Review

Photonic quantum information processing: a review

Fulvio Flamini, Nicolò Spagnolo and Fabio Sciarrino
Dipartimento di Fisica, Sapienza Università di Roma, Piazzale Aldo Moro 5, I-00185 Roma, Italy
E-mail: fabio.sciarrino@uniroma1.it

Abstract.
Photonic quantum technologies represent a promising platform for several applications, ranging from long-distance communications to the simulation of complex phenomena. Indeed, the advantages offered by single photons do make them the candidate of choice for carrying quantum information in a broad variety of areas with a versatile approach. Furthermore, recent technological advances are now enabling first concrete applications of photonic quantum information processing. The goal of this manuscript is to provide the reader with a comprehensive review of the state of the art in this active field, with a due balance between theoretical, experimental and technological results. When more convenient, we will present significant achievements in tables or in schematic figures, in order to convey a global perspective of the several horizons that fall under the name of photonic quantum information.
Introduction

Nearly thirty years ago, a short period in the history of modern physics, quantum algorithms were presented to the scientific community as ingenious strategies to realize tasks thought to be hard with classical approaches. Significant advances in this sense sprouted within only a few years from different areas of research in cryptography [1], algorithms [2], simulation [3] and communication [4], ever since placing a quantum- before the name of each field. This shift of paradigm required to think out of the box and to start considering quantum mechanics not only as a stage to investigate but, as much interestingly, as a resource for practical purposes.

Photons naturally fit this quantum revolution [5] as an effective system to process information: they propagate fast, do not interact with the environment and can be easily manipulated. Moreover, future advances will benefit from the technological infrastructures and know-how already developed in the classical context, thus further encouraging to proceed in this direction. While this aspect is particularly relevant for instance for quantum communication, where the availability of fiber networks can play a key role, milestone achievements have been reached also in the scope of information processing, raising a bridge between the linear-optical platform and information processing [6].

Encouraged by these considerations, we will review the state of the art in photonic quantum information to provide the reader with a broad perspective in a unified framework. This review article is structured in three chapters, where we attempt to present the numerous works in a convenient classification, even though most of them easily overlap. Chapter 1 focuses on the single-photon encoding schemes and on the technological state of the art for experimental implementations, namely single-photon sources, integrated circuits and single-photon detectors. Chapter 2 delves into the field of quantum communication, describing various theoretical schemes developed to this purpose, overviewing the developments of quantum repeaters and distributedblind quantum computing protocols for photonic quantum networks. This chapter also presents recent significant achievements in long-distance communication and quantum key distribution. Finally, Chapter 3 presents the latest achievements in photonic quantum simulation, discussing the potentialities of single- and multi-photon quantum walks for quantum computing and simulation in the domain of quantum chemistry. For the sake of clarity and completeness, we will also refer the interested reader to more specialized literature and review articles on each topic.

1. Implementing quantum information with single photons

Quantum information can be encoded in a variety of physical systems, ranging from photonic states, solid state devices, atomic or nuclear spin systems to electrons, Josephson junctions, superconducting devices (see Table 1). Photonic states present several advantages with respect to other platforms, due to the lack of interaction with the external environment that thus corresponds to long decoherence times. As we discuss in the next sections, this feature is particularly relevant in applications such as long-distance quantum communications. In this section we will review the encoding of quantum information in single photons with a focus on discrete-variable approach in the visible domain. For an overview of quantum information processing in the microwave regime, the interested reader can refer to Refs. [7–9] for specialized, comprehensive reviews on the field, while for continuous-variable quantum information we refer the reader to Ref. [10]. Section 1.1 reviews the main degrees of freedom employed to encode qubits or qudits in this physical platform, while Section 1.2 summarizes the main recently-developed technological platforms to generate, manipulate and detect single-photon states.

1.1. Single-photon encoding

Photon-based quantum information uses the degrees of freedom of light (see Fig. 1), suitable quantities related to propagation directions (path encoding), to momentum (polarization encoding), to light spatial distribution (orbital angular momentum encoding) and to time (time-bin and time-frequency encoding). All encoding strategies present their own advantages and weaknesses, and can be combined in a hybrid configuration. In this section we will review each of them focusing on discrete-variable systems, briefly recalling their operation with examples from the latest literature.

1.1.1. Encoding in angular momentum – The angular momentum of light concerns the rotation of the electromagnetic field vector, a dynamic quantity that influences light-matter interaction. Two forms of angular momentum exist: spin angular momentum (SAM), associated to its circular polarization, and orbital angular momentum (OAM), associated to the spatial structure of the wavefront. While the two mechanisms cannot be separated in the general case of focused or divergent light beams, their nature becomes manifest for sufficiently collimated ones [11]. In the latter case, the total angular momentum \( \mathbf{J} \) takes the
simpler form

\[ J \propto \int d^3 r \left( |E_L|^2 - |E_R|^2 \right) - \sum_{j=x,y,z} \left( \iota E_j \frac{\partial E_j}{\partial \phi} \right) \]  

(1)

where the first term, the SAM contribution, corresponds to the familiar left (L) and right (R) circular polarizations while the second, associated to the OAM, describes wavefronts with the typical helical profiles and is thus related to light spatial distribution. The paraxial approximation is the natural framework for light manipulation and encoding [12], thus in the following sections we will focus on this regime. For specialized reviews, we refer the reader to Refs. [13, 14].

**Polarization.** Polarization qubits represent a common and practical way to encode quantum information for most applications, thanks to the ease of generation (see Section 1.2.1) and to the availability of effective tools for manipulation. Indeed, in the limit of paraxial waves of Eq.(1), the SAM component interacts with anisotropic transparent systems such as birefringent crystals, which are consequently widely employed for polarization manipulation.

A qubit encoded in polarization is usually written as |ψ⟩ = α |H⟩ + β |V⟩, where H and V stand for horizontal and vertical polarization, respectively, and

\[ |p⟩ = \int_{-\infty}^{q} dk f(k) e^{-\iota w_k t} \hat{a}^\dagger(k,p) |0⟩ \]  

(2)

where \( p = (H,V) \), \( f(.) \) is a wave packet mode function and \( \hat{a}^\dagger(k,p) \) is the creation operator for a photon with momentum \( k \) and polarization \( p \) [12]. Polarization qubits can be as well expressed in the diagonal basis \(|±⟩ = \frac{1}{\sqrt{2}} (|H⟩ ± |V⟩) \) or with left and right circular polarizations as \(|\uparrow/R⟩ = \frac{1}{\sqrt{2}} (|H⟩ ± i|V⟩) \). Together, the three pairs of states form a set of mutually unbiased bases encoded in polarization [15], at the core of several applications that we will overview in the following sections.

Polarization encoding has always played an important role in a significant number of investigations in quantum information, ranging from quantum simulation [16, 17] to quantum computation [18–22] and communication [23, 24]. Its ubiquitous presence in quantum information processing has been further enhanced by the numerous advances in entanglement generation, manipulation and distribution [25–34] and to the development of suitable theoretical and experimental frameworks for its manipulation in integrated devices [35–37]. Moreover, polarization qubits are increasingly coupled to other degrees of freedom of single photons, such as orbital angular momentum [33, 34, 38, 39], path [18, 19, 22, 25, 40, 41], time-energy [42, 43] and all together [44] in so-called hyper-entangled states [45], efficient resources for quantum computation, communication and work extraction protocols.

**Orbital angular momentum.** The OAM component, related to the spatial distribution of the electromagnetic field, can be in turn divided in two terms: one internal, origin-independent and associated to twisted wavefronts, and one external, given by \( L_e = r × P \) and thus origin-dependent. Quantum information processing based on OAM refers to the first component. The OAM carried by such optical vortices is described by the phase term \( e^{-\iota q \theta} \), where \( \theta \) is the angular coordinate and \( q \) is an unbounded integer. For eigenstates of the orbital angular momentum we have \( q = Q = \frac{1}{2\pi} \int dξ \),

---

**Table 1.** Physical systems for encoding a qubit. Some degrees of freedom also allow for the implementation of qudits. The choice for the most suitable system for implementing a qubit depends on the task: quantum computation, communication or simulation. In this review we will focus on discrete-variable photonic implementations.

| System | Quantity | Encoding |
|--------|----------|----------|
| Single photon | Polarization | Horizontal / Vertical |
| | Orbital angular momentum | Left / Right |
| | Number | 0/1 photons |
| | Time | Early / Late |
| Continuous-variable fields | Quadratures | Amplitude-/Phase- squeezing |
| | Charge | 0/1 Cooper pair |
| | Current | Clock-/Counter- clockwise |
| | Energy | Ground/Excited state |
| Quantum dot, Optical lattice, Nuclear spin | Spin | ↑ / ↓ |
| Electrons | Charge | 0/1 electrons |
| | Spin | ↑ / ↓ |
| Non-abelian anyons | Topology | Braiding |

---
An important aspect for OAM encoding is to develop practical and reliable techniques to analyze it. While, in fact, polarization encoding requires to resolve only two components, which can be done easily by means of waveplates and polarizing beam splitters, the number of OAM modes is potentially unbounded and as such challenging to characterize [68]. Several methods exist so far (see Ref. [63] and references therein): the above-mentioned spiral phase plates [47, 48], holograms and spatial light modulators [51–54] and q-plates [46, 51, 54, 59–64, 66], as well as diffractions through apertures, interference with uniform plane waves, Dove prism interferometers, rotational Doppler frequency shifts and spatial sorting of helical modes [33, 59]. In this direction, a spectrum analyzer is a device capable to measure the instantaneous power and phase distributions of OAM components [48, 52, 69–74]. Once generated and analyzed, OAM states can be manipulated with high degree of control to encode quantum information in the infinite OAM Hilbert space spanned by $l \in Z$, i.e. in the qudits $\psi = \sum_{l} \alpha_{l} |l\rangle$ [34, 62, 64, 66, 75–80].

OAM states represent a fundamental resource for several applications in quantum information. At a fundamental level, OAM has enabled research on optimal quantum cloning of OAM-encoded qubits [66, 81] and photonic quantum walks in the orbital angular momentum states, with theoretical analyses [82, 83] and experimental demonstrations [51, 54, 60]. Additional features include the capability of performing a coined quantum walk in the OAM space, providing a viable alternative to other bulk or integrated implementations (see Section 3.1). Long-distance quantum communication (see Section 2.2) benefits from the availability of photonic information carriers able to distribute multiple superposition states in OAM entangled [33, 67, 78, 84–93] or hyperentangled [34, 39, 49, 61, 64, 67, 94, 95] states. Moreover, photonic 'flying' qubits encoded in OAM can be prepared in alignment-free states [67, 95], being insensitive to rotation of the reference frame. These features have unlocked a number of advancements in free-space quantum key distribution and quantum communication [67, 81, 86, 96–103] with high bit exchange rates [104, 105]. Related to the capability of producing alignment-free states, hybrid encoding

\begin{equation}
\begin{aligned}
Q \begin{bmatrix} L/\hbar \end{bmatrix} |l\rangle = & \begin{bmatrix} L/\hbar \end{bmatrix} |l \pm 2q\rangle, \quad \text{i.e. it flips the qubit polarization in the circular basis and shifts the OAM of a quantity } \Delta l = \pm 2q. \quad \text{Here, } q \text{ is related to the topological charge of the } \text{QP, which in turn depends on its internal pattern. Applications offered by the QP } [39, 49, 64, 65, 67] \text{ include the generation of intra-photon entanglement between polarization and OAM degrees of freedom by producing states of the form}
\end{aligned}
\end{equation}
between polarization and OAM can be exploited to enhance the sensitivity to angular rotations [65, 106]. The confidence in its potential has led to several investigations to support OAM-based photonic quantum networks for delivering information, from sorting [59, 79, 99, 100, 107] and routing OAM states [90, 108, 109] to implementing quantum repeaters with teleportation [85, 110, 111] and quantum memories [90, 108, 109]. First results towards integration of OAM devices have also been reported [114]. The feasibility of this approach for free-space communication has been further supported by a number of theoretical [93, 115–118] and experimental [84, 87, 95] investigations in non-optimal conditions, addressing the issue of beam propagation in a turbulent atmosphere.

1.1.2. Encoding in propagation direction – Path encoding, or encoding in the optical modes in the case of single photons, is the representation of qubits in terms of occupied spatial modes. Path-encoded qubits, as well as qudits [119], are perfectly fit for photonic integrated circuits, since waveguide arrays inherently implement a spatial separation and coupling between modes is easily accomplished with directional couplers. Moreover, the high stability and interferometric complexity offered by integrated circuits are useful features for most applications in quantum technologies [22, 120, 121]. Indeed, accurate control over these qubits for universal manipulation is possible with relatively low technological requirements when compared to other encoding schemes [37, 122]. Conversely, an integrated manipulation of polarization qubits requires ad-hoc designs that represent additional challenges, as demonstrated for instance by the fabrication of rotated waveplates in integrated femtosecond laser-written circuits [20, 123]. To this aim, several experimental demonstrations have been shown for tunable all-optical path-entanglement generation via parametric down-conversion in integrated non-linear waveguides [124–127], mostly on SoI and LiNbO$_3$ [128]. Fiber integrated sources have also been reported for the generation of high-dimensional path-encoded qubits, as interface or preliminary step towards the integration in a circuit [129]. Finally, control over non-ideal implementation has been strengthened with investigations on the effect of losses over path-entanglement [130] and on state tomographies on tunable integrated circuits [121].

1.1.3. Encoding in time – Using time as degree of freedom offers various advantages over other encoding schemes. We present an overview of the approach and of its latest achievements, with a distinction between time-bin and time-energy encodings.

Time-bin encoding. Time is a natural and effective resource to write information on single-photon quantum states. The mechanism to encode information involves a Mach-Zehnder interferometer with one arm longer than the other. The amplitude associated to an incoming photon is split at the first beam splitter of the Mach-Zehnder and passes through the unbalanced arms: we denote with $|l\rangle$ the state of a photon that has taken the long path, while $|s\rangle$ represents a photon that has taken the short one. This path difference must be stable, i.e. any fluctuation in the temporal delay must be smaller than one wavelength, and longer than the coherence length of each photon to allow a reliable discrimination of the arrival times. A proper dynamic control of the temporal delay is thus desirable to compensate for mechanic and thermal instabilities. A qubit encoded in the photon arrival time can then be written in the superposition $|\Psi\rangle = \frac{1}{\sqrt{2}} (|l\rangle + |s\rangle)$, where the states $|p\rangle$ are given by

$$|p\rangle = \int_{-\infty}^{\infty} dz f\left( t - \frac{z}{c} + p\tau \right) e^{-i\omega(t - \frac{z}{c} + p\tau)} \hat{a}^\dagger |0\rangle \quad (4)$$

being $p = (l, s)$, $f(\cdot)$ a wave packet mode function, $\omega$ a fixed angular frequency and $\tau$ the time delay experienced between the two arms of length $L$.

Time-bin encoding presents some advantages with respect to the previous schemes. First, it is suitable for integrated photonic devices, where photons can be generated, manipulated and measured without the need for external encoding devices. Moreover, its resilience to noise acting on polarization, such as depolarizing media or decoherence and mode dispersion, makes time-bin a good candidate for applications in state teleportation [131–133], quantum communication and quantum key distribution, both free-space and in-fiber [134–137]. In this direction, several experiments have been carried out for tests of non-locality [135, 138–140]. Entangled photon pairs have been reported with femtosecond pulses [139], including deterministic and narrowband atom-cavity sources [141], sources integrated on type-II periodically poled lithium niobate [142] and silicon wire [143] waveguides or micro-ring resonators [144]. Time-bin manipulation on chip [145], storage [137] and measurement [138] have been reported to provide the necessary components for linear-optical quantum networks. Besides quantum communication, time-bin encoding has been proposed as a suitable scheme also for quantum walks [146–148] and for photonic BOSON SAMPLING [149, 150] (see Section 3.2).

Time-frequency/energy encoding. Starting from time-bin encoding, where the allowed states are ‘early’ and ‘late’, an extension of this scheme to multiple states consists in correlating the arrival time with single-photon’s energy [43, 151, 152]. Relevant applications
can be found in quantum communication and quantum key distribution to take advantage of the low decoherence with qubits delivery [43, 151–156]. Notwithstanding, frequency-encoded experimental demonstrations have been reported also in the context of quantum computation [157–163] often operating with cluster states. Extensions to more than two photons have also been reported [164], representing a proof-of-principle investigation for multi-photon Franson interferometry and for engineering discrete- and continuous-variable hyperentangled states. We conclude this paragraph mentioning theoretical and experimental investigations to manipulate photonic qubits encoded in time [138, 163, 165] and time-frequency [153, 166–171].

1.2. Photonic technologies

In this section we will overview the main technological components for photonic quantum information processing. Three main stages can be identified, as shown schematically in Fig. 2. First, a crucial requirement is the capability of efficiently generating single-photon states (Sec.1.2.1), requiring indistinguishability of correlated states and good control over the degrees of freedom. Then, suitable platforms should be capable of manipulating single- or multi-photon states to perform unitary transformations (Sec.1.2.2). Finally, photons should be efficiently measured with appropriate detection systems (Sec.1.2.3).

1.2.1. Single-photon sources – Ideally, a good single-photon source should emit only one photon at a time, on demand, at high generation rates and in well-defined states in spatial, temporal and spectral modes. Moreover, different sources should be capable to generate identical photons and their implementation should allow for integration in miniaturized platforms. In parallel, it is crucial to generate correlated states of more than one photon, being entanglement a key resource in several quantum information protocols (see Section 2.1.1). Current sources can fulfill only a limited number of the above requirements, while keeping very high performances for specific applications.

Several approaches for single-photon sources have been developed in the last decades (see Table 2) [172–175, 177–214]. Among probabilistic sources we mention (a) parametric down-conversion (PDC) in bulk crystals [204], semiconductors [166, 215], microresonators [183, 185] and optical waveguides [32, 172–175, 177–182, 209, 210, 212–214] and (b) four-wave mixing (FWM) in optical waveguides [184, 189, 211], few-mode fibers [186] and microdisks [187]. Deterministic sources include trapped ions [205], colour centers [203] and quantum dots (QD) [216] with GaAs [217], InGaAs [29, 191–193, 199], InAsP NW [201, 202] or InAs/GaAs [195–198].

| Process | Ref. | Platform | $\lambda$ (nm) |
|---------|------|----------|----------------|
| PDC     | [172] | PPKTP    | 795+795        |
|         | [173] | PPKTP    | 810+810        |
|         | [174] | PPKTP    | 1570+1570      |
|         | [175] | PPKTP    | 800+1590       |
|         | [176] | PPKTP    | 1550+1550      |
|         | [177] | PPLN     | 1310+1560      |
|         | [178] | PPLN     | 1551+1611+1625 |
|         | [179] | PPLN     | 1560+1560      |
|         | [180] | PPLN     | 1560+1560      |
|         | [181] | PPLN     | 1551+1571      |
|         | [182] | AlGaAs   | 1566+1566      |
|         | [183] | AIN $\mu R$ | 1550+1550     |
| FWM     | [184] | AlGaAs   | 1553+1577      |
|         | [185] | Si$_3$N$_4$ $\mu R$ | 1550+1550   |
|         | [186] | Few-mode fiber | 620+777       |
|         | [187] | Silicon microdisk | 1497+1534   |
|         | [188] | LF-HC-PCF | 1552+1552      |
|         | [189] | Silica FLWw | 830+1130      |
| QD exciton | [190] | InGaAs | 1550          |
|         | [191] | InGaAs | 945           |
|         | [192] | InGaAs | 890           |
|         | [193] | InGaAs | 932           |
|         | [194] | InGaAs | 907           |
|         | [195] | InAs/GaAs | 925         |
|         | [196] | InAs/GaAs | 933         |
|         | [197] | InAs/GaAs | 897         |
|         | [198] | InAs/GaAs | 1130        |
| QD biexciton | [199] | InGaAs | 905+905      |
|         | [200] | GaAs    | 786+786       |
|         | [201] | InAsP   | 930+930       |
| QD triexciton | [202] | InAsP | 894+940       |
| Fluorescence | [203] | Si-V center | ~750      |

PDC: spontaneous parametric down-conversion; FWM: four-wave mixing; FLWw: femtosecond laser written waveguide; QD: quantum dot. PPLN: periodically poled lithium niobate. PPKTP: periodically poled potassium titanyl phosphate. InAs: indium arsenide; GaAs: gallium arsenide; InGaAs: indium gallium arsenide; InAsP: indium arsenic phosphide; AlGaAs: aluminium gallium arsenide; AIN: aluminium nitride; Si–V: silicon-vacancy in diamond; LF-HC-PCF: liquid-filled hollow-core photonic crystal-fiber. $\mu R$: microresonator.

1.2.2. Integrated quantum circuits – Traditional optical instruments consisted of bulk optical components, unavoidably large and impractical, more susceptible to problems of stability, scalability and adaptability to different applications. Just like the evolution undergone by the electronic components, the last decade has seen a strong effort for an optical miniaturization in dielectric materials [232, 233]. Integrated optical circuits are built upon architectures of directional couplers, with additional geometries to account for deformation-induced phase shifts. Furthermore, recent developments have shown the capability to introduce active reconfigurable elements, thus allowing the fabrication
Table 3. Integrated circuits for quantum information processing.

| Year | Ref. | Technology | Photons | Modes | $\lambda$ (nm) | Tunable $\phi$ | Application |
|------|------|------------|---------|--------|----------------|----------------|-------------|
| 2008 | [218]| SoS        | 2       | 6      | 804           | n.r.           | CNOT        |
| 2009 | [219]| SoS        | 4       | 12     | 790           | n.r.           | Shor’s factoring algorithm |
|      | [220]| UVW, SoS   | 2       | 2      | 830           | 1              | First reconfigurable UVW circuit |
|      | [120]| SoS        | 4       | 2      | 780           | 1              | First reconfigurable SoS circuit |
| 2010 | [221]| SoS        | 2       | 6      | 804           | n.r.           | CNOT        |
|      | [27] | FLW        | 2       | 2      | 806           | n.r.           | Polarization insensitive BS |
| 2011 | [222]| FLW        | 2       | 4      | 806           | n.r.           | CNOT with partially polarizing BS |
| 2012 | [121]| SoS        | 2       | 6      | 808           | 8              | State generation/detection, Bell test |
|      | [27] | Ti:LN      | 2       | 2      | 1550          | 1              | First reconfigurable Ti:LN circuit |
|      | [37] | FLW        | 2       | 2      | 830           | 1              | Strain-optic active control |
|      | [223]| SoI        | 2       | 2      | 1550          | 1              | First reconfigurable SoI circuit |
| 2014 | [20] | FLW        | 1       | 2      | 815           | n.r.           | Integrated waveplates |
|      | [123]| FLW        | 2       | 6      | 800           | n.r.           | Integrated waveplates |
|      | [124]| SoI        | 2       | 2      | 1550          | 1              | On-chip interference of two sources |
|      | [125]| LN         | 2       | 4      | 1560          | 1              | On-chip interference of two sources |
|      | [224]| FLW        | 2       | 2      | 830           | 1              | Strain-optic active control |
|      | [225]| UVW, SoS   | 3       | 6      | 830           | 1              | Teleportation |
| 2015 | [226]| SoS        | 2       | 6      | n.a.          | 8              | Variational eigenvalue solver |
|      | [227]| FLW        | 2       | 2      | 1550          | 1              | First reconfigurable FLW circuit |
|      | [122]| SoS        | 3       | 6      | 808           | 30             | H, CNOT, $\sigma, R(\alpha)$ |
|      | [145]| Si$_3$N$_4$| 2       | 5      | 1550          | 15             | Time-bin entanglement |
| 2016 | [24] | Si         | 3       | 4+2    | 1550          | 4$^{(a,b)}$    | BB84 protocol |
|      | [25] | SoI        | 2       | 4+2    | 1550          | 5              | Entanglement distribution |
|      | [228]| SiN        | 2       | 6      | 1550          | n.r.           | CNOT        |
|      | [229]| SoI        | 3       | 5      | 1550          | 5$^{(c)}$      | QKD protocol |
| 2017 | [230]| SoI        | 3       | 5+10   | 1550          | 8+10$^{(d)}$   | QKD protocol |
|      | [231]| SoI        | 2       | 1570   | 176           | Quantum transport |

SoS: silica on silicon; SoI: silica on insulator; FLW: femtosecond laser written; UVW: UV written; BS: beam splitter; Ti:LN: titanium indiffusion lithium niobate; SiN: Silicon nitride.

Modulation in (a) polarization, (b) intensity, (c) pulse. (d): two integrated circuits. n.r.: non-reconfigurable; n.a.: not available.

of multi-purpose devices [122, 227, 231]. One widely adopted material for the integration remains fused silica thanks to its numerous benefits: low propagation losses, low birefringence, operation from visible to infrared, good coupling efficiency with single mode fibers and low temperature dependence. Notwithstanding, and differently from miniaturized electronic circuits, linear optical circuits do not have unique platform and manufacturing technique (see Table 3) [234]:

Silica-on-Silicon (SoS). A crystal silicon substrate is covered by a layer of silica (SiO$_2$), wherein waveguides are etched with rectangular cross sections. A second layer of undoped silica is then laid on top of the structure to enclose the doped silica core and protect the waveguides [218]. Limitations of the SoS technique are the need for a mask and the restriction to one polarization, due to the birefringence induced by the rectangular cross-sections.

Silica-on-Insulator (SoI). Si-based platforms, including silicon (Si), silicon nitride (SiN) and silicon carbide (SiC), are advanced platforms whose development benefits from the know-how given by electronics technologies [235]. Si-based devices present a very high refractive index that allows for reduced-size circuits and that is suitable for nonlinear processes. Limitations are the low mode-matching with optical fibers and the relatively high propagation losses. Slightly more favorable conditions can be met with devices based on III-V compound semiconductors, which include indium phosphide [236], gallium arsenide [237] and gallium nitride [238].

UV writing. Waveguides are inscribed by focusing a strong laser pulse in a photosensitive B- and Ge-doped silica layer, placed within two layers of undoped silica and on top of a third translating silicon layer [225, 239, 240]. This technique does not require the adoption of masks, thus reducing the complexity of fabrication, and allows for arbitrary 3D geometries.

Femtosecond laser writing (FLW). The mechanism underlying the process is the non-linear absorption of strong pulses tightly focused in a glass substrate, which causes a permanent and localized modification in the refractive index. Waveguides are drawn by translating the sample at constant speed in 3D geometries [241,
The possibility of writing circular cross-sections and the low birefringence of silica allow for waveguides with low dependence on polarization [16, 36, 123].

On the above platforms, photonic circuits can be implemented [243, 244] according to linear-optical interferometric schemes capable to perform arbitrary unitary evolutions [245, 246], or designs optimized for Fourier and Hadamard transformations [241, 244].

2. Quantum communication

2.1. Protocols for quantum communication

Ever since the intuition of Bennett and Brassard with the famous BB84 protocol [1], it is known that quantum information allows one to devise algorithms to achieve classically unparalleled results in information transfer. Quantum infrastructures for managing information and delivering entanglement are now believed to join current technologies in a number of relevant tasks. Photons are by far the most suitable physical system to implement flying qubits to deliver information: they experience negligible decoherence through free space or optical fibers, they allow a high spatial control, and the technology for linear-optical devices to manipulate qubits is accessible and at an advanced stage [316, 317].

Dense coding. Quantum mechanics allows to increase the capacity of a quantum communication channel by transferring two bits of classical information with only one qubit [322]. Suppose Alice and Bob share an entangled photon pair, each keeping one photon. Alice can encode two bits on her photon by choosing and applying on her photon one between four unitary transformations: the identity operation $I$ (00), a bit flip $\sigma_x$ (01), a phase flip $\sigma_z$ (10) or both a bit flip and a phase flip $\sigma_y$ (11). Alice sends her particle to Bob, who measures both particles in the Bell basis. The outcome of the Bell measurement (BM) will then correspond to the two bits of information sent by Alice.

One challenge for implementing dense coding is represented by the BM stage, since achieving a never-failing BM is impossible using only linear-optical elements such as beam splitters, phase shifters, detectors and ancillary particles [323]. A solution to this issue consists in exploiting hyperentangled photons [44], leading to complete BM demonstrations in orbital angular momentum/polarization [324], momentum/polarization [325] and time/polarization [326, 327]. The latter schemes have the additional
Figure 2. Technologies for photonic quantum information processing. Three main stages can be identified. (i) Generation of photonic states, either indistinguishable single photons or entangled states. (ii) Manipulation, where integrated platforms enable apparatuses of increasing complexity. (iii) Measurement of photonic states, where detectors either with photon number resolution or without are currently under development. Legend - PDC: parametric down-conversion, FWM: four-wave mixing, FLW: femtosecond laser writing, SPAD: single-photon avalanche photodiode, TES: transition edge sensor.

Table 4. Worldwide in-fiber photonic quantum networks (not exhaustive list).

| Network                        | Ref.   | Launch | Location | Nodes | Distance (km) |
|-------------------------------|--------|--------|----------|-------|---------------|
| DARPA                         | [308]  | 2003   | USA      | 10    | 29            |
| SECOQC                        | [309]  | 2003   | Austria  | 6     | 200           |
| SwissQuantum                  | [310]  | 2009   | Switzerland | 3  | 35            |
| Hierarchical Quantum Network  | [311,312] | 2009 | China    | 32    | 2000          |
| Tokyo QKD Network             | [313,314] | 2010 | Japan    | 5     | 45            |
| Los Alamos National Lab       | [315]  | 2011   | USA      | n.a.  | 50            |

DARPA: Defense Advanced Research Projects Agency; SECOQC: SEcure COmmunication based on Quantum Cryptography.

advantage of being feasible to prepare and of enabling an efficient transmission through optical fibers. So far, the maximum channel capacity \((1.665 \pm 0.018)\) has been reported in Ref. [327], beating the limit of \(\log_2 3 \sim 1.585\) bits obtainable by means of only linear optics and entanglement, due to the impossibility of perfectly discriminating all four Bell states in this case.

Entanglement purification. One requirement is the capability of delivering entanglement without having it spoilt between distant nodes of a network, as it happens with a probability increasing exponentially in the length of a noisy transmission. Entanglement purification allows to circumvent this issue by extracting high-quality entangled pairs from a given ensemble using only local transformations and classical communication [328]. More specifically [319], suppose Alice and Bob share two copies of the mixed state

\[
\rho_{A,B} = F \ket{\phi^1}_{A,B} \bra{\phi^1} + (1 - F) \ket{\psi^1}_{A,B} \bra{\psi^1},
\]

with \(\ket{\psi^1} \propto |0,1\rangle + |1,0\rangle\) and \(\ket{\phi^1} \propto |0,0\rangle + |1,1\rangle\), and they want to purify it so as to increase the probability of having a maximally-entangled state \(\ket{\phi^1}\). The original approach was based on CNOT operations [328]; few years later a simpler solution was introduced [329] and verified experimentally [330] based on only polarizing beam splitters. While the probability of success is 50% lower than the one with CNOT gates, the quality of these optical elements allow for a purification with much higher precision and control. Via a proper combination of projective measurements in polarization, it is possible to increase the amplitude associated to the maximally-entangled pair \(\ket{\phi^1}\), which can be used to quantify the fidelity of the transmission,
as $\mathcal{F} \rightarrow \mathcal{F}^2 / (\mathcal{F}^2 + (1 - \mathcal{F})^2)$ when $\mathcal{F} > \frac{1}{2}$.

Entanglement purification is a key ingredient also in quantum computation, such as for quantum error-correction protocols, in quantum cryptography and quantum teleportation. For a more complete overview of the state of the art we refer to Refs. [319, 331–334].

Quantum state teleportation. Ever since its introduction [4], quantum state teleportation (QST) has been one of the most notable examples of quantum communication. In terms of classical communication, QST enables the transfer of one qubit by sending two bits of classical information, i.e. a reversed dense coding. The mechanism works as follows: suppose Alice and Bob share an entangled photon pair $|\psi^-\rangle_{A,B} = \frac{1}{\sqrt{2}} (|0,1\rangle_{A,B} - |1,0\rangle_{A,B})$ and Alice wants to teleport to Bob the -unknown- qubit $|\psi\rangle_T = \frac{1}{\sqrt{2}} (|\alpha\rangle_T + |\beta\rangle_T)$. The complete system of three photons has the form

$$|\psi\rangle_T \otimes |\psi^-\rangle_{A,B} = -\frac{1}{2} |\psi^-\rangle_{T,A} (|\alpha\rangle_B + |\beta\rangle_B) \quad (6)$$

$$-\frac{1}{2} |\psi^+\rangle_{T,A} (|\alpha\rangle_B - |\beta\rangle_B) \quad (7)$$

$$+ \frac{1}{2} |\phi^-\rangle_{T,A} (|\alpha\rangle_B + |\beta\rangle_B) \quad (8)$$

$$+ \frac{1}{2} |\phi^+\rangle_{T,A} (|\alpha\rangle_B - |\beta\rangle_B). \quad (9)$$

Alice can then perform a joint Bell measurement on her two photons $A$ (entangled with Bob’s) and $T$, associate two bits to the Bell state found out of the four and send them to Bob via a classical channel. At this point, Bob can simply perform one of four transformations (identity operation for (6), phase flip $\sigma_z$ for (7), bit flip $\sigma_x$ for (8) or both bit flip and phase flip $\sigma_y$ for (9)) on his entangled photon $B$ to shape it as the one -unknown- possessed by Alice.

The original work by Bennett et al. [4] has rapidly triggered a large number of investigations [316] for a broad range of applications [335]. Among all, teleportation schemes were shown to enable new approaches for universal quantum computation [336, 337], in particular as one-way quantum computers [338]. From the experimental perspective, numerous achievements have been reported on photonic platforms proving the feasibility of the scheme already with state-of-the-art technology. After the first demonstrations in 1997-1998 [339, 340], one further proof appeared with the unconditional teleportation of optical coherent states with squeezed-state entanglement [341]. Later on, in 2001 Kim et al. reported an experimental teleportation where all four states were distinguished in the Bell-state measurement [23], while Jennewein et al. provided a proof of the nonlocality of the process and of entanglement swapping [342]. One year later, in 2002 Pan et al. were performing four-photon experiments for high-fidelity teleportation [343] and Lombardi et al. teleported qubits encoded in vacuum–one-photon states [344]. The beginning of the new century saw a true race towards more complex implementations. In 2004, for instance, a single-mode discrete teleportation scheme using a quantum dot single-photon source has been demonstrated [359]. At the same time, increasing the teleportation distances [346] became an interesting benchmark to assess the feasibility of practical implementations for future quantum networks [131–133, 347–350]. Today the current record for the longest distance is kept by Ren et al. who teleported single-photon qubits from a ground observatory to a satellite 1400 km high in atmosphere [351]. Next to the discrete-variable schemes of the first demonstrations, teleportation was also reported on squeezed entangled states [352–358], for which a review is available [359]. Indeed, the main reasons behind the increasing interest toward continuous-variable schemes concern practical advantages, since Bell measurements can be realized by means of only passive linear-optical elements and homodyne detection with very high precision. To bridge the gap between discrete and continuous variables, a hybrid approach has been recently proposed and tested [360]. Finally, interesting achievements on photonic teleportation have been demonstrated with the first implementation on integrated circuits [225], which may turn useful for future realizations of quantum network nodes, as well as schemes with simultaneous teleportation of multiple degrees of freedom [110] and teleportation of qudits [85], as opposed to the conventional two-level discrete approach.

In the above realizations, where photons encode information through all the stages of the protocol, the state of the qubit was transferred from one photon to another. Though the sources of single photons and photon pairs are still spatially close, the process is indeed the core of future long-distance quantum communication as we envisage it today (see Section 2.2) [320, 361]. One further requirement for a reliable and practical quantum communication is the capability of storing information for subsequent uses. The past decade has seen a strong effort directed towards the development of matter-light interfaces as building blocks for quantum computation and communication, where entanglement between single-photon states and atomic ensembles represents an effective solution. In nearly ten years several works have been carried out in this context [362]. Single-photon qubits have been teleported on atomic ensembles [363, 364] such as Caesium atoms [365] or $^{87}$Rb atoms [366–368], on a pair of trapped calcium ions [369] or diamond [370]. In this sense, single photons can also turn effective as mediators between distant matter qubits, as already
reported with single trapped ytterbium ions [371], quantum dots [372], rare-earth-ion doped crystals [113] or diamond spin qubits [373].

Entanglement swapping. In order to increase the distance between nodes of a quantum network without decreasing the quality of the transmission, i.e. the degree of entanglement distributed, it is necessary to develop techniques to protect or restore the state of the encoding photon. Entanglement swapping is a promising solution to this issue [374] and, nowadays, entanglement distribution includes it as a fundamental routine in quantum repeaters (see Section 2.2.1) [319]. Entanglement swapping is actually very similar to teleportation, the only difference being that the particle to be teleported is part of a second entangled pair. Schematically, given two pairs of entangled particles \( A-B \) and \( C-D \) shared by Alice and Bob, for instance in the Bell state \( |\psi^-\rangle \), the goal is to convert the whole system to a new entangled pair \( A-D \) by performing a Bell measurement on \( B \) and \( C \):

\[
|\psi^\pm\rangle_{A,B} \rightarrow |\psi^\pm\rangle_{C,D} \propto |\psi^\pm\rangle_{A,D} |\psi^\pm\rangle_{B,C} + |\psi^\mp\rangle_{A,D} |\phi^\pm\rangle_{B,C} + |\phi^\mp\rangle_{A,D} |\phi^\pm\rangle_{B,C}
\]

After the Bell measurement on \( B-C \), and whatever outcome Alice receives, Bob remains with an entangled pair \( A-D \) even though they did not share any entanglement or interaction. Similarly to teleportation, photons offer a convenient solution for an implementation of the scheme.

First demonstrations of entanglement swapping go back to 1998 by Pan et al. [375], to 2001 by Jennewein et al. and to 2002 by Sciarrino et al., all based on parametric down-conversion sources. Subsequent experiments still employed probabilistic single-photon sources at near-infrared and telecom wavelengths, the telecommunication windows for optical fibers, in bulk or waveguide as in Ref. [376] and references therein. Entanglement swapping has also been tested with discrete [377,378] and continuous variables [354], or even with a hybrid approach [379]. Future implementations of quantum repeaters in optical networks will require active synchronization of the single-photon sources involved in the exchange of information between the various nodes. To this aim, proof-of-principle demonstrations of this scheme have been reported in the last decade, where two synchronized independent sources generated entangled photon pairs for entanglement swapping and non-locality tests [319].

2.1.2. Decoherence-free communication – So far, we have described how entanglement purification, entanglement swapping, dense coding and teleportation allow for the distribution of entanglement, the essential resource for quantum communication, between in-principle arbitrarily distant locations. However, non-ideal operating conditions may hinder or completely prevent their concrete implementation. Two methods can be adopted to circumvent the issue of noisy channels: to increase the resilience of a protocol to losses and noise [380–382] (two-way classical communications), or to decrease their influence by encoding information in immune states (decoherence-free subspaces, DFS), for both quantum computation [383] and quantum communication tasks [384]. In the following we provide simple examples of DFS schemes, while further on we will overview some of the most recent experimental demonstrations.

In DFS protocols, qubits are encoded in states that do not experience decoherence in a given channel thanks to known symmetries of the subspace. As an example [319], let us consider two qubits evolving through a unitary transformation \( U(t) \) such that \( U(t) |0\rangle = e^{-i\omega t} |0\rangle \) and \( U(t) |1\rangle = e^{-i\omega t} |0\rangle \). We can see that \( |\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \) is an invariant of \( U(t) \) since \( U(t) |\psi^+\rangle = e^{-i(\omega_1 + \omega_2)t} |\psi^+\rangle \), which is equivalent to \( |\psi^+\rangle \) up to a global phase. A second example is given by the unitary transformation

\[
\begin{align*}
U(\theta, \alpha) |0\rangle &= \cos \theta |0\rangle + e^{i\alpha} \sin \theta |1\rangle \\
U(\theta, \alpha) |1\rangle &= e^{-i\alpha} \sin \theta |0\rangle + \cos \theta |1\rangle
\end{align*}
\]

The transformation \( U(\theta, 0) \) is called collective rotation noise. In this case, the states \( |\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \) and \( |\phi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \) are invariants, while \( |\phi^-\rangle \) remains unchanged even under the more generic \( U(\theta, \alpha) \). Thus, by modelling the noise in a given quantum channel, it is in principle possible to construct quantum states that are immune to all decoherence effects corresponding to that specific pattern.

The first experimental demonstration of DFS communication was reported in 2000 by Kwiat et al. [385], where the authors induced a controllable collective decodherence on an entangled photon pair generated by spontaneous parametric down-conversion (PDC) and observing that, as predicted, one specific entangled state was immune to decoherence. More recently, in 2005 Jiang et al. reported a test of DFS against collective noise on polarization and phase with four two-qubit states again from PDC [386], while in 2006 Chen et al. used single photons, entangled in polarization and time, to compensate for errors induced by a collective rotation of the polarization [42]. Importantly, their scheme was also alignment-free, i.e. with no need for a shared reference frame, and
insensitive to phase fluctuations in the interferometer. In the same year, Zhang et al. reported a fault-tolerant implementation of quantum key distribution (see Section 2.2.3) with polarization encoding, capable to account for bit-flip errors and collective rotation of the polarization state, without the need for a calibration of the reference frame [387]. In 2008, Yamamoto et al. demonstrated an entanglement distribution scheme with state-independent DFS from PDC, with an approach robust against fluctuations of the reference frame between distant nodes [388]. Other significant features reported in their work were the capability to extend the scheme to multipartite states, thanks precisely to the state-independence, and its applicability also with single-mode fibers.

More recently, various proposals and experimental tests have been reported on variants or improvements of the original schemes. For instance, Ikuta et al. in 2011 proposed and demonstrated a solution for increasing the efficiency of DFS-based entanglement distribution over lossy channels [389]. Additional features of their work were the use of backward propagation of coherent light in combination with single-photon states, and the violation of the Clauser-Horne-Shimony-Holt inequality [316] to prove non-locality in the transmission. In 2017, novel investigations on matter qubits were reported by Wang et al., with a room-temperature quantum memory realized with two nuclear spins coupled to the electronic spin of a single nitrogen-vacancy center in diamond [390], and by Zwerger et al., with the demonstration of a quantum repeater (see Section 2.2.1) using ion-photon entangled states protected via DFS against collective dephasing [391].

2.2. Long-distance quantum communication

Future quantum networks, engineered to deliver quantum information between distant nodes on the globe, are the sought-after goal underlying most of the investigations described above (see Fig. 4). This challenge already counts first demonstrations in Austria [309], China [311, 312], Japan [313, 314], Switzerland [310] and USA [308, 315] (see Table 4). We will now overview the state of the art towards their implementations.

2.2.1. Quantum repeaters – Quantum communication promises to enable quantum information protocols distributed over distant locations. In the previous section we have shortly analyzed some of the main theoretical ingredients of these quantum networks, together with the first concrete demonstrations of their feasibility. The key resource for its fulfillment is pro-
vided by quantum entanglement, at the core of quantum dense coding, teleportation, entanglement purification and entanglement swapping. By using these schemes it is possible to create entanglement between two nodes of a network to transfer quantum information. We have also described how this resource deteriorates easily and exponentially fast with the length of transmission for several reasons. Photon losses are the first cause of deterioration: even though fiber attenuation at telecom wavelength can be partly reduced, even ultra-low loss optical fibers still unavoidably lead to an exponential decrease in the generation rate of entangled pairs. This is a fundamental limitation imposed by quantum mechanics: the maximum number of entanglement bits (ebits) that can be distributed over a lossy channel with transmissivity $T$ is in fact equal to $-\log_2(1 - T)$ ebits per channel use [392]. In addition, errors can occur all along the transmission due to imperfect gates or measurements, without the possibility of duplicating quantum states deterministically [316] and with conditions much more sensitive than in the classical case. Notwithstanding, two approaches exist to circumvent these issues: reducing the transmission loss using free-space communication [43,96,105,348,350,351,393–399] and decoherence-free subspaces [42,116,385,386,388–391], or employing quantum repeaters.

Quantum repeaters (QR), proposed in 1998 by Briegel et al. [400], currently represent a strong candidate to circumvent these issues. In principle, QRs allow to improve the fidelity of transmission with time-overhead polynomial in the transmission length. In the original proposal, QRs operate by splitting the channel into a suitable number of intermediate segments linked by as many QRs, where active control can compensate for fiber attenuation, gate errors and possible noise. Once a sufficiently strong entanglement is established between two target nodes, routine quantum communication can start effectively. Today numerous schemes and platforms exist for long-distance quantum communication based on QRs [401]. QRs can be grouped in three main classes, according to the technique adopted for correcting propagation errors [401], as summarized schematically in Table 5.

**Table 5.** Quantum repeaters can be classified in three generations according to the approach used to correct errors. Table adapted from Ref. [401].

| Error | Solution | I | II | III |
|-------|----------|---|----|-----|
| Loss  | HEG (++) | ✓ | ✓  | ✓  |
|       | QEC (→)  |   |    | ✓  |
| Gate  | HEP (++) | ✓ |    | ✓  |
|       | QEC (→)  |   | ✓  | ✓  |

HEG: Heralded entanglement generation. HEP: Heralded entanglement purification. QEC: quantum error correction. $\rightarrow$: one-way communication; $\leftrightarrow$: two-way communication.

The first generation of QRs (I) employs heralded entanglement generation (HEG) and heralded entanglement purification (HEP) to reduce the deterioration...
induced by losses from an exponential to a polynomial scaling (see Section 2.1.1) [400,402–406]. The idea here is to create entanglement between adjacent nodes and to use teleportation to exchange information. Entanglement swapping and purification can then be properly combined to sequentially extend the distribution of entangled photon pairs until two nodes are connected. The overall rate for quantum communication based on this scheme decreases polynomially with the distance; however, a good solution to this drawback could be multiplexing in one of the degrees of freedom (see Section 1.1) to increase the transmission rate. A number of other approaches have been tested experimentally in the last decade. An efficient scheme using double-photon guns based on semiconductor quantum dots, polarizing beam splitters and probabilistic optical CNOT gates was proposed in 2003 by Kok et al. [407]. Active purification of arbitrary errors using only two qubits at each QR, based on nuclear and electronic spins in nitrogen-vacancy color centers in diamond, was proposed by Childress et al. [408]. Further proposals involve multi-mode memories based on photon echo in solids doped with rare-earth ions [409]. A combination of photonic and atomic platforms was also investigated by Sangouard et al. [402,410], while combinations of quantum-dot qubits and optical microwavities have been studied by Wang et al. [411]. Recently, a novel measurement-based QR was shown to enable entanglement purification and entanglement swapping [406] for one- and two-dimensional networks using cluster states and photon-ion entanglement [391,412]. A thorough analysis under noisy conditions of measurement-based quantum network coding scheme for QRs was later provided by Matsuo et al. [413]. Finally, for an overview on quantum memories in the context of quantum communication we refer to Ref. [333] and references therein.

The second generation of QRs (II) employs (i) HEG to reduce the deterioration induced by losses and (ii) quantum error correction (QEC) to correct gate errors [414,415]. Teleportation with CNOT gates and entanglement swapping are still sequentially applied to extend the entanglement to distant nodes; however, the use of QEC in place of HEP speeds up the process by avoiding the time delays due to non-adjacent-nodes signalling [416]. With this approach, quantum memories are employed at each side of a QR to save the state of the entangled photon pairs while waiting for the classical signals to carry out teleportation [112,113,137,158,334,366–368,409,417–420]. Indeed, QEC with qubit-repetition codes and Calderbank-Shor-Steane codes [316] were shown to be effective against imperfect quantum memories operation, photon losses and gate errors [421]. However, starting from 2012, alternative all-photonic schemes without quantum memories were presented by Munro et al. [417] and by Azuma et al. [422,423] based on multi-photon cluster-states, loss-tolerant measurements and local high-speed active feedforward controls. Recently, Ewert et al. achieved similar results using only locally-prepared Bell states, instead of more demanding cluster states non-locally entangled between nodes of a segment [424]. One further scheme, feasible with current technology, was proposed in 2017 by Vinay et al. [425] based on double- heralded entanglement generation and brokered Bell-state measurements.

The third generation of QRs (III) employs QEC to deterministically correct errors from both propagation losses and gate errors [417,423,426–431]. The idea is to iteratively transfer a block of ~200 qubits [417,428] from one node to the next in each lossy segment and to apply QEC to recover the encoding. Differently from the first two schemes (I, II), the latter is fully fault-tolerant and it involves one-way signalling between the segments, thus being much faster than the previous ones, in particular than type I. However, schemes II and III represent more demanding solutions from a purely technological perspective, mainly for the high control required to perform reliable error correction and, consequently, for the reduced maximal distance allowed between nodes.

2.2.2. Blind quantum computing – In the previous sections we reviewed the physical resources for the implementation of a linear-optical quantum network. Entanglement plays a fundamental role for quantum communication, while various quantum repeaters have been developed with increasing performances, paving the way for an effective management of quantum information in intra-city and global networks. However, building a network with hundreds of nodes and synchronized single-photon sources seems still a demanding target for the near-term future. In this section we discuss quantum computation in an optical quantum network, where a client resorts to a central server with more advanced quantum technology to perform computation in a manner as safe as possible: the server should obtain no information on client’s inputs, algorithms and outputs [432].

The first model of blind quantum computation (BQC) was proposed by Childs in 2001 [433], where Alice, who cannot access a quantum computer, asks Bob to help her perform quantum computation without telling him her input, output and task. Childs described a protocol where Alice succeeds in this goal, with the possibility of even detecting whether Bob is honest or introducing errors. His solution was later improved by Arrighi and Salvail in 2003 [434], with a blind protocol for the class of functions admitting an efficient generation of random input-
output pairs like factoring. However, these schemes still allocate high resources to the client, who is supposed to have access to quantum memories and SWAP quantum gates. A step ahead was achieved in 2009 by Broadbent, Fitzsimons, and Kashefi with an interactive one-way BQC model (BFK) employing measurement-based quantum computing, where Alice only needs to produce single-qubit states with no need for quantum memories [435] and where she is capable to detect malicious errors (see Section 3.3). From 2009 several other BQC protocols have been proposed, which may be classified according to the number of servers employed [436]: single-server BQC protocols [433, 434, 437–451], where Alice is capable to generate quantum states and distribute them to Bob, two-server [435, 436, 452] and three-server [453], where Alice can get rid of quantum capabilities. Results have been reported also for a purely classical user [451], though some limitations have been recently opposed by Aaronson et al. [454] building upon complexity considerations analogous to those for BosonSAMPLING (see Section 3.2). In measurement-only BQC, the idea is for Alice to secretly hide trap qubits in her state. If Alice discovers an unwanted change of a trap she can conclude that Bob is not honest and quit the task. The probability that Alice accepts a malicious Bob can then be made exponentially small using quantum error correcting codes [443, 449].

The feasibility of BQC has already been proved by various photonic experiments. The first demonstration was reported in 2011 by Barz et al. [437], where photon states were sent by the client to the quantum server, which produced four-photon blind cluster states to perform Grover search and Deutsch algorithms [316]. In 2013, Barz et al. [455] proposed and demonstrated experimentally a technique to test whether a quantum computer is really quantum and whether it provides correct outputs (see Section 3.3). In the same year, Fisher et al. [444] demonstrated arbitrary computations on encrypted qubits, only requiring the client to prepare single qubits with limited classical communication. Finally, in 2016 Greganti et al. [456] reported photonic BQC where the client sends four-qubit states to the server to implement arbitrary two-qubit entangling gates.

The above demonstrations represent significant achievements for BQC, showing that integration of these algorithms on linear-optical networks are in principle feasible using single photons. We mention that also continuous variables schemes have been proposed [457, 458], while numerous works have analyzed their feasibility with respect to efficiency [440, 450, 459] and resilience to errors [439, 441, 446] and to noisy implementations (see also Section 2.1.2) [436, 448]. However, it was observed that hybrid systems with matter qubits for carrying out quantum computation and single photons for quantum communication could offer an even more advantageous solution in larger-size distributed protocols [432].

2.2.3. Photonic quantum key distribution – Quantum key distribution (QKD) is a technique to generate a shared random secret key between two parties. The advantage of QKD is the possibility to detect possible attacks from a malicious third party, since any measurement carried out by the latter influences the shared system. Once a secret key is shared, the two parties can start standard classical communication.

Technological requirements and security. The security of a QKD system is measured with the distance $\epsilon$ between the corresponding outcomes probability distribution and the ideal one with a perfect key, typically $\sim 10^{-10}$. This difference can be made in principle arbitrarily small, at the price of requiring more stringent hardware performances and by applying suitable privacy amplification [316]; however, one should bear in mind that this threshold must include all subroutines involved in a QKD system, so that only the overall composable security $\tilde{\epsilon} = \sum \epsilon_k$ is relevant. There are still many limitations to overcome to develop QKD systems [321], the main being (i) the transmission rate and range, much lower than in classical communications, (ii) the high cost to produce and maintain the hardware, (iii) the need for authentication and integrity and (iv) that new classical algorithms can be designed to be immune to quantum agents. First QKD prototypes have also been hacked [486, 487], though techniques exist to correct gate errors with linear optics [418, 488–490].

QKD protocols are capable to establish secure communication channels, but no protection is warranted to the single-photon sources and detectors employed in the system. Alice’s source represents probably the safest stage, since it can be secured by optical isolators and verified in situ [491], thus most quantum hacking algorithms currently exploit the receiver’s detectors (e.g. detection efficiency and dead time), even though a complete list of weak points would involve also attacks based on channel/device calibration or photon wavelength [486]. In principle, countermeasures could be found any time a loophole is discovered just like for classical cryptosystems. However, this is naturally not desirable for an approach that aims to build inherently secure protocols of communication. One approach to counter hacking attacks is device-independent (DI) QKD [492, 493] where Alice’s and Bob’s devices are considered as black boxes and the security depends on the violation of a Bell inequality to confirm quantum correlations [494]. However,
hardware technological challenges still make DI-QKD impractical for current state-of-the-art. A second approach based on time-reversed QKD is measurement-device-independent (MDI-) QKD [495,496], which allows Alice and Bob to perform QKD protocols even in the case of untrusted devices [497], reasonably assuming trusted sources. One advantage of MDI-QKD is its feasibility with state-of-the-art technology, with key rates orders of magnitude higher than in DI-QKD.

Table 6. Several experimental demonstrations of quantum communication have been reported in the last two years, from specific applications to long-distance communication.

| Year | Ref. | Focus for QKD | Distance (km) |
|------|------|---------------|---------------|
| 2016 | [460] | Renes2004 protocol | 0 |
|      | [461] | BBM92 protocol | 50 |
|      | [462] | WDM GPOM | 24 |
|      | [463] | QDS | 90 |
|      | [464] | MDI DS | 36 |
|      | [465] | MDI DS | 404 |
|      | [466] | Phase-encoded passive-DS | 10 |
|      | [467] | DP-QPSK DS | 100 |
|      | [468] | HD DS DO | 43 |
|      | [469] | HD | 0 |
|      | [470] | HD MCF DS | 0.3 |
|      | [471] | MCF | 53 |
|      | [472] | Free-space in daylight DS | 53 |
| 2017 | [473] | QSDC | 0 |
|      | [474] | Free-space HD | 0.3 |
|      | [475] | DS on tunable circuit | 20 |
|      | [476] | HD MCF DS | 20 |
|      | [477] | Entanglement swapping | 12 |
|      | [478] | WDM QAM DS | 80 |
|      | [479] | QDS | 90/134 |
|      | [480] | MDI DS QDS | 50 |
|      | [481] | MDI DS QDS | 55 |
|      | [482] | DS BB84 | 200/240 |
|      | [483] | Polarization/phase-encoding | 45 |
|      | [484] | Free-space | 10 |
|      | [485] | Satellite | 1200 |
|      | [486] | Satellite DS | 700 |
|      | [487] | Satellite | 1000 |
|      | [488] | Satellite DS | 1200 |
|      | [489] | Satellite teleportation | 1400 |
|      | [490] | Satellite DS | 7600 |

WDM: wavelength-division-multiplexing; GPOM: gigabit-capable passive optical network; MCF: multicore fiber; QDS: quantum digital signature; MDI: measurement-device-independent; DS: decoy-state; DP-QPSK: dual polarization quadrature phase shift keying; QAM: quadrature amplitude modulation; HD: high-dimension; DO: dispersive optics; QSDC: quantum secure direct communication. a: 134 km is simulated with additional optical attenuation. b: with/without multiplexing.

Implementation of QKD. Currently the most widely adopted protocols for QKD are BB84 [1] and E91 [498], as well as quantum secret sharing [499] and third-man quantum cryptography [500], though numerous other schemes have been developed [316,501,502] based on discrete variables, continuous variable or distributed phase reference coding. Single photons offer the most promising platform to encode information that can be secretly shared thanks to entanglement. In particular, both quantum secret sharing and third-man quantum cryptography rely on three-particle polarization entangled states $|\psi\rangle \propto |000\rangle + |111\rangle$ known as GHZ [500]. Other schemes based on attenuated entangled states are also of importance, for instance for differential phase shift [463,502], coherent one-way (COW) [503] and decoy-state protocols [377,393,466,470]. We refer the reader to recent comprehensive reviews [321,486,487] on the topic for a thorough overview of the extensive field. For a list of the most recent implementations see instead Table 6.

Information can be transferred between distant locations either via free-space ($\lambda \sim 800$ nm) or via optical fibers ($\lambda \sim 1310$ nm or $\lambda \sim 1550$ nm) using any of the degrees of freedom overviewed in Section 1.1. Polarization or orbital angular momentum are indeed more fit for free-space communication, since birefringence and mechanical instabilities in fibers can affect them heavily, thus making time-bin or frequency encoding more suitable. Protocols based on entangled photon pairs could achieve the longest distances tolerating higher losses up to $\sim 70$ dB, as well as requiring higher technological requirements, while distributed-phase-reference QKD is a more promising solution for shorter distances ($\sim 100$ km) [502,503].

In the context of in-fiber QKD, a new approach that was recently introduced to achieve higher key rates is offered by wavelength-division multiplexing (WDM), where two quantum signals are transferred simultaneously on the same optical fibers. Quantum information can be exchanged even with strong classical signals thanks to dense wavelength multiplexing on the same fiber, showing that the integration of QKD protocols on existing telecom networks can be a viable path. In 2009, Chapuran et al. demonstrated WDM-QKD in a reconfigurable network with single photons at 1310 nm and classical channels at 1550 nm [504], while Peters et al. reported WDM-QKD at 1550 nm for both quantum and strong classical channels [505]. More recently, in 2014 Patel and coworkers set a new record by transferring bidirectional 10 Gb/s classical channels with a key rate of 2.38 Mbps and fiber distances up to 70 km [399]. One of the main sources of noise in these experiments was due to spontaneous anti-Stokes Raman scattering [504,505], whose influence was shown to be mitigated by selecting an optimal wavelength, allowing
for unprecedented terabit classical data transmission up to 80 km [462,474].

While in-fiber QKD could achieve high transmission rates for short distances, by exploiting pre-existing telecom infrastructures, free-space QKD represents an alternative promising way for future QKD networks on a global scale. First demonstrations of ground-based quantum communication with single photons were reported with progressively higher records in distance and key rate [43, 96, 105, 348, 350, 393–396, 506–508]. Yet, one further promising approach would be to employ satellites as nodes of the network, an ambitious project that could allow to cover the whole globe. Preliminary tests in this direction were carried out independently in 2013 by Wang et al., simulating three experiments of QKD with decoy states [393,466,470] with a setup operating on moving (ground) and floating (hot-air balloon) platforms with high-loss channels [397], and by Nauerth et al., demonstrating an instance of BB84 between a high-speed airplane and a ground station for a distance of 20 km [398]. Later on, in 2015 and 2016, two papers reported the transmission of single photons using satellite corner cube retroreflectors as quantum transmitters in orbit [509,510]. In 2017 six further achievements were reported: ground-to-aircraft [480] and satellite-to-ground [482–484] QKD, satellite-based entanglement distribution over 1200 kilometers [481] and ground-to-satellite teleportation of single-photon qubits for a distance up to 1400 km [351]. Finally, in 2018 Liao et al. successfully performed decoy-state QKD between a low-Earth-orbit satellite and multiple ground stations separated by 7600 km on Earth [485], providing landmark steps forward toward the realization of future long-distance quantum networks.

3. Photonic quantum simulation

In this chapter we will review the field of photonic quantum simulation, starting with single-photon dynamics in quantum walks (Section 3.1) and extending it to multiphoton evolution (Section 3.2). In Section 3.3 we will review some of the most recent results on the problem of verification, whose increasing relevance goes in parallel to the developments in quantum simulation. Finally, in Section 3.4 we describe the first applications in quantum chemistry and condensed matter. For a comprehensive review of quantum simulation in various fields and physical platforms we refer the reader to Refs. [511,512].

3.1. Photonic quantum walks

Quantum walks (QW), the extension of classical random walks to a quantum framework, have gained an increasing role in modelling single- and multi-particle evolutions in several scenarios [513] thanks to their platform-independent formulation. Importantly, the universality of the linear-optical platform for quantum computation [514] has further prompted several experimental tests of QWs with single photons. Two classes of QWs exist (see Fig.5): discrete-time (DTQW), where the evolution is split in discrete steps and random events suddenly influence the dynamics, and continuous-time (CTQW), where the evolution on a given lattice is described by a time-independent Hamiltonian and by the adjacency matrix of the corresponding graph. In this section we will focus on the experimental implementation of photonic QWs, reviewing the latest achievements in this area with some links to the theoretical background. The reader interested in the theory of quantum walks may refer to Ref. [515] for a comprehensive collection.

Discrete-time quantum walks. DTQWs can be described by single photons evolving through a network of beam splitters. In this pictorial representation, each time a photon enters a beam splitter its wave function is split in two parts proceeding on separate optical modes. In terms of creation operators acting on the two modes, the evolution can be ruled for instance by the Hadamard coin

$$\begin{pmatrix} a_1^+ \\ a_2^+ \end{pmatrix}_{in} \rightarrow \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \begin{pmatrix} a_1^+ \\ a_2^+ \end{pmatrix}_{out}$$ (12)

We stress that also other approaches can accomplish the same task [51,54]: we only need a process $Q$ that, given a chosen encoding, operates the transformation $Q |1\rangle \rightarrow \alpha |0\rangle + \beta |1\rangle$. Choosing $Q$ as a building block for the QW, after $n$ steps the walker will be in the superposition $\sum_j c_j a_j^+ |0\rangle$, where the amplitudes $c_j$ can be balanced, symmetric or asymmetric over the optical modes according to the symmetries of the walker [16,516] and to the evolution [517,518].

First implementations of DTQWs were reported in the first years of this century, motivated by the connection found between QWs and quantum computation [519,520] for which, just at that time, Knill, Laflamme and Milburn were showing that linear-optical platforms are universal [514]. The very first demonstrations were carried out on bulk optics, confirming the theoretical predictions for single photons dynamics [521,522] and wave packet interference [523]. However, bulk implementations unavoidably suffer from mechanical instabilities and issues of alignment critical for larger-size experiments. A first solution was found in 2010 with novel fiber-loop designs [146,147,517,524], which provided a more stable approach suitable for further improvements in the direction of scalable schemes. Thanks to this new
approach it was possible to investigate QWs with a larger number of steps, yielding a richer landscape of photon interference. A relevant step forward was given by the introduction of integrated photonic circuits (see Section 1.2.2), which provided further advantages in stability, alignment and compactness [16,231,516,518,525]. Moreover, integrated circuits are fit for realizing reconfigurable photonic architectures, allowing to dynamically tune the evolution and, thus, to explore more complex scenarios within the same quantum walk [122, 227, 231]. Relevant tests on the foundations of quantum mechanics carried out on integrated circuits include, for instance, bosonic-fermionic evolutions [16], indistinguishable-distinguishable bosons [516] and quantum transport phenomena [231] such as wavefunction localization in disordered media [518]. Very recently, in 2015 an approach for DTQWs was reported based on the orbital angular momentum of light, so that the evolution takes place in the OAM degree of freedom without the need for an interferometer [51, 54]. This new approach provides indeed a flexible solution that may enable scalable investigations. Finally, in 2016 Boutari et al. proposed and demonstrated experimentally a time-bin-encoded scheme for QWs, based on a network of optical ring cavities, which simultaneously achieves low losses, high fidelity, reconfigurability. Such scheme can be further generalized to multidimensional lattices [148].

Continuous-time quantum walks. CTQWs represent another platform for investigating statistical features of the evolution of bosonic states [530, 531, 533, 542, 543] and simulating complex processes [17, 35, 536, 537, 539–541]. CTQWs can be implemented with arrays of $N$ evanescently-coupled waveguides tailored to produce a time-dependent or time-independent lattice Hamiltonian [545]

$$\hat{H} = \hbar \sum_{i=1}^{N} \left( \beta_i a_i^\dagger a_i + \sum_{j=1}^{N} \kappa_{i,j} a_j^\dagger a_i \right)$$ (13)

Figure 5. Quantum walks are classified in two types: discrete-time and continuous-time. While the former can count on various photonic implementations, the latter has been enabled by integrated waveguide lattices. In each subfigure, $Q_i$ indicates the different steps of the quantum walks. Legend - QWP: quarter-wave plate, HWP: half-wave plate, PBS: polarizing beam splitter, BS: beam splitter, GP: glass plate, POL: polarizer, FPBS: fiber polarizing beam splitter.
Table 7. Photonic discrete-time quantum walks (QW).

| Year | Ref.  | Platform               | Focus                                      | Photons | Structure |
|------|-------|------------------------|--------------------------------------------|---------|-----------|
| 2005 | [521] | Bulk optics            | Quantum quincunx                           | 1       | 8 modes   |
| 2008 | [523] | Bulk optics            | Wave packet reshaping                      | 1       | 1 step    |
| 2010 | [146] | Fiber loop             | Robust implementation                      | 2       | 5 steps   |
|      | [522] | Bulk optics            | QW with tunable decoherence                | 1       | 6 steps   |
| 2011 | [524] | Fiber loop             | Features of the dynamics                   |         | 70 steps  |
|      | [517] | Fiber loop             | Decoherence and disorder                   |         | 28 steps  |
| 2012 | [526] | Bulk optics            | Topological phases                         | 1       | 7 steps   |
|      | [16]  | Integrated photonics   | Bosonic-fermionic evolution                | 2       | 8 modes   |
|      | [147] | Fiber loop             | Entanglement on 2D QW                      |         | 12 steps  |
| 2013 | [518] | Integrated photonics   | Anderson localization                      | 2       | 16 modes  |
|      | [527] | Fiber loop             | Delayed-choice 2D QW, Grover QW            | 1       | 4 steps   |
| 2014 | [525] | Integrated photonics   | High-order single-photon W-states          |         | 2,4,5,8,16 modes |
| 2015 | [51]  | Orbital angular momentum | Wave packet dynamics                      | 2       | 5 steps   |
| 2016 | [148] | Optical ring cavities  | Low-loss tunable QW                        |         | 62 steps  |
|      | [54]  | Orbital angular momentum | Topological quantum transitions           |         | 6 steps   |
| 2017 | [528] | Orbital angular momentum | Zak phases, topological invariants         |         | 7 steps   |
|      | [529] | Integrated photonics   | Entanglement after spin chain quench       | 2       | 5 modes   |
|      | [231] | Integrated photonics   | Quantum transport                          |         | 26 modes  |

Table 8. Photonic continuous-time quantum walks implemented with integrated circuits.

| Year | Ref.  | Technology                    | Focus                                      | Photons | Waveguides |
|------|-------|--------------------------------|--------------------------------------------|---------|------------|
| 2007 | [530] | Optical induction\(^{(a)}\)  | Transport, Anderson localization          |         | n.a.       |
| 2008 | [531] | SoI                            | Evolution on quantum walks                 |         | ~ 100      |
| 2010 | [532] | SiO\(_x\)N\(_y\)             | Quantum correlations                       | 2       | 21         |
| 2011 | [533] | FLW                           | Evolution in an elliptic waveguide array   | 2       | 6          |
|      | [534] | FLW                           | Anderson localization                      |         | 101        |
| 2012 | [535] | n.a.                          | Quantum correlations                       |         | 29         |
|      | [35]  | FLW                           | Quantum Rabi model                        |         | 15         |
| 2013 | [536] | FLW                           | Floquet topological insulator             |         | 49/308 \(^{(b)}\) |
|      | [537] | FLW                           | Bosonic coalescence                       | 3       | 3          |
|      | [17]  | SiO\(_x\)N\(_y\)             | Fermionic statistics                       | 2       | 10         |
| 2014 | [128] | LiNbO\(_3\)                  | Tunably-entangled biphoton states          | 2       | 21         |
|      | [516] | SiO\(_x\)N\(_y\)             | Bosonic clouding                          | 3,4,5   | 21         |
|      | [538] | FLW                           | Quantum correlations                       | 2       | 9          |
| 2015 | [539] | FLW                           | Majorana dynamics                         |         | 26         |
|      | [540] | FLW                           | Quantum decay and Fano interference       | 2       | 27         |
|      | [541] | FLW                           | N00N state Bloch oscillations              | 2       | 16         |
| 2016 | [542] | FLW                           | Quantum transport                         |         | 4+30       |
|      | [543] | FLW                           | Quantum transport                         |         | 18+62      |
|      | [544] | FLW                           | Discrete fractional Fourier transform      | 2       | 8          |

FLW: femtosecond laser written. SoI: silicon on insulator. n.a.: not available.
\(^{(a)}\): in Sr\(_{0.6}\)Ba\(_{0.4}\)Nb\(_2\)O\(_6\); \(^{(b)}\): for two honeycomb photonic lattices.

where \(\beta_i\) is the propagation constant for the \(i\)th waveguide and \(\kappa_{i,j}\) is the coupling between waveguides \((i,j)\), with the usual restriction to \(j = i \pm 1\). For an analogy with DTQWs, where the free evolution is decomposed in discrete steps, now waveguides are arranged in 1D or 2D structures in such a way that light can continuously jump between neighbor sites. The evolution of the \(k\)th creation operator is given by \[^{545}\]

\[
\begin{align*}
    a_k^\dagger(z) &= e^{i\beta z} \sum_i U_{k,i}(z) a_i^\dagger(z_0) \\
    U_{k,l}(z) &= (e^{i\kappa z})_{k,l}
\end{align*}
\]

where \(z\) is the position along the propagation direction. Waveguide arrays have been implemented so far on
integrated photonic circuits, inscribed using one of the fabrication techniques described in Section 1.2.2.

**Quantum transport.** Quantum transport phenomena concern the spatial evolution of the wave function during a QW. This process can occur in two regimes: in ordered and in disordered lattices. A photon propagating through a static-ordered lattice shows a ballistic spread for a distance proportional to the evolution time $T$, due to the interference of the wave packet amplitudes across the CTQW. For disordered systems a further distinction can be made: dynamic disorders are associated to diffusive transports, where interference no longer affects the evolution and a classical-like spreading is found for a distance proportional to $\sqrt{T}$, while static disorders lead to a complete halting in the process, a phenomenon known as Anderson localization [546, 547] where the wave packet localizes on the initial sites of the lattice [518, 530, 534, 548]. Several analyses show that a suitable combination of quantum coherence and environmental noise can provide an effective enhancement in quantum transport [231, 542, 549–553]. In this context, reconfigurable photonic circuits can provide a useful platform to characterize it, allowing to study the continuous transitions between different regimes [231]. Finally, we mention that lattices subject to external gradient forces exhibit a characteristic periodic oscillation between spreading and localization of the wave packet, the so-called Bloch oscillations, which have been observed experimentally in photonic platforms [524, 541, 554–556].

**Multi-photon quantum walks.** So far we have reviewed studies that focus on single-particle evolutions in discrete- or continuous-time QWs. However, the full landscape of phenomena gets enriched if we consider photonic states with $n = 2$ photons [16, 17, 51, 128, 146, 516, 518, 532, 533, 537, 538, 540, 541, 544], thanks to the emergence of more complex interference patterns [516, 544], highlighting for instance two-photon quantum correlations [532, 538] with bosonic-fermionic transitions [16, 17], and enabling the possibility of simulating relevant physical processes [540, 541]. Finally, the possibility of further increasing the number of injected photons to $n = 3$ [537, 557] or $n > 3$ photons is believed to disclose even larger potentialities, which we briefly discuss in the next section with the BosonSampling problem.

### 3.2. BosonSampling

In the previous section we reviewed the recent achievements in photonic quantum walks, which gained increasing attention after the discovery that multiparticle quantum walks with interactions allow for universal quantum computation [514, 558]. A milestone result in the intertwined developments of quantum walks and quantum computation is represented by the proof, by Aaronson and Arkhipov [559] in 2010, that $n$-photon states evolving in a discrete-time quantum walk can provide a first experimental evidence of a superior quantum computational power [560, 561].

BosonSampling consists in sampling from the output distribution of an interferometer implementing a Haar-random $m$-mode transformation $U$ on $n$ indistinguishable bosons. The computational complexity of the problem is rooted in the hardness [562] of evaluating the permanent in the scattering amplitudes [563]

$$
\langle t_1, \ldots, t_m | U | s_1, \ldots, s_m \rangle = \left( \prod_{i=1}^{m} s_i! t_i! \right)^{-\frac{1}{2}} \text{Per}(U_{S,T}) \tag{15}
$$

where the integer $s_k$ ($t_k$) is the occupation number for the input (output) mode $k$ ($\sum s_k = \sum t_k = n$) and $U_{S,T}$ is the $n \times n$ matrix obtained by repeating $s_k$ ($t_k$) times the $k$th column (row) of $U$. Assuming two highly plausible conjectures [559], Aaronson and Arkhipov showed that, should a classical polynomial-time algorithm exist capable to solve BosonSampling, it would imply the collapse of the polynomial hierarchy of complexity classes to the third level, a possibility of huge consequences widely believed to be unlikely.

Despite its simple formulation, requiring only single photons with no entanglement, no adaptive measurements and no ancillary qubits, the necessity to scale up the number of photons and modes represents a technological challenge. For an overview of the state of the art in the development of single-photon sources, integrated photonic interferometers and single-photon detectors, the reader can refer to Sections 1.2.1, 1.2.2 and 1.2.3. State-of-the-art classical simulation of BosonSampling depends on the number of photons as in Table 9.

**Table 9.** The largest classical simulation of BosonSampling (up to 30 photons) was reported in 2017 based on Metropolised independence sampling (MIS) [564]. The computational complexity for exact classical BosonSampling was given in the same year in Ref. [565] by Clifford and Clifford (CC): state-of-the-art sampling time is equal, within a factor of 2, to computing the permanent of one single scattering matrix [566].

| Approach | $n$ | Hardware | Classical technique |
|----------|-----|----------|---------------------|
| Simulated | 30 | Laptop | MIS [564] |
| Exact | 10 | Laptop | Brute force |
| | 50 | Tianhe-2 [566] | CC [565] |

Soon after its introduction, in 2013 four experimental demonstrations with $n = 3$ photons were re-
ported [240, 567–569]. Since then, several investigations have been performed to study the scalability in imperfect conditions, such as in the presence of losses [570–573], partial distinguishability [574, 575] and generic experimental errors [571, 576–578]. Furthermore, the scalability of parametric down-conversion sources and the relevance of non-ideal detectors’ efficiency have been addressed in Ref. [579] and investigated experimentally in 2015 with the scattershot implementation [580, 581].

Since 2015, a number of alternative schemes have been proposed: driven BosonSampling, where the input photons are generated within the interferometer [585], BosonSampling with microwave photons [586] or squeezed states [587, 588], one using Gaussian measurements and the symmetry of the evolution under time reversal [589, 590], and one time-bin loop-based [150]. Furthermore, somehow in analogy with the link between quantum walks and quantum computation, recently BosonSampling was shown to be equivalent to short-time evolutions of n excitations in a XY model of 2n spins [586]. This feature has suggested multiport photonic interferometers as good candidates for the implementation of quantum simulators or even general-purpose quantum computers [586, 591, 592]. Nevertheless, in 2017 new classical algorithms have been proposed to solve BosonSampling for systems with dimensionality larger than that allowed by near-term technological advances [564, 565, 572, 573, 593, 594], thus increasing the challenge to achieve quantum supremacy, i.e. the regime with quantum advantage [560, 561]. Experimental state of the art for photonic BosonSampling is shown in Table 10 and in Fig. 6.

3.3. Verification of quantum simulation

The problem of verification, fundamental for both classical and quantum computation, is closely related to the issue of security in information processing. One good example is offered by BosonSampling [559]: a computational problem where a special-purpose quantum device is believed to outperform classical supercomputers. For similar problems that live outside the complexity class NP, it is in general not possible to verify the correctness of an outcome. Thus, in a scenario where untrusted parties can deviate calculations from their ideal flow, it is essential to develop techniques to ensure that robust computation is guaranteed to the maximum possible extent (fault-tolerance, i.e. amplification of the detection rate) or, equivalently, that malicious processes can be easily detected (e.g. using traps to detect errors) [435]. In this sense, the problem of verification in quantum computation is connected with the universal blind computation model described in Section 2.2.2. In the last few years, several protocols for verifiable quantum computations have been proposed [435, 443, 447, 493, 596–603], where the attention focused on schemes with either fewer experimental requirements or higher generality and security. We refer the reader to Ref. [449] for a comprehensive review on the problem of verification in blind quantum computing and to Refs. [599, 600] for a short overview of the differences between the various protocols.

We have shortly described in Section 2.2.2 the first experimental demonstrations of verifiable blind quantum computing, performed using polarization qubits represented by multi-photon states generated via parametric down-conversion [437, 444, 455, 456]. Beyond these works, the problem of verification has drawn large attention also in quantum communication
and quantum simulation. In the scope of secure quantum communication, for instance, where quantum networks are employed to perform distributed quantum computations over possibly untrusted nodes, it is necessary to verify the goodness of the shared multipartite entangled states, the key resource behind these protocols [525, 604]. To this aim, in 2014 Bell et al. reported the experimental demonstration of a graph-state quantum secret sharing protocol [605], whose implementation was subsequently verified using the scheme in Ref. [604]. In 2016, further improvements led McCutcheon et al. to a verification of multipartite entanglement for photonic quantum networks, adopting two single-photon sources similar to Ref. [605] to produce three- and four-photon polarization encoded states [606].

We conclude this section discussing the role of verification in quantum simulation and, in particular, in BosonSAMPLING. In the latter case, as for analogous experiments involving multi-photon interference in linear-optical multiport interferometers, it is crucial to check the indistinguishability of the input photons to ensure the correctness of the overall operation. The validation of BosonSAMPLING developed rapidly in the last few years just after the first experimental demonstrations, and its applications will potentially go beyond its original purpose. Since a full certification of BosonSAMPLING is believed to be not possible [607], all current protocols aim at ruling out the most plausible unwanted scenarios, namely experiments where devices are injected with distinguishable input photons and with mean-field states [608]. Currently there exist several protocols to validate BosonSAMPLING, most of which have already been successfully demonstrated experimentally [122, 149, 241, 474, 516, 581, 582, 595, 609–613]. An efficient certification protocol for photonic state preparation was also introduced theoretically [614], allowing to discriminate relevant classes of Fock states and Gaussian/non-Gaussian pure states. We summarize them in Table 11, with an overview of the techniques adopted and the hypotheses which are designed for.

### 3.4. Photonic simulation in quantum chemistry and condensed matter

Computational chemistry employs simulations to study properties of molecules or to predict unknown chemical phenomena. Indeed, analytical solutions for quantum many-body problems are available only for the simplest systems, thus making simulations necessary and heavily based on classical techniques such as the

| Test          | Ref.            | U | D | MF | O |
|---------------|-----------------|---|---|----|---|
| RNE           | [149, 581, 582, 595, 607] | ✓ |   |    |   |
| LR            | [149, 581, 582, 584, 595] | ✓ | ✓ |    |   |
| ZTL           | [122, 241, 608–610, 615–617] | ✓ | ✓ |    |   |
| Bayesian      | [149, 584, 610, 611] | ✓ | ✓ |    |   |
| Bunching      | [516, 618] | ✓ |   |    |   |
| CG            | [612, 619] | ✓ | ✓ |    |   |
| n = m         | [620] | ✓ | ✓ |    |   |
| Statistical   | [613, 621] | ✓ | ✓ | ✓ |   |

Table 11. Validation of multi-photon interference against uniform distribution (U), experiments with distinguishable photons (D), mean-field states (MF) or other hypotheses (O). See Table 10 for a cross reference with BosonSAMPLING experiments. RNE: row-norm estimator; LR: likelihood ratio; ZTL: zero-transmission law (suppression law); CG: Coarse-graining.
Born-Oppenheimer or Hartree-Fock approximations, the density-functional theory or even machine learning [622]. Notwithstanding, when modelling the quantum nature of highly correlated many-body systems, it became clear that the only solution to counteract the exponential increase in computational resources, the so-called curse of dimensionality, was to exploit other quantum systems for information processing [623]. The belief in this quantum approach was indeed supported in the 90’s by the first efficient quantum algorithms [316], which were rapidly followed by breakthrough discoveries applicable to quantum chemistry [3, 624]. The algorithm developed in 2005 by Aspuru-Guzik et al. [625] offered an exponential speed-up in computational resources, scaling linearly in the number of qubits and polynomially in the number of gates. Today there exist numerous algorithms for simulating quantum chemistry, for which a complete review goes beyond the scope of this section. The reader interested in a detailed and comprehensive excursion of the state of the art may find Ref. [622] a useful resource, while Refs. [626, 627] may be suitable for a more experiments-oriented overview. In the following, we will briefly describe the latest achievements of quantum chemistry simulations on photonic platforms.

Photonic technologies provide an effective platform for quantum simulation, thanks to the single photons’ low decoherence, speed and controllability that we discussed in the previous chapters. First experimental demonstrations in bulk optics were reported in 2009 for the simulation of anyons, fractional-statistics particles responsible for the fractional quantum Hall effect [628, 629] and for the calculation of the energy spectrum of a hydrogen molecule [630]. The approach adopted in the latter work consisted in encoding the state of the system in entangled states. It was possible to perform QPE separately on the polarization qubit of the quantum register, accessing the outcome via the control entangled photon [630]. In 2010, Kaltenbaek et al. generated a photonic valence-bond-solid state, the gapped ground state of a two-body Hamiltonian on a spin-1 chain, as a useful ressource for the implementation of single-qubit quantum logic gates [631]. In 2011, Ma et al. used two polarization entangled photon pairs to study the process of frustration in a tetramer, a system with four spin-1/2 particles, observing the transition between localized and resonating-valence-bond states at varying Heisenberg interaction strength [632, 633]. The analog simulation required measuring the output of tunable beam splitter injected with single-photon states from each pair. All states have been characterized by retrieving the total energy and the pairwise quantum correlations, whose values are conditioned by the quantum monogamy. In 2012, Kitagawa et al. employed a discrete-time bulk quantum walk to demonstrate the topological protection of bound states in both static and dynamic scenarios, a useful tool that finds application for instance in quantum computation. Topological transitions have been also the focus of a recent study carried out with orbital angular momentum encoding [54].

Recently the development of integrated photonic circuits for quantum walks (QW) has prompted the realization of various quantum simulations (see Section 3.1). Among discrete-time QWs, for instance, we have discussed the experimental investigation on the transition between fermionic and bosonic states [16], enabled by polarization-encoded symmetric (bosonic) or anti-symmetric (fermionic) wave functions. Very recently, a new quantum approach based on variational coding [54].

Within this framework, in 2015 Huh et al. found the first application of BosonSampling for quantum simulation to evaluate molecular vibronic spectra [586, 591, 592].

Discussion

Photonic quantum technologies provide a promising platform for researches and applications in several contexts. This review attempted to gather their most recent advances, to provide the reader with a unified framework for the various ingredients. General aspects
addressed in this manuscript are the generation, manipulation and detection of single-photon states from the technological perspective, as well as the fundamental theoretical tools developed for quantum communication and quantum simulation. The large effort devoted to these technologies is indeed testified also by the several achievements reported during the completion of this review, which make it challenging to stay up-to-date in this rapidly evolving field.

Acknowledgments

This work was supported by the ERC-Starting Grant 3D-QUEST (3D-Quantum Integrated Optical Simulation; grant agreement no.641039; http://www.3dquest.eu) and by the H2020-FETPROACT-2014 Grant QUCHIP (Quantum Simulation on a Photonic Chip; grant agreement no.641039; http://www.quchip.eu).

References

[1] Bennett C H and Brassard G 1984 Quantum cryptography: Public key distribution and coin tossing
[2] Shor P 1994 Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer Proceedings of the 35th Annual Symposium on Foundations of Computer Science
[3] Lloyd S 1996 Science 273 1073–1076
[4] Bennett C H, Brassard G, Crépeau C, Jozsa R, Peres A and Wootters W K 1993 Phys. Rev. Lett. 70 1895–1899
[5] Dowling J P and Milburn G J 2003 Philosophical Transactions of The Royal Society A: Mathematical Physical and Engineering Sciences 361 1655-1674
[6] Knill E and Laflamme R 2001 Inform. Process. Lett. 79 173–179
[7] Gu X, Kockum A F, Miranowicz A, Liu Y X and Nori F 2010 Phys. Rev. A 82 033830
[8] You J Q and Nori F 2011 Phys. Rev. A 83 052323
[9] Gu X, Kockum A F, Miranowicz A, Liu Y X and Nori F 2017 Phys. Rev. A 95 012301(R)
[10] Martínez-Herrero R and Mejías P M 2010 Opt. Express 18 7995–7971
[11] Kok P and Lovett B W 2010 Introduction to optical quantum information processing (Cambridge University Press)
[12] Bliokh K Y and Nori F 2015 Phys. Rep. 592 1–38
[13] Bliokh K Y, Rodríguez-Fortuño F J, Nori F and Zayats A V 2015 Nat. Photon. 9 796–808
[14] Bliokh K Y and Nori F 2015 Phys. Rev. Lett. 115 033601
[15] Bliokh K Y, Rodríguez-Fortuño F J, Nori F and Zayats A V 2014 Phys. Rev. A 90 063823
[16] Bliokh K Y and Nori F 2015 Phys. Rev. A 91 062303
[17] Barreiro J T, Wei T C and Kwiat P G 2010 Phys. Rev. Lett. 105 033601
[18] Crespi A, Longhi S and Oseleev R 2012 Phys. Rev. Lett. 108 133601
[19] Rojas-Rojas S, Morales-Inostroza L, Neather X, Xavier G B, Bolte S, Szameit A, Vicenço R A, Lima G and Delgado A 2014 Phys. Rev. A 90 063823
[20] Bonneau D, Lobino M, Jiang P, Natarajan C M, Tanner M G, Hadfield R H, Dorenbos S N, Zwiller V, Thompson M G and O’Brien J L 2012 Phys. Rev. Lett. 108 030503
[21] Fickler R, Lapkiewicz R, Plick W N, Krenn M, Schaeff C, Ramelow S and Zeilinger A 2012 Science 338 640–643
[22] Steinlechner F, Ecker S, Fink M, Huber M, Scheidl T and Ursin R 2017 Nat. Commun. 8 15971
[23] Barreiro J T, Langford N K, Peters N A and Kwiat P G 2005 Phys. Rev. Lett. 95 260501
[24] Kwiat P G 1997 J. Mod. Opt. 44 2173–2184
[25] Cardano F, Karimi E, Slussarenko S, Marrucci L, de Lisio C and Santamato E 2012 Appl. Opt. 51 C1–C6
[26] Schemmel P, Pisano G and Maffei B 2014 Opt. Express 22 14712–14726
[81] Pan Z, Cai J and Wang C 2017
[82] Hamilton C S, Gábris A, Jex I and Barnett S M 2011 New J. Phys. 13 013015
[83] Innocenti L, Majury H, Giordani T, Spagnolo N, Sciarrino F, Paternostro M and Ferraro A 2017 Phys. Rev. A 96 062326
[84] Ibrahim A H, Roux F S, McLaren M, Konrad T and Forbes A 2013 Phys. Rev. A 88 012312
[85] Goyal S K, Boukama-Dzoussi P E, Ghosh S, Roux F S and Konrad T 2014 Sci. Rep. 4 4543
[86] Goyal S, Ibrahim A H, Roux F S, Konrad T and Forbes A 2014 Experimental orbital angular momentum based quantum key distribution through turbulence. preprint at arXiv:1412.0788
[87] Krenn M, Handsteiner J, Fink M, Erhard M, Huber M, Krenn M, Fickler R and Zeilinger A 2017 Proc. Natl. Acad. Sci. USA 114 14197–14201
[88] Hiesmayr B C, de Dood M J A and Loßler W 2016 Phys. Rev. Lett. 116 073601
[89] Malik M, Erhard M, Huber M, Krenn M, Fickler R and Zeilinger A 2016 New. Photon. 10 248–252
[90] Erhard M, Malik M and Zeilinger A 2017 Quantum Sci. Technol. 2 014001
[91] Fickler R, Campbell G T, Buchler B C, Lam P K and Zeilinger A 2014 Proc. Natl. Acad. Sci. USA 111 13642–13647
[92] Erhard M, Malik M, Krenn M and Zeilinger A 2017 Experimental ghe entanglement beyond quibits. preprint at arXiv:1708.03881
[93] Leonhard N, Sorelli G, Shatokhin V N, Reinlein C and Buchleitner A 2017 Phys. Rev. A 97 012321
[94] Jabir M V, Apurv Chaitanya N, Manoj Mathew V and Samanta G K 2017 Sci. Rep. 7 7331
[95] Fairas O J, D’Ambrosio V, Taballione C, Bisetso F, Slussarenko S, Aolita L, Marrucci L, Walborn S P and Sciarrino F 2015 Sci. Rep. 5 8424
[96] Vallone G, D’Ambrosio V, Sponselli A, Slussarenko S, Marrucci L, Sciarrino F and Villoresi P 2014 Phys. Rev. Lett. 113 060503
[97] Mirohosseini M, Magaña Loaiza O S, O’Sullivan M N, Rodenburg B, Malik M, Lavery M P J, Padgett M J, Gauthier D J and Boyd R W 2015 New J. Phys. 17 033033
[98] Lei T, Zhang M, Li Y, Jia P, Liu G N, Xu X, Li Z, Min C, Liu J, Yu C, Niu H and Yuan X 2015 Light Sci. Appl. 4 e257
[99] Wei S, Earl S K, Yuan X C, Kou S S and Lin J 2017 Active sorting of orbital angular momentum states of light with cascaded tunable resonators. preprint at arXiv:1704.01703
[100] Wang F X, Chen W, Yin Z Q, Wang S, Guo G C and Han Z F 2017 Phys. Rev. A 95 019903
[101] Pan Z, Cai J and Wang C 2017 Int. J. Theor. Phys. 56 2622–2634
[102] Sit A, Bouchard F, Fickler R, Gagnon-Bischoff J, Larocque H, Heshami K, Elser D, Peuntinger C, Günthner K, Heim B, Marquardt C, Leuchs G, Boyd R W and Karimi E 2017 Optica 4 1006–1010
[103] Mafu M, Dudley A, Goyal S, Giovannini D, McLaren M, Konrad T, Petruccione F, Lütkenhaus N and Forbes A 2013 Phys. Rev. A 88 032305
Venegas-Andraca SE 2012 Quantum Information Processing vol 11 (Springer US) chap Quantum walks: a comprehensive review, pp 1015–1106

Childs A M 2009 Phys. Rev. Lett. 102 180501

Do B, Stohler M L, Balasubramanian S, Elliott D S, Eash C, Fischbach E, Fischbach M A, Mills A and Zwickl B 2005 JOSA B 22 489–504

Broome M A, Fedrizzi A, Lanyon B P, Kassal I, Abouraddy A F, Di Giuseppe G, Christodoulides D N and Szameit A 2011 Nat. Photon. 5 197–204

Cardano F, D’Errico A, Dauphin A, Maffei M, Piccirillo B, Crespi A, Osellame R, Ramponi R, Giovannetti V, Fazio R, Sansoni L, De Nicola F, Sciarrino F and Mataloni P 2013 Nat. Photon. 7 322–328

Chiadis A M, Cleve R, Dorott E, Farhi E, Gutmann S and Spielman D A 2003 Exponential algorithmic speedup by a quantum walk Proceedings of the 35th ACM Symposium on Theory of Computing (STOC) pp 59–68

Chiadis A M 2009 Phys. Rev. Lett. 102 180501

Do B, Stohler M L, Balasubramanian S, Elliott D S, Eash C, Fischbach E, Fischbach M A, Mills A and Zwickl B 2005 JOSA B 22 489–504

Broome M A, Fedrizzi A, Lanyon B P, Kassal I, Abouraddy A F, Di Giuseppe G, Christodoulides D N and Szameit A 2011 Nat. Photon. 5 197–204

Cardano F, D’Errico A, Dauphin A, Maffei M, Piccirillo B, Crespi A, Osellame R, Ramponi R, Giovannetti V, Fazio R, Sansoni L, De Nicola F, Sciarrino F and Mataloni P 2013 Nat. Photon. 7 322–328

Chiadis A M, Cleve R, Dorott E, Farhi E, Gutmann S and Spielman D A 2003 Exponential algorithmic speedup by a quantum walk Proceedings of the 35th ACM Symposium on Theory of Computing (STOC) pp 59–68
[621] Walschaers M, Kuipers J, Urbina J D, Mayer K, Tichy M C, Richter K and Buchleitner A 2016 New J. Phys. 18 032001

[622] Olson J, Cao Y, Romero J, Johnson P, Dallaire-Demers P L, Sawaya N, Narang P, Kivlichan I, Wasielewski M and Aspuru-Guzik A 2017 Quantum information and computation for chemistry. preprint at arXiv:1706.05413

[623] Feynman R 1982 Int. J. Theor. Phys. 21 467–488

[624] Abrams D S and Lloyd S 1999 Phys. Rev. Lett. 83 5162–5165

[625] Aspuru-Guzik A, Dutoi A D, Love P J and Head-Gordon M 2005 Science 309 1704–1707

[626] Aspuru-Guzik A and Walther P 2012 Nat. Phys. 8 285–291

[627] Noh C and Angelakis D G 2016 Rep. Prog. Phys. 80 016401

[628] Lu C Y, Gao W B, Gühne O, Zhou X Q, Chen Z B and Pan J W 2009 Phys. Rev. Lett. 102 030502

[629] Pachos J K, Wieczorek W, Schmid C, Kiesel N, Pohlner R and Weinfurter H 2009 New J. Phys. 11 083010

[630] Lanyon B P, Whitfield J D, Gillett G G, Goggin M E, Almeida M P, Kassal I, Biamonte J D, Mohseni M, Powell B J, Barbieri M, Aspuru-Guzik A and White A G 2010 Nat. Chem. 2 106–111

[631] Kaltenbaek R, Lavoie J, Zeng B, Bartlett S D and Resch K J 2010 Nat. Phys. 6 850–854

[632] Ma X, Dakic B, Naylor W, Zeilinger A and Walther P 2011 Nat. Phys. 7 399–405

[633] Ma X S, Dakić B, Kropatschek S, Naylor W, Chan Y H, Gong Z X, Duan L M, Zeilinger A and Walther P 2014 Sci. Rep. 4 3583

[634] Santagati R, Wang J, Gentile A A, Paesani S, Wiebe N, McClean J R, Morley-Short S, Shadbolt P J, Bonneau D, Silverstone J W, Tew D P, Zhou X, O’Brien J L and Thompson M G 2018 Sci. Adv. 4 eaap9646