Quantum information

Ryszard Horodecki*

International Centre for Theory of Quantum Technologies, University of Gdańsk, Wita Stwosza 63, 80-308 Gdańsk, Poland and Institute of Theoretical Physics and Astrophysics, National Quantum Information Centre Faculty of Mathematics, Physics and Informatics, University of Gdańsk, Wita Stwosza 57,80-308 Gdańsk, Poland

Dedicated to memory of Roman Stanisław Ingarden on his centennial birthday

"...the quantum information theory is not only scientifically interesting subject, but is a practical need"

R.S. Ingarden

This article reviews the extraordinary features of quantum information predicted by the quantum formalism, which, combined with the development of modern quantum technologies, have opened new horizons in quantum physics that can potentially affect various areas of our live, leading to new technologies such as quantum cybersecurity, quantum communication, quantum metrology, and quantum computation.

topics: quantum cryptography, quantum entanglement, nonlocality, entanglement witness

1 Introduction

The concept of quantum information was born on the border between quantum mechanics and information theory science. The stunning success of the former has led to think that the concept of information cannot be separated from the mathematical structure of quantum formalism that imposes fundamental constraints on the form of physical laws.

Already in the 1930s, von Neumann defined entropy [1] for quantum states as an analogue of the classical Boltzmann-Gibbs entropy, which later turned out to be the quantum counterpart of Shannon entropy [2] – the concept underlying of classical communication theory. At about the same time, Einstein Podolsky and Rosen pointed out the unusual features of quantum formalism that seemed to lead to the conclusion that quantum mechanics is incomplete [3]. In 1970, two young physicists, Park [4] from the Department of Physics at Washington State University and Wiesner [5] from Columbia University in New York, independently analyzed the physical implications of quantum formalism. While the former discovered a fundamental limitation on copying quantum information, the latter discovered the first application of quantum information to unforgeable quantum money. Unfortunately, both discoveries were ahead of their time and passed unnoticed. Three years later Holevo proved [6] that there is a bound for our ability to access classical information from quantum systems which confirmed earlier Gordon's [7] and Levitin's [8] conjectures. This strengthened the conviction that Shannon's communication theory is incomplete, in a sense that it did not consider the transmission of all physical information carriers such as quantum particles. A few years later, Ingarden, a Polish mathematical-physicist, published a work entitled: "**Quantum information theory**" in which he proposed a quantum generalization of Shannon's theory in terms of the generalized quantum mechanics of open systems [9] (see also [10]). However, it was only a series of seminal papers [11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27] that revealed specific features the quantum code of nature pointing to the quantum origins of information.

There were various reasons for the relatively late advent of the quantum information era crowned with the bilding of Shannon's quantum theory (see [28]). In particular, the unusual suc-

*e-mail: ryszard.horodecki@ug.edu.pl

cess of Shannon's theory led to the belief that the laws of physics could be derived from information processing as a purely mathematical concept detached from physical information carries. On the other hand the identification of peculiar features of quantum information such as monogamy of entanglement [29, 30, 31] required advanced quantum technologies. Additionally, the obstacle was the abstract, mathematical and non-intuitive nature of the standard quantum formalism, which looked like inscription, not all predictions of which were entirely clear even for its fathers.

2 Quantum inscription as a paradigm for quantum information

Roughly speaking, quantum inscription is an instruction – a set of prescriptions that determine the way of probabilistic prediction of the results of future measurements in laboratories [32, 33].

Each physical system corresponds to complex vector space Hilbert H equipped with the linear scalar product $\langle .|.\rangle$ such that the space is complete with respect to the norm

$$\|\psi\| = \sqrt{\langle\psi|\psi\rangle}. \tag{1}$$

The space H of system S compound of n subsystems $S_1, S_2, \ldots, S_n$ is a tensor product $H = H_1 \otimes H_2, \ldots \otimes H_n$ of the Hilbert space of subsystems. The subsystems can represent distinguishable particles, various complex objects, e.g. atoms, molecules, or different degrees of freedom of the same object, e.g. photon polarization and propagation modes.

The central object is the wave function (state vector) $|\psi\rangle$ with the unit norm $\|\psi\| = 1$, which is an element of a Hilbert space. It contains all probabilistic information about the system and satisfies the Schrödinger equation: $i\hbar\frac{\partial|\psi\rangle}{\partial t} = H|\psi\rangle$, where H is linear self-adjoint operator called Hamiltonian. The symbol ϱ denotes the state of the system about which we only have partial information. It can be described by a Hermitian positive semidefinite operator with unit trace: $\varrho = \varrho^\dagger$, $\varrho \geq 0$, $\mathrm{Tr}(\varrho) = 1$ where trace $\mathrm{Tr}(\varrho) = \sum_k \langle\phi_k|\varrho|\phi_k\rangle$ and sum runs over diagonal elements in arbitrary orthonormal basis $\{\phi_k\}$. The symbol U stands for unitary operations that transform states, and in the case of pure states, they keep the scalar product preserved.

Observable quantities correspond to Hermitian linear operators O acting on the state space H. In contrast to classical observables the quantum ones can be noncommutative: $[O_1, O_2] = O_1 O_2 - O_2 O_1 \neq 0$. The most familiar example is $[Q, P] = i$ where Q and P are the position and

momentum operators. The structures and mutual interrelations of noncommutative observables bring deep questions concerning the properties of the quantum systems related to the fundamental principles: uncertainty and complementarity. The first one limits the precision of the statistics of the results of two complementary observables, such as position and momentum [34]. The complementarity principle says that two quantum observables cannot be measured simultaneously, and thus provide "independent" information about physical systems [35].

Contrary to classical theories, quantum measurement is active. It creates properties, does it randomly, and can change state if the latter is not specially tailored for a given measurement. The measurement does not always provide information about state but it can be part of a quantum operation. Any state ϱ defines the probability distribution as the mapping assigning to each measurement result i the probability p_i of that measurement result (the Born rule):

$$p_i = \mathrm{Tr}[\Pi_i \varrho] \tag{2}$$

where $\{\Pi_i\}$, $\sum_i \Pi_i = \boldsymbol{I}$ are elements of a positive operator-value measure (POVM) and $\boldsymbol{I}$ is unit operator. In particular, if Π_i is projector operator then the generalized measurement correspond to the von Neumann measurement, which completely determines the post-measurement state. After the measurement with the outcome i, the system goes to the post-measurement state

$$\varrho_i' = p_i^{-1} \Lambda_i(\varrho) \tag{3}$$

where $\Lambda_i(\varrho) = \Pi_i \varrho \Pi_i$ is particular positive superoperator which clearly maps positive operators to positive operators and normalization of ϱ_i' requires the condition to be met $\mathrm{Tr}[\varrho\Pi_i] = \mathrm{Tr}[\Lambda_i(\varrho)]$ where $\Lambda_i(\varrho) = p_i\varrho_i'$. The most general physically implementable map is a completely positive map Λ which satisfies condition: $\Lambda \otimes \boldsymbol{I}_n \in B(H_1 \otimes C^n, H_2 \otimes C^n)$, where B is space of positive maps between the Hilbert spaces $H_1 \otimes C^n$ and $H_2 \otimes C^n$, $\boldsymbol{I}_n$ is unit operator on n dimensional Hilbert space C^n. If in addition Λ is trace-preserving it determines quantum channel which play a central role in the processing of quantum information [28]. Any completely positive map on a system S in a given state ϱ can be realised via unitary interaction of S with some other system (ancilla) in a pure state followed by von Neumann measurement and final partial trace. This fact comes from so called Stinespring dilation theorem [32].

The crucial difference between the quantum description of physical reality and the classical one

is the principle of superposition: if $|\Psi_1\rangle$, $|\Psi_2\rangle$ are system states then their superposition;

$$|\Psi\rangle = a|\Psi_1\rangle + b|\Psi_2\rangle \qquad (4)$$

is also in good state, provided that a and b are chosen so that $|\Psi\rangle$ is normalized.

The prediction power of quantum inscription is astonishing: "**All our experience so far using quantum theory seems to say: What is predicted by quantum formalism must come to the laboratory**" [36]. In the early 1970s, it seemed that all possible predictions of quantum inscription had already been recognized. The papers of Einstein, Podolsky and Rosen [3] and Schrödinger [37] were initially treated rather as a mathematical artefact detached from its physical implications. Ironically, it was them who drew attention to the extraordinary implications of quantum inscription, which revealed the existence at a fundamental level of a subtle order governed by quantum information. In the classical world, quantum information is "unspeakable". It cannot be written with discrete symbols, e.g. on a tape of a Turing machine. So far, there is no commonly accepted definition of quantum information.

For our purposes, it is convenient to adopt the following interpretation: *Quantum information is what is carried by quantum particles and the wave function ψ is its mathematical image* [38].

Quantum information (QI) can be processed (manipulated) [32, 39], using combinations of unitary operations and measurements. QI is the source of quantum resources [40] such as entanglement [36, 41, 42], steering [43], quantum correlation beyond entanglement [44], quantum coherence [45], asymmetry [46]. It allows to perform nonclassical tasks such as quantum cryptography [13, 16, 47, 48], teleportation [19, 25, 26, 27], quantum computing [15, 14, 18], not feasible with classical resources. QI is resource for quantum metrology [49], computational complexity [50, 51, 52].

However, this subtle resource has a very unpleasant feature. As one knows, non-diagonal elements of the density matrix ϱ called coherence in the state ϱ, provide information about quantum interference. Unfortunately, as a result of the system's interaction with the environment, the process of decoherence [53] occurs, which causes disappearance of non-diagonal elements of density matrix of the state. Reversing the degradation of quantum information still remains a great challenge for effective processing of quantum information.

3 Quantum bit – the unit of quantum information

The concept of qubit appeared for the first time in the context of the theory of quantum information transmission [23] as a two-level system, the state of which can be written as a superposition of two base states $|0\rangle$ and $|1\rangle$

$$|\Psi\rangle = a|0\rangle + b|1\rangle \qquad (5)$$

where a and b are complex numbers, $|\Psi\rangle \in \boldsymbol{C}^2$ (two-dimensional Hilbert space).

Contrary to the classical bit, the qubit represents a continuum of possible states defined by its wave function, which can be visualized by the two-dimensional Bloch sphere with two real parameters θ and φ where $a = \cos(\theta/2)$, $b = \sin(\theta/2 \exp(i\varphi))$ where $0 \leq \theta \leq \pi$, $0 \leq \varphi \leq 2\pi$. For illustration, consider a photon as a paradigmatic example of a qubit. It requires a Hilbert space H which is a tensor product $H = H_{prop} \otimes H_{pol}$, where H_{prop} represents the photon propagation modes while $H_{pol} = \boldsymbol{C}^2$ describes the photon polarization modes. If one disregards the propagation modes, the photon can be treated as a photonic qubit in polarization degree of freedom.

Consider now a photon in the superposition of the base states $|0\rangle \equiv |\updownarrow\rangle$, $|1\rangle \equiv |\leftrightarrow\rangle$ corresponding to vertical and horizontal polarization $|\Psi\rangle = \sin\Theta\,|0\rangle + \cos\Theta\,|1\rangle$. If we direct it to a vertical polarizer, it will change to one of the states $|0\rangle$ or $|1\rangle$ with probabilities $p_0 = Tr[\Pi_o\varrho] = \sin^2\Theta$, $p_1 = Tr[\Pi_1\varrho] = \cos^2\Theta$ respectively, where $\Pi_0 = |0\rangle\langle 0|$, $\Pi_1 = |1\rangle\langle 1|$ are projectors and density matrix of the state $|\Psi\rangle$ is given by

$$\varrho = |\Psi\rangle\langle\Psi| = \begin{bmatrix} \sin^2\theta & \sin\theta\cos\theta \\ \sin\theta\cos\theta & \cos^2\theta \end{bmatrix} \qquad (6)$$

where the diagonal elements are interpreted as the probabilities of the basis state, while the off-diagonal elements represent the coherence of the basis states.

If we now place a specially cut birefringent crystal with the optical axis at an angle of 22.5 degrees on the path of a vertically polarized photon, the photon will be in a state of linear superposition (Fig. 1). This is nothing but the photonic realization of the Hadamard H gate. It has no classical counterpart and plays a fundamental role in quantum information processing including quantum computing. Note that arbitrary photonic wave plate operations for photonic polarization qubits realizing Hadamard, Pauli-X, and rotation gates were implemented on the chip [54].

In Fig. 1, $\boldsymbol{B}_1$ and $\boldsymbol{B}_2$ denote the computation base and the Hadamard base, respectively, which

Figure 1: The photonic realization of the Hadamard H gate. $\boldsymbol{B}_1$ and $\boldsymbol{B}_2$ denote the computation base and the Hadamard base.

are mutually unbiased, i.e. they are mutually exclusive. Perfect information about the polarization along the selected axis implies that there is no information about the polarization along the axis rotated by $45°$. This is a purely quantum mechanical effect resulting from the fact that the vectors $|0\rangle$, $|1\rangle$ and $|+\rangle \equiv |\nearrow\rangle$, $|-\rangle \equiv |\searrow\rangle$ are the eigenstates of the Pauli operators σ_z and σ_x, respectively, which do not commute, ie. $[\sigma_z, \sigma_x] = \sigma_z\sigma_x - \sigma_x\sigma_z \neq 0$.

There have been many proposals for the physical realization of a qubit on quantum dots [55] electron spins [56], semiconductor spin [57], superconducting charge qubits based on Josephson junction [58, 59]. Remarkably it has been demonstrated, that linear optics is sufficient for efficient quantum information processing with photonic qubits in two optical modes (such as horizontal or vertical polarization) [60, 61]. There has recently taken place a quite progress in parallelized quantum information processing which includes tailored quantum memories to simultaneously handle multiple photons [62].

4 Fundamental limitations on quantum information processing

Already in 1961 Wigner pointed out that the existence of self-reproduction in the quantum world is unlikely [63]. In 1970. Park [4], and later Wooters and Żurek [64] and Dieks [65] proved that it is impossible to build a quantum machine that can perfectly copy arbitrary unknown quantum state Ψ:

$$|\Psi\rangle|0\rangle|M\rangle \nrightarrow |\Psi\rangle|\Psi\rangle|M_\psi\rangle \qquad (7)$$

where $|0\rangle$ means a blank state, while $|M\rangle$, $|M_\psi\rangle$ are machine state before and after cloning respectively. The process realized by such a machine would have to be nonunitary and non-linear, which is forbidden by the linearity of quantum formalism. Thus copying destroys the state and it cannot be reconstructed from a single copy. Hence the quantum signals cannot be noiselessly amplified. Later the limitation for the unperfect cloning in terms of the so called fidelity function $f(\varrho_{out}) = \langle\Psi|\varrho_{out}|\Psi\rangle$ measuring similarity of the state of either of the two outcome registers has been provided within the framework of imperfect quantum cloning machines [66, 67]. There is dual the non-deleting theorem, which states that, in general, given two copies of some arbitrary quantum state, it is impossible to delete one of the copies [68]. In the above mentioned paper Holevo [6] proved an fundamental theorem that sets an upper limit to the amount of information available about a quantum state. It implies that with the help of one qubit is impossible to send more than one bit of classical information.

Quite unexpectedly, it turned out that there is also a restriction on the possibility of generating of quantum superposition. Namely, it has been independently shown [69, 70] that there is no universal probabilistic quantum protocol generating superposition of the two unknown states. Interestingly, a probabilistic protocol generating a superposition of two unknown states having a fixed overlap with a known pure reference state has been proposed [70]. This protocol has been carried out experimentally in a three-quadrant NMR system as well as on unknown photonic quantum states [71, 72].

5 Quantum cryptography based on no-cloning

Parallel to Park's paper on non-cloning, Wiesner, based on principle of uncertainty introduced the

4

concept of conjugate coding to make up quantum money [4]. This idea paved the way for the quantum information encryption Bennett's and Brassard's protocol (BB84) [13]. It has the following main three steps:

1. Alice sends randomly polarized photons through the quantum channel in the selected computing bases $\{B_1\}$ $|0\rangle$, $|1\rangle$ and Hadamard $\{B_2\}$ $|+\rangle$, $|-\rangle$; saves bases and bits.

2. Bob measures photons in randomly selected bases B_1 and B_2, registers bases and bits.

3. Via the classic public (authenticated) channel, Alice and Bob transmit their choices bases. When their bases match, they retain the appropriate bits.

Thus, they receive a raw key that requires further processing. To check for eavesdropping, they calculate the quantum bit error of a randomly selected data subset that they reveal each other via the public channel and check if the error (percentage of mismatched bits) is below a certain threshold value. Using classic post-processing protocols such as error correction and privacy amplification, they generate the final secure key.

Since 1992, when Bennett and Brassard and colleagues demonstrated the first 32cm quantum distribution of the key in free space [73], there has been tremendous progress in the development of quantum cryptography in free space and in fiber. There is a continuous improvement of cryptographic keys over long distances [74] as well as an increase in key generation speed using single photon detectors [75]. Quantum key distribution (QKD) networks were established in the US, Austria, Switzerland, China and Japan. and the European SECOQC network [76]. Due to exponential signal attenuation and decoherence, the effective distribution range of the quantum key of terrestrial networks is limited to 300 km [77]. In cosmic space, both of these factors are many times weaker. In 2016, the first satellite distribution of the BB84 protocol was performed using a one-time key cipher via the Micius satellite at intercontinental distances, thanks to which the photos of Schrödinger and the philosopher Micius were safely transferred between Vienna and Beijing [78].

Despite the enormous advances in quantum cryptography, there are still some problems related to the fact that practical implementations of quantum key decomposition use realistic photonic qubits and imperfect single photon detectors. This creates gaps between QKD theory and practice enabling quantum hacking, e.g. The Bright illumination Attack, Photon number splitting [79]. Therefore, QKD implementations are still in the testing phase and these gaps are identified. Stronger versions of BB84 were developed, such as the BB84 decoy state and protocols resistant to photon number breaking attacks [47]. As a result, QKD protocols become more and more secure.

6   Quantum entanglement – the most non-classical feature of quantum information

As we have seen, already at the level of simple systems, the properties of quantum information differ substantially from those of classical information that can be amplified and copied. Much earlier, in the 30s, EPR and Schrödinger revealed a peculiar feature of quantum information in complex quantum systems rooted in the principle of superposition called entanglement. According to the quantum inscription, the state space H_S of the quantum system S compound from distinguishable subsystems $S_1, S_2, \ldots S_n$ is given by $H_{S1} \otimes H_{S2}, \ldots \otimes H_{Sn}$ which is the tensor product of the Hilbert space of the subsystems.

We say that a pure state is entangled if it cannot be written as the product of the states of the individual subsystems

$$|\Psi\rangle_{12\ldots n} \neq |\phi\rangle_1 \otimes |\psi\rangle_2 \ldots \otimes |\chi\rangle_n \qquad (8)$$

In general a mixed state ϱ of n systems is entangled if it cannot be written as a convex combination of product states

$$\varrho \neq \varrho_{sep} = \sum_i p_i \varrho_1^i \otimes \cdots \otimes \varrho_n^i \qquad (9)$$

In particular, for any two-part pure entangled state $|\psi\rangle_{12} \in H_1 \otimes H_2$ there exist orthonormal Schmidt bases $\{\phi_i\rangle, \{\chi_i\rangle$ in H_1, H_2 respectively such that:

$$|\Psi\rangle_{12} = \sum_i^d c_i |\phi_i\rangle \otimes |\chi_i\rangle \qquad (10)$$

where the summation takes place on the smaller dimensions of the two systems $d = \min(d_1, d_2)$. In particular, the two-part maximally entangled state in the space $H_1 \otimes H_2$ with the dimension d^2 is defined as:

$$|\Psi_{\max}\rangle = \frac{1}{\sqrt{d}} \sum_i^d |\phi_i\rangle \otimes |\chi_i\rangle \qquad (11)$$

In particular there is a two qubit entangled state:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_1 |0\rangle_2 + |1\rangle_1 |1\rangle_2) \qquad (12)$$

where $\{|0\rangle, |1\rangle\}$ is the computational basis for qubits. Using von Neumann entropy as a measure of entanglement for pure states, it is easy to check that the above state above contains one ebit of entanglement, i.e. the maximum amount of entanglement that a system with dimension $d = 2^2$ allows. In general, for a system consisting of n pairs of entangled qubits and a Hilbert space dimension, $d = 2^n$ contains n ebits of entanglement. Most of the pure state vectors in a pure state two-part Hilbert space are not maximally entangled.

For systems divided into more than two parts, the Schmidt distribution in general does not exist. However, many of the important states in quantum information processing take the form of a multi-part Schmidt distribution. Among them, three-particle W and GHZ states: $|\Psi\rangle_{GHZ} = (|000\rangle + |111\rangle)/\sqrt{2}$ [80], $|\Psi\rangle_W = (|001\rangle + |010\rangle + |100\rangle)/\sqrt{3}$ [81], which represent two different types of entanglement that cannot be transformed into each other through local operations and classical communications (LOCC). Interestingly experimental W-to-GHZ state conversion were recently demonstrated [82, 83].

Let us emphasize that the above mathematical description of quantum entanglement between the various degrees of freedom of complex systems is adequate in a scenario where each subsystem (e.g. qubit) can be individually addressed / manipulated. In situation when one consider indistinguishable systems in connection with symmetrisation postulate the complete characterization of entanglement is still challenge. Many different approaches have been proposed with different entanglement definitions. Recently, Benatti et al. [84] made an extensive comparative analysis of different approaches to the definition of entanglement of quantum systems composed of indistinguishable particles based on natural physical requirements.

There are many ways to generate quantum entanglement. Entangled states are most often generated in the spontaneous parametric down-conversion and spontaneous four-wave mixing [85, 86, 87]. It is intriguing that it is possible to entangle together particles from two independent sources that did not interact with each other in the past [88, 20]. Another peculiar behaviour of entanglement called a sudden entanglement death was described in a dynamic scenario. Namely, when two entangled qubits interact with natural reservoirs, the entanglement can disappear in a finite time while the coherence disappears asymptotically [89, 90, 91]. The source of this phenomenon is due to the fact that in finite-dimensional systems the set of separable (non-entangled) states has a finite volume [92]. This important result was in particular discussed in the context of quantum computing on NMR which operates on highly mixed, separable states [93].

The discovery of Einstein, Podolsky, and Rosen that entangled states could show "ghostly" correlations independent of distance, until the appearance of John Bell's famous work, was not given much interest. On the one hand, they were considered more philosophical than physical, on the other hand, it was believed that such correlations could be simulated classically.

7 Photons entangled in polarization

To illustrate this phenomenon, consider the probabilistic generation of photons entangled in polarization degrees of freedom using Type-II down-conversion [94]. In this process, a high-energy photon in an optical nonlinear medium (BBO crystal) is converted into two lower-energy photons that are emitted along the surface of two anti-correlated intersecting cones with vertical and horizontal polarization (Fig. 2). In particular, the photons emitted along the intersections cannot be assigned a specific polarization because we do not know which cone they come from. We write it down as a quantum alternative

$$|\Psi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A |1\rangle_B + |1\rangle_A |0\rangle_B), \qquad (13)$$

where $|0\rangle$, $|1\rangle$ correspond to vertical, and horizontal polarisation respectively. Here $|\Psi^+\rangle$ is one of four canonical Bell-states (Bell basis) [95]: $|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A |1\rangle_B \pm |1\rangle_A |0\rangle_B)$, $|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A |0\rangle_B \pm |1\rangle_A |1\rangle_B)$, Now, if we direct the photons from the entangled pair (EPR pair) in the polarization to the distant Alice's and Bob's laboratories, respectively, who independently measure the polarization of the same type, it turns out that they get anti-correlations $0 - 1$ or $1 - 0$. What is striking is the fact that individual photons do not carry any bit because their polarization is completely random [16], so local measurement results turn out to be completely random too. EPR reasoned as follows: If it is possible to "remotely" predict some property of a particle without interacting with it, then this property must have existed before, ie. before the measurement. They called it the "reality elements", and from there they concluded that quantum inscription offered an incomplete description of physical reality.

8 Nonlocality of quantum correlations. Bell tests

It was a serious objection that no one, including Bohr himself, was able to convincingly re-
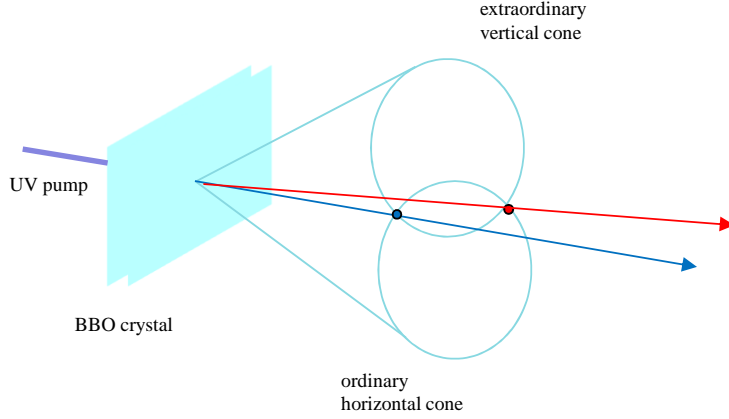
Figure 2: Generation of photons entangled in polarization using Type-II conversion in the Bell state $|\Psi^+\rangle_{AB}$

fute. The Gordian knot was cut by John Bell [11]. Namely, he formalized the concepts of reality elements by introducing a model of local hidden variables based on the following assumptions: i) the measurement results are determined by the properties of the particle carried before and independent of the measurement, ii) the results determined in one place are independent of any actions in the space-like separation, iii) the settings of local apparatus do not depend on hidden variables that determine the results of local measurements. These assumptions, as Bell showed, impose constraints on correlations called Bell's inequalities. The key point is that they can be verified in the laboratory regardless of any theory.

Let us briefly illustrate the Bell inequalities by exemplifying the correlation of polarized entangled photons that were sent to the distant Alice and Bob laboratories along the z axis. The partners measure dichotomous observables ie polarizations that have only two values $+1$ or -1. Each partner measures two such observables. Alice chooses the settings of detectors a, a', Bob b, b', which are unit vectors showing different angles in the x-y plane along which they can orient polarizing filters. For each pair of settings, correlation functions can be constructed: $\langle a, b\rangle$, $\langle a, b'\rangle$, $\langle a', b\rangle$ $\langle a', b'\rangle$, where $\langle\rangle$ means the average of the product of outputs. On this basis, it is possible to build a new Bell observable $B = a, b + a, b' + a', b + a', b'$. Now, if we accept the assumptions of local realism, in particular that each photon had a certain polarization value ($+1$ or -1) before the measurement, it is easy to check that the absolute value of Bell observable cannot exceed 2. Hence, we obtain Bell-CHSH inequality [96]:

$$|\langle ab + a'b + ab' - a'b'\rangle_{kl}| \equiv |\langle B\rangle| \leq 2 \quad (14)$$

Quantum mechanics predicts that the mean value of the B observable satisfies the inequality $|\langle B_{QM}\rangle| \leq 2\sqrt{2}$ which means that it breaks Bell-CHSH inequality, where $2\sqrt{2}$ is the so-called Tsirelson's bound [97].

The verification of Bell's inequality based on the assumptions of local realism proved to be a great challenge for experimentalists, as it required the closure of three loopholes: i) Locality demands that no signal traveling at the speed of light can inform the distant detector of its settings or the result of a measurement on the local detector before Alice and Bob complete the measurements; ii) Fair-sampling (or detector efficiency) demands that the sample of entangled pairs be a faithful representation of the entire ensemble being broadcast; iii) Freedom of choice requires that the hypothetical local variable should not influence the local choices of measurement setups on the part of Alice and Bob.

The first ground breaking experiment that convincingly demonstrated breaking the Bell CHSH inequality and good agreement with the predictions of quantum mechanics was performed by Aspect et al. [12]. In their experiment, entangled photon pairs were emitted by the process of atomic calcium cascades. For the first time, the authors used acousto-optical switches, which pseudo-randomly changed the orientation of the analyzers in a short time compared to the photon transit time and detection. They achieved more than 95% of the detection efficiency.

Only in 2015, a series of Bell tests based on quantum random number generators was performed, which closed both locality and fair-sampling loophole in the same experiments [98]. Recently, two cosmic Bell tests with photons entangled in polarization were performed, in which

measurement settings were determined by real-time photon wavelength measurements from high redshift quasars, light emitted billions of years ago; Thus, the authors closed two loopholes at once: locality and freedom of choice [99, 100]. However, these experiments failed to close the fair-sampling loophole. Quite recently Pan et al. [101] performed an impressive local realism test that closes both locality and fair-sampling loophole and rules out common cause 11.5 years before the experiment, which largely closes the freedom of choice loophole.

The interpretation of violating Bell's inequality is still the subject of the discussions [102, 103]. The Bell tests show that the quantum correlations cannot be explained using any theoretical model based solely on local variables. This particular feature of quantum information, which has become known as quantum nonlocality (Bell nonlocality), provides the resource for device-independent quantum key distribution [104, 105, 106] (see however [107]).

9   Weaker forms of breaking realism

While I'm not going to do a detailed review of the vast field of difference in Bell's inequality, let me mention two important related concepts. First, it should be mentioned that violation of local realism by composed quantum systems has it's a weaker quantum analog called quantum contextuality, observed with help of random measurements of specially designed sets of quantum measurements pioneered by [108] which has many further developments (see [109, 110, 111]) can be mathematically quantified [112]. Quite remarkably it have the so called state variant fully analogous to Bell inequalities [113] as well as state-independent one which is valid for any state, and basically reports the nonclassicality of the sent of measurement involved [114].

The fundamental difference is that roughly speaking quantum contextuality can contradict classical realism only under assumption of some bound on dimension of Hilbert space, while violation of Bell inequalities via quantum states is the phenomenon that is independent on that assumption in general. This is why violation of the inequalities in many cases leads to the powerful concept of quantum *self-testing* [115]. In the case of the inequality (14) self-testing means that independently of complexity of local systems (for instance one may assume that each of the observables in (14) may concern not polarisation but some other or even all of the photon internal degrees of freedom) the saturation of the quantum bound $2\sqrt{2}$ guarantees that up to local isometries

and local partial traces the state is in the *unique* qubit form (13). This is an essence of the device independent variant of the Ekert's entanglement-based encryption protocol (E91) [16] (see Sec. 11). Quantum self-testing is a cornerstone of device independent quantum cryptography which is based on the idea that only the output statistics of the devices are enough to guarantee cryptographic security without need of knowing the physical structure of the devices (for example see [116]. Finally there is a weaker variant of Bell inequalities on composite systems that is still much stronger than contextuality. This is based on the so called quantum steering [43] in which we assume that for one of the particles the dimension of the Hilbert space is known (much like in contextuality tests) while in the other is not. This leads to the so called semi-device independent quantum cryptography (see [117] and reference therein), [118].

10   Nonlocality and the principle of informational causality

The discovery of quantum nonlocality shook our perception of the foundation of quantum physics. Hence the natural question arose: Is there a nonlocality stronger than that predicted by quantum formalism? Is this the only description that allows for nonlocal phenomena consistent with special relativity? In the 1994 paper, Popescu and Rohrlich (PR) [119, 120] took nonlocality as the basic axiom and have proposed a model independent approach, consistent with special relativity, based on the conception of input-output black-box devices. In the approach the experiments of Alice and Bob are space-like separated and each experiment is treated as a black-box. Then all the physical information obtained in the experiment is encapsulated in the joint probability $P(a, b|x, y)$ that Alice obtains a and Bob b when Alice inputs x and Bob inputs y respectively. In the simplest case where x, y, a, b have only two possible values, they must satisfy the constraints: $a \oplus b = xy$ where $\oplus$ denotes addition modulo 2. It is not difficult to verify that PR nonlocality leads to algebraic breaking of CHSH inequality equal to 4 which drastically breaks Tsirelson's limit $2\sqrt{2}$. Does nature allow information to be processed using such super-quantum correlations? Remarkably the physical principle of information causality was proposed [121], which excludes such possibility. The information causality principle can be formulated briefly as: ***The message cannot contain access to more information than the amount contained in it.*** Contrary to its laconic form, this principle has strong implications:

- It strictly determines the maximum value of

quantum correlations $\leq 2\sqrt{2}$

- it is fulfilled by both classical theories and quantum mechanics

- it excludes the physicality of the super strong Popescu-Rohrlich correlations

It is significant that although the properties of quantum and classical information are basically different, they both follow the principle of informational causality. It should be noted here that nonlocal PR boxes although nonphysical provide a conceptual tool in the modeling of nonlocality in the quantum physics and beyond [122, 123, 124]. It is remarkable that the PR correlations are under some circumstances much more powerful resource than quantum entanglement as they lead to trivialising quantum communication complexity [125, 126]. However they are weaker in another sense since in their language there is no room for nontrivial dynamics and continuous chance of settings of the measurements.

Finally it is worth noting that in the case of three parties the concept of relativistic causality that goes beyond the no-signaling paradigm is possible when space-time variables are explicitly involved [127, 128]. Quite recently the general axiomatic approach to causality of the evolution of the spatial statistic detection has been initiated [129, 130].

11 Entanglement-based cryptography

As mentioned above, quantum correlations, apart from nonlocality, have another feature – they are random. It was intriguing that this randomness ensures the peaceful coexistence of quantum inscription predictions and special relativity, as partners cannot use the correlation to the instant telegraph. This specific "telegraphic no-go" has not yet had clear theoretical foundations, although recently an attempt to explain this phenomenon has been made [131].

As we saw, singlet-state photon pairs entangled generate anti-correlated random numbers at distant locations. Ekert first noticed that the randomness of these correlations could be used to generate a secure cryptographic key and proposed the protocol E91 [16] based on the entangled spin$\frac{1}{2}$ particles in singled state and Bell's theorem and proposed implementation using nonlocal correlations between maximally entangled photon-pairs. Soon after, the Bennett, Brassard and Mermin proposed a simplified protocol based on entanglement without Bell's theorem, and showed that it is equivalent to BB84. The security of E91 is due to the fundamental property called monogamy

of entanglement which express the fact that entanglement represents correlations that cannot be shared by third parties [29, 30, 31]. This peculiar entanglement trait not only provides the security of entanglement-based cryptography, but sheds new light on physical phenomena in many correlated systems [132].

Experiment implementations of the E91 protocol have been made at ground stations [133, 134]. Recently, both production and analysis of entangled states have been tested with the SpooQy satellite, which is a step towards the realization of a cryptographic key generator based on entanglement in cosmic space [135]. Quite recently, the quantum key distribution has been analyzed with a small block length, which is crucial in entanglement-based quantum communication [136]. It should be emphasized that the original E91 protocol was prophetic as it suggested device-independent cryptography [137, 105], based on Bell inequality breaking, which ensures that the data produced by quantum devices has a certain degree of secrecy, no matter how exactly the data was generated.

12 Canonical effects based on quantum entanglement

Ekert's work was important for another reason, namely, it was the first to show that "ghostly" EPR correlations can be harnessed into something useful. Since then, entanglement has been viewed not as a curiosity, but as a real physical resource that can offer completely new unexpected effects. The breakthrough was the discovery of dual effects, i.e. dense coding and quantum teleportation in which the ebit plays a central role, i.e. a pair of qubits in a maximally entangled state, distributed between the sender and receiver. Remarkably both entanglement-based effects circumvent the non-cloning and Holevo theorem.

12.1 Super dense-coding

Suppose Bob wants to send to Alice two bits of information, using only one noiseless qubit. According to Holevo's theorem, only one bit can be transferred with one qubit. So Bob would need two qubits for this. Bennett and Wiesner showed [17] that if Alice and Bob have one ebits then it is enough to send only one qubit to transmit one of the four messages (00,01,10,11) to Alice. To do this, Bob encodes messages using local different unitary operations $U_{00}, U_{01}, U_{10}, U_{11}$ on his qubit, generating orthogonal Bell states (Bell base), and sends the qubit to Alice, which measures the combined two qubits. The four orthogonal Bell states

represent the four distinguishable messages. The first implementation of a super-dense photon encoding protocol was made by Mattle et al. [138] in which Bob performed unitary operations using a combination of half and quarter revolutions of the wavelet. The dense coding protocol was later implemented in particular on atoms [139] and nuclear magnetic resonance [140].

12.2 Quantum teleportation

The most astonishing prediction of quantum inscription is quantum teleportation – a dual effect to dense coding that demonstrates the remarkable power "exotic" combination quantum and classical resources (see the fascinating story of the discovery [141]).

This time Alice wants to send one qubit to Bob in an unknown state, but not by physical qubit transfer, having two classic bits at her disposal. Obviously, quantum information cannot be transferred with classical bits. Let now consider the situation if we provide partners with 1 ebit of entanglement. Now Alice can perform a measurement on her two particles, i.e. a qubit in an unknown state ϕ and a particle from the entangled pair. It is not hard to see that this measurement is identical to what Bob made in high-density coding. Alice gets one of four possible outcomes with a $\frac{1}{4}$ probability: 00,01,10,11. Having two bits at her disposal, Alice can send information via the classical channel to Bob which of the results she received. Depending on the result, Bob uses one of the transformations: $U_{00} \cong I$, $U_{01} \cong \sigma_x$, $U_{10} \cong \sigma_y$, $U_{11} \cong \sigma_z$ where σ_x, σ_y, σ_z, are standard Pauli operators. At this point, his particle from the entangled pair it will be in state ϕ. Note that Alice's measurement provides no state information (the bits are completely random), but is part of a quantum operation. So the transmission of the qubit had to take place immediately at the moment of Alice's measurement. There is no conflict with special relativity here because quantum inscription predicts that any operation on one subsystem does not cause measurable changes on the other subsystem regardless of the state of the entire system. Note that there is no contradiction here with the prohibition on cloning, since the initial state of the qubit was completely erased in Alice's laboratory and then recreated, but not known in Bob's laboratory. It should be finally stressed that here no information about the unknown state ϕ is transferred via a classical channel that only conveys the message about the recovery operation at Bob's lab which is completely independent on ϕ.

Original teleportation protocol was extended including to continuum variables [142, 143]. Quantum teleportation, was demonstrated in pioneering experiments by the Zeilinger [25] and De Martini [26] teams. Furusawa and co-workers [27] independently carried out a unconditional teleportation on continuous variables (see in this context [142, 143, 144, 145, 146]). Later, quantum teleportation was demonstrated in many beautiful experiments [147, 148, 149, 150, 151, 152]. In 2017, a photon was teleported from Ngari ground station to the Micius satellite (with an orbit from 500 to 1400) [78, 153].

Quantum teleportation has been continuously researched for more than 20 years (see ref. [154]) due to its central role in the development of quantum information processing including quantum computing [147, 155], the quantum internet and its relationship to the foundations of physics. Various generalisations of the original protocol have been proposed. In particular, the original protocol was generalized including general teleportation channel [156], multiport teleportation [157, 158, 159], teleportation with multiple sender-receiver pairs [160], telecloning [161].

12.3 Entanglement swapping

The peculiarity of multi-particle entanglement is that one can entangle particles that have never interacted with each other in the past. That such an effect may take place was suggested by the first Yurke and Stoler (1992b) [88]. This idea was implemented in the pioneering paper: *"Event-ready-detectors" Bell experiment via entanglement swapping*. In this scenario, arbitrarily distant partners Alice and Cecilia and Bob and David share entangled EPR pairs of photons coming from independent sources:

$$|\Phi^+\rangle_{AC} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),$$
$$|\Phi^+\rangle_{BD} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{15}$$

The system is then described as

$$|\Phi^+\rangle_{AC} \otimes |\Phi^+\rangle_{BD} \tag{16}$$

Now Cecilia and Bob make a combined measurement in Bell's basis on B and C particles. As a result, A and D particles become entangled even though they never interacted with each other. Note that this is equivalent to teleporting entanglement of one EPR pair through the other. Soon the entanglement swapping was generalised to multiparticle systems [162]. It provided the operational foundations of multi-photon interferometry, in particular the method of interference of photon pairs from independent sources (see review [163]).

The entanglement swapping [164, 165, 166] has found applications among other in the generation of multi-photon entangled states [167], device-independent key distribution [168] and construction of quantum repeaters [169, 170, 171], quantum photonic [172], secret sharing [173, 174].

13 Detection of quantum entanglement

All of the above effects and many other non-classical tasks based on quantum information processing require high purity quantum entanglement. Unfortunately, this subtle resource is extremely sensitive to interaction with the environment and it degrades very quickly, i.e. pure states change into mixed (noisy) states with less entanglement. This opened up important issues: how to theoretically check whether a given state is entanglement and is it possible to detect noisy entanglement in the laboratory?

In general, characterizing entangled states regardless of the measure of utility for specific tasks is so-called NP difficult problem [175]. The partial characterization was achieved using criteria that provide the necessary but not sufficient conditions for deciding whether a state is entangled or not. The breakthrough was the paper of Peres [176], who proposed an extremely strong separability test based on the partial transposition operation. From mathematical point of view it is positive but not completely positive map thus nonphysical one. Such an operation is performed on one S_1 or S_2 of subsystem on complex state of the system S. If the state subjected to such nonphysical surgery does not survive in the sense that it will cease to be positive and lose its probabilistic interpretation, then the state was entangled. Mathematically speaking, this means that its partially transposed density matrix has at least one negative eigenvalue. Based on the complete classification of positive mappings for low dimensions [177] it was proved that the PPT condition is a necessary and sufficient condition for the separability of 2×2 and 2×3 systems [178] which gives a complete characterization for low-dimensional states of systems. In general necessary and sufficient, albeit non-operational, separability condition based on positive mappings was provided [36].

The above structural criteria based on positive non-physical mappings of the quantum state, while strong, that they cannot be implemented in a laboratory. Fortunately, based on the geometric properties of convex sets, it was possible to formulate a linear separability criterion that could be implemented physically. Namely, from the convex set theory and the Hahn-Banach theorem, it follows that for any entangled state ϱ_{ent} there exists a hyperplane in the space of operators separating ϱ_{ent} from the set of separable states S. Such a hyperplane is defined uniquely by the Hermitian operator W (entanglement witness) [179]. Then the state is entangled iff expectation value W on ϱ_{ent} is negative i.e. $\langle W \rangle \varrho_{ent} < 0$ whereas its expectation value on all separable states $\langle W \rangle \varrho_{sep} \geq 0$ (see Fig. 3). It was shown, that such a witness can be optimized by shifting the hyperplane parallel to the set S [180, 181]. Thus the detection of entanglement consists in measuring the mean value of a properly selected observable. Remarkably there is a "footbridge" Jamiolkowski isomorphism [182] which allow to go from nonphysical positive maps to the physical measurable quantities to Hermitian operators (entanglement witness), which provides a necessary and sufficient condition separability [178].

The entanglement witness criterion has a number of advantages: i) it is universal in the sense that for any entangled state always exist entanglement witness; ii) It certifies entanglement in experiments in the presence of noise; iii) It allows to detect the presence of entanglement even in several measurements in contrast to tomography, where the number of measurements increases exponentially with the number of particles. The disadvantage is that the witness must be precisely selected for the examined state. The quantum entanglement detection based on entanglement witnesses has found wide applications for the certification of two- and multi-partite states [183, 184, 185, 186, 187, 188, 189, 190, 191] in different physical scenarios. Interestingly, the concept of measurement-device-independent entanglement witness which allow one to demonstrate entanglement of all entangled quantum states with untrusted measurement apparatuses was introduced [192].

The theory of entanglement detection was developed in different directions [36, 193]. The other separability criteria based on correlation tensor was proposed [194, 195, 196] for bipartite and multipartite scenario. Recently it has been proved that or enhanced nonlinear realignment criterion [197] is equivalent to the family of linear separability criteria based on correlation tensor i.e. the family of (linear) entanglement witnesses [198]. It was also demonstrated that the separability criteria based of the correlation tensor are weaker than positive partial transposition criterion [199].

14 Entanglement distillation and bound entanglement

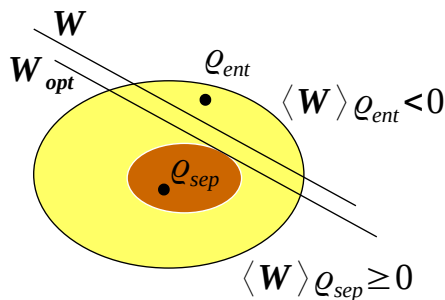After Peres discovered the entanglement criterion of partial transposition, a problem arose. If the

Figure 3: The line represents hyperplane corresponding to the entanglement witness W. All states located to the left of the hyperplane or belonging to it (in particular all separable states) provide non-negative mean value of the witness, i.e. $\mathrm{Tr}(W\varrho_{sep}) \geq 0$ while those located to the right are entangled states detected by the witness. W_{opt} is optimized entanglement witness.

state was untangled, it will remain untangled after the partial transposition operation. It was natural to ask are there states in nature that are entangled and have positive partial transposition? When such states were discovered in 1997 [200] they were treated as a mathematical singularity with no reference to physical reality. At about the same time, Bennett and colleagues were working on the problem of how to reverse the entanglement degradation process. In 1996, they published a paper that played a key role in the theory of entanglement manipulation [201] (see also [202]). Namely, they introduced a natural class of entanglement manipulation operations by experimentalists in distant laboratories: the two partners can perform any local operations on their entangled particles and communicate via the classical channel (LOCC). Consequently, they introduced the entanglement distillation protocol: The partners share n copies of the ϱ_{AB} state which contains noisy entanglement. With the help of local quantum operations and classical communication, they determine a smaller number of m $(m < n)$ of almost maximally entangled pairs – two-qubit singlet states $|\Psi^-\rangle_{AB}$. When the protocol is optimal, the constant $m/n = D$ is a measure of entanglement in a noisy state ϱ (distillable entanglement).

Distillation protocol raised the natural question: Can all noisy states be distilled in this way? It turned out that all noisy entangled two-qubit states can be distilled [203]. It was a big surprise that the distillation protocol does not work for the higher dimension systems [204, 31]. It turned out that the environment can contaminate pure entanglement in such a way that it is no longer possible to recover it by distillation with LOCC. Thus, the entangled states with positive partial transposition are non-distillable. Thus, in Nature there are at least two types of noise entanglement: free, that is, distillable entanglement, and bound

entanglement that cannot be distilled with LOCC [205]. After 12 years, several centers simultaneously created the bound entanglement in the laboratory on the photons [206, 207], on ions [208], in liquid in NMR [209], with light in continuous variable [210] regime.

It has been shown that the bound entanglement is not a rare phenomenon , since its presence was detected in thermal spin systems [211, 212]. Another surprise was that the bound entanglement can be activated [213] and that a cryptographic key can be extracted from bound entangled states it [214]. The latter lead to the general paradigm for distilling classical key from quantum states in terms of so called private bits (P-bits) [215] [See experimental implementation [216])]. Moreover bound entangled states can violate Bell inequalities [217] and can be useful in quantum metrology [218, 219, 220]. Another an interesting open problem is the use of bound entanglement states in the device-independent quantum key distribution [221, 222, 223].

15   Breaking the classical order

When analysing the structure of entangled states, Schrödinger noticed another peculiarity of quantum correlations that astonished him, as evidenced by the three question marks that appear in his unpublished notes in 1932 [Note in arxiv]. In 1935, he makes a laconic conclusion: "Best possible knowledge of a whole does not include best possible knowledge of its parts – and that is what keeps coming back to haunt us." [224]. It was very disturbing because it meant breaking the classical order in complex systems. As is known in the classical world, the measure of the randomness (disorder) of an individual random variable X is the

Shannon entropy:

$$H(X) = -\sum_i p_i \log p_i \qquad (17)$$

where p_i – probabilities of events, $\sum p_i = 1$.

For two random variables X and Y, the total Shannon entropy is $H(X,Y) = \sum_{ij} p_{ij} \log p_{ij}$ and conditional entropies $H(X|Y)$, $H(Y|X)$ are always:

$$H(X|Y) \equiv H(X,Y) - H(Y) \geq 0, \quad H(Y|X) \geq 0 \qquad (18)$$

which shows that the entropy of a subsystems $H(X)$, $H(Y)$ never exceeds the total entropy of the system $H(X,Y)$.

In the quantum world, the measure of quantum disorder is the von Neumann entropy $S(\varrho)$ defined for the state ϱ:

$$S(\varrho) = -\operatorname{Tr}(\varrho \log \varrho) = \sum \langle \phi_i | \varrho \log \varrho | \phi_i \rangle \qquad (19)$$

where $\{\phi_i\}$ any complete orthogonal system in H. When density matrix ϱ is diagonal, it can be regarded as a quantum counterpart of a classical discrete probability distribution as a natural description of quantum information source. Then von Neumann entropy can be written in a form similar to the Shannon entropy

$$S(\varrho) = -\sum_i p_i \log p_i, \qquad (20)$$

where the quantum probabilities p_i are the eigenvalues of the operator ϱ satisfy $\sum p_i = 1$.

The Schrödinger observation was quantified using the von Neumann entropy [225, 226]. It has been proved that the entropy of the subsystem A or B can be greater than the entropy of the entire system AB only when the system is in a entangled state. This implies that quantum conditional entropies $S(A|B) \equiv S(AB) - S(B)$, $S(B|A)$ can be negative, which means that the disorder in the whole AB system may be smaller than in the subsystems A or B. Recalling our example with photons entangled in polarization, we can see that everything happens agrees. The polarizations of the photons measured in the laboratories of Alice and Bob are completely random, while the entangled pair is in perfect order. Thus entanglement can break the classical order which is the source of the informational "paradox" of Schrödinger.

16   Negative information in quantum communication

The breaking of the classical order was both intriguing and incomprehensible, especially in the context of Shannon's theory, in view of the fact that the negativity of quantum conditional entropy had no operational significance. Let us recall that at the heart of the classical Shannon communication theory is the theorem of noiseless coding, which says that a necessary and sufficient number of bits for faithful transmission is equal to Shannon's entropy H [2]. Schumacher showed that if in Shannon's theory we replace messages by quantum states and bits by qubits, then the necessary and sufficient number of qubits for faithful transmission is equal to the von Neumann entropy $S(\varrho)$ [23]. Soon after Schumacher and Westmoreland [227] and Holevo [228] generalized Shannon's channel coding theorem. Three kinds of quantum channel capacities was introduced: classical, quantum and private capacity, which play an important role in quantum communication [29, 229, 230, 231, 232]. The essential difference between the last two capacities is the following: The quantum capacity is achieved in the process which guarantees that information in any basis stays uncorrelated from the environment after the transfer (which may be shown to be equivalent to BB84 paradigm). Remarkably in the definition private capacity much more relaxed condition is required: only one base is needed to stay uncorrelated in the above sense. Note that the private capacity while in general higher than the quantum one may have subject to severe restriction in quantum repeater scenario [233] (see more [28]).

Meanwhile, for a long time there was no quantum counterpart of Slepian-Wolf theorem [234]. Namely in 1973 Slepian and Wolf formulated in framework of classical communication the following problem: The two partners Alice and Bob have random variables X and Y that are correlated with each other. Bob is given some incomplete information of Y in advance. Alice is in possession of the missing information of X. Bob's job is to obtain the missing information of X. The question is how much additional information Alice has to send to her partner. Slepian and Wolf proved that the amount of information that Bob needs is expressed by the conditional entropy: $H(X|Y) \equiv H(XY) - H(Y)$ which is a measure of the partial information that Alice must send to Bob. This quantity is always positive.

In 2005, Horodecki et al. [235] proposed a quantum version of the above scenario: Alice and Bob have a system in some unknown quantum state ϱ_{AB} which contains the complete information. Bob has some information about state ϱ_B, while Alice has the missing information ϱ_A. The task is as follows: how much information does Alice have to send to Bob for him to have com-

plete information. The quantum equivalent of the Slepian Wolf theorem says that this quantity is given by the von Neumann quantum conditional entropy:

$$S(A|B) \equiv S(AB) - S(B) \qquad (21)$$

where $S(B)$ is the entropy of the Bob state while $S(AB)$ is the entropy of the cumulative ϱ_{AB} state. Contrary to the classical conditional entropy $H(X|Y)$, the conditional entropy can be both positive and negative. Conditional quantum entropy has an operational interpretation of missing information: If $S(A|B)$ is positive – this is the missing information that Alice must send to Bob via qubits (classical analogue). If $S(A|B)$ negative, Alice does not need to send the missing information via qubits. Additionally, Bob and Alice get free "quantum impulses" to send a certain number of qubits in the future, for example for teleportation.

Finally it should be stressed that the above analysis is a strong completion of the previous result [236] which says that for any state with the quantity (21) negative there exists an entanglement distillation protocol with one way classical communication (from Alice to Bob) that achieves the number of e-bits per input noisy pair given by (21).

17   Entropy inequalities – nonlinear witnesses of entanglement

Von Neumann entropy can be generalised to the Rényi family α-entropy $S_\alpha(\varrho)$

$$S_\alpha(\varrho) = \frac{1}{1-\alpha} \ln \text{Tr}\, \varrho^\alpha, \quad \alpha > 1 \qquad (22)$$

It is easy to check that the Rényi entropy in the $\alpha \to 1$ limit turns into the von Neumann entropy $S(\varrho)$. The natural question was whether there are quantum states that satisfy the analog of classical inequalities (18). In 1996 [237] it was proved that all non-entangled (separable) states at a finite dimensional Hilbert space for $\alpha = 1.2$ satisfy α-entropic inequalities:

$$S_\alpha(A|B) = S_\alpha(\varrho_{AB}) - S_\alpha(\varrho_B) \geq 0,$$
$$S_\alpha(B|A) = S_\alpha(\varrho_{AB}) - S_\alpha(\varrho_A) \geq 0 \qquad (23)$$

It presents entropic nonlinear entanglement criterion which does not require a priori knowledge of the state.

Nonlinear experimentally friendly collective entanglement witnesses were also proposed, which also do not require prior knowledge of a given state [238, 239]. In [240] Bovino et al. demonstrated first experimental measurement of a non-linear entanglement witness $S_2(\varrho) = - \text{Tr} \ln \varrho^2$, using local measurement on two pairs of polarization entangled photons.

At first, it seemed that the entropy criterion based on nonlinear entanglement witnesses, generally weaker than the criterion based on linear ones, will not play a major role. However, it turned out that, the feature of non-linearity is its strength. In particular, the nonlinear entanglement witnesses "feel" the subtle features of entanglement in quantum multi-body systems. In last decade there has been a renaissance of entropic witnesses opening up the field for wide applications. For pure or nearly pure states, entanglement was detected using Rényi S_2 entropy via a multi-body quantum interference [241, 242, 243, 244, 245] and local random measurements [246, 247, 248, 249, 250]. An experimental measurement of nonlinear witnesses of collective entanglement using hyper-entangled two-quart states has been performed [251], see also [252]. Quite recently, an experimental multi-body mixed state detection method has been proposed based on the positive partial transposition of a density matrix condition. This protocol gives the first direct PT measurement of moments in a multi-body system [253].

18   Quantum parallelism as the basis for quantum computing

Quantum computing is processing information using sequence of unitary operations (quantum gates) in order to obtain an answer to a predetermined question, e.g. is a given number factorizable with high probability [254]. As we have seen single qubit allows two basic states to be stored and processed simultaneously. The problem is that the decoherence process being a result of disturbance by environment occurs within a short time (decoherence time) destroys coherence. Roughly speaking decoherence time is the characteristic time for a generic qubit state (2) to be transformed into the mixture $\varrho = |a|^2 |0\rangle\langle 0| + |b|^2 |1\rangle\langle 1|$. One of the basic conditions for effective quantum computing requires that long relevant decoherence times, much longer than the gate operation time. This is one of the five basic DiVincenzo criteria required for a physical implementation of quantum computing [255]. If we take a superposition of n qubits then a pure state will represent a simultaneous superposition of $N = 2^n$ possible distinct basic states.

$$|\Psi\rangle = \sum_{i=0}^{N-1} C_i |i\rangle \qquad (24)$$

It is remarkable, that one can processes simultaneously an exponential number of basic states. This feature (quantum parallelism) underlies the superiority of quantum computing over classical one. To illustrate the latter suppose that we have access to quantum oracle that computes a given function $f(i)$ from an input i of n qubits $(i = 0, 1 \ldots 2^n)$.

Having a prepared string of qubits in the fiducial state of 0 and applying to each qubit, in parallel, Hadamard gate, we obtain a register of n qubits in an equal superposition of all bit strings

$$H|0\rangle \otimes H|0\rangle \otimes \cdots \otimes H|0\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle \quad (25)$$

where $|i\rangle$ is the computational basis state indexed by the binary number that would correspond to the number i in base-10 notation.

Now suppose that the function f is evaluated by unitary transformation $U_f : |x\rangle|0\rangle \rightarrow |x\rangle|f(x)\rangle$. Then the linearity of quantum formalism implies

$$U_f : \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle|0\rangle \quad \rightarrow \quad \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle|f(0)\rangle \tag{26}$$

This means that all possible evaluations of the function $f(x)$ can be evaluated in a single step.

The idea of quantum computing received a lot of support when it was discovered that certain difficult computational problems such as number factoring (Shor's algorithm [22]) and searching unstructured data (Grover's algorithm [24]) can be solved far more efficiently than classically. The efficiency of computation is measured by the computation complexity that is number of steps required to solve a given task as a function of the size of the input. The important algorithms: Deutsch-Jozsa [18], Shor [22] and Grover [24] have been discovered that demonstrate quantum supremacy over classical computing. All three algorithms have be implemented on primitive quantum computers based on NMR techniques [256], in ions traps [257] and quantum dots [258]. Since then many other algorithms have been discovered, such as quantum simulations, [259] variational quantum solvers [260] which demonstrate quantum supremacy [see more [261]].

Any realistic implementation of universal quantum computation is big challenge. It must meet the DiVincenzo criteria [255]. Except decoherence criterion, there are four more:

1. A scalable physical system with well characterized qubits.

2. The ability to initialize the state of the qubits to a simple fiducial state.

3. A "universal" set of quantum gates.

4. A qubit-specific measurement capability.

Notoriously the quantum computing process is disturbed by the interaction with the environment, causing the occurrence of errors. Therefore both bit (0,1) and phase ("0 + 1", "0 − 1") they must be protected. This seems impossible due to the non-cloning theorem. Fortunately, Shor [21] and Steane [262] overcame this difficulty by introduction of the error correction codes. The trick is that the information of a one logical qubit can be spread onto a highly entangled state of several physical qubits.

$$|0\rangle \rightarrow |\mathbf{0}\rangle_{\boldsymbol{L}} = [(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$$
$$\times (|000\rangle + |111\rangle)]/2\sqrt{2} \tag{27}$$
$$|1\rangle \rightarrow |\mathbf{1}\rangle_{\boldsymbol{L}} = [(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)$$
$$\times (|000\rangle - |111\rangle)]/2\sqrt{2} \tag{28}$$

This code first introduced by Shor [21] corrects both bit error σ_x and phase error σ_z.

Of course the error correction procedure itself is not error-free. Fortunately the possibility of efficient quantum computing is based on the so-called the threshold theorem: Error probability of elementary operation smaller than some threshold value $p < p'$ then efficient quantum computing possible [263, 264]. In practice, this condition, which is the basis of efficient quantum computing, is extremely demanding. Already in 1995 it was demonstrated that the quantum computing can be implemented with cold ions confined in linear trap and interacting laser beams [265]. The first 7-qubit quantum computer from IBM and Stanford University based on nuclear magnetic resonance realized Shor's algorithm, decomposition of the number $15 = 3 \times 5$ [256]. The scale of the difficulties is evidenced by the fact that a qualitative breakthrough in this field took place only after 18 years. Namely researchers at Google's quantum-computing laboratory in Santa Barbara, California, announced the first-ever demonstration of quantum supremacy on the 53 qubit quantum computer Sycomore, made of superconducting circuits that are kept at ultracold temperatures [266]. It executes algorithms quantum with 1500 gates. It is impressive achievement, however, it was designed for a specific problem — boson sampling [267], which is simplified non-universal model for quantum computing that may hold the key to implementing the first ever post-classical quantum computer. More specifically this is the process in which a very nontrivial output statistic is achieved quantumly which requires (under some reasonable assumptions) exponentially longer time to be produced by classical machines. While it is not a

quantum algorithm in a standard form its remarkable practical application to fast finding of some graph properties are predicted.

Quite recently Jian-Wei Pan and colleagues at the University of Science and Technology of China in Hefei et al. announced in December 2020 photon-based quantum computer, which demonstrates quantum supremacy via boson-sampling with 50-70 detected photons [268]. It could find solutions to the boson-sampling problem in 200 seconds, while classical China's Taihu-Light supercomputer. need 2.5 billion years. In in contrast to Google's Sycamore, the Chinese team's photonic circuit is not programmable [269].

19 Entanglement – resource in quantum metrology

The discovery that the use of entangled states in quantum metrology can improve the precision of measurements [270, 271] led to the rapid development of quantum enhanced metrology [49] which allows measure physical quantities by estimating the phase shift θ using interferometric techniques. A basic problem in quantum metrology can be formulated as in the diagram (Fig. 4): A probe state ϱ of N particles is prepared and then subject to a parameter-dependent quantum channel Λ_θ. The state $\varrho_\theta = \Lambda_\theta(\varrho)$ is finally measured via POVM measurement $\{\Pi_i\}_I$. It provides conditional probability distribution $p(i|\theta)$, which is used to estimate of θ via estimator function $\tilde{\Theta}(i)$ for given the measurement outcome i. The estimation of the phase shift is limited by uncertainty:

$$\Delta^2\tilde{\theta} = \langle(\tilde{\theta} - \theta)^2\rangle \qquad (29)$$

where $\langle\ \rangle$ means the average over all measurement results. The task is to find the optimal probe state ϱ, the optimal measurement Π and estimator , which minimize the uncertainty. For unbiased estimators and m independent measurements the phase uncertainty is limited by the quantum Cramer-Rao bound:

$$\Delta\tilde{\theta} \geq \frac{1}{\sqrt{mF_Q(\varrho_\theta)}} \qquad (30)$$

where F_Q is quantum Fisher information which quantifies asymptotic usefulness of quantum state and it can be estimated for the different quantum channels [49].

For unitary and noiseless quantum channel $\varrho_\theta = \Lambda_\theta(\varrho) = e^{-iH\theta}\varrho\, e^{+iH\theta}$ the quantum Fisher information optimized over measurement can be expressed in the form:

$$F_Q[\varrho, H] = 2\sum_{k,l} \frac{(\lambda_k - \lambda_l)^2}{\lambda_k + \lambda_l}|\langle k|H|l\rangle|^2 \qquad (31)$$

where H is the generator of the phase shift of the system, and $\varrho = \sum_k \lambda_k|k\rangle\langle k|$, $\sum_k \lambda_k = 1$.

For unitary dynamics of the linear two-mode interferometer the generator of the phase shift is $H \equiv \boldsymbol{J}_{\vec{n}} = \vec{n} \cdot \boldsymbol{J}$ where $\boldsymbol{J}_{\vec{n}}$ is a component of the collective spin operator angular momentum in the direction $\vec{n}$. It has been shown [272, 273], that for the separable input N-particle states, the quantum Fisher information is bounded by $F_Q[\varrho_{sep}, \boldsymbol{J}_{\vec{n}}] \leq N$. Hence the phase uncertainty $\Delta\tilde{\theta}$ is bounded by standard quantum limit (SQL) $\Delta\theta_{SN} : \Delta\tilde{\theta} \geq \Delta\theta_{SN}$ where

$$\Delta\theta_{SN} = \frac{1}{\sqrt{mN}} \qquad (32)$$

By using entangled probe states it is possible to overcome the SQL [49]. Quantum formalism imposes fundamental constraints on measurement precision that scales like $1/N$. It has been shown that, for general probe states of N particles F_Q is bounded by $F_Q[\varrho, \boldsymbol{J}_{\vec{n}}] \leq N^2$, [272, 273] and this inequality can be saturated by certain maximally entangled states. It allows to obtain optimal Heisenberg bound for the phase uncertainty

$$\Delta\theta_{HN} = \frac{1}{\sqrt{mN}} \qquad (33)$$

Note that the genuine multipartite entanglement is needed for reaching the highest sensitivities in some metrological tasks using two-mode linear interferometer [274, 275, 276]. Recently, various experiments have demonstrated beating the SQL (see [277] and references there in).

In a realistic scenario, quantum phase estimation requires taking into account the influence effects of losses and decoherence [278, 279, 280, 281, 282, 283, 284, 285]. In particular for N probe particles prepared in state ϱ^N and noisy channel $\Lambda_\Theta^{\otimes N}$, that acts independently on each particle $\varrho_\theta^N = \Lambda_\Theta^{\otimes N}(\varrho^N)$, quantum Fisher information $F_Q(\varrho_\theta^N)$ has asymptotically in N a bound that scales linearly with N: $F_Q(\varrho_\theta^N) \leq N\alpha$ giving bound [281]:

$$\Delta\tilde{\theta} \geq \frac{1}{\sqrt{\alpha mN}}, \qquad (34)$$

where α is constant. Thus the supremacy over SQL is only limited to constants factor. In particular, in the optical interferometry with losses for a generic two mode input N-photon state with precisely defined total photon number N the limit of phase sensitivity is:

$$\Delta\tilde{\theta} \geq \sqrt{\frac{1-\eta}{\eta N}} \qquad (35)$$

where η is optical transfer coefficient. This bound generalized to states having uncertainty photon
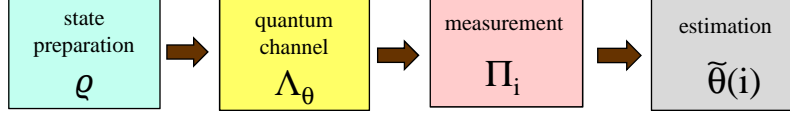
Figure 4: Phase estimation scheme

number such as coherent states and squeezed states was used to estimate the fundamental bound on GEO 600 interferometer strain sensitivity [286] where the phase noise decoherence [287], and quantum back-action are negligible [270]. It has been shown that the coherent-state squeezed vacuum strategy is optimal one for phase estimation with high precision on absolute scale [286].

Recently, a framework for optimization of quantum metrological protocols based on the tensor network approach for the channel with the correlated noise and the phase parameter unitarily encoded were presented [285]. Note that multiparameter estimation theory offers a general framework to explore imaging techniques beyond the Rayleigh limit [288].

Overall, the relationship between quantum metrology and the structure of quantum states is still not entirely clear. For example there are very weakly entangled states (bound entangled states) metrologically useful [218, 219] as well highly entangled states that are not useful for metrology [289]. It leads to the question: Are there situations were some synergy effects occurs possibly with analogy to previous communication protocols such as activation of bound entanglement? In attempt to answer this question, the criterion of metrological usefulness have been proposed as follows [290]:

The state ϱ is metrologically useful iff there exists Hamiltonian H such that Fisher quantum information (31) is sharply greater than Fisher information for separable states $F_Q[\varrho_{sep}, H]$ maximized over all separable states:

$$F_Q[\varrho, H] > \max_{\varrho_{sep}} = F_Q[\varrho_{sep}, H] =: F_Q^{(sep)}(H)$$

(36)

Then the metrological gain with respect to the Hamiltonian H defines as $g_H(\varrho) = F_Q[\varrho, H]/F_Q^{(sep)}(H)$ leads to the optimal gain $g(\varrho) = \max_{localH} g_H(\varrho)$. Having such defined metrological usefulness it has been shown that the bipartite entangled states that cannot outperform separable states in any linear interferometer, however can still be more useful than separable ones if several copies of them are considered or an ancilla is added to the quantum system. In particular it has been proved that all entangled bipartite pure states are metrologically useful.

20   Final remarks

In this article, I have focused only on selected aspects of quantum information. There are many other fascinating phenomena that deserve presentation. These include quantum correlations beyond entanglement [44, 291], nonlocality without entanglement [292], quantum channel super activation effect [293, 44], locking classical correlations in quantum states [294], resources theoretical approach to quantum thermodynamics [40], quantum Darwinism [295, 296, 297], objectivity [298, 299, 300, 301], quantum based randomness amplification against postquantum attacks [302, 303, 304] and others. They all underline the extremely complex nature of quantum information, which is not yet fully understood and provokes many open questions (see for example [305]). Among others there is a long-standing question: If the quantum formalism can be consistently extend to include quantum gravitation effect? If so, how it will impact on the quantum information concept?

Acknowledgments

References

[1] J. von Neumann. *Mathematische Grundlagen der Quantenmechanic.* Springer, Berlin (1932).

[2] C. E. Shannon. *A Mathematical Theory of Communication.* Bell System Technical Journal **27**, 379–423 (1948). DOI: 10.1002/j.1538-7305.1948.tb01338.x.

[3] A. Einstein, B. Podolsky, and N. Rosen. *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?* Physical Review **47**, 777–780 (1935). DOI: 10.1103/physrev.47.777.

[4] J. L. Park. *The concept of transition in quantum mechanics.* Foundations of Physics **1**, 23–33 (1970). DOI: 10.1007/bf00708652.

[5] S. Wiesner. *Conjugate coding.* ACM SIGACT News **15**, 78–88 (1983). DOI: 10.1145/1008908.1008920.

[6] A. S. Holevo. *Bounds for the Quantity of Information Transmitted by a Quantum Communication Channel.* Probl. Peredachi Inf. **9**, 3 (1973).

[7] J. P. Gordon. *Noise at optical frequencies; information theory.* In *P. A. Miles, editor, Quantum Electronics and Coherent Light; Proceedings of the International School of Physics Enrico Fermi, Course XXXI*, 156. Academic Press New York (1964).

[8] L. B. Levitin. *On the quantum measure of information.* In *Proceedings of the Fourth All-Union Conference on Information and Coding Theory, Sec. II.* Tashkent (1969).

[9] R. S. Ingarden. *Quantum information theory.* Reports on Mathematical Physics **10**, 43–72 (1976). DOI: 10.1016/0034-4877(76)90005-7.

[10] R. Ingarden, A. Kossakowski, and M. Ohya. *Information Dynamics and Open Systems: Classical and Quantum Approach.* Kluwer Academic Publishers (1997).

[11] J. S. Bell. *On the Einstein Podolsky Rosen paradox.* Physics Physique **1**, 195–200 (1964). DOI: 10.1103/physicsphysiquefizika.1.195.

[12] A. Aspect, J. Dalibard, and G. Roger. *Experimental Test of Bell's Inequalities Using Time- Varying Analyzers.* Physical Review Letters **49**, 1804–1807 (1982). DOI: 10.1103/physrevlett.49.1804.

[13] C. H. Bennett and G. Brassard. *Quantum Cryptography: Public Key Distribution and Coin Tossing.* In *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, 175–179. IEEE Computer Society Press, New York, Bangalore, India, December 1984 (1984).

[14] D. Deutsch. *Quantum theory, the Church–Turing principle and the universal quantum computer.* Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences **400**, 97–117 (1985). DOI: 10.1098/rspa.1985.0070.

[15] R. P. Feynman. *Quantum mechanical computers.* Foundations of Physics **16**, 507–531 (1986). DOI: 10.1007/bf01886518.

[16] A. K. Ekert. *Quantum cryptography based on Bell's theorem.* Physical Review Letters **67**, 661–663 (1991). DOI: 10.1103/physrevlett.67.661.

[17] C. H. Bennett and S. J. Wiesner. *Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states.* Physical Review Letters **69**, 2881–2884 (1992). DOI: 10.1103/physrevlett.69.2881.

[18] D. Deutsch and R. Jozsa. *Rapid solution of problems by quantum computation.* Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences **439**, 553–558 (1992). DOI: 10.1098/rspa.1992.0167.

[19] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels.* Physical Review Letters **70**, 1895–1899 (1993). DOI: 10.1103/physrevlett.70.1895.

[20] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert. *"Event-ready-detectors" Bell experiment via entanglement swapping.* Physical Review Letters **71**, 4287–4290 (1993). DOI: 10.1103/physrevlett.71.4287.

[21] P. W. Shor. *Scheme for reducing decoherence in quantum computer memory.* Physical Review A **52**, R2493–R2496 (1995). DOI: 10.1103/physreva.52.r2493.

[22] P. W. Shor. *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.* SIAM Journal on Computing **26**, 1484–1509 (1997). DOI: 10.1137/s0097539795293172.

[23] B. Schumacher. *Quantum coding.* Physical Review A **51**, 2738–2747 (1995). DOI: 10.1103/physreva.51.2738.

[24] L. K. Grover. *Quantum Mechanics Helps in Searching for a Needle in a Haystack.* Physical Review Letters **79**, 325–328 (1997). DOI: 10.1103/physrevlett.79.325.

[25] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger. *Experimental quantum teleportation. Nature* **390**, 575–579 (1997). DOI: 10.1038/37539.

[26] D. Boschi, S. Branca, F. D. Martini, L. Hardy, and S. Popescu. *Experimental Realization of Teleporting an Unknown Pure Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels. Physical Review Letters* **80**, 1121–1125 (1998). DOI: 10.1103/physrevlett.80.1121.

[27] A. Furusawa, J. L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzika. *Unconditional Quantum Teleportation. Science* **282**, 706–709 (1998). DOI: 10.1126/science.282.5389.706.

[28] M. Wilde. *From Classical to Quantum Shannon Theory.* Cambridge University Press (2019).

[29] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters. *Mixed-state entanglement and quantum error correction. Physical Review A* **54**, 3824–3851 (1996). DOI: 10.1103/physreva.54.3824.

[30] V. Coffman, J. Kundu, and W. K. Wootters. *Distributed entanglement. Physical Review A* **61**, 052306 (2000). DOI: 10.1103/physreva.61.052306.

[31] B. M. Terhal, M. M. Wolf, and A. C. Doherty. *Quantum Entanglement: A Modern Perspective. Physics Today* **56**, 46–52 (2003). DOI: 10.1063/1.1580049.

[32] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, Cambridge (2000).

[33] H.-P. Breuer and F. Petruccione. *The Theory of Open Quantum Systems.* Oxford University Press (2002).

[34] W. Heisenberg. *Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik. Zeitschrift für Physik* **43**, 172–198 (1927). DOI: 10.1007/bf01397280.

[35] N. Bohr. *New Problems in Quantum Theory. Nature* **121**, 579–579 (1928). DOI: 10.1038/121579a0.

[36] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki. *Quantum entanglement. Reviews of Modern Physics* **81**, 865–942 (2009). DOI: 10.1103/revmodphys.81.865.

[37] E. Schrödinger. *Discussion of Probability Relations between Separated Systems. Mathematical Proceedings of the Cambridge Philosophical Society* **31**, 555–563 (1935). DOI: 10.1017/s0305004100013554.

[38] R. Horodecki, M. Horodecki, and P. Horodecki. *Quantum information isomorphism: Beyond the dilemma of the Scylla of ontology and the Charybdis of instrumentalism. IBM Journal of Research and Development* **48**, 139–147 (2004). DOI: 10.1147/rd.481.0139.

[39] J. M. Raimond, M. Brune, and S. Haroche. *Manipulating quantum entanglement with atoms and photons in a cavity. Reviews of Modern Physics* **73**, 565–582 (2001). DOI: 10.1103/revmodphys.73.565.

[40] E. Chitambar and G. Gour. *Quantum resource theories. Reviews of Modern Physics* **91**, 025001 (2019). DOI: 10.1103/revmodphys.91.025001.

[41] L. Amico, R. Fazio, A. Osterloh, and V. Vedral. *Entanglement in many-body systems. Reviews of Modern Physics* **80**, 517–576 (2008). DOI: 10.1103/revmodphys.80.517.

[42] O. Gühne and G. Tóth. *Entanglement detection. Physics Reports* **474**, 1–75 (2009). DOI: 10.1016/j.physrep.2009.02.004.

[43] H. M. Wiseman, S. J. Jones, and A. C. Doherty. *Steering, Entanglement, Nonlocality, and the Einstein-Podolsky-Rosen Paradox. Physical Review Letters* **98**, 140402 (2007). DOI: 10.1103/physrevlett.98.140402.

[44] K. Modi, A. Brodutch, H. Cable, T. Paterek, and V. Vedral. *The classical-quantum boundary for correlations: Discord and related measures. Reviews of Modern Physics* **84**, 1655–1707 (2012). DOI: 10.1103/revmodphys.84.1655.

[45] A. Streltsov, G. Adesso, and M. B. Plenio. *Colloquium : Quantum coherence as a resource. Reviews of Modern Physics* **89**, 041003 (2017). DOI: 10.1103/revmodphys.89.041003.

[46] J. Goold, M. Huber, A. Riera, L. del Rio, and P. Skrzypczyk. *The role of quantum information in thermodynamics—a topical review. Journal of Physics A: Mathematical and Theoretical* **49**, 143001 (2016). DOI: 10.1088/1751-8113/49/14/143001.

[47] V. Scarani, A. Acín, G. Ribordy, and N. Gisin. *Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations.* Physical Review Letters **92**, 057901 (2004). DOI: 10.1103/physrevlett.92.057901.

[48] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. *Quantum cryptography.* Reviews of Modern Physics **74**, 145–195 (2002). DOI: 10.1103/revmodphys.74.145.

[49] L. Pezzè, A. Smerzi, M. K. Oberthaler, R. Schmied, and P. Treutlein. *Quantum metrology with nonclassical states of atomic ensembles.* Reviews of Modern Physics **90**, 035005 (2018). DOI: 10.1103/revmodphys.90.035005.

[50] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf. *Nonlocality and communication complexity.* Reviews of Modern Physics **82**, 665–698 (2010). DOI: 10.1103/revmodphys.82.665.

[51] Č. Brukner, M. Żukowski, J.-W. Pan, and A. Zeilinger. *Bell's Inequalities and Quantum Communication Complexity.* Physical Review Letters **92**, 127901 (2004). DOI: 10.1103/physrevlett.92.127901.

[52] P. Trojek, C. Schmid, M. Bourennane, Č. Brukner, M. Żukowski, and H. Weinfurter. *Experimental quantum communication complexity.* Physical Review A **72**, 050305 (2005). DOI: 10.1103/physreva.72.050305.

[53] W. H. Zurek. *Decoherence, einselection, and the quantum origins of the classical.* Reviews of Modern Physics **75**, 715–775 (2003). DOI: 10.1103/revmodphys.75.715.

[54] R. Heilmann, M. Gräfe, S. Nolte, and A. Szameit. *Arbitrary photonic wave plate operations on chip: Realizing Hadamard, Pauli-X and rotation gates for polarisation qubits.* Scientific Reports **4**, 4118 (2014). DOI: 10.1038/srep04118.

[55] V. V. Samartsev and T. G. Mitrofanova. *Qubits based on the exciton degrees of freedom of a semiconductor quantum dot.* Journal of Physics: Conference Series **1283**, 012012 (2019). DOI: 10.1088/1742-6596/1283/1/012012.

[56] R. Hanson, J. M. Elzerman, L. H. W. van Beveren, L. M. K. Vandersypen, and L. P. Kouwenhoven. *Electron spin qubits in quantum dots.* In *IEDM Technical Digest. IEEE International Electron Devices Meeting, 2004*, 533. IEEE (2005).

[57] D. Press, T. D. Ladd, B. Zhang, and Y. Yamamoto. *Complete quantum control of a single quantum dot spin using ultrafast optical pulses.* Nature **456**, 218–221 (2008). DOI: 10.1038/nature07530.

[58] T. Yamamoto, Y. A. Pashkin, O. Astafiev, Y. Nakamura, and J. S. Tsai. *Demonstration of conditional gate operation using superconducting charge qubits.* Nature **425**, 941–944 (2003). DOI: 10.1038/nature02015.

[59] A. F. Kockum and F. Nori. *Quantum Bits with Josephson Junctions.* In *Fundamentals and Frontiers of the Josephson Effect*, 703–741. Springer International Publishing (2019). DOI: 10.1007/978-3-030-20726-7_17.

[60] E. Knill, R. Laflamme, and G. J. Milburn. *A scheme for efficient quantum computation with linear optics.* Nature **409**, 46–52 (2001). DOI: 10.1038/35051009.

[61] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn. *Linear optical quantum computing with photonic qubits.* Reviews of Modern Physics **79**, 135–174 (2007). DOI: 10.1103/revmodphys.79.135.

[62] M. Parniak, M. Dąbrowski, M. Mazelanik, A. Leszczyński, M. Lipka, and W. Wasilewski. *Wavevector multiplexed atomic quantum memory via spatially-resolved single-photon detection.* Nature Communications **8**, 2140 (2017). DOI: 10.1038/s41467-017-02366-7.

[63] E. P. Wigner. *The Probability of the Existence of a Self-Reproducing Unit* London. (1961).

[64] W. K. Wootters and W. H. Zurek. *A single quantum cannot be cloned.* Nature **299**, 802–803 (1982). DOI: 10.1038/299802a0.

[65] D. Dieks. *Communication by EPR devices.* Physics Letters A **92**, 271–272 (1982). DOI: 10.1016/0375-9601(82)90084-6.

[66] V. Bužek and M. Hillery. *Quantum copying: Beyond the no-cloning theorem.* Physical Review A **54**, 1844–1852 (1996). DOI: 10.1103/physreva.54.1844.

[67] H. Fan, Y.-N. Wang, L. Jing, J.-D. Yue, H.-D. Shi, Y.-L. Zhang, and L.-Z. Mu. *Quantum cloning machines and the applications.* Physics Reports **544**, 241–322 (2014). DOI: 10.1016/j.physrep.2014.06.004.

[68] A. K. Pati and S. L. Braunstein. *Impossibility of deleting an unknown quantum state.* Nature **404**, 164–165 (2000). DOI: 10.1038/404130b0.

[69] U. Alvarez-Rodriguez, M. Sanz, L. Lamata, and E. Solano. *The Forbidden Quantum Adder.* Scientific Reports **5**, 11983 (2015). DOI: 10.1038/srep11983.

[70] M. Oszmaniec, A. Grudka, M. Horodecki, and A. Wójcik. *Creating a Superposition of Unknown Quantum States.* Physical Review Letters **116**, 110403 (2016). DOI: 10.1103/physrevlett.116.110403.

[71] K. Li, G. Long, H. Katiyar, T. Xin, G. Feng, D. Lu, and R. Laflamme. *Experimentally superposing two pure states with partial prior knowledge.* Physical Review A **95**, 022334 (2017). DOI: 10.1103/physreva.95.022334.

[72] X.-M. Hu, M.-J. Hu, J.-S. Chen, B.-H. Liu, Y.-F. Huang, C.-F. Li, G.-C. Guo, and Y.-S. Zhang. *Experimental creation of superposition of unknown photonic quantum states.* Physical Review A **94**, 033844 (2016). DOI: 10.1103/physreva.94.033844.

[73] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. *Experimental quantum cryptography.* Journal of Cryptology **5**, 3–28 (1992). DOI: 10.1007/bf00191318.

[74] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden. *Quantum key distribution over 67 km with a plug&play system.* New Journal of Physics **4**, 41–41 (2002). DOI: 10.1088/1367-2630/4/1/341.

[75] S. Wengerowsky, S. K. Joshi, F. Steinlechner, J. R. Zichi, S. M. Dobrovolskiy, R. van der Molen, J. W. N. Los, V. Zwiller, et al. *Entanglement distribution over a 96-km-long submarine optical fiber.* Proceedings of the National Academy of Sciences **116**, 6684–6688 (2019). DOI: 10.1073/pnas.1818752116.

[76] M. Peev, T. Länger, T. Lorünser, A. Happe, O. Maurhart, A. Poppe, and T. Themel. *The SECOQC Quantum-Key-Distribution Network in Vienna.* In Optical Fiber Communication Conference and National Fiber Optic Engineers Conference. OSA (2009). DOI: 10.1364/ofc.2009.othl2.

[77] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, et al. *Provably secure and practical quantum key distribution over 307 km of optical fibre.* Nature Photonics **9**, 163–168 (2015). DOI: 10.1038/nphoton.2014.327.

[78] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, et al. *Satellite-Relayed Intercontinental Quantum Network.* Physical Review Letters **120**, 030501 (2018). DOI: 10.1103/physrevlett.120.030501.

[79] W. O. Krawec, R. Liss, and T. Mor. *Security Proof Against Collective Attacks for an Experimentally Feasible Semi-Quantum Key Distribution Protocol.* arXiv e-prints, arXiv:2012.02127 (2020).

[80] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger. *Bell's theorem without inequalities.* American Journal of Physics **58**, 1131–1143 (1990). DOI: 10.1119/1.16243.

[81] W. Dür, G. Vidal, and J. I. Cirac. *Three qubits can be entangled in two inequivalent ways.* Physical Review A **62**, 062314 (2000). DOI: 10.1103/physreva.62.062314.

[82] W.-X. Cui, S. Hu, H.-F. Wang, A.-D. Zhu, and S. Zhang. *Deterministic conversion of a four-photon GHZ state to a W state via homodyne measurement.* Optics Express **24**, 15319 (2016). DOI: 10.1364/oe.24.015319.

[83] T. Haase, G. Alber, and V. M. Stojanovic. *W-to-GHZ state conversion in the Rydberg-blockade regime of neutral-atom systems: dynamical-symmetry-based approach.* arXiv e-prints, arXiv:2012.15169 (2020).

[84] F. Benatti, R. Floreanini, F. Franchini, and U. Marzolino. *Entanglement in indistinguishable particle systems.* Physics Reports **878**, 1–27 (2020). DOI: 10.1016/j.physrep.2020.07.003.

[85] R. Y. Chiao, P. G. Kwia, and A. M. Steinberg. *Quantum non-locality in two-photon experiments at Berkeley.* Quantum and Semiclassical Optics: Journal of the European Optical Society Part B **7**, 259–278 (1995). DOI: 10.1088/1355-5111/7/3/006.

[86] M. Erhard, M. Krenn, and A. Zeilinger. *Advances in high-dimensional quantum entanglement. Nature Reviews Physics* **2**, 365–381 (2020). DOI: 10.1038/s42254-020-0193-5.

[87] N. Akopian, N. H. Lindner, E. Poem, Y. Berlatzky, J. Avron, D. Gershoni, B. D. Gerardot, and P. M. Petroff. *Entangled Photon Pairs from Semiconductor Quantum Dots. Physical Review Letters* **96**, 130501 (2006). DOI: 10.1103/physrevlett.96.130501.

[88] B. Yurke and D. Stoler. *Einstein-Podolsky-Rosen effects from independent particle sources. Physical Review Letters* **68**, 1251–1254 (1992). DOI: 10.1103/physrevlett.68.1251.

[89] K. Życzkowski, P. Horodecki, M. Horodecki, and R. Horodecki. *Dynamics of quantum entanglement. Physical Review A* **65**, 012101 (2001). DOI: 10.1103/physreva.65.012101.

[90] T. Yu and J. Eberly. *Sudden death of entanglement: Classical noise effects. Optics Communications* **264**, 393–397 (2006). DOI: 10.1016/j.optcom.2006.01.061.

[91] T. Yu and J. H. Eberly. *Sudden Death of Entanglement. Science* **323**, 598–601 (2009). DOI: 10.1126/science.1167343.

[92] K. Życzkowski, P. Horodecki, A. Sanpera, and M. Lewenstein. *Volume of the set of separable states. Physical Review A* **58**, 883–892 (1998). DOI: 10.1103/physreva.58.883.

[93] M. Kuś and K. Życzkowski. *Geometry of entangled states. Physical Review A* **63**, 032307 (2001). DOI: 10.1103/physreva.63.032307.

[94] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih. *New High-Intensity Source of Polarization-Entangled Photon Pairs. Physical Review Letters* **75**, 4337–4341 (1995). DOI: 10.1103/physrevlett.75.4337.

[95] S. L. Braunstein, A. Mann, and M. Revzen. *Maximal violation of Bell inequalities for mixed states. Physical Review Letters* **68**, 3259–3261 (1992). DOI: 10.1103/physrevlett.68.3259.

[96] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. *Proposed Experiment to Test Local Hidden-Variable Theories. Physical Review Letters* **23**, 880–884 (1969). DOI: 10.1103/physrevlett.23.880.

[97] B. S. Cirel'son. *Quantum generalizations of Bell's inequality. Letters in Mathematical Physics* **4**, 93–100 (1980). DOI: 10.1007/bf00417500.

[98] D. I. Kaiser. *Tackling Loopholes in Experimental Tests of Bell's Inequality. arXiv e-prints*, arXiv:2011.09296 (2020).

[99] T. Scheidl, R. Ursin, J. Kofler, S. Ramelow, X.-S. Ma, T. Herbst, L. Ratschbacher, A. Fedrizzi, et al. *Violation of local realism with freedom of choice. Proceedings of the National Academy of Sciences* **107**, 19708–19713 (2010). DOI: 10.1073/pnas.1002780107.

[100] D. Aktas, S. Tanzilli, A. Martin, G. Pütz, R. Thew, and N. Gisin. *Demonstration of Quantum Nonlocality in the Presence of Measurement Dependence. Physical Review Letters* **114**, 220404 (2015). DOI: 10.1103/physrevlett.114.220404.

[101] M.-H. Li, C. Wu, Y. Zhang, W.-Z. Liu, B. Bai, Y. Liu, W. Zhang, Q. Zhao, et al. *Test of Local Realism into the Past without Detection and Locality Loopholes. Physical Review Letters* **121**, 080404 (2018). DOI: 10.1103/physrevlett.121.080404.

[102] M. Żukowski and Č. Brukner. *Quantum non-locality—it ain't necessarily so... Journal of Physics A: Mathematical and Theoretical* **47**, 424009 (2014). DOI: 10.1088/1751-8113/47/42/424009.

[103] E. G. Cavalcanti and H. M. Wiseman. *Bell Nonlocality, Signal Locality and Unpredictability (or What Bohr Could Have Told Einstein at Solvay Had He Known About Bell Experiments). Foundations of Physics* **42**, 1329–1338 (2012). DOI: 10.1007/s10701-012-9669-1.

[104] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani. *Device-independent quantum key distribution secure against collective attacks. New Journal of Physics* **11**, 045021 (2009). DOI: 10.1088/1367-2630/11/4/045021.

[105] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner. *Bell nonlocality. Reviews of Modern Physics* **86**, 419–478 (2014). DOI: 10.1103/revmodphys.86.419.

[106] R. Arnon-Friedman and J.-D. Bancal. *Device-independent certification of one-shot distillable entanglement. New Journal of Physics* **21**, 033010 (2019). DOI: 10.1088/1367-2630/aafef6.

[107] M. Farkas, M. Balanzó-Juandó, K. Łukanowski, J. Kołodyński, and A. Acín. *Bell nonlocality is not sufficient for the security of standard device-independent quantum key distribution protocols. arXiv e-prints*, arXiv:2103.02639v1 (2021).

[108] S. Kochen and E. Specker. *The Problem of Hidden Variables in Quantum Mechanics. Indiana University Mathematics Journal* **17**, 59–87 (1967). DOI: 10.1512/iumj.1968.17.17004.

[109] A. Cabello, J. Estebaranz, and G. García-Alcaine. *Bell-Kochen-Specker theorem: A proof with 18 vectors. Physics Letters A* **212**, 183–187 (1996). DOI: 10.1016/0375-9601(96)00134-x.

[110] A. Cabello. *Experimentally Testable State-Independent Quantum Contextuality. Physical Review Letters* **101**, 210401 (2008). DOI: 10.1103/physrevlett.101.210401.

[111] B. Marques, J. Ahrens, M. Nawareg, A. Cabello, and M. Bourennane. *Experimental Observation of Hardy-Like Quantum Contextuality. Physical Review Letters* **113**, 250403 (2014). DOI: 10.1103/physrevlett.113.250403.

[112] A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, R. Horodecki, P. Joshi, W. Kłobus, and A. Wójcik. *Quantifying Contextuality. Physical Review Letters* **112**, 120401 (2014). DOI: 10.1103/physrevlett.112.120401.

[113] A. A. Klyachko, M. A. Can, S. Binicioğlu, and A. S. Shumovsky. *Simple Test for Hidden Variables in Spin-1 Systems. Physical Review Letters* **101**, 020403 (2008). DOI: 10.1103/physrevlett.101.020403.

[114] N. D. Mermin. *Simple unified form for the major no-hidden-variables theorems. Physical Review Letters* **65**, 3373–3376 (1990). DOI: 10.1103/physrevlett.65.3373.

[115] I. Šupić and J. Bowles. *Self-testing of quantum systems: a review. Quantum* **4**, 337 (2020). DOI: 10.22331/q-2020-09-30-337.

[116] S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, et al. *Random numbers certified by Bell's theorem. Nature* **464**, 1021–1024 (2010). DOI: 10.1038/nature09008.

[117] N. Miklin, J. J. Borkała, and M. Pawłowski. *Semi-device-independent self-testing of unsharp measurements. Physical Review Research* **2**, 033014 (2020). DOI: 10.1103/physrevresearch.2.033014.

[118] R. Ramanathan, D. Goyeneche, S. Muhammad, P. Mironowicz, M. Grünfeld, M. Bourennane, and P. Horodecki. *Steering is an essential feature of non-locality in quantum theory. Nature Communications* **9**, 4244 (2018). DOI: 10.1038/s41467-018-06255-5.

[119] S. Popescu and D. Rohrlich. *Quantum nonlocality as an axiom. Foundations of Physics* **24**, 379–385 (1994). DOI: 10.1007/bf02058098.

[120] S. Popescu. *Nonlocality beyond quantum mechanics. Nature Physics* **10**, 264–270 (2014). DOI: 10.1038/nphys2916.

[121] M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Żukowski. *Information causality as a physical principle. Nature* **461**, 1101–1104 (2009). DOI: 10.1038/nature08400.

[122] M. Piani, M. Horodecki, P. Horodecki, and R. Horodecki. *Properties of quantum nonsignaling boxes. Physical Review A* **74**, 012305 (2006). DOI: 10.1103/physreva.74.012305.

[123] K. Horodecki, A. Grudka, P. Joshi, W. Kłobus, and J. Łodyga. *Axiomatic approach to contextuality and nonlocality. Physical Review A* **92**, 032104 (2015). DOI: 10.1103/physreva.92.032104.

[124] J.-D. Bancal and N. Gisin. *Non-Local Boxes for Networks. arXiv e-prints* , arXiv:2102.03597v1 (2021).

[125] W. van Dam. *Nonlocality & Communication Complexity.* Ph.D. thesis, Oxford (2000).

[126] G. Brassard, H. Buhrman, N. Linden, A. A. Méthot, A. Tapp, and F. Unger. *Limit on Nonlocality in Any World in Which Communication Complexity Is Not Trivial. Physical Review Letters* **96**, 250401 (2006). DOI: 10.1103/physrevlett.96.250401.

[127] J. Grunhaus, S. Popescu, and D. Rohrlich. *Jamming nonlocal quantum correlations. Physical Review A* **53**, 3781–3784 (1996). DOI: 10.1103/physreva.53.3781.

[128] P. Horodecki and R. Ramanathan. *The relativistic causality versus no-signaling paradigm for multi-party correlations. Nature Communications* **10**, 1701 (2019). DOI: 10.1038/s41467-019-09505-2.

[129] M. Eckstein, P. Horodecki, T. Miller, and R. Horodecki. *Operational causality in spacetime. Physical Review A* **101**, 042128 (2020). DOI: 10.1103/physreva.101.042128.

[130] T. Miller, M. Eckstein, P. Horodecki, and R. Horodecki. *Generally covariant N-particle dynamics. Journal of Geometry and Physics* **160**, 103990 (2021). DOI: 10.1016/j.geomphys.2020.103990.

[131] A. Dragan and A. Ekert. *Quantum principle of relativity. New Journal of Physics* **22**, 033038 (2020). DOI: 10.1088/1367-2630/ab76f7.

[132] M. Koashi and A. Winter. *Monogamy of quantum entanglement and other correlations. Physical Review A* **69**, 022309 (2004). DOI: 10.1103/physreva.69.022309.

[133] M. P. Peloso, I. Gerhardt, C. Ho, A. Lamas-Linares, and C. Kurtsiefer. *Daylight operation of a free space, entanglement-based quantum key distribution system. New Journal of Physics* **11**, 045007 (2009). DOI: 10.1088/1367-2630/11/4/045007.

[134] M. Fujiwara, K. ichiro Yoshino, Y. Nambu, T. Yamashita, S. Miki, H. Terai, Z. Wang, M. Toyoshima, et al. *Modified E91 protocol demonstration with hybrid entanglement photon source. Optics Express* **22**, 13616 (2014). DOI: 10.1364/oe.22.013616.

[135] H. Y. Lim, T. Vergoossen, R. Bedington, X. Bai, A. Villar, A. Lohrmann, and other. *Thermo-mechanical design for a miniaturized quantum light source on board the SpooQy-1 CubeSat. arXiv e-prints* , arXiv:2006.14442v1 (2020).

[136] C. C.-W. Lim, F. Xu, J.-W. Pan, and A. Ekert. *Security analysis of quantum key distribution with small block length and its application to quantum space communications. arXiv e-prints*, arXiv:2009.04882 (2020).

[137] J. Barrett, L. Hardy, and A. Kent. *No Signaling and Quantum Key Distribution. Physical Review Letters* **95**, 010503 (2005). DOI: 10.1103/physrevlett.95.010503.

[138] K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger. *Dense Coding in Experimental Quantum Communication. Physical Review Letters* **76**, 4656–4659 (1996). DOI: 10.1103/physrevlett.76.4656.

[139] T. Schaetz, M. D. Barrett, D. Leibfried, J. Chiaverini, J. Britton, W. M. Itano, J. D. Jost, C. Langer, et al. *Quantum Dense Coding with Atomic Qubits. Physical Review Letters* **93**, 040505 (2004). DOI: 10.1103/physrevlett.93.040505.

[140] D. Wei, X. Yang, J. Luo, X. Sun, X. Zeng, and M. Liu. *NMR experimental implementation of three-parties quantum superdense coding. Chinese Science Bulletin* **49**, 423–426 (2004). DOI: 10.1007/bf02900957.

[141] R. Liss and T. Mor. *From Practice to Theory: The "Bright Illumination" Attack on Quantum Key Distribution Systems.* In *Theory and Practice of Natural Computing*, vol.12494, 82–94. Springer International Publishing (2020). DOI: 10.1007/978-3-030-63000-3_7.

[142] L. Vaidman. *Teleportation of quantum states. Physical Review A* **49**, 1473–1476 (1994). DOI: 10.1103/physreva.49.1473.

[143] S. L. Braunstein and H. J. Kimble. *Teleportation of Continuous Quantum Variables. Physical Review Letters* **80**, 869–872 (1998). DOI: 10.1103/physrevlett.80.869.

[144] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, and N. Gisin. *Long-distance teleportation of qubits at telecommunication wavelengths. Nature* **421**, 509–513 (2003). DOI: 10.1038/nature01376.

[145] R. Ursin, T. Jennewein, M. Aspelmeyer, R. Kaltenbaek, M. Lindenthal, P. Walther, and A. Zeilinger. *Quantum teleportation across the Danube. Nature* **430**, 849–849 (2004). DOI: 10.1038/430849a.

[146] J. Yin, J.-G. Ren, H. Lu, Y. Cao, H.-L. Yong, Y.-P. Wu, C. Liu, S.-K. Liao, et al. *Quantum teleportation and entanglement distribution over 100-kilometre free-space channels. Nature* **488**, 185–188 (2012). DOI: 10.1038/nature11332.

[147] D. Gottesman and I. L. Chuang. *Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. Nature* **402**, 390–393 (1999). DOI: 10.1038/46503.

[148] X.-S. Ma, T. Herbst, T. Scheidl, D. Wang, S. Kropatschek, W. Naylor, B. Wittmann, A. Mech, et al. *Quantum teleportation over 143 kilometres using active feedforward. Nature* **489**, 269–273 (2012). DOI: 10.1038/nature11472.

[149] C. Nölleke, A. Neuzner, A. Reiserer, C. Hahn, G. Rempe, and S. Ritter. *Efficient Teleportation Between Remote Single-Atom Quantum Memories. Physical Review Letters* **110**, 140403 (2013). DOI: 10.1103/physrevlett.110.140403.

[150] W. Pfaff, B. J. Hensen, H. Bernien, S. B. van Dam, M. S. Blok, T. H. Taminiau, M. J. Tiggelman, R. N. Schouten, et al. *Unconditional quantum teleportation between distant solid-state quantum bits. Science* **345**, 532–535 (2014). DOI: 10.1126/science.1253512.

[151] Y.-H. Luo, H.-S. Zhong, M. Erhard, X.-L. Wang, L.-C. Peng, M. Krenn, X. Jiang, L. Li, et al. *Quantum Teleportation in High Dimensions. Physical Review Letters* **123**, 070505 (2019). DOI: 10.1103/physrevlett.123.070505.

[152] X.-M. Hu, C. Zhang, B.-H. Liu, Y. Cai, X.-J. Ye, Y. Guo, W.-B. Xing, C.-X. Huang, et al. *Experimental High-Dimensional Quantum Teleportation. Physical Review Letters* **125**, 230501 (2020). DOI: 10.1103/physrevlett.125.230501.

[153] J.-G. Ren, P. Xu, H.-L. Yong, L. Zhang, S.-K. Liao, J. Yin, W.-Y. Liu, W.-Q. Cai, et al. *Ground-to-satellite quantum teleportation. Nature* **549**, 70–73 (2017). DOI: 10.1038/nature23675.

[154] N. Gisin. *Entanglement 25 Years after Quantum Teleportation: Testing Joint Measurements in Quantum Networks. Entropy* **21**, 325 (2019). DOI: 10.3390/e21030325.

[155] H. Salih, J. R. Hance, W. McCutcheon, T. Rudolph, and J. Rarity. *Deterministic Teleportation and Universal Computation Without Particle Exchange. arXiv e-prints*, arXiv:2009.05564 (2020).

[156] M. Horodecki, P. Horodecki, and R. Horodecki. *General teleportation channel, singlet fraction, and quasidistillation. Physical Review A* **60**, 1888–1898 (1999). DOI: 10.1103/physreva.60.1888.

[157] S. Ishizaka and T. Hiroshima. *Asymptotic Teleportation Scheme as a Universal Programmable Quantum Processor. Physical Review Letters* **101**, 240501 (2008). DOI: 10.1103/physrevlett.101.240501.

[158] S. Ishizaka and T. Hiroshima. *Quantum teleportation scheme by selecting one of multiple output ports. Physical Review A* **79**, 042306 (2009). DOI: 10.1103/physreva.79.042306.

[159] P. Kopszak, M. Mozrzymas, M. Studzinski, and M. Horodecki. *Multiport based teleportation – transmission of a large amount of quantum information. arXiv e-prints*, arXiv:2008.00856v2 (2021).

[160] S. Roy, T. Das, D. Das, A. Sen(De), and U. Sen. *How efficient is transport of quantum cargo through multiple highways? Annals of Physics* **422**, 168281 (2020). DOI: 10.1016/j.aop.2020.168281.

[161] M. Murao, D. Jonathan, M. B. Plenio, and V. Vedral. *Quantum telecloning and multiparticle entanglement. Physical Review A* **59**, 156–161 (1999). DOI: 10.1103/physreva.59.156.

[162] S. Bose, V. Vedral, and P. L. Knight. *Multiparticle generalization of entanglement swapping. Physical Review A* **57**, 822–829 (1998). DOI: 10.1103/physreva.57.822.

[163] J.-W. Pan, Z.-B. Chen, C.-Y. Lu, H. Weinfurter, A. Zeilinger, and M. Żukowski. *Multiphoton entanglement and interferometry. Reviews of Modern Physics* **84**, 777–838 (2012). DOI: 10.1103/revmodphys.84.777.

[164] J.-W. Pan, D. Bouwmeester, H. Weinfurter, and Z. A. *Experimental entanglement swapping: Entangling photons that never interacted. Phys. Rev. Lett.* **80**, 3891–3894 (1998).

[165] R.-B. Jin, M. Takeoka, U. Takagi, R. Shimizu, and M. Sasaki. *Highly efficient entanglement swapping and teleportation at telecom wavelength. Scientific Reports* **5**, 9333 (2015). DOI: 10.1038/srep09333.

[166] F. B. Basset, M. B. Rota, C. Schimpf, D. Tedeschi, K. D. Zeuner, S. F. C. da Silva, M. Reindl, V. Zwiller, et al. *Entanglement Swapping with Photons Generated on Demand by a Quantum Dot. Phys. Rev. Lett.* **123**, 160501 (Published 14 October 2019). DOI: 10.1103/PhysRevLett.123.160501.

[167] Y. Zhang, M. Agnew, T. Roger, F. S. Roux, T. Konrad, D. Faccio, J. Leach, and A. Forbes. *Simultaneous entanglement*

swapping of multiple orbital angular momentum states of light. Nature Communications **8**, 632 (2017). DOI: 10.1038/s41467-017-00706-1.

[168] V. Zapatero and M. Curty. *Long-distance device-independent quantum key distribution. Scientific Reports* **9**, 17749 (2019). DOI: 10.1038/s41598-019-53803-0.

[169] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller. *Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication. Physical Review Letters* **81**, 5932–5935 (1998). DOI: 10.1103/physrevlett.81.5932.

[170] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller. *Long-distance quantum communication with atomic ensembles and linear optics. Nature* **414**, 413–418 (2001). DOI: 10.1038/35106500.

[171] B. K. Behera, S. Seth, A. Das, and P. K. Panigrahi. *Demonstration of entanglement purification and swapping protocol to design quantum repeater in IBM quantum computer. Quantum Information Processing* **18**. DOI: 10.1007/s11128-019-2229-2.

[172] M. Zopf, R. Keil, Y. Chen, J. Yang, D. Chen, F. Ding, and O. G. Schmidt. *Entanglement Swapping with Semiconductor-generated Photons. Phys. Rev. Lett.* **123**, 160502 (2019). DOI: 10.1103/PhysRevLett.123.160502.

[173] Z. Zhang and X. Man. *Multiparty Quantum Secret Sharing Based on Entanglement Swapping. Physical Review A* **72**, 022303 (June 2004). DOI: 10.1103/PhysRevA.72.022303.

[174] N. T. V. Luu and S. Shimamoto. *Advanced Multiparty Quantum Secret Sharing using Entanglement Swapping.* In *2006 2nd International Conference on Information Communication Technologies*, volume 2, 2051–2056 (2006). DOI: 10.1109/ICTTA.2006.1684717.

[175] L. Gurvits. *Classical deterministic complexity of Edmonds' Problem and quantum entanglement.* In *Proceedings of the thirty-fifth ACM symposium on Theory of computing - STOC '03*, 10. ACM Press (2003). DOI: 10.1145/780542.780545.

[176] A. Peres. *Separability Criterion for Density Matrices. Physical Review Letters* **77**, 1413–1415 (1996). DOI: 10.1103/physrevlett.77.1413.

[177] S. L. Woronowicz. *Nonextendible positive maps. Communications in Mathematical Physics* **51**, 243–282 (1976). DOI: 10.1007/bf01617922.

[178] M. Horodecki, P. Horodecki, and R. Horodecki. *Separability of mixed states: necessary and sufficient conditions. Physics Letters A* **223**, 1–8 (1996). DOI: 10.1016/s0375-9601(96)00706-2.

[179] B. M. Terhal. *Bell inequalities and the separability criterion. Physics Letters A* **271**, 319–326 (2000). DOI: 10.1016/s0375-9601(00)00401-1.

[180] M. Lewenstein, B. Kraus, J. I. Cirac, and P. Horodecki. *Optimization of entanglement witnesses. Physical Review A* **62**, 052310 (2000). DOI: 10.1103/physreva.62.052310.

[181] M. Lewenstein, B. Kraus, P. Horodecki, and J. I. Cirac. *Characterization of separable states and entanglement witnesses. Physical Review A* **63**, 044304 (2001). DOI: 10.1103/physreva.63.044304.

[182] A. Jamiołkowski. *Linear transformations which preserve trace and positive semidefiniteness of operators. Reports on Mathematical Physics* **3**, 275–278 (1972). DOI: 10.1016/0034-4877(72)90011-0.

[183] M. Barbieri, F. D. Martini, G. D. Nepi, P. Mataloni, G. M. D'Ariano, and C. Macchiavello. *Detection of Entanglement with Polarized Photons: Experimental Realization of an Entanglement Witness. Physical Review Letters* **91**. DOI: 10.1103/physrevlett.91.227901.

[184] M. Bourennane, M. Eibl, C. Kurtsiefer, S. Gaertner, H. Weinfurter, O. Gühne, P. Hyllus, D. Bruß, et al. *Experimental Detection of Multipartite Entanglement using Witness Operators. Physical Review Letters* **92**, 087902 (2004). DOI: 10.1103/physrevlett.92.087902.

[185] C. F. Roos. *Control and Measurement of Three-Qubit Entangled States. Science* **304**, 1478–1480 (2004). DOI: 10.1126/science.1097522.

[186] J. B. Altepeter, E. R. Jeffrey, P. G. Kwiat, S. Tanzilli, N. Gisin, and A. Acín. *Experimental Methods for Detecting Entanglement. Physical Review Letters*

95, 033601 (2005). DOI: 10.1103/physrevlett.95.033601.

[187] H. Häffner, W. Hänsel, C. F. Roos, J. Benhelm, D. C. al kar, M. Chwalla, T. Körber, U. D. Rapol, et al. *Scalable multiparticle entanglement of trapped ions. Nature* **438**, 643–646 (2005). DOI: 10.1038/nature04279.

[188] H. Mikami, Y. Li, K. Fukuoka, and T. Kobayashi. *New High-Efficiency Source of a Three-PhotonWState and its Full Characterization Using Quantum State Tomography. Physical Review Letters* **95**, 150404 (2005). DOI: 10.1103/physrevlett.95.150404.

[189] N. K. Langford, T. J. Weinhold, R. Prevedel, K. J. Resch, A. Gilchrist, J. L. O'Brien, G. J. Pryde, and A. G. White. *Demonstration of a Simple Entangling Optical Gate and Its Use in Bell-State Analysis. Physical Review Letters* **95**, 210504 (2005). DOI: 10.1103/physrevlett.95.210504.

[190] W. Laskowski, D. Richart, C. Schwemmer, T. Paterek, and H. Weinfurter. *Experimental Schmidt Decomposition and State Independent Entanglement Detection. Physical Review Letters* **108**. DOI: 10.1103/physrevlett.108.240501.

[191] B. Dirkse, M. Pompili, R. Hanson, M. Walter, and S. Wehner. *Witnessing entanglement in experiments with correlated noise. Quantum Science and Technology* **5**, 035007 (2020). DOI: 10.1088/2058-9565/ab8d88.

[192] C. Branciard, D. Rosset, Y.-C. Liang, and N. Gisin. *Measurement-Device-Independent Entanglement Witnesses for All Entangled Quantum States. Physical Review Letters* **110**, 060405 (2013). DOI: 10.1103/physrevlett.110.060405.

[193] M. Oszmaniec and M. Kuś. *Universal framework for entanglement detection. Physical Review A* **88**, 052328 (2013). DOI: 10.1103/physreva.88.052328.

[194] P. Badziag, Č. Brukner, W. Laskowski, T. Paterek, and M. Żukowski. *Experimentally Friendly Geometrical Criteria for Entanglement. Physical Review Letters* **100**, 140403 (2008). DOI: 10.1103/physrevlett.100.140403.

[195] W. Laskowski, M. Markiewicz, T. Paterek, and M. Żukowski. *Correlation-tensor criteria for genuine multiqubit entanglement.*

Physical Review A **84**, 062305 (2011). DOI: 10.1103/physreva.84.062305.

[196] M. Markiewicz, A. Kołodziejski, Z. Puchała, A. Rutkowski, T. Tylec, and W. Laskowski. *Unified approach to geometric and positive-map-based nonlinear entanglement identifiers. Physical Review A* **97**, 042339 (2018). DOI: 10.1103/physreva.97.042339.

[197] C.-J. Zhang, Y.-S. Zhang, S. Zhang, and G.-C. Guo. *Entanglement detection beyond the computable cross-norm or realignment criterion. Physical Review A* **77**, 060301(R) (2008). DOI: 10.1103/physreva.77.060301.

[198] G. Sarbicki, G. Scala, and D. Chruściński. *Family of multipartite separability criteria based on a correlation tensor. Physical Review A* **101**, 012341 (2020). DOI: 10.1103/physreva.101.012341.

[199] G. Sarbicki, G. Scala, and D. Chruściński. *Detection power of separability criteria based on a correlation tensor: a case study. arXiv e-prints* , arXiv:2011.10159 (2020).

[200] P. Horodecki. *Separability criterion and inseparable mixed states with positive partial transposition. Physics Letters A* **232**, 333–339 (1997). DOI: 10.1016/s0375-9601(97)00416-7.

[201] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters. *Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels. Physical Review Letters* **76**, 722–725 (1996). DOI: 10.1103/physrevlett.76.722.

[202] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera. *Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels. Physical Review Letters* **77**, 2818–2821 (1996). DOI: 10.1103/physrevlett.77.2818.

[203] M. Horodecki, P. Horodecki, and R. Horodecki. *Inseparable Two Spin-12Density Matrices Can Be Distilled to a Singlet Form. Physical Review Letters* **78**, 574–577 (1997). DOI: 10.1103/physrevlett.78.574.

[204] M. Horodecki, P. Horodecki, and R. Horodecki. *Mixed-State Entanglement and Distillation: Is there a "Bound" Entanglement in Nature? Physical Review Letters* **80**, 5239–5242 (1998). DOI: 10.1103/physrevlett.80.5239.

[205] R. Horodecki. *Bound entanglement – mysterious invention of nature.* Europhysics News **41**, 21–24 (2010). DOI: 10.1051/epn/2010603.

[206] E. Amselem and M. Bourennane. *Experimental four-qubit bound entanglement.* Nature Physics **5**, 748–752 (2009). DOI: 10.1038/nphys1372.

[207] J. Lavoie, R. Kaltenbaek, M. Piani, and K. J. Resch. *Experimental Bound Entanglement in a Four-Photon State.* Physical Review Letters **105**, 130501 (2010). DOI: 10.1103/physrevlett.105.130501.

[208] J. T. Barreiro, P. Schindler, O. Gühne, T. Monz, M. Chwalla, C. F. Roos, M. Hennrich, and R. Blatt. *Experimental multiparticle entanglement dynamics induced by decoherence.* Nature Physics **6**, 943–946 (2010). DOI: 10.1038/nphys1781.

[209] H. Kampermann, D. Bruß, X. Peng, and D. Suter. *Experimental generation of pseudo-bound-entanglement.* Physical Review A **81**, 040304(R) (2010). DOI: 10.1103/physreva.81.040304.

[210] J. DiGuglielmo, A. Samblowski, B. Hage, C. Pineda, J. Eisert, and R. Schnabel. *Experimental Unconditional Preparation and Detection of a Continuous Bound Entangled State of Light.* Physical Review Letters **107**, 240503 (2011). DOI: 10.1103/physrevlett.107.240503.

[211] G. Tóth, C. Knapp, O. Gühne, and H. J. Briegel. *Optimal Spin Squeezing Inequalities Detect Bound Entanglement in Spin Models.* Physical Review Letters **99**, 250405 (2007). DOI: 10.1103/physrevlett.99.250405.

[212] A. Ferraro, D. Cavalcanti, A. García-Saez, and A. Acín. *Thermal Bound Entanglement in Macroscopic Systems and Area Law.* Physical Review Letters **100**, 080502 (2008). DOI: 10.1103/physrevlett.100.080502.

[213] P. Horodecki, M. Horodecki, and R. Horodecki. *Bound Entanglement Can Be Activated.* Physical Review Letters **82**, 1056–1059 (1999). DOI: 10.1103/physrevlett.82.1056.

[214] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim. *Secure Key from Bound Entanglement.* Physical Review Letters **94**, 160502 (2005). DOI: 10.1103/physrevlett.94.160502.

[215] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim. *General Paradigm for Distilling Classical Key From Quantum States.* IEEE Transactions on Information Theory **55**, 1898–1929 (2009). DOI: 10.1109/tit.2008.2009798.

[216] K. Dobek, M. Karpiński, R. Demkowicz-Dobrzański, K. Banaszek, and P. Horodecki. *Experimental Extraction of Secure Correlations from a Noisy Private State.* Physical Review Letters **106**, 030501 (2011). DOI: 10.1103/physrevlett.106.030501.

[217] T. Vértesi and N. Brunner. *Disproving the Peres conjecture by showing Bell nonlocality from bound entanglement.* Nature Communications **5**, 5297 (2014). DOI: 10.1038/ncomms6297.

[218] Ł. Czekaj, A. Przysiężna, M. Horodecki, and P. Horodecki. *Quantum metrology: Heisenberg limit with bound entanglement.* Physical Review A **92**, 062303 (2015). DOI: 10.1103/physreva.92.062303.

[219] G. Tóth and T. Vértesi. *Quantum States with a Positive Partial Transpose are Useful for Metrology.* Physical Review Letters **120**, 020506 (2018). DOI: 10.1103/physrevlett.120.020506.

[220] K. F. Pál, G. Tóth, E. Bene, and T. Vértesi. *Bound entangled "singlets" for quantum metrology. arXiv e-prints*, arXiv:2002.12409 (2020).

[221] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick. *Practical device-independent quantum cryptography via entropy accumulation.* Nature Communications **9**. DOI: 10.1038/s41467-017-02307-4.

[222] R. Arnon-Friedman and F. Leditzky. *Upper bounds on device-independent quantum key distribution rates and a revised Peres conjecture. arXiv e-prints*, arXiv:2005.12325 (2020).

[223] M. Christandl, R. Ferrara, and K. Horodecki. *Upper bounds on the rate in device-independent quantum key distribution. arXiv e-prints*, arXiv:2005.13511v2 (2020).

[224] E. Schrödinger. *Die gegenwärtige Situation in der Quantenmechanik.* Naturwissenschaften **23**, 807-812 (1935).

[225] R. Horodecki and P. Horodecki. *Quantum redundancies and local realism. Physics*

28

Letters A **194**, 147–152 (1994). DOI: 10.1016/0375-9601(94)91275-0.

[226] N. J. Cerf and C. Adami. *Negative Entropy and Information in Quantum Mechanics. Physical Review Letters* **79**, 5194–5197 (1997). DOI: 10.1103/physrevlett.79.5194.

[227] B. Schumacher and M. D. Westmoreland. *Sending classical information via noisy quantum channels. Physical Review A* **56**, 131–138 (1997). DOI: 10.1103/physreva.56.131.

[228] A. Holevo. *The capacity of the quantum channel with general signal states. IEEE Transactions on Information Theory* **44**, 269–273 (1998). DOI: 10.1109/18.651037.

[229] I. Devetak. *The Private Classical Capacity and Quantum Capacity of a Quantum Channel. IEEE Transactions on Information Theory* **51**, 44–55 (2005). DOI: 10.1109/tit.2004.839515.

[230] C. H. Bennett, I. Devetak, P. W. Shor, and J. A. Smolin. *Inequalities and Separations Among Assisted Capacities of Quantum Channels. Physical Review Letters* **96**, 150502 (2006). DOI: 10.1103/physrevlett.96.150502.

[231] K. Horodecki, M. Horodecki, P. Horodecki, D. Leung, and J. Oppenheim. *Quantum Key Distribution Based on Private States: Unconditional Security Over Untrusted Channels With Zero Quantum Capacity. IEEE Transactions on Information Theory* **54**, 2604–2620 (2008). DOI: 10.1109/tit.2008.921870.

[232] K. Li, A. Winter, X. Zou, and G. Guo. *Private Capacity of Quantum Channels is Not Additive. Physical Review Letters* **103**, 120501 (2009). DOI: 10.1103/physrevlett.103.120501.

[233] S. Bäuml, M. Christandl, K. Horodecki, and A. Winter. *Limitations on quantum key repeaters. Nature Communications* **6**. DOI: 10.1038/ncomms7908.

[234] D. Slepian and J. Wolf. *Noiseless coding of correlated information sources. IEEE Transactions on Information Theory* **19**, 471–480 (1973). DOI: 10.1109/tit.1973.1055037.

[235] M. Horodecki, J. Oppenheim, and A. Winter. *Partial quantum information. Nature* **436**, 673–676 (2005). DOI: 10.1038/nature03909.

[236] I. Devetak and A. Winter. *Distillation of secret key and entanglement from quantum states. Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences* **461**, 207–235 (2005). DOI: 10.1098/rspa.2004.1372.

[237] R. Horodecki and M. Horodecki. *Information-theoretic aspects of inseparability of mixed states. Physical Review A* **54**, 1838–1843 (1996). DOI: 10.1103/physreva.54.1838.

[238] P. Horodecki and A. Ekert. *Method for Direct Detection of Quantum Entanglement. Physical Review Letters* **89**, 125003 (2002). DOI: 10.1103/physrevlett.89.127902.

[239] P. Horodecki. *Measuring Quantum Entanglement without Prior State Reconstruction. Physical Review Letters* **90**, 167901 (2003). DOI: 10.1103/physrevlett.90.167901.

[240] F. A. Bovino, G. Castagnoli, A. Ekert, P. Horodecki, C. M. Alves, and A. V. Sergienko. *Direct Measurement of Nonlinear Properties of Bipartite Quantum States. Physical Review Letters* **95**, 240407 (2005). DOI: 10.1103/physrevlett.95.240407.

[241] R. Islam, R. Ma, P. M. Preiss, M. E. Tai, A. Lukin, M. Rispoli, and M. Greiner. *Measuring entanglement entropy in a quantum many-body system. Nature* **528**, 77–83 (2015). DOI: 10.1038/nature15750.

[242] A. M. Kaufman, M. E. Tai, A. Lukin, M. Rispoli, R. Schittko, P. M. Preiss, and M. Greiner. *Quantum thermalization through entanglement in an isolated many-body system. Science* **353**, 794–800 (2016). DOI: 10.1126/science.aaf6725.

[243] N. M. Linke, S. Johri, C. Figgatt, K. A. Landsman, A. Y. Matsuura, and C. Monroe. *Measuring the Rényi entropy of a two-site Fermi-Hubbard model on a trapped ion quantum computer. Physical Review A* **98**, 052334 (2018). DOI: 10.1103/physreva.98.052334.

[244] C. M. Alves and D. Jaksch. *Multipartite Entanglement Detection in Bosons. Physical Review Letters* **93**, 110501 (2004). DOI: 10.1103/physrevlett.93.110501.

[245] A. J. Daley, H. Pichler, J. Schachenmayer, and P. Zoller. *Measuring Entanglement Growth in Quench Dynamics of Bosons in an Optical Lattice. Physical Review Letters* **109**, 020505 (2012). DOI: 10.1103/physrevlett.109.020505.

[246] T. Brydges, A. Elben, P. Jurcevic, B. Vermersch, C. Maier, B. P. Lanyon, P. Zoller, R. Blatt, et al. *Probing Rényi entanglement entropy via randomized measurements. Science* **364**, 260–263 (2019). DOI: 10.1126/science.aau4963.

[247] S. J. van Enk and C. W. J. Beenakker. *Measuring* $\mathrm{Tr}\,\rho^n$ *on Single Copies of ρ Using Random Measurements. Physical Review Letters* **108**, 110503 (2012). DOI: 10.1103/physrevlett.108.110503.

[248] A. Elben, B. Vermersch, M. Dalmonte, J. Cirac, and P. Zoller. *Rényi Entropies from Random Quenches in Atomic Hubbard and Spin Models. Physical Review Letters* **120**, 050406 (2018). DOI: 10.1103/physrevlett.120.050406.

[249] A. Elben, B. Vermersch, C. F. Roos, and P. Zoller. *Statistical correlations between locally randomized measurements: A toolbox for probing entanglement in manybody quantum states. Physical Review A* **99**, 052323 (2019). DOI: 10.1103/physreva.99.052323.

[250] H.-Y. Huang, R. Kueng, and J. Preskill. *Predicting many properties of a quantum system from very few measurements. Nature Physics* **16**, 1050–1057 (2020). DOI: 10.1038/s41567-020-0932-7.

[251] V. Trávníček, K. Bartkiewicz, A. Černoch, and K. Lemr. *Experimental measurement of a nonlinear entanglement witness by hyperentangling two-qubit states. Physical Review A* **98**, 032307 (2018). DOI: 10.1103/physreva.98.032307.

[252] K. Bartkiewicz, K. Lemr, A. Černoch, and A. Miranowicz. *Bell nonlocality and fully entangled fraction measured in an entanglement-swapping device without quantum state tomography. Physical Review A* **95**, 030102(R) (2017). DOI: 10.1103/physreva.95.030102.

[253] A. Elben, R. Kueng, H.-Y. R. Huang, R. van Bijnen, C. Kokail, M. Dalmonte, P. Calabrese, B. Kraus, et al. *Mixed-State Entanglement from Local Randomized Measurements. Physical Review Letters* **125**, 200501 (2020). DOI: 10.1103/physrevlett.125.200501.

[254] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, et al. *Elementary gates for quantum computation. Physical Review A* **52**, 3457–3467 (1995). DOI: 10.1103/physreva.52.3457.

[255] D. P. DiVincenzo. *The Physical Implementation of Quantum Computation. Fortschritte der Physik* **48**, 771–783 (2000). DOI: 10.1002/1521-3978(200009)48:9/11<771::aid-prop771>3.0.co;2-e.

[256] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang. *Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. Nature* **414**, 883–887 (2001). DOI: 10.1038/414883a.

[257] W.-L. Yang, H. Wei, C.-Y. Chen, and M. Feng. *Implementation of a many-qubit Grover search with trapped ultracold ions. Journal of the Optical Society of America B* **25**, 1720 (2008). DOI: 10.1364/josab.25.001720.

[258] P. Bianucci, A. Muller, C. K. Shih, Q. Q. Wang, Q. K. Xue, and C. Piermarocchi. *Experimental realization of the one qubit Deutsch-Jozsa algorithm in a quantum dot. Physical Review B* **69**, 161303(R) (2004). DOI: 10.1103/physrevb.69.161303.

[259] S. Lloyd. *Universal Quantum Simulators. Science* **273**, 1073–1078 (1996). DOI: 10.1126/science.273.5278.1073.

[260] A. Peruzzo, J. McClean, P. Shadbolt, M.-H. Yung, X.-Q. Zhou, P. J. Love, A. Aspuru-Guzik, and J. L. O'Brien. *A variational eigenvalue solver on a photonic quantum processor. Nature Communications* **5**, 4213 (2014). DOI: 10.1038/ncomms5213.

[261] Y. Alexeev, D. Bacon, K. R. Brown, R. Calderbank, L. D. Carr, F. T. Chong, B. DeMarco, D. Englund, et al. *Quantum Computer Systems for Scientific Discovery. arXiv e-prints*, arXiv:1912.07577 (2019).

[262] A. M. Steane. *Simple quantum error-correcting codes. Physical Review A* **54**, 4741–4751 (1996). DOI: 10.1103/physreva.54.4741.

[263] D. Aharonov and M. Ben-Or. *Fault-tolerant quantum computation with constant error.* In *Proceedings of the twenty-ninth annual ACM symposium on Theory of computing - STOC '97*, 176. ACM Press (1997). DOI: 10.1145/258533.258579.

[264] E. Knill, R. Laflamme, and W. H. Zurek. *Resilient Quantum Computation. Science* **279**, 342–345 (1998). DOI: 10.1126/science.279.5349.342.

[265] J. I. Cirac and P. Zoller. *Quantum Computations with Cold Trapped Ions. Physical Review Letters* **74**, 4091–4094 (1995). DOI: 10.1103/physrevlett.74.4091.

[266] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, et al. *Quantum supremacy using a programmable superconducting processor. Nature* **574**, 505–510 (2019). DOI: 10.1038/s41586-019-1666-5.

[267] S. Aaronson and A. Arkhipov. *The Computational Complexity of Linear Optics. Theory of Computing* **9**, 143–252 (2013). DOI: 10.4086/toc.2013.v009a004.

[268] H.-S. Zhong, H. Wang, Y.-H. Deng, M.-C. Chen, L.-C. Peng, Y.-H. Luo, J. Qin, D. Wu, et al. *Quantum computational advantage using photons. Science* **370**, 1460-1463 (2020).

[269] P. Ball. *Physicists in China challenge Google's 'quantum advantage'. Nature* **588**, 380–380 (2020). DOI: 10.1038/d41586-020-03434-7.

[270] C. M. Caves. *Quantum-mechanical noise in an interferometer. Physical Review D* **23**, 1693–1708 (1981). DOI: 10.1103/physrevd.23.1693.

[271] V. Giovannetti. *Quantum-Enhanced Measurements: Beating the Standard Quantum Limit. Science* **306**, 1330–1336 (2004). DOI: 10.1126/science.1104149.

[272] V. Giovannetti, S. Lloyd, and L. Maccone. *Quantum Metrology. Physical Review Letters* **96**, 010401 (2006). DOI: 10.1103/physrevlett.96.010401.

[273] L. Pezzé and A. Smerzi. *Entanglement, Nonlinear Dynamics, and the Heisenberg Limit. Physical Review Letters* **102**, 100401 (2009). DOI: 10.1103/physrevlett.102.100401.

[274] G. Tóth. *Multipartite entanglement and high-precision metrology. Physical Review A* **85**, 022322 (2012). DOI: 10.1103/physreva.85.022322.

[275] P. Hyllus, W. Laskowski, R. Krischek, C. Schwemmer, W. Wieczorek, H. Weinfurter, L. Pezzé, and A. Smerzi. *Fisher information and multiparticle entanglement. Physical Review A* **85**, 022321 (2012). DOI: 10.1103/physreva.85.022321.

[276] G. Tóth and I. Apellaniz. *Quantum metrology from a quantum information science perspective. Journal of Physics A: Mathematical and Theoretical* **47**, 424006 (2014). DOI: 10.1088/1751-8113/47/42/424006.

[277] T. Xie et al. *Beating the Standard Quantum Limit under Ambient Conditions with Solid-State Spins. arXiv e-prints* , arXiv:2101.12048v1 (2021).

[278] S. F. Huelga, C. Macchiavello, T. Pellizzari, A. K. Ekert, M. B. Plenio, and J. I. Cirac. *Improvement of Frequency Standards with Quantum Entanglement. Physical Review Letters* **79**, 3865–3868 (1997). DOI: 10.1103/physrevlett.79.3865.

[279] R. Demkowicz-Dobrzański, U. Dorner, B. J. Smith, J. S. Lundeen, W. Wasilewski, K. Banaszek, and I. A. Walmsley. *Quantum phase estimation with lossy interferometers. Physical Review A* **80**, 013825 (2009). DOI: 10.1103/physreva.80.013825.

[280] Y. Matsuzaki, S. C. Benjamin, and J. Fitzsimons. *Magnetic field sensing beyond the standard quantum limit under the effect of decoherence. Physical Review A* **84**, 012103 (2011). DOI: 10.1103/physreva.84.012103.

[281] R. Demkowicz-Dobrzański, J. Kołodyński, and M. Guţă. *The elusive Heisenberg limit in quantum-enhanced metrology. Nature Communications* **3**, 1063 (2012). DOI: 10.1038/ncomms2067.

[282] A. W. Chin, S. F. Huelga, and M. B. Plenio. *Quantum Metrology in Non-Markovian Environments. Physical Review Letters* **109**, 233601 (2012). DOI: 10.1103/physrevlett.109.233601.

[283] R. Demkowicz-Dobrzański, J. Czajkowski, and P. Sekatski. *Adaptive Quantum Metrology under General Markovian Noise. Physical Review X* **7**, 041009 (2017). DOI: 10.1103/physrevx.7.041009.

[284] S. Zhou, M. Zhang, J. Preskill, and L. Jiang. *Achieving the Heisenberg limit in quantum metrology using quantum error correction. Nature Communications* **9**, 78 (2018). DOI: 10.1038/s41467-017-02510-3.

[285] K. Chabuda, J. Dziarmaga, T. J. Osborne, and R. Demkowicz-Dobrzański. *Tensor-network approach for quantum metrology*

in many-body quantum systems. *Nature Communications* **11**, 250 (2020). DOI: 10.1038/s41467-019-13735-9.

[286] R. Demkowicz-Dobrzański, K. Banaszek, and R. Schnabel. *Fundamental quantum interferometry bound for the squeezed-light-enhanced gravitational wave detector GEO 600. Physical Review A* **88**, 041802(R) (2013). DOI: 10.1103/physreva.88.041802.

[287] A. Franzen, B. Hage, J. DiGuglielmo, J. Fiurášek, and R. Schnabel. *Experimental Demonstration of Continuous Variable Purification of Squeezed States. Physical Review Letters* **97**, 150505 (2006). DOI: 10.1103/physrevlett.97.150505.

[288] M. Parniak, S. Borówka, K. Boroszko, W. Wasilewski, K. Banaszek, and R. Demkowicz-Dobrzański. *Beating the Rayleigh Limit Using Two-Photon Interference. Physical Review Letters* **121**, 250503 (2018). DOI: 10.1103/physrevlett.121.250503.

[289] P. Hyllus, O. Gühne, and A. Smerzi. *Not all pure entangled states are useful for sub-shot-noise interferometry. Physical Review A* **82**. DOI: 10.1103/physreva.82.012337.

[290] G. Tóth, T. Vértesi, P. Horodecki, and R. Horodecki. *Activating Hidden Metrological Usefulness. Physical Review Letters* **125**, 020402 (2020). DOI: 10.1103/physrevlett.125.020402.

[291] C. H. Bennett, A. Grudka, M. Horodecki, P. Horodecki, and R. Horodecki. *Postulates for measures of genuine multipartite correlations. Physical Review A* **83**, 012312 (2011). DOI: 10.1103/physreva.83.012312.

[292] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters. *Quantum nonlocality without entanglement. Physical Review A* **59**, 1070–1091 (1999). DOI: 10.1103/physreva.59.1070.

[293] G. Smith and J. Yard. *Quantum Communication with Zero-Capacity Channels. Science* **321**, 1812–1815 (2008). DOI: 10.1126/science.1162242.

[294] D. P. DiVincenzo, M. Horodecki, D. W. Leung, J. A. Smolin, and B. M. Terhal. *Locking Classical Correlations in Quantum States. Physical Review Letters* **92**, 067902 (2004). DOI: 10.1103/physrevlett.92.067902.

[295] W. H. Zurek. *Quantum Darwinism. Nature Physics* **5**, 181–188 (2009). DOI: 10.1038/nphys1202.

[296] F. G. S. L. Brandão, M. Piani, and P. Horodecki. *Generic emergence of classical features in quantum Darwinism. Nature Communications* **6**, 7908 (2015). DOI: 10.1038/ncomms8908.

[297] T. P. Le and A. Olaya-Castro. *Strong Quantum Darwinism and Strong Independence are Equivalent to Spectrum Broadcast Structure. Physical Review Letters* **122**, 010403 (2019). DOI: 10.1103/physrevlett.122.010403.

[298] J. Korbicz, P. Horodecki, and R. Horodecki. *Objectivity in a Noisy Photonic Environment through Quantum State Information Broadcasting. Physical Review Letters* **112**, 120402 (2014). DOI: 10.1103/physrevlett.112.120402.

[299] R. Horodecki, J. K. Korbicz, and P. Horodecki. *Quantum origins of objectivity. Physical Review A* **91**, 032122 (2015). DOI: 10.1103/physreva.91.032122.

[300] M.-C. Chen, H.-S. Zhong, Y. Li, D. Wu, X.-L. Wang, L. Li, N.-L. Liu, C.-Y. Lu, et al. *Emergence of classical objectivity of quantum Darwinism in a photonic quantum simulator. Science Bulletin* **64**, 580–585 (2019). DOI: 10.1016/j.scib.2019.03.032.

[301] C. M. Scandolo, R. Salazar, J. K. Korbicz, and P. Horodecki. *The origin of objectivity in all fundamental causal theories. arXiv e-prints*, arXiv:1805.12126v6 (2020).

[302] R. Colbeck and R. Renner. *Free randomness can be amplified. Nature Physics* **8**, 450–453 (2012). DOI: 10.1038/nphys2300.

[303] R. Gallego, L. Masanes, G. D. L. Torre, C. Dhara, L. Aolita, and A. Acín. *Full randomness from arbitrarily deterministic events. Nature Communications* **4**, 2654 (2013). DOI: 10.1038/ncomms3654.

[304] F. G. S. L. Brandão, R. Ramanathan, A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, T. Szarek, and H. Wojewódka. *Realistic noise-tolerant randomness amplification using finite number of devices. Nature Communications* **7**, 11345 (2016). DOI: 10.1038/ncomms11345.

[305] P. Horodecki, Łukasz Rudnicki, and K. Życzkowski. *Five open problems in quantum information. arXiv e-prints*, arXiv:2002.03233v2 (2020).