Romanian Reports in Physics, Vol. 67, No. 4, P. 1300–1318, 2015

Dedicated to
International Year of Light 2015

QUANTUM INFORMATION AND QUANTUM TECHNOLOGIES

RADU IONICIOIU[1,2]

[1]Department of Theoretical Physics, National Institute of Physics and Nuclear Engineering IFIN-HH, 077125 Bucharest–Măgurele, Romania
[2]Research Center for Spatial Information – CEOSpaceTech, University Politehnica of Bucharest, 313 Splaiul Independenţei, 061071 Bucharest, Romania

Received September 14, 2015

Abstract. Quantum information is a recently emerged, paradigm-changing field which lays the foundations for quantum technologies. In this article we overview this fascinating subject, introduce the main mathematical concepts (entanglement, teleportation etc) and discuss forthcoming technologies like quantum computation, quantum cryptography, quantum imaging and quantum metrology.

Key words: Quantum information, quantum computation, quantum cryptography, quantum technologies.

1. INTRODUCTION

Quantum information (QI) and quantum technologies emerged recently as the "second quantum revolution" [1]. This turning point is based on a paradigm shift of how we view and process information.

The first quantum revolution started at the beginning of the last century with the development of quantum mechanics. This development enabled us to understand the structure of matter, from the atomic spectra to the structure of solids. In turn, the ability to calculate and predict these properties lead to the inception of key technologies, like laser, transistor and integrated circuit. These ubiquitous devices touch every aspect of our life and play a crucial role in the digital age, from computers and mobile phones to satellites and GPS.

If the first quantum revolution gave us the ability *to explain* the properties of matter (atoms, molecules, solids), the main focus of the second quantum revolution is the capacity *to control* individual quantum systems. Among other things, this ability enables us to construct new quantum systems with properties not found in nature. An example are artificial atoms (quantum dots) whose quantum properties (energy levels) can be tailored according to our needs, unlike those of natural atoms.

The paradigm change behind quantum information is rooted in Landauer's in-

sight that *information is physical*. Thus, if we store and process information using classical devices and the laws of classical physics, we have classical information science. In contrast, in quantum information science we use the laws of quantum mechanics to store and process information in quantum devices.

The main message behind the second quantum revolution [1] is simple: *quantum is a resource*. In other words, if we use quantum systems and manipulate them according to the laws of quantum (instead of classical) physics, we can perform things we cannot do with classical systems. Thus, although QI shares some similarities with classical information science, it goes beyond it and enables us to achieve results impossible by classical means only. Metaphorically, QI extends classical information science in the same way colour extends black-and-white imaging.

One can define quantum information as *the art of encoding and manipulating information in a quantum coherent way, using quantum systems and the laws of quantum mechanics*.

Historically, the field of quantum information emerged in the 1980s. Feynman realized that quantum systems can be more efficient than classical ones for certain problems, like the simulation of other quantum systems [2]. Deutsch introduced the first models of quantum computation, the quantum Turing machine [3] and the quantum network model [4]. Soon afterwards quantum algorithms outperforming classical ones were discovered: Deutsch-Jozsa [5], Simon [6], Shor [7, 8], Grover [9].

The "killer app" which launched the field of quantum information was Shor's algorithm: a quantum computer can factor large numbers in polynomial time, in contrast to the best classical algorithm which is exponential. This has huge implications for security (banking, internet transactions etc), since a quantum computer would be able to break codes efficiently, in contrast to a classical computer.

Starting from 1993 the field of quantum information grew exponentially. One of the main insights responsible for this growth was the realization that quantum resources allow us to perform tasks not possible classically – quantum teleportation [22] is a prime example. The central theme of the second quantum revolution is to harness the power of quantum resources like entanglement, superposition and nonlocality. This gave rise to a rapid development of several subjects like quantum computation, quantum cryptography, quantum metrology, quantum communication and quantum control.

The aim of this article is to give an overview of this fascinating field and of its many ramifications (Fig.1). The article is intended for a general audience with minimal background in quantum mechanics. We start by introducing the mathematical framework and the main concepts, like qubit, entanglement and teleportation. Then we will present the main research areas: quantum information, quantum computation, quantum communication and cryptography, quantum metrology. We end with a

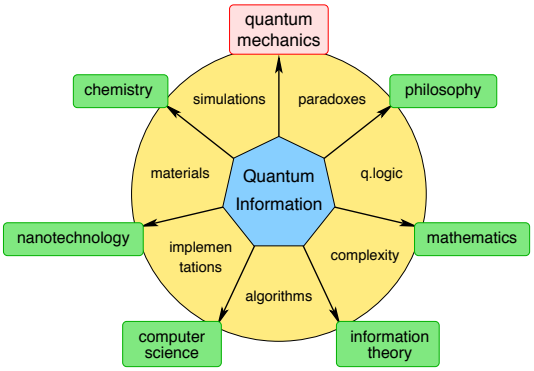


Fig. 1 – Quantum information is a paradigm-changing, multidisciplinary field having an impact in several areas.

discussion about the future quantum technologies and their impact.

2. QUANTUM INFORMATION: MATHEMATICAL BACKGROUND

In this section we introduce the fundamental concepts of quantum information and the required mathematical background. Some concepts will be familiar from classical information theory; other will be new and counterintuitive from a classical perspective. For more in-depth information, there are several overview articles [1, 10–12] and textbooks [13–17].

2.1. KINEMATICS

The basic element of quantum information is the *qubit*, or quantum bit. A qubit is a two-level quantum system and is described mathematically by a Hilbert space $\mathcal{H}$: a two-dimensional, complex vector space with inner product. The state of the qubit is a column vector in this space $|\psi\rangle \in \mathcal{H}$. The Hermitian conjugate of $|\psi\rangle$, denoted by $\langle\psi|$, is a row vector in the dual space:

$$|\psi\rangle = \begin{bmatrix} a \\ b \end{bmatrix} \quad , \quad \langle\psi| = \begin{bmatrix} \overline{a} & \overline{b} \end{bmatrix} \quad , \quad a, b \in \mathbb{C} \tag{1}$$

The scalar product between a vector $|x\rangle$ and a dual vector $\langle y|$ is a complex number $\langle x|y| \in \rangle \mathbb{C}$. Thus $\langle\psi|\psi| = \rangle |a|^2 + |b|^2$ is the norm (squared) of $|\psi\rangle$.

The state of a closed (isolated) quantum system is described by a unit vector $|\psi\rangle \in \mathcal{H}$, $\langle\psi|\psi| = \rangle 1$, called a *pure state*; open systems, described by mixed states ρ, will be discussed later. Since $|\psi\rangle$ and $e^{i\alpha}|\psi\rangle$ describe the same physical state, an overall phase is physically irrelevant. Thus an arbitrary pure state $|\psi\rangle$ of a qubit is parametrized by two real parameters (θ, φ) and can be viewed as a vector on the

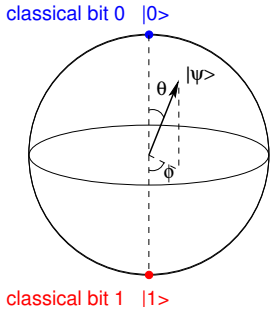


Fig. 2 – The Bloch sphere. Pure states, like $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$, are described by points on the surface of the sphere. The states $|0\rangle$ and $|1\rangle$ correspond to the north, and respectively south, pole. Mixed states are mapped to points inside the sphere, with the totally mixed state $\rho = \frac{1}{2}I$ at the center of the ball.

Bloch sphere, Fig.2:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle = \begin{bmatrix}\cos\frac{\theta}{2}\\ e^{i\varphi}\sin\frac{\theta}{2}\end{bmatrix} \tag{2}$$

where the vectors $|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}$ and $|1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$ form an orthonormal basis in the 2-dimensional Hilbert space of a qubit, $\langle j|i| = \rangle \delta_{ij},\ i,j = 0,1$.

One can straightforwardly generalize the qubit to a d-level quantum system, i.e., a *qudit*. The state of the qudit is a unit vector in a d-dimensional complex vector space

$$|\psi\rangle = \sum_{i=0}^{d-1} a_i|i\rangle = \begin{bmatrix}a_0\\ \vdots \\ a_{d-1}\end{bmatrix} \tag{3}$$

with $\sum_{i=0}^{d-1}|a_i|^2 = 1$, $a_i \in \mathbb{C}$. An arbitrary state of a qudit contains $2d-2$ real parameters (an overall phase is physically irrelevant).

Superposition principle. If $|\psi_1\rangle$, $|\psi_2\rangle$ are two states of a quantum system, then any linear combination $a|\psi_1\rangle + b|\psi_2\rangle$, $a,b \in \mathbb{C}$, is also a state (called a superposition state).

Composite systems. What happens if we have two quantum systems, for example two qubits? The total Hilbert space is the *tensor product* of individual Hilbert spaces

$$\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$$

and its dimension is the product of the two dimensions, $\dim\mathcal{H} = \dim\mathcal{H}_1 \cdot \dim\mathcal{H}_2$. This is in stark contrast with classical physics, where the composite system is de-

scribed by the *cartesian product* of individual spaces

$$\mathcal{S} = \mathcal{S}_1 \times \mathcal{S}_2$$

and the total dimension is $\dim \mathcal{S} = \dim \mathcal{S}_1 + \dim \mathcal{S}_2$. Thus for n quantum systems the total Hilbert space grows exponentially, $\dim \mathcal{H} = \prod_i \dim \mathcal{H}_i$; for n qubits we have $\dim \mathcal{H} = 2^n$. On the other hand, the resources required to describe a classical system grow only polynomially with the number of subsystems since $\dim \mathcal{S} = \sum_i \dim \mathcal{S}_i$; for n two-dimensional classical systems the total space has dimension $2n$.

This brings us to Feynman's insight mentioned before: it is very difficult to simulate a quantum system on a classical computer due to the exponential increase of the Hilbert space with the number of subsystems [2]. In order to simulate the evolution of n qubits we need to keep track of 2^n coefficients, for example, in a computer register. Feynman turned this problem on its head: why not simulate a quantum system on another (well-controlled) quantum system. Thus he introduced the idea of a *universal quantum simulator* which can simulate a quantum system using only polynomial resources. This was the first hint that quantum computers can be more efficient than classical ones for certain problems.

2.2. DYNAMICS

So far we have discussed the kinematics of qubits, i.e., the structure of the Hilbert space $\mathcal{H}$ of quantum states. We now turn to dynamics, namely how quantum states change in time.

There are two different processes through which a state can change. The first is the unitary evolution and this is a reversible process. We can transform a quantum state $|\psi\rangle$ by acting on it with a device; for a photon, examples include wave-plates changing the polarisation, or beam-splitters acting on spatial modes. Such a transformation is reversible since we can undo it by acting with another wave-plate with opposite rotation and hence recover the initial state $|\psi\rangle$.

Unitary evolution. The evolution of a closed system between two states $|\psi_0\rangle$ and $|\psi_1\rangle$ is given by a unitary matrix U

$$|\psi_0\rangle \mapsto |\psi_1\rangle = U|\psi_0\rangle \tag{4}$$

with $UU^\dagger = U^\dagger U = I$. This transformation is linear, i.e., the evolution of an arbitrary superposition is $\alpha|\phi_0\rangle + \beta|\phi_1\rangle \mapsto \alpha U|\phi_0\rangle + \beta U|\phi_1\rangle$. Note also that a unitary transformation preserves the norm, $\langle\psi_1|\psi_1| =\rangle \langle\psi_0|U^\dagger U|\psi_0\rangle = \langle\psi_0|\psi_0|$.

The second way a state can change is by measuring an observable $\mathcal{A}$, and this is an irreversible process.

Observables. A physical observable $\mathcal{A}$ corresponds to a Hermitian operator $A^\dagger = A$ acting on the Hilbert space $\mathcal{H}$ of the system, $A : \mathcal{H} \to \mathcal{H}$. Denote by a_i and $|a_i\rangle$ the eigenvalues and, respectively, eigenvectors of A; thus $A|a_k\rangle = a_k|a_k\rangle$. The

eigenvectors form an orthonormal basis $\langle a_j|a_i| =\rangle \delta_{ij}$ and the eigenvalues are real $a_i = a_i^*$ (since A is Hermitian). From the singular value decomposition theorem, we have $A = \sum_i a_i |a_i\rangle \langle a_i|$.

Measurement. The result of the measurement of observable $\mathcal{A}$ on the quantum system gives one of the eigenvalues a_j of the associated operator A. Suppose the quantum system is prepared in the initial state $|\psi\rangle$. Since the eigenvectors of A form an orthonormal basis, we can decompose the initial state as

$$|\psi\rangle = \sum_i x_i |a_i\rangle$$

with $\sum_i |x_i|^2 = 1$ since $\langle\psi|\psi| =\rangle 1$. The measurement randomly projects the initial state $|\psi\rangle$ onto one of the basis eigenvectors, say $|a_j\rangle$, with probability $p_j = |\langle\psi|a_j||\rangle^2 = |x_j|^2$; for simplicity we assumed the eigenvalues are nondegenerate. After the measurement the system will be found in the eigenstate $|a_j\rangle$ corresponding to the measured eigenvalue a_j.

Two important observations are in order here. First, the outcome of a measurement is *probabilistic* – one cannot predict the result of a measurement, only the probability of obtaining a particular value.

Second, a measurement corresponds to a set of orthogonal projectors $\{P_j = |a_j\rangle \langle a_j|\}$, with $P_i = P_i^\dagger$ and $P_i P_j = \delta_{ij} P_i$. Thus a measurement has an associated basis $\{|a_j\rangle\}$ on which it projects. A different physical observable $\mathcal{B}$ has associated a Hermitian operator B and another set of projectors $\{P'_j = |b_j\rangle \langle b_j|\}$. The measurement of $\mathcal{B}$ projects the qubit state into one of the basis vectors $\{|b_k\rangle\}$. Thus the same initial state $|\psi\rangle$ has different decompositions in the two bases, i.e., $|\psi\rangle = \sum_i x_i |a_i\rangle = \sum_k x'_k |b_k\rangle$.

Consider a simple example. Suppose we prepare a qubit in the initial state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. If we measure $|\psi\rangle$ in the computational basis $\{|0\rangle, |1\rangle\}$, one will randomly obtain either $|0\rangle$, with probability $|\alpha|^2$, or $|1\rangle$, with probability $|\beta|^2$. However, assume we measure the same state $|\psi\rangle$ in the basis $\{|+\rangle, |-\rangle\}$, with $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. Since

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \tfrac{\alpha+\beta}{\sqrt{2}}|+\rangle + \tfrac{\alpha-\beta}{\sqrt{2}}|-\rangle$$

this measurement will now project either on $|+\rangle$, with probability $\frac{1}{2}|\alpha+\beta|^2$, or on $|-\rangle$, with probability $\frac{1}{2}|\alpha-\beta|^2$.

As the state *collapses* after the measurement, we cannot recover the full description of the state (the coefficients α, β) from a *single* measurement. This brings us to another crucial distinction between the classical and quantum worlds: a quantum measurement perturbs the system. In order to reconstruct the initial state $|\psi\rangle$ we need to perform *quantum tomography* on several identically prepared systems. From

this statistics we calculate α and β.

There are other fundamental differences between classical and quantum systems which play an important role in quantum information. The linearity of quantum mechanics implies two key results that have no classical analog: the *no cloning* and *no deleting* theorems.

No-cloning theorem [18]: *An unknown quantum state $|\psi\rangle$ cannot be cloned.*

The theorem states that there is no quantum process (or device) which can *perfectly* copy an unknown quantum state $|\psi\rangle$:

$$|\psi\rangle |0\rangle \not\mapsto |\psi\rangle |\psi\rangle$$

The proof follows from the linearity of unitary evolution discussed above.

Nevertheless, one can clone an unknown state *imperfectly*; and we can perfectly clone only certain states (e.g., from a known orthogonal basis).

The no-cloning theorem is a cornerstone of quantum cryptography and ensures the secrecy of the transmitted key. Thus an eavesdropper cannot make perfect copies of an unknown quantum state, and consequently cannot reconstruct the initial state by measuring the copies.

No-deleting theorem [19]: *An unknown quantum state $|\psi\rangle$ cannot be deleted.*

This is the inverse of the no-cloning theorem and follows, again, from the linearity of quantum mechanics.

2.3. MIXED STATES

So far we have discussed closed quantum systems described by pure states $|\psi\rangle$. However, not all quantum systems can be described by pure states – unpolarized light is an example.

Another example are systems interacting with the environment. Such a system is no longer in a pure state. In this case the system is described by a mixed state ρ. One can view ρ as an incoherent (probabilistic) mixture of different pure states $|\psi_i\rangle$

$$\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i| \tag{5}$$

where $0 \leq p_i \leq 1$, $\sum_i p_i = 1$ are probabilities. The state is pure if the sum has only one term, $p_i = \delta_{i0}$.

For qubits, mixed states are mapped to points inside the Bloch sphere, Fig.2. For example, unpolarized light is described by the totally mixed state and corresponds to the center of the sphere

$$\rho = \tfrac{1}{2} I = \tfrac{1}{2}(|H\rangle \langle H| + |V\rangle \langle V|) = \tfrac{1}{2}(|R\rangle \langle R| + |L\rangle \langle L|)$$

and this decomposition is not unique. Thus one can view unpolarized light as an incoherent mixture of H- and V-polarised photons, or equally valid, as an incoherent

mixture of right- and left-polarized photons; more generally, as an incoherent mixture of photons polarised along any two orthogonal directions. Importantly, a mixed state is different from a coherent superposition of states like $|+\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$; the two states give experimentally distinct statistics upon measurement in various bases.

Mathematically, the density matrix $\rho \in \mathcal{L}(\mathcal{H})$ is a linear operator acting on the Hilbert space $\mathcal{H}$. It is Hermitian $\rho = \rho^\dagger$, normed $\mathrm{Tr}\,(\rho) = 1$ and semi-positive definite (has eigenvalues $\lambda_i \geq 0$). It is straightforward to see that $\mathrm{Tr}\,(\rho^2) \leq 1$. Moreover, ρ is a pure state if and only if $\rho^2 = \rho$, hence $\mathrm{Tr}\,(\rho^2) = 1$. For pure states $\rho = |\psi\rangle\langle\psi|$ is a projector.

Assume we have a quantum system prepared in the state ρ and we measure the observable $A = \sum_i a_i |a_i\rangle\langle a_i|$; as before, a_i and $|a_i\rangle$ are the eigenvalues and, respectively, eigenvectors of A. The probability to measure the eigenvalue a_i, corresponding to eigenvector $|a_i\rangle$, is $p_i = \mathrm{Tr}\,(\rho |a_i\rangle\langle a_i|)$. Therefore the *expectation value* (i.e., the experimental average) of A for a system prepared in the state ρ is: $\langle A\rangle = \sum_i p_i a_i = \mathrm{Tr}\,(\rho A)$. For pure states this reduces to $\langle A\rangle = \langle\psi| A |\psi\rangle$.

To summarize, in this section we introduced the mathematical background of quantum information. A quantum system has associated a complex Hilbert space $\mathcal{H}$. The state of the system is described by a density operator $\rho \in \mathcal{L}(\mathcal{H})$; for pure states, ρ is a projector and we can describe the system by a vector $|\psi\rangle \in \mathcal{H}$. For qudits, the Hilbert space is finite dimensional with $\dim\mathcal{H} = d$. The Hilbert space of a composite system is the tensor product $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \ldots$ and has dimension $\dim\mathcal{H} = \prod_i \dim\mathcal{H}_i$. The dynamics of a quantum system is given by two distinct processes: either a unitary (reversible) evolution U, or a projective (irreversible) measurement $\{|a_j\rangle\langle a_j|\}$ associated with a Hermitian operator A.

3. QUANTUM COMPUTATION

We now turn to quantum computation and the quantum network model. Similar to a classical computer, a universal quantum computer can be build from a set of single- and two-qubit gates. We then discuss quantum entanglement and its essential role as a resource in quantum protocols.

3.1. QUANTUM GATES

As in the classical case, quantum computation is performed by a succession of elementary steps. A gate – classical or quantum – is a transformation between an input state and an output state (Fig.3(a)).

Classical logic is described in the framework of boolean algebras. An important result is that any boolean function can be decomposed as a product of elementary gates belonging to a universal set of gates. This gives the universality theorem of

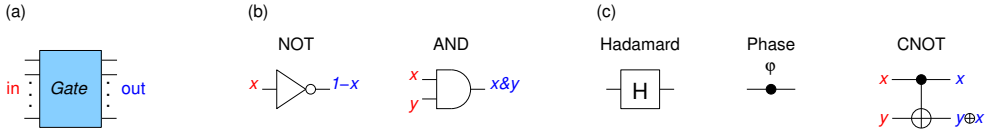


Fig. 3 – (a) A gate is a transformation between input and output. Universal sets of gates: (b) classical computing $\{\mathsf{NOT}, \mathsf{AND}\}$; (c) quantum computing $\{\mathsf{H}, \mathsf{P}_\varphi, \mathsf{CNOT}\}$.

classical logic: any classical computer can be constructed by implementing only this universal set of gates. There are several equivalent universal set of classical gates, such as $\{\mathsf{NOT}, \mathsf{AND}\}$, $\{\mathsf{NOT}, \mathsf{OR}\}$ or $\{\mathsf{NAND}\}$, Fig.3(b).

In the quantum case there exists a similar universality result. Any quantum algorithm on n qudits can be decomposed as a product of elementary gates from the universal set. A quantum gate is a unitary matrix (acting on the Hilbert space of n qudits) and maps an input state to an output state. Thus a single qudit gate is a unitary $d \times d$ matrix (2×2 for a qubit) and a two-qudit gate is a $d^2 \times d^2$ unitary matrix (4×4 for qubits). In the following we will focus only on qubit gates. Examples of single-qubit gates include the Pauli matrices

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \; Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \; Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{6}$$

the Hadamard gate $H = \frac{1}{\sqrt{2}}(X + Z) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ and the phase-shift gate $P_\varphi = \mathrm{diag}(1, \mathrm{e}^{\mathrm{i}\varphi}) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix}$. We denote by I the identity and by $\mathbf{0}$ the zero-matrix. The action of the X gate is a *bit flip*, $|x\rangle \mapsto |x \oplus 1\rangle$ and of Z gate a *sign flip* $|x\rangle \mapsto (-1)^x |x\rangle$.

Like in the classical case, there are several equivalent universal sets of gates – this freedom allows us to implement different universal gates tailored to the physical system used to implement the qubit. Various quantum systems have different types and strengths of qubit interactions. Consequently, on a given quantum system some gates are easier to implement than others.

Universality. The following set of gates is universal for quantum computation [20], Fig.3(c):

$$\{\mathsf{H}, \mathsf{P}_\varphi, \mathsf{CNOT}\} \tag{7}$$

The single qubit gates H and P_φ generate all single-qubit rotations $U \in U(2)$. Any 2×2 unitary matrix can be written as a product of three rotations along two different axes x, z:

$$U = e^{i\phi} e^{i\alpha Z} e^{i\beta X} e^{i\gamma Z}$$

α, β, γ play the role of the Euler angles for a rotation in 3-dimensions and ϕ is an overall phase. In terms of the universal gates $\mathsf{H}, \mathsf{P}_\varphi$ we have $U = e^{i\phi'} \mathsf{P}_{\alpha'} \mathsf{H} \mathsf{P}_{\beta'} \mathsf{H} \mathsf{P}_{\gamma'}$ for some angles α', β', γ'.

The two-qubit CNOT gate is an entangling gate:

$$\mathsf{CNOT} = \begin{bmatrix} I & \mathbf{0} \\ \mathbf{0} & X \end{bmatrix} \tag{8}$$

The CNOT gate maps $|x\rangle |y\rangle \mapsto |x\rangle |y \oplus x\rangle$. The universality theorem ensures that an arbitrary n-qubit quantum algorithm can be implemented efficiently by an array of gates from the set (7).

This is known as the *quantum network model* [4] and is the "standard model" of quantum computation. Other computational models are: the quantum Turing machine [3], quantum cellular automata, adiabatic quantum computation and measurement-based quantum computation [21]. Although these models are computationally equivalent to the standard quantum network model, the way the computation is realised is very different. For example, in the adiabatic quantum computation the final result is encoded in the ground state of a Hamiltonian.

3.2. ENTANGLEMENT

An important open problem in quantum information is to identify the key resources which make quantum computation more powerful than classical one. Although the problem is not fully solved, entanglement is one such resource (other resources are nonlocality, discord etc). In this section we introduce and discuss briefly this fascinating topic.

Entanglement is a quintessential quantum property – it has no classical analog and cannot be described intuitively. For Schrödinger, entanglement was "*the* characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought". Einstein, on the other hand, called it *spooky action at a distance*.

Entanglement is also a quantum resource which enables us to perform tasks impossible in a classical world: teleportation of an unknown state, superdense coding and quantum cryptography, among others.

So, what is entanglement? A quantum state is *entangled* if it cannot be written as a tensor product $|\psi\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle$. A tensor product state $|\psi_1\rangle \otimes |\psi_2\rangle$ is called *separable*. For simplicity we will denote tensor product states like $|\psi_1\rangle \otimes |\psi_2\rangle$ by $|\psi_1\rangle |\psi_2\rangle$ or $|\psi_1 \psi_2\rangle$.

Bell states. The simplest example of entanglement is found in a two-qubit system. The following four states play an crucial role in quantum information and are called

the Bell states:

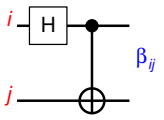
$$\left|\Phi^{\pm}\right\rangle = \tfrac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)\ , \quad \left|\Psi^{\pm}\right\rangle = \tfrac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \tag{9}$$

These states are maximally entangled and form an orthogonal basis (the Bell basis) in the two-qubit Hilbert space. A compact notation for the Bell states is

$$|\beta_{ij}\rangle = \tfrac{1}{\sqrt{2}}(|0\,i\rangle + (-1)^j\,|1\,i\oplus 1\rangle)\ , \quad i,j=0,1$$

Thus $|\beta_{00}\rangle = |\Phi^+\rangle$, $|\beta_{01}\rangle = |\Phi^-\rangle$ etc.

Starting from the separable basis states $|ij\rangle$, we can generate the four Bell states with the following quantum network:



The reverse network (first CNOT, then the Hadamard gate H) is equivalent to a Bell-state measurement. A Bell state measurement (or Bell measurement) projects a two-qubit state on one of the four Bell states $|\beta_{ij}\rangle$.

The following is a simple criterion to determine if a two-qubit state is entangled or not.

Proposition. *A (pure) two-qubit state* $\sum_{i,j=0,1} a_{ij}\,|ij\rangle$ *is entangled if and only if* $|a_{00}a_{11} - a_{01}a_{11}| \neq 0$.

Thus, for a pure two-qubit state we can define an entanglement measure, called *concurrence*:

$$C = \sqrt{2|a_{00}a_{11} - a_{01}a_{10}|} \tag{10}$$

We can show that $0 \leq C \leq 1$. For all separable states $C = 0$; for the maximally entangled Bell states $C = 1$.

Crucially, entanglement is invariant under arbitrary local unitaries $U_A \otimes U_B$. Thus, starting with a separable state $|\psi_A\rangle\,|\psi_B\rangle$ one cannot create an entangled state by performing only local operations and classical communication (LOCC). In order to produce entanglement we need to have an interaction between the two qubits A and B, or use a quantum channel (like in entanglement swapping, see below).

Multi-qubit entanglement. Although two-qubit entanglement is straightforward to characterise, multipartite entanglement between several qubits or qudits is much more difficult to analyse. This is an active research area, but so far there is no general classification of multipartite entanglement. We do not have a complete picture of how to characterise entanglement between different quantum systems or what is a good (and complete) entanglement measure.

Nevertheless, there are several important results. For example, three qubits can

be entangled in two nonequivalent ways, the so called GHZ and W families:

$$|GHZ\rangle = \tfrac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \tag{11}$$

$$|W\rangle = \tfrac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle) \tag{12}$$

These two states have different "flavours" of entanglement and can be generalized to n qubits:

$$|GHZ_n\rangle = \tfrac{1}{\sqrt{2}}(|0\ldots0\rangle + |1\ldots1\rangle) = \tfrac{1}{\sqrt{2}}(|0\rangle^{\otimes n} + |1\rangle^{\otimes n}) \tag{13}$$

$$|W_n\rangle = \tfrac{1}{\sqrt{n}}(|10\ldots0\rangle + |01\ldots0\rangle + \ldots + |0\ldots01\rangle) = \tfrac{1}{\sqrt{n}}\sum_{k=1}^{n} X_k\,|0\rangle^{\otimes n} \tag{14}$$

where X_k is a bit flip acting on qubit k. The GHZ- and W-type of states can be used as a resource for different quantum protocols, i.e., to perform different tasks. Many other families of entangled states are known, like Dicke states, stabilizer/graph states, concatenated GHZ states, matrix product states etc.

Entanglement generation. Since entanglement is a *sine-qua-non* resource in different quantum information tasks (communication, computation, teleportation) generating different entangled states in a controlled way is very important.

Photonic entanglement is generated by spontaneous parametric down conversion (SPDC): a pump laser, incident on a nonlinear crystal, randomly produces pairs of entangled photons. The problem of SPDC is the low efficiency (roughly only one in 10^{12} pump photons yields an entangled photon pair) and the random nature of the process.

Thus an important milestone for quantum technologies is to have an on-demand source of entangled photons working at room temperature: whenever we press a button, an entangled photon pair is produced. Promising technologies for generating on-demand photonic entanglement are NV centers in diamond, quantum dots and integrated photonic chips.

3.3. QUANTUM PROTOCOLS

After discussing entanglement in the previous section, we now turn to its use as a resource. In this section we describe several well-known quantum protocols. These protocols have no classical equivalent and can be viewed as building blocks, or primitives, for more complex quantum communication tasks. The two parties involved are usually called Alice and Bob.

Teleportation [22]. In this protocol Alice and Bob share an entangled state, say $|\Phi^+\rangle = |\beta_{00}\rangle$. Alice also has another qubit, in an unknown state $a\,|0\rangle + b\,|1\rangle$, which she wants to teleport to Bob. She performs a Bell state measurement on this qubit and her half of the entangled pair, thus obtaining two classical bits $i, j = 0, 1$ which

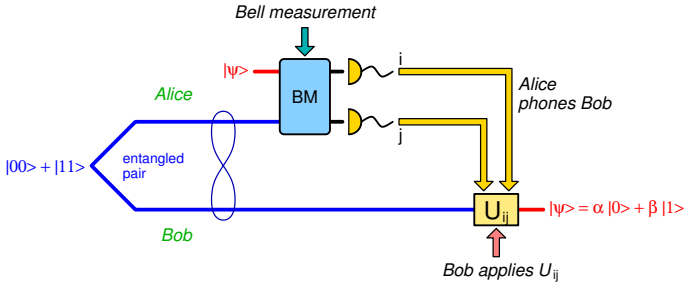


Fig. 4 – Quantum teleportation.

she sends to Bob. Upon receiving the two bits i,j, Bob applies a transformation on his half of the entangled pair shared with Alice and recovers the unknown state $a|0\rangle + b|1\rangle$. The protocol is shown in Fig.4.

We can write the state of the three qubits (the first qubit is the unknown one and the other two are the entangled pair $|\Phi^+\rangle_{23}$) in the following way:

$$\begin{aligned}(a|0\rangle + b|1\rangle)_1 \otimes |\Phi^+\rangle_{23} = \tfrac{1}{2}\{ & |\Phi^+\rangle_{12} \otimes (a|0\rangle + b|1\rangle)_3 \\ & + |\Phi^-\rangle_{12} \otimes (a|0\rangle - b|1\rangle)_3 \\ & + |\Psi^+\rangle_{12} \otimes (a|1\rangle + b|0\rangle)_3 \\ & + |\Psi^-\rangle_{12} \otimes (a|1\rangle - b|0\rangle)_3\} \end{aligned} \tag{15}$$

In a compact notation this is $\sum_{i,j} |\beta_{ij}\rangle_{12}\ [U_{ij}(a|0\rangle + b|1\rangle)]_3$, where $U_{ij} \in \{I, Z, X, XZ\}$, $i,j = 0,1$ is a unitary transformation.

After Alice performs a Bell measurement on the first two qubits (and obtains two classical bits i,j), the third qubit will collapse to $[U_{ij}(a|0\rangle + b|1\rangle)]_3$. To recover the unknown state $a|0\rangle + b|1\rangle$, Bob has to apply the corresponding inverse transformation $U_{ij}^{-1} \in \{I, Z, X, ZX\}$. This explains why Alice needs to send Bob the two classical bits i,j.

Superdense coding [23]. This protocol is the dual of teleportation: Alice transmits to Bob two classical bits by sending one physical qubit, Fig.5(a).

As before, Alice and Bob share an entangled pair. Alice encodes two classical bits i,j by applying to its state one of the four unitaries $U_{ij} \in \{I, Z, X, XZ\}$, then sends her qubit to Bob. On his side, Bob performs a Bell measurement and obtains the two bits i,j encoded by Alice.

It is important to note that in both teleportation and superdense coding Alice and Bob consume a maximally entangled state (Bell pair). Thus entanglement is a consumable resource which has to be replenished.

Entanglement swapping [24]. Suppose we start with two pairs of entangled particles (1,2) and (3,4): $|\Phi^+\rangle_{12}|\Phi^+\rangle_{34}$. This state can be written as a sum of pairs of

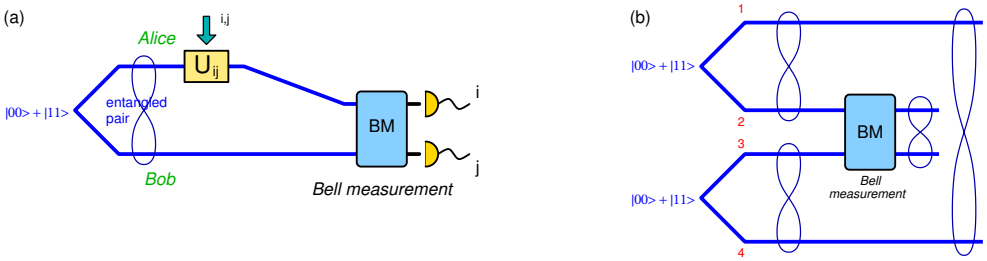


Fig. 5 – Quantum protocols. (a) Superdense coding. (b) Entanglement swapping.

entangled Bell states, but now between particles (1,4) and (2,3): $|\Phi^+\rangle_{12}|\Phi^+\rangle_{34} = \frac{1}{2}\sum_{ij}|\beta_{ij}\rangle_{14}|\beta_{ij}\rangle_{23}$. Explicitly, we have

$$|\Phi^+\rangle_{12}|\Phi^+\rangle_{34} = \tfrac{1}{2}\{|\Phi^+\rangle_{14}|\Phi^+\rangle_{23} + |\Phi^-\rangle_{14}|\Phi^-\rangle_{23} + |\Psi^+\rangle_{14}|\Psi^+\rangle_{23} + |\Psi^-\rangle_{14}|\Psi^-\rangle_{23}\} \quad (16)$$

Assume we now perform a Bell-state measurement on particles (2,3). This will randomly project particles (2,3) on one of the Bell states and, simultaneously, also project the other two particles (1,4) on the same Bell state. The result of this operation is to swap the entanglement between the pairs: (1,2) (3,4) → (1,4) (2,3), see Fig.5(b).

This protocol shows that two particles which never interacted directly can be entangled. Entanglement swapping is an essential primitive for entanglement distribution over arbitrary distances. In optical fibres single photons can travel ∼300 km before they are absorbed. Since cloning is forbidden, quantum repeaters use entanglement swapping in order to extend the entanglement link beyond the distance of direct communication. The protocol is thus essential for a future *quantum internet*.

4. QUANTUM TECHNOLOGIES

In this section we briefly overview several applications of quantum information. We will see how previously discussed concepts – superposition, entanglement, no-cloning etc – are the cornerstones of new quantum technologies. These technologies play an increasingly important role and mark the dawn of the second quantum revolution [1].

4.1. QUANTUM CRYPTOGRAPHY

Quantum key distribution (QKD), also known as quantum cryptography [25], is the most mature quantum technology. This is an active research field with new

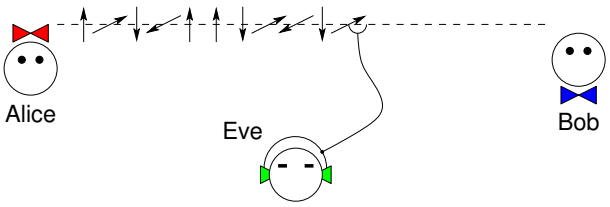


Fig. 6 – The BB84 protocol. Alice sends single photons polarized $|H\rangle, |V\rangle, |+\rangle$ or $|-\rangle$. Bob randomly measures in either H/V or $\pm$ basis. The no-cloning theorem ensures an eavesdropper (Eve) will increase the error rate hence will be detected.

protocols discovered (and improved) regularly. Here we briefly describe only the Bennett-Brassard (BB84) protocol. Other examples can be found in Ref. [25].

In BB84 the two parties, Alice and Bob, establish a secret key which they subsequently use for encryption. The classical part of the protocol employs the one-time pad (Vernam cipher) which is provably secure if:
(i) the key is a random number with the same length as the message;
(ii) the key is never reused;
(iii) the key is known only to Alice and Bob.

To encode the message, Alice XORs bitwise the plaintext with the secret key. The resulting cipher-text is transmitted via a public channel to Bob. To decrypt the message, Bob XORs the cipher-text with the same secret key and obtains the original message.

The main problem of the one-time pad is to ensure the distribution of the secret key between Alice and Bob. The key is consumable (it is never reused) so the parties need a fresh key for each message. In a classical world an eavesdropper can intercept and copy the key without Alice and Bob knowing. Quantum cryptography solves the problem of distributing securely the key between Alice and Bob (hence the name QKD).

In the BB84 protocol Alice sends Bob single photons prepared in one of the four polarizations (Fig.6): $|H\rangle, |V\rangle, |+\rangle, |-\rangle$, where $H(V)$ denote horizontal (vertical) polarization and $|\pm\rangle = \frac{1}{\sqrt{2}}(|H\rangle \pm |V\rangle)$. Bob randomly measures in either H/V or $\pm$ basis. In the basis reconciliation step, Alice publicly announces the basis (but not the value) in which she sent the photons. Bob compares this with the basis in which he measured the photons and they both keep only those measurements for which the two bases coincide. Only in this case the value of the qubit sent by Alice is the same as the value measured by Bob. These values form the raw key from which the final secret key is extracted following other classical steps (privacy amplification etc).

The no-cloning theorem ensures that an eavesdropper (Eve) cannot perfectly copy an unknown state. If Eve tries to measure the single photon, she will introduce

errors and thus will be detected. In case the measured error rate is above a certain threshold (depending on the protocol), the communication is insecure and Alice and Bob abort the protocol.

QKD systems already exists on the market and are commercialised by companies like ID Quantique [26] and MagiQ [27]. State of the art QKD experiments have a range of $\sim$144 km in free space and $\sim$300 km in optical fibre [28]. In order to extend the range of optical fiber QKD systems above 300 km we need to use quantum repeaters. However, quantum repeaters are not yet implemented due to technological difficulties (like viable quantum memories); these, nevertheless, can be overcome in the foreseeable future.

For a global quantum network (quantum internet) a crucial step is to achieve a QKD exchange between a ground station and a satellite [29]. Several research groups from Austria, Canada, China, Italy are working to implement ground-to-space QKD in the near future.

4.2. QUANTUM METROLOGY, SENSING, IMAGING

After quantum cryptography, the second generation of quantum technologies most likely to emerge are quantum metrology [30, 31], sensing and imaging [32].

Quantum sensing/imaging technologies [32] are developing fast and several applications have been proposed recently: quantum lithography [33], quantum illumination [34], quantum-enhanced positioning and clock synchronisation [35], longer-baseline telescopes [36], super-resolving quantum radar [37], quantum spectroscopy [38], compressive object tracking with entangled photons [39], entanglement-enhanced microscope [40], quantum-secured imaging [41], probing delicate materials [42]. The main idea is to use entangled states as a resource to beat the standard quantum limit (shot-noise limit), in the case of metrology and sensing, or the diffraction limit, in the case of lithography.

To understand how quantum metrology works, consider the standard way to measure an unknown parameter φ. We prepare a probe in a known state, then we let the probe to interact with the system, and finally we measure the probe. This is equivalent to apply a known signal at the input of a "black box" (the unknown parameter) and then to measure the output; by processing the output signal we estimate the parameter φ (prepare, probe, measure, estimate).

A very general scheme is shown in Fig. 7, where the unknown parameter φ is the phase difference between two arms of a Mach-Zehnder Interferometer (MZI). Here the phase difference is proportional to the length difference x between the two arms $\varphi = \frac{2\pi}{\lambda}x$. The same scheme can be used for atomic clocks, in which case $\varphi = \omega t$, with ω the transition frequency between two atomic levels. The precision of the clock is given by how precise we measure the phase φ.

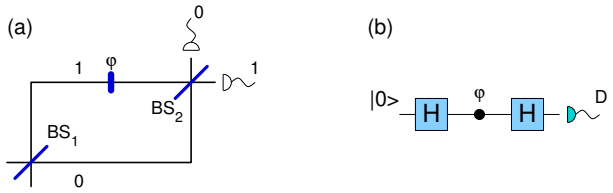


Fig. 7 – (a) A Mach-Zehnder interferometer (MZI) used to measure an unknown phase φ. (b) The equivalent quantum network, where the beam-splitters correspond to a Hadamard gate H and the phase shifter to P_φ.

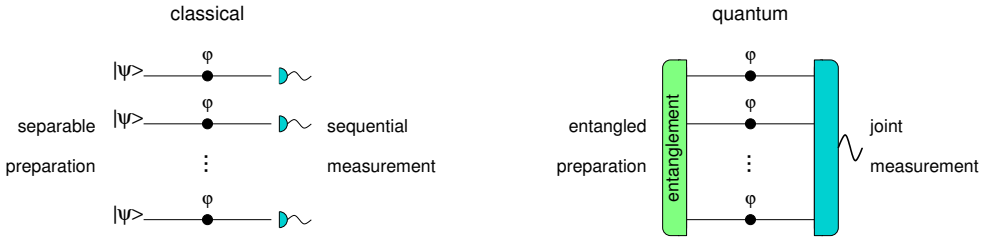


Fig. 8 – Classical vs. quantum measurement protocols [30, 31] for estimating an unknown parameter φ. Classical: the N photons are prepared in a separable state $|\psi\rangle^{\otimes N}$. Quantum: the initial N-photon state is entangled.

Microscopically, a signal is composed of a number N of photons prepared in some initial state. For a classical signal, the photons are uncorrelated, hence the initial state is equivalent to a separable state $|\psi\rangle^{\otimes N}$. In this case the error in estimating the parameter φ (giving the measurement precision) is [30, 31]:

$$\delta\varphi_C \sim \frac{1}{\sqrt{N}}$$

Suppose now we use as a probe a quantum signal, i.e., we prepare the N photons in an entangled state (Fig. 8). In this case the resolution becomes

$$\delta\varphi_Q \sim \frac{1}{N}$$

Which quantum states can achieve this precision? An example is the $|GHZ_N\rangle$ state. For N photons in a Mach-Zehnder interferometer, this is equivalent to the $NOON$-state, $|NOON\rangle = \frac{1}{\sqrt{2}}(|N0\rangle + |0N\rangle)$. To summarize, we have:

	classical	quantum
$\|\psi_{in}\rangle$	$\|+\rangle^{\otimes N}$	$\|GHZ_N\rangle$
$\delta\varphi$	$\frac{1}{\sqrt{N}}$	$\frac{1}{N}$

In conclusion, using entangled states as quantum probes improves the measurement

precision by $\sqrt{N}$ compared to a classical state.

A similar result can be achieved in quantum lithography [33] and quantum microscopy [40]. By using $NOON$ states we can achieve super-resolution $\delta x \sim \frac{\lambda}{2N}$, thus beating the Abbe limit $\delta x \sim \frac{\lambda}{2}$ from classical optics.

5. CONCLUSION AND FUTURE IMPACT

It is difficult to overstate the role of fundamental physics in the history of civilisation. Thermodynamics played a central role in developing efficient steam engines crucial to the Industrial Revolution. Electromagnetism and Maxwell equations were the main drivers of technology during the 20th century – electricity, radio, television, interplanetary communication, radar, computer, internet etc – culminating with the Digital Revolution.

In the 21st century quantum technologies, rooted in quantum mechanics and Schrödinger equation, will come center stage. Quantum information science and quantum mechanics are expected to play a similar role to that of classical information theory and electromagnetism in the past century.

The 2012 Nobel Prize for physics reflects the growing importance of quantum information. The prize was awarded to Serge Haroche and David Wineland [43]

"for ground-breaking experimental methods that enable measuring and manipulation of individual quantum systems."

We are at the beginning of the second Quantum Revolution [1] and it is impossible to predict where this journey will end or what discoveries will be made on the way. But one thing is certain – like previous fundamental theories of physics, it will have a profound impact on society.

REFERENCES

1. J.P. Dowling and G.J. Milburn, Phil. Trans. R. Soc. A **361**, 1655 (2003); quant-ph/0206091.
2. R.P. Feynman, Int. J. Theor. Phys. **21**, 467 (1982).
3. D. Deutsch, Proc. Roy. Soc. Lon. A **400**, 97 (1985).
4. D. Deutsch, Proc. Roy. Soc. Lon. A **425**, 73 (1989).
5. D. Deutsch and R. Jozsa, Proc. Roy. Soc. Lon. A **439**, 553 (1992).
6. D.R. Simon, *On the power of quantum computation*, Proceedings of the 35th Annual Symposium on the Foundations of Computer Science (IEEE Press, Los Alamitos, 1994), p. 116.
7. P.W. Shor, *Algorithms for Quantum Computation: Discrete Logarithms and Factoring*, Proceedings of the 35th Annual Symposium on the Foundations of Computer Science (IEEE Press, Los Alamitos, 1994), p. 124.
8. P.W. Shor, SIAM J. Sci. Stat. Comput. **26**, 1484 (1997).
9. L.K. Grover, Phys. Rev. Lett. **79**, 325 (1997).
10. C.H. Bennett and D.P. DiVincenzo, Nature **404**, 247 (2000).

11. C.M. Caves, arXiv:1302.1864.
12. E.G. Rieffel and W. Polak, arXiv:quant-ph/9809016.
13. M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2010.
14. N.S. Yanofsky and M.A. Mannucci, *Quantum Computing for Computer Scientists*, Cambridge University Press, 2008.
15. E.G. Rieffel and W.H. Polak, *Quantum Computing: A Gentle Introduction*, MIT Press, 2011.
16. N.D. Mermin, *Quantum Computer Science: An Introduction*, Cambridge University Press, 2007.
17. Scott Aaronson, *Quantum Computing since Democritus*, Cambridge University Press, 2013.
18. W. Wootters and W. Zurek, Nature **299**, 802 (1982).
19. A.K. Pati and S.L. Braunstein, Nature **404**, 104 (2000).
20. A. Barenco *et al.*, Phys. Rev. A. **52**, 3457 (1995).
21. R. Raussendorf and H.J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
22. C.H. Bennett *et al.*, Phys. Rev. Lett. **70**, 1895 (1993).
23. C.H. Bennett and S.J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
24. M. Żukowski, A. Zeilinger, M.A. Horne, and A.K. Ekert, Phys. Rev. Lett. **71**, 4287 (1993).
25. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
26. http://www.idquantique.com
27. http://www.magiqtech.com
28. B. Korzh *et al.*, Nature Photonics **9**, 163 (2015).
29. N. Horiuchi, Nature Photonics **9**, 13 (2015).
30. V. Giovannetti, S. Lloyd, and L. Maccone, Science **306**, 1330 (2004).
31. V. Giovannetti, S. Lloyd, and L. Maccone, Nature Photonics **5**, 222 (2011).
32. M. Malik and R.W. Boyd, Rivista del Nuovo Cimento **37**, 274 (2014); arXiv:1406.1685.
33. A.N. Boto *et al.*, Phys. Rev. Lett. **85**, 2733 (2000).
34. S. Lloyd, Science **321**, 1463 (2008).
35. V. Giovannetti, S. Lloyd, and L. Maccone, Nature **412**, 417 (2001).
36. D. Gottesman, T. Jennewein, and S. Croke, Phys. Rev. Lett. **109**, 070503 (2012).
37. K. Jiang *et al.*, J. Appl. Phys. **114**, 193102 (2013).
38. M. Kira *et al.*, Nature Physics **7**, 799 (2011).
39. O.S. Magaña-Loaiza *et al.*, Appl. Phys. Lett. **102**, 231104 (2013).
40. T. Ono, R. Okamoto, and S. Takeuchi, Nat. Commun. **4**, 2426 (2013).
41. M. Malik, O.S. Magaña-Loaiza, and R.W. Boyd, Appl. Phys. Lett. **101**, 241103 (2012).
42. F. Wolfgramm, C. Vitelli, F.A. Beduini, N. Godbout, and M.W. Mitchell, Nature Photonics **7**, 28 (2013).
43. `www.nobelprize.org/nobel_prizes/physics/laureates/2012/`