values. This work was supported by the DARPA InPho program. M.M. acknowledges funding from the European Commission through a Marie Curie fellowship. R.W.B. acknowledges support from the Canada Excellence Research Chairs program.

REFERENCES

[1] Wootters W. K. and Zurek W. H., *Nature*, **299** (1982) 802.
[2] Bennett C. and Brassard G., *Quantum cryptography: Public key distribution and coin tossing*, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (Bangalore) 1984, p. 175.
[3] Boto A. N., Kok P., Abrams D. S., Braunstein S. L., Williams C. P. and Dowling J. P., *Phys. Rev. Lett.*, **85** (2000) 2733.
[4] Nagata T., Okamoto R., O'Brien J. L., Sasaki K. and Takeuchi S., *Science*, **316** (2007) 726.
[5] Plato and Jowett B., *Plato's The Republic* (The Modern Library, New York) 1941.
[6] Rhys, `http://goodcanadiankid.com/schrodingers-cat/` (2012).
[7] Romero-Isart O., Juan M. L., Quidant R. and Cirac J. I., *New J. Phys.*, **12** (2010) 033015.
[8] Schrödinger E., *Naturwiss.*, **23** (1935) 823.
[9] Bell J., *Physics*, **1** (1964) 195.
[10] Clauser J., Horne M., Shimony A. and Holt R., *Phys. Rev. Lett.*, **23** (1969) 880.
[11] Aspect A., Dalibard J. and Roger G., *Phys. Rev. Lett.*, **49** (1982) 1804.
[12] Ekert A. K., *Phys. Rev. Lett.*, **67** (1991) 661.

[13] Bouwmeester D., Pan J.-W., Mattle K., Eibl M., Weinfurter H. and Zeilinger A., *Nature*, **390** (1997) 575.
[14] Boyd R. W. and Dowling J. P., *Quantum Inf. Process*, **11** (2011) 891.
[15] Pittman T., Shih Y., Strekalov D. and Sergienko A., *Phys. Rev. A*, **52** (1995) R3429.
[16] Monken C., Ribeiro P. and Padua S., *Phys. Rev. A*, **57** (1998) 3123.
[17] Walborn S. P. and Monken C., *Phys. Rev. A*, **76** (2007) 062305.
[18] Beth R. A., *Phys. Rev.*, **50** (1936) 115.
[19] Allen L., Beijersbergen M., Spreeuw R. and Woerdman J. P., *Phys. Rev. A*, **45** (1992) 8185.
[20] Aharonov Y., Albert D. Z. and Vaidman L., *Phys. Rev. Lett.*, **60** (1988) 1351.
[21] Dressel J., Miatto F. M., Jordan A. N., Boyd R. W. and Malik M., *Rev. Mod. Phys.*, **86** (2014) 307.
[22] Ritchie N., Story J. and Hulet R., *Phys. Rev. Lett.*, **66** (1991) 1107.
[23] Giovannetti V., Lloyd S. and Maccone L., *Science*, **306** (2004) 1330.
[24] Dutton Z., Shapiro J. H. and Guha S., *J. Opt. Soc. Am. B*, **27** (2010) A63.
[25] Steane A., *Rep. Prog. Phys.*, **61** (1999) 117.
[26] Bennett C. H. and DiVincenzo D. P., *Nature*, **404** (2000) 247.
[27] Gisin N., Ribordy G., Tittel W. and Zbinden H., *Rev. Mod. Phys.*, **74** (2002) 145.
[28] Lo H.-K., Ma X. and Chen K., *Phys. Rev. Lett.*, **94** (2005) 230504.
[29] Agnew M., Leach J. and Boyd R., *Eur. Phys. J. D*, **66** (2012) 156.
[30] Strekalov D., Sergienko A. and Klyshko D., *Phys. Rev. Lett.*, **74** (1995) 3600.
[31] Bennink R., Bentley S. and Boyd R. W., *Phys. Rev. Lett.*, **89** (2002) 113601.
[32] Gatti A., Brambilla E., Bache M. and Lugiato L., *Phys. Rev. Lett.*, **93** (2004) 093602.
[33] Bennink R., Bentley S., Boyd R. W. and Howell J., *Phys. Rev. Lett.*, **92** (2004) 033601.
[34] Ferri F., Magatti D., Gatti A., Bache M., Brambilla E. and Lugiato L., *Phys. Rev. Lett.*, **94** (2005) 183602.
[35] Meyers R. E., Deacon K. S. and Shih Y., *Appl. Phys. Lett.*, **98** (2011) 111115.
[36] Dixon P., Howland G., Chan K., O'Sullivan M., Rodenburg B., Hardy N., Shapiro J., Simon D., Sergienko A. and Boyd R. W., *Phys. Rev. A*, **83** (2011) 051803.
[37] Katz O., Bromberg Y. and Silberberg Y., *Appl. Phys. Lett.*, **95** (2009) 131110.
[38] Bromberg Y., Katz O. and Silberberg Y., *Phys. Rev. A*, **79** (2009) 053840.
[39] Magaña-Loaiza O. S., Howland G. A., Malik M., Howell J. C. and Boyd R. W., *Appl. Phys. Lett.*, **102** (2013) 231104.
[40] Brida G., Genovese M. and Berchera I. R., *Nat. Photon.*, **4** (2010) 227.
[41] Lemos G. B., Borish V., Cole G. D., Ramelow S., Lapkiewicz R. and Zeilinger A., arXiv:1401.4318 (2014).
[42] Ferrie C. and Combes J., *Phys. Rev. Lett.*, **112** (2014) 040406.
[43] Jordan A. N., Martínez-Rincón J. and Howell J. C., *Phys. Rev. X*, **4** (2014) 011031.
[44] Altepeter J., Jeffrey E. and Kwiat P., *Adv. At. Mol. Opt. Phys.*, **52** (2005) 105.
[45] Lundeen J. S., Sutherland B., Patel A. and Stewart C., *Nature*, **474** (2011) 188.
[46] Lundeen J. S. and Bamber C., *Phys. Rev. Lett.*, **108** (2012) 070402.
[47] Salvail J. Z., Agnew M., Johnson A. S., Bolduc E., Leach J. and Boyd R. W., *Nat. Photon.*, **7** (2013) 316.
[48] Haapasalo E., Lahti P. and Schultz J., *Phys. Rev. A*, **84** (2011) 052107.
[49] Roome S. J., *Electron. Commun. Engin. J.*, **2** (1990) 147.
[50] Malik M., Magaña-Loaiza O. S. and Boyd R. W., *Appl. Phys. Lett.*, **101** (2012) 241103.
[51] Goodman J., *Introduction to Fourier Optics* (Roberts & Company) 2005.
[52] Broadbent C., Zerom P., Shin H., Howell J. and Boyd R. W., *Phys. Rev. A*, **79** (2009) 033802.

[53] Malik M., Shin H., O'Sullivan M. N., Zerom P. and Boyd R. W., *Phys. Rev. Lett.*, **104** (2010) 163602.
[54] Abouraddy A., Saleh B. and Sergienko A., *J. Opt. Soc. Am. A*, **19** (2002) 1174.
[55] He G., Wang X., Li D. and Hu J., *Optik-Int. J. Light Electron Opt.*, **119** (2008) 548.
[56] Turin G., *IEEE Trans. Inf. Theor.*, **6** (1960) 311.
[57] Morris G., *Appl. Opt.*, **23** (1984) 3152.
[58] An X., Psaltis D. and Burr G., *Appl. Opt.*, **38** (1999) 386.
[59] Hiskett P. A., Rosenberg D., Peterson C. G., Hughes R. J., Nam S., Lita A. E., Miller A. J. and Nordholt J. E., *New J. Phys.*, **8** (2006) 193.
[60] Ursin R., Tiefenbacher F., Schmitt-Manderbach T., Weier H., Scheidl T., Lindenthal M., Blauensteiner B., Jennewein T., Perdigues J., Trojek P., Ömer B., Fürst M., Meyenburg M., Rarity J., Sodnik Z., Barbieri C., Weinfurter H. and Zeilinger A., *Nat. Phys.*, **3** (2007) 481.
[61] Bourennane M., Karlsson A., Bjork G., Gisin N. and Cerf N., *J. Phys. A-Math. Gen.*, **35** (2002) 10065.
[62] Groblacher S., Jennewein T., Vaziri A., Weihs G. and Zeilinger A., *New J. Phys.*, **8** (2006) 75.
[63] Cerf N., Bourennane M., Karlsson A. and Gisin N., *Phys. Rev. Lett.*, **88** (2002) 127902.
[64] Paterson C., *Phys. Rev. Lett.*, **94** (2005) 153901.
[65] Tyler G. and Boyd R. W., *Opt. Lett.*, **34** (2009) 142.
[66] Smith B. and Raymer M., *Phys. Rev. A*, **74** (2006) 062104.
[67] Gbur G. and Tyson R. K., *J. Opt. Soc. Am. A*, **25** (2008) 225.
[68] Roux F., *Phys. Rev. A*, **83** (2011) 053822.
[69] Malik M., O'Sullivan M. N., Rodenburg B., Mirhosseini M., Leach J., Lavery M. P. J., Padgett M. J. and Boyd R. W., *Opt. Express*, **20** (2012) 13195.
[70] Rodenburg B., Mirhosseini M., Malik M., Magaña-Loaiza O. S., Yanakas M., Maher L., Steinhoff N. K., Tyler G. A. and Boyd R. W., *New. J. Phys.*, **16** (2014) 033020.
[71] Krenn M., Fickler R., Fink M., Handsteiner J., Malik M., Scheidl T., Ursin R. and Zeilinger A., arXiv:1402.2602 (2014).
[72] Shannon C. E., *Bell Syst. Tech. J.*, **27** (1948) 379.
[73] Nielsen M. and Chuang I., *Quantum Computation and Quantum Information* (Cambridge University Press) 2004.
[74] Wootters W. K. and Fields B. D., *Ann. Phys. (N.Y.)*, **191** (1989) 363.
[75] Bruss D., *Phys. Rev. Lett.*, **81** (1998) 3018.
[76] Scarani V., Bechmann-Pasquinucci H., Cerf N. J., Dusek M., Luetkenhaus N. and Peev M., *Rev. Mod. Phys.*, **81** (2009) 1301.
[77] Heckenberg N. R., McDuff R., Smith C. P. and White A. G., *Opt. Lett.*, **17** (1992) 221.
[78] Arrizon V., Ruiz U., Carrada R. and Gonzalez L. A., *J. Opt. Soc. Am. A.*, **24** (2007) 3500.
[79] Gruneisen M. T., Miller W. A., Dymale R. C. and Sweiti A. M., *Appl. Opt.*, **47** (2008) A32.
[80] Leach J., Padgett M. J., Barnett S. M. and Franke-Arnold S., *Phys. Rev. Lett.*, **88** (2002) 257901.
[81] Berkhout G. C. G., Lavery M. P. J., Courtial J., Beijersbergen M. W. and Padgett M. J., *Phys. Rev. Lett.*, **105** (2010) 153601.
[82] Lavery M. P. J., Robertson D. J., Berkhout G. C. G., Love G. D., Padgett M. J. and Courtial J., *Opt. Express*, **20** (2012) 2110.
[83] Bryngdahl O., *JOSA*, **64** (1974) 1092.
[84] Mirhosseini M., Malik M., Shi Z. and Boyd R. W., *Nat. Commun.*, **4** (2013) 2781.
[85] O'Sullivan M. N., Mirhosseini M., Malik M. and Boyd R. W., *Opt. Express*, **20** (2012) 24444.

[86] Prongue D., Herzig H. P., Dandliker R. and Gale M. T., *Appl. Opt.*, **31** (1992) 5706.
[87] Romero L. A. and Dickey F. M., *J. Opt. Soc. Am. A*, **24** (2007) 2280.
[88] Lütkenhaus N. and Jahma M., *J. Opt.*, **4** (2002) 44.
[89] Schmitt-Manderbach T., *Long distance free-space quantum key distribution*, Ph.D. thesis, Ludwig-Maximilians-Universitat Munchen (2008).
[90] Zhao Y., Qi B., Ma X., Lo H.-K. and Qian L., *Phys. Rev. Lett.*, **96** (2006) 070502.
[91] Schmitt-Manderbach T., Weier H., Fürst M., Ursin R., Tiefenbacher F., Scheidl T., Perdigues J., Sodnik Z., Kurtsiefer C., Rarity J., Zeilinger A. and Weinfurter H., *Phys. Rev. Lett.*, **98** (2007) 010504.
[92] Ma X., Qi B., Zhao Y. and Lo H.-K., *Phys. Rev. A*, **72** (2005) 012326.
[93] Makkaveev A., Molotkov S., Pomozov D. and Timofeev A., *J. Exp. Theor. Phys.*, **101** (2005) 230.
[94] Huttner B. and Ekert A. K., *J. Mod. Opt.*, **41** (1994) 2455.
[95] Mirhosseini M., Magaña Loaiza O., O'Sullivan M., Rodenburg B., Malik M., Gauthier D. J. and Boyd R. W., arXiv:1402.7113 (2014).
[96] Ekert A. and Knight P., *Am. J. Phys.*, **63** (1995) 415.
[97] Galvez E., Holbrow C., Pysher M., Martin J., Courtemanche N., Heilig L. and Spencer J., *Am. J. Phys.*, **73** (2005) 127.
[98] Mair A., Vaziri A., Weihs G. and Zeilinger A., *Nature*, **412** (2001) 313.
[99] Dada A. C., Leach J., Buller G. S., Padgett M. J. and Andersson E., *Nat. Phys.*, **7** (2011) 677.
[100] Pires H. D. L., Florijn H. C. B. and van Exter M. P., *Phys. Rev. Lett.*, **104** (2010) 020505.
[101] Krenn M., Fickler R., Huber M., Lapkiewicz R., Plick W., Ramelow S. and Zeilinger A., *Phys. Rev. A*, **87** (2013) 012326.
[102] Collins D., Gisin N., Linden N., Massar S. and Popescu S., *Phys. Rev. Lett.*, **88** (2002) 040404.
[103] Dixon A. R., Yuan Z. L., Dynes J. F., Sharpe A. W. and Shields A. J., *Appl. Phys. Lett.*, **96** (2010) 161102.
[104] Rodrigo P. J., Perch-Nielsen I. R. and Glückstad J., *Opt. Express*, **14** (2006) 5588.
[105] Mirhosseini M., Magaña-Loaiza O. S., Chen C., Rodenburg B., Malik M. and Boyd R. W., *Opt. Express*, **21** (2013) 30204.
[106] D'Ariano G. M., Paris M. G. A. and Sacchi M. F., *Adv. Imaging Electron Phys.*, **128** (2003) 205.
[107] Thew R. T., Nemoto K., White A. G. and Munro W. J., *Phys. Rev. A*, **66** (2002) 012303.
[108] Agnew M., Leach J., McLaren M., Roux F. S. and Boyd R. W., *Phys. Rev. A*, **84** (2011) 062101.
[109] Malik M., Mirhosseini M., Lavery M. P. J., Leach J., Padgett M. J. and Boyd R. W., *Nat. Commun.*, **5** (2014) 3115.
[110] Barnett S. M. and Pegg D. T., *Phys. Rev. A*, **41** (1990) 3427.
[111] Banaszek K., D'Ariano G., Paris M. and Sacchi M., *Phys. Rev. A*, **61** (1999) 010304.
[112] Molina-Terriza G., Torres J. P. and Torner L., *Nat. Phys.*, **3** (2007) 305.
[113] Yao A. and Padgett M. J., *Adv. Opt. Photon.*, **3** (2011) 161.
[114] Fickler R., Lapkiewicz R., Plick W. N., Krenn M., Schaeff C., Ramelow S. and Zeilinger A., *Science*, **338** (2012) 640.
[115] Leach J., Jack B., Romero J., Ritsch-Marte M., Boyd R. W., Jha A. K., Barnett S. M., Franke-Arnold S. and Padgett M. J., *Opt. Express*, **17** (2009) 8287.
[116] Leach J., Jack B., Romero J., Jha A. K., Yao A. M., Franke-Arnold S., Ireland D. G., Boyd R. W., Barnett S. M. and Padgett M. J.,, *Science*, **329** (2010) 662.
[117] Krenn M., Huber M., Fickler R., Lapkiewicz R., Ramelow S. and Zeilinger A., *Proc. Natl. Acad. Sci. U.S.A.*, **111** (2014) 6243.

[118] Yao E., Franke-Arnold S., Courtial J., Barnett S. and Padgett M. J., *Opt. Express*, **14** (2006) 9071.
[119] Aharonov Y., Popescu S. and Tollaksen J., *Phys. Today*, **63** (2010) 27.
[120] Lundeen J. S. and Resch K. J., *Phys. Lett. A*, **334** (2005) 337.
[121] von Neumann J., *Mathematical Foundations of Quantum Mechanics* (Princeton University, Princeton, NJ) 1955.
[122] Davis J., McNamara D., Cottrell D. and Sonehara T., *Appl. Opt.*, **39** (2000) 1549.
[123] Dirac P., *Rev. Mod. Phys.*, **17** (1945) 195.
[124] Chaturvedi S., Ercolessi E., Marmo G., Morandi G., Mukunda N. and Simon R., *J. Phys. A-Math. Gen.*, **39** (2006) 1405.

Direttore responsabile: LUISA CIFARELLI

Prodotto e realizzato dalla Redazione del Nuovo Cimento, Bologna
Stampato da Compositori Comunicazione S.r.l. - Bologna
nel mese di Giugno 2014
su carta patinata ecologica chlorine-free
prodotta dalle *Cartiere del Garda S.p.A.*, Riva del Garda (TN)

Questo periodico
è iscritto
all'Unione Stampa
Periodica Italiana