Journal of Physics B: Atomic, Molecular and Optical Physics

TUTORIAL

Quantum computing with photons: introduction to the circuit model, the one-way quantum computer, and the fundamental principles of photonic experiments

To cite this article: Stefanie Barz 2015 *J. Phys. B: At. Mol. Opt. Phys.* **48** 083001

J. Phys. B: At. Mol. Opt. Phys. **48** (2015) 083001 (25pp) doi:10.1088/0953-4075/48/8/083001

Tutorial

Quantum computing with photons: introduction to the circuit model, the one-way quantum computer, and the fundamental principles of photonic experiments

Stefanie Barz

Clarendon Laboratory, Department of Physics, University of Oxford, Parks Road, Oxford OX1 3PU, UK

E-mail: barz@physics.ox.ac.uk

Received 24 June 2014, revised 15 December 2014
Accepted for publication 30 December 2014
Published 20 March 2015

Abstract

Quantum physics has revolutionized our understanding of information processing and enables computational speed-ups that are unattainable using classical computers. This tutorial reviews the fundamental tools of photonic quantum information processing. The basics of theoretical quantum computing are presented and the quantum circuit model as well as measurement-based models of quantum computing are introduced. Furthermore, it is shown how these concepts can be implemented experimentally using photonic qubits, where information is encoded in the photons' polarization.

Keywords: quantum information, quantum computing, photonics

(Some figures may appear in colour only in the online journal)

1. Introduction

Over the last decades, the omnipresence of computers has revolutionized our lives in the dawn of a new information age. At the same time, computers have grown smaller and faster due to the miniaturization of transistors—the most basic computational element. A celebrated empirical trend, known as Moore's law, states that the number of transistors in a computer and thus its computing power doubles every two years. Obviously, this exponential growth cannot continue forever and at some point the basic building blocks of computers will reach a size where the laws of quantum physics become important. On the other hand, it has been realized that this seemingly-fundamental limitation opens up new possibilities for information processing and paves the way for a completely new kind of computing: the field of quantum computing.

Quantum computers are expected to play an important role in future information processing since they can outperform classical computers at many tasks. Their importance was realized as early as 1982 [1] when Feynman pointed out that they can simulate quantum systems, whose properties are too complex to be calculated with a classical computer. It was shown in the following decade that quantum computers are superior to classical computers in various tasks. One of the first algorithms to demonstrate an improvement over the classical analog was the Deutsch–Josza algorithm, which determines if a function is constant or balanced [2, 3]. While this algorithm has no direct application, it inspired the subsequent development of other algorithms like Shor's algorithm and Grover's algorithm which both provide a practical benefit. Shor's factoring algorithm facilitates the factorization of large numbers into their prime factors in polynomial time on a quantum computer [4], and Grover's algorithm enables searching in an unordered list with a quadratic speed-up compared to the classical case [5]. Recently, another quantum algorithm was invented which solves certain systems of linear equations with exponential speed-up compared to a classical computer [6, 7].

This tutorial aims for introducing the basic principles of quantum computing and their application in experiments with photonic systems. Photons allow the encoding of information in various degrees of freedom; here, we will mainly focus on polarization. Polarization-encoded systems are well-suited for quantum computing due to their low decoherence and the simple realization of single-qubit gates. The challenge in photonic quantum computing is the realization of two-qubit gates, which are necessary for universal quantum computing. While at first sight it seems that strong optical nonlinearities are required for realization of those gates, it was shown in 2001 that efficient quantum computing is possible using only linear optics, single-photon sources and detectors [8].

2. Outline

The tuturial is structured as follows. In section 3 the basic principles of theoretical quantum computing are presented. The quantum circuit model is introduced, where a computation is performed by a quantum circuit acting on quantum states. In section 4, measurement-based models of quantum computing are presented, where quantum information is processed by sequences of adaptive measurements. The one-way quantum computer, a special type of measurement-based quantum computer, is introduced, and it is shown that single-qubit measurements on highly-entangled resource states perform quantum computation. Further, it is presented how this concept can be applied to implement secure delegated quantum computations, a recently discovered feature of quantum computers. In section 5, the fundamental principles of photonic quantum computing are presented and it is shown how single-qubit and multi-qubit gates can be implemented experimentally using polarization-encoded systems. Furthermore, it is shown, how single photons can be generated experimentally. The section is concluded with an example of a photonic quantum computing experiment and it is shown how the introduced concepts can be applied in experiments. Finally, this tutorial ends with a conclusion and an outlook in section 6.

3. Quantum computing

This first section briefly reviews the basic elements of quantum computing. The fundamental units—the qubits—and the basic building blocks of a quantum computer—the quantum gates—are introduced. Furthermore, the circuit model, the most prominent circuit model of quantum computing, is introduced.

3.1. Classical bit versus quantum bits

The fundamental unit of a classical computer is a bit which can take binary values: zero or one. Quantum bits (qubits) are the quantum-mechanical analog of classical binary bits and can take infinitely many values. These qubits are quantum-mechanical states, which in experiments are represented by states of atoms, photons, nuclei, etc. A qubit can be described as a superposition of basis states, $|0\rangle$ and $|1\rangle$:

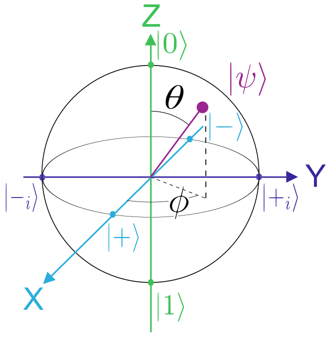


Figure 1. The Bloch sphere is used for the geometric visualization of qubits.

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle, \tag{3.1}$$

where α, β are complex numbers and $|\alpha|^2 + |\beta|^2 = 1$. The states $|0\rangle$ and $|1\rangle$ create an orthonormal basis of a Hilbert space and are often called computational-basis states [9].

Whereas it is possible to determine the state of a classical bit in one single measurement, a measurement in quantum mechanics gives a specific result only with a certain probability. If a measurement on the state $|\psi\rangle$ is performed, the outcome zero is obtained with the probability $|\alpha|^2$ and the result is one with the probability $|\beta|^2$. After the measurement, the qubit is in the state $|0\rangle$ or $|1\rangle$, depending on the outcome [10].

3.1.1. Representation on the Bloch sphere. The state $|\psi\rangle$ can be represented geometrically on a unit sphere in three dimensions (see figure 1), called the Bloch sphere [11]. For this, the state $|\psi\rangle$ can be rewritten in the following form:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + \mathrm{e}^{\mathrm{i}\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle. \tag{3.2}$$

In this representation, θ and ϕ are real numbers which correspond to the polar angle and the azimuthal angle, respectively. The description of quantum states as points on the Bloch sphere is useful for the visualization of single-qubits and operations on single-qubits.

The most frequently used states in quantum information lie on the axes of the Bloch sphere:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),\ |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{3.3}$$

on the x-axis,

$$|+_i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + \mathrm{i}\,|1\rangle),\ |-_i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - \mathrm{i}\,|1\rangle) \tag{3.4}$$

on the y-axis, and the basis states $|0\rangle$ and $|1\rangle$ lie on the z-axis.

If the qubits are written in a vector notation:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \tag{3.5}$$

it is easy to see that these states exactly correspond to the eigenvectors of the Pauli matrices:

$$\sigma_x = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = Y = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix},$$

$$\sigma_z = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{3.6}$$

3.1.2. Multi-qubit states. States of multiple qubits can be described using the same formalism. For two qubits, a set of four possible basis states is given by:

$$|00\rangle = |0\rangle \otimes |0\rangle, \tag{3.7}$$

$$|01\rangle = |0\rangle \otimes |1\rangle, \tag{3.8}$$

$$|10\rangle = |1\rangle \otimes |0\rangle, \tag{3.9}$$

$$|11\rangle = |1\rangle \otimes |1\rangle. \tag{3.10}$$

They form a basis for the product Hilbert space of the two qubits. A general two-qubit state can be written as a superposition of these four basis states:

$$|\psi\rangle = \alpha\, |00\rangle + \beta\, |01\rangle + \gamma\, |10\rangle + \delta\, |11\rangle, \tag{3.11}$$

where $|\,\alpha\,|^2 + |\,\beta\,|^2 + |\,\gamma\,|^2 + |\,\delta\,|^2 = 1$. Similar to the single-qubit case, a measurement gives a result (00, 01, 10, or 11) with certain probability, $|\,\alpha\,|^2$, $|\,\beta\,|^2$, $|\,\gamma\,|^2$, or $|\,\delta\,|^2$. However, a simple analog of the Bloch-sphere representation for multiple qubits is not known.

Two-qubit states that cannot be separated or be written as a product of two single-qubit state are called entangled [12]:

$$|\psi^-\rangle = \tfrac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \neq (\alpha\, |0\rangle + \beta\, |1\rangle) \otimes (\alpha' |0\rangle + \beta' |1\rangle). \tag{3.12}$$

An important set of entangled two-qubit states are the maximally-entangled Bell-states [13–15]:

$$|\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle), \tag{3.13}$$

$$|\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle). \tag{3.14}$$

These show strict correlations or anti-correlations and also form an orthonormal basis.

A general multi-qubit state, describing n qubits, can also be expressed in terms of state vectors:

$$|\psi\rangle = \sum_{i=1}^{2^n} \alpha_i\, |x_1 x_2 \ldots x_n\rangle, \tag{3.15}$$

with 2^n different probability amplitudes α_i, with $\sum_i |\alpha_i|^2 = 1$, and $x_i \in \{0, 1\}$.

3.1.3. Density operators. An alternate way to describe quantum states is with the density matrix formalism [16]. If a quantum system is in a state $|\psi_i\rangle$ with probability p_i, its density operator (or density matrix) is defined as:

$$\rho = \sum_i p_i\, \left|\psi_i\right\rangle\left\langle\psi_i\right|. \tag{3.16}$$

A quantum state is pure if $p_i = 1$ for only one i and all other p_j, $j \neq i$, are equal to zero. Whereas the state-vector formalism of the previous sections describes only pure states, i.e. systems that are with certainty in a state $|\psi_i\rangle$, density matrices can also represent mixed states.

General properties of the density operator are:

- ρ is trace-preserving: $\mathrm{Tr}\,(\rho) = 1$,
- ρ is positive semidefinite: $\rho \geqslant 0$ (meaning that the eigenvalues are non-negative), and
- ρ is self-adjoint: $\rho = \rho^\dagger$.

For completely mixed states, the density matrix becomes $\rho = 1/d\ \mathbf{I}_d$, where $\mathbf{I}_d$ is the d-dimensional identity matrix. This representation is not unique, meaning that different mixtures can lead to the same density matrix.

Mixed states of a single qubit can also be represented on the Bloch sphere as each density matrix can be rewritten as follows:

$$\rho = \frac{\mathbf{I} + \vec{r} \cdot \vec{\sigma}}{2}. \tag{3.17}$$

The Bloch vector $\vec{r}$ can be calculated from $\vec{r} = \mathrm{Tr}\,(\rho \cdot \vec{\sigma})$ with $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$. A state is pure and thus lies on the surface on the sphere, if and only if $\left|\vec{r}\right| = 1$. The Bloch vector of a general mixed state lies inside the sphere.

3.1.4. Measures for experiments. The density matrix of a quantum state can be used to analyze various properties of a state [12, 17]. In experiments, these properties are very useful for quantitatively verifying the quality of a quantum state.

A useful mean for the discrimination of pure and mixed state is the *purity* P which is defined via [18, 19]:

$$P = \mathrm{Tr}\left(\rho^2\right), \tag{3.18}$$

where Tr is the trace. $P = 1$ for pure states and $P < 1$ for mixed states. For a totally mixed state of dimension d, the purity is given by $1/d$.

The *fidelity* F of a general quantum state ρ determines how close that state is to a desired state. For a pure state $|\psi\rangle$ it is defined via:

$$F(\rho, |\psi\rangle) = \langle\psi|\,\rho\,|\psi\rangle. \tag{3.20}$$

The fidelity of two mixed states ρ and $\tilde{\rho}$ is given by [20]:

$$F\left(\rho, \tilde{\rho}\right) = \left(\mathrm{Tr}\left(\sqrt{\sqrt{\tilde{\rho}}\,\rho\,\sqrt{\tilde{\rho}}}\right)\right)^2. \tag{3.21}$$

Another way to quantify the mixedness of a quantum state is the measure of *entropy* which determines how much information is present when compared to the possible maximum [16]. The von Neumann entropy of a quantum state ρ is defined by:

$$S(\rho) = -\mathrm{Tr}\,\rho\,\log_2\rho = -\sum_i \lambda_i\,\log_2\lambda_i, \qquad (3.21)$$

where λ_i are the eigenvalues of ρ. The von Neumann entropy is zero for a pure state and equal to $\log_2(d)$ for a totally mixed state of dimension d.

For experiments, a more useful form is the linear entropy which can be calculated directly from the density matrix without the necessity of any diagonalization. It is directly related to the purity of a quantum state and obtained from the von Neumann entropy by approximating the logarithm with the first-order term of its Taylor expansion. The linear entropy is defined via

$$S(\rho) = \frac{d}{d-1}\left(1 - \mathrm{Tr}\left(\rho^2\right)\right) = \frac{d}{d-1}(1-P), \qquad (3.22)$$

and its values range from zero (pure state) to one (totally mixed state) [18, 19].

The density matrix can also be used to quantify the amount of entanglement of a state. One measure which is often used in experiments is the *concurrence* [21, 22]. The concurrence of a density matrix ρ of a two-qubit system is defined by:

$$C = \max\left(\sqrt{\lambda_1} - \sqrt{\lambda_2} - \sqrt{\lambda_3} - \sqrt{\lambda_4},\, 0\right), \qquad (3.23)$$

where λ_i are the eigenvalues of the matrix $\rho\tilde{\rho}$ in decreasing order with

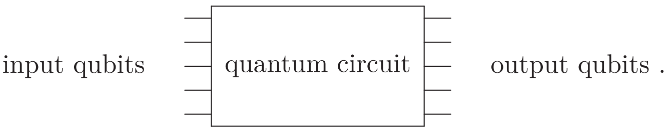
$$\tilde{\rho} = \left(\sigma_y \otimes \sigma_y\right)\rho^*\left(\sigma_y \otimes \sigma_y\right) \qquad (3.24)$$

and ρ^* being the complex conjugate of ρ.

The two-tangle τ, where $\tau = C^2$, is another value commonly used to characterize density matrices obtained experimentally [23].

3.2. The circuit model of quantum computation

The main components of a classical computer are the memory and the processor. Binary logic gates are carried out on classical bits; which and how many gates are used depends on the underlying program [9, 24]. In quantum physics, information is stored in the qubit and quantum logic gates acting on qubits can process the information, similar to classical information processing:



(3.25)

A comparison of the efficiency of both concepts shows that N input qubits can store 2^N (classical) amplitude coefficients. Information can thus be stored and obtained much more efficiently in a quantum circuit than in a classical circuit. The basic building blocks of a quantum circuit, single-qubit and two-qubit gates, are described in the next paragraph. As will be shown, only a few different types of gates or basic building blocks are necessary to build a universal quantum computer, meaning that it can be programmed to perform any computational task.

3.2.1. Single-qubit gates. A single qubit gate is a unitary operation U that takes a single qubit $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ as an input and transforms it into an output state $|\psi'\rangle = a'|0\rangle + b'|1\rangle$ with:

$$|\psi'\rangle = U\,|\psi\rangle. \qquad (3.26)$$

In the circuit formalism, this transformation is depicted as [25, 26]:

$$|\psi\rangle \;-\!\boxed{U}\!-\; |\psi'\rangle\,. \qquad (3.27)$$

The gate changes the amplitude coefficients, which can be seen when the transformation is written in form of a matrix:

$$\begin{pmatrix} a' \\ b' \end{pmatrix} = \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix}. \qquad (3.28)$$

The unitarity of the transformation follows from the fact that the norm must be preserved:

$$\langle\psi|\psi\rangle = \langle\psi'|\psi'\rangle = \langle\psi\,|U^\dagger U|\,\psi\rangle = 1 \rightarrow U^\dagger U = \mathbf{I}. \qquad (3.29)$$

From this it follows that all quantum gates are reversible [9, 24].

Important single-qubit gates in quantum computation are the Pauli operators σ_x, σ_y, and σ_z. Beyond that, there are three major gates, that are often used in quantum computing. The Hadamard gate H turns basis states into superposition states and vice versa:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \qquad (3.30)$$

A phase gate or S gate adds a phase of $\pi/2$ to the computational basis state $|1\rangle$:

$$S = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{i} \end{pmatrix}, \qquad (3.31)$$

and the T gate or $\pi/8$ gate:

$$T = \begin{pmatrix} 1 & 0 \\ 0 & \exp\,(\mathrm{i}\pi/4) \end{pmatrix} \qquad (3.32)$$

adds a phase of $\pi/4$ to the computational basis state $|1\rangle$ and enables universal quantum computing. Two useful algebraic identities are given by: $H = (X + Z)/\sqrt{2}$ and $S = T^2$.

All single-qubit gates can be represented geometrically on the Bloch sphere. The application of a X (Y, Z)-Pauli gate is equivalent to a rotation of π about the x (y, z)-axis of the Bloch sphere. Thus, the Pauli gates can generate rotations about the three axes of the sphere. For example, a rotation about the x-axis can be written as:

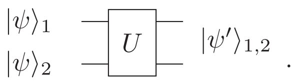
$$\begin{aligned} R_x(\theta) &= \exp\left(-\frac{\mathrm{i}\,\theta X}{2}\right) \\ &= \cos\left(\frac{\theta}{2}\right)\mathbf{I} - \mathrm{i}\,\sin\left(\frac{\theta}{2}\right)X, \end{aligned} \tag{3.33}$$

where similar equations also exist for Y and Z gates. Furthermore, a general rotation $R_{\hat{n}}(\theta)$ about an arbitrary axis $\hat{n} = (n_x, n_y, n_z)$ can be decomposed into Pauli gates [9]:

$$\begin{aligned} R_{\hat{n}}(\theta) &= \exp\left(-\frac{\mathrm{i}\,\theta\hat{n}\cdot\vec{\sigma}}{2}\right) \\ &= \cos\left(\frac{\theta}{2}\right)\mathbf{I} - \mathrm{i}\,\sin\left(\frac{\theta}{2}\right)\left(n_x X + n_y Y + n_z Z\right). \end{aligned} \tag{3.34}$$

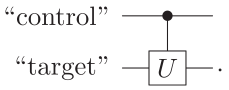
For example, the Hadamard gate can be created out of two different rotations, first a rotation of π about the z-axis, followed by a rotation of $\pi/2$ about the y-axis.

3.2.2. Multi-qubit gates and controlled operations. Multi-qubit gates take multiple qubits as input and perform operations on them. In the circuit formalism, this is depicted as [26]:



(3.35)

The operation can be conditioned on the state of one or more qubits. These qubits are called control qubits in contrast to the qubits on which the operation is performed, the target qubits. For example, a two-qubit controlled unitary operation (CU) applies a unitary operation U on the target qubit if the control is in the state $|1\rangle$:

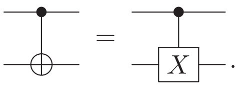


(3.36)

Important two-qubit gates for quantum computing are the controlled-NOT gate (CNOT or CX) and the controlled-phase gate (CPhase or CZ). Acting on two input qubits $|i\rangle$ and $|j\rangle$, $(i, j \in 0, 1)$, the CNOT gate performs the following operation:

$$\text{CNOT }|i\rangle|j\rangle = |i\rangle|i \oplus j\rangle, \tag{3.37}$$

where $\oplus$ is the binary addition. Thus, the state of the target qubit is changed from $|0\rangle$ to $|1\rangle$ (or vice versa) if the control qubit is in the state $|1\rangle$. In a quantum circuit, the CNOT gate is depicted by the symbol:

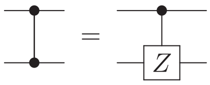


(3.38)

The CPhase gate also acts on two input qubits $|i\rangle$, $|j\rangle$ and performs the transformation:

$$\text{CPhase }|i\rangle|j\rangle = (-1)^{ij}|i\rangle|j\rangle. \tag{3.39}$$

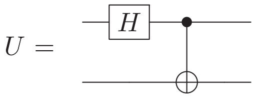
If the input qubits are in the state $|11\rangle$, they acquire a phase of -1. The symbol



(3.40)

is used in quantum circuits for the representation of CPhase gates.

These two gates are also called entangling gates, since they can perform entangling operations. For example, a quantum circuit consisting of a Hadamard gate and a CNOT gate:



(3.41)

can transform a product state $|xy\rangle$, $x, y \in \{0, 1\}$, into the following maximally entangled Bell states:

$$|00\rangle \xrightarrow{U} (|00\rangle + |11\rangle)/\sqrt{2} \tag{3.42}$$

$$|01\rangle \xrightarrow{U} (|01\rangle + |10\rangle)/\sqrt{2} \tag{3.43}$$

$$|10\rangle \xrightarrow{U} (|00\rangle - |11\rangle)/\sqrt{2} \tag{3.44}$$

$$|11\rangle \xrightarrow{U} (|01\rangle - |10\rangle)/\sqrt{2}\,. \tag{3.45}$$

3.2.3. Universal set of gates. Arbitrary multi-qubit gates can be generated by a universal set of single- and multi-qubit gates. A widely-used set of gates consists of the CNOT gate, the Hadamard gate and the $\pi/8$ gate. Using only these three gates, any computation can be realized. In more detail: any unitary operation can be approximated to arbitrary accuracy using only these gates [9, 24, 26–29]. Here, also other non-trivial phase gates can in principle be used instead of the $\pi/8$ gate. Another universal set of gates is, for example, the set of all single-qubit gates, together with a CNOT gate.

This statement has particular importance to experimental efforts. If this gate set can be physically implemented and the gates arbitrarily concatenated, it will thereby be possible to physically realize any unitary transformation.

4. Measurement-based models

In the circuit model, which is described in the previous section, quantum information is processed by applying quantum gates, which realize a coherent unitary evolution [30]. In contrast, in measurement-based models, quantum information is processed by sequences of adaptive measurements [31, 32]. Among measurement-based models there are two different approaches: the teleportation-based model [33], which is based on Bell-pairs and two-qubit measurements, and the one-way model which consists of highly-entangled multi-particle states and single-qubit measurements. Both models are equivalent [34]; it can be shown that they are conceptually closely related and rely on the same primitives [34–38]. In general, measurement-based quantum computing (MBQC) is related to different fields of physics, for example

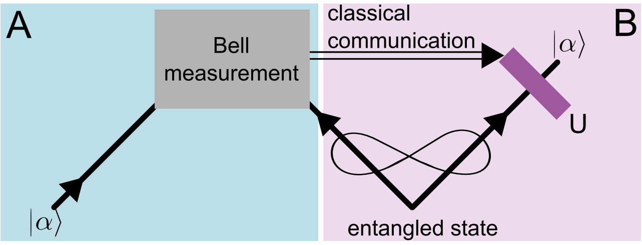


Figure 2. The figure illustrates the principle of quantum teleportation. Alice and Bob share an entangled state. Alice performs a so-called Bell-state measurement on the state $|\alpha\rangle$ and her half of the entangled state. This Bell-state measurement projects the input states onto one of the four Bell states. Alice shares the outcome of this measurement with Bob via a classical communication channel and Bob chooses the unitary operation U accordingly (details see text). After applying the operation U to his half of the entangled state, Bob's qubit is in state $|\alpha\rangle$.

entanglement theory, topology, graph theory, and mathematical logic [39].

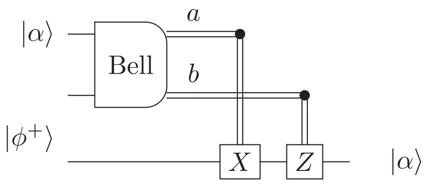
4.1. Teleportation-based quantum computing

The teleportation-based model uses teleportation [33, 40] as a way to realize unitary transformations. Historically, the field started with the invention of the Gottesman–Chuang teleportation trick, described below. This trick lead to the invention of a variety of teleportation-based concepts. Furthermore, it is the basis of a landmark paper in the field of photonic quantum computing which shows that limitations in photonic quantum computing due to missing interactions in photonic systems can be overcome [8].

4.1.1. Quantum teleportation. The aim of quantum teleportation is to send a quantum state $|\alpha\rangle$ from A (Alice) to B (Bob), where A and B can be far apart, and Alice is only allowed to transmit classical information to Bob [33, 40]. Furthermore, Alice does neither know the quantum state, nor can she determine it since she holds only a single copy. Teleportation enables Alice to send the state $|\alpha\rangle$ to Bob, by utilizing an entangled photon pair and classical communication. The basic principle of quantum teleportation is depicted in figure 2.

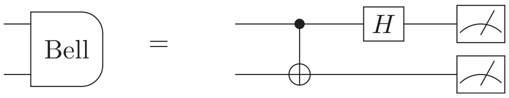
It is important to note that quantum teleportation does not allow faster-than-light communication. The teleportation protocol requires Alice to send classical information to Bob. This process is clearly limited by the speed of light.

In more detail, the quantum circuits that accomplishes the teleportation of a state $|\alpha\rangle$ is the following:

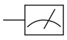


(4.1)

Here, the double lines carry classical bits and the box 'Bell' represents a Bell-state measurement, which determines the values of a and b:

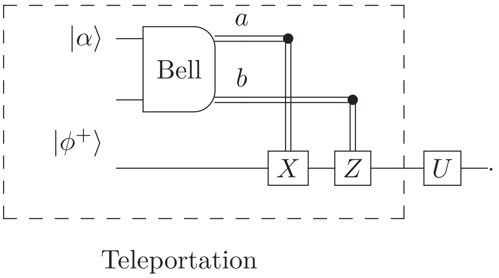


(4.2)

The measurement symbol  on the right of this circuit denotes a measurement in the computational basis. If the qubits are found to be in the state $(|00\rangle + |11\rangle)/\sqrt{2}$, then the output is $a = b = 0$ (for the state $(|01\rangle + |01\rangle)/\sqrt{2}$, it is $a = 1, b = 0$; for the state $(|00\rangle - |11\rangle)/\sqrt{2}$: $a = 0, b = 1$; and for the state $(|01\rangle - |01\rangle)/\sqrt{2}$: $a = b = 1$). These classical outputs determine whether additional Pauli gates need to be applied to the teleported state (the unitary U in figure 2) in order to obtain the state $|\alpha\rangle$.

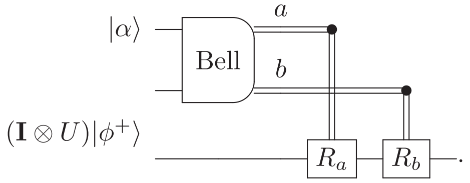
4.1.2. The Gottesman–Chuang teleportation trick. In 1999, Gottesman and Chuang published a 'teleportation' trick which enables universal quantum computation using only single-qubit operations, Bell-basis measurements and entangled states as resources [41]. Their scheme—also known as teleporting a state 'through' a unitary operation—is a generalization of quantum teleportation and reduces the required resources [41]. Instead of directly applying a gate to a state, that state is teleported using a modified resource as compared to the original teleportation protocol [33, 40].

In more detail, an operation U can either be applied to a state $|\alpha\rangle$, or that state $|\alpha\rangle$ can be teleported using the modified Bell state $(\mathbf{I} \otimes U)|\phi^+\rangle$ as a resource, which leads to the same output up to local Pauli corrections. The following circuit shows a state $|\alpha\rangle$ which is first teleported (dashed box, describes in the previous section) and then experiences a unitary gate U:



(4.3)

This is equivalent to the following circuit, where the unitary operation is absorbed in the entangled resource state:



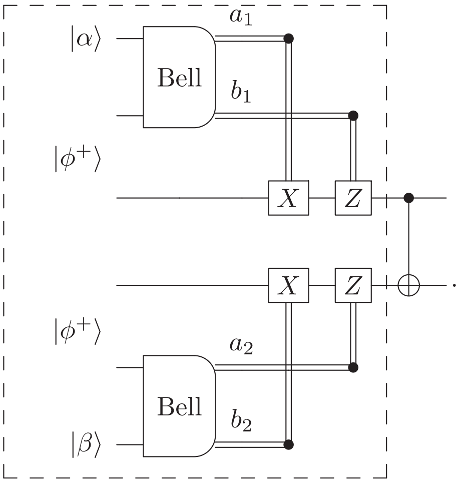
(4.4)

For example, the unitary U could be a Hadamard gate and instead of applying this gate directly to the state $|\alpha\rangle$, one teleports $|\alpha\rangle$ using a modified resource $(\mathbf{I} \otimes H)|\phi^+\rangle = (|0+\rangle + |1-\rangle)/\sqrt{2}$.

The advantages of this method are obvious: instead of performing operations on unknown states, it is just necessary to construct known states as offline resources. The operation

U could be a logic gate that is difficult to implement, but the creation of the resource state might be much easier. Furthermore, it is no longer necessary to perform probabilistic gates.

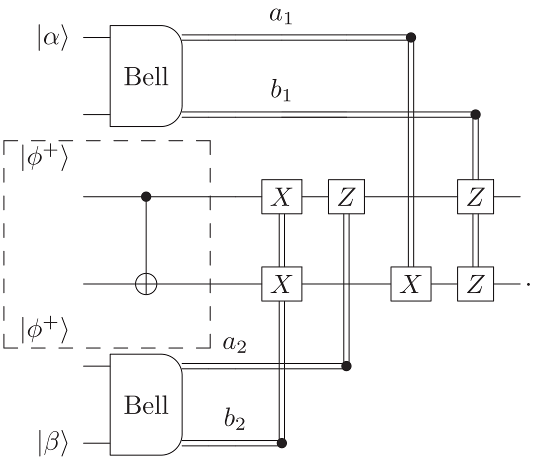
The advantage of this teleportation trick becomes even more obvious in the case of multi-qubit gates like the CNOT gate. Applying the gate to two qubits $|\alpha\rangle|\beta\rangle$ is equivalent to absorbing it in the preparation of the resource state. If the state $|\alpha\rangle|\beta\rangle$ is first teleported and then the CNOT gate is applied, after implementing corrections dependent on the Bell measurement outcome, we obtain:



(4.5)

Two teleportations

This is again equivalent to the following circuit, where the CNOT gate is absorbed in the resources and which leads to the same output state CNOT $|\alpha\rangle|\beta\rangle$:



(4.6)

Absorption of the CNOT gate
in the resources

The resource state CNOT $|\phi^+\rangle|\phi^+\rangle$ can for example be created out of two three-qubit Greenberger–Horne–Zeilinger (GHZ) states; where an n-qubit GHZ state is an entangled quantum state of the form $|\mathrm{GHZ}\rangle = (|0\rangle^{\otimes n} + |1\rangle^{\otimes n})/\sqrt{2}$.

The Gottesman–Chuang scheme was very important for the invention of teleportation-based concepts and for the development of quantum computing with linear optics since their requirements—GHZ states, Bell measurements, teleportation, and single-qubit measurements—are easily realizable in optical experiments.

4.1.3. The Knill–Laflamme–Milburn (KLM) scheme. In their seminal paper in 2001, KLM showed that efficient quantum computation is possible using only beam splitters, phase shifters, single-photon sources and photo-detectors [8].

For many years, it was strongly believed that quantum computing with only linear optics is not possible due to the missing interaction between photonic qubits and the resulting lack of entangling gates. KLM revolutionized linear-optics quantum computing (LOQC) by developing an efficient scheme based on the Gottesman–Chuang teleportation trick. They took advantage of the fact that there is a hidden nonlinearity in the photon detection process and transferred this nonlinearity to the qubits via measurements to enable universal computing.

In their paper [8], they first show that non-deterministic quantum computation is possible with linear optics. For this demonstration, they use dual-rail encoded qubits, where the information is stored in the photon number of an optical mode. They show that a non-deterministic sign change, dependent on the photon number, is possible:

$$\alpha_0\,|0\rangle + \alpha_1\,|1\rangle + \alpha_2\,|2\rangle \rightarrow \alpha_0\,|0\rangle + \alpha_1\,|1\rangle - \alpha_2\,|2\rangle. \quad (4.7)$$

Their gate—the so-called NS gate—just requires photon counters that are able to count the number of photons in one mode. Applying the NS gate twice, they can achieve an entangling gate—a conditional sign flip—with a success probability of 1/16 through projective measurements. Figure 3 shows the basic principle of the NS gate and how to use it in order to achieve a conditional sign flip. A detailed description of the NS gate and the KLM scheme in general can be found in [42] or in [43].

By using a generalized, near-deterministic form of teleportation and by applying the Gottesman–Chuang teleportation trick, they further show that this success probability can be increased to $n^2/(n + 1)^2$ with $2n$ ancilla qubits. Here, it is important to note that a complete Bell state measurement is impossible for photonic qubits encoded in one degree of freedom (see [44] for Bell-state measurements using hyper-entanglement and [45] for a review on Bell-state measurements). This is the reason for the use of the $2n$ ancilla qubits, which enable near-deterministic teleportation. Thus, an arbitrarily high success probability is possible at the cost of ancillary resources—the more ancilla qubits, the higher the success—which makes the scheme quite resource-intensive. Their final and main result, robust LOQC being possible with polynomial resources, provides practical scalability of photonic quantum computing experiments [46].

Often, the KLM model of quantum computing is referred to as the photonic quantum circuit model. However, a closer look reveals that although the KLM model superficially resembles the circuit model, it is still a measurement-based scheme [47]. The KLM scheme is based on entangled ancilla photon pairs and thus provides entanglement from the very beginning. The photons do not interact as in standard circuit models, but the interaction is created via the application of a

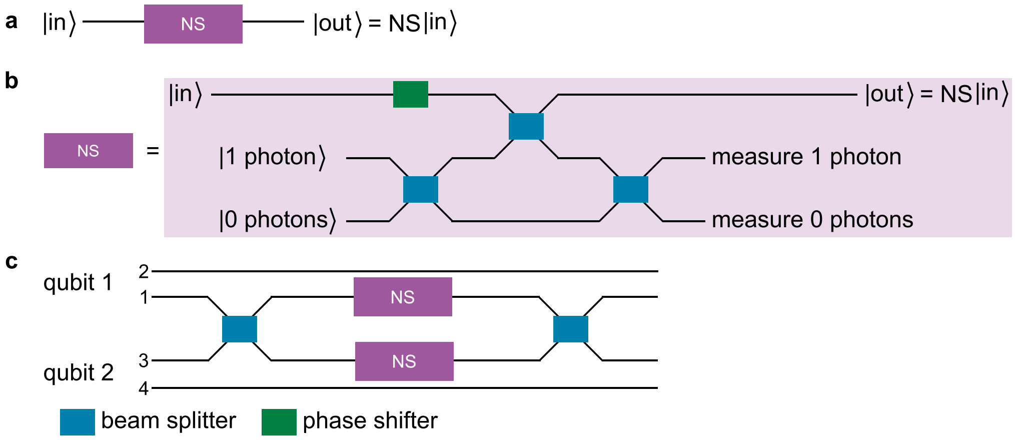


Figure 3. The basic principle of the NS gate and how to use it for conditional sign flips. (a) The NS gate realizes a non-deterministic phase shift NS on one mode. (b) It is implemented by using additional modes and a network of phase shifters and beam splitters. A phase shifter adds a phase of $e^{i\phi}$ to an optical mode, a beam splitter splits an incidents beam into two parts (see section 5.2 for a full mathematical description) and adds phases to the output modes. The ratio of transmission and reflection of the beam splitter and the phases, acquired from the phase shifter and the beam splitter, determine the phase shift NS. For certain settings [8], one can achieve that a phase shift of NS = −1 for the case of two photons entering the input, $|\text{in}\rangle = |2\rangle$ and thus obtain the operation $\alpha_0\,|0\rangle + \alpha_1\,|1\rangle + \alpha_2\,|2\rangle \rightarrow \alpha_0\,|0\rangle + \alpha_1\,|1\rangle - \alpha_2\,|2\rangle$. The phase shift has been applied successfully to the upper mode, if one and zero photons have been registered in the ancilliary mode, respectively. (c) The NS gate can be used to implement a conditional phase shift. Two qubits are encoded into four spatial modes, 1, 2, 3 and 4, respectively. If modes 1 and 3 both contain a photon, $|11\rangle_{13}$, the state after the beam splitter will be $|02\rangle_{13} + |02\rangle_{13}$ and the NS gates will add a phase of '−1' to that state. After the second beam splitter, the state will then be $-|11\rangle_{13}$. If no or only one photon enter the modes 1 and 3, no phase shift will be applied.

teleportation-based scheme. Consequently, the KLM scheme for quantum computing is a truly teleportation-based and thus a measurement-based scheme.

4.2. One-way quantum computer

The basis of the one-way quantum computer is a highly-entangled resource state. Single-qubit measurements on that state enable the processing of quantum information [30–32]. The computational power of the one-way model is strongly related to the properties of the underlying resource state. It is required that every possible quantum state can be created out of the resource state just by single-qubit measurements. Since single-qubit measurements cannot create entanglement, also entanglement must be included in the resource state itself. Possible resource states for this task are graph states in the form of different two-dimensional (2D) lattices [48, 49].

4.2.1. Graph states. A graph state is a multi-qubit quantum state which can be represented by a mathematical graph $G(V, E)$ with vertices V and edges E. The vertices of a graph state correspond to the physical qubits whereas the edges indicate an entangling operation between the qubits.

Mathematically, a graph state can be described in the stabilizer language, which was invented by Gottesman [43, 49, 50]. For every vertex a of a graph, an operator S_a can be defined:

$$S_a := \sigma_x^a \prod_{b\in N_a} \sigma_z^b, \tag{4.8}$$

where N_a are all vertices in the neighborhood of vertex a. The corresponding graph state $|G\rangle$ is defined as the unique eigenstate with eigenvalue +1 for all stabilizer operators:

$$S_a\,|G\rangle \;=\; +|G\rangle. \tag{4.9}$$

The resource state for the one-way quantum computer is special kind of graph state, known as cluster state, where the underlying graph forms a 2D lattice. A graph or cluster state can be created by preparing a qubit in the $|+\rangle$ state for each vertex and using CPhase gates to entangle each pair of qubits which should be connected by an edge as nearest neighbors (see figure 4).

The choice of nearest-neighbor two-qubit interactions defines the structure of the cluster state, which determines the basic type of quantum circuit it can implement. Different graph states and cluster states are shown in figure 5. Certain families of cluster states (combined with single-qubit measurements and feed-forward) comprise a set of resources sufficient for universal quantum computing.

4.2.2. One-way computation. A computation in the one-way model is described by a sequence of consecutive single-qubit measurements and a feed-forward protocol. The basic principle of one-way computation is depicted in figure 6.

Measuring a qubit of a one-dimensional cluster state in the basis:

$$\left|+_\phi\right\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle + e^{i\phi}\,|1\rangle\Big) \tag{4.10}$$

has the effect of applying the single-qubit rotation $R_z(-\phi) = \exp\,(i\phi\sigma_z/2)$ on an encoded qubit in the cluster up to a Hadamard operation.

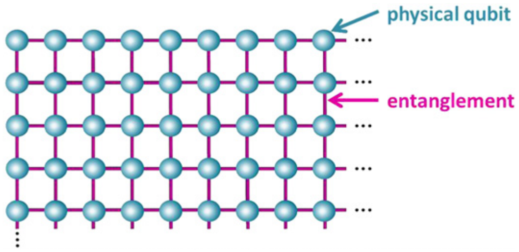
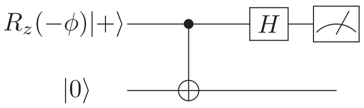


Figure 4. General cluster state, where the blue circles denote the physical qubits and the edges between the qubits denote entanglement.

Measuring a qubit in the computational basis $|0\rangle$ or $|1\rangle$ disconnects the qubits from the cluster and deletes all affected edges.

In the case where the outcome is found to be zero, the computation is correct, however if the outcome is found to be one, a Pauli error is introduced. This error is corrected by applying a feed-forward mechanism that compensates for the known errors by adapting further measurement angles [51].

In the following, I will describe in more detail how a measurement on an entangled state leads to a computation; the derivation follows [52]. Starting with a simple teleportation circuit, an input state $R_z(-\phi)|+\rangle$ is teleported to the output up to a local Pauli correction [52]:



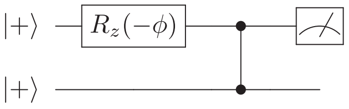
measurement in basis σ_z with outcome "m"

$$|\text{out}\rangle = Z^m R_z(-\phi)|+\rangle \ . \tag{4.11}$$

The CNOT gate can be transformed to a CPhase gate applying the relation

$$\text{CNOT} = \left(\mathbf{I} \otimes H\right)\text{CPhase}\left(\mathbf{I} \otimes H\right). \tag{4.12}$$

Additionally, the rotation $R_z(-\phi)$ can be implemented within the circuit and all Hadamard gates can be absorbed in the measurement basis or the target input qubit, which leads to the following circuit:



measurement in basis σ_x with outcome "m"

$$|\text{out}\rangle = HZ^m R_z(-\phi)|+\rangle \tag{4.13}$$

with

$$|\text{out}\rangle = HZ^m R_z(-\phi)|+\rangle = X^m H R_z(-\phi)|+\rangle. \tag{4.14}$$

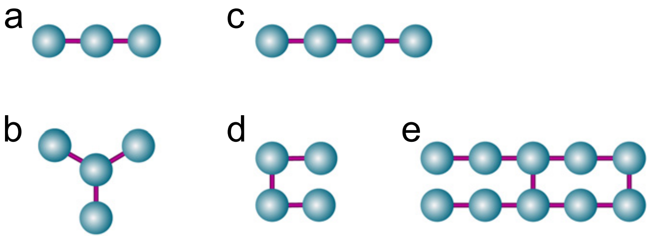
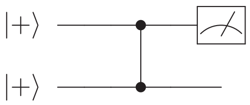


Figure 5. The figure shows different graphs states. (a) A three-qubit entangled state. (b) A four-qubit GHZ state. (c) A four-qubit cluster state. GHZ and cluster states have different entanglement structures and cannot be converted into each other by local operations. For the case of three qubits, shown in (a), the three-qubit GHZ and the three-qubit cluster state are the same. (d) The horseshoe cluster state is a two-dimensional cluster state and allows for the generation of two-qubit logic gates. (e) The brickwork state is universal resource for measurement-based quantum computing.

The rotation $R_z(-\phi)$ in the upper wire commutes with the CPhase gate and thus can also be absorbed in the measurement basis, leading to a general measurement in the X–Y plane of the Bloch sphere:



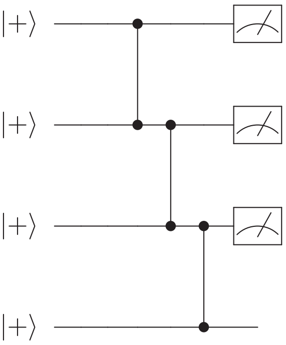
measurement in basis $|+_\phi\rangle$ with outcome "m"

$$|\text{out}\rangle = X^m H R_z(-\phi)|+\rangle \ . \tag{4.15}$$

A measurement in the basis $|\pm_\phi\rangle$ leads to a rotated output qubit up to a Pauli X correction depending on the measurement outcome. Thus single-qubit measurements can implement general $HR_z(\phi)$ rotations. These are sufficient to implement arbitrary single-qubit rotations, since every rotation can be decomposed into rotations about the x-axis and the z-axis using the Euler angles, $R_z(\gamma)\ R_x(\beta)\ R_z(\alpha)$. By applying the relations $H^2 = \mathbf{I}$ and $HR_z(\phi)\ H = R_x(\phi)$, the Euler angles can be rewritten in terms of single-qubit rotations R_z:

$$R_z(\gamma)R_x(\beta)R_z(\alpha) = H\left(HR_z(\gamma)\right)\left(HR_z(\beta)\right)\left(HR_z(\alpha)\right). \tag{4.16}$$

In order to obtain such a general rotation, single-qubit teleportations can simply be concatenated:



measurement in basis $|+_\alpha\rangle$ with outcome "k"

measurement in basis $|+_\beta\rangle$ with outcome "l"

measurement in basis $|+_\gamma\rangle$ with outcome "m"

$$|\text{out}\rangle \ . \tag{4.17}$$

The output state is equal to

$$|\text{out}\rangle = X^m HR_z(-\gamma)X^l HR_z(-\beta)X^k HR_z(-\alpha)|+\rangle \tag{4.18}$$

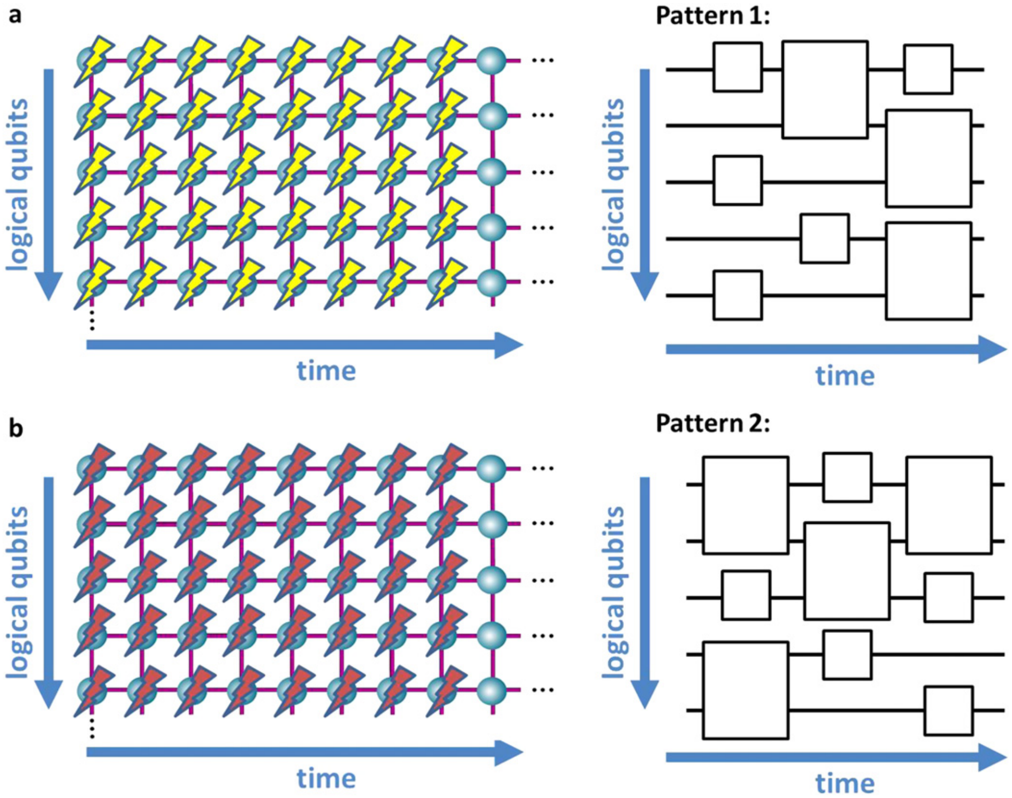
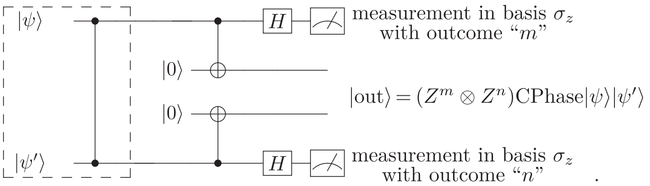


Figure 6. Principle of one-way computation. The pattern of single-qubit measurements on the cluster state determines the quantum circuits that is implemented. The figure illustrates how two different measurement patterns (yellow and red) on the same cluster state can lead to two different circuits. In order to implement such a pattern, one usually starts measuring the qubits from the left side of the cluster state and the continues to the right. This figure also illustrates the differents between the horizontal and vertical lines in the cluster state. The horizontal lines represent the logical qubits and the vertical lines are used to implement entangling gates between these qubits.

$$= X^m Z^l X^k H R_z\Big((-1)^l\gamma\Big) R_x\Big((-1)^k\beta\Big) R_z(-\alpha)|+\rangle, \qquad (4.19)$$

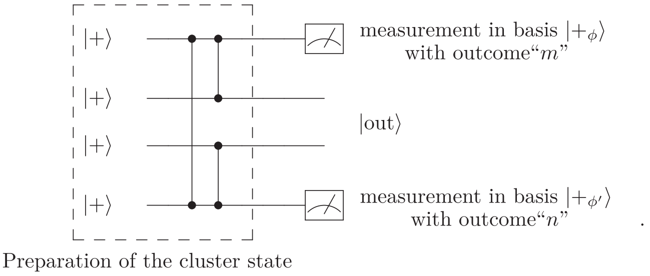
where the Pauli corrections were commuted through all rotations to the left. The dependency of the measurement bases on previous measurement outcomes also defines a temporal direction of the computation.

Up to now, only one-dimensional cluster states were introduced, which can still be simulated efficiently classically [53]. For universal quantum computing, 2D cluster states and two-qubit gates such as the CPhase gate are necessary. These CPhase gates can be implemented via vertical lines in the cluster state. This can be illustrated with the following circuit where an entangled input state CPhase $|\psi\rangle|\psi'\rangle$ is teleported up to local Pauli corrections combining two single-qubit teleportation circuits (here, the entangling CPhase gate is shown in the dashed box as part of the circuit):


$|\psi\rangle$
$|0\rangle$
$|0\rangle$
$|\psi'\rangle$
H
H
measurement in basis σ_z with outcome "m"
$|\text{out}\rangle = (Z^m \otimes Z^n)\text{CPhase}|\psi\rangle|\psi'\rangle$
measurement in basis σ_z with outcome "n"

(4.20)

Using the same transformations as in the above single-qubit teleportation and defining the input as $|\psi\rangle = R_z(-\phi)|+\rangle$ and $|\psi'\rangle = R_z(-\phi')|+\rangle$ converts the circuit into the following:


$|+\rangle$
$|+\rangle$
$|+\rangle$
$|+\rangle$
measurement in basis $|+_\phi\rangle$ with outcome"m"
$|\text{out}\rangle$
measurement in basis $|+_{\phi'}\rangle$ with outcome"n"
Preparation of the cluster state

(4.21)

This circuit prepares a cluster state (dashed box), the horseshoe cluster state shown in figure 5(e), by applying CPhase gates to qubits in a state $|+\rangle$. Subsequent measurements, specifically in the $|+_\phi\rangle$ basis ($|+_{\phi'}\rangle$ basis) for the upper (lower) qubit, perform a computation on these encoded qubits. The remaining qubits are in the output state:

$$|\text{out}\rangle = \big(H \otimes H\big)\big(Z^m \otimes Z^n\big) \times\Big(R_z(-\phi) \otimes R_z(-\phi')\Big)\text{CPhase}\,|+\rangle|+\rangle \qquad (4.22)$$

$$= \big(X^m \otimes X^n\big)\big(H \otimes H\big) \times\Big(R_z(-\phi) \otimes R_z(-\phi')\Big)\text{CPhase}\,|+\rangle|+\rangle. \qquad (4.23)$$

This confirms that the vertical lines in cluster states lead to the generation of entangling gates on the encoded qubits. If the underlying cluster state is large enough, any possible quantum computation can be performed.

4.2.3. Local complementation. Different types of graphs can be transformed into each other by applying a set of local operations. Experiments which can only prepare a restricted set of states thus have access to a much larger variety of states by simply applying local gates. This is a very useful procedure since it easily enables the preparation of a set of quantum states and thus the realization of different quantum algorithms.

The *local complementation* procedure is a simple graph transformation rule which utilizes a local Clifford operation on a quantum state to effect a transformation of its associated graph [49, 54, 55]. A Clifford operation maps a Pauli operator to the same or another Pauli operator; or, in other words, the Clifford group consists of all unitary operators which map the Pauli group to the Pauli group under conjugation.

A transformed graph or, more precisely, the local complement of a graph G at a vertex a, $\tau_a(G)$, can be obtained by complementing the neighborhood N_a of a; the neighborhood N_a of a consists of all vertices which are connected to a [49]:

$$\tau_a(G) := G + N_a. \tag{4.24}$$

In other words, all edges between the vertices of the neighborhood of a vertex a are erased; if there are unconnected vertices, new edges are created between them (see figure 7).

The corresponding action on the graph state is described by the local *complementation rule*: a graph state $|\tau_a(G)\rangle$ equivalent to a state $|G\rangle$ under local Clifford transformations $U_a^\tau(G)$ is obtained by local complementation of a graph G at a vertex a:

$$|\tau_a(G)\rangle = U_a^\tau(G)|G\rangle. \tag{4.25}$$

The transformation $U_a^\tau(G)$ is defined by:

$$U_a^\tau(G) = \sqrt{-\mathrm{i}\sigma_x^a}\sqrt{-\mathrm{i}\sigma_z^{N_a}}. \tag{4.26}$$

Here, the operator

$$\sqrt{-\mathrm{i}\sigma_x^a} = \exp\left[-\mathrm{i}\pi/4 \cdot \sigma_x^a\right] \tag{4.27}$$

transforms the qubit at vertex a and the operator

$$\sqrt{-\mathrm{i}\sigma_z^{N_a}} = \exp\left[-\mathrm{i}\pi/4 \cdot \sigma_z^{N_a}\right] \tag{4.28}$$

transforms all neighboring vertices.

If two graph states can be related by a series of local complementations, they are equivalent under local Clifford transformations. Interestingly, it was proven that two graph states that are equivalent under general local unitary transformations are not necessarily equivalent under local Clifford operations [56].

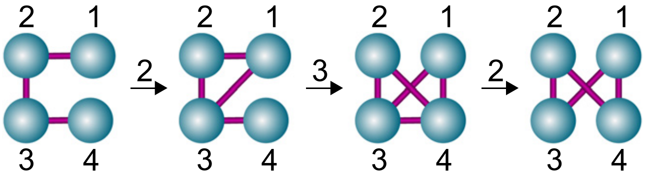


Figure 7. Example of a local complementation (LC) procedure. In the first step, LC on vertex 2 creates an edge between vertices 1 and 3. LC on vertex 3 then deletes the edge between the vertices 1 and 2 and creates a new edge between the vertices 1 and 4 and between vertices 2 and 4. The final LC on vertex 2 then deletes the edges between the vertices 3 and 4.

4.3. Comparison of the different quantum computing models

At first sight, the teleportation-based model and the one-way quantum computer seem to be very different models of quantum computing. Figure 8 provides a schematic overview of both models and their characteristics [35–37, 47, 57].

Teleportation-based quantum computation, which arose from the ideas of Gottesman and Chuang [41] and KLM [8], relies on teleportation using bipartite entangled pairs and two-qubit measurements. In some aspects, it is similar to the standard circuit model: interactions are required during the performance of the algorithm, and no actions are performed unless a non-identity gate is applied.

This is different from the one-way quantum computer [31, 32] where no quantum interactions are required after the preparation of the multi-partite entangled resource (the cluster state). The cluster state itself is independent of the computation, which is performed by single-qubit measurements on the cluster state. The one-way model also presents a paradigm shift in the theory of quantum computing since it is the only model which clearly separates the quantum and the classical parts of a computation.

However, both models are measurement-based models and it can be shown that the underlying principle is one-bit teleportation [37]. In this framework, deterministic quantum computations can be performed up to local Pauli corrections [36]. Both models have the same efficiency and are polynomial-time equivalent to the circuit model [32], solving the same class of problems.

There exist not only pure teleportation-based or one-way models, but also a variety of schemes which combine properties of both. These hybrid models were mostly invented to overcome the enormous resource requirements of the original methods [43, 58–63].

4.4. An application: blind quantum computing (BQC)

Recently, a new application of MBQC was invented [64]. It was shown that quantum computers [1, 3–5], besides offering substantial computational speedups, are also expected to preserve the privacy of a computation [64–69] as manifested in the BQC protocol [64].

This security is a new aspect of quantum computers which enables a client to delegate a quantum computation to a server such that the user's data and the whole computation remain perfectly private (see figure 9). The quantum server

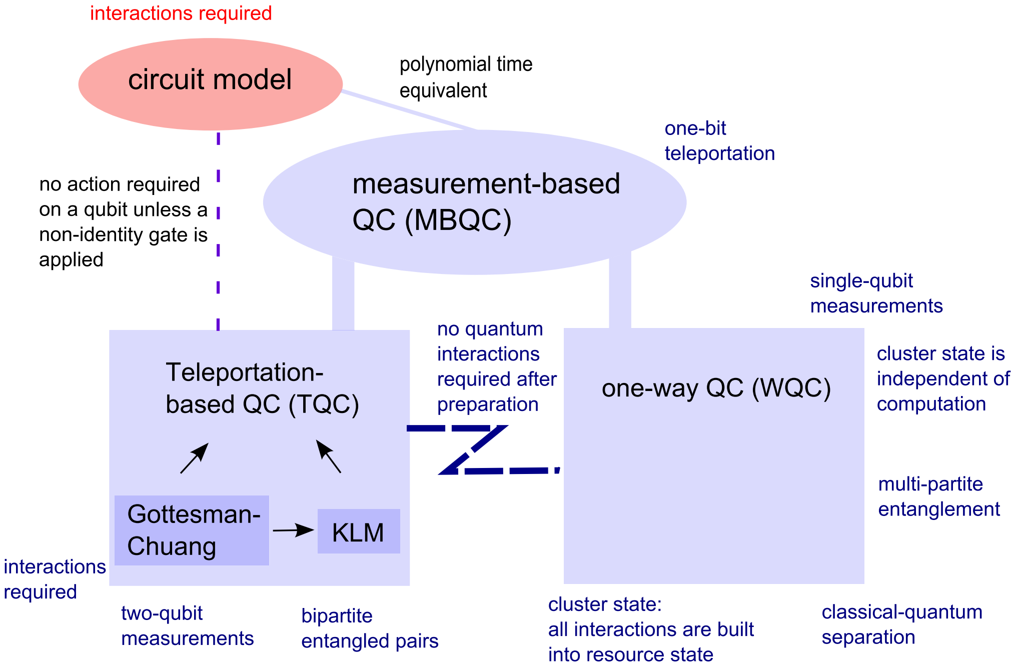

interactions required
circuit model
polynomial time equivalent
one-bit teleportation
measurement-based QC (MBQC)
no action required on a qubit unless a non-identity gate is applied
single-qubit measurements
Teleportation-based QC (TQC)
no quantum interactions required after preparation
one-way QC (WQC)
cluster state is independent of computation
Gottesman-Chuang
KLM
multi-partite entanglement
interactions required
two-qubit measurements
bipartite entangled pairs
cluster state: all interactions are built into resource state
classical-quantum separation

Figure 8. Comparison of different measurement-based models of quantum computing.

performs calculations, but has no means to find out what it is doing—it knows neither the input nor the output of the computation and cannot infer what is actually being calculated. Remarkably, the only quantum power that is required from the client is the preparation of single qubits and their transmission to the server.

The BQC protocol [64] is in detail explained in figure 10 and uses the concept of one-way quantum computing [30–32, 72, 73].

Reference [70] shows the implementation of an optimized version of the original protocol [64] using photonic qubits. Photons are ideally suited for BQC as they provide the natural choice as quantum information carrier for the client and enable quantum computing for the server. Further, it was shown, that the concept of BQC allows testing if a quantum computation was performed correctly [74], which has also been demonstrated experimentally [7].

5. Optical quantum information processing

Experimental implementations of quantum computing have been realized in many systems including photons [46, 51, 70, 75–79], ions [80–88], atoms [89–91], nuclear magnetic resonance [92–95], superconducting systems [96–103], and solid state systems [104–106]. Each system displays very particular advantages. Photonic qubits are especially well-suited for quantum information processing as they show low decoherence and can be easily transmitted over large distances. Furthermore, photonic states can be manipulated with very high precision and photonic systems are among the fastest systems available for quantum information processing [43, 107, 108].

All those properties make photons ideal carriers of information and have led to a variety of photonic experiments ranging from quantum computing, quantum simulation, and quantum communication to the foundations of quantum mechanics [108, 109].

5.1. Photonic qubits and quantum gates

There are different ways to encode information in photonic qubits, for example path or polarization [107, 108]. Here, we focus on the polarization degree of freedom, where a photonic qubit can be defined as:

$$|0\rangle = |H\rangle, \tag{5.1}$$

$$|1\rangle = |V\rangle, \tag{5.2}$$

where $|H\rangle$ denotes horizontal polarization and $|V\rangle$ denotes vertical polarization.

A convenient way to treat polarization states is the Jones formalism—a matrix formalism describing polarization by a 2D polarization vector $\vec{J}$ [110]:

$$\vec{J} = \begin{pmatrix} a_H \exp\left(\mathrm{i}\phi_H\right) \\ a_V \exp\left(\mathrm{i}\phi_V\right) \end{pmatrix}, \tag{5.3}$$

where a_H and a_V denote the amplitude of the wave vector in the horizontal and vertical direction, respectively, and ϕ_H and ϕ_V denote the corresponding phases. Operations on states can be represented by the Jones matrices, M:

$$\vec{J}' = M\vec{J}, \tag{5.4}$$

where $\vec{J}'$ is the vector obtained when M acts on the state $\vec{J}$. This vector definition is consistent with the definition of qubits given in section 3 and the Jones matrices can be seen as being equivalent to single-qubit gates.

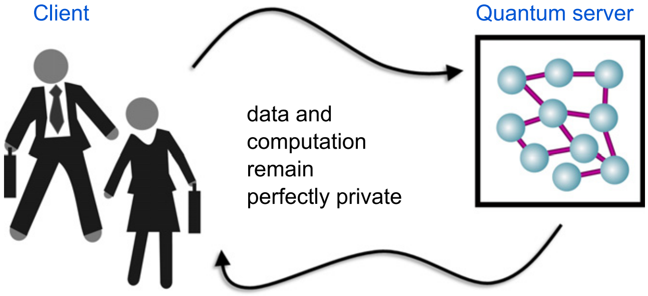


Figure 9. Given the challenges inherent in physically realizing a quantum computer, it is conceivable that, in the future, quantum computing capabilities may be limited to a few specialized facilities around the world. Similar to classical cloud computing, users might then interact remotely with quantum computers and delegate their computations.

5.1.1. Photonic single-qubit gates on polarization-encoded qubits. Experimentally, the polarization of light can be manipulated with phase retarders or 'wave plates' [111]. These uniaxial, birefringent crystals introduce a polarization-dependent phase shift. Combining multiple wave plates facilitates the realization of every possible single-qubit gate on polarization-encoded qubits.

When light travels through a wave plate, it experiences different refractive indices for its ordinary (o) and extraordinary (e) components. The extraordinary polarization lies parallel to the plane which is spanned by the optical axis and the $\vec{k}$ vector of the pump beam, whereas the ordinary polarization is perpendicular to that plane. Thus, each component travels with a different velocity (see figure 11).

After passing through the plate, the two perpendicular polarizations have acquired a difference in phase that is given by:

$$\phi = \frac{2\pi}{\lambda} d \left| n_{\mathrm{e}} - n_{\mathrm{o}} \right|, \tag{5.5}$$

where λ is the wavelength, d the thickness of the crystal, and n_{e} and n_{o} the refractive indices for the extraordinarily and ordinarily polarized components.

Wave plates are commonly produced from quartz or calcite, although wave plates made from other birefringent materials including magnesium fluoride, sapphire, and some polymers are also available. The difference of the two refractive indices n_{e} and n_{o} can either be positive or negative, depending on the material. The axis along which the phase velocity is fastest is called the fast axis, whereas the axis along which the phase velocity is slowest is called the slow axis.

If the fast axis of a wave plate is oriented horizontally, the phase shift can be described by the following matrix [111]:

$$T(\phi) = \begin{pmatrix} 1 & 0 \\ 0 & \exp(-\mathrm{i}\phi) \end{pmatrix}, \tag{5.6}$$

where the vertical component of the beam acquires a phase shift of $-\phi$.

If the fast axis of the wave plate is oriented along at an arbitrary angle θ with respect to the horizontal axis, the transformation matrix can be determined by applying rotation matrices $R(\theta)$:

$$\begin{aligned} T'(\phi) &= R(\theta) T(\phi) R(-\theta) \\ &= \begin{pmatrix} \cos^2(\theta) + \mathrm{e}^{-\mathrm{i}\phi}\sin^2(\theta) & \left(1 - \mathrm{e}^{-\mathrm{i}\phi}\right)\cos(\theta)\sin(\theta) \\ \left(1 - \mathrm{e}^{-\mathrm{i}\phi}\right)\cos(\theta)\sin(\theta) & \mathrm{e}^{-\mathrm{i}\phi}\cos^2(\theta) + \sin^2(\theta) \end{pmatrix} \end{aligned} \tag{5.7}$$

with $R(\theta) = (\cos(\theta), -\sin(\theta);\ \sin(\theta), \cos(\theta))$. Note that the angle θ is a physical rotation in the laboratory, not to be confused with a logical rotation on the Bloch sphere.

Half-wave plates (HWPs) and quarter-wave plates (QWPs) are special cases of phase retarders which are particularly useful in implementing photonic single-qubit gates. A half-wave plate has a thickness such that the phase retardance is $\phi = \pi$. It can be described by the matrix (overall phases, which are important only for certain interference experiments and not for the implementation of quantum logic gates, have been omitted in all calculations presented here):

$$U_{\mathrm{HWP}}(\theta) = \begin{pmatrix} \cos(2\theta) & \sin(2\theta) \\ \sin(2\theta) & -\cos(2\theta) \end{pmatrix}, \tag{5.8}$$

where, again, overall phases are omitted. For $\theta = 0$ the HWP implements a Z-gate, for $\theta = \pi/4$ it is an X-gate, whereas for $\theta = \pi/8$ it represents a Hadamard gate. The HWP can thus be used to convert linearly polarized light into other linear polarization states. This allows the manipulation of polarization-encoded quantum states, e.g. a HWP can turn the states $|0\rangle$ and $|1\rangle$ into the states $|+\rangle$ and $|-\rangle$ and vice versa.

A QWP implements a phase shift of $\phi = \pi/2$ and can mathematically be described via:

$$U_{\mathrm{QWP}}(\theta) = \begin{pmatrix} 1 + \mathrm{i}\cos(2\theta) & \mathrm{i}\sin(2\theta) \\ \mathrm{i}\sin(2\theta) & 1 - \mathrm{i}\cos(2\theta) \end{pmatrix}. \tag{5.9}$$

For θ equal to zero, a QWP adds a phase of (–i) to the vertical component, whereas for $\theta = \pi/2$, the phase shift is equal to (+i). QWPs can create circularly polarized light from linearly polarized light and are able to turn, for example, the states $|+\rangle$ and $|-\rangle$ into the states $|+_i\rangle$ and $|-_i\rangle$ and vice versa. In contrast to HWPs, the orientation (i.e. vertical or horizontal fast axis) of a QWP has an effect on the polarization, and this must be considered in experiments.

Any general unitary transformation U can be achieved by using a combination of HWPs and QWPs. In many cases, a HWP is sandwiched between two QWPs

$$U = U_{\mathrm{QWP}}(\theta_3) U_{\mathrm{HWP}}(\theta_2) U_{\mathrm{QWP}}(\theta_1), \tag{5.10}$$

which enables arbitrary transformations of the polarization [112].

5.2. Beam splitters and polarizing beam splitters (PBS)

Although photonic quantum systems do not allow for direct interactions, the implementation of photonic two-qubit gates is still possible using concepts like the KLM approach. Beam splitters, PBSs, and the Hong–Ou–Mandel (HOM) effect

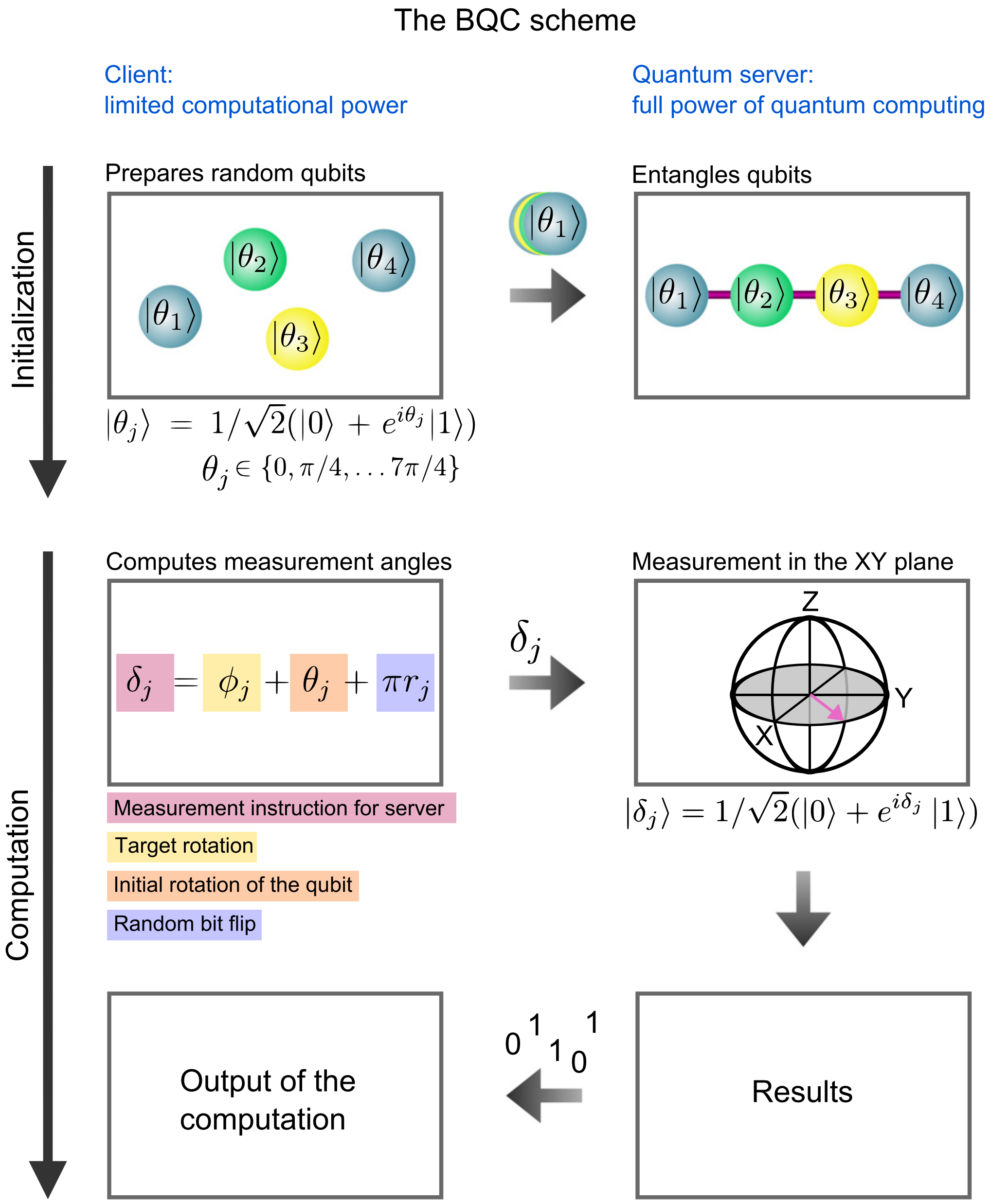

The BQC scheme
Client:
limited computational power
Quantum server:
full power of quantum computing
Initialization
Prepares random qubits
$|\theta_2\rangle$
$|\theta_4\rangle$
$|\theta_1\rangle$
$|\theta_3\rangle$
$|\theta_j\rangle = 1/\sqrt{2}(|0\rangle + e^{i\theta_j}|1\rangle)$
$\theta_j \in \{0, \pi/4, \ldots 7\pi/4\}$
$|\theta_1\rangle$
Entangles qubits
$|\theta_1\rangle$ $|\theta_2\rangle$ $|\theta_3\rangle$ $|\theta_4\rangle$
Computation
Computes measurement angles
$\delta_j = \phi_j + \theta_j + \pi r_j$
Measurement instruction for server
Target rotation
Initial rotation of the qubit
Random bit flip
δ_j
Measurement in the XY plane
Z
Y
X
$|\delta_j\rangle = 1/\sqrt{2}(|0\rangle + e^{i\delta_j}\,|1\rangle)$
Output of the computation
0 1 1 0 1
Results

Figure 10. Scheme of BQC [64, 70]. A nearly-classical client with limited computational power can delegate a computation to a quantum server with the full power of quantum computing such that the input, the output and the whole computation remain perfectly private. To this end, the client prepares single-qubits in a state $|\theta_j\rangle = 1/\sqrt{2}\,(|0\rangle + \mathrm{e}^{\mathrm{i}\theta_j}\,|1\rangle)$, where θ_j is chosen uniformly at random from the set $\{0, \pi/4, \ldots, 7\pi/4\}$. The qubits are then sent to the server who entangles them to a blind cluster state by applying CPhase gates. Although the cluster state changes with the underlying qubits, it can be used for any computation. The actual computation is measurement-based and performed by applying a pattern of consecutive adaptive single-qubit measurements. The client calculates measurement instructions δ_j which are sent to the server. These depend on the measurement angle ϕ_j that the client wants to hide, the phase of the blind qubit θ_j, and a random bitflip $\pi\, r_j$. These classical measurement angles are set in such a way to compensate for the initial random rotation θ_j and any other Pauli byproducts [51, 71] produced by previous measurements. The server now holds qubits and measurement instructions, but does neither know the state of the qubit, $|\theta_j\rangle$, nor the measurement angle ϕ_j. The server then performs measurements in the basis $|\pm_{\delta_j}\rangle = 1/\sqrt{2}\,(|0\rangle \pm \mathrm{e}^{\mathrm{i}\delta_j}\,|1\rangle)$ on the blind cluster state. Without knowledge about the state $|\theta_j\rangle$ or the hidden measurement angle ϕ_j, the measurement outcomes do not reveal any information about the computation. The results are then sent back to the client who is the only one able to interpret them.

[113] play a crucial role in experimental implementations of these concepts.

5.2.1. Beam splitters. A beam splitter is a semi-reflective mirror which splits an incident beam into two parts: a transmitted part and a reflected part (see figure 12(a)).

If a_1 and b_1 are input modes of a beam splitter, the state of the output modes a_2 and b_2 can be calculated using the following relations [52, 114, 115]:

$$a_2^\dagger = \cos\theta \cdot a_1^\dagger + \mathrm{i}\mathrm{e}^{-\mathrm{i}\phi}\sin\theta \cdot b_1^\dagger, \qquad (5.11)$$

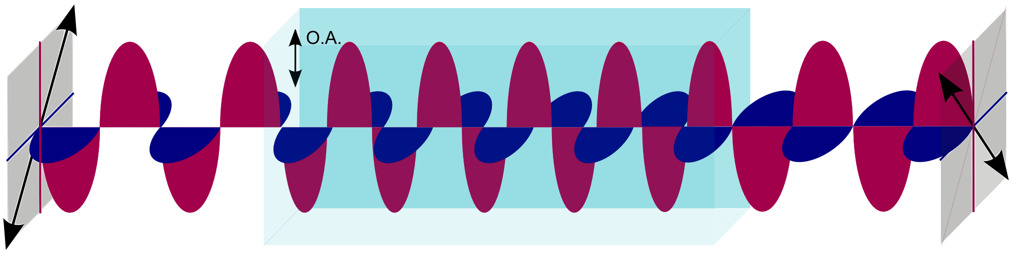


Figure 11. Working principle of a wave plate. This example shows a beam passing through a half-wave plate with an optical axis long the vertical direction. When traveling through the wave plate, the extraordinary and the ordinary polarization components experience different refractive indicices, n_e and n_o, due to the birefringence of the material. Thus, the two polarization components have two different phase velocities; in this example the optical axis defines the slow axis. After passing the wave plate, the two different polarization components have acquired a phase shift of π, which effectively leads to a polarization rotation of 90°.

$$b_2^\dagger = \mathrm{i}e^{\mathrm{i}\phi}\sin\theta \cdot a_1^\dagger + \cos\theta \cdot b_1^\dagger, \tag{5.12}$$

where $a^\dagger$ and $b^\dagger$ are creation operators representing a photon in mode a and b, respectively, and the angle θ specifies the transmittance of the beam splitter. This can be expressed more conveniently by the transmission coefficient $T = \cos^2(\theta)$ and the reflection coefficient $R = \sin^2(\theta)$, which obey the relation $T + R = 1$. The phase shift ϕ between the reflected and the transmitted modes ensures the unitarity of the beam splitter operation [114] and is defined by the physical properties of the beam splitter; i.e. the coating of the mirror. Interestingly, if ϕ_1 (ϕ_2) is the phase shift between the transmitted and the reflected mode for a photon entering from mode a_1 (b_1), unitarity requires that $\phi_1 + \phi_2$ be equal to π [114].

A symmetric beam splitter which splits the light equally into the two output modes ($\theta = \pi/4$), and which acts symmetrically on the two input ports ($\phi = 0$) is defined by:

$$a_2^\dagger = \frac{1}{\sqrt{2}}a_1^\dagger + \mathrm{i}\frac{1}{\sqrt{2}}b_1^\dagger, \tag{5.13}$$

$$b_2^\dagger = \mathrm{i}\frac{1}{\sqrt{2}}a_1^\dagger + \frac{1}{\sqrt{2}}b_1^\dagger. \tag{5.14}$$

The beam splitters used in experiments are manufactured to show a behavior close to that of an ideal symmetric beam splitter, but given the difficulty of constructing a perfect beam splitter it may be necessary to add additional phases to equation (5.13) to achieve a full description of an actual experimental situation [52, 116].

5.2.2. Polarizing beam splitters and measurements.

A PBS splits a beam depending on its polarizations, usually separating an input beam into two modes with orthogonal polarization. Light that is vertically polarized is reflected, whereas horizontally polarized light is transmitted through a PBS (see figure 12(b)).

PBSs can be used for the analysis of a polarization state. Combined with HWPs and QWPs, they facilitate measurements in each possible direction on the Bloch sphere.

In experiments, measurements of σ_x, σ_y, and σ_z are particularly interesting as may be used to reconstruct density matrices [17] which contain the full information about the underlying quantum state. The relevant settings for measurements in these bases using polarization-encoded qubits and a configuration of QWPs and HWPs (see figure 12(c)) are given in table 1.

5.2.3. The HOM effect.

The HOM effect is a two-photon interference effect that occurs when two indistinguishable photons enter a beam splitter from two input ports [113] (see figure 12(d)). The effect is purely quantum and does not occur in classical optics. Mathematically, two photons entering a symmetric beam splitter can be described by their respective creation operators $a_1^\dagger$, $b_1^\dagger$ acting on the vacuum state $|0\rangle|0\rangle$ (for the description of the HOM effect, we use the photon number basis, where $|n\rangle$ represents a state containing n photons). Applying the relations that were introduced in the previous section, we obtain:

$$a_1^\dagger b_1^\dagger\ |0\rangle|0\rangle \simeq \left(a_2^\dagger - \mathrm{i}b_2^\dagger\right)\left(a_2^\dagger + \mathrm{i}b_2^\dagger\right)|0\rangle|0\rangle \tag{5.15}$$

$$\simeq \left(\left(a_2^\dagger\right)^2 + \left(b_2^\dagger\right)^2\right)|0\rangle|0\rangle \tag{5.16}$$

$$\simeq \left(|2\rangle_{a_2}\ |0\rangle_{b_2} + |0\rangle_{a_2}\ |2\rangle_{b_2}\right), \tag{5.17}$$

where normalization factors were omitted. The two photons exit the BS either both in the output mode a_2 or both in the output mode b_2; they never split up and exit in different output modes.

It is important to note that the HOM effect is not the interference of two photons (‘that meet at a beam splitter’), but the interference of the respective two-photon amplitudes occurring in the detectors. Interestingly it was shown that the photons do not even have to arrive at the beam splitter at the same time in order to interfere [117].

The HOM effect also occurs in PBSs if the information about the polarization (and thus the which-path information) is extinguished. In experiments this can achieved with PBSs and measurements in the basis $\{|+\rangle, |-\rangle\}$ [43].

5.3. Multi-qubit gates

One of the main advantages of photonic systems is their very low decoherence. Even if photonic states are transmitted over large distances [118–120], the quantum states remain mostly unaffected. On the other hand, the low decoherence rate seems, at first sight, to prevent the implementation of multi-qubit gates since the photons do not interact with each other.

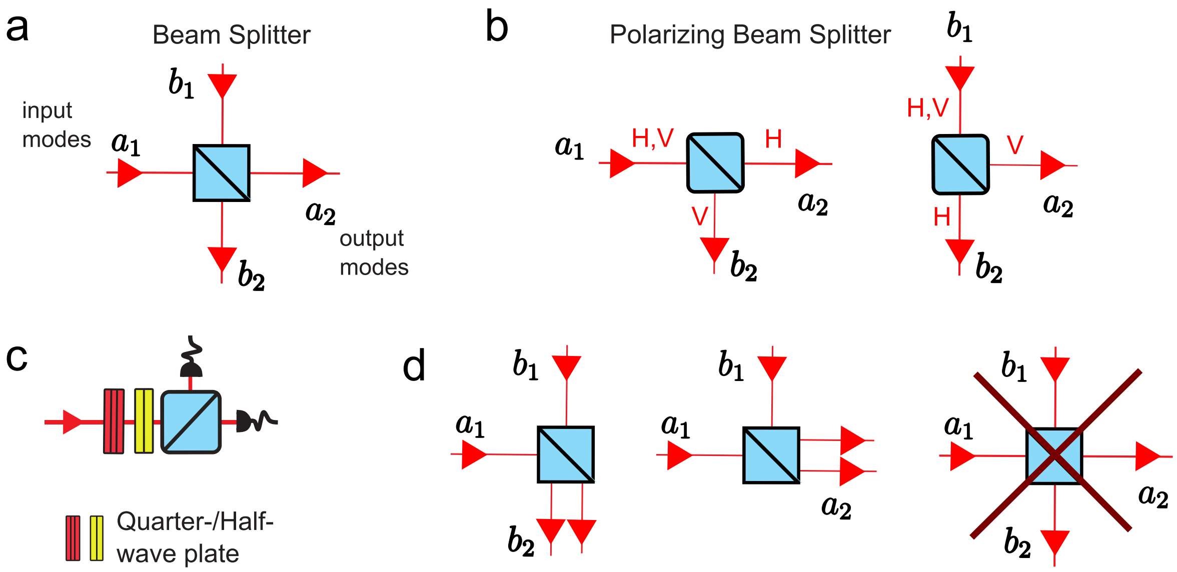


Figure 12. The figure shows the working principle and applications of (polarizing) beam splitters. (a) A beam splitter (BS) splits incident photons into two output modes depending on the splitting ratio. (b) A polarization beam splitter (PBS) transmits horizontally polarized light and reflects vertically polarized light. (c) A PBS together with half-wave and quarter-wave plates can be used for the analysis of arbitrary polarizations. (d) Demonstration of the HOM effect: if two indistinguishable photons enter a beam splitter, they will both exit one or the other port and will never split up into two different ports.

There are mainly two different approaches to overcome this problem in photonic quantum information processing: concepts along the line of KLM [8] using ancilla photons and postselection to provide measurement-induced nonlinearities, and concepts using optical nonlinearities [121]. In this section 1 will briefly introduce these approaches and outline the major advantages as well as disadvantages.

5.3.1. Photonic CNOT and CPhase gates. To illustrate the working principle of most linear-optics two-qubit gates, I will briefly review two examples.

The CPhase gate, which is shown in figure 13(a), consists of a polarization-dependent beam splitter (PDBS) which has a different transmission coefficient for horizontally polarized light ($T = 1$) as for vertically polarized light ($T = 1/3$) [122]. If two vertically-polarized photons are reflected at this PDBS, they acquire a phase shift of π. Two successive PDBSs with the opposite splitting ratios then equalize the output amplitudes. The gate operation has been successful if one photon exists in each of the output modes.

Whereas the experimental implementation of this gate is relatively easy, its scalability is very limited. Since a destructive photon measurement is necessary to verify the correct operation of the gate, the state of the photons is destroyed which makes the realization of a subsequent gate impossible.

In contrast, the CNOT gate shown in figure 13(b) is scalable, but requires an entangled ancilla photon pair as resource [58, 123]. If two photons are registered in the ancilla modes, the gate has been successful without the need for a verification of the output state. Thus, it is possible to use these gates in succession.

Table 1. This table shows the measurement settings for the measurements of σ_x, σ_y, and σ_z. A half-wave and a quarter-wave plate are combined with a PBS as shown in figure 12(c).

Basis	QWP setting	HWP setting
σ_x	$\pi/4$	$\pi/8$
σ_y	$\pi/4$	0
σ_z	0	0

However, applying this type of gate to photons generated from a down-conversion source (a probabilistic source for the generation of single photons, see section 5.4 for details) is still challenging since higher-order emissions can lead to incorrect gate operations. If a double-pair emission enters the gate input, it can split into all four output modes even if no ancilla photons are present. These events have the same generation probability as the correct events, but lead to an incorrect gate operation. This issue can be solved using heralded photon pairs where a signal announces the presence of entangled photons in the right modes. The generation of heralded entangled photon pairs can also be realized by using only linear optics [124, 125].

Both gates presented here resemble the circuit model, but a closer look reveals that they are actually based on measurements—either by postselecting the output states or by measurements of ancilla photons. Thus, these examples demonstrate the necessity of measurements in photonic quantum computing and indicate that a pure circuit model cannot be realized using only linear optics.

5.3.2. Measurement-based photonic quantum computing. In MBQC, quantum information is processed by single-qubit

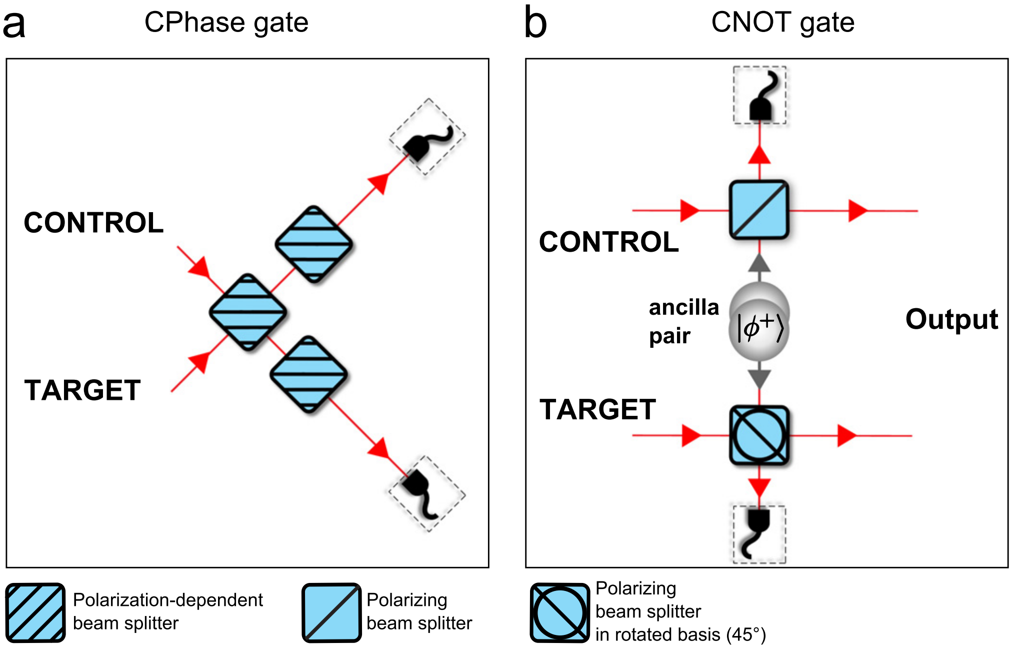


Figure 13. Sketch of two photonic entangling gates. The CPhase gate (a) uses polarization-dependent beam splitters and requires a measurement of the output modes to verify the correct operation of the gate. The CNOT gate (b) requires an entangled ancilla photon-pair and a measurement of two ancilla modes to herald that the gate has worked correctly. Thus, the CPhase gate is limited in scalability since a measurement destroys the quantum state and does not allow for a subsequent gate operation. Figure adapted from [122] and [58].

measurements on cluster states [30]. For photonic systems, the generation of cluster states requires entangling operations and thus relies on postselection techniques. This means that measurements are necessary for the creation of cluster states, but the same measurements also implement the computation in MBQC. In other words, in photonic systems, the measurements which are necessary for the processing of quantum information arise naturally from the creation of photonic cluster states. Thus, despite the high propagation speed of photons and the lack of multi-photon interaction, photonic systems are well-suited for MBQC [51, 70, 76, 126]. Section 5.5 shows an example of how cluster states can be implemented experimentally.

5.3.3. Optical nonlinearities for entangling gates. Another approach to realize photonic quantum computing is to use optical nonlinearities for the implementation of (nearly) deterministic two-qubit gates.

For example, Kerr-nonlinearities can induce photon–photon interactions [52] and enable a phase shift in one mode depending on the number of photons in another mode. Another type of nonlinear entangling gate is based on the Zeno effect [127, 128] where failure events in two-qubit gate operations are suppressed by continuous two-photon absorptions.

One of the main challenges in such experiments is that the available materials provide only small nonlinearities and, so far, only lead to relatively small phase shifts [129]. Nevertheless, the application of theses schemes may significantly reduce the number of required ancillary photons and thus significantly improve the scalability of photonic quantum computing.

5.4. Generation of entangled photons

The workhorse of almost all photonic quantum computing experiments is spontaneous parametric down-conversion (SPDC)—a process where a pump photon is converted into two daughter photons in a nonlinear crystal. The selection of photons with a particular frequency and spatial emission can facilitate the availability of polarization-entangled photon pairs. In the following, I will describe the process in more detail and explain how multi-photon states can be created.

5.4.1. SPDC. SPDC occurs when laser light interacts with a nonlinear crystal such as β-barium borate (BBO) [130]. When an electromagnetic field interacts with a nonlinear medium, the dielectric polarization P generated in the medium shows a nonlinear dependency on the electric field:

$$P_i = \chi^{(1)}_{i,j} E_j + \chi^{(2)}_{i,j,k} E_j E_k + \chi^{(3)}_{i,j,k,l} E_j E_k E_l + \cdots, \qquad (5.18)$$

where χ^m is the susceptibility of order m, E_i denotes the electric field and double indices indicate a sum [131]. The first term ($\chi^1 \approx 1$) describes linear effects such as diffraction, and refraction and the third term ($\chi^3 \approx 10^{-17}$) is very small and describes four-wave mixing processes.

Of interest here is the second term ($\chi^2 \approx 10^{-10}$), which leads to three-wave mixing processes like SPDC. If two waves, $E_1 \cos(\omega_1 t)$ and $E_2 \cos(\omega_2 t)$ interact with a nonlinear medium, this second term can be rewritten in the following form:

$$P_i = \chi^{(2)} E_1 \cos(\omega_1 t) E_2 \cos(\omega_2 t) \qquad (5.19)$$

$$= \chi^{(2)} E_1 E_2 \cos\big((\omega_1 + \omega_2)t\big) \cos\big((\omega_1 - \omega_2)t\big), \qquad (5.20)$$

showing that sum-frequency ($\omega_1 + \omega_2$) and difference-frequency ($\omega_1 - \omega_2$) waves are generated.

SPDC is the reverse configuration: a pump field with a wavelength $\omega = \omega_1 + \omega_2$ creates two new fields with frequencies ω_1 and ω_2, called signal and idler [111, 132]. Two different types of SPDC are distinguished: both created photons can either have the same polarization which is orthogonal to the polarization of the pump laser (type-I), or both photons have orthogonal polarizations (type-II); in the following, we will focus on type-II SPDC.

The down-converted photons show correlations in frequency as well as momentum:

$$\omega_\text{p} = \omega_\text{e} + \omega_\text{o}, \qquad (5.21)$$

$$\vec{k}_\text{p} = \vec{k}_\text{e} + \vec{k}_\text{o}. \qquad (5.22)$$

Only certain propagation directions $\vec{k}$ are possible for the photons due to the phase matching conditions in the nonlinear crystal. For the degenerate case, where $\omega_\text{e} = \omega_\text{o}$, the emission direction of the created photons is along the surface of cones (see figure 14), where one cone has extraordinary polarization and the other ordinary. For our experiments, this corresponds to vertically and to horizontally polarized light, respectively.

For certain incidence angles of the pump beam, these cones intersect (figure 14). Photons emitted into the directions of the lines of intersection can therefore not be assigned to one of the cones. If one photon is emitted into the direction of one of the intersections, the other one must be in the other intersection line due to momentum conservation. These photons are entangled in polarization (figure 14) with a state given by:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\Big(|H\rangle|V\rangle + \mathrm{e}^{\mathrm{i}\phi}\,|V\rangle|H\rangle\Big). \qquad (5.23)$$

The ordinarily and the extraordinarily polarized photons experience different refractive indices, n_o and n_e, in the crystal. Thus, firstly, the propagation velocities are different for both components (longitudinal walk-off effect) and secondly, both photons experience a spatial displacement (transversal walk-off effect). These two effects may lead to a distinguishability of the photons and, as a consequence, to the annihilation of the entanglement. For the generation of properly entangled pairs, it is therefore very important to take into account both effects (for details, see figure 15).

5.4.2. Quantum-mechanical treatment. In order to fully characterize the down-conversion process, a quantum mechanical treatment is necessary. The following interaction Hamiltonian describes the process in terms of the creation and annihilation operators, $a^\dagger$ and a:

$$H = \gamma a_1^\dagger a_2^\dagger a_\text{p} + \gamma^* a_1 a_2 a_\text{p}^\dagger, \qquad (5.24)$$

where the coupling constant γ depends on the nonlinearity χ^2. The first term expresses the down-conversion process, where one pump photon (a_p) creates two down-converted photons ($a_1^\dagger$ and $a_2^\dagger$). The second term describes the opposite process where under annihilation of two photons (a_1 and a_2), a photon is created ($a_\text{p}^\dagger$).

In the case of type-II SPDC, the output state can be written as follows [133]:

$$|\psi\rangle = Z \cdot \exp\Big(-\mathrm{i}\alpha\big(a_H^\dagger b_V^\dagger + a_V^\dagger b_H^\dagger\big)\Big)|0\rangle, \qquad (5.25)$$

where Z is a normalization constant and α is a parameter depending on χ^2 and on the pump power. The creation operators $a_H^\dagger$ ($b_V^\dagger$) describe the generation of a horizontally (vertically) polarized photon in mode a (b) and act on the vacuum state $|0\rangle$. Expanding the exponential function leads to:

$$|\psi\rangle = Z \cdot \Bigg[1 - \underbrace{\mathrm{i}\alpha\big(a_H^\dagger b_V^\dagger + a_V^\dagger b_H^\dagger\big)}_{(1)} \underbrace{- \frac{\alpha^2}{2}\big(a_H^\dagger b_V^\dagger + a_V^\dagger b_H^\dagger\big)^2}_{(2)} \underbrace{+ \mathrm{i}\frac{\alpha^3}{3}\big(a_H^\dagger b_V^\dagger + a_V^\dagger b_H^\dagger\big)^3}_{(3)} + \cdots\Bigg]|0\rangle. \qquad (5.26)$$

The first term (1) corresponds to the generation of a two-photon Bell state with a probability $\simeq Z^2\alpha^2$. The higher orders represent multi-photon emissions, where a four-photon emission (2) is generated with a probability $\simeq Z^2\alpha^4$ and a six-photon emission (3) with probability $\simeq Z^2\alpha^6$. The probabilities to create multi-photon states are low compared to the two-photon case and depend polynomially on the pump power.

Continuous-wave (cw) lasers with typical powers of about 50 mW lead primarily to the emission of two-photon states, since the power is too low to create substantial multi-photon emissions. The high-pump powers necessary to obtain multi-photon events can be achieved with pulsed lasers having sufficiently high peak powers for the generation of higher-order photon states (see next section).

However, increasing the pump power also affects the quality of the states, because the noise terms emerging from the next-order emissions are also increased. The signal-to-noise ratio depends on the parameter α and in this way on the pump power:

$$\frac{\text{signal}}{\text{noise}} = \frac{1}{\alpha^2} \underset{\alpha\to\infty}{\longrightarrow} 0. \qquad (5.27)$$

This noise is intrinsic to all SPDC sources: the higher the pump power, the higher the effect of the noise. In experiments it is therefore necessary to find the right balance between a pump power that is high enough to create the desired emission and one which is, on the other hand, low enough to minimize the noise.

5.4.3. Pulsed SPDC. Photonic quantum information processing requires the coherent generation of multi-photon states. These can be created by pumping a SPDC source with

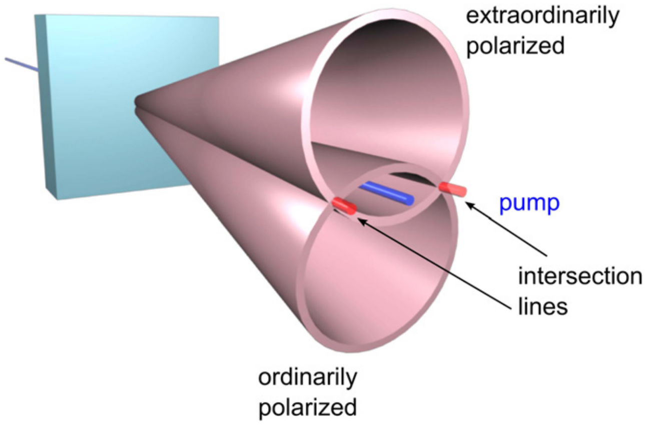


Figure 14. View of a parametric down-conversion process where the down-converted photon pairs are emitted along the surfaces of cones. For the degenerate case, where $\omega_e = \omega_o$, the opening angles of both cones are equal and the setup can be aligned such that the cones intersect as depicted. Photons emitted into the direction of the intersection lines are polarization-entangled, since it cannot be distinguished to which cone they belong. Figure adapted from [130].

a pulsed laser, where the pulse length is on the order of hundreds of femtoseconds.

Pulsed lasers reduce the uncertainty of the emission time for a given down-converted pair [134] and fulfill a necessary condition for coherent higher-order emissions: the variance in emission time, which is determined by the duration of the pump pulse, must be smaller than the coherence time of the down-converted photons [134–137].

On the other hand, pulsed lasers have the disadvantage that the properties of down-converted photon pairs are different from those generated by a cw pump. A pulsed pump contains a broad range of frequencies; the shorter the pulse length, the broader the spectral bandwidth [138]. This leads to down-converted photons which are no longer exactly anticorrelated in frequency since they do not required to fulfill a constant frequency sum (as in equation (5.21)). Furthermore, the spectra of the ordinary and extraordinary photons are no longer identical [134]. In the temporal domain, a pulsed pump leads to a reduced coherence time of the down-converted photons as their bandwidth increases.

These effects make the down-converted photons distinguishable and decrease the visibility in the two-photon interference [137]. The use of narrowband filters and a spectral postselection can recover the indistinguishability and improve the two-photon interference visibilities at the cost of reduced count rates.

5.5. Example: experimental generation of blind cluster states

In section 4.4, we introduced the concept of BQC. In order to show how the experimental concepts presented in this section are used in actual experiments, we will now outline how blind cluster states can be generated experimentally.

Blind quantum computing starts with the generation of blind qubits that are entangled to blind cluster states [64, 70]. Standard cluster states have already been generated in a range of experiments [138, 139]. Blind cluster states are a generalization of those in which the underlying qubits exhibit arbitrary phases θ_j. They are created by entangling qubits in states $|\theta_j\rangle = \frac{1}{\sqrt{2}}(|0\rangle + \mathrm{e}^{\mathrm{i}\theta_j}\,|1\rangle)$, where θ_j is chosen from $\{0, \pi/4, \ldots, 7\pi/4\}$.

For the experiment which is presented here [70], the cluster state consists of four blind qubits, where the phases of $|\theta_1\rangle$ and $|\theta_4\rangle$ are chosen to be zero:

$$|\theta_1\rangle|\theta_2\rangle|\theta_3\rangle|\theta_4\rangle = \frac{1}{4}(|0\rangle + |1\rangle)(|0\rangle + \mathrm{e}^{\mathrm{i}\theta_2}\,|1\rangle) \times (|0\rangle + \mathrm{e}^{\mathrm{i}\theta_3}\,|1\rangle)(|0\rangle + |1\rangle). \tag{5.28}$$

Applying a CPhase gate between qubits 1–2, 2–3 and 3–4 creates a linear cluster state:

$$\left|\Phi^{\hat{\theta}}\right\rangle = \frac{1}{2}\Big(|+\rangle|00\rangle|+\rangle + \mathrm{e}^{\mathrm{i}\theta_3}\,|+\rangle|01\rangle|-\rangle + \mathrm{e}^{\mathrm{i}\theta_2}\,|-\rangle|10\rangle|+\rangle - \mathrm{e}^{\mathrm{i}(\theta_2+\theta_3)}|-\rangle|11\rangle|-\rangle\Big), \tag{5.29}$$

where $\hat{\theta} = (n_2, n_3)$ and $(\theta_2, \theta_3) = (\frac{n_2\pi}{4}, \frac{n_3\pi}{4})$.

In the following, it will be shown how the state of equation (5.29) can be generated in an experiment. However, it should be stressed that this implementation is just one example how this state can be generated and other implementations are also possible.

The experimental setup for the generation of a blind cluster state in shown in figure 16. It consists of a SPDC source, which is pumped in two directions, called the forward and the backward direction, respectively. The blind cluster state is composed of four terms, which correspond to different four-photon emissions. These are achieved by pumping the BBO crystal with a pulsed laser system at a high laser power (200 fs pulses at a repetition rate of 76 MHz at 394.5 nm). A four-photon emission can be obtained experimentally either by an emission of two entangled pairs, one in the forward and one in the backward mode, or by double-pair emissions into respective modes. As is shown below, the generation of blind cluster states exploits coherent superpositions of these different four-pair contributions and utilizes the properties of the PBSs as well as post-selection to obtain the appropriate state.

In the following, the equations are written in terms of state vectors for the sake of clarity. However, the derivation of these equations should be performed in terms of creation operators to obtain the correct results. Here, I will neglect mathematical rigor for the benefit of an intuitive understanding and also omit the normalization factors.

In order to create a blind cluster state, the experiment is aligned such that pairs in a state $|\phi^{-}_{\theta_3}\rangle_{ab} = (|HH\rangle_{ab} - \mathrm{e}^{\mathrm{i}\theta_3}\,|VV\rangle_{ab})\big/\sqrt{2}$ are emitted in the forward direction (modes *a, b*), and pairs in a state $|\phi^{+}_{\theta_2}\rangle_{cd} = (|HH\rangle_{cd} + \mathrm{e}^{\mathrm{i}\theta_2}\,|VV\rangle_{cd})\big/\sqrt{2}$ are emitted in the backward direction (modes *c, d*).

The emission of only one entangled pair in the forward direction (*a, b*) and only one pair in the backward direction (*c,*

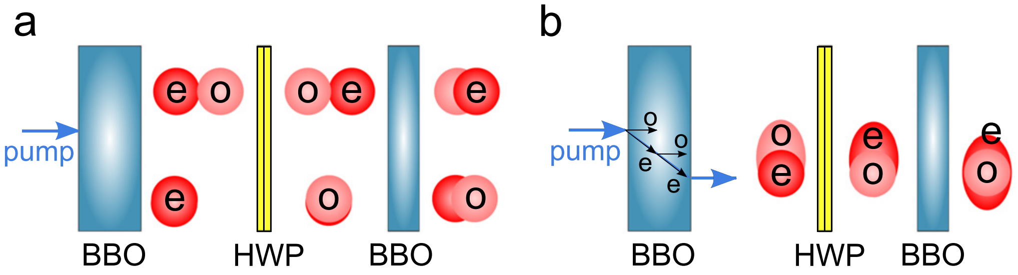


Figure 15. Compensation of walk-off effects. (a) Longitudinal walk-off effect: the arrival time of the photons can reveal information about their polarizations and destroy the entanglement. The time difference after which both photons have passed the crystal depends crucially on the point in the crystal where the photons are created. If the photon pair is created at the beginning of the crystal, the ordinarily polarized photon passes the crystal faster (top example of (a)) and arrives earlier. If the photons are created at the end of the crystal, they arrive simultaneously (bottom example of (a)). The longitudinal walk off needs to be compensated if the time difference $\delta t = (n_o - n_e)d/c$ after the two photons have passed through the crystal is larger than the coherence time $t_c = \sqrt{2\ln 2}\,\lambda^2/(\pi\Delta\lambda c)$ of the photons. Compensation can be accomplished by rotating the polarization of both photons by 90° with a HWP, which exchanges the position of the ordinary and extraordinary photons. If both photons subsequently pass a compensation crystal with a thickness that is half that of the first crystal, the arrival time no longer contains information about the polarization. (b) Transversal walk-off effect. The ordinary and extraordinary photons have different propagation directions in the crystal due to polarization-dependent refractive indices of the crystal. Together with the extraordinary polarization of the pump, this leads to a broadening of the ordinary beam which needs to be counteracted if this broadening is larger than the beam waist. Again, by interchanging both polarizations and letting the two beams pass through a compensation crystal, the effect can be compensated.

d) results in two different four-photon terms:

$$\left|\phi^-_{\theta_3}\right\rangle_{ab}\left|\phi^+_{\theta_2}\right\rangle_{cd} \approx |HHHH\rangle_{abcd} + e^{i\theta_2}\,|HHVV\rangle_{abcd} - e^{i\theta_3}\,|VVHH\rangle_{abcd} - e^{i(\theta_3+\theta_2)}\,|VVVV\rangle_{abcd}. \tag{5.30}$$

The photons then pass the PBSs and only the terms leading to a fourfold coincidence in modes 1–4 are post-selected:

$$\left|\phi^-_{\theta_3}\right\rangle_{ab}\left|\phi^+_{\theta_2}\right\rangle_{cd} \xrightarrow{\text{PBS and postselection}} |HHHH\rangle_{1234} - e^{i(\theta_3+\theta_2)}\,|VVVV\rangle_{1234}. \tag{5.31}$$

In the same way, the emission of two photon pairs in the forward modes (*a, b*) can be calculated:

$$\left|\phi^-_{\theta_3}\right\rangle_{ab}\left|\phi^-_{\theta_3}\right\rangle_{ab} \approx |HH\rangle_a|HH\rangle_b - e^{i\theta_3}\,|HV\rangle_a \times |HV\rangle_b + e^{i(2\theta_3)}\,|VV\rangle_a|VV\rangle_b, \tag{5.32}$$

$$\xrightarrow{\text{PBS and postselection}} - e^{i\theta_3}\,|HHVV\rangle_{1234} \tag{5.33}$$

where $|HH\rangle_a$ denotes two horizontally polarized photons in mode *a*, etc. In the backward modes (*c, d*), the double-pair emission leads to a state:

$$\left|\phi^+_{\theta_2}\right\rangle_{cd}\left|\phi^+_{\theta_2}\right\rangle_{cd} \approx |HH\rangle_c|HH\rangle_d + e^{i\theta_2}\,|HV\rangle_c \times |HV\rangle_d + e^{i(2\theta_2)}\,|VV\rangle_c|VV\rangle_d \tag{5.34}$$

$$\xrightarrow{\text{PBS and postselection}} e^{i\theta_2}\,|VVHH\rangle_{1234}. \tag{5.35}$$

In the experiment, the phase of the term $-e^{i\theta_3}\,|H\rangle_1|H\rangle_2|V\rangle_3|V\rangle_4$ is then shifted by π by applying an additional rotation using a HWP, which has the desired effect [76].

All three states given in equations (5.31), (5.32), and (5.34) build a coherent superposition with the phases defined by the relative phase Δ between the forward and the backward emission:

$$\left|\Phi^{\hat{\theta}}{}_L(\Delta)\right\rangle = e^{i\Delta}\,|HHHH\rangle_{1234} + e^{i\theta_3}\,|HHVV\rangle_{1234} + e^{2i\Delta}e^{i\theta_2}\,|VVHH\rangle_{1234} - e^{i\Delta}e^{i(\theta_3+\theta_2)}\,|VVVV\rangle_{1234}. \tag{5.36}$$

The phase Δ is set equal to multiples of 2π and the final output state $|\Phi^{\hat{\theta}}{}_L\rangle$ obtained in the laboratory is given by:

$$\left|\Phi^{\hat{\theta}}{}_L\right\rangle = |HHHH\rangle_{1234} + e^{i\theta_3}\,|HHVV\rangle_{1234} + e^{i\theta_2}\,|VVHH\rangle_{1234} - e^{i(\theta_3+\theta_2)}\,|VVVV\rangle_{1234}. \tag{5.37}$$

The blind cluster state $|\Phi^{\hat{\theta}}{}_L\rangle$ that is produced in the experiment is equivalent under local unitary transformations to the blind cluster state $|\Phi^{\hat{\theta}}\rangle$. Applying Hadamard gates on qubits 1 and 4 and using the definition $|H\rangle = |0\rangle$ and $|V\rangle = |1\rangle$ finally leads to the blind cluster state:

$$\left|\Phi^{\hat{\theta}}\right\rangle = (H \otimes I \otimes I \otimes H)\left|\Phi^{\hat{\theta}}{}_L\right\rangle. \tag{5.38}$$

These Hadamard gates can be implemented in the experiment by two additional HWPs; alternatively, they may be absorbed in the measurement basis which leads to a simple reinterpretation of the data. Note that after the PBSs two quarter-wave plates were inserted in modes 3 and 4 to compensate for birefringence effects and additional phases.

By changing the phases of the entangled pairs, the values of θ_2 and θ_3 in the blind cluster state can be manipulated arbitrarily, for example using a combination of additional

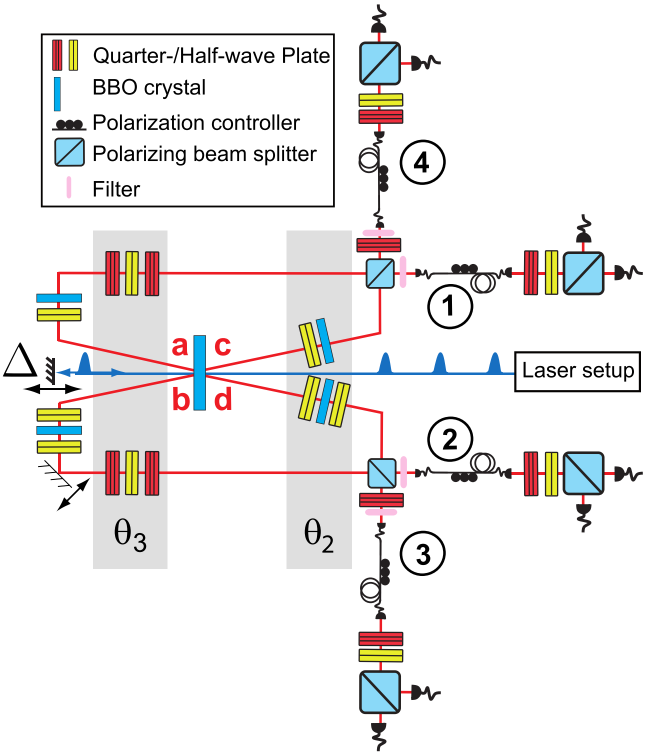


Figure 16. The experimental setup to produce and measure blind cluster states. The various blind cluster states are created by adjusting the settings of the half-wave plates, quarter-wave plates and BBO crystals located along the path of the state emitted into the forward (θ_3) and backward (θ_2) modes.

QWPs and HWPs in the forward mode [112]:

$$\left|\phi^-_{\theta_3}\right\rangle = \left[U_{\mathrm{QWP}}(-\pi/4)\,U_{\mathrm{HWP}}\left(\theta_3/8\right)U_{\mathrm{QWP}}(-\pi/4)\right.$$
$$\left.\otimes\, U_{\mathrm{QWP}}(\pi/4)\,U_{\mathrm{HWP}}\left(-\theta_3/8\right)U_{\mathrm{QWP}}(\pi/4)\right]\ |\phi^-\rangle, \quad (5.39)$$

with the Bell state $|\phi^-\rangle = (|HH\rangle - |VV\rangle)/\sqrt{2}$. Equation (5.39) shows that by rotating both HWPs, any phase θ_3 can be obtained. For practical reasons, the phase of the backward pair is adapted by tilting one of the compensation crystals. The case of standard cluster states can be obtained by choosing $\theta_2 = \theta_3 = 0$.

This example of a photonic experiment shows how the basic concepts of photonic quantum information processing can be used to generate cluster states. These cluster states allow performing various blind delegated computations, including one- and two-qubit gates and the Deutsch and Grover quantum algorithms [70]. Further, it was shown, that the concept of BQC allows testing if a quantum computation was performed correctly [74], which was also demonstrated experimentally [7].

6. Conclusion and outlook

In order to develop scalable LOQC experiments, several steps will have to be taken in the future. Different technical challenges need to be overcome and, in short, more efficient methods for the creation, interaction and detection of single photons must be developed.

Firstly, the standard process of creating entangled photons, SPDC, works probabilistically and with low efficiency. The heralded generation of entangled photon pairs can be realized [124, 125], but the actual rates are still low.

Additionally, the quality of multi-photon states generated in a SPDC process are intrinsically limited due to noise caused by higher-order emissions. Therefore, the development of a high-efficiency push-button source which produces single-photons or multi-photons states on-demand is crucial. Promising candidates for this task are semiconductor quantum dots [140–146], atoms or ions [147–150], superconducting qubits [151], and nitrogen-vacancy centers [152–155].

Secondly, the development of efficient photonic two-qubit gates is of great importance. Although it has been shown that quantum computing is possible with only linear optics and photon detection, in practice these schemes become inefficient due to an enormous amount of required ancilla photons [8]. In order to overcome these challenges, the advancement and utilization of optical nonlinearities [52, 129] on the one hand, and the development of schemes which enable photon–photon interactions on the other hand [127, 128], are crucial tasks. Furthermore, the future of photonic quantum information processing might lie in integrated optics which enable a higher stability and better implementation of quantum circuits while at the same time reducing photon losses [156–158]. So far, these setups use path encoded qubits with only a few modes and are thus still limited in their complexity. In the future, also using the polarization degrees of freedom in integrated optics might enable the implementation of much more complex circuits. Efforts are currently underway to realize integrated sources where the photons are directly generated in a waveguide [159–161]. The ultimate aim for the future is to integrate photon generation, processing and detection on a single photonic chip.

Thirdly, current experiments are limited by the low detection efficiencies of avalanche photodiodes which are widely-used in photonic quantum computing experiments. Much higher detection efficiencies can be obtained by employing superconducting transition-edge detectors or superconducting nano-wire detectors [162–167]. While poor time resolution of the former impedes their application in pulsed multi-photon experiments, the latter are ideally suited for this task.

Furthermore, it will be interesting to see in general in the future which physical system will prevail [168]. One forward-looking concept might be the development of hybrid systems combining the advantages of photons, in particular the low decoherence, with the advantages of other quantum systems which enable multi-qubit interactions [169, 170]. For these hybrid systems, the development of interfaces between the different physical systems, for example between optical and microwave photons [171–174], or the mapping of photonic states to atomic states is a crucial task [91, 175–184].

Besides these technical advances, the future will also show which computational model is best-suited for experimental quantum computing. Also on the theoretical side approaches combining advantages of different models might be beneficial [61, 62]. Breaking through the boundaries of different fields, e.g. physics and computer science, might inspire future research.

Acknowledgments

The author is grateful to Philip Walther and Anton Zeilinger for discussions; and to Wolfgang Duer, Marissa Giustina, Tim Langen, and Michael Zwerger for critical reading of the manuscript. This work was supported by the Marie Curie Actions within the Seventh Framework Programme for Research of the European Commission, under the Initial Training Network PICQUE, Grant No. 608062.

References

[1] Feynman R 1982 Simulating physics with computers *Int. J. Theor. Phys.* **21** 467–88

[2] Deutsch D 1985 Quantum theory, the church-turing principle and the universal quantum computer *Proc. R. Soc.* A **400** 97–117

[3] Deutsch D and Jozsa R 1992 Rapid solution of problems by quantum computation *Proc. R. Soc.* A **439** 553–8

[4] Shor P W 1997 Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer *SIAM J. Comput.* **26** 1484–509

[5] Grover L K 1996 A fast quantum mechanical algorithm for database search *Proc. 28th Annual ACM Symp. on the Theory of Computing* pp 212–9

[6] Harrow A W, Hassidim A and Lloyd S 2009 Quantum algorithm for linear systems of equations *Phys. Rev. Lett.* **103** 150502

[7] Barz S, Kassal I, Ringbauer M, Lipp Y O, Dakić B, Aspuru-Guzik A and Walther P 2014 A two-qubit photonic quantum processor and its application to solving systems of linear equations *Sci. Rep.* **4** 6115

[8] Knill E, Laflamme R and Milburn G J 2001 A scheme for efficient quantum computation with linear optics *Nature* **409** 46–52

[9] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)

[10] Sakurai J J 2003 *Modern Quantum Mechanics* (Reading, MA: Addison-Wesley)

[11] Fox M 2006 *Quantum Optics. An Introduction* (Cambridge: Cambridge University Press)

[12] Horodecki R, Horodecki P, Horodecki M and Horodecki K 2009 Quantum entanglement *Rev. Mod. Phys.* **81** 865–942

[13] Einstein A, Podolski B and Rosen N 1935 Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.* **47** 777–80

[14] Bell J 1964 On the Einstein–Podolsky–Rosen paradox *Physics* **1** 195–200

[15] Clauser J F, Horne M A, Shimony A and Holt R A 1969 Proposed experiment to test local hidden-variable theories *Phys. Rev. Lett.* **23** 880–4

[16] von Neumann J 1932 *Mathematische Grundlagen der Quantenmechanik* vol 42 (Berlin: Springer)

[17] James D F V, Kwiat P G, Munro W J and White A G 2001 Measurement of qubits *Phys. Rev.* A **64** 52312

[18] Wei T, Nemoto K, Goldbart P M, Kwiat P G, Munro W J and Verstraete F 2003 Maximal entanglement versus entropy for mixed quantum states *Phys. Rev.* A **67** 022110

[19] Williams C P 2010 *Explorations in Quantum Computing* (Berlin: Springer)

[20] Uhlmann A 1976 The 'transition probability' in the state space of a*-algebra *Rep. Math. Phys.* **9** 273–9

[21] Hill S and Wootters W K 1997 Entanglement of a pair of quantum bits *Phys. Rev. Lett.* **78** 5022–5

[22] Wootters W K 1998 Entanglement of formation of an arbitrary state of two qubits *Phys. Rev. Lett.* **80** 2245–8

[23] Coffman V, Kundu J and Wootters W K 2000 Distributed entanglement *Phys. Rev.* A **61** 052306

[24] Deutsch D 1989 Quantum computational networks *Proc. R. Soc.* A **425** 73–90

[25] Feynman R P 1986 Quantum mechanical computers *Found. Phys.* **16** 507–31

[26] Barenco A, Bennett C H, Cleve R, DiVincenzo D P, Margolus N, Shor P, Sleator T, Smolin J A and Weinfurter H 1995 Elementary gates for quantum computation *Phys. Rev.* A **52** 3457–67

[27] Kitaev A Y 1997 Quantum computations: algorithms and error correction *Russ. Math. Surv.* **52** 1191–249

[28] Shi Y 2002 Both toffoli and controlled-not need little help to do universal quantum computation arXiv:quant-ph/0205115

[29] Aharonov D 2003 A simple proof that toffoli and hadamard are quantum universal arXiv:quant-ph/0301040

[30] Briegel H-J, Browne D E, Dür W, Raussendorf R and Van den Nest M 2009 Measurement-based quantum computation *Nat. Phys.* **5** 19–26

[31] Raussendorf R and Briegel H J 2001 A one-way quantum computer *Phys. Rev. Lett.* **86** 5188–91

[32] Raussendorf R, Browne D E and Briegel H J 2003 Measurement-based quantum computation with cluster states *Phys. Rev.* A **68** 022312

[33] Bennett C H, Brassard G, Crépeau C, Jozsa R, Peres A and Wootters W K 1993 Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels *Phys. Rev. Lett.* **70** 1895–9

[34] Verstraete F and Cirac J I 2004 Valence-bond states for quantum computation *Phys. Rev.* A **70** 060302

[35] Leung D W 2001 Two-qubit projective measurements are universal for quantum computation arXiv:quant-ph/0111122

[36] Aliferis P and Leung D W 2004 Computation by measurements: a unifying picture *Phys. Rev.* A **70** 062314

[37] Childs A M, Leung D W and Nielsen M A 2005 Unified derivations of measurement-based schemes for quantum computation *Phys. Rev.* A **71** 032318

[38] Jorrand P and Perdrix S 2005 Unifying quantum computation with projective measurements only and one-way quantum computation *Proc. SPIE* **5833** 44–51

[39] van den Nest M and Briegel H J 2008 Measurement-based quantum computation and undecidable logic *Found. Phys.* **38** 448–57

[40] Bouwmeester D, Pan J-W, Mattle K, Eibl M, Weinfurter H and Zeilinger A 1997 Experimental quantum teleportation *Nature* **390** 575–9

[41] Gottesman D and Chuang I L 1999 Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations *Nature* **402** 390–3

[42] Myers C R and Laflamme R 2005 Linear optics quantum computation: an overview arXiv:quant-ph/0512104

[43] Kok P, Munro W J, Nemoto K, Ralph T C, Dowling J P and Milburn G J 2007 Linear optical quantum computing with photonic qubits *Rev. Mod. Phys.* **79** 135–74

[44] Kim Y-H, Kulik S P and Shih Y 2001 Quantum teleportation of a polarization state with a complete bell state measurement *Phys. Rev. Lett.* **86** 1370–3

[45] Lee S-W and Jeong H 2013 Bell-state measurement and quantum teleportation using linear optics: two-photon pairs, entangled coherent states, and hybrid entanglement arXiv:1304.1214

[46] O'Brien J L, Pryde G J, White A G, Ralph T C and Branning D 2003 Demonstration of an all-optical quantum controlled-not gate *Nature* **426** 264–7

[47] Popescu S 2007 Knill–Laflamme–Milburn linear optics quantum computation as a measurement-based computation *Phys. Rev. Lett.* **99** 250501

[48] Hein M, Eisert J and Briegel H J 2004 Multiparty entanglement in graph states *Phys. Rev.* A **69** 062311

[49] Hein M, Dür W, Eisert J, Raussendorf R, Nest M and Briegel H J 2006 Entanglement in graph states and its applications arXiv:quant-ph/0602096

[50] Gottesman D 1997 Stabilizer codes and quantum error correction *PhD Thesis* Caltech

[51] Prevedel R, Walther P, Tiefenbacher F, Böhi P, Kaltenbaek R, Jennewein T and Zeilinger A 2007 High-speed linear optics quantum computing using active feed-forward *Nature* **445** 65–69

[52] Kok P 2007 Lecture notes on optical quantum computing arXiv:0705.4193

[53] Nielsen M A 2006 Cluster-state quantum computation *Rep. Math. Phys.* **57** 147–61

[54] van den Nest M, Dehaene J and de Moor B 2004 Graphical description of the action of local Clifford transformations on graph states *Phys. Rev.* A **69** 022316

[55] van den Nest M, Dehaene J and de Moor B 2004 Efficient algorithm to recognize the local clifford equivalence of graph states *Phys. Rev.* A **70** 034302

[56] Ji Z, Chen J, Wei Z and Ying M 2010 The LU–LC conjecture is false *Quantum Inf. Comput.* **1** 97–108

[57] Leung D W 2004 Quantum computation by measurements *Int. J. Quantum Inf.* **2** 33–43

[58] Pittman T B, Jacobs B C and Franson J D 2001 Probabilistic quantum logic operations using polarizing beam splitters *Phys. Rev.* A **64** 062311

[59] Pittman T B, Jacobs B C and Franson J D 2002 Demonstration of non-deterministic quantum logic operations using linear optical elements *Phys. Rev. Lett.* **88** 257902

[60] Yoran N and Reznik B 2003 Deterministic linear optics quantum computation with single photon qubits *Phys. Rev. Lett.* **91** 037903

[61] Nielsen M A 2004 Optical quantum computation using cluster states *Phys. Rev. Lett.* **96** 040503

[62] Browne D E and Rudolph T 2005 Resource-efficient linear optical quantum computation *Phys. Rev. Lett.* **95** 10501

[63] Kieling K, Gross D and Eisert J 2007 Minimal resources for linear optical one-way computing *J. Opt. Soc. Am.* B **24** 184–8

[64] Broadbent A, Fitzsimons J and Kashefi E 2009 Universal blind quantum computation *Proc. 50th Annual Symp. on Foundations of Computer Science* pp 517–26

[65] Childs A 2005 Secure assisted quantum computation *Quantum Inf. Comput.* **5** 456–66

[66] Arrighi P and Salvail L 2006 Blind quantum computation *Int. J. Quantum Inf.* **4** 883–98

[67] Giovannetti V, Lloyd S and Maccone L 2008 Quantum private queries *Phys. Rev. Lett.* **100** 230502

[68] de Martini F, Giovannetti V, Lloyd S, Maccone L, Nagali E, Sansoni L and Sciarrino F 2009 Experimental quantum private queries with linear optics *Phys. Rev.* A **80** 10302

[69] Aharonov D, Ben-Or M and Eban E 2010 Interactive proofs for quantum computations *Proc. Innovations in Computer Science* pp 453–69

[70] Barz S, Kashefi E, Broadbent A, Fitzsimons J F, Zeilinger A and Walther P 2012 Demonstration of blind quantum computing *Science* **335** 303–8

[71] Danos V and Kashefi E 2006 Determinism in the one-way model *Phys. Rev.* A **74** 052310

[72] Danos V, Kashefi E and Panangaden P 2007 The measurement calculus *J. ACM* **54** 8

[73] Gross D, Eisert J, Schuch N and Perez-Garcia D 2007 Measurement-based quantum computation beyond the one-way model *Phys. Rev.* A **76** 052315

[74] Fitzsimons J F and Kashefi E 2012 Unconditionally verifiable blind computation arXiv:1203.5217

[75] Walther P, Resch K J, Rudolph T, Schenck E, Weinfurter H, Vedral V, Aspelmeyer M and Zeilinger A 2005 Experimental one-way quantum computing *Nature* **434** 169–76

[76] Kiesel N, Schmid C, Weber U, Tóth G, Gühne O, Ursin R and Weinfurter H 2005 Experimental analysis of a four-qubit photon cluster state *Phys. Rev. Lett.* **95** 210502

[77] Lu C-Y, Browne D E, Yang T and Pan J-W 2007 Demonstration of a compiled version of Shor's quantum factoring algorithm using photonic qubits *Phys. Rev. Lett.* **99** 250504

[78] Lanyon B P, Weinhold T J, Langford N K, Barbieri M, James D F V, Gilchrist A and White A G 2007 Experimental demonstration of a compiled version of shor's algorithm with quantum entanglement *Phys. Rev. Lett.* **99** 250505

[79] Gao W B, Lu C Y, Yao X C, Xu P, Gühne O, Goebel A, Chen Y A, Peng C Z, Chen Z B and Pan J W 2010 Experimental demonstration of a hyper-entangled ten-qubit schrödinger cat state *Nat. Phys.* **6** 331–5

[80] Cirac J I and Zoller P 1995 Quantum computations with cold trapped ions *Phys. Rev. Lett.* **74** 4091–4

[81] Monroe C, Meekhof D M, King B E, Itano W M and Wineland D J 1995 Demonstration of a fundamental quantum logic gate *Phys. Rev. Lett.* **75** 4714–7

[82] Kielpinski D, Monroe C and Wineland D J 2002 Architecture for a large-scale ion-trap quantum computer *Nature* **417** 709–11

[83] Blinov BB, Moehring DL, Duan L M and Monroe C 2004 Observation of entanglement between a single trapped atom and a single photon *Nature* **428** 153–7

[84] Gerritsma R, Kirchmair G, Zähringer F, Solano E, Blatt R and Roos CF 2010 Quantum simulation of the Dirac equation *Nature* **463** 68–71

[85] Kim K, Chang M-S, Korenblit S, Islam R, Edwards E E, Freericks J K, Lin G-D, Duan L-M and Monroe C 2010 Quantum simulation of frustrated Ising spins with trapped ions *Nature* **465** 590–3

[86] Schindler P, Barreiro J T, Monz T, Nebendahl V, Nigg D, Chwalla M, Hennrich M and Blatt R 2011 Experimental repetitive quantum error correction *Science* **332** 1059–61

[87] Lanyon BP *et al* 2011 Universal digital quantum simulation with trapped ions *Science* **334** 57–61

[88] Blatt R and Roos C 2012 Quantum simulations with trapped ions *Nat. Phys.* **8** 277–84

[89] Wieman C E, Pritchard D E and Wineland D J 1999 Atom cooling, trapping, and quantum manipulation *Rev. Mod. Phys.* **71** 253–62

[90] Duan L M, Lukin M D, Cirac J I and Zoller P 2001 Long-distance quantum communication with atomic ensembles and linear optics *Nature* **414** 413–8

[91] Wilk T, Webster S C, Kuhn A and Rempe G 2007 Single-atom single-photon quantum interface *Science* **317** 488–90

[92] Cory D G *et al* 2000 Nmr based quantum information processing: achievements and prospects *Fortschr. Phys.* **48** 875–907

[93] Vandersypen L M K, Steffen M, Breyta G, Yannoni C S, Sherwood M H and Chuang I L 2001 Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance *Nature* **414** 883–7

[94] Vandersypen L M K and Chuang I L 2005 Nmr techniques for quantum control and computation *Rev. Mod. Phys.* **76** 1037–69

[95] Bloch I, Dalibard J and Nascimbène S 2012 Quantum simulations with ultracold quantum gases *Nat. Phys.* **8** 267–76

[96] Yamamoto T, Pashkin Y A, Astafiev O, Nakamura Y and Tsai J S 2003 Demonstration of conditional gate operation using superconducting charge qubits *Nature* **425** 941–4

[97] Makhlin Y, Schön G and Shnirman A 2001 Quantum-state engineering with Josephson-junction devices *Rev. Mod. Phys.* **73** 357–400

[98] Neeley M *et al* 2009 Emulation of a quantum spin with a superconducting phase qudit *Science* **325** 722–5

[99] DiCarlo L *et al* 2009 Demonstration of two-qubit algorithms with a superconducting quantum processor *Nature* **460** 240–4

[100] DiCarlo L, Reed MD, Sun L, Johnson BR, Chow JM, Gambetta JM, Frunzio L, Girvin SM, Devoret MH and Schoelkopf RJ 2010 Preparation and measurement of three-qubit entanglement in a superconducting circuit *Nature* **467** 574–8

[101] Bialczak R C *et al* 2010 Quantum process tomography of a universal entangling gate implemented with josephson phase qubits *Nat. Phys.* **6** 409–13

[102] Mariantoni M *et al* 2011 Implementing the quantum von Neumann architecture with superconducting circuits *Science* **334** 61–65

[103] Reed MD, DiCarlo L, Nigg SE, Sun L, Frunzio L, Girvin SM and Schoelkopf RJ 2012 Realization of three-qubit quantum error correction with superconducting circuits *Nature* **482** 382–5

[104] Berezovsky J, Mikkelsen M H, Stoltz N G, Coldren L A and Awschalom D D 2008 Picosecond coherent optical manipulation of a single electron spin in a quantum dot *Science* **320** 349–52

[106] Fushman I, Englund D, Faraon A, Stoltz N, Petroff P and Vučković J 2008 Controlled phase shifts with a single quantum dot *Science* **320** 769–72

[106] Hanson R and Awschalom D D 2008 Coherent manipulation of single spins in semiconductors *Nature* **453** 1043–9

[107] O'Brien J L 2007 Optical quantum computing *Science* **318** 1567–70

[108] O'Brien J L, Furusawa J A and Vučković J 2009 Photonic quantum technologies *Nat. Photonics* **3** 687–95

[109] Aspuru-Guzik A and Walther P 2012 Photonic quantum simulators *Nat. Phys.* **8** 285–91

[110] Jones R C 1941 A new calculus for the treatment of optical systems *J. Opt. Soc. Am.* **31** 500–3

[111] Saleh B E A and Teich M C 1991 *Fundamentals of Photonics* (New York: Wiley)

[112] Langford N K 2007 Encoding, manipulating and measuring quantum information in optics *PhD Thesis* University of Queensland

[113] Hong C K, Ou Z Y and Mandel L 1987 Measurement of subpicosecond time intervals between two photons by interference *Phys. Rev. Lett.* **59** 2044–6

[114] Zeilinger A 1981 General properties of lossless beam splitters in interferometry *Am. J. Phys.* **49** 882–3

[115] Holbrow CH, Galvez E and Parks ME 2002 Photon quantum mechanics and beam splitters *Am. J. Phys.* **70** 260–5

[116] Zetie KP, Adams SF and Tocknell RM 2000 How does a Mach–Zehnder interferometer work? *Phys. Educ.* **35** 46–48

[117] Pittman TB, Strekalov DV, Migdall A, Rubin MH, Sergienko AV and Shih YH 1996 Can two-photon interference be considered the interference of two photons? *Phys. Rev. Lett.* **77** 1917–20

[118] Ursin R *et al* 2007 Entanglement-based quantum communication over 144 km *Nat. Phys.* **3** 481–6

[119] Yin J *et al* 2012 Quantum teleportation and entanglement distribution over 100 kilometre free-space channels *Nature* **488** 185–8

[120] Ma X-S *et al* 2012 Quantum teleportation over 143 kilometres using active feed-forward *Nature* **489** 269–73

[121] Franson J D, Donegan M M and Jacobs B C 2004 Generation of entangled ancilla states for use in linear optics quantum computing *Phys. Rev.* A **69** 052328

[122] Kiesel N, Schmid C, Weber U, Ursin R and Weinfurter H 2005 Linear optics controlled-phase gate made simple *Phys. Rev. Lett.* **95** 210505

[123] Gasparoni S, Pan J-W, Walther P, Rudolph T and Zeilinger A 2004 Realization of a photonic CNOT gate sufficient for quantum computation *Phys. Rev. Lett.* **93** 020504

[124] Wagenknecht C, Li C M, Reingruber A, Bao X H, Goebel A, Chen Y A, Zhang Q, Chen K and Pan J W 2010 Experimental demonstration of a heralded entanglement source *Nat. Photonics* **4** 549–52

[125] Barz S, Cronenberg G, Zeilinger A and Walther P 2010 Heralded generation of entangled photon pairs *Nat. Photonics* **4** 553–6

[126] Walther P, Pan J-W, Aspelmeyer M, Ursin R, Gasparoni S and Zeilinger A 2004 De Broglie wavelength of a non-local four-photon state *Nature* **429** 158–61

[127] Franson J D, Jacobs B C and Pittman T B 2004 Quantum computing using single photons and the zeno effect *Phys. Rev.* A **70** 062302

[128] Franson J D, Pittman T B and Jacobs B C 2007 Zeno logic gates using microcavities *J. Opt. Soc. Am.* B **24** 209–13

[129] Langford N K, Ramelow S, Prevedel R, Munro W J, Milburn G J and Zeilinger A 2011 Efficient quantum computing using coherent photon conversion *Nature* **478** 360–3

[130] Kwiat P G, Mattle K, Weinfurter H, Zeilinger A, Sergienko A V and Shih Y 1995 New high-intensity source of polarization-entangled photon pairs *Phys. Rev. Lett.* **75** 4337–41

[131] Gerry C and Knight P 2004 *Introductory Quantum Optics* (Cambridge: Cambridge University Press)

[132] Boyd R W 1992 *Nonlinear Optics* (San Diego, CA: Academic)

[133] Weinfurter H and Żukowski M 2001 Four-photon entanglement from down-conversion *Phys. Rev.* A **64** 010102

[134] Grice WP and Walmsley IA 1997 Spectral information and distinguishability in type-II down-conversion with a broadband pump *Phys. Rev.* A **56** 1627–34

[135] Żukowski M, Zeilinger A, Horne M A and Ekert A K 1993 'Event-ready-detectors' Bell experiment via entanglement swapping *Phys. Rev. Lett.* **71** 4287–90

[136] Zukowski M, Zeilinger A and Weinfurter H 1995 Entangling photons radiated by independent pulsed sources *Annals of the New York Academy of Sciences* (New York: New York Academy of Sciences) pp 91–102

[137] Di Giuseppe G, Haiberger L, De Martini F and Sergienko AV 1997 Quantum interference and indistinguishability with femtosecond pulses *Phys. Rev.* A **56** 21–24

[138] Prevedel R 2009 Experimental all-optical one-way quantum computing *PhD Thesis* University of Vienna

[139] Walther P 2005 Entanglement and nonlocality in multi-photon systems *PhD Thesis* University of Vienna

[140] Michler P, Kiraz A, Becher C, Schoenfeld W V, Petroff P M, Zhang L, Hu E and Imamoglu A 2000 A quantum dot single-photon turnstile device *Science* **290** 2282–5

[141] Santori C, Fattal D, Vuckovic J, Solomon G S and Yamamoto Y 2002 Indistinguishable photons from a single-photon device *Nature* **419** 594–7

[142] Yuan Z, Kardynal B E, Stevenson R M, Shields A J, Lobo C J, Cooper K, Beattie N S, Ritchie D A and Pepper M

2002 Electrically driven single-photon source *Science* **295** 102–5

[143] Lodahl P, Van Driel A F, Nikolaev I S, Irman A, Overgaag K, Vanmaekelbergh D and Vos W L 2004 Controlling the dynamics of spontaneous emission from quantum dots by photonic crystals *Nature* **430** 654–7

[144] Stevenson RM, Young RJ, Atkinson P, Cooper K, Ritchie DA and Shields AJ 2006 A semiconductor source of triggered entangled photon pairs *Nature* **439** 179–82

[145] Akopian N, Lindner NH, Poem E, Berlatzky Y, Avron J, Gershoni D, Gerardot BD and Petroff PM 2006 Entangled photon pairs from semiconductor quantum dots *Phys. Rev. Lett.* **96** 130501

[146] Shields A J 2007 Semiconductor quantum light sources *Nat. Photonics* **1** 215–23

[147] Kuhn A, Hennrich M and Rempe G 2002 Deterministic single-photon source for distributed quantum networking *Phys. Rev. Lett.* **89** 067901

[148] McKeever J, Boca A, Boozer AD, Miller R, Buck JR, Kuzmich A and Kimble HJ 2004 Deterministic generation of single photons from one atom trapped in a cavity *Science* **303** 1992–4

[149] Keller M, Lange B, Hayasaka K, Lange W and Walther H 2004 Continuous generation of single photons with controlled waveform in an ion-trap cavity system *Nature* **431** 1075–8

[150] Eisaman MD, André A, Massou F, Fleischhauer M, Zibrov AS and Lukin MD 2005 Electromagnetically induced transparency with tunable single-photon pulses *Nature* **438** 837–41

[151] Houck A A *et al* 2007 Generating single microwave photons in a circuit *Nature* **449** 328–31

[152] Kurtsiefer C, Mayer S, Zarda P and Weinfurter H 2000 Stable solid-state source of single photons *Phys. Rev. Lett.* **85** 290–3

[153] Rugar D, Budakian R, Mamin HJ and Chui BW 2004 Single spin detection by magnetic resonance force microscopy *Nature* **430** 329–32

[154] Neumann P, Mizuochi N, Rempp F, Hemmer P, Watanabe H, Yamasaki S, Jacques V, Gaebel T, Jelezko F and Wrachtrup J 2008 Multipartite entanglement among single spins in diamond *Science* **320** 1326–9

[155] Wrachtrup J and Jelezko F 2006 Processing quantum information in diamond *J. Phys.: Condens. Matter* **18** 807–24

[156] Politi A, Cryan M J, Rarity J G, Yu S and O'Brien J L 2008 Silica-on-silicon waveguide quantum circuits *Science* **320** 646–9

[157] Matthews J, Politi A, Stefanov A and O'Brien J 2009 Manipulation of multiphoton entanglement in waveguide quantum circuits *Nat. Photonics* **3** 346–50

[158] Politi A, Matthews J C F and O'Brien J L 2009 Shor's quantum factoring algorithm on a photonic chip *Science* **325** 1221–1221

[159] Fulconis J, Alibart O, Wadsworth W, Russell P and Rarity J 2005 High brightness single mode source of correlated photon pairs using a photonic crystal fiber *Opt. Express* **13** 7572–82

[160] Rarity J, Fulconis J, Duligall J, Wadsworth W and Russell P 2005 Photonic crystal fiber source of correlated photon pairs *Opt. Express* **13** 534–44

[161] Cohen O, Lundeen J S, Smith B J, Puentes G, Mosley P J and Walmsley I A 2009 Tailored photon-pair generation in optical fibers *Phys. Rev. Lett.* **102** 123603

[162] Gol'tsman G N, Okunev O, Chulkova G, Lipatov A, Semenov A, Smirnov K, Voronov B, Dzardanov A, Williams C and Sobolewski R 2001 Picosecond superconducting single-photon optical detector *Appl. Phys. Lett.* **79** 705–7

[163] Verevkin A, Zhang J, Sobolewski R, Lipatov A, Okunev O, Chulkova G, Korneev A, Smirnov K, Gol'tsman G N and Semenov A 2002 Detection efficiency of large-active-area nbn single-photon superconducting detectors in the ultraviolet to near-infrared range *Appl. Phys. Lett.* **80** 4687

[164] Rosenberg D, Lita A E, Miller A J and Nam S W 2005 Noise-free high-efficiency photon-number-resolving detectors *Phys. Rev.* A **71** 061803

[165] Gol'tsman G *et al* 2007 Middle-infrared to visible-light ultrafast superconducting single-photon detectors *IEEE Trans. Appl. Supercond.* **17** 246–51

[166] Lita A E, Miller A J and Nam S W 2008 Counting near-infrared single-photons with 95% efficiency *Opt. Express* **16** 3032–40

[167] Divochiy A *et al* 2008 Superconducting nanowire photon-number-resolving detector at telecommunication wavelengths *Nat. Photonics* **2** 302–6

[168] Ladd T D, Jelezko F, Laflamme R, Nakamura Y, Monroe C and O'Brien J L 2010 Quantum computers *Nature* **464** 45–53

[169] Mandel O, Greiner M, Widera A, Rom T, Hansch T W and Bloch I 2003 Controlled collisions for multi-particle entanglement of optically trapped atoms *Nature* **425** 937–40

[170] Weitenberg C, Endres M, Sherson J F, Cheneau M, Schauß P, Fukuhara T, Bloch I and Kuhr S 2011 Single-spin addressing in an atomic mott insulator *Nature* **471** 319–24

[171] André A, DeMille D, Doyle J M, Lukin M D, Maxwell S E, Rabl P, Schoelkopf R J and Zoller P 2006 A coherent all-electrical interface between polar molecules and mesoscopic superconducting resonators *Nat. Phys.* **2** 636–42

[172] Schoelkopf RJ and Girvin SM 2008 Wiring up quantum systems *Nature* **451** 664–9

[173] Verdú J, Zoubi H, Koller C, Majer J, Ritsch H and Schmiedmayer J 2009 Strong magnetic coupling of an ultracold gas to a superconducting waveguide cavity *Phys. Rev. Lett.* **103** 43603

[174] Togan E, Chu Y, Trifonov A S, Jiang L, Maze J, Childress L, Dutt MVG, Soerensen AS and Hemmer PR 2010 Quantum entanglement between an optical photon and a solid-state spin qubit *Nature* **466** 730–4

[175] Lukin MD 2003 Colloquium: trapping and manipulating photon states in atomic ensembles *Rev. Mod. Phys.* **75** 457–72

[176] Sherson J F, Krauter H, Olsson R K, Julsgaard B, Hammerer K, Cirac I and Polzik E S 2006 Quantum teleportation between light and matter *Nature* **443** 557–60 10

[177] Moehring DL, Maunz P, Olmschenk S, Younge KC, Matsukevich DN, Duan LM and Monroe C 2007 Entanglement of single-atom quantum bits at a distance *Nature* **449** 68–71

[178] Kimble H J 2008 The quantum internet *Nature* **453** 1023–30

[179] Olmschenk S, Matsukevich D N, Maunz P, Hayes D, Duan L-M and Monroe C 2009 Quantum teleportation between distant matter qubits *Science* **323** 486–9

[180] Duan L M and Monroe C 2010 Colloquium: quantum networks with trapped ions *Rev. Mod. Phys.* **82** 1209

[181] Hafezi M, Kim Z, Rolston SL, Orozco LA, Lev BL and Taylor JM 2012 Atomic interface between microwave and optical photons *Phys. Rev.* A **85** 020302

[182] Vitali D, Barzanjeh S, Abdi M, Tombesi P and Milburn G J 2012 A reversible optical to microwave quantum interface *Quantum Information and Measurement* (Washington, DC: Optical Society of America)

[183] Ritter S *et al* 2012 An elementary quantum network of single atoms in optical cavities *Nature* **484** 195–200

[184] Hofmann J, Krug M, Ortegel N, Gérard L, Weber M, Rosenfeld W and Weinfurter H 2012 Heralded entanglement between widely separated atoms *Science* **337** 72–75