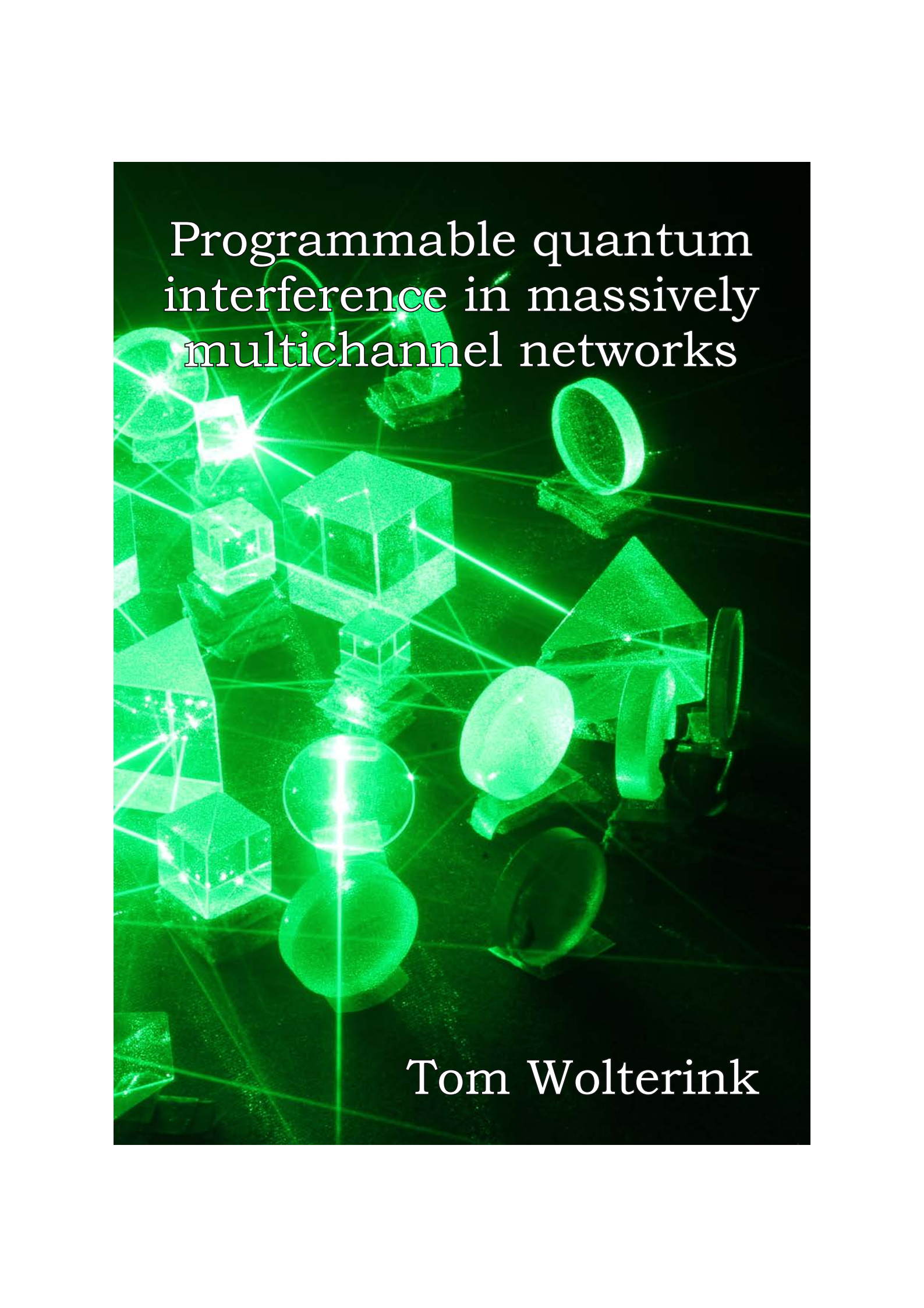


The background is a dark, textured surface with a complex arrangement of translucent green geometric shapes, including cubes, spheres, and pyramids. These shapes are interconnected by a network of bright green lines and rays, creating a sense of depth and connectivity. The overall aesthetic is futuristic and scientific, with a strong emphasis on the color green.

Programmable quantum interference in massively multichannel networks

Tom Wolterink

PROGRAMMABLE QUANTUM
INTERFERENCE IN MASSIVELY
MULTICHANNEL NETWORKS

Programmeerbare
kwantuminterferentie in netwerken
met myriaden kanalen

Promotiecommissie

Promotor	prof. dr. P.W.H. Pinkse
Copromotoren	prof. dr. K.-J. Boller prof. dr. W.L. Vos
Voorzitter en secretaris	prof. dr. ir. J.W.M. Hilgenkamp
Overige leden	prof. dr. A. Fiore dr. ir. H.L. Offerhaus prof. dr. I.A. Walmsley prof. dr. ir. W.G. van der Wiel

Cover image: photograph of laser beams by Kasper Orsel, Ravitej Uppu, and Tom Wolterink.

The work described in this thesis was carried out at the Complex Photonic Systems chair and the Laser Physics and Nonlinear Optics chair, Department of Science and Technology and MESA+ Institute for Nanotechnology, University of Twente, P.O. Box 217, 7500 AE Enschede, The Netherlands.

© 2016 Tom Wolterink
ISBN: 978-90-365-4214-2

PROGRAMMABLE QUANTUM INTERFERENCE IN MASSIVELY MULTICHANNEL NETWORKS

PROEFSCHRIFT

ter verkrijging van
de graad van doctor aan de Universiteit Twente,
op gezag van de rector magnificus,
prof. dr. H. Brinksma,
volgens besluit van het College voor Promoties
in het openbaar te verdedigen
op woensdag 26 oktober 2016 om 14.45 uur

door

Tom Aloys Wilhelmus Wolterink

geboren op 24 september 1987
te Winterswijk

Dit proefschrift is goedgekeurd door de promotor

prof. dr. P.W.H. Pinkse

en de copromotoren

prof. dr. K.-J. Boller

prof. dr. W.L. Vos

Contents

1	Introduction	1
1.1	Quantum interference	1
1.2	Quantum communication	3
1.3	Integrated optical networks	4
1.4	This thesis	4
2	Programmable linear networks	7
2.1	Quantum interference at a beam splitter	7
2.1.1	Beam splitters	7
2.1.2	Hong-Ou-Mandel interference	8
2.1.3	Lossy beam splitter	10
2.2	Quantum optics of lossy asymmetric beam splitters	12
2.2.1	Introduction	12
2.2.2	Energy constraints	13
2.2.3	Quantum interference of two single photons	15
2.2.4	Hong-Ou-Mandel-like interference	19
2.2.5	Discussion and conclusions	19
2.3	Arbitrarily programmable networks	22
2.4	Programmability by control of many input states	25
3	The single-photon source	27
3.1	Spontaneous parametric down-conversion	27
3.2	Experimental setup	28
3.3	Single-photon spectrum	29
3.4	Hong-Ou-Mandel interference	32
3.5	Multiphoton states	34
3.6	Non-degenerate single-photon pairs	37
3.7	Discussion	39
4	Programmable multiport optical circuits in opaque scattering materials	41
4.1	Introduction	41
4.2	Algorithm	43
4.3	Experimental setup and methods	49
4.3.1	Experimental setup	49
4.3.2	Measurement method	49
4.4	The 2×2 optical circuit	50
4.5	The 2×3 optical circuit	55
4.6	Conclusions and outlook	55

5	Programmable two-photon quantum interference in 10^3 channels in opaque scattering media	57
5.1	Introduction	57
5.2	Experimental setup	59
5.3	Model	61
5.4	Results	62
5.5	Discussion	65
6	Quantum-secure communication	67
6.1	Quantum-secure authentication	67
6.2	Authenticated quantum key distribution	68
6.3	Experimental setup	70
6.4	Results on authenticated quantum key distribution	72
6.5	PUF-enabled asymmetric quantum communication	78
6.6	Results on PUF-enabled asymmetric quantum communication . .	80
6.7	Discussion	80
7	Control of light propagation in integrated optical networks	83
7.1	Introduction	83
7.2	Model	84
7.3	Sample description	87
7.4	Experimental setup	88
7.5	Results	89
7.6	Discussion	93
8	Outlook	95
8.1	Straightforward extensions	95
8.2	New elements	95
8.3	Applications	96
A	Detailed drawing of the experimental setup	99
	References	101
	Summary	113
	Samenvatting	115

1 Introduction

1.1 Quantum interference

Even in our day and age, the quantum nature of light remains puzzling. We have been taught in school that light sometimes behaves as a wave and sometimes as a particle. A textbook example of a demonstration of this dual behaviour is Young's double-slit experiment. The result of that experiment can be understood with the wave-particle duality. But there are quantum interference experiments where our intuition is challenged even further.

A fascinating example is the case of two single photons impinging on different sides of a beam splitter. If the two photons are completely identical, i.e., not distinguishable by any means such as wavelength, polarization, or arrival time, the photons interact and bunch together to exit through a single output of the beam splitter. While the resulting output is a priori undetermined, both photons will definitely exit together. This quantum interference effect is known as the Hong-Ou-Mandel effect [1], and is famous in the field of quantum optics. It is used as a benchmark test for the non-classical behaviour of light. While this effect can be easily derived theoretically, and is discussed in almost every introductory textbook on quantum optics [2], even an expert scientist may lack a simple intuitive explanation.

Still, it is the Hong-Ou-Mandel effect that lies at the heart of all linear optical quantum information processing. Generalized to more dimensions [3], in networks containing a large number of channels, quantum interference can be employed to construct programmable quantum logic gates [4, 5], which are required for the construction of universal quantum computers [6–8]. Probably closer to realization are quantum simulators of, for instance, chemical processes [9–12], and a class of devices that are called boson samplers.

Boson samplers are tackling the boson sampling problem [13]. This problem concerns the quantum walk of multiple single-photon states through a linear optical network with a large number of channels. In short, the boson sampling problem raises essentially the question: what is the distribution of photons at the outputs of the network given a specific input state to the network? While this may seem a straightforward and easy calculation, it is intriguing that this is not simple at all. Estimating the distribution numerically requires calculation of matrix permanents, for which no classical efficient algorithm exists. The permanent of a matrix is similar to a matrix determinant, but with all positive signs. Alternatively, one could perform an experiment many times, each time sampling the output distribution of the photons. Boson sampling is of interest, since it probably is the quantum system closest to realization that can outperform a classical computer, albeit in the single task of sampling this distribution. Indeed, first experimental demonstrations of boson sampling in small networks have been shown to successfully sample the output distribution of the photons [14–21]. The classically intractable realm can already be reached in systems containing about twenty photons in four hundred channels [13, 22]. It is envisaged

that specific hard calculation problems might in future be mapped onto a boson sampling problem, and thus be solved using a quantum system. At present, no mapping of a practically useful problem has been found.

Any realization of large-scale optical quantum information processing, whether it is boson sampling, quantum simulation, or quantum computing, requires complete control over the generation, interaction, and detection of single photons. Each of these aspects is challenging in itself. In linear optical quantum computing, the interaction between photons occurs in a large linear optical network. The focus of this thesis lies on constructing large-scale optical networks with suitable, programmable, functionality.

At first glance opaque scattering media, such as white paint or paper, are absolutely useless for functional optical networks. Light waves propagating through an opaque scattering medium exhibit a random walk inside the medium, which is caused by multiple scattering from spatial inhomogeneities [23–25]. Coherent light incident on opaque scattering media gives rise to speckle patterns as a result of collective interference of the scattered waves. Correlations are induced between individual speckle spots, as if light would have propagated through a complex random linear optical network [26]. The opaque scattering medium couples a large number of input channels to a similarly large number of output channels [27]; in quantum terms, it has a high dimensionality. The number of coupled channels easily exceeds millions. Therefore one can view an opaque scattering medium as a massively multichannel linear optical network.

Recently it has been pioneered in Twente that a complete control over the propagation of light in opaque scattering media can be obtained using wavefront shaping [28–30]. By adaptive (phase) modulation of the incident wavefront, one can control the interference of all scattered waves contributing to a target speckle spot. Wavefront shaping is known for focusing and imaging through multiple-scattering media. Furthermore, it can be used to transform speckle patterns of opaque scattering media to act as linear optical elements, such as waveguides and lenses [29, 31], pulse compressors [32–34], wave plates [35] and beam splitters [36, 37]. These elements can be used to construct linear optical networks with arbitrary functionality. Since wavefront shaping is an adaptive technique that modulates only the incident light, not the scattering medium itself, the functionality of a linear optical network constructed by wavefront shaping is inherently programmable.

Because of their large number of controllable channels, allowing for programmable massively multichannel networks, opaque scattering media are of relevance to quantum information processing. Starting from work in Twente, it has been observed that quantum states are robust against multiple scattering [38–44]. Nevertheless it has so far remained an open question if quantum interference of multiple photons, required for quantum information processing, could be demonstrated with a multiple-scattering medium.

1.2 Quantum communication

Quantum properties of light are readily used in real-world applications. An example of a current, commercially available, application is in secure communication. It is well-known that secretly exchanging messages between two distant parties requires that the sender and receiver share a secret key. These keys can be used for one-time encryption of a message on a public classical channel, before new keys have to be distributed for subsequent encryption. Quantum key distribution (QKD), i.e., making use of the quantum properties of light and matter, has emerged as a method to securely distribute keys. The security of this method is directly rooted in quantum-physical principles.

A well-known protocol for quantum key distribution is the so-called BB84 protocol [45]. Here, two mutually unbiased bases are used, at both the sender and receiver, to transmit bits between sender and receiver. Two orthonormal bases are called mutually unbiased when, for a system prepared in a state of the first basis, all outcomes of a measurement in the other basis are equally probable. In the original implementation, the information is encoded in the polarization of single photons. The first basis consists of horizontal-vertical polarization. In this basis, a zero (0) for binary encoding may be represented by a horizontally polarized photon, and one (1) by a vertically polarized photon. The second basis is diagonal-antidiagonal polarization, with diagonal polarization representing 0, and antidiagonal polarization 1. Performing a measurement in the wrong basis reveals no information about the polarization of a photon, and therefore no information on the data. In the BB84 protocol, the sender transmits a string of random bits, encoded in the polarization of single photons, for each bit randomly choosing the basis to encode in. The receiver performs a measurement of these photons, independently choosing a random basis for each measurement as well. On average, the receiver will have chosen the wrong basis 50% of the time. Next, both parties communicate over a public classical channel to sift out the bits which were sent and received using the same basis without, however, telling the values of these bits. After some additional error checks to determine if an eavesdropper has been present (who due to the no-cloning theorem, which states that it is impossible to make a perfect copy of a quantum state, will introduce an error rate of 25%), the remaining unpublished bits are used to establish a shared key, only known to the sender and receiver. This key can now be used to encrypt a message of the same length as the key. The encrypted message can be safely sent over a public channel.

This method of distributing keys is perfectly secure, provided that the identity of the receiver has been authenticated. If this is not the case, the protocol is vulnerable for the so-called man-in-the-middle attack, where an adversary takes over the control of the communication while sender and receiver think that they are communicating directly with each other. A common method of authentication is performed using an initial shared secret, which has to have been exchanged between sender and receiver previously, and which has to be

stored secretly. Since storage of secrets is highly undesired, integrating a means of authentication directly into a protocol for quantum key distribution would be highly desirable.

1.3 Integrated optical networks

The wavefront-shaping technique we use to create linear optical networks with programmable functionality is not limited to opaque scattering media, but can also be applied to massively multichannel networks in integrated optics. Due to the high throughput of integrated optics, these networks are relevant to high-tech and on-chip implementations of quantum information processing. It is essential for constructing programmable linear optical networks by wavefront shaping on massively multichannel networks in integrated optics to understand the propagation of light through these networks. A first step to this end pursued in this thesis is to investigate the propagation of light through an integrated optical network with a large number of channels, that has a well-defined and simple geometry, such as an array of evanescently coupled waveguides.

1.4 This thesis

In this thesis, we demonstrate two-photon quantum interference in a massively multichannel linear optical network realized in an opaque scattering medium. Using adaptive phase modulation of the incident photons, the scattering medium is transformed to behave as a fully programmable beam splitter. Since the selected channels stem from a manifold of millions of channels, the programmed network need not fulfil energy conservation and could thus be lossy.

Surprisingly, losses are not detrimental. In fact, the losses introduce new freedom to the networks, in that the quantum correlations can be controlled and programmed to an extent not possible with a lossless network. In chapter 2, we theoretically investigate quantum interference of two single photons at a lossy asymmetric beam splitter, the most general passive 2×2 optical network. In this context, the current theoretical analysis establishes how the losses introduce a novel dimensionality to the networks. The level of programmability introduced by the losses is calculated and analyzed.

To demonstrate quantum interference in massively multichannel networks we require a source of multiple indistinguishable single-photon states. Since the networks of interest can easily contain thousands of channels over which the photons are distributed, a high-stability, high-brightness source is desired. We have constructed a versatile quantum light source based on spontaneous parametric down-conversion, whose output can be easily tuned from pure single-photon states to quantum states with a high photon number. Chapter 3 contains the description and characterization of the single-photon source.

In chapter 4 we introduce a method to program the functionality of general multiport linear optical networks in opaque scattering media by phase modulation of incident wavefronts. We demonstrate the power of our method by programming linear optical networks in white paint with 2 inputs and 2 outputs, and 2 inputs and 3 outputs. Using interferometric techniques we verify our ability to program any desired phase relation between the outputs.

The first demonstration of two-photon quantum interference in a massively multichannel linear optical network realized in an opaque scattering medium is presented in chapter 5. We observe two-photon quantum interference in a fully programmable 2×2 beam splitter. Exploiting the new freedom introduced by the losses, we not only show the well-known Hong-Ou-Mandel bunching of photons, but also demonstrate that this bunching can be made to vanish, or be transformed into antibunching.

While this demonstration of programmable quantum interference in opaque scattering media is at first of fundamental interest, the knowledge acquired about quantum transport in scattering media can be directly utilized towards applications. The high complexity offered by opaque scattering media is being used for applications in secure authentication, based on the quantum-secure readout of a physical unclonable function [46]. In chapter 6, we extend these ideas to authentication of secure communication. We create the first authenticated protocol for quantum key distribution, that removes the need of an initial shared secret for authentication of the parties. Moreover, we introduce and demonstrate the first protocol for authenticated and asymmetric quantum communication.

Finally, in chapter 7 we apply wavefront-shaping techniques, commonly employed on opaque scattering media, to networks in integrated optics. We show first steps in the control over the propagation of light through an array of evanescently coupled waveguides. Due to the high throughput of integrated optics, it is an attractive platform to program quantum interference between a large number of modes in these massively multichannel networks.

2 Programmable linear networks

Multiphoton quantum correlations are crucial for quantum information processing and quantum communication protocols in linear optical networks [6, 7]. For large-scale implementation of quantum information processing and quantum simulators, such as boson sampling [13–21] or programmable quantum logic gates [4, 5], a programmable functionality of a massively multichannel network is required. Beam splitters form a fundamental component in the implementation of these linear optical networks [47]. Starting from a generic beam splitter, the theoretical analysis in this chapter shows that losses in optical networks, which are unavoidable in experiments, introduce a novel dimensionality to the networks in that the functionality of the network [36, 37], and thus also quantum interference [48, 49], is programmable. By implementing losses in the form of uncontrolled and unmonitored channels of a massively multichannel network, it is possible to construct a fully programmable linear optical network. In this way one can induce programmable multiphoton correlations, which can be applied to a variety of useful quantum information processing and simulation protocols [8, 9].

2.1 Quantum interference at a beam splitter

2.1.1 Beam splitters

The simplest non-trivial linear optical network is a beam splitter. A 50:50 (balanced) beam splitter possesses two input ports a_1, a_2 and two output ports b_1, b_2 , as drawn in Fig. 2.1. The electric fields of light waves at the inputs and outputs

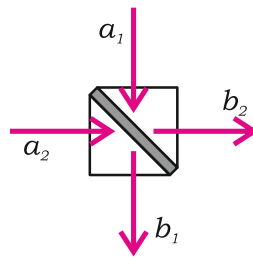


Figure 2.1 Schematic of a 50:50 beam splitter with two input ports a_1, a_2 and two output ports b_1, b_2 .

are related as:

$$\begin{bmatrix} E_{b_1} \\ E_{b_2} \end{bmatrix} = S \begin{bmatrix} E_{a_1} \\ E_{a_2} \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} \begin{bmatrix} E_{a_1} \\ E_{a_2} \end{bmatrix}, \quad (2.1)$$

where a symmetric representation of the beam splitter was used. S is the unitary scattering matrix of the beam splitter. The amplitudes of all four reflection and transmission coefficients are equal to $1/\sqrt{2}$, and at both reflections the light acquires a phase shift of $\pi/2$, while there is no phase shift for the transmissions. A physical realization of the beam splitter in Eq. (2.1) is for instance the symmetric beam splitter cube: a multilayer stack between two right-angle prisms, schematically drawn in Fig. 2.1.

One often also encounters other representations of a balanced beam splitter, where the total phase shift of π , that is required by conservation of energy, is distributed differently over the reflection and transmission coefficients. All these representations are physically equivalent, and the representation which exactly matches an experiment depends on the construction of the beam splitter [50]. For instance, for a 50% reflection at a single interface between two dielectrics, the suitable way to represent the beam splitter is:

$$\begin{bmatrix} E_{b_1} \\ E_{b_2} \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} E_{a_1} \\ E_{a_2} \end{bmatrix}, \quad (2.2)$$

where the light only acquires a phase shift of π at the reflection of the optically denser medium, as dictated by the Fresnel equations. Throughout this section the symmetric representation of the beam splitter will be used.

The description required for studying quantum interference at a beam splitter is given by the same scattering matrix as in Eq. (2.1). Quantum-mechanically, the input and outputs of the beam splitter are related through

$$\begin{bmatrix} \hat{a}_{b_1} \\ \hat{a}_{b_2} \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} \begin{bmatrix} \hat{a}_{a_1} \\ \hat{a}_{a_2} \end{bmatrix}, \quad (2.3)$$

where $\hat{a}_i$ is the annihilation operator for the input or output mode i .

2.1.2 Hong-Ou-Mandel interference

A famous example of quantum interference is the interference between two photons at a beam splitter. Consider a single photon incident in each of the two inputs of the beam splitter, in the state $|1_{a_1}, 1_{a_2}\rangle$. The two photons are assumed to be identical, hence indistinguishable, with regard to all of their physical properties. By inverting Eq. (2.3) and taking the Hermitian conjugate

$$\begin{bmatrix} \hat{a}_{a_1}^\dagger \\ \hat{a}_{a_2}^\dagger \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} \begin{bmatrix} \hat{a}_{b_1}^\dagger \\ \hat{a}_{b_2}^\dagger \end{bmatrix}, \quad (2.4)$$

the propagation of the input state $|1_{a_1}, 1_{a_2}\rangle = \hat{a}_{a_1}^\dagger \hat{a}_{a_2}^\dagger |0_{a_1}, 0_{a_2}\rangle$ can be calculated:

$$\begin{aligned}
 |1_{a_1}, 1_{a_2}\rangle &\rightarrow \frac{1}{\sqrt{2}} \left(\hat{a}_{b_1}^\dagger + i\hat{a}_{b_2}^\dagger \right) \frac{1}{\sqrt{2}} \left(i\hat{a}_{b_1}^\dagger + \hat{a}_{b_2}^\dagger \right) |0_{b_1}, 0_{b_2}\rangle \\
 &= \frac{1}{2} \left(i\hat{a}_{b_1}^\dagger \hat{a}_{b_1}^\dagger + \hat{a}_{b_1}^\dagger \hat{a}_{b_2}^\dagger - \hat{a}_{b_1}^\dagger \hat{a}_{b_2}^\dagger + i\hat{a}_{b_2}^\dagger \hat{a}_{b_2}^\dagger \right) |0_{b_1}, 0_{b_2}\rangle \\
 &= \frac{1}{\sqrt{2}} i \left(|2_{b_1}, 0_{b_2}\rangle + |0_{b_1}, 2_{b_2}\rangle \right). \tag{2.5}
 \end{aligned}$$

The surprising result is that the two photons leave the beam splitter through the same single output: either b_1 , or b_2 , which is called bunching. Equation (2.5) shows that the output state is in a superposition of two photons in output b_1 and two photons in output b_2 . This effect is known as Hong-Ou-Mandel (HOM) interference [1], and is caused by destructive interference of the two indistinguishable paths for the photons to arrive at different outputs. The interference can be measured by detecting the absence of coincidences between two detectors placed in the two output arms of the beam splitter.

For comparison, when the two photons are distinguishable, the photons do not interfere and the interaction of each photon with the beam splitter can be considered separately. Each of the photons has a 50% probability to be reflected or transmitted. In that case there is a 50% probability for both photons to arrive at different detectors, resulting in a coincidence. This different behaviour for distinguishable and indistinguishable photons leads to the common way for measuring Hong-Ou-Mandel interference. One records the number of coincidences between detectors in both outputs while varying the time delay between the arrival of the two photons at the beam splitter. By varying the difference in arrival times of the two photons one changes the indistinguishability of the photons. When they arrive simultaneously, the photons are indistinguishable. The Hong-Ou-Mandel interference shows up as a dip in the coincidences around zero time delay with a visibility of 100%, with the usual definition of the visibility of $V \equiv (P_{\text{indist}} - P_{\text{dist}}) / P_{\text{dist}}$, where P_{dist} and P_{indist} are the coincidence probabilities of distinguishable and indistinguishable photons, respectively. For more information about the Hong-Ou-Mandel dip, see section 2.2 and 3.4. Originally, Hong-Ou-Mandel interference was presented as a method to measure short time intervals [1].

For two indistinguishable single-photon states $|1_{a_1}, 1_{a_2}\rangle$ incident on the beam splitter the $\hat{a}_{b_1}^\dagger \hat{a}_{b_2}^\dagger$ terms in Eq. (2.5) fully vanish, resulting in a complete absence of coincidences between the two outputs. This changes when more photons are present in the inputs. For example, in case of a two-photon state $|2_{a_1}, 2_{a_2}\rangle$ incident in each of the inputs the $\hat{a}_{b_1}^\dagger \hat{a}_{b_2}^\dagger$ terms do not fully cancel. Due to the interference at the beam splitter the coincidence probability is still lower for indistinguishable photons than for distinguishable photons, but the probability does not drop to zero. The visibility of the interference dip now reaches a maximum of 71%, which can be derived using a similar procedure as in Eq. (2.5). For Fock states with an increasing number of photons the visibility of the Hong-

Ou-Mandel interference decreases [51, 52]. In case that the quantum states are produced by a spontaneous parametric down-conversion process (see chapter 3), the visibility decreases with increasing pump power, with a lower bound of 33% [53–55].

Observation of Hong-Ou-Mandel interference is usually interpreted as quantum behaviour of light. Indeed, for coherent state inputs $|\alpha_{a_1}, \alpha_{a_2}\rangle$, no Hong-Ou-Mandel interference occurs. In this case the output state, calculated in the same way as Eq. (2.5), is simply $|\alpha_{b_1}, \alpha_{b_2}\rangle$, ignoring any phase factors. Classical light can show interference effects similar to the Hong-Ou-Mandel dip. However, the visibility for any classical light input is bound to 50% [56], which can be reached using coherent-state inputs with rapidly varying phases. A visibility exceeding this bound of 50% is only possible for quantum states of light.

Whereas in this section the input-output formalism was used to calculate the output state of a single photon incident on each port of a beam splitter, one can also use a direct approach to determine the output state $|\Psi_{\text{out}}\rangle$ from the input state $|\Psi_{\text{in}}\rangle$.

$$|\Psi_{\text{out}}\rangle = \hat{S} |\Psi_{\text{in}}\rangle. \quad (2.6)$$

In this representation $\hat{S}$ is the beam splitter operator. The explicit form of $\hat{S}$ can be determined from the scattering matrix S for the annihilation operators of the beam splitter, given in Eq. (2.1) [83, 84]. This explicit form of $\hat{S}$ will be used in section 2.4;

The destructive interference of the $\hat{a}_{b_1}^\dagger \hat{a}_{b_2}^\dagger$ terms in Eq. (2.5) arises from the total phase shift of π inherent to the beam splitter. This π phase shift is required by the unitarity of the beam splitter, and ensures energy conservation. Suppose one could change this phase shift to deviate from π , then the $\hat{a}_{b_1}^\dagger \hat{a}_{b_2}^\dagger$ terms in Eq. (2.5) would not necessarily vanish, and even anti-bunching of photons could be observed for single-photon inputs. For this reason, in the next section a lossy beam splitter will be discussed, which does not necessarily fulfil unitarity and can allow a phase shift deviating from π .

2.1.3 Lossy beam splitter

A lossy balanced beam splitter can be described as:

$$\begin{bmatrix} E_{b_1} \\ E_{b_2} \end{bmatrix} = t \begin{bmatrix} 1 & 1 \\ 1 & e^{i\alpha} \end{bmatrix} \begin{bmatrix} E_{a_1} \\ E_{a_2} \end{bmatrix}. \quad (2.7)$$

The amplitudes of all four reflection and transmission coefficients are assumed to be equal and are denoted by t . α represents the total phase shift of the beam splitter, which is here for simplicity assigned to a single transmission coefficient. Since this beam splitter is lossy it need not fulfil energy conservation and could thus be non-unitary. Note that for a lossless balanced beam splitter $t = 1/\sqrt{2}$ and $\alpha = \pi$. By considering that the total output power should be less than or

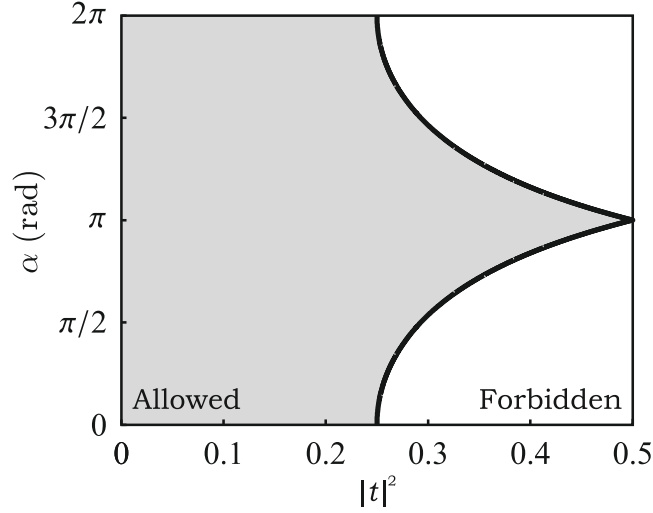


Figure 2.2 The allowed phase α as a function of transmittance $|t|^2$ for the balanced beam splitter (grey area). The white region is forbidden because of energy conservation.

equal to the input power, i.e.,

$$|E_{a_1}|^2 + |E_{a_2}|^2 \geq |E_{b_1}|^2 + |E_{b_2}|^2, \quad (2.8)$$

one can derive upper and lower bounds for the phase α as a function of the transmission coefficient t of the beam splitter:

$$\left| \cos \frac{\alpha}{2} \right| \leq \frac{1}{2t^2} - 1. \quad (2.9)$$

The bounds for α , as calculated with Eq. (2.9), are visualized in Fig. 2.2. The shaded area indicates the allowed values for α . The white region is forbidden since here the beam splitter would violate conservation of energy. At $t = 1/\sqrt{2}$ only $\alpha = \pi$ is allowed, which corresponds to a lossless beam splitter. For losses above 50%, i.e., for $t \leq 1/2$ the phase α is completely free. This shows that by introducing losses to a balanced beam splitter the restrictions on the phase in the beam splitter can be lifted, which has an impact on interference, both classical and quantum-mechanical. In the following section the effects of loss on the quantum interference at a general 2×2 beam splitter will be discussed.

2.2 Quantum optics of lossy asymmetric beam splitters

2.2.1 Introduction

We theoretically investigate quantum interference of two single photons at a lossy asymmetric beam splitter, the most general passive 2×2 optical circuit. The losses in the circuit result in a non-unitary scattering matrix with a non-trivial set of constraints on the elements of the scattering matrix. Our analysis using the noise operator formalism shows that the loss allows tunability of quantum interference to an extent not possible with a lossless beam splitter. Our theoretical studies support the experimental demonstrations of programmable quantum interference in highly multimodal systems such as opaque scattering media and multimode fibres.

Beam splitters form a fundamental component in the implementation of linear optical networks [47]. They have been realized in a variety of systems including integrated optics, atomic systems, scattering media, multimode fibres, superconducting circuits and plasmonic metamaterials [57–64]. In plasmonic systems, beam splitters have been used to generate coherent perfect absorption in the single-photon regime [65, 66] and on-chip two-plasmon interference [63, 64]. Losses are an inherent property of optical systems, i.e., unavoidable and arise from dispersive ohmic losses or from imperfect control and collection of light in dielectric scattering media. The effect of losses in beam splitters has attracted a lot of theoretical attention due to the fundamental implications of unavoidable dispersion in dielectric media [67–70]. However, all these studies have dealt with either symmetric (equal reflection-transmission amplitudes for both input arms) or balanced (equal reflection and transmission amplitudes in each arm) beam splitters. In this section, we analyze the most general two-port beam splitter which can be lossy, asymmetric and unbalanced, and find the non-trivial constraints on the matrix elements. We derive general expressions for the probabilities to detect zero, one or two photons in the two outputs when a single photon is injected in each of the two inputs. Furthermore, we comment on the possible measurements of quantum interference through coincidence detection in a Hong-Ou-Mandel-like setup [1]. The presented theoretical analysis establishes that losses allow programmability of quantum interference, which is required in a variety of useful quantum information processing and simulation protocols [6–9].

A general two-port beam splitter or a linear optical network consists of two input ports a_1, a_2 and two output ports b_1, b_2 as schematized in Fig. 2.3(a). The linearity of the beam splitter gives rise to a linear relation between the electric fields, $E(b_i) = \sum_j s_{ij} E(a_j)$. The complex numbers s_{ij} are the elements of a scattering matrix S and correspond to the transmission and reflection coefficients $s_{11} = t \exp i\phi_{11}$, $s_{22} = \tau \exp i\phi_{22}$, $s_{12} = \rho \exp i\phi_{12}$, and $s_{21} = r \exp i\phi_{21}$, where

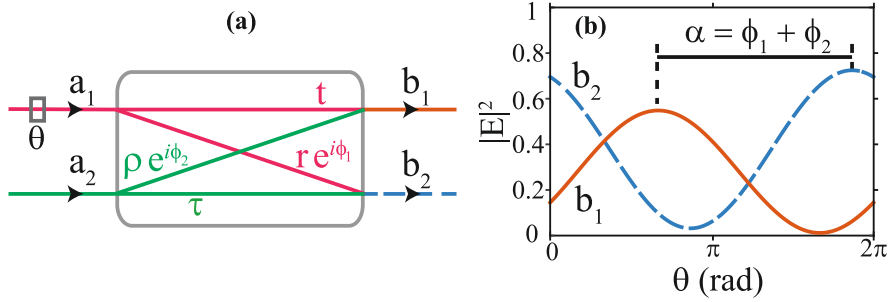


Figure 2.3 (a) Schematic of a general 2×2 beam splitter with input ports a_1 and a_2 and output ports b_1 and b_2 . The transmission-reflection amplitudes for light in input ports a_1 and a_2 are t - r and τ - ρ respectively. (b) Output power at ports b_1 (orange curve) and b_2 (blue curve) as phase θ is varied between 0 and 2π at input port a_1 . The phase between the peak amplitudes α is related to the phases of the reflection coefficients ϕ_1 and ϕ_2 as $\alpha = \phi_1 + \phi_2$.

t, τ, r, ρ are positive real numbers. The phases ϕ_{ij} are not all independent and can be reduced to ϕ_1 and ϕ_2 which correspond to the phase differences between transmission and reflection at a given input port. This gives the scattering matrix the following form:

$$S = \begin{bmatrix} t & \rho e^{i\phi_2} \\ r e^{i\phi_1} & \tau \end{bmatrix}. \quad (2.10)$$

Without further constraints on the matrix elements, the scattering matrix S need not be unitary. Special cases include the balanced beam splitter where $\tau = \rho$; $t = r$ and the symmetric beam splitter where $\tau = t$; $\rho \exp(i\phi_2) = r \exp(i\phi_1)$.

The six parameters in the scattering matrix are required to describe the behaviour of the output intensities. Fig. 2.3(b) illustrates the intensities $|E|^2$ at b_1 and b_2 as the phase of the input coherent field at a_1 is varied with a fixed phase at a_2 . For a general beam splitter, the amplitudes, intensity offsets and phase offsets at the two output ports can be completely free. Of particular interest is the value of the phase α between the output peak intensities, which is related to the phases of the reflection coefficients ϕ_1 and ϕ_2 as $\alpha = \phi_1 + \phi_2$. This phase α determines the visibility of quantum interference between two single photons, as discussed in the subsequent sections.

2.2.2 Energy constraints

The beam-splitter scattering matrix in Eq. (2.10) is defined without any constraints on the parameters. However, the physical constraint that the output energy must be less than or equal to the input energy imposes restrictions on the parameters as derived below. Let us consider the scenario where coherent

states of light with fields E_1 and E_2 are incident at input ports a_1 and a_2 respectively. Energy conservation at a lossy beam splitter imposes the restriction that the total output powers in the arms should be less than or equal to the input,

$$|tE_1 + \rho e^{i\phi_2} E_2|^2 + |rE_1 e^{i\phi_1} + \tau E_2|^2 \leq |E_1|^2 + |E_2|^2. \quad (2.11)$$

The two input coherent state fields can be related through a complex number $c = |c|e^{-i\delta}$ as $E_2 = cE_1$, which gives

$$t\rho \cos(\phi_2 - \delta) + \tau r \cos(\phi_1 + \delta) \leq \frac{(1 - t^2 - r^2) + |c|^2(1 - \tau^2 - \rho^2)}{2|c|}. \quad (2.12)$$

As the inequality holds for all values of $|c|$, it should also hold in the limiting case where the right hand side of Eq. (2.12) is minimized. This occurs for $|c|^2 = (1 - t^2 - r^2)/(1 - \tau^2 - \rho^2)$. Upon substitution, the inequality becomes

$$t\rho \cos(\phi_2 - \delta) + \tau r \cos(\phi_1 + \delta) \leq \sqrt{(1 - t^2 - r^2)(1 - \tau^2 - \rho^2)}. \quad (2.13)$$

The above inequality can be algebraically manipulated using trigonometric identities into the following form

$$\sqrt{t^2\rho^2 + \tau^2r^2 + 2\tau\rho r t \cos(\phi_1 + \phi_2) \sin(\delta + \theta_{\text{off}})} \leq \sqrt{(1 - t^2 - r^2)(1 - \tau^2 - \rho^2)}, \quad (2.14)$$

where $\theta_{\text{off}} = \arctan[(t\rho \cos \phi_2 + \tau r \cos \phi_1)/(t\rho \sin \phi_2 - \tau r \sin \phi_1)]$. As the inequality holds for all values of δ , it should hold in the limiting case of the maximum value of the left hand side which occurs when $\delta + \theta_{\text{off}} = \pi/2$. Substituting $\alpha = \phi_1 + \phi_2$ results in the following inequality in terms of the reflection and transmission amplitudes

$$\sqrt{t^2\rho^2 + \tau^2r^2 + 2\tau\rho r t \cos \alpha} \leq \sqrt{(1 - t^2 - r^2)(1 - \tau^2 - \rho^2)}. \quad (2.15)$$

For the lossless beam splitter, the equality results in $\alpha = \pi$. For a symmetric balanced beam splitter, i.e., $t = r = \tau = \rho$ and $\phi_1 = \phi_2$, Eq. (2.10) reduces to the well-known beam splitter matrix [2]

$$S_{\text{sym-bal}} = t \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}. \quad (2.16)$$

The inequality in Eq. (2.15) corresponds to the most general constraint on the parameters of a passive lossy asymmetric beam splitter. For the sake of clarity, we will discuss the specific case of a lossy symmetric beam splitter with $\tau = t$ and $\rho = r$. In this scenario, the inequality involves only three independent parameters

$$\left| \cos \frac{\alpha}{2} \right| \leq \frac{1 - t^2 - r^2}{2tr}. \quad (2.17)$$

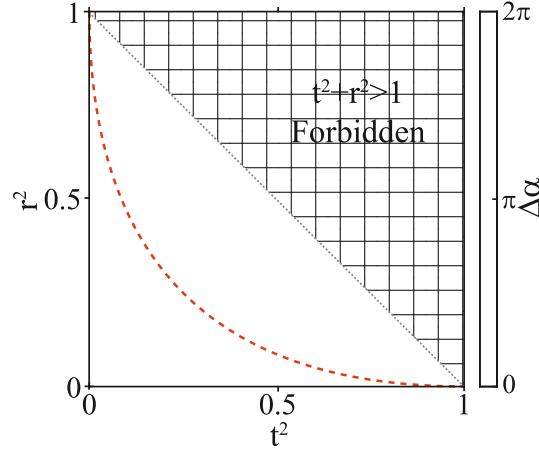


Figure 2.4 The figure depicts the allowed tunable width $\Delta\alpha$ around π . The anti-diagonal line ($r^2 + t^2 = 1$) separating the allowed from the forbidden region corresponds to lossless beam splitter. The red dashed line is the curve $t + r = 1$. Any lossy circuit that satisfies $t + r \leq 1$ allows complete tunability of $\alpha \in [0, 2\pi]$.

This inequality results in an allowed range of α between $[\pi - \frac{\Delta\alpha}{2}, \pi + \frac{\Delta\alpha}{2}]$. Fig. 2.4 depicts the tuning width $\Delta\alpha$ as a function of reflectance r^2 and transmittance t^2 . The lossless beam splitters lie on the diagonal line that separates the forbidden and allowed regions. Evidently, lossless beam splitters have $\Delta\alpha = 0$, i.e. the phase α between the output arms is fixed and equals π . With increasing losses in the beam splitter, $\Delta\alpha$ increases and achieves a maximum value of 2π , i.e., complete tunability of α . The beam splitters that exactly satisfy $t + r = 1$ correspond to those lossy beam splitters that allow completely programmable operation with maximum transmission or reflection. In the following section, we discuss the effect of this tunability on the quantum interference between two single photons incident at the input ports of the general beam splitter.

2.2.3 Quantum interference of two single photons

The quantum-mechanical input-output relation of the lossy asymmetric beam splitter can be written using the scattering matrix in Eq. (2.10). From this point, we explicitly take into account the optical-frequency dependence that is required to calculate the Hong-Ou-Mandel interference between non-monochromatic single photons incident at the input ports.

$$\begin{bmatrix} \hat{b}_1(\omega) \\ \hat{b}_2(\omega) \end{bmatrix} = \begin{bmatrix} t(\omega) & \rho(\omega)e^{i\phi_2} \\ r(\omega)e^{i\phi_1} & \tau(\omega) \end{bmatrix} \begin{bmatrix} \hat{a}_1(\omega) \\ \hat{a}_2(\omega) \end{bmatrix} + \begin{bmatrix} \hat{F}_1(\omega) \\ \hat{F}_2(\omega) \end{bmatrix}. \quad (2.18)$$

The operators $\hat{a}_i(\omega)$ and $\hat{b}_i(\omega)$ are creation-annihilation operators of photons at the input and output ports, respectively. The canonical commutation relations of these operators are satisfied even in the presence of loss:

$$[\hat{a}_i(\omega), \hat{a}_j(\omega')] = 0; \quad \forall i, j \in \{1, 2\}, \quad (2.19)$$

$$[\hat{a}_i(\omega), \hat{a}_j^\dagger(\omega')] = \delta_{ij}\delta(\omega - \omega'); \quad \forall i, j \in \{1, 2\}, \quad (2.20)$$

$$[\hat{b}_i(\omega), \hat{b}_j(\omega')] = 0; \quad \forall i, j \in \{1, 2\}, \quad (2.21)$$

$$[\hat{b}_i(\omega), \hat{b}_j^\dagger(\omega')] = \delta_{ij}\delta(\omega - \omega'); \quad \forall i, j \in \{1, 2\}. \quad (2.22)$$

The introduction of noise operators $\hat{F}_i(\omega)$ in Eq. (2.18), which represent quantum fluctuations, is necessary in the presence of loss as reported earlier [67, 71, 72]. We assume that the underlying noise process is Gaussian and uncorrelated across frequencies. The commutation relations of the noise operators can be calculated as the noise sources are independent of the input light, i.e.,

$$[\hat{a}_i(\omega), \hat{F}_j(\omega')] = [\hat{a}_i(\omega), \hat{F}_j^\dagger(\omega')] = 0; \quad \forall i, j \in \{1, 2\}, \quad (2.23)$$

which results in

$$[\hat{F}_i(\omega), \hat{F}_j(\omega')] = [\hat{F}_i^\dagger(\omega), \hat{F}_j^\dagger(\omega')] = 0; \quad \forall i, j \in \{1, 2\}, \quad (2.24)$$

$$[\hat{F}_1(\omega), \hat{F}_1^\dagger(\omega')] = \delta(\omega - \omega')[1 - t^2(\omega) - \rho^2(\omega)], \quad (2.25)$$

$$[\hat{F}_2(\omega), \hat{F}_2^\dagger(\omega')] = \delta(\omega - \omega')[1 - \tau^2(\omega) - r^2(\omega)], \quad (2.26)$$

$$[\hat{F}_1(\omega), \hat{F}_2^\dagger(\omega')] = -\delta(\omega - \omega')[t(\omega)r(\omega)e^{-i\phi_1} + \rho(\omega)\tau(\omega)e^{i\phi_2}], \quad (2.27)$$

$$[\hat{F}_2(\omega), \hat{F}_1^\dagger(\omega')] = -\delta(\omega - \omega')[t(\omega)r(\omega)e^{i\phi_1} + \rho(\omega)\tau(\omega)e^{-i\phi_2}]. \quad (2.28)$$

To calculate the effect of the quantum interference, let us suppose that a single photon with frequency ω_1 is incident at input a_1 and another single photon with frequency ω_2 is incident at input a_2 . The two photons together have a bi-photon amplitude $\psi(\omega_1, \omega_2)$ which results in the following input state,

$$|\Psi\rangle = |1_1, 1_2\rangle = \int_0^\infty d\omega_1 \int_0^\infty d\omega_2 \psi(\omega_1, \omega_2) \hat{a}_1^\dagger(\omega_1) \hat{a}_2^\dagger(\omega_2) |0\rangle. \quad (2.29)$$

The bi-photon amplitude $\psi(\omega_1, \omega_2)$ is normalized as $\int_0^\infty d\omega_1 \int_0^\infty d\omega_2 |\psi(\omega_1, \omega_2)|^2 = 1$, ensuring that the state vector $|\Psi\rangle$ is normalized.

In a lossy beam splitter, there are in total six possible outcomes with either two, one or zero photons at each output port. The probabilities of these outcomes can be represented as expectation values of the number operators for the output ports, defined as

$$\hat{N}_i(\omega) = \int_0^\infty d\omega \hat{b}_i^\dagger(\omega) \hat{b}_i(\omega) \quad i \in \{1, 2\}. \quad (2.30)$$

Assuming that detectors have a quantum efficiency of unity, the probabilities can be calculated using the Kelley-Kleiner counting formulae [73] and can be grouped into 3 sets:

1. No photon lost

$$P(2_1, 0_2) = \frac{1}{2} \langle \hat{N}_1(\hat{N}_1 - 1) \rangle, \quad (2.31)$$

$$P(0_1, 2_2) = \frac{1}{2} \langle \hat{N}_2(\hat{N}_2 - 1) \rangle, \quad (2.32)$$

$$P(1_1, 1_2) = \langle \hat{N}_1 \hat{N}_2 \rangle. \quad (2.33)$$

2. One photon lost

$$P(1_1, 0_2) = \langle \hat{N}_1 \rangle - \langle \hat{N}_1(\hat{N}_1 - 1) \rangle - \langle \hat{N}_1 \hat{N}_2 \rangle, \quad (2.34)$$

$$P(0_1, 1_2) = \langle \hat{N}_2 \rangle - \langle \hat{N}_2(\hat{N}_2 - 1) \rangle - \langle \hat{N}_1 \hat{N}_2 \rangle. \quad (2.35)$$

3. Both photons lost

$$P(0_1, 0_2) = 1 - \langle \hat{N}_1 \rangle - \langle \hat{N}_2 \rangle + \langle \hat{N}_1 \hat{N}_2 \rangle + \frac{1}{2} \langle \hat{N}_1(\hat{N}_1 - 1) \rangle + \frac{1}{2} \langle \hat{N}_2(\hat{N}_2 - 1) \rangle. \quad (2.36)$$

Of particular interest is the coincidence probability $P(1_1, 1_2)$ which decreases to zero at a lossless, symmetric balanced beam splitter, due to Hong-Ou-Mandel interference [1].

Under the assumption that the coefficients t, r, τ, ρ are frequency independent, the expectation values of the number operators are

$$\langle \hat{N}_1 \rangle = t^2 + \rho^2, \quad (2.37)$$

$$\langle \hat{N}_2 \rangle = \tau^2 + r^2, \quad (2.38)$$

$$\langle \hat{N}_1(\hat{N}_1 - 1) \rangle = 2t^2\rho^2[1 + I_{\text{ov}}(\delta t)], \quad (2.39)$$

$$\langle \hat{N}_1(\hat{N}_1 - 1) \rangle = 2\tau^2r^2[1 + I_{\text{ov}}(\delta t)], \quad (2.40)$$

$$\langle \hat{N}_1 \hat{N}_2 \rangle = t^2\tau^2 + r^2\rho^2 + 2\tau\rho tr I_{\text{ov}}(\delta t) \cos \alpha, \quad (2.41)$$

where $I_{\text{ov}}(\delta t)$ is the spectral overlap integral of the two single photons at the input ports of the beam splitter, given as

$$I_{\text{ov}}(\delta t) = \int_0^\infty d\omega_1 \int_0^\infty d\omega_2 \psi(\omega_1, \omega_2) \psi^*(\omega_2, \omega_1) \exp[-i(\omega_1 - \omega_2)\delta t]. \quad (2.42)$$

Usually, in experimental measurements of quantum interference, the time delay is varied to retrieve the Hong-Ou-Mandel dip in the coincidence rates.

The probabilities of different outcomes of the quantum interference between two single photons can be calculated for the general two-port beam splitter:

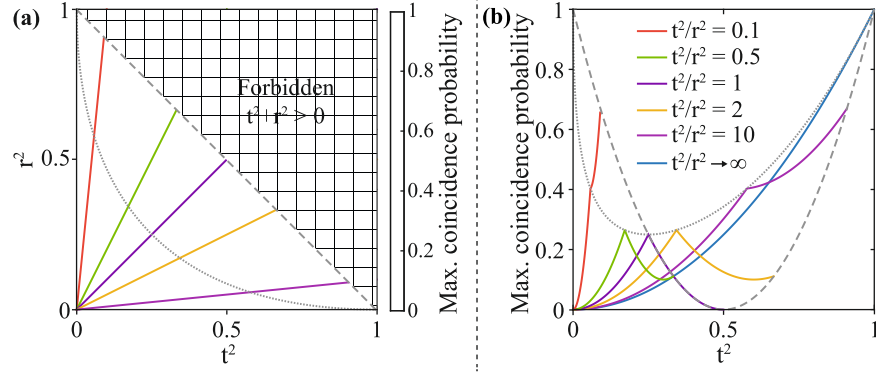


Figure 2.5 (a) The variation of the maximal coincidence rate $\max_{\alpha} P(1_1, 1_2)$ in a general beam splitter is shown as a function of reflectance and transmittance. The solid curves in (a) and (b) correspond to cross-sections along different imbalance values t^2/r^2 . The dashed curve in (a) and (b) is the coincidence probability in a lossless beam splitter. The dotted curve in (a) and (b) depicts the coincidence probability of beam splitters with $t + r = 1$.

$$P(1_1, 1_2) = t^2 \tau^2 + r^2 \rho^2 + 2\tau \rho t r I_{\text{ov}} \cos \alpha, \quad (2.43)$$

$$P(2_1, 0_2) = t^2 \rho^2 [1 + I_{\text{ov}}(\delta t)], \quad (2.44)$$

$$P(0_1, 2_2) = \tau^2 r^2 [1 + I_{\text{ov}}(\delta t)], \quad (2.45)$$

$$P(1_1, 0_2) = t^2 + \rho^2 - t^2 \tau^2 - r^2 \rho^2 - 2\{t^2 \rho^2 + I_{\text{ov}}(\delta t)[t^2 \rho^2 + \tau \rho t r \cos \alpha]\}, \quad (2.46)$$

$$P(0_1, 1_2) = \tau^2 + r^2 - t^2 \tau^2 - r^2 \rho^2 - 2\{\tau^2 r^2 + I_{\text{ov}}(\delta t)[\tau^2 r^2 + \tau \rho t r \cos \alpha]\}, \quad (2.47)$$

$$P(0_1, 0_2) = 1 - t^2 - \rho^2 - \tau^2 - r^2 + t^2 \tau^2 + r^2 \rho^2 + t^2 \rho^2 + \tau^2 r^2, \\ + I_{\text{ov}}(\delta t)[t^2 \rho^2 + \tau^2 r^2 + 2\tau \rho t r \cos \alpha]. \quad (2.48)$$

For the case of a symmetric beam splitter as discussed in Fig. 2.4, the probabilities of different outcomes reduce to

$$P(1_1, 1_2) = t^4 + r^4 + 2t^2 r^2 I_{\text{ov}}(\delta t) \cos \alpha, \quad (2.49)$$

$$P(2_1, 0_2) = P(0_1, 2_2) = t^2 r^2 [1 + I_{\text{ov}}(\delta t)], \quad (2.50)$$

$$P(1_1, 0_2) = P(0_1, 1_2) = t^2 + r^2 - t^4 - r^4 - 2t^2 r^2 \{1 + I_{\text{ov}}(\delta t)[1 + \cos \alpha]\}, \quad (2.51)$$

$$P(0_1, 0_2) = 1 - 2(t^2 + r^2) + t^4 + r^4 + 2t^2 r^2 \{1 + I_{\text{ov}}(\delta t)[1 + \cos \alpha]\}. \quad (2.52)$$

It can be seen from Eq. (2.49) that the coincidence probability $P(1_1, 1_2)$ varies sinusoidally with α . For a lossless and balanced beam splitter $\alpha = \pi$, which yields a coincidence probability of zero, corresponding to the well-known Hong-Ou-Mandel bunching of photons. However in a lossy beam splitter, the coincidence

probability between perfectly indistinguishable photons varies with α from $(t^2 - r^2)^2$ to $(t^2 + r^2)^2$, assuming $\Delta\alpha = 2\pi$. Furthermore, it is interesting to note that the probability of photon bunching at the first output port, $P(2_1, 0_2)$ or the second output port, $P(0_1, 2_2)$ is independent of α .

Fig. 2.5(a) depicts the maximal coincidence rate under a variation of α , $\max_\alpha P(1_1, 1_2)$, which is obtained at $\alpha = \pi - \frac{\Delta\alpha}{2}$, $\delta t = 0$ as a function of transmittance t^2 and reflectance r^2 . The cross-sections along the solid lines in Fig. 2.5(a) are shown in Fig. 2.5(b) in corresponding colours. The cross-sections correspond to different imbalance ratios t^2/r^2 . A common feature among all the curves is a point of inflexion along the dotted curve and termination on the dashed curve. In the limiting cases of $t^2/r^2 \rightarrow \infty$ or $t^2/r^2 \rightarrow 0$, the two points coincide. The dashed curve corresponds to the coincidence probability in a lossless beam splitter, which varies as $(1 - 2t^2)^2$. The dotted line corresponds to the coincidence rate at the largest value of t^2 that allows full programmability, i.e., $\Delta\alpha = 2\pi$.

2.2.4 Hong-Ou-Mandel-like interference

In an experiment, the quantum interference can be measured by performing a Hong-Ou-Mandel-like experiment, where the distinguishability of the photons is varied via a time delay, δt , between them. Let us suppose that the two photons are generated using collinear type-II spontaneous parametric down conversion in a periodically poled potassium titanyl phosphate (PPKTP) crystal, and let us suppose that pulsed pumping is used, where the centre frequency and Fourier-transformed pulse width of the pump are ω_p and τ_p respectively. The resulting bi-photon amplitude of the idler (ω_i) and signal (ω_s) photons is [74]

$$\psi(\omega_i, \omega_s) = \text{sinc} \left(\left(k_p - k_i - k_s - \frac{2\pi}{\Lambda} \right) \frac{L}{2} \right) \exp \left\{ - \left[(\omega_s + \omega_i - \omega_p) \frac{\tau_p}{2} \right]^2 \right\}, \quad (2.53)$$

where $\text{sinc } x = \frac{\sin x}{x}$, and Λ and L are the poling period and length of crystal, respectively. From the above bi-photon amplitude, the overlap integral $I_{ov}(\delta t)$ can be calculated, which gives the coincidence probability $P(1_1, 1_2)$. Fig. 2.6 elucidates the expected Hong-Ou-Mandel-like curve at various values of α for a symmetric balanced beam splitter with $t = r = \rho = \tau = 1/2$. The delay time is normalized to the coherence time $\Delta\tau_c$ of the single photons generated by the source. For $\alpha = \pi$, a Hong-Ou-Mandel like dip is evident which slowly evolves into a peak as α approaches 0 or 2π , indicating increased antibunching of photons. The sinusoidal variation of the coincidence probability $P(1_1, 1_2)$ with phase α for perfectly indistinguishable photons, i.e., $\delta t = 0$, indicates the programmability of quantum interference at these beam splitters.

2.2.5 Discussion and conclusions

Through the above theoretical analysis of a general two-port circuit, we have demonstrated that losses introduced in a beam splitter allow the tunability of

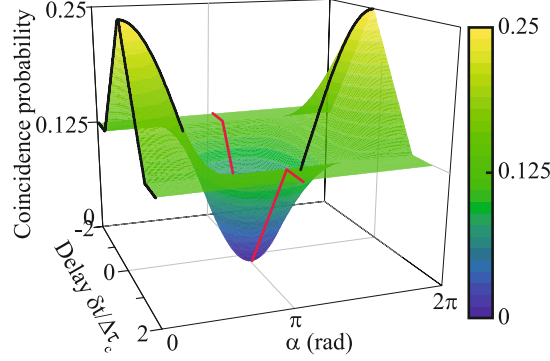


Figure 2.6 Coincidence probability $P(1_1, 1_2)$ as a function of delay time (δt) at various values of α in a lossy symmetric balanced beamsplitter with $t = \tau = r = \rho = 0.5$. The coincidence probability $P(1_1, 1_2)$ varies like a cosine with α for perfectly indistinguishable photons $\delta t = 0$. The conventional Hong-Ou-Mandel dip (red curve) is seen at $\alpha = \pi$ which becomes a peak at $\alpha = 0$ or 2π . The triangular shape of the Hong-Ou-Mandel dip or peak is a consequence of the photon pair generation process.

α and hence of the quantum interference. We quantify the programmability of quantum interference by defining the parameter $\Delta P(1_1, 1_2)$ which is the programmable range of coincidence probability, defined as

$$\Delta P(1_1, 1_2) \equiv \frac{\max_{\alpha} P(1_1, 1_2) - \min_{\alpha} P(1_1, 1_2)}{P(1_1, 1_2; \text{distinguishable})}, \quad (2.54)$$

where the numerator is the difference between maximum and minimum coincidence probabilities (see Fig. 2.6) with indistinguishable photons ($\delta t = 0$), and the denominator is the coincidence rate with distinguishable photons ($\delta t \rightarrow \pm\infty$). Fig. 2.7 depicts $\Delta P(1_1, 1_2)$ as a function of transmittance and reflectance with few representative contours shown. The lossless beam splitters, which lie on the diagonal separating the allowed and the forbidden regions, show no programmability. Maximal programmability of $\Delta P(1_1, 1_2) = 2$, is allowed by lossy balanced beam splitters for perfectly indistinguishable photons. The black dashed line in the figure corresponds to $t + r = 1$. While $\Delta\alpha = 2\pi$ in the region $t + r < 1$, the programmability is not uniform. This arises from the imbalance $t^2/r^2 \neq 1$ in unbalanced beam splitters.

Our theoretical calculations explain the recent experimental demonstrations of programmable quantum interference in opaque scattering media and multi-mode fibres [57, 60]. In these experiments, two-port circuits were constructed using wavefront shaping that selects two modes from an underlying large number of modes [28, 29]. Light that is not directed into the two selected modes

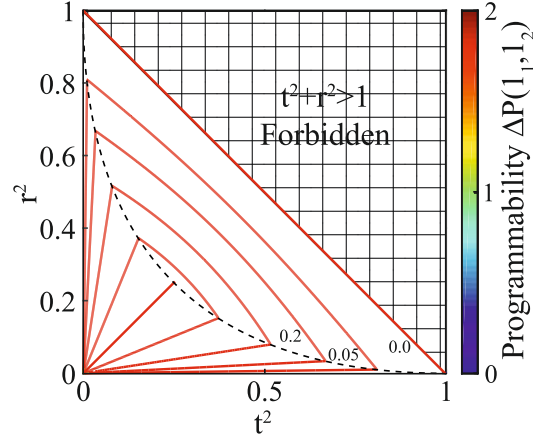


Figure 2.7 Programmability of the coincidence rate $\Delta P(1, 1_2)$ is depicted here together with few representative contours at values indicated beside them. The black dashed curve represents $t + r = 1$. The lossless beam splitters have $\Delta P(1, 1_2) = 0$, while the balanced lossy beam splitters satisfying $t + r < 1$ have maximal programmability with $\Delta P(1, 1_2) = 2$.

due to imperfect control or noise can be modeled as loss. A typical transmission of $\sim 10\%$ in opaque scattering media ensures the full programmability when a balanced two-port circuit is constructed [36, 37].

In summary, we have theoretically analyzed the most general passive linear two-port circuit from only energy considerations. We establish the programmability of quantum interference between two single photons in the context of recent experimental demonstrations in massively multichannel linear optical networks. These networks with the envisaged programmability of quantum interference has the potential for large-scale implementation of quantum simulators and programmable quantum logic gates. In this context, the current theoretical analysis establishes that imperfections or dissipation in optical networks, which are unavoidable in experiments, are not necessarily detrimental. In fact, the losses introduce a novel dimensionality to the networks, in that the quantum interference is programmable. The theoretical framework presented here can be extended to model larger programmable multiport devices [4, 5], which are required in a variety of useful quantum information processing and simulation protocols [8, 9].

2.3 Arbitrarily programmable networks

In the previous section, losses were introduced into a 2×2 network to achieve a programmable functionality of the network. In experiments, losses can be caused by dissipation, but also by leakage to unmonitored ports. The latter provides a way to realize these lossy networks, by implementing the losses as output in unmonitored ports. In that case the lossy network is a subnetwork of a larger unitary network, such that the total system still obeys conservation of energy [75, 76]. For example, the following lossy (non-unitary) 2×2 network,

$$\begin{bmatrix} E_{b_1} \\ E_{b_2} \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & e^{i\alpha} \end{bmatrix} \begin{bmatrix} E_{a_1} \\ E_{a_2} \end{bmatrix}, \quad (2.55)$$

which was discussed in section 2.1, can be implemented inside a larger 4×4 unitary matrix, as for instance:

$$\begin{bmatrix} E_{b_1} \\ E_{b_2} \\ E_{b_3} \\ E_{b_4} \end{bmatrix} = \frac{1}{2} \begin{bmatrix} \boxed{\begin{smallmatrix} 1 & 1 \\ 1 & e^{i\alpha} \end{smallmatrix}} & \begin{smallmatrix} 1 & -1 \\ -1 & e^{i\alpha} \end{smallmatrix} \\ \begin{smallmatrix} 1 & -1 \\ -1 & e^{i\alpha} \end{smallmatrix} & \boxed{\begin{smallmatrix} 1 & 1 \\ 1 & e^{i\alpha} \end{smallmatrix}} \end{bmatrix} \begin{bmatrix} E_{a_1} \\ E_{a_2} \\ E_{a_3} \\ E_{a_4} \end{bmatrix}. \quad (2.56)$$

The matrix corresponds to a lossless linear optical network with four inputs and four outputs. The lossy 2×2 network of interest occupies the top-left block of the matrix, indicated by the dashed square. One has effectively created the lossy 2×2 network of Eq. (2.55) between inputs a_1, a_2 and outputs b_1, b_2 .

The minimum dimensionality of a unitary matrix to include a lossy submatrix of dimension N is expected to be $2N$. This expectation is based on the heuristic argument that, to create a unitary system, for each of the N channels an extra channel is needed to act as a loss channel. These loss channels can be physical channels, associated with extra accessible outputs, or in the framework of the Langevin noise operators (section 2.2) extra connections to the reservoir. At this moment a proof for this $2N$ scaling of the minimum required size of a unitary matrix is outstanding. The case for $N = 1$ is intuitive: to convert light in a single mode to an arbitrary intensity and phase, one needs to add one variable beam splitter (with its extra input and output) and phase shifter, extending the dimensionality of the system to 2. The total 2×2 system is unitary, while the 1×1 subsystem of interest does not need to be.

Already for $N = 2$ the solution is less intuitive. We found that no 3×3 unitary matrix can encompass the lossy 2×2 submatrix of Eq. (2.55) for arbitrary α . The minimum size of a unitary matrix that includes this 2×2 lossy network is 4×4 , corresponding to $2N$. For the most general lossy 2×2 network of section 2.2:

$$\begin{bmatrix} te^{i\phi_{11}} & \rho e^{i\phi_{12}} \\ re^{i\phi_{21}} & \tau e^{i\phi_{22}} \end{bmatrix}, \quad (2.57)$$

indeed a 4×4 unitary matrix suffices. A procedure to construct an explicit form of this larger unitary from Eq. (2.57) follows. We will start with a specific

parametrization of this unitary, whose parameters can directly be interpreted as beam splitters and phase shifters in a linear optical network. Any unitary matrix U_M of dimension M can be parametrized as [77]:

$$U_M = D(\sigma_{1,1}, \dots, \sigma_{M,M}) \prod_{m=1}^{M-1} \left(\prod_{n=M-m+1}^M V_{M-m,n}(w_{M-m,n}, \sigma_{M-m,n}) \right), \quad (2.58)$$

in which D is a M -dimensional diagonal matrix whose diagonal elements are $\exp i\sigma_{1,1}$ to $\exp i\sigma_{M,M}$:

$$D_{ij} = e^{i\sigma_{i,i}} \delta_{ij}, \quad (2.59)$$

and $V_{p,q}(w_{p,q}, \sigma_{p,q})$ is a M -dimensional matrix with elements

$$(V_{p,q})_{ij} = \delta_{ij} + (\cos w_{p,q} - 1)(\delta_{ip}\delta_{jq} + \delta_{iq}\delta_{jp}) - \sin w_{p,q} e^{-i\sigma_{p,q}} \delta_{ip}\delta_{jq} + \sin w_{p,q} e^{i\sigma_{p,q}} \delta_{iq}\delta_{jp}. \quad (2.60)$$

Since any unitary can be constructed in linear optics [47], one can directly translate D and $V_{p,q}$ to optical elements. D corresponds to a phase shifter in every output of the optical network, and each $V_{p,q}$ can be viewed as a combination of a beam splitter with splitting ratio $\tan w_{p,q}$, and a phase shifter with phase $\sigma_{p,q}$. The correspondence to optical elements becomes more apparent by looking at for example the explicit form of $V_{1,2}$:

$$V_{1,2} = \begin{bmatrix} \cos w_{1,2} & -\sin w_{1,2} e^{-i\sigma_{1,2}} & 0 & \dots & 0 \\ \sin w_{1,2} e^{i\sigma_{1,2}} & \cos w_{1,2} & 0 & \dots & 0 \\ 0 & 0 & 1 & & \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & & & 1 \end{bmatrix}, \quad (2.61)$$

which represents a beam splitter between ports 1 and 2, with splitting ratio $\tan w_{1,2}$ and phase shift $\sigma_{1,2}$. In total there are M^2 independently tunable parameters: $\frac{1}{2}M(M-1)$ beam splitters $w_{p,q}$ and $\frac{1}{2}M(M+1)$ phase shifters $\sigma_{p,q}$. One now needs to find a parametrization of a unitary matrix U_4

$$U_4 = D(\sigma_{1,1}, \sigma_{2,2}, \sigma_{3,3}, \sigma_{4,4}) V_{3,4}(w_{3,4}, \sigma_{3,4}) V_{2,3}(w_{2,3}, \sigma_{2,3}) V_{2,4}(w_{2,4}, \sigma_{2,4}) \\ \times V_{1,2}(w_{1,2}, \sigma_{1,2}) V_{1,3}(w_{1,3}, \sigma_{1,3}) V_{1,4}(w_{1,4}, \sigma_{1,4}), \quad (2.62)$$

whose top-left four elements (or any other block) equal the 2×2 matrix of Eq. (2.57):

$$U_4 = \begin{bmatrix} te^{i\phi_{11}} & \rho e^{i\phi_{12}} & (U_4)_{13} & (U_4)_{14} \\ re^{i\phi_{21}} & \tau e^{i\phi_{22}} & (U_4)_{23} & (U_4)_{24} \\ (U_4)_{31} & (U_4)_{32} & (U_4)_{33} & (U_4)_{34} \\ (U_4)_{41} & (U_4)_{42} & (U_4)_{43} & (U_4)_{44} \end{bmatrix}. \quad (2.63)$$

We find a possible parametrization for $t, \tau, r, \rho \leq 1/2$, the case in which the lossy 2×2 network is fully programmable, by choosing the parameters:

$$\begin{aligned}
\sigma_{23} &= 0, \\
\sigma_{24} &= 0, \\
\sigma_{11} &= \phi_{11}, \\
\sigma_{22} &= \phi_{22}, \\
\sigma_{12} &= \phi_{11} - \phi_{12} + \pi, \\
\sigma_{13} &= \sigma_{23} + \phi_{21} - \phi_{22} + \pi, \\
\sigma_{14} &= \sigma_{24} + \phi_{11} - \phi_{12} + \pi, \\
w_{12} &= \arcsin \rho, \\
w_{14} &= \arccos \sqrt{c_5}, \\
w_{23} &= \arccos \sqrt{1 - \frac{c_3}{c_5 - c_2}}, \\
w_{13} &= \arccos \sqrt{\frac{c_2}{c_5}}, \\
w_{24} &= \arccos \sqrt{\frac{c_4}{1 - \frac{c_3}{c_5 - c_2}}}, \tag{2.64}
\end{aligned}$$

with constants c_1 – c_5 defined as:

$$\begin{aligned}
c_1 &\equiv \frac{\rho t \tau}{1 - \rho^2}, \\
c_2 &\equiv \frac{t^2}{1 - \rho^2}, \\
c_3 &\equiv r^2, \\
c_4 &\equiv \frac{\tau^2}{1 - \rho^2}, \\
c_5 &\equiv \frac{1}{2(c_4 - 1)} \left(c_1^2 - c_3 + (c_2 + 1)(c_4 - 1) \right. \\
&\quad \left. + \sqrt{(c_1^2 - c_3 - (c_2 - 1)(c_4 - 1))^2 - 4c_3(c_2 - 1)(c_4 - 1)} \right). \tag{2.65}
\end{aligned}$$

The remaining four parameters $\sigma_{33}, \sigma_{34}, \sigma_{44}, w_{34}$ are still completely free. Note that this specific 4×4 matrix is not a unique solution, even without considering the four free parameters. Since every unitary matrix can be realized as a linear optical network [47], it is now possible to construct a 4×4 network with up to six variable beam splitters and ten phase shifters, which between two inputs and two outputs behaves as a general lossy 2×2 network. By tuning the elements in the network according to Eq. (2.64) any lossy 2×2 network can be constructed. A general procedure for the construction of a lossy $N \times N$ network is still an

open question. Recently, programmable networks containing several tens of tunable elements have been demonstrated in integrated optics [4, 5], with the purpose to create arbitrary unitaries, not for creating general lossy networks. To construct a general lossy $N \times N$ network, one would need to actively control up to $(2N)^2$ elements, usually heaters. Therefore, scaling this approach to massively multichannel networks can be challenging.

2.4 Programmability by control of many input states

Our approach for constructing programmable networks is radically different, and avoids the need for actively tunable elements inside an integrated optical network. To realize a programmable network that performs operation $\hat{S}$, one would normally tune the optical network itself, i.e., $\hat{S}$ is programmable.

$$|\Psi_{\text{out}}\rangle = \hat{S} |\Psi_{\text{in}}\rangle. \quad (2.66)$$

Instead, we exploit a fixed high-dimensional optical network and achieve a programmable functionality by preparing the photons in a spatially entangled state over all input channels of the fixed network. As basis a fixed high-dimensional optical network $\hat{S}_{\text{fix}}$ is used. Experimentally this is implemented as an opaque scattering medium, containing millions of channels. To achieve the desired operation, the input state is projected on the eigenvectors of the fixed network using an operator $\hat{P}$:

$$|\Psi_{\text{out}}\rangle = \hat{S} |\Psi_{\text{in}}\rangle = \hat{S}_{\text{fix}} \hat{P} |\Psi_{\text{in}}\rangle. \quad (2.67)$$

For a complete control of the functionality one should have $\hat{P} = \hat{S}_{\text{fix}}^\dagger \hat{S}$. In our approach, the projection is done by adaptive spatial phase-modulation of the wavefront of the incident photons by a spatial light modulator (SLM). The photons are prepared in such an entangled state over all input channels, that they can be directed at targeted output channels with programmable amplitude and phase. In this way, the network formed by the combination of an SLM and a scattering medium contains the desired functionality. The number of control parameters on the SLM can be easily made to exceed millions, giving a large degree of control of the propagation of the photons through the opaque scattering medium. Hence, the functionality of the optical network is programmable. Full knowledge of the scattering matrix of the fixed network is not required, as one can employ adaptive wavefront shaping to find the needed projection for a desired functionality [28, 29]. Our method for constructing linear optical networks is described in detail in chapter 4, and used to achieve programmable quantum interference in chapter 5.

3 The single-photon source

To demonstrate quantum interference in massively multichannel networks, we require a source of multiple indistinguishable single-photon states. Since the networks of interest can easily contain thousands of channels over which the photons are distributed, a high-brightness source is desired. In future experiments it is planned to explore the interference of multiple photons inside the networks, both in the form of multiple single-photon states as well as multiphoton Fock states. To accommodate these demands, we have constructed a quantum light source based on spontaneous parametric down-conversion, the current workhorse for quantum interference experiments [78]. A spontaneous parametric down-conversion source probabilistically generates pairs of single photons. Detection of one photon out of such a photon pair heralds the presence of the second photon. This kind of source can be used for the generation of pairs of indistinguishable photons, pairs of entangled photons, and multiphoton Fock states when sufficient pump power is available. Because of these properties, a bright quantum light source based on spontaneous parametric down-conversion is very suitable for the experiments in this thesis.

3.1 Spontaneous parametric down-conversion

The quantum states used for the experiments in this thesis are generated using spontaneous parametric down-conversion (SPDC) [79, 80]. This is a spontaneous parametric nonlinear optical process where in the simplest case one pump photon is annihilated to create a pair of photons, having different properties than the pump photon: one signal and one idler photon. While the signal and idler fields individually exhibit thermal statistics [81], coincident detection of both signal and idler photons approximates a single-photon Fock state in each arm. A SPDC source acts as a heralded source of single photons. The interaction Hamiltonian for a collinear Type-II SPDC process [82], treating the pump light as a classical field, is given by

$$\hat{H}_I = i\hbar\eta\hat{a}_s^\dagger\hat{a}_i^\dagger + \text{h.c.}, \quad (3.1)$$

where $\eta \propto \chi^{(2)}E_p$, with $\hat{a}_s^\dagger$, $\hat{a}_i^\dagger$ the creation operators for the signal and idler fields, $\chi^{(2)}$ the second-order nonlinear susceptibility of the medium, and E_p the amplitude of the pump field. Initially, the signal and idler fields are considered to be in the vacuum state $|\Psi(0)\rangle = |0_s, 0_i\rangle$. Using the interaction Hamiltonian, one can calculate the time evolution of this initial state [84]:

$$|\Psi(t)\rangle = \text{sech } \mu \sum_{n=0}^{\infty} \tanh^n \mu |n_s, n_i\rangle, \quad (3.2)$$

where $\mu = \eta t$. For $\mu \ll 1$ this can be approximated, using $\tanh \mu \approx \mu$, as

$$\begin{aligned} |\Psi\rangle &\approx \sqrt{1 - \mu^2} \sum_{n=0}^{\infty} \mu^n |n_s, n_i\rangle \\ &= \sqrt{1 - \mu^2} \left(|0_s, 0_i\rangle + \mu |1_s, 1_i\rangle + \mu^2 |2_s, 2_i\rangle + \dots \right). \end{aligned} \quad (3.3)$$

Upon coincident detection of both signal and idler photons the quantum state approximates a single-photon Fock state $|1_s, 1_i\rangle$ in each arm for small μ . By considering four-fold coincidences between two signal and two idler photons one can access the $|2_s, 2_i\rangle$ state. This selection of quantum states using coincident detection can be extended to higher photon numbers.

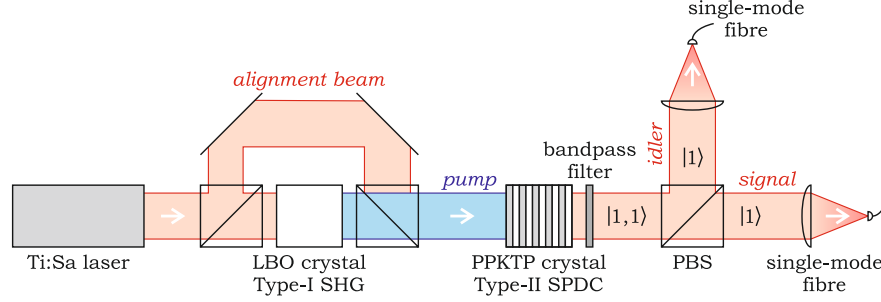


Figure 3.1 The quantum light source. Light from a mode-locked Ti:Sapphire laser is frequency doubled in an LBO crystal. The resulting light is used to pump a PPKTP crystal for spontaneous parametric down-conversion. The generated orthogonally-polarized signal and idler photons are separated by a polarizing beam splitter and coupled into single-mode fibres. The photons can be frequency-filtered by inserting a bandpass filter. The temporal delay between the two photons is controlled with a delay stage in the idler arm (not shown). The alignment beam is used for alignment of the quantum light source and is also coupled into the single-mode fibres to facilitate alignment of subsequent parts of the setup. This alignment beam is blocked while measuring with down-converted photons. A detailed drawing of the setup is in appendix A.

3.2 Experimental setup

Our quantum light source is illustrated in Fig. 3.1 and is based on previous work [43, 85, 86]. Light from a Kerr-lens mode-locked Ti:Sapphire oscillator, which emits transform-limited sech^2 -pulses with a pulse duration of 1.83 ± 0.04 ps

(FWHM) at a repetition rate of 76.0 MHz and a spectral width of 0.35 ± 0.05 nm (FWHM) centered around a wavelength of 790.0 nm, is frequency doubled to 395.0 nm in a 17 mm long lithium triborate (LBO) crystal cut for Type-I second-harmonic generation (SHG). Typically 900 mW of frequency-doubled pump light with a spectral width of 0.15 ± 0.05 nm is generated. The use of a frequency-doubled mode-locked laser, providing high peak power, as a pump source enables us to not only generate single-photon Fock states, but also quantum states with a higher photon number. After spectral and spatial filtering approximately 700 mW of pump light remains, which is focused into a 2 mm long periodically-poled potassium titanyl phosphate (PPKTP) crystal cut for frequency-degenerate collinear Type-II spontaneous parametric down-conversion. The output of this crystal consists of pairs of orthogonally-polarized photons with a spectral width of approximately 3 nm centered around a wavelength of 790.0 nm. Optionally, the photons are frequency-filtered by inserting a bandpass filter with a bandwidth of 1.5 nm. The two polarization modes, signal and idler, are separated using a polarizing beam splitter (PBS) and coupled into single-mode fibres (SMF), see Fig. 3.1. The temporal delay between the two photons is controlled with a delay stage in the idler arm (not shown). A small fraction of the light emitted from the Ti:Sapphire laser is routed around the LBO crystal and used as alignment beam for the quantum light source. This alignment beam is also coupled into the single-mode fibres to facilitate alignment of subsequent parts of the setup. This beam is blocked while measuring with down-converted photons.

3.3 Single-photon spectrum

For two photons to exhibit quantum interference it is of great importance that the two photons are indistinguishable (see section 2.2). The limiting factor for the indistinguishability of the two photons generated by a Type-II spontaneous parametric down-conversion process is the spectral overlap between signal and idler. The spectral distribution of the signal and idler photons is calculated from energy and momentum considerations. Firstly, the spectral distribution of the pump field amplitude, α , for a transform-limited broadband Gaussian pump with pulse duration τ_p is given by Eq. (3.4):

$$\alpha(\omega_s + \omega_i) \propto e^{-\left((\omega_s + \omega_i - \omega_p)\frac{\tau_p}{2}\right)^2}. \quad (3.4)$$

The pump field is already expressed in terms of the signal, idler, and pump frequencies, ω_s , ω_i and ω_p , to ensure energy conservation. Figure 3.2(a) shows the calculated pump field envelope for the frequency-doubled pump light with a spectral width of 0.15 nm centered around a wavelength of 395.0 nm, which yields a pump pulse duration of $\tau_p \approx 1.3$ ps for a transform-limited Gaussian pulse. The graph indicates all possible signal-idler frequency pairs which satisfy conservation of energy starting from the pump light. Covered in the figure is the

wavelength range where signal and idler have near-degenerate frequencies. The pump envelope is symmetric in the exchange of signal and idler frequencies. Secondly, conservation of momentum is given by the phase-matching function of the PPKTP crystal. To increase the efficiency of the SPDC process the crystal is periodically poled for quasi-phase-matching. The phase-matching function, Φ , often also named parametric-gain profile, is given by

$$\Phi(\omega_s, \omega_i) = \text{sinc} \left(\left(k_p(\omega_s + \omega_i) - k_s(\omega_s) - k_i(\omega_i) - \frac{2\pi}{\Lambda} \right) \frac{L}{2} \right), \quad (3.5)$$

where $\text{sinc } x = \frac{\sin x}{x}$. The wave vectors of the pump, signal, and idler fields are denoted by k_p , k_s , and k_i , and are assumed to be collinear. Λ and L are respectively the poling period and length of the PPKTP crystal [87]. The phase-matching function is visualized in Fig. 3.2(b) for a crystal temperature of 54.5 °C. Note that Φ is not symmetric upon exchange of signal and idler due to the birefringence of the crystal [88]. The envelope of the signal-idler fields can be obtained by multiplying the pump field envelope and phase-matching function [74]. The resulting bi-photon field envelope is shown in Fig. 3.2(c). Frequency-degenerate signal and idler photons occur at a centre wavelength of 790.0 nm.

By integrating the bi-photon field envelope over ω_i or ω_s , one obtains the spectrum of the signal or idler photons, respectively:

$$S_s(\omega) = \int_0^\infty |\alpha(\omega + \omega_i) \Phi(\omega, \omega_i)|^2 d\omega_i, \quad (3.6)$$

$$S_i(\omega) = \int_0^\infty |\alpha(\omega_s + \omega) \Phi(\omega_s, \omega)|^2 d\omega_s. \quad (3.7)$$

Figure 3.3 shows these spectra of the signal and idler photons. Shown are single-photon spectra calculated according to Eq. (3.6)-(3.7), as well as measured spectra. The calculated spectral width of the signal and idler photons is respectively 3.14 nm and 2.85 nm, bounded by the phase-matching bandwidth of the crystal. The measured spectra agree well with the predictions. The difference in spectral width of signal and idler is caused by the birefringence of the PPKTP crystal, which also shows up in Fig 3.2(b)-(c) as the asymmetry under exchange of signal and idler frequencies. To increase the relative spectral overlap, and therefore the indistinguishability of signal and idler, the photons can be filtered by a bandpass filter with a bandwidth of 1.5 nm. The resulting signal and idler spectra are also shown in Fig 3.3. Using this filter, the spectral width of the signal and idler is reduced to 1.32 nm and 1.29 nm, respectively. The slight discrepancy between the measurements and the calculations in the tails of the spectra are to be expected, since in the calculations a Gaussian pump envelope has been assumed for simplicity, while in experiments the pump light is derived from a passively mode-locked Ti:Sapphire oscillator, which emits sech^2 -pulses.

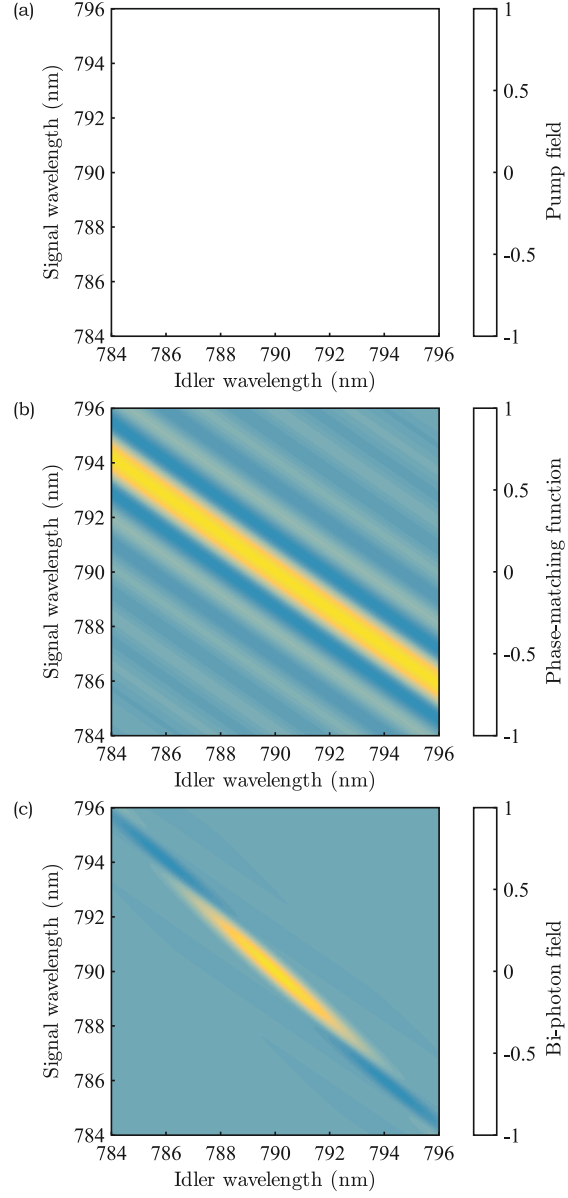


Figure 3.2 Calculation of the spectral distribution of the down-converted photons. a) Spectral envelope of the pump field. b) Phase-matching function of the PPKTP crystal. c) Spectral envelope of the down-converted bi-photon field.

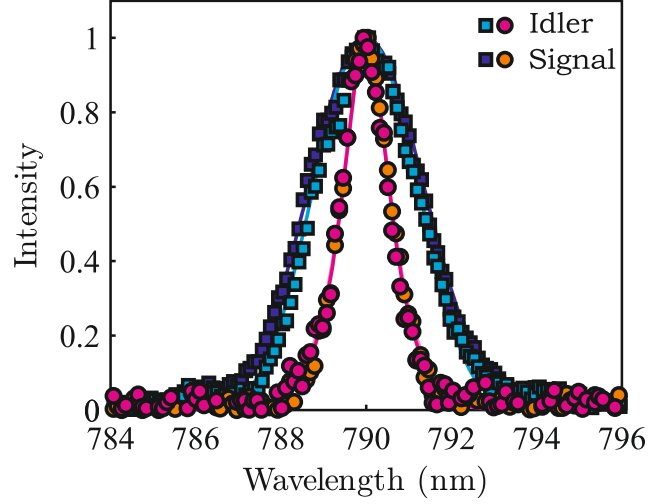


Figure 3.3 Measured spectra of the down-converted signal (blue squares) and idler (cyan squares) photons. The solid curves in the plot correspond to calculated single-photon spectra. The difference in spectral width of signal and idler is caused by the birefringence of the PPKTP crystal. Also shown are the spectra of the signal (orange circles) and idler (magenta circles) after inserting a bandpass filter with a bandwidth of 1.5 nm.

3.4 Hong-Ou-Mandel interference

To measure the degree of indistinguishability of the signal and idler photons, we observe Hong-Ou-Mandel (HOM) interference between signal and idler at a 50:50 beam splitter. The expected coincidence rate between the two outputs of the beam splitter can be calculated from the pump field envelope and phase-matching function [74]:

$$R_c(\delta\tau) \propto \int_0^\infty \int_0^\infty |\alpha(\omega_s + \omega_i)|^2 \left(|\Phi(\omega_s, \omega_i)|^2 - \Phi(\omega_s, \omega_i) \Phi^*(\omega_i, \omega_s) e^{-i(\omega_i - \omega_s)\delta\tau} \right) d\omega_i d\omega_s, \quad (3.8)$$

where $\delta\tau$ is the temporal delay between the signal and idler photons. At large $\delta\tau$ only the $|\Phi(\omega_s, \omega_i)|^2$ term contributes, creating the background level of coincidences. Around zero delay the second term, $\Phi(\omega_s, \omega_i) \Phi^*(\omega_i, \omega_s)$, becomes significant, causing a dip in the coincidence rate. This term relates to the spectral overlap of signal and idler, cf. Eq. (2.42). Note that at $\delta\tau = 0$ both terms do not

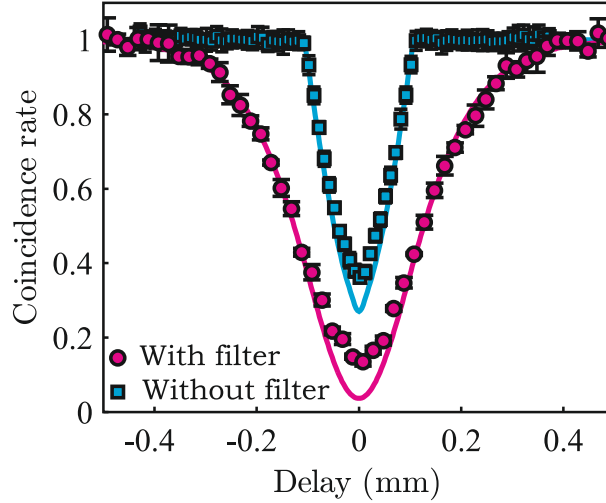


Figure 3.4 Measured Hong-Ou-Mandel interference without bandpass filter (cyan squares) and with bandpass filter (magenta circles) at a pump power of 10 mW. Error bars indicate the standard deviation in the measurements. The solid curves in the plot correspond to the calculated Hong-Ou-Mandel interference. The visibility is limited by the difference in spectral width of the signal and idler photons.

necessarily cancel, since in the second term the arguments of signal and idler in Φ^* are exchanged. Only in case of a phase-matching function that is symmetric under exchange of signal and idler, both terms cancel, resulting in zero coincidences. Since for broadband Type-II SPDC the phase-matching function is not symmetric under exchange of signal and idler, due to the birefringence of the crystal, see Fig. 3.2(b), the coincidence rate in such a Hong-Ou-Mandel experiment will not vanish. One can, however, narrow the spectrum of signal and idler by spectral filtering to increase the relative spectral overlap between both photons, leading to a deeper Hong-Ou-Mandel dip. The measured HOM interference between signal and idler photons is shown in Fig. 3.4. These measurements were performed at a pump power of 10 mW to ensure that only single-photon Fock states contribute to the interference (see also section 3.5). A Hong-Ou-Mandel dip with a visibility of 64% is observed, with the usual definition of the visibility of $V \equiv (R_{\text{indist}} - R_{\text{dist}}) / R_{\text{dist}}$, where R_{dist} and R_{indist} are the coincidence rates of distinguishable and indistinguishable photons, respectively. Also shown is the interference calculated using Eq. (3.8). It can be seen that the visibility is less than unity, which we address to a residual spectral distinguishability

of the two photons induced by the Type-II SPDC process. The lower visibility of the interference in the experiment compared to the calculations is attributed to imperfect mode-matching in the experiment. The fact that the visibility exceeds the classical bound of 50% shows that the source produces quantum states of light [56]. The measured width of the Hong-Ou-Mandel dip, which is related to the spectral width of the photons as shown in Fig. 3.3, matches the calculated width. To improve the spectral indistinguishability of signal and idler, a band-pass filter with a bandwidth of 1.5 nm was used that resulted in a HOM dip with an increased visibility of 86%. The decrease in the spectral width also increases the width of the HOM dip as is evident in the figure.

3.5 Multiphoton states

As briefly alluded to, spontaneous parametric down-conversion is not limited to generating pairs of single-photon Fock states $|1_s, 1_i\rangle$. One can see from the state in Eq. (3.2) that a much wider variety of quantum states is produced. Of interest are for example pairs of two-photon Fock states $|2_s, 2_i\rangle$, containing a total of four photons. The rate R_n for generating $|n_s, n_i\rangle$ pairs, with n photons in each of the signal and idler modes, scales as

$$R_n \propto |\langle n_s, n_i | \Psi \rangle|^2 = \text{sech}^2 \mu \tanh^{2n} \mu. \quad (3.9)$$

For $\mu \ll 1$ this can be approximated by

$$R_n \propto \mu^{2n} \propto E_p^{2n} \propto P_p^n, \quad (3.10)$$

where P_p is the power of the pump field. This power law shows that, for low pump powers, the $|1_s, 1_i\rangle$ generation rate is proportional to the pump power, the $|2_s, 2_i\rangle$ rate depends quadratically on the pump power, and so on.

To confirm this, and get a measure of the purity of the generated single-photon pairs, we have measured the $|1_s, 1_i\rangle$ and $|2_s, 2_i\rangle$ rates of the SPDC source. Figure 3.5 shows the measured $|1_s, 1_i\rangle$ rate as a function of pump power. The measured rates have been converted to generation rates by taking into account the measured collection and detection efficiencies. As is evident from the figure, the $|1_s, 1_i\rangle$ rate is proportional to the pump power, and can be varied from 10^2 s^{-1} to 10^8 s^{-1} by tuning the pump from 10^{-3} mW to 10^3 mW . Also shown is a linear fit to the data at low pump powers, in the spirit of Eq. (3.10). Furthermore, the measured $|2_s, 2_i\rangle$ rate is shown in the figure. This rate, exceeding 10^6 s^{-1} , was measured by recording the coincidences between the two outputs of a beam splitter placed into the idler arm. Here a quadratic fit to the data at low pump powers is shown, which agrees well with the experimental data. Using the fits to the single-photon and two-photon rates it is possible to calculate the expected generation rates of multiphoton states of higher order using Eq. (3.9). The predicted generation rates of multiphoton Fock states up to 6th order are shown in

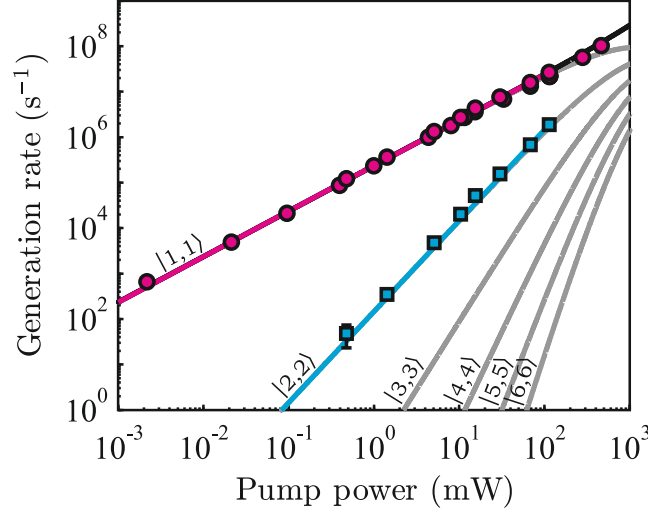


Figure 3.5 Generation rate of multiphoton states as a function of pump power. Shown are the measured generation rates of the single-photon $|1_s, 1_i\rangle$ (magenta circles) and two-photon $|2_s, 2_i\rangle$ (cyan squares) states. Error bars indicate the standard deviation in the measurements. Linear fits to these data at low pump powers (solid coloured lines) are used to predict the generation rates of multiphoton states of higher order (grey curves). The black curve represents the total number of generated photons.

the figure, as well as the total number of generated photons. We expect that the generation rates of the $|3_s, 3_i\rangle$ and $|4_s, 4_i\rangle$ states with our source, containing a total number of 6 and 8 photons, respectively, are sufficiently high to be readily accessible for use in experiments. Possibly, with the usage of high-efficiency detectors, even higher photon-number states become accessible, although the purity of the $|n_s, n_i\rangle$ Fock state, related to the ratio R_{n+1}/R_n , will be limited due to the high pump power required. At low pump powers the source operates as a source of single photons, by triggering on the two-fold coincidences between signal and idler. This does not exclude the possibility of triggering on multiphoton states. However, as seen in Fig. 3.5, at a pump power of 10 mW the difference in generation rates of the $|1_s, 1_i\rangle$ and $|2_s, 2_i\rangle$ states is already two orders of magnitude. For most of our experiments this difference is sufficient to only consider single-photon states, since triggering on multiphoton states is unlikely. By decreasing the pump power further the source generates single-photon states of higher purity, however the generation rate also decreases.

For experiments that require a high single-photon generation rate the SPDC

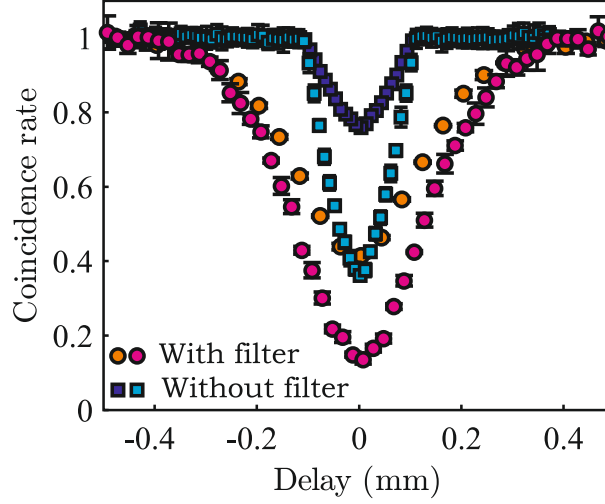


Figure 3.6 Influence of the pump power on the quantum state of the down-converted photons. Measured Hong-Ou-Mandel interference without bandpass filter (cyan squares) and with bandpass filter (magenta circles) at a pump power of 10 mW. Error bars indicate the standard deviation in the measurements. Also shown in the plot are Hong-Ou-Mandel dips at a pump power of 100 mW without bandpass filter (blue squares), and at a pump power of 40 mW with the filter in place (orange circles). The Hong-Ou-Mandel visibility decreases with increasing pump power due to the larger presence of multiphoton states.

source is often operated at a pump power of approximately 100 mW. At this pump power the photon generation rate is $17 \times 10^6 \text{ s}^{-1}$, of which routinely more than $4 \times 10^6 \text{ s}^{-1}$ single counts in each arm and approximately $0.76 \times 10^6 \text{ s}^{-1}$ coincidences between signal and idler are detected. Since in this case the source is pumped with a high power, the generation of pairs of two-photon states cannot anymore be neglected. At a pump power of 100 mW these two-photon states account for approximately 7% of the detector counts. While this fraction is seemingly small, it has a significant effect on the visibility of quantum interference, as is discussed next.

Figure 3.6 shows the influence of the pump power of the SPDC source on the Hong-Ou-Mandel interference of the down-converted photons. Shown is the measured HOM dip at a pump power of 10 mW, with a visibility of 64%. This graph is identical to Fig. 3.4. It can be seen that by increasing the pump power the visibility of the HOM interference decreases. At a pump power of 100 mW the visibility has decreased to 24%. The reduction in HOM visibility

at higher pump powers can be explained by the increased presence of higher photon-number states in a single pulse, which contribute to a higher number of coincidences [53–55] (see also section 2.1). At 100 mW pump power the visibility is now limited due to the presence of multiphoton states, whereas the visibility at 10 mW was limited by the difference in spectral width of signal and idler photons. Similar measurements have been performed with the bandpass filter in place at a pump power of 10 mW, with a visibility of 86%, and at a pump power of 40 mW, resulting in a visibility of 59%.

3.6 Non-degenerate single-photon pairs

The spectrum of the generated signal and idler photons depends on the phase-matching function of the crystal, which, via the wave vectors, depends on the index of refraction. Since the refractive index of the crystal is temperature dependent one can modify the phase-matching function by tuning the crystal temperature. For the generation of frequency-degenerate signal and idler photons at wavelength of 790.0 nm, phase matching is achieved at a temperature of 54.5 °C (see the spectra in Fig. 3.3). When signal and idler are degenerate in frequency they are maximally indistinguishable. To confirm this, we performed Hong-Ou-Mandel experiments with signal and idler photons that were not completely degenerate in frequency. By tuning the crystal temperature to 40.0 °C the phase-matching function was modified to separate the signal and idler photons by approximately 6 nm in wavelength. The measured spectra of signal and idler are shown in Fig. 3.7(a). The calculated spectra, according to Eq. (3.6)-(3.7), are also shown. The centre wavelength of signal and idler changed to 793 nm and 787 nm, respectively. Although signal and idler are not degenerate at the centre wavelength, it is still possible to observe quantum interference between them. This can be seen as a residual Hong-Ou-Mandel interference of these photons in Fig. 3.7(b). The measured HOM interference follows the prediction. Compared to the Hong-Ou-Mandel dip for frequency-degenerate photons (Fig. 3.4), firstly the visibility of the interference is lower. Secondly, the coincidence rate does not show a single dip, but it oscillates instead, peaking above the background coincidence rate and showing another minimum at zero delay. These peaks in the coincident rates indicate partial anti-bunching of the photons at the beam splitter. The total width of the dip is equal to the width for frequency-degenerate photons, since it is related to the spectral width of the down-converted photons, which did not change. A collection of Hong-Ou-Mandel curves measured for different temperatures of the PPKTP crystal is presented in Fig. 3.8. This non-trivial oscillating shape of the HOM interference has been observed before [89], even with photons that have been detuned in centre wavelength so far that no spectral overlap between them remains. Its origin is attributed to frequency entanglement of the signal and idler photons resulting from the spectral asymmetry in the down-converted bi-photon field introduced by the detuning [89].

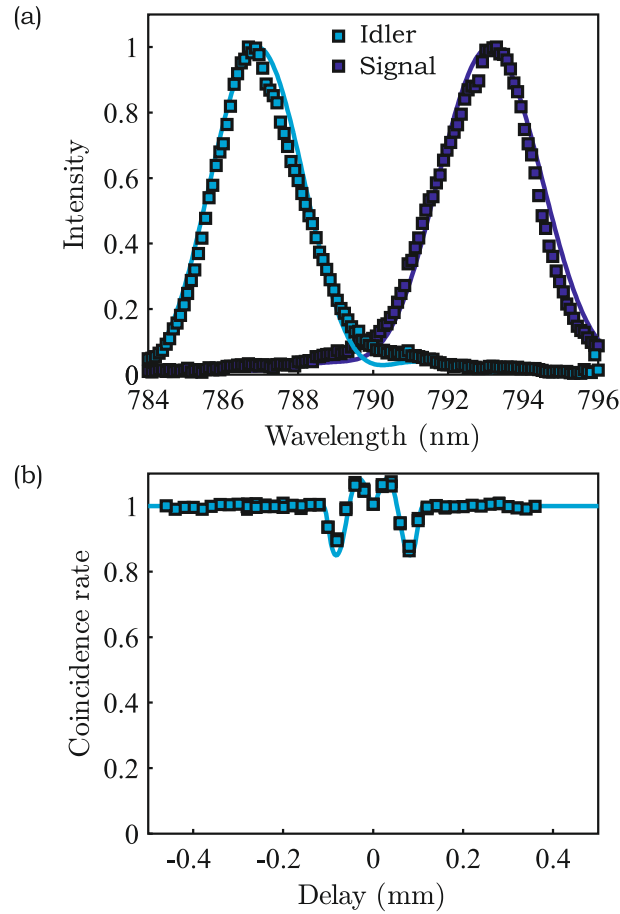


Figure 3.7 Comparison of measured and calculated single-photon spectra and Hong-Ou-Mandel interference without bandpass filter at a PPKTP crystal temperature of 40.0 °C and a pump power of 10 mW. At this crystal temperature phase matching is achieved only for non-degenerate signal and idler frequencies. a) Measured spectra of the down-converted signal (blue squares) and idler (cyan squares) photons. The solid curves represent calculated spectra. b) Measured (squares) and calculated (solid curve) Hong-Ou-Mandel interference. Error bars indicating the standard deviation in the measurements are smaller than the marker size. The shape of the Hong-Ou-Mandel dip is modified due to the non-degenerate signal and idler frequencies.

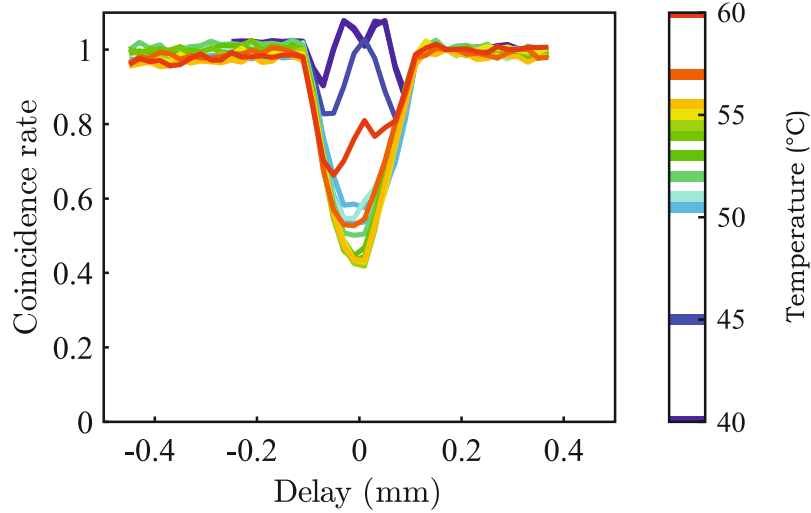


Figure 3.8 Measured Hong-Ou-Mandel interference for different temperatures of the PPKTP crystal without bandpass filter at a pump power of 10 mW. Phase-matching for frequency-degenerate signal and idler photons is fulfilled at a temperature of 54.5 °C, giving rise to a single deep Hong-Ou-Mandel dip. The asymmetry in the curves is due to non-perfect alignment of the quantum light source.

3.7 Discussion

We have constructed and characterized a versatile quantum light source based on spontaneous parametric down-conversion. Its output can be easily tuned from pure single-photon states to quantum states with a high photon number by tuning the pump power. Four-photon Fock states are estimated to be directly experimentally accessible. The source produces photon pairs at rates exceeding $17 \times 10^6 \text{ s}^{-1}$, of which routinely over $4 \times 10^6 \text{ s}^{-1}$ single counts are detected in each arm and approximately $0.76 \times 10^6 \text{ s}^{-1}$ coincidences between signal and idler. This coincidence rate can still be increased by improving the mode matching of the signal and idler with single-mode fibres. It would be also interesting to directly apply spatial shaping to the wavefront of the pump light using a spatial light modulator, and study if in this manner the spectral and spatial properties of the signal and idler photons can be influenced and controlled.

The system can be extended to generate four-photon $|1\rangle|1\rangle|1\rangle|1\rangle$ states in a straightforward manner. One could have the pump beam make a second pass through the PPKTP crystal to possibly generate an additional signal-idler pair in

the second pass. Alternatively a second PPKTP crystal can be added in which the second photon pair is generated. Since sufficient pump light is available, this can be extended further to multiple PPKTP crystals. High pump powers, which are required for generating multiphoton states, might lead to photochromic damage of the PPKTP crystal in the form of grey tracking [90], but this was so far not apparent. The combination of a high pump power and a collinear geometry could also enable a study of the crossover of spontaneous parametric down-conversion to classical optical parametric amplification.

In principle, the pump light source, which currently consists of a frequency-doubled mode-locked Ti:Sapphire oscillator, can be replaced by a continuous-wave blue diode laser. This would considerably simplify the quantum light source. As a consequence however, one would completely lose the ability to generate multiphoton states due to the low peak power. Also the photon pairs will be randomly distributed in time, instead of being confined to the short time intervals of the ultrashort laser pulses.

Inserting a quarter-wave plate at 45° in front of the polarizing beam splitter used to separate signal and idler, results in Hong-Ou-Mandel interference directly at this beam splitter, preparing the quantum states in a squeezed vacuum state. Alternatively, by replacing this polarizing beam splitter by a non-polarizing beam splitter, the source can be used to generate polarization-entangled photons in the Bell state $|\Psi^+\rangle = (|H\rangle|V\rangle + |V\rangle|H\rangle) / \sqrt{2}$. By selecting specific parts of the single-photon spectrum also the $|\Psi^-\rangle$ Bell state is accessible [91]. In these configurations the indistinguishability of signal and idler might be reduced by the residual distinguishability in arrival times of signal and idler photons, arising from the birefringence of the PPKTP crystal. This can be compensated by inserting an additional KTP crystal of length $L/2$ after the PPKTP crystal, with its axes rotated by 90° [92].

At low pump powers the visibility of Hong-Ou-Mandel interference is 86%. We expect that increasing the spectral indistinguishability of signal and idler, and thereby the visibility of quantum interference, can be achieved by additional spectral filtering. This does, however, introduce losses. The spectral bandwidth of the down-converted photons is currently given by the phase-matching bandwidth of the PPKTP crystal. Narrowing the spectral bandwidth without loss through filtering might be achieved by using a crystal of a longer length, because this narrows the bandwidth of phase matching. In that case one could also consider reducing the pump bandwidth. With the current crystal, however, reducing the pump bandwidth does not help. An alternative approach is to integrate the PPKTP crystal into a Sagnac interferometer [93]. A higher indistinguishability of the down-converted photons is also achieved by matching the group velocities of pump, signal and idler [94, 95]. Unfortunately in PPKTP this is not possible for signal and idler wavelengths around 790 nm. However, group-velocity matching can be realized in PPKTP for signal and idler wavelengths in the telecom range.

4 Programmable multiport optical circuits in opaque scattering materials

We propose and experimentally verify a method to program the effective transmission matrix of general multiport linear optical circuits in random multiple-scattering materials by phase modulation of incident wavefronts. We demonstrate our method by programming linear optical circuits in white paint layers with 2 inputs and 2 outputs, and 2 inputs and 3 outputs. Using interferometric techniques we verify the ability to program any desired phase relation between the outputs. The method works in a deterministic manner and can be directly applied to existing wavefront-shaping setups without the need of measuring a transmission matrix or to rely on sensitive interference measurements.

4.1 Introduction

In many optical experiments light propagates through linear optical circuits, involving beam splitters and interferometers. These optical circuits are often realized either in (i) free-space setups containing, e.g., mirrors, lenses, polarizers, wave plates, or in (ii) integrated photonics, such as coupled waveguides and cavities [96, 97]. Both free-space and integrated optical circuits are robust platforms for performing experiments with low optical losses. In principle, arbitrary complex linear circuits can be built this way [47, 98]. One can include, such as in Ref. [98], adaptive optical elements, which mostly give a controllable delay (phase shift). Especially in integrated photonics much effort is invested in controlling the refractive index [99–103] by, e.g., temperature tuning, free-carrier excitation, or optical Kerr switching. Nevertheless, doing this for a complex circuit remains a major experimental challenge.

Here we suggest the radically different approach to use wavefront shaping of light on random multiple-scattering materials as a platform for programmable linear optical circuits, as is illustrated in Fig. 4.1. Coherent light incident on stationary random multiple-scattering media, such as white paint, teeth, and paper, gives rise to speckle patterns as the result of the collective interference of scattered waves. The individual far-field speckle spots form diffraction-limited beams that are correlated to each other as if light would have propagated through a very complicated random linear optical circuit [26]. In essence one controls by modulating, e.g., the phase of the incident wavefront the degree of mode mixing of all scattered waves that contribute constructively to the target

The content of this chapter has been published as: S. R. Huisman, T. J. Huisman, T. A. W. Wolterink, A. P. Mosk, and P. W. H. Pinkse, *Opt. Express* **23**, 3102 (2015). This chapter contains simulations that have not been performed by the author of this thesis. However, they are included for consistency with the published article.

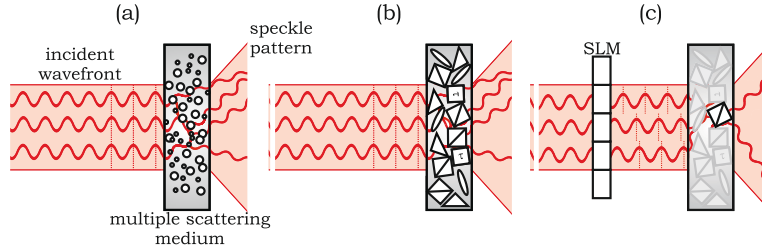


Figure 4.1 Wavefront-shaped programmable linear optical circuits. (a) Coherent light incident on a multiple-scattering medium results in a speckle pattern. (b) The scattered light can be described by a scattering matrix, representing a complicated linear optical circuit, made of many elements such as beam splitters, prisms, lenses, etc. The scattering matrix is here represented as light propagating through an effective medium with the same correlations as the optical circuit, however, the optical elements are not physically located at these positions in the material. (c) By phase modulation of the incident wavefront with a spatial light modulator (SLM) it becomes possible to address correlations in the scattering matrix to create an interference pattern with a desired functionality. In this picture light travels through the material as if it would have traveled through a beam splitter. Note: reflection is omitted in this figure for clarity.

spots [28, 29]. Adaptive wavefront shaping is generally known to enable focusing and imaging through multiple-scattering media. By wavefront shaping it is also possible to adaptively transform the speckle patterns of multiple-scattering materials to behave like many linear optical components, such as waveguides and lenses [29, 31], optical pulse compressors [32, 33], programmable wave plates [35] and beam splitters [36]. The manner in which the incident input modes are projected on the output modes by the scattering material can be conveniently described by a scattering matrix [27, 28]. To obtain the functionality of the desired linear optical device, one can, via wavefront shaping, address subsets of the scattering matrix to project the incident light on desired modes. Since one is in general not able to control all incident modes of the scattering matrix, and the scattering matrix might not contain all desired correlations, one has to tolerate losses that are typically higher than of custom fabricated optical circuits. On the other hand, an optical circuit constructed by wavefront shaping is inherently programmable in functionality, has a system size comparable to integrated photonics, and is in terms of optical hardware very easy to implement and adapt. In contrast to most integrated multimode-interference-based devices [104], our method exploits disorder for functionality and is therefore robust against imperfections and does not require careful fabrication of the scattering structure. However, up to now, a general method for creating arbitrary multiport linear optical circuits by wavefront shaping in random scattering materials was still

missing. A promising strategy is to measure the transmission matrix of the sample [105] and to adapt the wavefront to program the desired interference pattern. Unfortunately this requires many interference measurements, which is not always feasible.

We present a general wavefront-shaping method that controls the phase and amplitude correlations between the enhanced target spots. For this method it is not necessary to measure a transmission matrix or to rely on sensitive interference measurements. One only requires a phase-only spatial light modulator (SLM) and a camera; both are already present in most wavefront-shaping setups. We program in a deterministic manner an interference pattern that represents the functionality of multiport linear optical circuits, where the light interferes in a compact system with a size that is comparable with integrated photonics. We demonstrate the power of our method by realizing in an opaque scattering medium the equivalents of 2×2 and 2×3 linear optical circuits using wavefront shaping. As the random medium we use a layer of strongly scattering white paint deposited on glass. Our input basis consists of wavefront-shaped beams and the output basis consists of individual spots viewed on a CCD camera.

4.2 Algorithm

We show that it is possible to use a multiple-scattering material as an arbitrary mode-mixing circuit by combining the phase patterns of mode-by-mode wavefront-shaping optimizations. In the following we introduce our procedure, or algorithm, that describes the sequence of steps to be performed on the setup to arrive at the desired circuits. We describe here the most general implementation of our algorithm that should be valid for any existing wavefront-shaping setup. The algorithm is illustrated for a 2×2 optical circuit in Fig. 4.2 and explained for the general $n \times m$ optical system with n separate inputs and m separate outputs. We assume for simplicity that a single phase-only spatial light modulator is used, the incident input modes are spatially separated on the same SLM surface, and the resulting interference pattern is observed with a CCD camera. We use the term ‘optimization’ of a spot for intensity enhancing a target spot in a speckle pattern by phase modulation of the incident light. A single spot is considered as one independent output mode: the spots form an orthogonal basis. A single incident wavefront-shaped beam is considered to be a single input mode of the system. We assume that the desired optical circuit is supported by the scattering matrix of the multiple-scattering material. The algorithm consists of the following steps:

1. **Single input-output wavefront shaping:** Start with the first input mode incident on the SLM and the sample. Optimize by phase modulation of the incident light a target spot that forms output mode $1'$. Examples of algorithms for optimizing a single spot are described in [29, 106, 107]. Store the corresponding phase pattern on the SLM as $\theta_{1,1'}$. This corresponds to

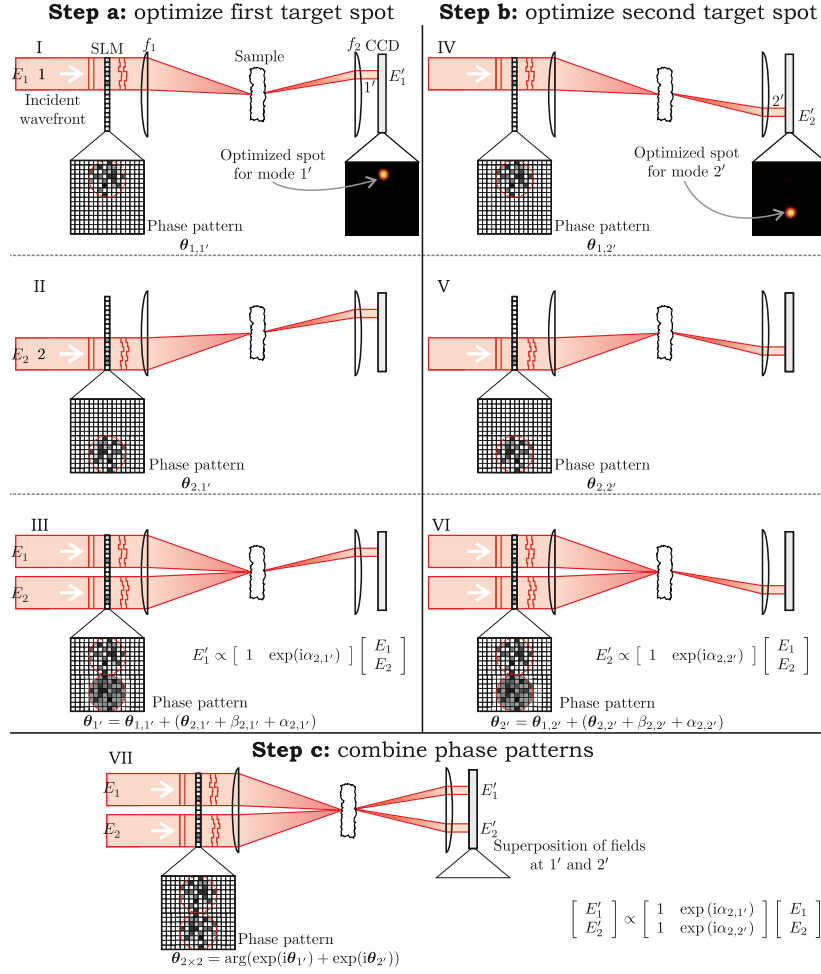


Figure 4.2 Schematic illustration for programming a 2×2 linear optical circuit. The incident input modes 1 and 2 are spatially separated on the SLM. (I-III) Optimization for output mode 1' providing phase pattern $\theta_{1'}$. (IV-VI) Optimization for output mode 2' providing phase pattern $\theta_{2'}$. (VII) Finally one writes phase pattern $\theta_{2 \times 2} = \arg(e^{i\theta_{1'}} + e^{i\theta_{2'}})$ to obtain a superposition of the fields in steps I and II. The CCD pictures are snapshots of our experiments on the 2×2 optical circuit.

Fig. 4.2 step I.

2. **Wavefront shaping of the other input modes for the same output mode:** Repeat step 1 to optimize a spot $1'$ for each other input mode. Store the final phase patterns $\theta_{2,1'} \cdots \theta_{n,1'}$. This corresponds to Fig. 4.2 step II. Now one has n phase patterns $\theta_{i,1'}$, each projecting one input i on output $1'$. Because all input modes are separated in space on the SLM surface, phase pattern $\theta_{i,1'}$ is only nonzero at the position of input mode i , and zero everywhere else (at the locations of the other input modes).
3. **Combination of phase patterns of individual optimizations:** Create a phase pattern:

$$\theta_{1,1'} + \theta_{2,1'}, \quad (4.1)$$

by blocking all but the first two input modes 1 and 2. Via the SLM and the sample this gives an enhanced spot at output mode $1'$ with light from both inputs. Adding the two phase patterns in Eq. (4.1) does not change the optimization of the individual inputs, since $\theta_{1,1'} = 0$ at the position of input 2 and vice versa. Until now only the intensity of the output mode has been considered. Therefore the relative phase of the contributions from both input modes still has to be adjusted in order to get constructive interference in the output. To realize this, a phase offset $\beta_{2,1'}$ is added at the corresponding illuminated pattern of the second input mode on the SLM (gray filled circle in Fig. 4.2 step III) that maximizes the intensity in output spot $1'$. The intensity is maximal when mode 1 and mode 2 are projected in phase on $1'$. Store this value for phase $\beta_{2,1'}$. After performing this adjustment, both input modes 1, 2 are projected in phase on output mode $1'$, and the phase pattern displayed by the SLM is:

$$\theta_{1,1'} + \theta_{2,1'} + \beta_{2,1'}. \quad (4.2)$$

4. **Combining all inputs for one output mode:** Block input mode 2 and open input mode 3, and repeat the procedure of the previous step for mode 1 and mode 3. Redo this for all remaining input modes. For $n \geq 2$ Eq. (4.2) can be generalized:

$$\theta_{1'} = \sum_{i=2}^n (\theta_{i,1'} + \beta_{i,1'}) + \theta_{1,1'}. \quad (4.3)$$

5. **Construction of one row of the transfer matrix:** In steps 3-4 we have enforced that all input modes are projected in phase on the target spot, where the first input mode was used as reference. Next we have all input modes incident on the sample with phase mask $\theta_{1'}$ on the SLM. In principle all input modes can be optimized simultaneous per output mode provided that the input modes are interferometrically stable during optimization. This phase mask automatically projects all input modes in phase on the

target spot. The corresponding complex field amplitude E'_1 at the target spot 1' becomes:

$$E'_1 = e^{i\phi_{1'}} \begin{bmatrix} |t_{1,1'}| & |t_{2,1'}| & \dots & |t_{n,1'}| \end{bmatrix} \begin{bmatrix} E_1 \\ E_2 \\ \vdots \\ E_n \end{bmatrix}, \quad (4.4)$$

where $\phi_{1'}$ is an overall phase factor with respect to a fixed reference and we have ignored an overall normalization factor. The amplitudes $|t_{i,1'}|$ are expected to be approximately equal to each other for an isotropic random scattering material, and are given by the square root of the intensity of the optimized spot. This equation can be simplified to a single-row transfer matrix equation describing a $n \times 1$ optical system:

$$E'_1 = \mathbf{T}_{n \times 1,1'} \begin{bmatrix} E_1 \\ E_2 \\ \vdots \\ E_n \end{bmatrix}. \quad (4.5)$$

6. **Amplitude control of each element in $\mathbf{T}_{n \times 1,1'}$:** One achieves amplitude control by manipulating the intensity enhancement of the spot for each input mode. Suppose one wants to decrease $|t_{2,1'}|$. In order to do so, add at the location of the second input mode a random phase pattern to $\theta_{1'}$ with a controlled amplitude to reduce the intensity enhancement to the desired level. Store this new phase pattern as $\theta_{1'}$. The phase of the transfer matrix element should remain unaffected if there are sufficient SLM segments used for the mode (about $\sim 10^2$ segments in our experiments). Otherwise one can compensate for this additional phase shift by repeating the procedure of step 4 for the specific input mode. It is important to note that this manner of controlling the amplitude of $|t_{i,1'}|$ will only reduce the amplitude level.
7. **Phase control of each element in $\mathbf{T}_{n \times 1,1'}$:** One achieves phase control over each input mode i by writing a desired phase offset $\alpha_{i,1'}$ to $\theta_{1'}$ at the corresponding illuminated region on the SLM. In this manner the unnormalized transfer matrix $\mathbf{T}_{n \times 1,1'}$ becomes:

$$\mathbf{T}_{n \times 1,1'} = e^{i\phi_{1'}} \begin{bmatrix} |t_{1,1'}| e^{i\alpha_{1,1'}} & |t_{2,1'}| e^{i\alpha_{2,1'}} & \dots & |t_{n,1'}| e^{i\alpha_{n,1'}} \end{bmatrix}. \quad (4.6)$$

We have now controlled independently both the phase and amplitude of each element in $\mathbf{T}_{n \times 1,1'}$. This is illustrated in Fig. 4.2 step III. In the remainder of this section we will explain how to get a desired transmission matrix with multiple inputs and multiple outputs.

8. **Wavefront shape inputs for other outputs:** Repeat steps 1-7 for the remaining number of orthogonal output spots. This is also illustrated in Fig. 4.2 steps IV-VI. At the end of this step one has m independent transfer matrices $\mathbf{T}_{n \times 1, m'}$ that each describe an $n \times 1$ optical system.
9. **Combine results for all outputs:** With all input modes incident, write the phase pattern $\theta_{n \times m}$:

$$\theta_{n \times m} = \arg \left(\sum_{j=1}^m c_j e^{i\theta_j} \right), \quad (4.7)$$

where subscript j denotes the j^{th} output mode, with $j \leq m$. The phase pattern $\theta_{n \times m}$ is a weighted vector sum of each of the m output optimizations θ_j , evaluated pixel by pixel. Consequently, the field in target output modes become related to the input modes as:

$$\begin{bmatrix} E'_1 \\ E'_2 \\ \vdots \\ E'_m \end{bmatrix} = f_1 \begin{bmatrix} c_1 \mathbf{T}_{n \times 1, 1'} \\ c_2 \mathbf{T}_{n \times 1, 2'} \\ \vdots \\ c_m \mathbf{T}_{n \times 1, m'} \end{bmatrix} \begin{bmatrix} E_1 \\ E_2 \\ \vdots \\ E_n \end{bmatrix}, \quad (4.8)$$

with f_1 a normalization factor. In this manner we have programmed an unnormalized transmission matrix $\mathbf{T}_{m \times n}$ given by:

$$\mathbf{T}_{m \times n} = \begin{bmatrix} c_1 \mathbf{T}_{n \times 1, 1'} \\ c_2 \mathbf{T}_{n \times 1, 2'} \\ \vdots \\ c_m \mathbf{T}_{n \times 1, m'} \end{bmatrix}. \quad (4.9)$$

This is illustrated for the 2×2 system in Fig. 4.2 VII. This transmission matrix projects the n input modes on the m output modes, with the desired linear optical functionality.

To illustrate what happens in Eq. (4.7), we consider a 1×2 circuit splitting one input mode equally into two output modes $1'$ and $2'$. For this circuit Eq. (4.7) reduces to $\theta_{1 \times 2} = \arg (e^{i\theta_{1'}} + e^{i\theta_{2'}})$, with $\theta_{1'}$ the phase pattern optimized to produce output mode $1'$ and $\theta_{2'}$ the pattern for output mode $2'$. To produce both outputs simultaneously, one performs a vector addition of the fields $1'$ and $2'$. The resulting phase pattern $\theta_{1 \times 2}$ contributes to both output modes. In Eq. (4.7) the superposition of the individual incident field patterns results into the desired correlations between the output modes because the scattering material is a linear system. This procedure requires that the individual output spots behave as independent uncorrelated output modes. If this is the case, all individual matrices describing patterns $e^{i\theta_j}$ in Eq. (4.7) should be orthogonal to each other. This condition is met if all $e^{i\theta_{i,j'}}$ for a given input mode i are orthogonal to each

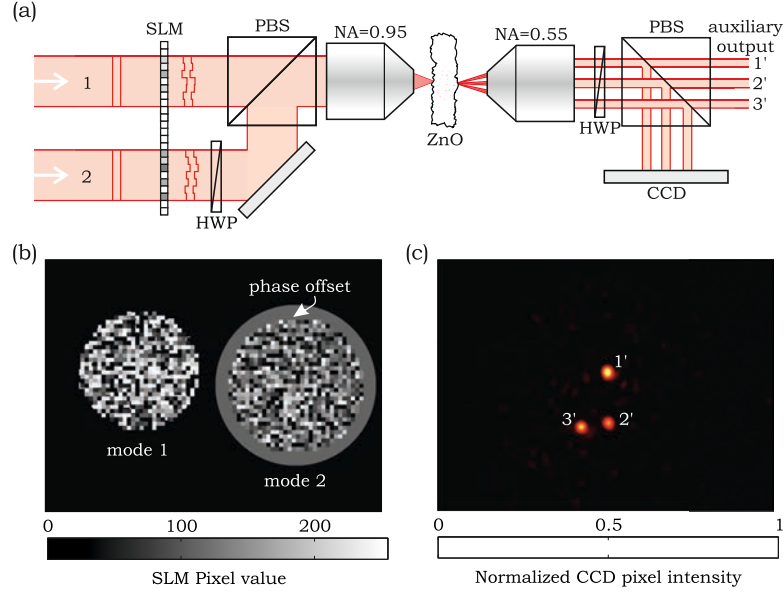


Figure 4.3 Setup for wavefront-shaped optical circuits. (a) Two input modes (1,2) are phase-modulated with a spatial light modulator (SLM). Both modes are spatially overlapped with a polarizing beam-splitter cube (PBS). The modes are focused on a layer of white paint (ZnO particles) that has been spray coated on a 1.5 mm thick microscope slide. The transmitted light is projected on a CCD camera. Three output modes 1', 2', and 3' are selected. (b) Optimized phase pattern on the SLM. A phase offset is applied to the second incident mode. (c) Camera image for three optimized spots when both input modes are incident on the phase pattern of (b).

other. Nonorthogonality results in background speckle and decreases the contrast of the output spots. In practice complete orthogonality is not met since the spots are weakly correlated with each other, which can be caused by the correlations in the scattering matrix of the material itself [25, 108], or by the fact that one only addresses subsets of the scattering matrix of the sample by wavefront shaping [109]. However, if this subset is large enough, typically $\sim 10^2$ independent SLM segments per wavefront describing an input mode in our experience, the spots behave approximately orthogonal to each other and therefore also the phase masks become orthogonal and the algorithm will work.

4.3 Experimental setup and methods

We demonstrate our method by wavefront shaping a programmable 2×2 and 2×3 transmission matrix in an opaque layer of white paint. In this section we describe our experimental setup and our measurement method.

4.3.1 Experimental setup

Our setup is illustrated in Fig. 4.3(a). This is the same setup as described in Ref. [36]. The light source is a mode-locked Ti:Sapphire laser (Spectra-Physics, Tsunami) emitting transform-limited pulses at a repetition rate of 80 MHz with a pulse width of approximately 0.3 ps at a centre wavelength of 790.0 nm. The beam is split and coupled into two separate single-mode fibres. The output of the two fibres have identical polarization and beam waist and form the input modes 1 and 2. The two modes are phase-modulated with a SLM (Hamamatsu, LCOS-SLM). Figure 4.3(b) illustrates an optimized phase pattern. Clearly, both modes are spatially separated on the SLM surface. Behind the SLM, the two modes are spatially overlapped with a half-wave plate (HWP) and polarizing beam splitter (PBS) cube, resulting in collinear propagation of modes with orthogonal polarization. This allows us to completely fill the aperture of the objective (NA=0.95) that images the SLM on the conjugate plane of the layer of white paint. Creating a configuration with more than 2 inputs requires spatial shaping of the inputs to have orthogonal incident modes arriving at the sample, e.g. by creating angular gradients, patterned beams, etc. The surface of the SLM is imaged on the back focal plane of the objective with two lenses in a 4- f configuration (not shown). Both pulses arrive simultaneously at the sample. We make sure that the power of both input modes on the objective are the same (approximately 0.5 mW per mode). However, input mode 1 is transmitted more efficiently by the objective than input mode 2 because of experimental imperfections. This causes the optimized spots for mode 1 to have a higher intensity. The layer of white paint consists of ZnO powder with a scattering mean free path of $0.7 \pm 0.2 \mu\text{m}$. The layer is approximately $30 \mu\text{m}$ thick and is spray painted on a glass microscope slide of 1.5 mm thickness. The transmitted pattern is collected with a second objective (NA=0.55) and directly projected on a CCD camera after reflection on a PBS, see for example Fig. 4.3(c) where three optimized spots are visible. The intensity values for the CCD pixels that correspond to the target spots are spatially integrated to obtain the output powers for the interference pattern.

4.3.2 Measurement method

We start with a single input mode incident on the material and select on the camera an arbitrary location for intensity enhancing a target spot. The SLM is divided by us into segments of 10×10 pixels. As a result, one input mode is controlled by approximately 500 segments. We found that this provides maximum

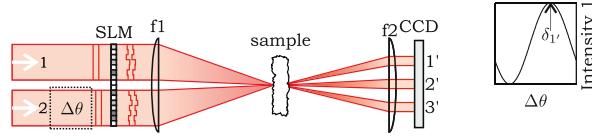


Figure 4.4 Interference measurement of the effective transmission matrix. A phase difference $\Delta\theta$ is applied between the two input modes. The intensity in the target optimized spots is measured as a function of this phase difference.

intensity enhancement. The SLM controls the phase by addressing the pixels with 8-bit pixel values. In our experiment a pixel value of 207 corresponds to a phase difference of 2π rad. We first pre-optimize spots by fitting the optimal phase for each segment that provides maximum constructive interference in the target spot, as used in Ref. [29]. We apply this method twice to reduce the effect of read-out noise of the camera, in spirit of the work in Ref. [107]. We obtain a higher enhancement when a final optimization is made by sequentially addressing each segment with a random phase and accept it if the intensity increased. We apply this procedure about 5 times for each pixel. In case there is no initial intensity present at the intended target, the random phase procedure is also used as an initial optimization. The total optimization time for one input mode to one output mode is approximately 1.5 hours. The typical intensity enhancement for an individual spot is in the order of 50 times the average intensity of the other spots. The throughput of the sample and imaging optics is not crucial for this proof-of-principle demonstration and is estimated to be on the percent level.

This procedure is repeated for each input and each output mode. With the algorithm leading to Eq. (4.9) the phase pattern that provides the desired transmission matrix is generated. The obtained transmission matrix is characterized with interference measurements, as described in Ref. [36] and Fig. 4.4. A phase difference $\Delta\theta$ is applied between the input modes, see Fig. 4.4, to monitor the interference in the output modes. From these interference measurements we extract the phase of each element of the transmission matrix. This phase difference $\Delta\theta$ is applied with the SLM on input mode 2. Figure 4.3(b) shows an example. We define $\delta_{j'}$ as the phase $\Delta\theta$ for which maximum intensity occurs in output mode j' , as indicated for mode 1' in Fig. 4.4.

4.4 The 2×2 optical circuit

We demonstrate our algorithm by first programming a 2×2 optical circuit with a transmission matrix of the form:

$$\mathbf{T}_{2 \times 2} = \begin{bmatrix} |T_{11}| & |T_{12}| \\ |T_{21}| & |T_{22}|e^{i\alpha} \end{bmatrix}. \quad (4.10)$$

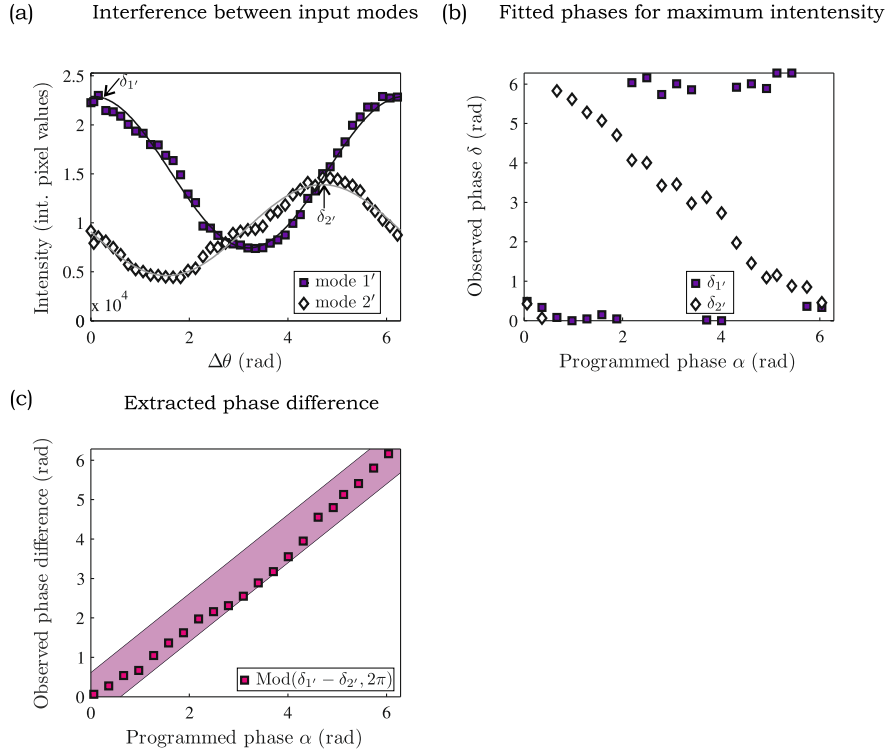


Figure 4.5 Experimental realization of a programmed 2×2 linear optical circuit. A transmission matrix is programmed for which output mode $2'$ has a programmable phase difference α with respect to output mode $1'$. (a) Example of a measured (symbols) interference characterization, by applying a phase difference $\Delta\theta$ between the input modes, of the transmission matrix for $\alpha = 2$ rad. Sinusoidal fits (solid) are used to determine the phases δ for which maximum intensity occurs. (b) Extracted phases δ as a function of the programmed phase α . Note that the displayed phase is wrapped, so there are no 2π jumps in $\delta_{1'}$ and $\delta_{2'}$. Hence the difference $\delta_{1'} - \delta_{2'} \approx -4.7$ rad in panel (a) becomes 1.6 rad in panel (c). (c) Extracted phase difference between the output modes (symbols) in comparison with the expected phase difference (diagonal band) based on the programmed phase α . The observed phase differences between the output modes match the programmed phase differences excellently.

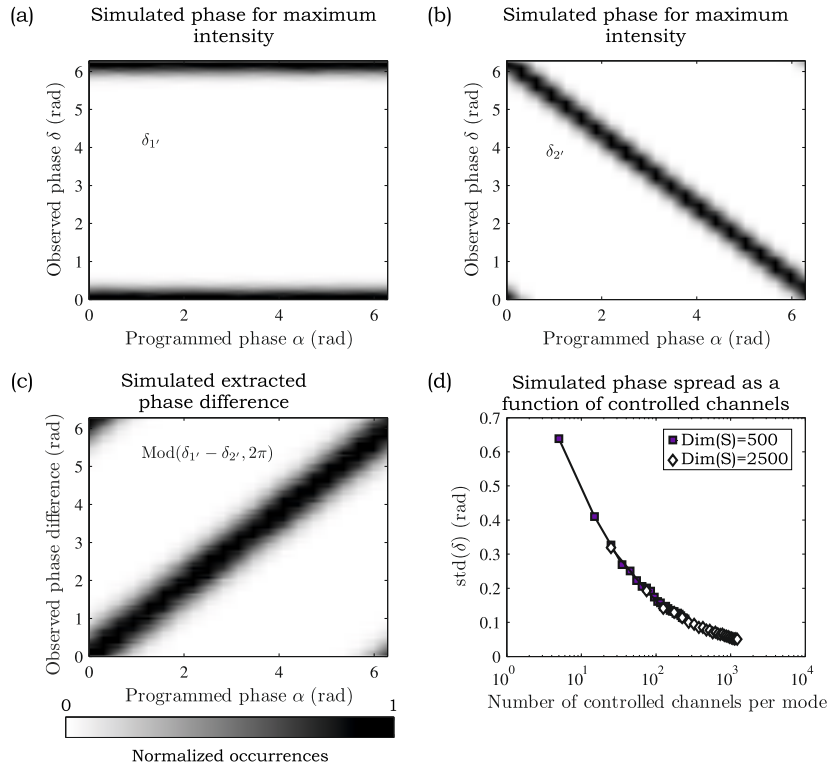


Figure 4.6 Computational results on the phase differences of the 2×2 linear optical circuit. 10,000 realizations were simulated for systems with a scattering matrix of dimension 1000 and with 50 controlled channels per input mode. (a) Obtained distribution for phase $\delta_{1'}$. (b) Obtained distribution for phase $\delta_{2'}$. (c) Extracted phase difference between the output modes. (d) Width of the phase distributions as a function of controlled channels for scattering matrices of dimension 500 and 2500.

For simplicity we only control the phase correlations inside the transmission matrix and not the amplitude. The amplitudes $|T_{a,b}|$ are set by the intensity enhancement of the individual spots and are approximately equal. We let the phase of element $T_{2 \times 2}(2,2)$ vary with controllable phase α , to demonstrate the ability to program the phase correlations of this optical circuit. The four phase patterns $\theta_{1,1'}$, $\theta_{2,1'}$, $\theta_{1,2'}$, $\theta_{2,2'}$ were combined to overall phase pattern $\theta_{2 \times 2}(\alpha)$ following our algorithm, in which step 6 was excluded. First we find the four phase patterns $\theta_{1,1'}$, $\theta_{2,1'}$, $\theta_{1,2'}$, $\theta_{2,2'}$ projecting the individual inputs 1, 2 on the individual outputs $1'$, $2'$ (steps 1-2 of the algorithm). Next both input modes are projected in phase on the output modes by finding $\beta_{2,1'}$ and $\beta_{2,2'}$ (steps 3-5). Then we program the phase of element $T_{2 \times 2}(2,2)$ according to Eq. (4.10) by setting $\alpha_{2,2'} = \alpha$ (step 7). Finally all phase patterns are combined to the overall phase pattern $\theta_{2 \times 2}(\alpha)$ (steps 8-9). Phase α is varied in 21 steps. Therefore in total 21 different phase patterns $\theta_{2 \times 2}(\alpha)$ were made for our measurements. Note that the transmission matrix for $\alpha = \pi$ represents the equivalent of a standard optical beam splitter [83], which is in the case of the current algorithm fully controlled, in contrast to the algorithm for the wavefront-shaped beam splitters obtained in Ref. [36].

The results are presented in Fig. 4.5. Figure 4.5(a) shows the interference results for the two optimized spots for $\alpha = 2$ rad. Two sine functions are fitted to the output modes to determine the phases $\delta_{1'}$ and $\delta_{2'}$ at which maximum intensity occurs. The phases $\delta_{1'}$ and $\delta_{2'}$ for each α are shown in Fig. 4.5(b). We observe that $\delta_{1'}$ is approximately constant as function of α , while $\delta_{2'}$ decreases linearly with α . Ideally, for circuit with the transmission matrix of Eq. (4.10), one would expect that $\delta_{1'}$ remains exactly constant as function of α . Phase fluctuations due to a lack of stability of our setup can be neglected. However, there is crosstalk between the modes since they are not perfectly orthogonal. Figure 4.5(c) presents the main results of the 2×2 optical circuit: the observed phase difference between the output modes as a function of the programmed value for α . The diagonal band represents the expected phase difference, based on the target phase α , and the experimental uncertainties in phase offsets $\beta_{2,1'}$ and $\beta_{2,2'}$. We observe an excellent agreement between our measurements and predicted values. Our proof-of-principle experiments demonstrate full phase control of wavefront shaping 2×2 optical circuits in opaque scattering media in a deterministic manner.

For comparison, we also performed simulations to support our measurements. Figures 4.6(a)-4.6(c) present computational results in which we have repeated our experiment 10,000 times on simulated random unitary scattering matrices with a dimension of 1000 and 50 controlled channels per input mode (a scattering matrix of dimension 1000 means that there are 1000 independent channels). Similar simulations were performed by us in [36], but now we have implemented the algorithm presented in this chapter. Figure 4.6(a) shows the histograms for the fitted phase $\delta_{1'}$ as a function of α . Figure 4.6(b) shows the histograms for fitted phase $\delta_{2'}$. Figure 4.6(c) shows the histogram for the phase

difference between the output modes. All three figures demonstrate histograms with a finite width. This width is a manifestation of the non-orthogonality caused by addressing a subset of the scattering matrix, as described below step 9 of the algorithm. In these simulations a subset of the scattering matrix becomes addressed that consists of 2 rows, corresponding to the output spots, and 100 columns, corresponding to the two modes that are controlled by 50 independent channels each. This subset does not consist of orthogonal rows anymore, resulting in the output spots being weakly correlated, which also occurs in our experiment. Apparently, the width of the observed phases $\delta_{1'}$ and $\delta_{2'}$ is independent of α and is identical for $\delta_{1'}$ and $\delta_{2'}$.

Figure 4.6(d) shows another set of simulations where the standard deviation of the phase distributions is plotted as a function of the controlled number of independent channels per wavefront-shaped input mode. We have performed these simulations for scattering matrices with dimension 500 and 2500. Each data point was obtained by ensemble averaging over 1,000 different realizations. We observe that the standard deviation of these phase distributions decreases with an increased number of controlled elements. More computational and theoretical work is necessary to understand the efficiency, in terms of power throughput, and accuracy of wavefront-shaping optical circuits, which is beyond the scope of this chapter.

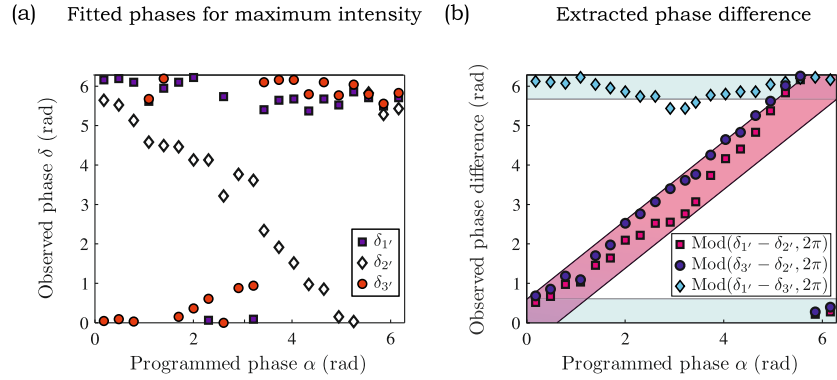


Figure 4.7 Experimental realization of a programmed 2×3 linear optical circuit. A transmission matrix is programmed for which output mode $2'$ has a programmable phase difference α with respect to output modes $1'$ and $3'$. (a) Extracted phases δ (symbols) as a function of the programmed phase difference α . (b) Extracted phase difference between the output modes (symbols) in comparison with the expected phase differences (horizontal and diagonal bands) based on the programmed phase α . The observed phase differences between the output modes match the programmed phase differences excellently. The pink band indicates the uncertainty in the phase determination.

4.5 The 2×3 optical circuit

Here we present experiments for a 2×3 optical circuit. The transmission matrix of the 2×3 optical circuit is given by:

$$\mathbf{T}_{2 \times 3} = \begin{bmatrix} |T_{11}| & |T_{12}| \\ |T_{21}| & |T_{22}| e^{i\alpha} \\ |T_{31}| & |T_{32}| \end{bmatrix}, \quad (4.11)$$

with controllable phase difference α . We let the phase of element $\mathbf{T}_{2 \times 3}(2,2)$ vary with controllable phase α . First we find the six phase patterns projecting the individual inputs 1, 2 on the individual outputs $1'$, $2'$, $3'$ (steps 1-2 of the algorithm). Next, both input modes are projected in phase on the output modes (steps 3-5). Then we program the phase of element $\mathbf{T}_{2 \times 3}(2,2)$ by setting $\alpha_{2,2'} = \alpha$ in Eq. (4.11) (step 7). Finally all phase patterns are combined to the overall phase pattern $\theta_{2 \times 3}(\alpha)$ (steps 8-9). Phase α is varied in 21 steps.

The results are presented in Fig. 4.7. The phases for which maximum interference occurs in the output modes, $\delta_{1'}$, $\delta_{2'}$, and $\delta_{3'}$, are shown in Fig. 4.7(a) for each programmed phase α . We observe that $\delta_{1'}$ and $\delta_{3'}$ are approximately constant as function of α , while $\delta_{2'}$ decreases linearly with α . The fluctuations in $\delta_{1'}$ and $\delta_{3'}$ are caused by the non-orthogonality of the output modes, as was explained in more detail for the 2×2 optical circuit in the previous section. Figure 4.7(b) shows the main result, the relative phase differences between the output modes. The symbols represent the measurements and the bands represent the expected phases based on the accuracy at which we program the transmission matrix. The observed phase differences between the output modes match very well the expected phase differences. Our proof-of-principle experiments demonstrate full phase control of wavefront shaping 2×3 optical circuits in white paint in a deterministic manner.

4.6 Conclusions and outlook

In summary, we have presented a method that transforms random multiple-scattering materials into programmable multiport linear optical circuits by phase modulation of incident wavefronts. The method provides the desired transmission matrix in a deterministic manner and it can be implemented in most existing wavefront-shaping setups. We have described proof-of-principle experiments in which we have used a white paint layer as programmable 2×2 and 2×3 optical circuits. The experimental observed phase relations demonstrate a very good agreement with theory.

We anticipate that our method can be implemented to make more advanced linear optical circuits with a larger number of inputs and outputs. More research is required to understand how efficiently one can shape an interference pattern

with a programmed correlation to achieve the functionality of the desired optical circuit. Many parameters have to be explored to identify the restrictions of our algorithm. It would be fascinating to explore the influence of the scattering properties of the material, e.g., the sample geometry, the sample thickness, and scattering mean free path. The performance of our algorithm is expected to be affected by the efficiency of the wavefront-shaping process, which determines the intensity enhancement and the amount of light that gets focused in a target spot. Based on the linearity of the intensity of the optimized spots with the number of controlled channels [29], we expect the efficiency, in terms of power throughput, of our algorithm to scale as $1/n$ where n is the number of inputs. However, it is an open question if more efficient configurations exist. Using random scattering media described by scattering matrices of lower dimension, such as disordered multimode fibres or planar disordered structures, will reduce optical losses caused by uncontrolled channels. This would make it possible to use these wavefront-shaped optical circuits for those adaptive quantum optical experiments in multiple-scattering materials [43, 46] where efficiencies in the order of 1% are acceptable. Our presented method requires the setup to be interferometrically stable during the optimization of a single speckle spot. To program a 2×2 circuit now took about 6 hours, because each phase pattern required about 1.5 hours of optimization. We anticipate that by using a micromirror based SLM, in combination with faster algorithms, the time to program a similar circuit can be reduced to a matter of seconds [110]. In our experiments we worked with linearly-polarized light. By using polarization-selective components for the incident light and the scattered light, and additional cameras for detection, it becomes possible to use our algorithm for any polarization basis for the input and output modes, such as circularly-polarized light. In addition, it would be intriguing to use structured scattering materials in order to more efficiently address certain correlations in the scattering matrix for programmed functionality.

There exist alternative approaches for programmable optical circuits that provide orders of magnitude less scattering losses, such as achieved in integrated photonics. Each approach requires a scattering platform and adaptive optical components to control the mode mixing. The more complex the transmission matrix needs to be, the more advanced the scattering platform and adaptive optical components should become to obtain a high energy efficiency. In our experiment we have sacrificed energy efficiency: on the order 1% of the light travels through the effective desired optical circuit. However, we have gained in simplicity of the experimental design. Our method for a programmable optical circuit is robust against fabrication disorder, versatile to operate, and the mode-mixing heart of the circuit takes place in a compact system size comparable with integrated photonics.

5 Programmable two-photon quantum interference in 10^3 channels in opaque scattering media

We investigate two-photon quantum interference in an opaque scattering medium that intrinsically supports a large number of transmission channels. By adaptive spatial phase-modulation of the incident wavefronts, the photons are directed at targeted speckle spots or output channels. From 10^3 experimentally available coupled channels, we select two channels and enhance their transmission, to realize the equivalent of a fully programmable 2×2 beam splitter. By sending pairs of single photons from a parametric down-conversion source through the opaque scattering medium, we observe two-photon quantum interference. The programmed beam splitter need not fulfil energy conservation over the two selected output channels and hence can be non-unitary. Consequently, we have the freedom to tune the quantum interference from bunching (Hong-Ou-Mandel-like behaviour) to antibunching. Our results establish opaque scattering media as a platform for high-dimensional quantum interference that is notably relevant for boson sampling and physical-key-based authentication.

5.1 Introduction

Light waves propagating through an opaque scattering medium exhibit a random walk inside the medium, which is caused by multiple scattering from spatial inhomogeneities [25]. An alternative description describes this phenomenon by a transmission matrix [27, 28]. The transmission matrix describes how many input channels are coupled to a similarly large number of output channels, see Fig. 5.1. The number of these channels can be controlled, and easily made to exceed millions, by controlling the illuminated area on the medium. Recent advances in control of light propagation through wavefront shaping allow for complete control over these channels in multiple-scattering media [28–30]. Because of their large number of controllable channels, we explore the use of multiple-scattering media to study quantum interference between multiple photons. Employed as a platform for high-dimensional quantum interference, over a large number of channels, multiple-scattering media are of relevance to boson sampling [13–21], quantum information processing [4–7], and physical-key-based authentication [46].

The content of this chapter has been published as: T. A. W. Wolterink, R. Uppu, G. Cstis, W. L. Vos, K. -J. Boller, and P. W. H. Pinkse, *Phys. Rev. A* **93**, 053817 (2016).

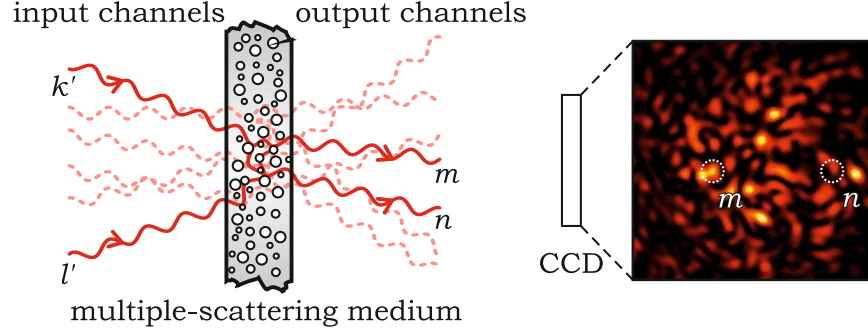


Figure 5.1 A multiple-scattering medium couples millions of input and output channels. Light incident in the input channels results through multiple scattering in a complex interference pattern (speckle, see right panel) at the output, which can be imaged by a CCD camera. Each speckle spot in the image corresponds to an independent output channel. In this chapter we have programmed their interaction to create a network with 2 inputs (k', l') and 2 outputs (m, n).

It has previously been observed that quantum states are robust against multiple scattering. Correlations in two-photon speckle patterns in single-scattering media have been studied [40, 42]. Furthermore, propagation of quantum noise [38, 39, 41] and propagation of single photons (Fock states) through multiple-scattering media [43, 44] have also been explored. So far it has remained an open question if quantum interference of multiple photons could be demonstrated inside a multiple-scattering medium. A fundamental hurdle one might expect in an experimental implementation is the extremely low transmission of almost all channels in the multiple-scattering medium. Remarkably, the transmission per channel is not necessarily low since wavefront shaping allows the funneling of light into selected output modes [28, 30].

Here we report on an experiment in which we study quantum interference in a multiple-scattering medium. We observe quantum interference of pairs of single photons in a programmable 2×2 beam splitter [36, 37], made of a multiple-scattering medium and a spatial light modulator (SLM). In our experiment, the SLM controls approximately 10^3 optical channels that are coupled in a reproducible yet unpredictable way in the multiple-scattering medium. The wavefront-shaping technique using the SLM allows us to select two out of N output channels by enhancing the optical power transmitted in these channels. Programmability in this beam splitter is achieved by controlling the relative phase between the input and output arms, beyond what is possible with a conventional beam splitter (as described in chapter 2). We exploit this freedom in programming the relative phase for demonstrating not only the well-known Hong-Ou-Mandel-like bunching [1], but also the antibunching of the outgoing photon

pairs, as well as any intermediate quantum correlation. Our result establishes opaque scattering media as a platform for high-dimensional quantum interference experiments as needed in, e.g., boson sampling. At present we control about 10^3 channels, but this can readily be scaled up to a number comparable to the number of pixels in modern SLMs, which is of the order of 10^6 .

5.2 Experimental setup

Pairs of single photons in our experiment are generated using collinear Type-II spontaneous parametric down-conversion (SPDC) with a mode-locked and frequency doubled pump laser beam at a wavelength centred at 395 nm [43, 85, 86]. For a complete description of the quantum light source, see chapter 3. To measure the degree of indistinguishability of the two photons, we observe Hong-Ou-Mandel (HOM) interference at a conventional 50:50 beam splitter as shown in Fig. 3.4. At a pump power of 10 mW, a HOM dip with a visibility of 64% is observed. The spectral indistinguishability can be improved by using a bandpass filter with a bandwidth of 1.5 nm, resulting in a HOM dip with an increased visibility of 86%.

To demonstrate programmable quantum interference in a multiple-scattering medium, we direct the light from the quantum light source to a wavefront-shaping setup with two SMFs as shown in Fig. 5.2(a). The two fibre outputs have identical polarization and beam waist and form the input modes k and l for the quantum interference experiment. The wavefronts of both modes are phase modulated with a liquid-crystal SLM, and afterwards spatially overlapped using a half-wave plate and a PBS, resulting in a collinear propagation of the two modes with orthogonal polarizations. The orthogonal input polarizations ease the process of creating multiport circuits using wavefront shaping [37]. The multiple three-dimensional scattering within the medium results in an unpolarized speckle pattern, on-average. However the degree of polarization is preserved within each speckle [111, 112]. Using wavefront shaping the transmitted light can be projected into any chosen polarization [35]. An objective (NA=0.95) is used to focus the light onto the scattering medium which comprises of a 500 μm thick layer of polytetrafluoroethylene (PTFE, Teflon), with scattering mean free path of $150 \pm 10 \mu\text{m}$ (measured by coherent backscattering [23, 24]). The experimental setup, including multiple-scattering medium, is interferometrically stable for a duration longer than a month. The transmitted light is collected by an objective (NA=0.6) and after transmission through a PBS it is coupled into two multimode fibres (output modes m and n) connected to single-photon counting modules (SPCM). This PBS ensures that the output modes have the same, well-defined linear polarization. The fibres have a core diameter of 200 μm , which is smaller than the size of a single speckle in the transmitted light. This ensures light collection from only a single mode. The total number of contributing modes (speckles), N , is approximately 10^4 . By rotating a half-wave plate this

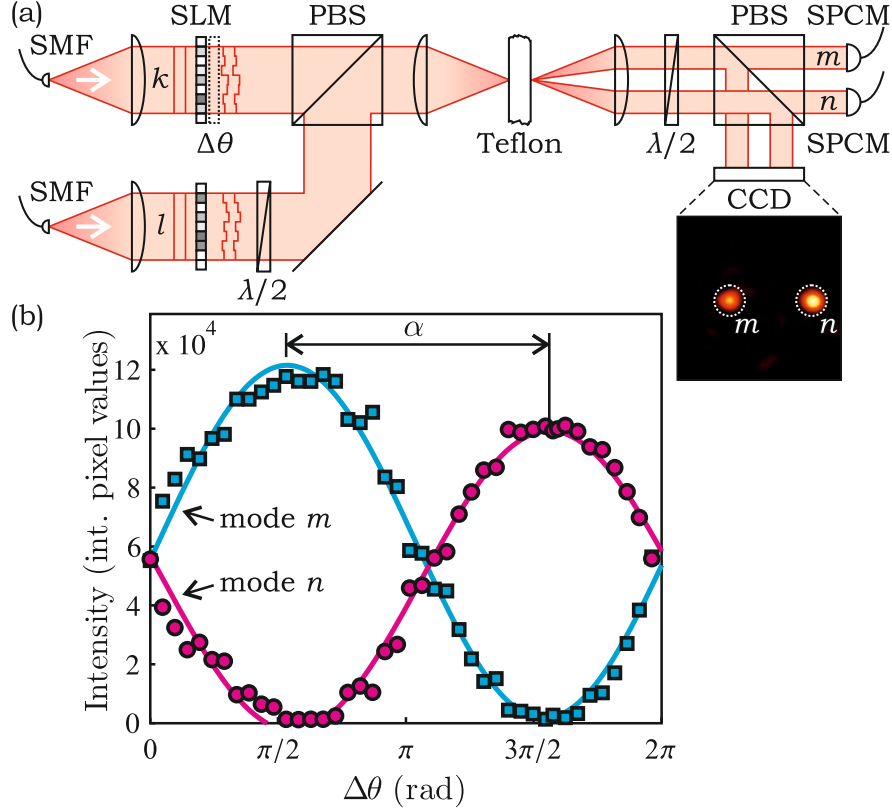


Figure 5.2 Wavefront-shaping setup for programming quantum interference. (a) Two input modes (k, l) are modulated with a SLM, spatially overlapped with orthogonal polarizations, and focused on a layer of Teflon. The transmitted light is either projected onto a CCD, or onto two fibres connected to SPCMs which are selectively observing two output modes (m, n). (b) Interference between the input modes onto the output modes m (cyan) and n (magenta). The solid curves indicate sine fits to the data, resulting in $\alpha = 1.02\pi$.

light can also be reflected off the PBS and projected onto a CCD camera for wavefront shaping.

Realization of a programmable 2×2 beam splitter inside a scattering medium follows a wavefront-shaping process (see chapter 4). To ease this process, we couple classical laser light ($\lambda_c = 790$ nm) into the SMFs and monitor the light in the output modes using amplified photodiodes. In short, the process starts with a single input mode k incident on the scattering medium. We optimize the output mode m by fitting the optimal phase for each SLM segment that re-

sults in maximum constructive interference in the fibre [29]. Each input mode is controlled by approximately 960 segments on the SLM. The average intensity of each output mode before optimizing is $1/N$, i.e., all output modes are nearly equiprobable for single photons. For our experimental setup with $N \approx 10^4$, we estimate an extremely low coincidence detection rate in a photon correlation measurement between two modes of $0.02^2 (1/N)^2 10^6 \text{ s}^{-1} = 4 \times 10^{-6} \text{ s}^{-1} \approx 1/(3 \text{ days})$, considering a photon-pair generation rate of 10^6 s^{-1} and an effective detection probability of 2%, as set by all optical losses in the setup and detector efficiencies. However after optimizing, the intensity of the enhanced output mode coupled to the fibre is about 200 times higher, i.e., the sampling probability of this mode is $200/N$. In photon correlation measurements, this enhancement would result in a strong increase by a factor of 10^4 in coincidence detection rates, now giving coincidence detection rates of $0.04 \text{ s}^{-1} \approx 100 \text{ h}^{-1}$. We optimize the second output mode n in the same way. A camera image of two optimized output modes is shown in Fig. 5.2(a). This optimization procedure is repeated for the input mode l , resulting in four phase patterns. As the final step, by combining these four interference patterns we program any 2×2 circuit [37], in which the relative phase between the input and output modes can still be selected as desired.

5.3 Model

The transmission through the circuit in this experiment is described by the following equation, cf. Eq. (2.7), that relates the electric field of the two output modes E_m and E_n to that of the two input modes, E_k and E_l through the transmission matrix $\mathbf{T}$:

$$\begin{bmatrix} E_m \\ E_n \end{bmatrix} = \mathbf{T} \begin{bmatrix} E_k \\ E_l \end{bmatrix} = t \begin{bmatrix} 1 & 1 \\ 1 & \exp(i\alpha) \end{bmatrix} \begin{bmatrix} E_k \\ E_l \end{bmatrix}, \quad (5.1)$$

where the parameter α is set in the algorithm when combining the interference patterns. The amplitude transmission coefficient t has $|t| < 1/\sqrt{2}$, emphasizing that the circuit is inherently lossy for the two selected output modes. Since the two selected modes stem from a manifold of N modes, the programmed 2×2 circuit need not fulfil energy conservation and could thus be non-unitary. Only for $\alpha = \pi$ and $|t| = 1/\sqrt{2}$ we do have a unitary matrix, i.e., $\mathbf{T}^\dagger \mathbf{T} = 1$, and this transmission matrix represents an ideal 50:50 beam splitter. To confirm the functionality of each circuit, classical light is injected into both input modes k and l and the intensities of the output modes m and n are monitored while applying a phase difference $\Delta\theta$ between the input modes. An example of such an interference measurement is shown in Fig. 5.2(b) for $\alpha = \pi$. A similar measurement at $\alpha = 0$ shows two overlapping $(1 + \sin \Delta\theta)$ -shaped curves, indicating the inherent non-unitary behaviour of this 2×2 circuit. After programming the functionality, we switch back from classical light to single photons.

Quantum-mechanically, the circuit of Eq. (5.1) can be described using ladder operators $\hat{a}$ as follows (see also chapter 2.2):

$$\begin{bmatrix} \hat{a}_m \\ \hat{a}_n \end{bmatrix} = \mathbf{T} \begin{bmatrix} \hat{a}_k \\ \hat{a}_l \end{bmatrix} + \begin{bmatrix} \hat{F}_m \\ \hat{F}_n \end{bmatrix}, \quad (5.2)$$

where $\hat{F}_m$ and $\hat{F}_n$ are the Langevin noise operators that model the losses in the selected output modes [67, 113]. These losses also include the residual intensity in unmonitored modes. Writing the input of the circuit described by Eq. (5.2) as $\Psi_{\text{in}} = |1\rangle_k |1\rangle_l$, one can find the probabilities for all possible outcomes in a straightforward manner [67] for indistinguishable photons, by substituting $\rho = r = \tau = t$ and $I_{\text{ov}} = 1$ in Eq. (2.43)-(2.48):

$$\begin{aligned} P(2_m, 0_n) &= P(0_m, 2_n) = 2|t|^4, \\ P(1_m, 1_n) &= 2|t|^4 (1 + \cos \alpha), \\ P(1_m, 0_n) &= P(0_m, 1_n) = 2|t|^2 - 2|t|^4 (3 + \cos \alpha), \\ P(0_m, 0_n) &= 1 - 4|t|^2 + 2|t|^4 (3 + \cos \alpha). \end{aligned} \quad (5.3)$$

Of interest are the probabilities $P(2_m, 0_n)$, $P(0_m, 2_n)$, and $P(1_m, 1_n)$, for which both photons arrive in output modes m and n . As is evident from the α -dependence of $P(1_m, 1_n)$, we have the freedom to program the quantum interference from bunching (Hong-Ou-Mandel-like behaviour) to antibunching by tuning α . The contribution of the unmonitored modes shows up as the nonzero probabilities $P(1_m, 0_n)$, $P(0_m, 1_n)$, and $P(0_m, 0_n)$, which account for losses of photons in the output modes m and n .

5.4 Results

Using the circuit of Fig. 5.2(b) programmed with $\alpha = \pi$, representing a 50:50 beam splitter, should result in HOM interference in the scattering medium. Figure 5.3(a) shows the measured quantum interference for this circuit which indeed shows a HOM dip. These measurements were done using a pump power of 100 mW and without a bandpass filter. While this higher pump power (in comparison to Fig. 3.4) generates more photon pairs ($17 \times 10^6 \text{ s}^{-1}$), it also increases the generation rate of higher photon-number states. These states reduce the visibility of the HOM dip. The measured HOM dip with a conventional beam splitter at this pump power indeed shows a reduced visibility of 24%. To consolidate the quantum nature of the interference via a larger-than-50% visibility [56], we repeated the measurements at a reduced pump power of 40 mW and with a bandpass filter in place, which results in a visibility of 59% as shown in Fig 5.3(b). Indeed the data match the prediction and therefore confirms the quantum nature of the interference.

We now explore the programmability of the quantum interference. For indistinguishable single photons and for arbitrary α , we expect the probability to

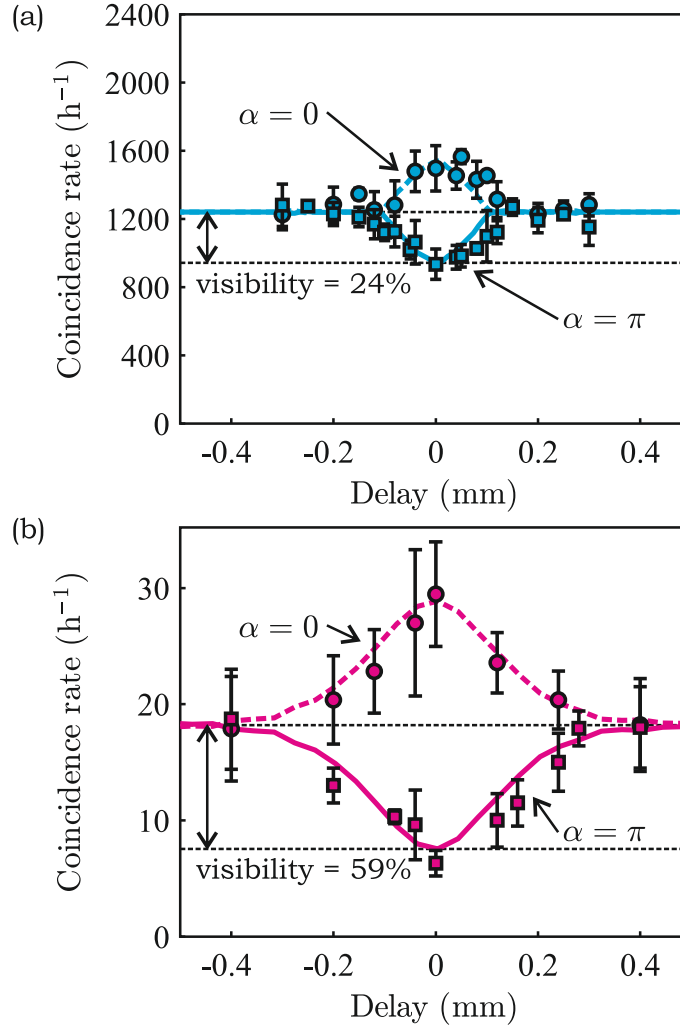


Figure 5.3 Programmable quantum interference. Setting $\alpha = \pi$ gives rise to a dip in coincidence counts (squares), while $\alpha = 0$ gives a peak (circles). Error bars indicate the standard deviations in the measurements. (a) depicts measurements performed at a pump power of 100 mW without bandpass filter, and (b) at a pump power of 40 mW with the filter in place. The solid curves in the plots correspond to the measured coincidence dips using a conventional beam splitter. The flipped traces of these are shown by the dashed curves as a guide to the eye.

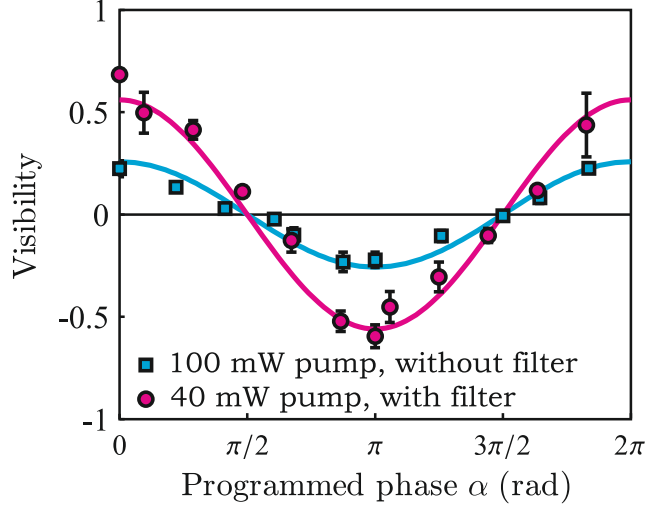


Figure 5.4 Programmable quantum interference as a function of programmed phase α at a pump power of 100 mW without filter (cyan), and at 40 mW with bandpass filter (magenta). Error bars indicate the standard deviation in the measurements. The solid curves indicate $V_0 \cos \alpha$ fits to these data.

detect coincidences between output modes m and n to scale as $(1 + \cos \alpha)$. For instance, setting $\alpha = 0$ in the patterns on the SLM would double the rate of coincidences compared to the rate obtained for distinguishable photons. This corresponds to a peak instead of a dip in the measured coincidences as shown in Fig. 5.3. Although the case with $\alpha = 0$ can not be realized in a conventional beam splitter, we show a flipped trace of the measured HOM dip with a conventional beam splitter as a guide to the eye. Note that the probabilities for bunched photons in the outputs is independent of α , as is evident from Eq. (5.3), which makes the output state different from the states typically found when recombining the two outputs from a traditional HOM experiment in a Mach-Zehnder type interferometer [114–116].

Fully programmable quantum interference is demonstrated in our complex scattering medium in Fig. 5.4. Here the visibility of the quantum interference V is plotted as a function of phase α . Negative visibility corresponds to a dip in the coincidence counts and positive visibility to a peak. At $\alpha = 0$ a coincidence peak is observed. The visibility of this peak vanishes at phase $\alpha = \pi/2$, after which the visibility increases again as a coincidence dip. The well-known HOM dip with a high visibility occurs at phase $\alpha = \pi$. Also indicated are $V_0 \cos \alpha$ fits to these data with the prefactor V_0 as the only free parameter.

5.5 Discussion

For the measurements at a pump power of 100 mW the average coincidence detection rate is only 1240 h^{-1} , corresponding to a single photon detection rate of 2500 s^{-1} . This detection rate is small in comparison to the generation rate of $17 \times 10^6 \text{ s}^{-1}$ as a result of our choice to be deep in the multiple-scattering regime. In this way, we approach the assumption of maximal entropy of the matrix in random-matrix theory [27]. Multimode fibres that were recently exploited for two-photon quantum interference [57], do not provide such a high entropy, since the transmission matrix of a multimode fibre can be transformed into a block-diagonal matrix by a suitable basis [117, 118]. We note that having maximal entropy is essential for the application of a scattering medium in quantum-secure authentication [46], which requires a physical unclonable function with a transmission matrix that cannot predictably be approximated by a near-diagonal matrix [119].

In summary, we demonstrate two-photon quantum interference in a high-dimensional linear optical network realized in an opaque scattering medium. Our networks are ideal for quantum information processing [6, 7] and boson sampling [13–21]. Excitingly, adaptive control adds programmable functionality to these networks [4, 5]. Out of the available channels, we control about 10^3 channels to form a programmable 2×2 circuit. In the selected channels, we increase the coincidence detection rates by a factor of 10^4 via shaping of the wavefronts of single-photon pairs. We demonstrate that by programming the functionality of this circuit, the well-known Hong-Ou-Mandel bunching can be made to vanish, or be transformed into antibunching.

6 Quantum-secure communication

In this chapter, we apply the principles of quantum-secure authentication to quantum key distribution to create an authenticated quantum key distribution protocol, removing the need of an initial shared secret for authentication. Excitingly, this protocol is turned into an asymmetric quantum-secure communication method.

6.1 Quantum-secure authentication

Recently, quantum-secure authentication (QSA) has been demonstrated as a secure means of authentication of persons or objects [46, 120, 121]. At the basis of QSA lies an optical physical unclonable function (PUF) [119, 122], which acts as a physical key. A PUF is a physical object that cannot be cloned feasibly, due to a large number of degrees of freedom that cannot be controlled during fabrication. A PUF is called a function, since when given a challenge (stimulus) the PUF replies with a response. The transformation from challenge to response is unique for the specific PUF. Therefore, by probing the PUF, one can verify its authenticity. By reading out the PUF using quantum states one becomes resistant against digital emulation of the key [121], as well as quantum state estimation attacks [120].

In the recent experimental demonstration of QSA, the physical unclonable function, or key, consists of an opaque scattering medium [46]. The entire function of the key, connecting all challenges and responses, is assumed to be publicly known. Thus QSA does not require the storage of secret information, and also allows for authentication of the key by everyone. The quantum-secure readout of this key is performed using weak coherent states of light. The wavefront of this light is modulated using a spatial light modulator to create a challenge wavefront that is sent to the key. The response of the key is transformed back to a plane wavefront using a second SLM, and then focused onto a detector. Only with the correct key a bright focus is obtained, leading to photodetections of the photons, which can be used to authenticate the key. With an incorrect key a random speckle pattern is observed at the detector plane, which does not result in a significant number of photodetections.

The security of QSA can be captured in the quantum security parameter S , which is defined as the ratio of the number of controlled modes N and the average photon number n in the challenge wavefront:

$$S \equiv \frac{N}{n}. \quad (6.1)$$

A quantum-secure readout is obtained by ensuring that $S > 1$, such that even a measurement of all n photons cannot reveal information about all N modes,

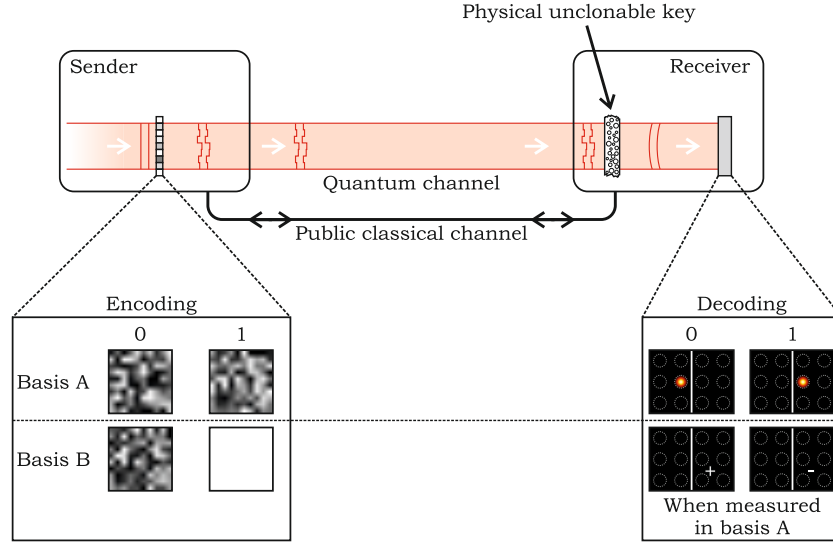


Figure 6.1 Scheme for authenticated quantum key distribution. The sender encodes bits in a high-dimensional wavefront of photons, which are transmitted over a quantum channel to the receiver. After transmission through a physical unclonable key the photons focus to a spot, which can be efficiently detected. The sent bit can be decoded using the location of the focused spot. A second basis for encoding is constructed by superposition. At the receiver photons encoded in the second basis form two spots, whose phase difference is used for encoding. The receiver measures response wavefronts in a random basis. After comparing the choices of bases of the sender and receiver over a two-way public classical channel a shared key is established between the sender and receiver. The presence of the physical unclonable key authenticates the receiver.

but only about n of them [46]. A large, but finite, number of orthogonal challenge wavefronts is available to readout the key. For authentication one has to use arbitrary superpositions of these orthogonal challenge wavefronts. If one would only use the orthogonal challenges, it would be easier for an adversary to recognize which challenge is sent, due to their finite number, and to construct an appropriate response.

6.2 Authenticated quantum key distribution

We combine the ideas behind quantum-secure authentication with quantum key distribution. We incorporate a physical unclonable function, of which the prop-

erties are publicly known, as key in the quantum channel to authenticate the receiver during the transmission, see Fig. 6.1. As in the BB84 protocol, the sender sends out bits in random bases. But instead of using a polarization basis, a high-dimensional spatial wavefront, with dimension N , is used. The bits are encoded in a wavefront using a spatial light modulator, see Fig. 6.1.

At the receiver, the wavefronts are incident on a physical unclonable key, which responds with a different wavefront. The sent wavefronts are chosen such that the response on the receiver's side is in the form of a focused spot, which can be efficiently detected. The responses are grouped into two sets, corresponding to the symbols 0 and 1. For encoding of each of the symbols, a large number of orthogonal wavefronts, which result in focused spots, is available. One half of the focused spots is chosen to correspond to 0, and the other half to 1. The distinction between 0 and 1 can for instance be made as the separation between the left and right half of the detector area, as indicated in Fig. 6.1.

The receiver measures the response wavefronts, consisting of focused spots, in two mutually unbiased bases. The representation of 0 and 1 discussed above constitutes the first basis (basis A) for quantum key distribution. The second basis (basis B) for quantum key distribution to send the symbols in is constructed in a similar way as in the BB84 protocol. Basis B can be constructed by superposition of two wavefronts of basis A on the sender's side, of which one corresponds to symbol 0 and the other to symbol 1. In basis B, the symbols 0 and 1 are encoded in the relative sign used in the creation of the superposition of the two wavefronts. At the receiver, wavefronts sent in basis B will not focus to a single spot, when measured in basis A. Instead, two spots will be formed. The relative phase between these spots is determined by the sign used in the creation of the superposition. Thus, an interferometric measurement of this phase, a measurement in basis B, reveals the sent symbol. For symbols encoded in basis B (sign used in the superposition), a measurement in basis A (location on the detector) will give a random result, providing no information about the sent symbol. Similarly, encoding in basis A and measuring in basis B leads to random results.

In the authenticated QKD protocol, the receiver measures response wavefronts in a randomly chosen basis. After comparing the choices of bases of the sender and receiver over a two-way public classical channel a shared key is established between the sender and receiver. Only a receiver who is in possession of the correct physical unclonable key can efficiently decode the bits sent.

To intercept the sent bits, an eavesdropper who does not possess the physical unclonable key first has to measure the photons from the sender in the correct basis, which she does with 50% probability. Secondly, the eavesdropper, even in possession of all information about the PUF challenge-response pairs, has to recognize the sent N -dimensional wavefront, which we expect her to be able to do with an efficiency of at most $1/N$. The probability for correct decoding of a sent bit by an eavesdropper is therefore $1/(2N)$. In contrast, the receiver can decode a sent bit using the physical unclonable key with a much larger efficiency, namely when he chooses the correct basis, with 50% probability. There-

fore, separate authentication of the receiver is not necessary. To be unnoticed after measuring the sent bits, an eavesdropper has to send new encoded bits to the receiver. Here, in contrast to the BB84 protocol, an eavesdropper will not only introduce errors when she has chosen the wrong basis for measurement, but also when the correct basis was chosen. She will introduce an error rate of $1/2 - 1/(4N)$, which approaches 50% for large N , that will easily be noticed. Note that the authenticated QKD protocol presented here, although it employs high-dimensional wavefronts, is distinct from high-dimensional quantum key distribution [123, 124], where a high dimensionality is used to increase the security and information content of a QKD protocol by increasing the number of bases and symbols used. In high-dimensional QKD the problem of authentication of the receiver persists.

While a security proof of this protocol for authenticated quantum key distribution is still outstanding, it is expected to be similar to the proof for quantum-secure authentication. An important difference with QSA is that whereas in QSA an adversary needs to recognize the exact wavefront that has been sent to determine an appropriate response, in the current authenticated quantum key distribution scheme it would be in principle sufficient to recognize the set the wavefront belongs to: symbol 0 or 1. We expect, and this is ongoing work, that the security can still be captured in the form of a quantum security parameter, requiring a larger number of controlled modes than the number of photons for a quantum-secure system. Note that a possible security breach of the quantum channel does not mean that an adversary instantly has access to the transmitted keys, since a QKD protocol already offers security on its own, by the random choices of basis. By breaking the authentication, the authenticated QKD protocol reverts back to standard QKD, and becomes again vulnerable to a man-in-the-middle attack on the public classical channel.

6.3 Experimental setup

The setup for the authenticated quantum key distribution experiments is shown in Fig. 6.2. The light source consists of a spontaneous parametric down-conversion source, which generates pairs of single photons (see chapter 3). One of the photons is used as a herald, while the other photon is directed to the setup for authenticated quantum key distribution. There the wavefront of the photon is phase modulated with a liquid-crystal SLM by the sender. Next the light is sent to the receiver in a fixed linear polarization. At the receiver an objective (NA=0.95) is used to focus the light onto the scattering medium which comprises an approximately $12\text{ }\mu\text{m}$ thick layer of zinc oxide (ZnO), with a scattering mean free path of $0.7 \pm 0.2\text{ }\mu\text{m}$. The total number of contributing modes (speckles) is approximately 10^4 . The transmitted light is collected by an objective (NA=0.85) and, after decomposition into its two linear polarization components by a polarizing beam splitter, imaged on two multimode fibres connected to single-photon

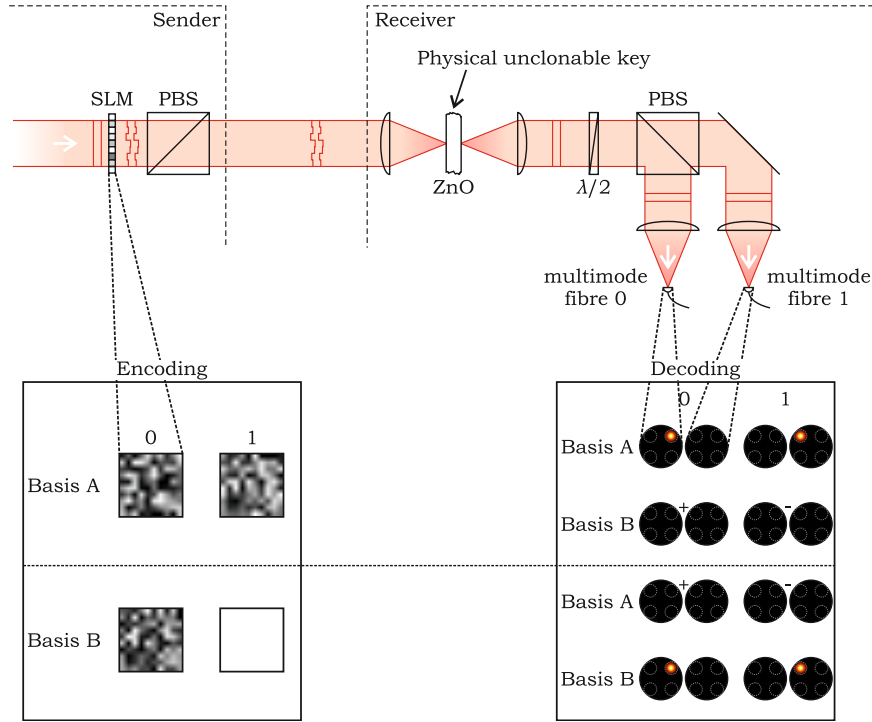


Figure 6.2 Setup for authenticated quantum key distribution. Linearly-polarized light is modulated with a SLM by the sender, and transferred to the receiver. There, the light is focused on a physical unclonable key consisting of a layer of ZnO. The transmitted light is decomposed into its two linear polarization components, corresponding to symbols 0 and 1, by a PBS and imaged on two multimode fibres connected to SPCMs. The encoded wavefronts are transformed by the physical unclonable key into focused spots on the facets of the multimode fibres. By rotating a half-wave plate the receiver can select the basis for detection of the light.

counting modules. One polarization component is associated with symbol 0, and the other component with symbol 1. Here, the separation into two polarization components is equivalent to the spatial separation into a left and right half as shown in Fig. 6.1. The fibres have a core diameter of $50 \mu\text{m}$, such that light from approximately 550 wavefront-shaped spots can be collected. By rotating a half-wave plate, the receiver can select the basis for detection of the light. Not shown in the figure are CCD cameras in the same plane as the input facets of the fibres, which are used for wavefront shaping.

Creation of the required wavefronts follows a wavefront-shaping process. To

ease this process, we couple classical laser light into the setup along the exact same modes, and monitor the light at the positions of the two output fibres using CCD cameras. We optimize the intensity in a focus on the fibre facet by fitting the optimal phase for each SLM segment that results in maximum constructive interference [29]. For each polarization in the transmitted light, 3600 different optimized foci are constructed, resulting in 7200 wavefronts. The incident light is controlled by approximately 960 segments on the SLM. After optimizing, the intensity of the enhanced focus coupled to the fibre is about 200 times higher.

6.4 Results on authenticated quantum key distribution

To characterize the setup for authenticated quantum key distribution, the signal on the detectors of the receiver has been measured for each of the 7200 distinct wavefronts available to the sender. The incident photon rate for these measurements was approximately $2 \times 10^5 \text{ s}^{-1}$. The integration time for each measurement was 0.1 s, in which approximately 2×10^4 photons have been sent. Figure 6.3(a) shows the signal on the SPCM corresponding to symbol 0 when a 0 was sent (correct detection), for the wavefronts located around the centre of the fibre. Each small dot represents a different wavefront corresponding to a different focus on the fibre. The colour of the dots indicates the measured count rate on the single-photon counting module (SPCM). The bright spot in the centre of the figure corresponds to wavefronts which couple decently into the fibre. Simultaneously, Fig. 6.3(b) shows the signal on the SPCM for symbol 1, when a symbol 0 was sent (wrong detection). No clear signal is visible above the background. The results for sending a symbol 1 are shown in Fig. 6.3(c)-(d), and show similar behaviour. On average, the signal on a detector for a correct detection is about 1.5 times higher than the signal for a wrong detection. This shows that we can easily detect the sent symbol by assigning it to the detector that has the highest signal.

The representation of 0 and 1 in Fig. 6.3 constitutes the first basis (basis A) for quantum key distribution. The wavefronts required for sending in the second basis (basis B) on the sender's side can be constructed by a superposition of two wavefronts of basis A, of which one corresponds to symbol 0 and the other to symbol 1. On the receiving side this is implemented by inserting a half-wave plate at 22.5° (see Fig. 6.2), transforming the horizontal-vertical polarization basis of basis A to a diagonal-antidiagonal polarization basis for basis B.

Figure 6.4 shows results of a proof-of-principle experiment of authenticated quantum key distribution. The figure shows the signal on the two SPCMs of the receiver for all combinations of symbol 0, 1 and basis A, B on both the sender's and receiver's side. The different rows correspond to the four combinations of symbol 0, 1 and basis A, B of the sender. The columns represent detection of the signal of symbol 0, 1 in basis A, B. The top-left quarter of the image con-

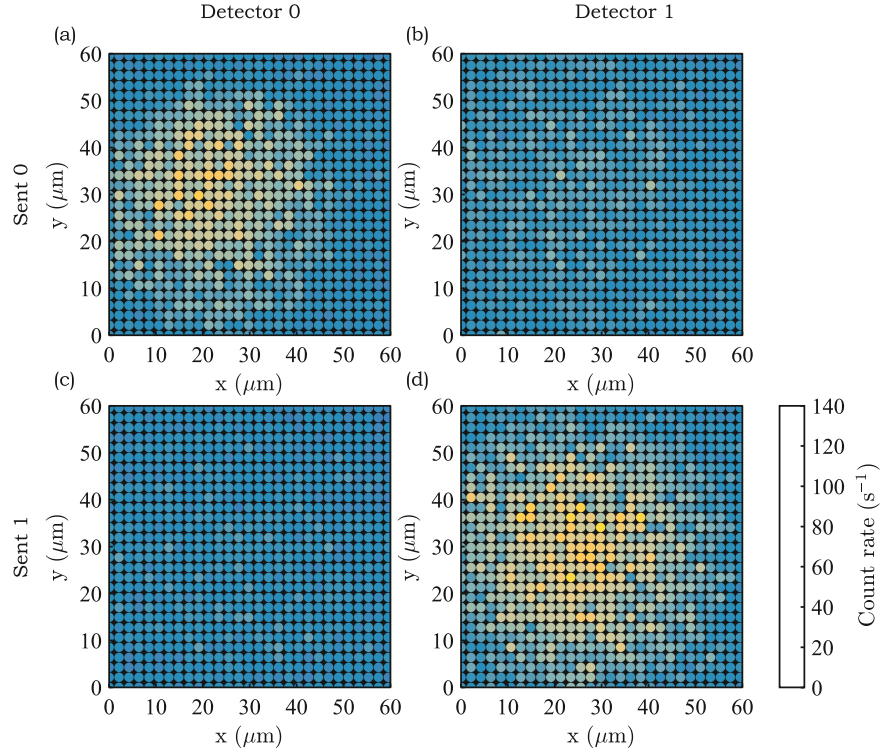


Figure 6.3 Count rates on the SPCMs of the receiver. (a) shows the counts on the SPCM corresponding to symbol 0 when a symbol 0 is sent. Each small dot represents a different wavefront corresponding to a different spot on the fibre. The colour of the dots represents the detected count rate. The incident photon rate is approximately $2 \times 10^5 \text{ s}^{-1}$. Each measurement is integrated for 0.1 s, in which approximately 2×10^4 photons are sent. The detector counts of the SPCM for symbol 1 for a sent symbol 0 are shown in (b). In (c) and (d) the detector counts are shown for SPCM 0 and 1, respectively, for a sent symbol 1.

tains similar data as Fig. 6.3. It shows that when sender and receiver use the same basis (top-left and bottom-right quadrants) the sent symbol can be clearly detected. When different bases are used by the sender and receiver, the signal is equally distributed over both detectors (top-right and bottom-left quadrants), not revealing any information about the symbol sent. For these measurements the wavefronts for basis B have not been constructed by superposition of wavefronts of basis A, as this requires the two multimode fibres for detection to be identically aligned. Since this was not the case in the experiment, a second

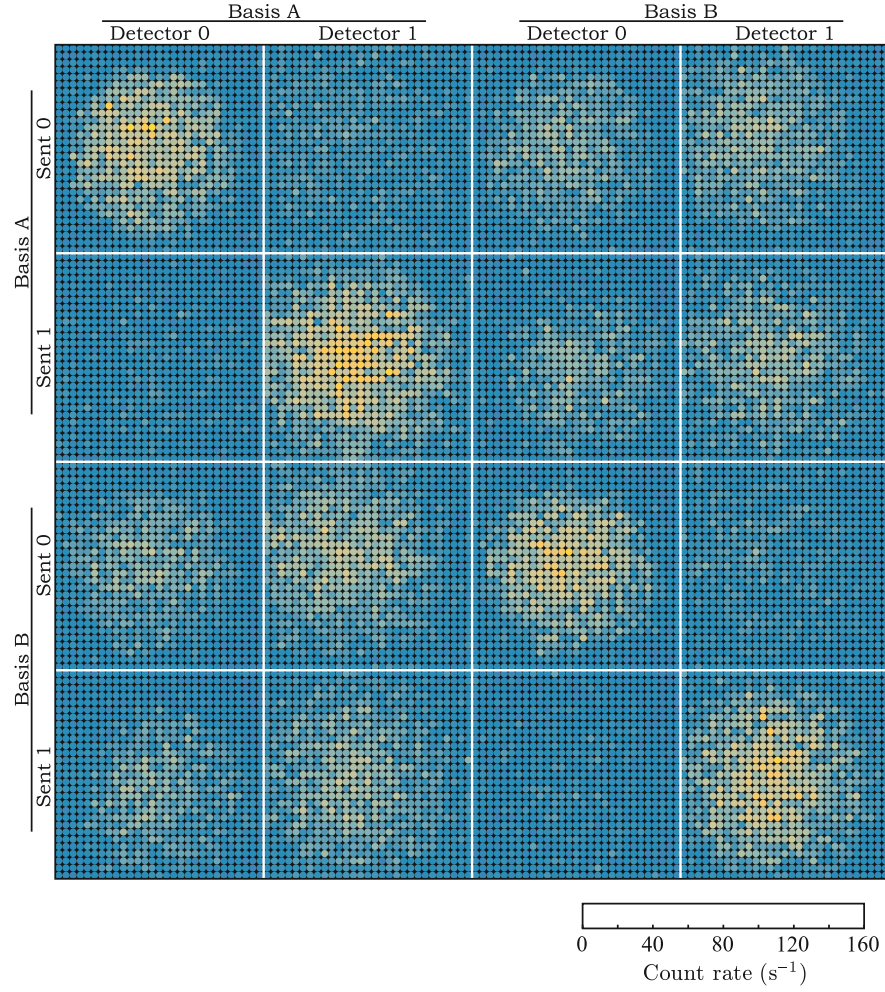


Figure 6.4 Count rates on the SPCMs of the receiver for all combinations of symbol and basis. Each small dot represents a different wavefront corresponding to a different spot on the fibre. The colour of the dots represents the detected count rate. The incident photon rate is approximately $2 \times 10^5 \text{ s}^{-1}$. Each measurement is integrated for 0.1 s, in which approximately 2×10^4 photons are sent. Different rows correspond to the four combinations of symbol 0, 1 and basis A, B of the sender. The columns represent the SPCM for symbol 0, 1 in basis A, B. The top-left quadrant of the image contains similar data as Fig. 6.3.

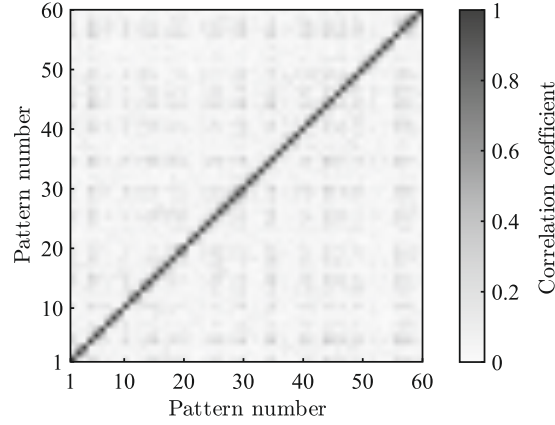


Figure 6.5 Absolute value of Pearson's linear correlation coefficients between the different wavefronts used to send symbol 0. Only the first 60 wavefronts are shown.

wavefront-shaping process was used to construct the wavefronts for basis B.

Since the contrast between correct and wrong detections is approximately 1.5, the receiver can detect the sent symbol by assigning it to the detector that has the highest signal. To check the performance of this method, we have transmitted a series of 20000 random bits in a randomly chosen basis, each with approximately 2×10^4 photons. Each bit was sent with a wavefront chosen randomly out of a set of approximately 300 that resulted in a contrast greater than 1.4. For the bits where the sender and receiver used the same basis, 99.5% of the bits were detected correctly. When different bases were used for sending and receiving, 55% of the bits were detected correctly, which approaches the probability of 50% expected for mutually unbiased bases of dimension two. The small deviation can be explained by a difference in efficiencies of the SPCMs.

The wavefronts used by the sender that encode a single symbol should not be similar. Otherwise, it is an easy task for an eavesdropper to recognize which symbol is sent. To check the similarity of the wavefronts used in the experiment, we have correlated all wavefronts with each other. Figure 6.5 shows the absolute value of Pearson's linear correlation coefficient of $\exp(i\theta)$, where θ represents each phase pattern on the SLM. Only the first 60 wavefronts for symbol 0 are shown here. The diagonal elements equal 1, since these represent the correlation of a wavefront with itself. The average correlation of the off-diagonal elements is 4%. The average correlation for two random wavefronts with the same number of segments as used in the experiment would be 3%, indicating that there is nearly no similarity between the wavefronts used.

The measurements shown so far have been done using a rather high incident

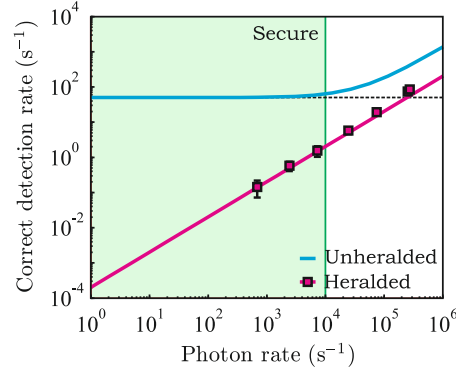


Figure 6.6 Measured count rates at the SPCM corresponding to the sent symbol (correct detection) as a function of incident single-photon rate (magenta squares). Error bars indicate the standard deviation in the measurements. Only wavefronts that, at high photon rates, result in a contrast between correct and wrong detection of 1.5 have been used. Also shown are the expected count rates for heralded detection (magenta curve), unheralded detection (cyan curve), and the SPCM dark count rate of 50 s^{-1} (dashed line). Approximately 960 segments on the SLM have been controlled. The quantum-secure region with $S > 1$ is indicated (green area).

single-photon rate of $2 \times 10^5 \text{ s}^{-1}$. The integration time for each measurement was 0.1 s , in which $n \approx 2 \times 10^4$ photons have been sent. Since $N \approx 960$ segments on the SLM have been controlled, the quantum security parameter for these measurements is $S \approx 0.05$, cf. Eq (6.1). To reach a quantum-secure system, with $S > 1$, this number of photons must be reduced. Figure 6.6 shows the measured detection rate at the detector corresponding to the correct symbol as a function of the incident photon rate. The results are averaged over multiple wavefronts that, at high photon rates, result in a contrast between correct and wrong detection of 1.5. Also shown is the expected detection rate for a heralded detection, based on the efficiency of the setup, the heralding efficiency and dark counts of the detectors. As expected, the detection rate decreases linearly with the incident photon rate. In case one would not use a heralded detection, the dark counts of the SPCMs, 50 s^{-1} in this experiment, limit going to low photon rates. The latter is of central importance here because the secure regime with $S > 1$ is reached at low photon rates, below 10^4 s^{-1} .

While the detection rate decreases with decreasing incident photon rate, the probability for correct detection of a symbol is preserved, as is visible in Fig. 6.7. The graph shows the average probability for correct detection as a function of incident single-photon rate for a contrast between correct and wrong detection of 1.5 at high photon rates. The measured data match the expected constant be-

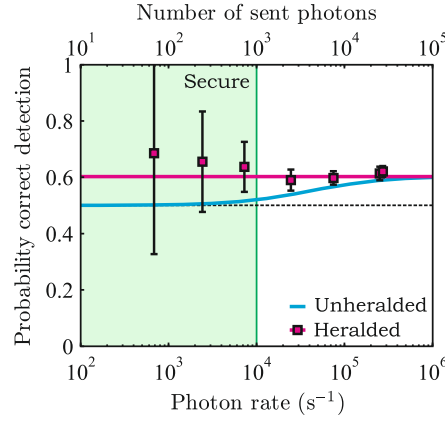


Figure 6.7 Measured probability of correct detection of a sent symbol as a function of incident single-photon rate (magenta squares). Error bars indicate the standard deviation in the measurements. Only wavefronts that, at high photon rates, result in a contrast between correct and wrong detection of 1.5 have been used. Also shown are the expected probability of correct detection for heralded detection (magenta curve) and unheralded detection (cyan curve). Approximately 960 segments on the SLM have been controlled. The quantum-secure region with $S > 1$ is indicated (green area).

haviour. For unheralded detection the probability for correct detection decreases to 50% at low pump powers, where the detector dark counts dominate.

As visible in Fig. 6.6, the detection probability of a sent photon at the correct detector is on the order of 10^{-4} . This can be broken down in (1) the fraction of input light that is transmitted through the scattering medium of 10%, (2) optical losses in the setup of 90%, (3) a probability for correct detection of 60%, and (4) a heralded photon detection efficiency of 5%. The optical losses in the setup and detector efficiency are specific to the current implementation of the setup, and can be reduced, increasing the detection probability by two orders of magnitude. Furthermore, by increasing the number of control parameters in the sent wavefront, i.e., the number of segments used for wavefront shaping, the contrast between correct and wrong detection can possibly be increased, resulting in an even higher probability for correct detection of the photons. We expect that, ultimately, the limit on the throughput of the setup will be set by the transmission of the scattering medium, on the 10-percent level.

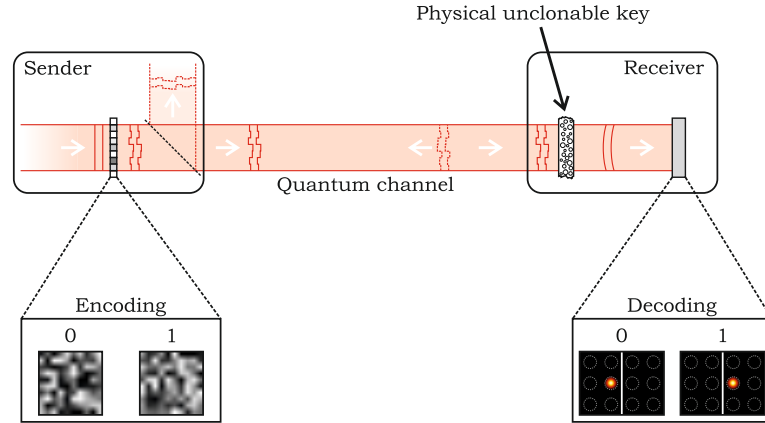


Figure 6.8 Scheme for PUF-enabled asymmetric quantum communication. The sender encodes bits in a high-dimensional wavefront of photons, which are transmitted over a quantum channel to the receiver. After transmission through a physical unclonable key the photons focus to a spot, which can be efficiently detected. The sent bit can be decoded using the location of the focused spot. The message is directly contained within the sent wavefronts, and does not require the existence of a classical channel between sender and receiver. The presence of the physical unclonable key authenticates the receiver. Optionally, the sender can record the response of the physical unclonable key on his side, to simultaneously confirm the authentication and presence of the receiver.

6.5 PUF-enabled asymmetric quantum communication

In the previous section, we demonstrated how to combine the ideas behind quantum-secure authentication with quantum key distribution to construct an authenticated QKD protocol. The security of this protocol is based on the quantum-secure readout of a physical unclonable key, for which a breach of security is not expected to be possible. However, after a security breach the QKD system would again be vulnerable to a man-in-the-middle attack on the public classical channel, rendering it insecure. For this reason, in the current authenticated QKD scheme, the random choices of basis do not add significantly to the security, and can be left out. In the case that no random choices of basis are used, also the public classical channel is not required any more. Removal of the need of a public classical channel opens an exciting new possibility for quantum-secure communication in an asymmetric fashion.

Here, we introduce PUF-enabled asymmetric quantum communication (PEAQC). PEAQC is an asymmetric method that allows for the secure transmission of messages (not limited to keys) over a quantum channel, which can only be read by an authenticated receiver. A major advantage of this communication method is that it is asymmetric, which can be seen as follows: since the properties of the physical unclonable key are publicly known, anyone can send messages which only the designated receiver, in possession of the key, can decode. No two-way communication channel is required. To the best of our knowledge, no asymmetric quantum communication protocol currently exists.

PEAQC is explained in Fig. 6.8. We incorporate a physical unclonable function, of which the properties are publicly known, as key in the quantum channel to authenticate the receiver during the transmission, see Fig. 6.8. The sender directly transmits a message. The bits are encoded in a high-dimensional spatial wavefront, with dimension N , using a spatial light modulator.

At the receiver, the wavefronts are incident on a physical unclonable key, which responds with a different wavefront. The receiver is capable, due to the PUF, to detect these response wavefronts, since the sent wavefronts are chosen such that the response on the receiver's side is in the form of a focused spot, which can be efficiently detected. The responses are grouped into two sets, corresponding to the symbols 0 and 1. For encoding of each of the symbols, a large number of orthogonal wavefronts, which result in focused spots, is available. One half of the focused spots is chosen to correspond to 0, and the other half to 1. A possible distinction between 0 and 1 could be made as indicated in Fig. 6.8, by distinguishing between the left and right half of the detector area. The sent bits can only be efficiently decoded by a receiver who is in possession of the correct physical unclonable key.

Optionally, the method allows for separate authentication of the receiver by the sender, by employing QSA on the response wavefront on the sender's side. In this way also the reception of a message can easily be verified by the sender.

To decode the sent bits, an eavesdropper, without the physical unclonable key, has to recognize the sent N -dimensional wavefront, which we expect her to be able to do with an efficiency of at most $1/N$. In contrast, the receiver can perfectly decode a sent bit using the physical unclonable key. Therefore, separate authentication of the receiver is not necessary. A receiver of the message is inherently authenticated. Note that, by abolishing the random choices of basis, the probability for correct decoding of a sent bit by an eavesdropper did not change significantly, from $1/(2N)$ for authenticated QKD to $1/N$ for PEAQC. Just as for authenticated quantum key distribution, a security proof of PUF-enabled asymmetric quantum communication is still outstanding, and expected to be similar to the proof for quantum-secure authentication.

6.6 Results on PUF-enabled asymmetric quantum communication

Note that an experimental implementation of PEAQC is almost identical to that of authenticated quantum key distribution in the previous section. The only difference is that no random choices of basis are needed. Therefore, the results of experiments on authenticated quantum key distribution (section 6.4) can be directly used for a demonstration of PEAQC. Only basis A, for which results are shown in Fig. 6.3, is used. The measurements of the previous section directly demonstrate that, for a message sent using PEAQC in the setup of Fig. 6.2, 99.5% of the bits are detected correctly. Because PEAQC does not employ a two-way classical channel, the remaining 0.5% erroneous bits cannot simply be ignored. These bits contain a part of the sent message and have to be corrected, which can for example be done using a low-density parity-check (LDPC) code [125].

PEAQC is a communication protocol, not a method for key distribution. Its method of operation can thus be directly demonstrated by the communication of a message. This is shown in Fig. 6.8. First, a 39-symbol plain-text message is converted to a bit string of 273 bits using ASCII encoding. Subsequently, this bit string is encoded onto randomly chosen wavefronts of multiple single photons by the SLM of the sender, that are sent to the receiver. Each bit is sent with a wavefront (with $N \approx 960$ segments) chosen randomly out of a set of approximately 300 that results in a contrast greater than 1.4. The single-photon rate in this experiment is $2 \times 10^5 \text{ s}^{-1}$ and the integration time per bit is 0.1 s, such that per bit $n \approx 2 \times 10^4$ photons are transmitted. For these measurements the quantum security parameter S is approximately 0.05, which does not yet fall in the quantum-secure regime. At the receiver, the photons are incident on the physical unclonable key, and its response is measured. Fig. 6.8(a) shows the measured count rate at the receiver for each sent bit. Indicated are the signals at detector 0 and detector 1. The histogram shows the occurrence of the detected count rates, indicating the contrast in count rates between the detectors. To retrieve the transmitted bit string, the value of each bit is assigned to the detector with the highest signal. The resulting bit string is shown in Fig. 6.8(b). It can be seen that this received bit string is identical to the sent bit string, which is also shown in the figure. Finally, ASCII decoding is used to exactly retrieve the sent message: “Ravi, what kind of cake would you like?” This result shows that messages are transmitted successfully using PEAQC. By decreasing the number of photons sent per bit by one order of magnitude (cf. Fig. 6.7), the method becomes quantum secure.

6.7 Discussion

In this chapter we have shown an authenticated quantum key distribution protocol. More importantly, we have introduced a novel protocol for authenticated

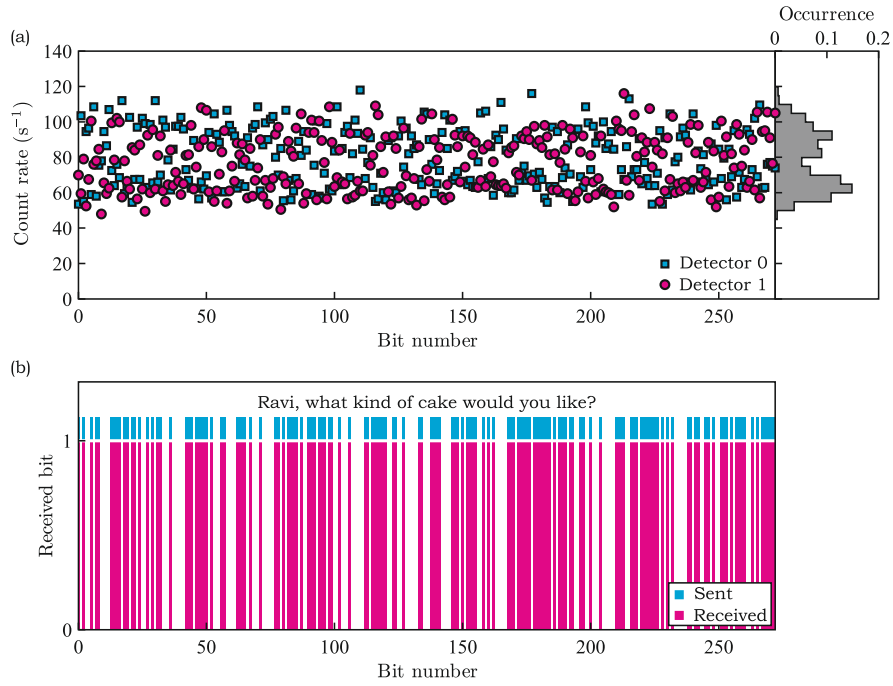


Figure 6.9 Received message transmitted using PEAQC, with approximately 2×10^4 photons per bit. An ASCII-encoded message was sent as a bit string. (a) Count rates on detector 0 (cyan) and 1 (magenta). The histogram shows the occurrence of the detected count rates. (b) Bit string received by comparing the count rates at detectors 0 and 1. The received bit string can be decoded to retrieve the message: “Ravi, what kind of cake would you like?”

and asymmetric quantum communication and have shown first results. The security of both of these protocols is based on the quantum-secure readout of a physical unclonable function [46, 120, 121]. Although a rigorous theoretical proof of security for these specific applications of quantum-secure readout of PUFs still remains to be shown, we expect that the quantum security parameter S , defined as the ratio of the number of controlled modes over the number of photons, acts as the key parameter. In case that a sufficient requirement for security is indeed $S > 1$, our implementations of authenticated quantum key distribution and PUF-enabled asymmetric quantum communication are secure.

Focusing on transferring authenticated quantum key distribution and PUF-enabled asymmetric quantum communication from proof-of-principle demonstrations, as presented in this chapter, to real-world applications, several modifications and improvements are available. While in the current experiments single-photon states have been used, these are not strictly required. A simplified, though still secure, implementation could employ weak coherent states, as used in the recent demonstration of quantum-secure authentication [46]. To vastly increase the bit rate of the transmission a digital micromirror-based SLM can be used. At the moment only a single bit of information is encoded in the photons. To increase the information content per photon, the protocols for authenticated quantum key distribution and PUF-enabled asymmetric quantum communication can be straightforwardly extended to a larger alphabet. As a large alphabet requires detection of a high number of symbols, the use of an intensified CCD camera instead of multiple single-pixel single-photon counting modules would be more attractive.

7 Control of light propagation in integrated optical networks

7.1 Introduction

In the previous chapters of this thesis we have used wavefront shaping to achieve control over the propagation of light through opaque scattering media. Here, an alternate scattering platform is studied, consisting of an array of thousands of weakly coupled waveguides in integrated optics. Due to the high throughput of integrated optics, compared to opaque scattering media, it is an attractive platform to program quantum interference between a large number of modes in these massively multichannel networks. To our knowledge, large arrays containing thousands of waveguides, creating massively multichannel systems, have not yet been investigated. Scattering of light in coupled waveguide arrays has been thoroughly studied, using a tight-binding approach as well as a Floquet-Bloch analysis [126–128]. A wide variety of optical phenomena has been observed, such as discrete diffraction [129–132], excitation of Bloch waves [133, 134], Bloch oscillations [135, 136], the optical Zeno effect [137, 138], and transverse localization [139, 140], as well as phenomena based on nonlinear optical effects, such as soliton formation [141, 142] and light bullets [143].

Planar integrated optics where light can propagate and scatter only in two dimensions, not necessarily restricted to coupled waveguide arrays, allows for monitoring of light in such structures from the third dimension (top or bottom). Furthermore, when studying integrated optical circuits, usually a well-defined geometry can be realized, periodic as well as random, with extremely high long-term stability. Monitoring light in such structures provides “literally” insight in light propagation and its modification by wavefront shaping, which is generally not straightforward in opaque scattering media. The results can be compared with wavefront shaping in opaque scattering media.

Arrays of coupled waveguides are also of great interest in the field of quantum optics. To date, quantum correlations [144, 145], Bloch oscillations [146, 147], quantum walks [14, 148–150], and Anderson localization [151–154] with quantum states have been observed in coupled waveguide arrays. Furthermore, coupled waveguide arrays allow to construct quantum simulators [9] and quantum logic gates [155]. Recently, quantum simulations of Majorana dynamics [10] and entangled state transfer [156] have been demonstrated in arrays of coupled waveguides.

Our focus is the realization of massively multichannel linear optical networks with programmable quantum correlations, again without requiring tuning of the network itself. The desired programmable functionality is achieved by adaptive modulation of the incident quantum states. In this chapter, as a first step, we em-

ploy wavefront shaping to achieve control over the propagation of light through an integrated optical array of coupled waveguides.

7.2 Model

The propagation of light through an array of weakly coupled waveguides can be described, for instance, using a set of coupled-mode equations. Assuming only nearest-neighbour interactions, the change of the complex electric field in waveguide m is given as [126, 127]

$$\frac{\partial E_m(z)}{\partial z} = i\beta E_m(z) + iC(E_{m-1}(z) + E_{m+1}(z)), \quad (7.1)$$

where $\beta = 2\pi n_{\text{eff}}/\lambda$ is the propagation constant of the waveguide, C is the coupling constant between neighbouring waveguides, and z is the propagation direction. This description is equivalent to the tight-binding model used in solid-state physics [157, 158]. For an infinite array of waveguides, these coupled-mode equations can be solved analytically. In the case of light with electric field amplitude A_0 incident in a single waveguide with index 0, and zero field in all other waveguides, i.e., $E_m(0) = A_0\delta_{m0}$, the electric field in waveguide m is given as

$$E_m(z) = A_0(i)^m \exp(i\beta z) J_m(2Cz), \quad (7.2)$$

where J_m is the Bessel function of the first kind of order m . The evolution of a light field with other initial conditions, such as with light incident at $z = 0$ in more than a single waveguide, can be obtained by superposition of Eq. (7.2) for all input waveguides. Figure 7.1(a) shows the propagation of light inside the coupled waveguide array, when a single centre waveguide is illuminated. Here, a finite array of 51 waveguides with a spacing of $3 \mu\text{m}$ is considered, with a propagation constant matching that of the waveguides used in the experiments in this chapter. The coupling constant is set at $C = 0.01\beta$, to clearly visualize the transfer of light between waveguides on the length scale displayed in the figure. Because in the figure an array containing a finite number of waveguides is displayed, the propagation is calculated by solving Eq. (7.1) numerically using a Runge-Kutta method. Since one is interested in the envelope of the electric field, the $i\beta E_m(z)$ term, which only gives rise to a rapidly varying phase $\exp(i\beta z)$, can be ignored. It can be seen in Fig. 7.1(a) that the light fans out in the transverse direction while propagating through the array. The highest intensity is found at the outer edges of the fan. Its opening angle is determined by the coupling constant of neighbouring waveguides. The intensity profile follows a Bessel function, as predicted by Eq. (7.2). Although the solution in Eq. (7.2) is strictly valid only for a infinite array of waveguides, it is still approximately valid here, since the light has not yet reached the sides of the waveguide array.

From Eq. (7.1), the diffraction relation, which is a dispersion relation, of an

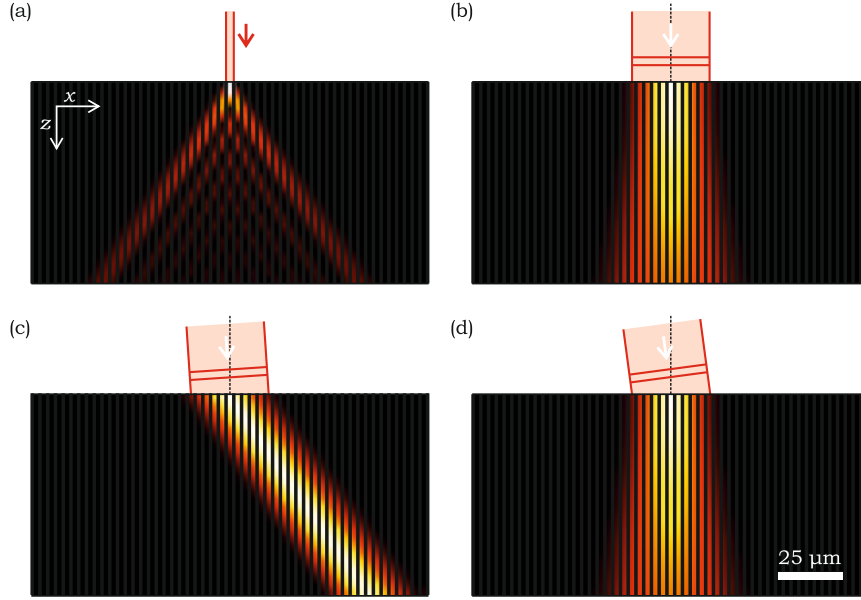


Figure 7.1 Calculated intensity distributions in a coupled array of 51 waveguides for various inputs at $z = 0$. (a) Light incident in a single waveguide. (b) A Gaussian beam incident with a $1/e^2$ -width of $30 \mu\text{m}$. (c) A Gaussian beam incident with a $1/e^2$ -width of $30 \mu\text{m}$ at an angle of 3.8° , corresponding to $k_x d = \pi/2$. (d) A Gaussian beam incident with a $1/e^2$ -width of $30 \mu\text{m}$ at an angle of 7.6° , corresponding to $k_x d = \pi$.

infinite array of coupled waveguides follows:

$$k_z = \beta + 2C \cos(k_x d), \quad (7.3)$$

where k_x and k_z are, respectively, the x and z components of the wave vector, and d is the spacing of the waveguides. Note that this dispersion relation is a one-dimensional tight-binding approximation [157, 158]. The diffraction relation is visualized in Fig. 7.2. It can be seen from the figure and Eq. (7.3), that a Brillouin zone exists for $-\pi < k_x d \leq \pi$. A coupled-mode theory approach only describes the first propagation band of the coupled waveguide array, for which the energy is concentrated inside the waveguides. The complete band structure of the coupled waveguide array, also considering modes where the energy is not necessarily concentrated inside the waveguides, would be obtained using a Floquet-Bloch analysis [133, 134]. However, this degree of detail is not further considered in the initial investigations.

The diffraction relation imposes a limit on the transverse velocity of light in the waveguide array, and thus a limit for the maximum angle of propaga-

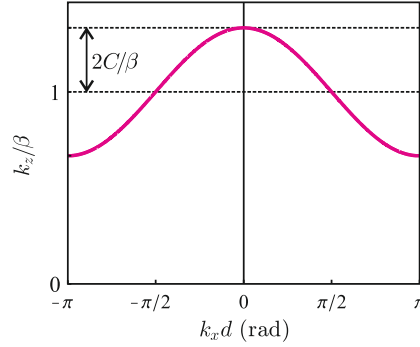


Figure 7.2 Diffraction relation for a coupled waveguide array. Higher order bands, where the energy is not necessarily concentrated inside the waveguides, have been omitted.

tion. The angle of propagation of light, $\theta = \arctan \frac{\partial k_z}{\partial k_x}$, reaches a maximum of $\theta_{\max} \approx 2Cd$ for $k_x d = \pi/2$. Also of interest is the divergence of the light $D = \frac{\partial^2 k_z}{\partial k_x^2}$, often called diffraction in this context, which changes sign, and even vanishes, at $k_x d = \pi/2$. These effects can be seen in Fig. 7.1(b)-(d). Figure 7.1(b) shows the propagation of a Gaussian beam of $30 \mu\text{m}$ $1/e^2$ -width incident at normal incidence, i.e., $k_x(0) = 0$. The beam diverges while propagating, and maintains its Gaussian shape. By changing the angle of incidence of the Gaussian beam at the input, the light refracts and propagates through the waveguide array at an angle. At an angle of incidence of 3.8° , corresponding to $k_x d = \pi/2$, the beam propagates at a maximum angle of $\theta_{\max} \approx 36^\circ$. The beam completely retains its shape and size (with a flat phase front), as the divergence D vanishes. This case is shown in Fig. 7.1(c). A further increase of the angle of incidence results in a decrease of the angle of propagation. At an angle of incidence of 7.6° , corresponding to $k_x d = \pi$, shown in Fig. 7.1(d), the beam again propagates straight through the waveguide array, as if it were injected at normal incidence. Indeed, the intensity distributions in Fig. 7.1(b) and Fig. 7.1(d) are identical. The difference in these cases is the sign of the divergence D , and therefore the curvature of the phase fronts: negative curvature in Fig. 7.1(b) and positive curvature in Fig. 7.1(d).

The spread of the light to mainly two outer lobes in Fig. 7.1(a) and the anomalous refraction and diffraction in Fig. 7.1(b)-(d) are examples that show that propagation of light in a coupled waveguide array, also called discrete diffraction, is radically different from diffraction in continuous media, such as free space. In the following sections, we will study how this discrete diffraction can be controlled by shaping the wavefront of the incident light.

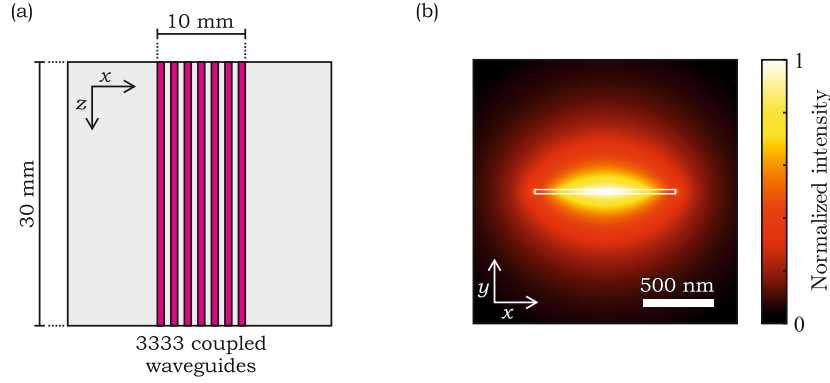


Figure 7.3 (a) Schematic drawing of the coupled waveguide array, consisting of 3333 weakly coupled waveguides with a length of 30 mm. (b) Calculated intensity distribution of the fundamental quasi-TE mode of a single waveguide for a wavelength of 790 nm. The silicon nitride core of the waveguide, with a width of $1\ \mu\text{m}$ and a height of 30 nm, is indicated.

7.3 Sample description

The specific coupled waveguide array considered in this chapter is shown in Fig. 7.3(a). The array consists of a 10 mm-wide section of silicon nitride waveguides at a spacing of $3\ \mu\text{m}$, thus forming an array of 3333 evanescently coupled waveguides. The length of the waveguides is 30 mm. Each single waveguide consists of a rectangular silicon nitride core (Si_3N_4), with a width of $1\ \mu\text{m}$ and a height of 30 nm, which is surrounded by a cladding of silica (SiO_2), with a thickness of $8\ \mu\text{m}$ on both top and bottom. At a wavelength of 790 nm, as used in the experiments, the refractive indices of the Si_3N_4 core and SiO_2 cladding are $n_{\text{core}} = 2.00$ and $n_{\text{clad}} = 1.45$, respectively. Waveguides of this type can support modes with different polarizations. By convention, the modes polarized mainly in the x direction are called quasi-TE polarized, and the modes polarized in the y direction quasi-TM polarized. The waveguides considered here support only a single, fundamental, mode in each of the two polarizations. Figure 7.3(b) shows the theoretical intensity distribution of the fundamental TE mode of the waveguide, which is the mode of interest in this work, for a wavelength of 790 nm. This distribution was numerically calculated by solving the electromagnetic modal vector wave equation using a finite-element method (COMSOL Multiphysics). The effective refractive index of this TE mode is $n_{\text{eff}} \approx 1.46$. In addition to this TE mode, the waveguide also supports a single TM mode, which is less confined than the TE mode. The TM mode, however, is not considered further because in the experiments we injected only TE polarized light.

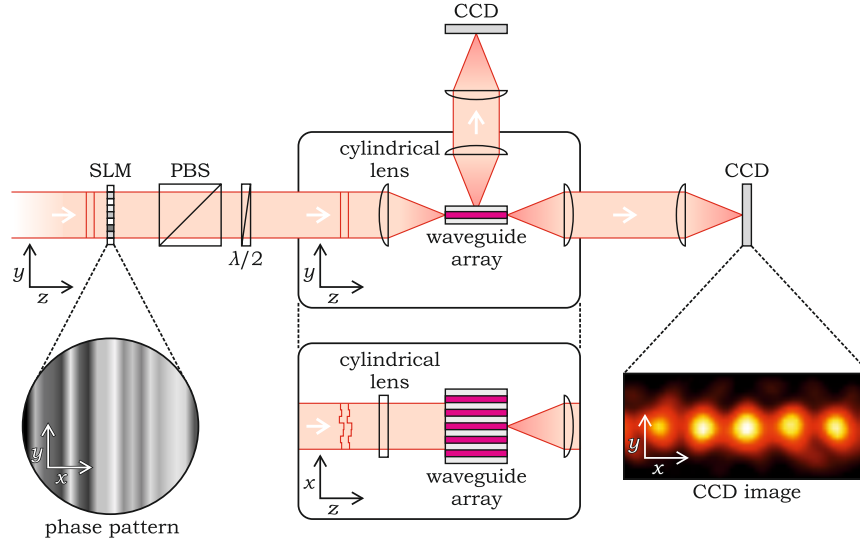


Figure 7.4 Setup for wavefront shaping on the coupled waveguide array. The input wavefronts are modulated with a SLM, and focused, in the y direction, on the input of the coupled waveguide array using a cylindrical lens. The SLM only modulates the wavefront in the x direction. The output facet of the coupled waveguide array, as well as out-of-plane scattering from waveguides, are imaged onto CCD cameras. The CCD image shows a part of the output facet. For experiments that require excitation of a single waveguide, the cylindrical lens is replaced by an aspheric lens.

7.4 Experimental setup

Figure 7.4 shows the setup for experiments on wavefront shaping in coupled waveguide arrays. As light source a Kerr-lens mode-locked Ti:Sapphire oscillator, which emits transform-limited sech^2 -pulses with a pulse duration of 1.83 ± 0.04 ps at a repetition rate of 76.0 MHz and a spectral width of 0.35 ± 0.05 nm centered around a wavelength of 790.0 nm, is used. The input wavefronts of the light are phase modulated (shaped) with a liquid-crystal spatial light modulator, and subsequently polarized such that only the TE mode of the coupled waveguide array becomes excited. Next, the light is focused in the y direction, on the input facet of the coupled silicon nitride waveguide array using a cylindrical lens ($f=11$ mm). The cylindrical lens creates a line focus that is used to couple light into approximately 1000 waveguides. For wavefront shaping, the SLM only needs to modulate the wavefront in the x direction. This is achieved

by combining pixels on the SLM into columnar segments. For experiments that require excitation of a single waveguide, an aspheric lens ($f=11$ mm) is used for focusing. Using an objective ($20\times$, $NA=0.4$), the output facet of the waveguide array is imaged on a CCD camera. This camera is also used for feedback during the wavefront-shaping processes. Simultaneously, the top surface of the coupled waveguide array is also imaged on a CCD camera with an objective ($40\times$, $NA=0.6$) to observe out-of-plane scattering from the waveguides. Both cameras are able to resolve light coming from single waveguides.

7.5 Results

To characterize the coupled waveguide array before the wavefront-shaping experiments, we first aimed on the observation of discrete diffraction of light in the array. For this purpose, we inject light into a single waveguide using an aspheric lens. Figure 7.5 shows the measured propagation of the light through the waveguide array, in comparison with calculations using Eq. (7.1). A camera image of the entire waveguide array taken from the top is shown in Fig. 7.5(a). The image contains 3333 waveguides, which is too many to resolve in the image. One can see that the light tunnels between the waveguides and fans out. From the opening angle of this fan, the coupling constant is determined to be $C \approx 0.001\beta$. A zoom-in at the location indicated by the arrow is shown in Fig. 7.5(b), revealing individual waveguides. This camera image shows oscillations in the distribution of the light in the transverse direction. The experimental data in Fig. 7.5(a), and the zoom-in in Fig. 7.5(b), can be compared with the calculated intensity distributions in Fig. 7.5(c)-(d). In the calculations, the coupling constant, the only free parameter, is set to $C = 0.001\beta$, as determined from the opening angle of the fan. The measured intensity in each waveguide at the output of the waveguide array is shown in Fig. 7.5(e). Shown is the intensity profile at the edge of the fan. At the input of the array, the light is incident in waveguide 0. The average intensity in each waveguide is obtained by integrating the intensity measured by a CCD camera over the area corresponding to each waveguide. Because the field of view of the objective is not sufficiently large to observe the entire waveguide array at once, the objective and camera are scanned to capture the entire waveguide array. Thereafter, multiple camera images have to be stitched together to construct a complete image. Figure 7.5(e) also shows the calculated intensity profile at the output. It can be seen that the experimental data agree qualitatively with the calculations for the outer three oscillations of the Bessel function. The remaining discrepancy can be caused by a imperfect alignment of the incident light beam, resulting in an excitation of multiple waveguides at the input of the coupled waveguide array, by nonuniform coupling constants between every waveguide, and by additional errors that might be introduced by stitching together multiple camera images. We have also studied the propagation of incident Gaussian beams at various different angles of incidence (not shown here), which matches

the prediction from calculations shown in Fig. 7.1.

Next, we demonstrate wavefront shaping in an array of coupled waveguides. The incident light is focused on the input facet of the waveguide array using a cylindrical lens. Approximately 1000 waveguides are illuminated with an approximately Gaussian intensity distribution in the x direction. Next, we observe the light output from a single, arbitrarily selected waveguide of the array using the CCD camera. We optimize this waveguide output by fitting the optimal phase for each SLM segment that results in maximum constructive interference in the area on the camera corresponding to this waveguide. The input wavefront is controlled by 400 columnar segments on the SLM.

The results are presented in Fig. 7.6. In this case we selected the target for the optimization as the waveguide output at $x = 0$. Shown is the intensity distribution of the central section of the waveguide array after optimizing the wavefront. Note that a logarithmic intensity scale is used, to be able to display the strongly varying intensities spanning three orders of magnitude. Every small peak in the curve with μm -size transverse extent corresponds to the centre of an individual waveguide of the array. Indeed, a high intensity is achieved in the target waveguide. The increase in intensity is clearly visible by comparing with the average intensity distribution for a random incident wavefront. The intensity in the enhanced target is about 640 times higher after optimization. Note that in the figure only a central section of the waveguide array is shown, covering about 150 waveguides, which corresponds to 4.5% of the full array. The large increase in intensity in this central section is accompanied by a decrease of intensity in the outer parts of the waveguide array. Another observation in Fig. 7.6 is that not only the intensity in the target waveguide is enhanced. Of the section of the coupled waveguide array displayed in Fig. 7.6, the intensity in the majority of the neighbouring waveguides increases as well by optimizing on a single waveguide. The most enhanced region is a section covering approximately 7 waveguides surrounding the target waveguide. This behaviour is notably different from wavefront shaping on opaque scattering media. We suspect that to achieve a full concentration of the light into a single waveguide, also amplitude control of the incident wavefront is required.

We find that the enhancement of the intensity in the target waveguide depends on the degree of control one has over the incident wavefront, and therefore on the number of control segments on the SLM that are used. In Fig. 7.7 we investigate this dependence. Shown is the enhancement in the target waveguide, defined as the ratio of the intensity in the target before optimization (with random wavefronts) and after optimization, as a function of the number of segments used on the SLM. The diameter of the incident beam is held constant. Thus, changing the number of controlled segments changes the number of waveguides that are addressed by each SLM segment. The figure shows that the enhancement increases by increasing the number of controlled segments. The scaling of enhancement with the number of segments is notably different from wavefront shaping in opaque scattering media, where a linear behaviour with slope

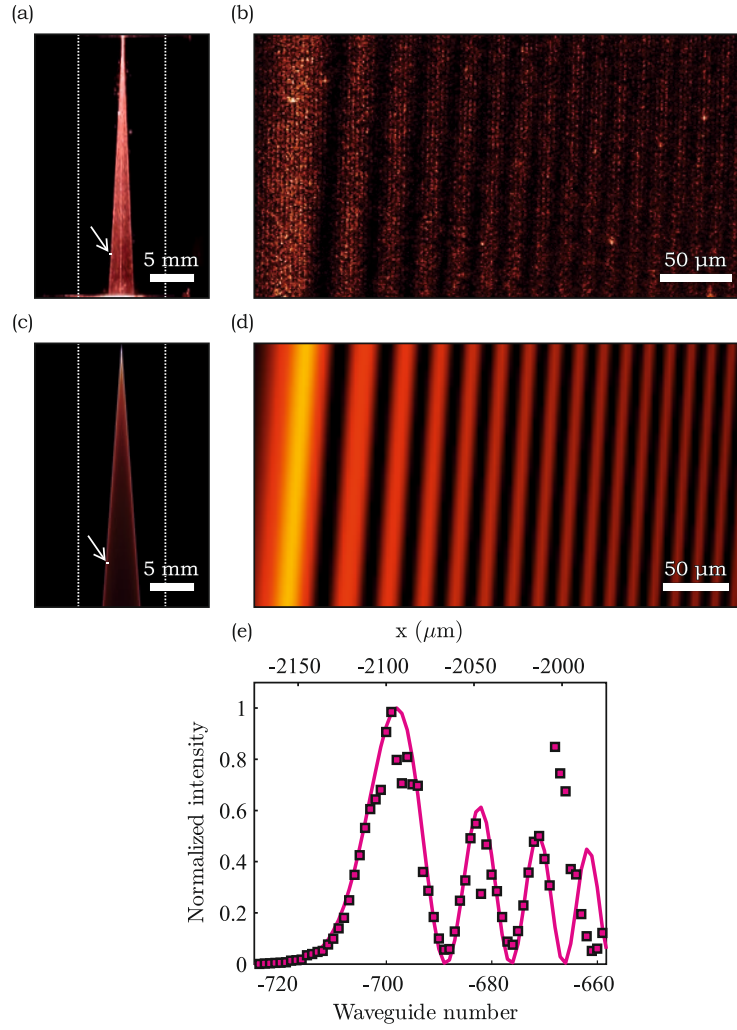


Figure 7.5 Evolution of light incident in a single waveguide. (a) Camera image of the top of the coupled waveguide array. A zoom-in at the location indicated by the arrow is shown in (b), revealing individual waveguides. The calculated intensity distribution in the coupled waveguide array is shown in (c), and a corresponding zoom-in in (d). (e) shows a part of the measured (magenta squares) and calculated (magenta curve) intensity at the output facet of the coupled waveguide array.

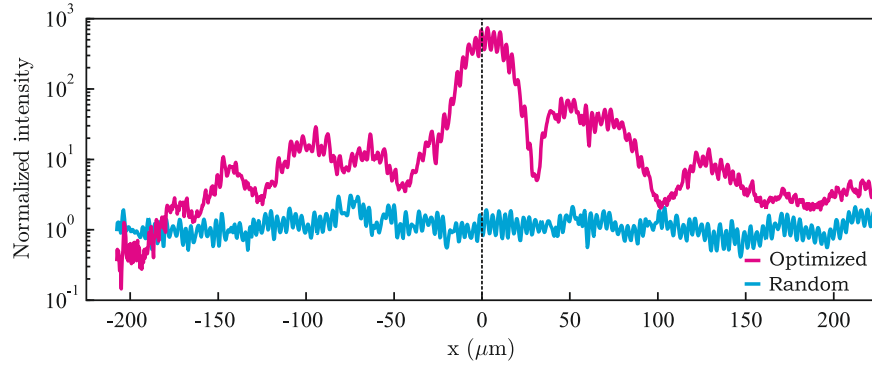


Figure 7.6 Intensity measured at the output facet in the central section of the coupled waveguide array. Every peak in the curves corresponds to the centre of an individual waveguide of the array. There are approximately 150 waveguides visible in this figure. At the input approximately 1000 waveguides are illuminated. The magenta curve shows the intensity distribution after wavefront shaping on a target waveguide at $x = 0$. The average intensity distribution for random wavefronts is indicated by the cyan curve. Note the logarithmic vertical axis.

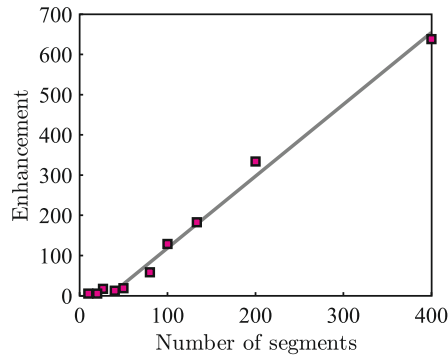


Figure 7.7 Enhancement of the intensity in the target waveguide (magenta squares) as a function of the number of segments used on the SLM. Also shown is a linear fit (grey curve) to the six rightmost data points, corresponding to optimizations using 50 or more segments.

$\pi/4 \approx 0.79$ is expected [29]. In the coupled waveguide array, the enhancement does not scale linearly with the number of segments. Surprisingly, when using more than 50 segments, the enhancement increases more rapidly, with a slope of approximately 1.8, than it would in opaque scattering media. More analysis is needed to understand the scaling of enhancement as a function of number of control segments in coupled waveguide arrays.

7.6 Discussion

We have demonstrated control over the propagation of light through an array of 3333 coupled integrated optical waveguides. By adaptive phase modulation of the incident wavefront, the light can be directed to a target waveguide, of which the intensity increased about 640 times, as compared to random wavefronts. Building on these first steps, it appears straightforward to construct, in the next step, arbitrarily programmable linear optical networks, using the algorithm presented in chapter 4. As a start, these networks can be used for two-photon quantum interference experiments similar to the experiments of chapter 5. As an important difference, due to the high throughput of integrated optics, theoretically close to 100% [159], it is realistic to program quantum interference between a large number of modes in these massively multichannel networks. Also studies of quantum interference between multiphoton Fock states should become accessible. In this way we realize massively multichannel linear optical networks with programmable quantum correlations, without tuning the network itself.

To fully understand the process of wavefront shaping in coupled waveguide arrays, more theoretical analysis is needed. For example, it is intriguing that, while directing the light to a single waveguide, the light settles into a section covering multiple waveguides. We suspect that this settling into multiple waveguides is due to the use of phase-only modulation of the incident wavefront, and can be resolved by adding amplitude control. This can be readily employed in the current experimental setup, where a cylindrical lens is used to inject the light into the waveguide array. While columnar segments, in the shape of columns, on the SLM are used to achieve phase control between adjacent waveguides, tabular segments, in the shape of rows, can be used for adjusting the focusing in the y direction. Since the coupling efficiency into the waveguide array critically depends on the focusing of the light, changing the focus effectively should enable an amplitude modulation of the light in the waveguide array.

Propagation of light through a coupled waveguide array significantly deviates from opaque scattering media. Nevertheless, integrated optical systems may give insight in the process of wavefront shaping, for instance on the distribution of energy inside the structure [160], that can be applied to opaque scattering media. Especially planar integrated optics are of interest since they allow for monitoring from the top, by, for example, out-of-plane scattering or via

a near-field scanning optical microscope. A structure of interest, because it can form an intermediate system between three-dimensional random scattering and two-dimensional periodic scattering, would be a highly multimode waveguide containing artificial scatterers, that might exhibit behaviour similar to an opaque scattering medium.

While coupled waveguide arrays themselves have been tailored to control the discrete diffraction for specific purposes [129, 132, 161, 162], it is an open question if a coupled waveguide array is the most suitable basis for creating programmable linear optical networks. In chapter 8 we will suggest a variety of other systems that should be investigated.

8 Outlook

8.1 Straightforward extensions

In this thesis, we have demonstrated programmable quantum interference between single photons in massively multichannel networks. Programmable quantum interference between a large number of modes in a massively multichannel network has the potential for large-scale quantum information processing. A next step, building on the current experiments on quantum interference in a programmable 2×2 network, is to study quantum correlations between more photons in larger networks. One could extend the number of channels in this network and study the quantum interference of single photons in a large number of modes. Furthermore, one could study interference between more than two photons, for which different approaches can be followed. The first approach is to study the interference of multiple, i.e., three, four, or perhaps even more, single photons. Alternatively, interference of multiple multiphoton states in a programmable network is of interest, for instance interference of two two-photon Fock states. Interference in these networks can be captured in a framework similar to the one used in chapter 2. Experiments pursuing these directions have already started.

To register multiphoton correlations in a large number of channels, detectors that are more attractive than multiple single-pixel single-photon counting modules are available. Of relevance are arrays of superconducting single-photon detectors, offering high detection efficiencies and photon-number resolution, or intensified CCD cameras, allowing single-shot coincidence detection and photon-number resolution over a megapixel area.

8.2 New elements

Platforms used for studying programmable multiphoton correlations could be opaque scattering media or arrays of coupled waveguides, as used in this thesis. Excitingly, a much larger variety of massively multichannels networks can be explored. It would be fascinating to investigate quantum transport of light in different systems, such as multimode fibres [57], arrays of waveguides that are coupled through ring resonators [163] to allow also backward propagation of the light, arrays of corrugated waveguides that provide coupling constants which change with propagation, waveguide arrays with a periodically varying coupling constant in the transverse direction, highly multimode waveguides containing artificial scatterers, or large networks of numerous directional couplers (beam splitters) [164] as are currently employed for demonstrations of boson sampling. By monitoring out-of-plane scattering of light in these structures, one might even gain insight into light propagation and its modification by wavefront shaping, that can be applied to opaque scattering media.

The desired functionality of the programmable optical networks in this thesis

is achieved by preparing the photons in a spatially entangled state over all input channels of the fixed network, using a spatial light modulator and a scattering medium, such that they can be directed at targeted output channels with programmable amplitude and phase. In integrated optics an alternative approach of actively tuning the network itself is used. To provide the maximum freedom in programmability and the ultimate richness in variety of addressable quantum circuits, it looks promising to combine these two approaches in a single system: first inducing the desired functionality internally, by tuning the elements in the network, and then externally by wavefront shaping on the same network with all tuning elements turned off. This could for instance be done with a large network of tunable directional couplers [4, 5, 164].

Finally, one is not restricted to linear optical networks to induce programmable quantum correlations. Also programmable multiphoton correlations in nonlinear optical systems can be envisaged, which, apart from fundamental interest, would be of assistance to optical quantum computing [8]. One could for example create a scattering medium which not only contains scatterers, but also cavities and emitters. It would be intriguing to apply wavefront-shaping techniques to such a system, and possibly create programmable pathways between the resonators. Alternatively, it is possible to exploit the nonlinear optical material response for, say, the Kerr effect, spontaneous parametric down-conversion or spontaneous four-wave mixing inside a scattering medium. Although these effects will be extremely weak in such a medium, perhaps one could realize complex multimode entangled states this way [165–167]. Excitingly, first steps into this direction can be readily taken. One could apply spatial shaping to the pump light of the spontaneous parametric down-conversion source, and investigate if one can influence, and control, spectral and spatial properties of the signal and idler photons, or the correlations between them.

8.3 Applications

By vastly extending the number of monitored channels of the network, and measuring quantum correlations between the outputs using a few incident photons, one enters the field of boson sampling in massively multichannel systems. In boson sampling one is interested in the photon correlations at the outputs of a large optical network, given a specific input state. Measuring the output photon distribution in a boson sampling experiment on a massively multichannel network, such as an opaque scattering medium, is extremely challenging, since these networks contain a large number of channels, which all have to be controlled. Unmonitored channels, for instance channels due to undesired scattering, will act as losses. As discussed in this thesis, by preparing the photons in a spatially entangled state over all input channels using a spatial light modulator, we can program desired correlations at the outputs of a network. Theoretically, if one injects single photons into the programmed outputs of this network, in-

terference again results in the same spatially entangled state over all inputs. Therefore, the correlations in this spatially entangled state are given by the boson sampling matrix of the inverse network. A measurement of the correlations of the entangled state then matches the boson sampling problem of the inverse network. As the entangled state is created through a unitary projection on the spatial light modulator, which carries the information of the massively multichannel network, the hardness of this inverse boson sampling problem is similar to conventional boson sampling. Such a correlation measurement is performed in between the spatial light modulator and the massively multichannel network, and can thus be done without the network in place, avoiding losses.

To ease the wavefront-shaping process used for constructing the programmable optical networks, we have used classical coherent laser light to simulate the spatiotemporal modes of the single-photon states. This approach has shown to be suitable for controlling the propagation of light, and allows for interferometric measurements. However, it would be appealing to investigate the process of wavefront shaping directly on single-photon states and multiphoton states. This would bring security to quantum communication protocols which require wavefront shaping on a regular basis. Such experiments on direct wavefront shaping of single-photon and multiphoton states can be realized using our versatile quantum light source.

In chapter 6 we have introduced a physical unclonable key, in the form of an opaque scattering medium, into a protocol for quantum key distribution. A secure read-out of this physical unclonable key allows authentication of the parties participating in the protocol. This authentication method can be incorporated into a wide variety of quantum protocols, to realize for example authenticated quantum teleportation [168–170] or authenticated entanglement swapping [171].

A Detailed drawing of the experimental setup

Figure A.1 shows a detailed schematic drawing of the optical part of the experimental setup used for most of the experiments in this thesis. The light source for the experiments is a mode-locked picosecond Ti:Sapphire oscillator (right). Part of the light of this laser is sent to a diagnostics section, containing, among others, a spectrometer and autocorrelator. Also light of a continuous-wave diode laser can be merged into the main beam path. Next, the power of the light is divided into two parts. Most of the laser light is frequency doubled in an LBO crystal. After spectral and spatial filtering, the frequency-doubled light is used for spontaneous parametric down-conversion in a PPKTP crystal (centre). The other part of the laser light, which is not routed through the LBO crystal, is coupled through a single-mode fibre and overlapped with the frequency-doubled light. This direct laser light is used for alignment, as well as for wavefront shaping processes. A PBS is used to separate the down-converted photon pairs, after which the photons are coupled into two single-mode fibres (yellow). The outputs of both fibres (left) are modulated using a spatial light modulator and recombined at a PBS, before focusing on a sample, which can consist of an opaque scattering medium or an integrated optical circuit. Both the transmission and reflection of the sample can be directly monitored using CCD cameras or coupled into two fibres for detection by photodiodes, spectrometers, or single-photon counting modules.

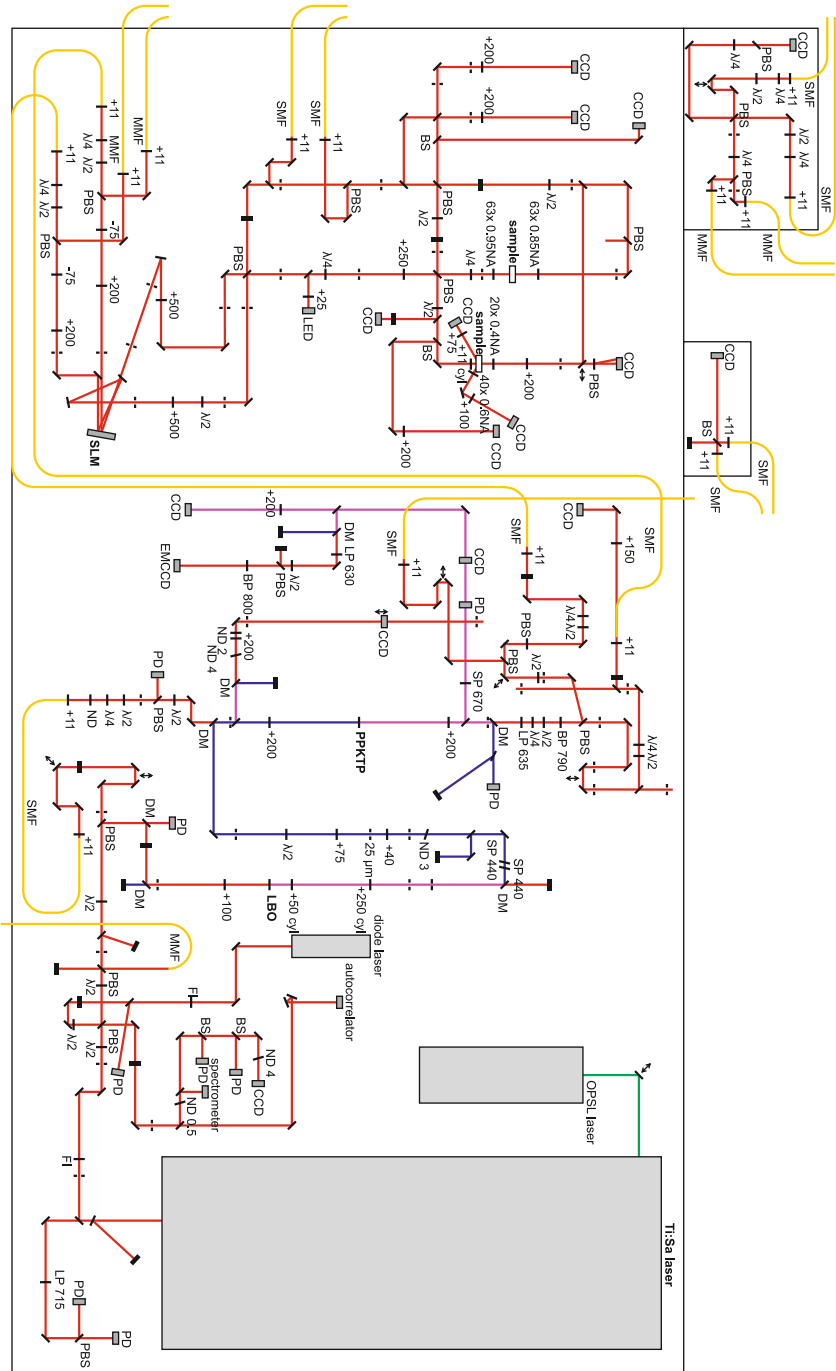


Figure A.1 Schematic drawing of the optical part of the experimental setup.

References

- [1] C. K. Hong, Z. Y. Ou, and L. Mandel, "Measurement of subpicosecond time intervals between two photons by interference," *Phys. Rev. Lett.* **59**, 2044 (1987).
- [2] C. C. Gerry and P. L. Knight, *Introductory Quantum Optics* (Cambridge University Press, New York, 2005).
- [3] M. Tillmann, S. -H. Tan, S. E. Stoeckl, B. C. Sanders, H. de Guise, R. Heilmann, S. Nolte, A. Szameit, and P. Walther, "Generalized Multiphoton Quantum Interference," *Phys. Rev. X* **5**, 041015 (2015).
- [4] J. Carolan, C. Harrold, C. Sparrow, E. Martín-López, N. J. Russell, J. W. Silverstone, P. J. Shadbolt, N. Matsuda, M. Oguma, M. Itoh, G. D. Marshall, M. G. Thompson, J. C. F. Matthews, T. Hashimoto, J. L. O'Brien, and A. Laing, "Universal linear optics," *Science* **349**, 711 (2015).
- [5] N. C. Harris, G. R. Steinbrecher, J. Mower, Y. Lahini, M. Prabhu, T. Baehr-Jones, M. Hochberg, S. Lloyd, and D. Englund, "Bosonic transport simulations in a large-scale programmable nanophotonic processor," *arXiv:1507.03406* (2015).
- [6] E. Knill, R. Laflamme, and G. J. Milburn, "A scheme for efficient quantum computation with linear optics," *Nature* **409**, 46 (2001).
- [7] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, "Linear optical quantum computing with photonic qubits," *Rev. Mod. Phys.* **79**, 135 (2007).
- [8] I. A. Walmsley, "Quantum optics: Science and technology in a new light," *Science* **348**, 525 (2015).
- [9] A. Aspuru-Guzik and P. Walther, "Photonic quantum simulators," *Nat. Phys.* **8**, 285 (2012).
- [10] R. Keil, C. Noh, A. Rai, S. Stützer, S. Nolte, D. G. Angelakis, and A. Szameit, "Optical simulation of charge conservation violation and Majorana dynamics," *Optica* **5**, 454 (2015).
- [11] P. J. J. O'Malley, R. Babbush, I. D. Kivlichan, J. Romero, J. R. McClean, R. Barends, J. Kelly, P. Roushan, A. Tranter, N. Ding, B. Campbell, Y. Chen, B. Chiaro, A. Dunsworth, A. G. Fowler, E. Jeffrey, E. Lucero, A. Megrant, J. Y. Mutus, M. Neeley, C. Neill, C. Quintana, D. Sank, A. Vainsencher, J. Wenner, T. C. White, P. V. Coveney, P. J. Love, H. Neven, A. Aspuru-Guzik, and J. M. Martinis, "Scalable Quantum Simulation of Molecular Energies," *Phys. Rev. X* **6**, 031007 (2016).
- [12] D. G. Olivares, B. Peropadre, A. Aspuru-Guzik, and J. J. García-Ripoll, "Quantum Simulation with a Boson Sampling Circuit," *arXiv:1604.03682* (2016).
- [13] S. Aaronson and A. Arkhipov, "The computational complexity of linear

- optics," in *Proceedings of the ACM Symposium on Theory of Computing '11* (ACM, New York, 2011), p. 333.
- [14] A. Peruzzo, M. Lobino, J. C. F. Matthews, N. Matsuda, A. Politi, K. Poulios, X. -Q. Zhou, Y. Lahini, N. Ismail, K. Wörhoff, Y. Bromberg, Y. Silberberg, M. G. Thompson, and J. L. O'Brien, "Quantum Walks of Correlated Photons," *Science* **329**, 1500 (2010).
 - [15] A. M. Childs, D. Gosset, and Z. Webb, "Universal Computation by Multi-particle Quantum Walk," *Science* **339**, 791 (2013).
 - [16] M. A. Broome, A. Fedrizzi, S. Rahimi-Keshari, J. Dove, S. Aaronson, T. C. Ralph, and A. G. White, "Photonic Boson Sampling in a Tunable Circuit," *Science* **339**, 794 (2013).
 - [17] J. B. Spring, B. J. Metcalf, P. C. Humphreys, W. S. Kolthammer, X.-M. Jin, M. Barbieri, A. Datta, N. Thomas-Peter, N. K. Langford, D. Kundys, J. C. Gates, B. J. Smith, P. G. R. Smith, and I. A. Walmsley, "Boson Sampling on a Photonic Chip," *Science* **339**, 798 (2013).
 - [18] M. Tillmann, B. Daki, R. Heilmann, S. Nolte, A. Szameit, and P. Walther, "Experimental boson sampling," *Nat. Photon.* **7**, 540 (2013).
 - [19] A. Crespi, R. Osellame, R. Ramponi, D. J. Brod, E. F. Galvo, N. Spagnolo, C. Vitelli, E. Maiorino, P. Mataloni, and F. Sciarrino, "Integrated multimode interferometers with arbitrary designs for photonic boson sampling," *Nat. Photon.* **7**, 545 (2013).
 - [20] N. Spagnolo, C. Vitelli, M. Bentivegna, D. J. Brod, A. Crespi, F. Flamini, S. Giacomini, G. Milani, R. Ramponi, P. Mataloni, R. Osellame, E. F. Galvão, and F. Sciarrino, "Experimental validation of photonic boson sampling," *Nat. Photon.* **8**, 615 (2014).
 - [21] J. Carolan, J. D. A. Meinecke, P. J. Shadbolt, N. J. Russell, N. Ismael, K. Wörhoff, T. Rudolph, M. G. Thompson, J. L. O'Brien, J. C. F. Matthews, and A. Laing, "On the experimental verification of quantum complexity in linear optics," *Nat. Photon.* **8**, 621 (2014).
 - [22] P. P. Rohde and T. C. Ralph, "Error tolerance of the boson-sampling model for linear optics quantum computing," *Phys. Rev. A* **85**, 022332 (2012).
 - [23] M. P. Van Albada and A. Lagendijk, "Observation of Weak Localization of Light in a Random Medium," *Phys. Rev. Lett.* **55**, 2692 (1985).
 - [24] P. -E. Wolf and G. Maret, "Weak Localization and Coherent Backscattering of Photons in Disordered Media," *Phys. Rev. Lett.* **55**, 2696 (1985).
 - [25] E. Akkermans and G. Montambaux, *Mesoscopic Physics of Electrons and Photons* (Cambridge University Press, New York, 2007).
 - [26] I. Freund, "Looking through walls and around corners," *Physica A* **168**, 49 (1990).

-
- [27] C. W. J. Beenakker, "Random-matrix theory of quantum transport," *Rev. Mod. Phys.* **69**, 731 (1997).
 - [28] A. P. Mosk, A. Lagendijk, G. Leroosey, and M. Fink, "Controlling waves in space and time for imaging and focusing in complex media," *Nat. Photon.* **6**, 283 (2012).
 - [29] I. M. Vellekoop and A. P. Mosk, "Focusing coherent light through opaque strongly scattering media," *Opt. Lett.* **32**, 2309 (2007).
 - [30] S. M. Popoff, A. Goetschy, S. F. Liew, A. D. Stone, and H. Cao, "Coherent Control of Total Transmission of Light through Disordered Media," *Phys. Rev. Lett.* **112**, 133903 (2014).
 - [31] E. G. van Putten, D. Akbulut, J. Bertolotti, W. L. Vos, A. Lagendijk, and A. P. Mosk, "Scattering lens resolves sub-100 nm structures with visible light," *Phys. Rev. Lett.* **106**, 193905 (2011).
 - [32] J. Aulbach, B. Gjonaj, P. M. Johnson, A. P. Mosk, and A. Lagendijk, "Control of light transmission through opaque scattering media in space and time," *Phys. Rev. Lett.* **106**, 103901 (2011).
 - [33] O. Katz, E. Small, Y. Bromberg, and Y. Silberberg, "Focusing and compression of ultrashort pulses through scattering media," *Nat. Photon.* **5**, 372 (2011).
 - [34] D. J. McCabe, A. Tajalli, D. R. Austin, P. Bondareff, I. A. Walmsley, S. Gigan, and B. Chatel, "Spatio-temporal focusing of an ultrafast pulse through a multiply scattering medium," *Nat. Commun.* **2**, 447 (2011).
 - [35] Y. Guan, O. Katz, E. Small, J. Zhou, and Y. Silberberg, "Polarization control of multiply scattered light through random media by wavefront shaping," *Opt. Lett.* **37**, 4663 (2012).
 - [36] S. R. Huisman, T. J. Huisman, S. A. Goorden, A. P. Mosk, and P. W. H. Pinkse, "Programming balanced optical beam splitters in white paint," *Opt. Express* **22**, 8320 (2014).
 - [37] S. R. Huisman, T. J. Huisman, T. A. W. Wolterink, A. P. Mosk, and P. W. H. Pinkse, "Programmable multiport optical circuits in opaque scattering materials," *Opt. Express* **23**, 3102 (2015).
 - [38] P. Lodahl, A. P. Mosk, and A. Lagendijk, "Spatial Quantum Correlations in Multiple Scattered Light," *Phys. Rev. Lett.* **95**, 173901 (2005).
 - [39] P. Lodahl and A. Lagendijk, "Transport of Quantum Noise through Random Media," *Phys. Rev. Lett.* **94**, 153905 (2005).
 - [40] C. W. J. Beenakker, J. W. F. Venderbos, and M. P. van Exter, "Two-photon speckle as a probe of multi-dimensional entanglement," *Phys. Rev. Lett.* **102**, 193601 (2009).
 - [41] S. Smolka, A. Huck, U. L. Andersen, A. Lagendijk, and P. Lodahl, "Obser-

- vation of Spatial Quantum Correlations Induced by Multiple Scattering of Nonclassical Light," *Phys. Rev. Lett.* **102**, 193901 (2009).
- [42] W. H. Peeters, J. J. D. Moerman, and M. P. van Exter, "Observation of two-photon speckle patterns," *Phys. Rev. Lett.* **104**, 173601 (2010).
 - [43] T. J. Huisman, S. R. Huisman, A. P. Mosk, and P. W. H. Pinkse, "Controlling single-photon Fock-state propagation through opaque scattering media," *Appl. Phys. B* **116**, 603 (2014).
 - [44] H. Defienne, M. Barbieri, B. Chalopin, B. Chatel, I. A. Walmsley, B. J. Smith, and S. Gigan, "Nonclassical light manipulation in a multiple-scattering medium," *Opt. Lett.* **39**, 6090 (2014).
 - [45] C.H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of the IEEE International Conference on Computers, Systems & Signal Processing*, (IEEE Press, New York, 1984), p. 175.
 - [46] S. A. Goorden, M. Horstmann, A. P. Mosk, B. Škorić, and P. W. H. Pinkse, "Quantum-secure authentication of a physical unclonable key," *Optica* **1**, 421 (2014).
 - [47] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, "Experimental realization of any discrete unitary operator," *Phys. Rev. Lett.* **73**, 58 (1994).
 - [48] A. Trenti, M. Borghi, M. Mancinelli, H. M. Price, G. Fontana, and L. Pavesi, "Quantum interference in an asymmetric Mach-Zehnder interferometer," *J. Opt.* **18**, 085201 (2016).
 - [49] R. Uppu, T. A. W. Wolterink, T. B. H. Tentrup, and P. W. H. Pinkse, "Quantum optics of lossy asymmetric beam splitters," *Opt. Express* **24**, 16440 (2016).
 - [50] M. W. Hamilton, "Phase shifts in multilayer dielectric beam splitters," *Am. J. Phys.* **68**, 186 (2000).
 - [51] Z. Y. Ou, J. -K. Rhee, and L. J. Wang, "Observation of Four-Photon Interference with a Beam Splitter by Pulsed Parametric Down-Conversion," *Phys. Rev. Lett.* **83**, 959 (1999).
 - [52] Z. Y. Ou, J. -K. Rhee, and L. J. Wang, "Photon bunching and multiphoton interference in parametric down-conversion," *Phys. Rev. A* **60**, 593 (1999).
 - [53] O. Cosme, S. Pádua, F. A. Bovino, A. Mazzei, F. Sciarrino, and F. De Martini, "Hong-Ou-Mandel interferometer with one and two photon pairs," *Phys. Rev. A* **77**, 053822 (2008).
 - [54] E. M. Nagasako, S. J. Bentley, R. W. Boyd, and G. S. Agarwal, "Nonclassical two-photon interferometry and lithography with high-gain parametric amplifiers," *Phys. Rev. A* **64**, 043802 (2001).
 - [55] E. M. Nagasako, S. J. Bentley, R. W. Boyd, G. S. Agarwal, "Parametric

- downconversion vs optical parametric amplification: a comparison of their quantum statistics," *J. Mod. Opt.* **49**, 529 (2002).
- [56] R. Ghosh and L. Mandel, "Observation of Nonclassical Effects in the Interference of Two Photons," *Phys. Rev. Lett.* **59**, 1903 (1987).
 - [57] H. Defienne, M. Barbieri, I. A. Walmsley, B. J. Smith, and S. Gigan, "Two-photon quantum walk in a multimode fiber," *Sci. Adv.* **2**, e1501054 (2016).
 - [58] A. Politi, M. J. Cryan, J. G. Rarity, S. Yu, and J. L. O'Brien, "Silica-on-Silicon waveguide quantum circuits," *Science* **320**, 646 (2008).
 - [59] R. Lopes, A. Imanaliev, A. Aspect, M. Cheneau, D. Boiron, and C. I. Westbrook, "Atomic Hong-Ou-Mandel experiment," *Nature* **520**, 66 (2015).
 - [60] T. A. W. Wolterink, R. Uppu, G. Ctistis, W. L. Vos, K. -J. Boller, and P. W. H. Pinkse, "Programmable two-photon quantum interference in 10^3 channels in opaque scattering media," *Phys. Rev. A* **93**, 053817 (2016).
 - [61] J. R. Petta, H. Lu, and A. C. Gossard, "A coherent beam splitter for electronic spin states," *Science* **327**, 669 (2010).
 - [62] C. Lang, C. Eichler, L. Steffen, J. M. Fink, M. J. Woolley, A. Blais, and A. Wallraff, "Correlations, indistinguishability and entanglement in Hong-Ou-Mandel experiments at microwave frequencies," *Nat. Phys.* **9**, 345 (2013).
 - [63] R. W. Heeres, L. P. Kouwenhoven, and V. Zwiller, "Quantum interference in plasmonic circuits," *Nat. Nanotechnol.* **8**, 719 (2013).
 - [64] J. S. Fakonas, H. Lee, Y. A. Kelaita, and H. A. Atwater, "Two-plasmon quantum interference," *Nat. Photon.* **8**, 317 (2014).
 - [65] T. Roger, S. Vezzoli, E. Bolduc, J. Valente, J. J. F. Heitz, J. Jeffers, C. Soci, J. Leach, C. Couteau, N. I. Zheludev, and D. Faccio, "Coherent perfect absorption in deeply subwavelength films in the single-photon regime," *Nat. Commun.* **6**, 7031 (2015).
 - [66] L. Baldacci, S. Zanutto, G. Biasiol, L. Sorba, and A. Tredicucci, "Interferometric control of absorption in thin plasmonic metamaterials: general two port theory and broadband operation," *Opt. Express* **23**, 9202 (2015).
 - [67] S. M. Barnett, J. Jeffers, A. Gatti, and R. Loudon, "Quantum optics of lossy beam splitters," *Phys. Rev. A* **57**, 2134 (1998).
 - [68] T. Gruner and D. -G. Welsch, "Quantum-optical input-output relations for dispersive and lossy multilayer dielectric plates," *Phys. Rev. A* **54**, 1661-1677 (1996).
 - [69] J. Jeffers, "Interference and the lossless lossy beam splitter," *J. Mod. Opt.* **47**, 1819 (2000).
 - [70] S. Scheel, L. Knöll, T. Opatrný, and D. -G. Welsch, "Entanglement transformation at absorbing and amplifying four-port devices," *Phys. Rev. A* **62**, 043803 (2000).

- [71] B. Huttner and S. M. Barnett, "Quantization of electromagnetic field in dielectrics," *Phys. Rev. A* **46**, 4306 (1992).
- [72] J. Zmuidzinas, "Thermal noise and correlations in photon detection," *Appl. Opt.* **42**, 4989 (2003).
- [73] P. L. Kelley and W. H. Kleiner, "Theory of electromagnetic field measurement and photoelectron counting," *Phys. Rev.* **136**, A316 (1964).
- [74] W. P. Grice and I. A. Walmsley, "Spectral information and distinguishability in type-II down-conversion with a broadband pump," *Phys. Rev. A* **56**, 1627 (1997).
- [75] K. Poullos, D. Fry, A. Politi, N. Ismail, K. Wörhoff, J. L. O'Brien, and M. G. Thompson, "Two-photon quantum interference in integrated multi-mode interference devices," *Opt. Express* **21**, 23401 (2013).
- [76] D. Bonneau, E. Engin, K. Ohira, N. Suzuki, H. Yoshida, N. Iizuka, M. Ezaki, C. M. Natarajan, M. G. Tanner, R. H. Hadfield, S. N. Dorenbos, V. Zwiller, J. L. O'Brien, and M. G. Thompson, "Quantum interference and manipulation of entanglement in silicon wire waveguide quantum circuits," *New J. Phys.* **14**, 045003 (2012).
- [77] F. D. Murnaghan, *The Unitary and Rotation Groups* (Spartan Books, Washington, D.C., 1962).
- [78] M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov, "Invited Review Article: Single-photon sources and detectors," *Rev. Sci. Instrum.* **82**, 071101 (2011).
- [79] S. E. Harris, M. K. Oshman, and R. L. Byer, "Observation of Tunable Optical Parametric Fluorescence," *Phys. Rev. Lett.* **18**, 732 (1967).
- [80] D. C. Burnham and D. L. Weinberg, "Observation of Simultaneity in Parametric Production of Optical Photon Pairs," *Phys. Rev. Lett.* **25**, 84 (1970).
- [81] B. Yurke and M. Potasek, "Obtainment of thermal noise from a pure quantum state," *Phys. Rev. A* **36**, 3464.
- [82] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, "New High-Intensity Source of Polarization-Entangled Photon Pairs," *Phys. Rev. Lett.* **75**, 4337 (1995).
- [83] R. A. Campos, B. E. A. Saleh, and M. C. Teich, "Quantum-mechanic lossless beam splitter: SU(2) symmetry and photon statistics," *Phys. Rev. A* **40**, 1371 (1989).
- [84] Z. -Y. J. Ou, *Multi-Photon Quantum Interference* (Springer, New York, 2007).
- [85] S. R. Huisman, N. Jain, S. A. Babichev, F. Vewinger, A. N. Zhang, S. H. Youn, and A. I. Lvovsky, "Instant single-photon Fock state tomography," *Opt. Lett.* **34**, 2739 (2009).
- [86] E. Bimbard, N. Jain, A. MacRae, and A. I. Lvovsky, "Quantum-optical state engineering up to the two-photon level," *Nat. Photon.* **4**, 243 (2010).

-
- [87] R. W. Boyd, *Nonlinear Optics* (Academic Press, San Diego, 2008).
 - [88] K. Kato and E. Takaoka, "Sellmeier and thermo-optic dispersion formulas for KTP," *Appl. Opt.* **41**, 5040 (2002).
 - [89] A. Fedrizzi, T. Herbst, M. Aspelmeyer, M. Barbieri, T. Jennewein, and A. Zeilinger, "Anti-symmetrization reveals hidden entanglement," *New J. Phys.* **11**, 103052 (2009).
 - [90] T. A. Driscoll, H. J. Hoffman, R. E. Stone, and P. E. Perkins, "Efficient second-harmonic generation in KTP crystals," *J. Opt. Soc. Am. B* **3**, 683 (1986).
 - [91] G. Brida, M. Chekhova, M. Genovese, and L. Krivitsky, "Generation of different Bell states within the spontaneous parametric down-conversion phase-matching bandwidth," *Phys. Rev. A* **76**, 053807 (2007).
 - [92] C. E. Kuklewicz, M. Fiorentino, G. Messin, F. N. C. Wong, and J. H. Shapiro, "High-flux source of polarization-entangled photons from a periodically poled KTiOPO₄ parametric down-converter," *Phys. Rev. A* **69**, 013807 (2004).
 - [93] T. Kim, M. Fiorentino, and F. N. C. Wong, "Phase-stable source of polarization-entangled photons using a polarization Sagnac interferometer," *Phys. Rev. A* **73**, 012316 (2006).
 - [94] T. E. Keller and M. H. Rubin, "Theory of two-photon entanglement for spontaneous parametric down-conversion driven by a narrow pump pulse," *Phys. Rev. A* **56**, 1534 (1997).
 - [95] F. König and F. N. C. Wong, "Extended phase matching of second-harmonic generation in periodically poled KTiOPO₄ with zero group-velocity mismatch," *Appl. Phys. Lett.* **84**, 1644 (2004).
 - [96] E. Hecht, *Optics* (Addison Wesley, San Francisco, 2002).
 - [97] B. E. A. Saleh and M. C. Teich, *Fundamentals of Photonics* (Wiley-Interscience, New York, 2007).
 - [98] D. A. B. Miller, "Self-configuring universal linear optical component," *Photon. Res.* **1**, 1 (2013).
 - [99] S. W. Leonard, H. M. van Driel, J. Schilling, and R. B. Wehrspohn, "Ultrafast band-edge tuning of a two-dimensional silicon photonic crystal via free-carrier injection," *Phys. Rev. B* **66**, 161102 (2002).
 - [100] W. Zhang, K. Aljaseem, H. Zappe, and A. Seifert, "Completely integrated, thermo-pneumatically tunable microlens," *Opt. Express* **19**, 2347 (2011).
 - [101] P. J. Shadbolt, M. R. Verde, A. Peruzzo, A. Politi, A. Laing, M. Lobino, J. C. F. Matthews, M. G. Thompson, and J. L. O'Brien, "Generating, manipulating and measuring entanglement and mixture with a reconfigurable photonic circuit," *Nat. Photon.* **6**, 45 (2012).

- [102] D. Bonneau, M. Lobino, P. Jiang, C. M. Natarajan, M. G. Tanner, R. H. Hadfield, S. N. Dorenbos, V. Zwiller, M. G. Thompson, and J. L. O'Brien, "Fast path and polarization manipulation of telecom wavelength single photons in lithium niobate waveguide devices," *Phys. Rev. Lett.* **108**, 053601 (2012).
- [103] E. Yüce, G. Ctistis, J. Claudon, E. Dupuy, K. J. Boller, J. M. Gérard, and W. L. Vos, "Competition between electronic Kerr and free-carrier effects in an ultimate-fast optically switched semiconductor microcavity," *J. Opt. Soc. Am. B* **29**, 2630 (2012).
- [104] L. B. Soldano and E. C. M. Pennings, "Optical multi-mode interference devices based on self-imaging: principles and applications," *J. Lightwave Technol.* **13**, 615 (1995).
- [105] S. M. Popoff, G. Lerosey, R. Carminati, M. Fink, A. C. Boccara, and S. Gigan, "Measuring the transmission matrix in optics: an approach to the study and control of light propagation in disordered media," *Phys. Rev. Lett.* **104**, 100601 (2010).
- [106] I. M. Vellekoop and A. P. Mosk, "Phase control algorithms for focusing light through turbid media," *Opt. Commun.* **281**, 3071 (2008).
- [107] H. Yılmaz, W. L. Vos, and A. P. Mosk, "Optimal control of light propagation through multiple-scattering media in the presence of noise," *Biomed. Opt. Express* **4**, 1759 (2013).
- [108] P. Sheng, *Introduction to Wave Scattering, Localization, and Mesoscopic Phenomena* (Academic Press, San Diego, 1995).
- [109] I. M. Vellekoop and A. P. Mosk, "Universal optimal transmission of light through disordered materials," *Phys. Rev. Lett.* **101**, 120601 (2008).
- [110] S. A. Goorden, J. Bertolotti, and A. P. Mosk, "Superpixel-based spatial amplitude and phase modulation using a digital micromirror device," *Opt. Express* **22**, 17999 (2014).
- [111] J. W. Goodman, "Some fundamental properties of speckle*," *J. Opt. Soc. Am.* **66**, 1145 (1976).
- [112] J. Li, G. Yao, and L. V. Wang, "Degree of polarization in laser speckles from turbid media: Implications in tissue optics," *J. Biomed. Opt.* **7**, 307 (2002).
- [113] M. Patra and C. W. J. Beenakker, "Propagation of squeezed radiation through amplifying or absorbing random media," *Phys. Rev. A* **61**, 063805 (2000).
- [114] J. G. Rarity, P. R. Tapster, E. Jakeman, T. Larchuk, R. A. Campos, M. C. Teich, and B. E. A. Saleh, "Two-photon interference in a Mach-Zehnder interferometer," *Phys. Rev. Lett.* **65**, 1348 (1990).
- [115] J. Chen, K. F. Lee, and P. Kumar, "Deterministic quantum splitter based on time-reversed Hong-Ou-Mandel interference," *Phys. Rev. A* **76**, 031804(R) (2007).

-
- [116] J. W. Silverstone, D. Bonneau, K. Ohira, N. Suzuki, H. Yoshida, N. Iizuka, M. Ezaki, C. M. Natarajan, M. G. Tanner, R. H. Hadfield, V. Zwiller, G. D. Marshall, J. G. Rarity, J. L. O'Brien and M. G. Thompson, "On-chip quantum interference between silicon photon-pair sources," *Nat. Photon.* **8**, 104 (2014).
 - [117] J. Carpenter, B. J. Eggleton, and J. Schröder, "110x110 optical mode transfer matrix inversion," *Opt. Express* **22**, 96 (2014).
 - [118] M. Plöschner, T. Tyc, and T. Čižmár, "Seeing through chaos in multimode fibres," *Nat. Photon.* **9**, 529 (2015).
 - [119] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical One-Way Functions," *Science* **297**, 2026 (2002).
 - [120] B. Škorić, A. P. Mosk, and P. W. H. Pinkse, "Security of Quantum-Readout PUFs against quadrature-based challenge-estimation attacks," *Int. J. Quantum. Inform.* **11**, 1350041 (2013).
 - [121] B. Škorić, "Quantum readout of Physical Unclonable Functions," *Int. J. Quantum. Inform.* **10**, 1250001 (2012).
 - [122] J. D. R. Buchanan, R. P. Cowburn, A.-V. Jausovec, D. Petit, P. Seem, G. Xiong, D. Atkinson, K. Fenton, D. A. Allwood, and M. T. Bryan, "'Fingerprinting' documents and packaging," *Nature* **436**, 475 (2005).
 - [123] H. Bechmann-Pasquinucci and W. Tittel, "Quantum cryptography using larger alphabets," *Phys. Rev. A* **61**, 062308 (2000).
 - [124] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, "Security of Quantum Key Distribution Using d-Level Systems," *Phys. Rev. Lett.* **88**, 127902 (2002).
 - [125] R. G. Gallager, *Low-Density Parity-Check Codes* (MIT Press, Cambridge, 1963).
 - [126] A. L. Jones, "Coupling of Optical Fibers and Scattering in Fibers," *J. Opt. Soc. Am.* **55**, 261 (1965).
 - [127] S. Somekh, E. Garmire, A. Yariv, H. L. Garvin, and R. G. Hunspergerk, "Channel optical waveguide directional couplers," *Appl. Phys. Lett.* **22**, 46 (1973).
 - [128] D. N. Christodoulides, F. Lederer, and Y. Silberberg, "Discretizing light behaviour in linear and nonlinear waveguide lattices," *Nature* **424**, 817 (2003).
 - [129] H. S. Eisenberg, Y. Silberberg, R. Morandotti, and J. S. Aitchison, "Diffraction Management," *Phys. Rev. Lett.* **85**, 1863 (2000).
 - [130] T. Pertsch, T. Zentgraf, U. Peschel, A. Bräuer, and F. Lederer, "Anomalous Refraction and Diffraction in Discrete Optical Systems," *Phys. Rev. Lett.* **88**, 093901 (2002).
 - [131] M. J. Ablowitz and Z. H. Musslimani, "Discrete spatial solitons in a

- diffraction-managed nonlinear waveguide array: a unified approach," *Physica D* **184**, 276 (2003).
- [132] J. M. Moison, N. Belabas, C. Minot, and J. A. Levenson, "Discrete photonics in waveguide arrays," *Opt. Lett.* **34**, 2462 (2009).
 - [133] D. Mandelik, H. S. Eisenberg, Y. Silberberg, R. Morandotti, and J. S. Aitchison, "Band-Gap Structure of Waveguide Arrays and Excitation of Floquet-Bloch Solitons," *Phys. Rev. Lett.* **90**, 053902 (2003).
 - [134] J. -M. Moison, N. Belabas, J. A. Levenson, and C. Minot, "Light-propagation management in coupled waveguide arrays: Quantitative experimental and theoretical assessment from band structures to functional patterns," *Phys. Rev. A* **86**, 033811 (2012).
 - [135] T. Pertsch, P. Dannberg, W. Elfle, A. Bräuer, and F. Lederer, "Optical Bloch Oscillations in Temperature Tuned Waveguide Arrays," *Phys. Rev. Lett.* **83**, 4752 (1999).
 - [136] R. Morandotti, U. Peschel, J. S. Aitchison, H. S. Eisenberg, and Y. Silberberg, "Experimental Observation of Linear and Nonlinear Optical Bloch Oscillations," *Phys. Rev. Lett.* **83**, 4756 (1999).
 - [137] S. Longhi, "Nonexponential Decay Via Tunneling in Tight-Binding Lattices and the Optical Zeno Effect," *Phys. Rev. Lett.* **97**, 110402 (2006).
 - [138] P. Biagioni, G. Della Valle, M. Ornigotti, M. Finazzi, L. Duò, P. Laporta, and S. Longhi, "Experimental demonstration of the optical Zeno effect by scanning tunneling optical microscopy," *Opt. Express* **16**, 3762 (2008).
 - [139] H. De Raedt, A. Lagendijk, and P. de Vries, "Transverse Localization of Light," *Phys. Rev. Lett.* **62**, 47 (1989).
 - [140] Y. Lahini, A. Avidan, F. Pozzi, M. Sorel, R. Morandotti, D. N. Christodoulides, and Y. Silberberg, "Anderson Localization and Nonlinearity in One-Dimensional Disordered Photonic Lattices," *Phys. Rev. Lett.* **100**, 013906 (2008).
 - [141] D. N. Christodoulides and R. I. Joseph, "Discrete self-focusing in nonlinear arrays of coupled waveguides," *Opt. Lett.* **13**, 794 (1988).
 - [142] H. S. Eisenberg, Y. Silberberg, R. Morandotti, A. R. Boyd, and J. S. Aitchison, "Discrete Spatial Optical Solitons in Waveguide Arrays," *Phys. Rev. Lett.* **81**, 3383 (1998).
 - [143] S. Minardi, F. Eilenberger, Y. V. Kartashov, A. Szameit, U. Röpke, J. Kolbelke, K. Schuster, H. Bartelt, S. Nolte, L. Torner, F. Lederer, A. Tünnermann, and T. Pertsch, "Three-Dimensional Light Bullets in Arrays of Waveguides," *Phys. Rev. Lett.* **105**, 263901 (2010).
 - [144] Y. Bromberg, Y. Lahini, R. Morandotti, and Y. Silberberg, "Quantum and Classical Correlations in Waveguide Lattices," *Phys. Rev. Lett.* **102**, 253904 (2009).

-
- [145] Y. Bromberg, Y. Lahini, E. Small, and Y. Silberberg, "Hanbury Brown and Twiss interferometry with interacting photons," *Nat. Photon.* **4**, 721 (2010).
 - [146] Y. Bromberg, Y. Lahini, and Y. Silberberg, "Bloch Oscillations of Path-Entangled Photons," *Phys. Rev. Lett.* **105**, 263604 (2010).
 - [147] E. Poem, Y. Gilead, and Y. Silberberg, "Two-Photon Path-Entangled States in Multimode Waveguides," *Phys. Rev. Lett.* **108**, 153602 (2012).
 - [148] H. B. Perets, Y. Lahini, F. Pozzi, M. Sorel, R. Morandotti, and Y. Silberberg, "Realization of Quantum Walks with Negligible Decoherence in Waveguide Lattices," *Phys. Rev. Lett.* **100**, 170506 (2008).
 - [149] Y. Lahini, M. Verbin, S. D. Huber, Y. Bromberg, R. Pugatch, and Y. Silberberg, "Quantum walk of two interacting bosons," *Phys. Rev. A* **86**, 011603(R) (2012).
 - [150] P. M. Preiss, R. Ma, M. E. Tai, A. Lukin, M. Rispoli, P. Zupancic, Y. Lahini, R. Islam, and M. Greiner, "Strongly correlated quantum walks in optical lattices," *Science* **347**, 1229 (2015).
 - [151] Y. Lahini, Y. Bromberg, D. N. Christodoulides, and Y. Silberberg, "Quantum Correlations in Two-Particle Anderson Localization," *Phys. Rev. Lett.* **105**, 163905 (2010).
 - [152] Y. Lahini, Y. Bromberg, Y. Schechtman, A. Szameit, D. N. Christodoulides, R. Morandotti, and Y. Silberberg, "Hanbury Brown and Twiss correlations of Anderson localized waves," *Phys. Rev. A* **84**, 041806(R) (2011).
 - [153] G. Di Giuseppe, L. Martin, A. Perez-Leija, R. Keil, F. Dreisow, S. Nolte, A. Szameit, A. F. Abouraddy, D. N. Christodoulides, and B. E. A. Saleh, "Einstein-Podolsky-Rosen Spatial Entanglement in Ordered and Anderson Photonic Lattices," *Phys. Rev. Lett.* **110**, 150503 (2013).
 - [154] Y. Gilead, M. Verbin, and Y. Silberberg, "Ensemble-Averaged Quantum Correlations between Path-Entangled Photons Undergoing Anderson Localization," *Phys. Rev. Lett.* **115**, 113602 (2015).
 - [155] Y. Lahini, G. R. Steinbrecher, A. D Bookatz, and D. Englund, "Quantum Logic with Interacting Bosons in 1D," arXiv:1501.04349 (2015).
 - [156] R. J. Chapman, M. Santandrea, Z. Huang, G. Corrielli, A. Crespi, M. -H. Yung, R. Osellame, and A. Peruzzo, "Experimental perfect state transfer of an entangled photonic qubit," *Nat. Commun.* **7**, 11339 (2016).
 - [157] N. W. Ashcroft and N. D Mermin, *Solid State Physics* (Thomson Learning, New York, 1976).
 - [158] J. Lian, *Control of Resonances in Photonic Crystal Waveguides* Ph.D. thesis, University of Twente (2016).
 - [159] J. F. Bauters, M. J. R. Heck, D. D. John, J. S. Barton, C. M. Bruinink, A. Leinse, R. G. Heideman, D. J. Blumenthal, and J. E. Bowers, "Planar wave-

- uities with less than 0.1 dB/m propagation loss fabricated with wafer bonding," *Opt. Express* **19**, 24090 (2011).
- [160] O. S. Ojambati, H. Yilmaz, A. Lagendijk, A. P. Mosk, and W. L. Vos, "Coupling of energy into the fundamental diffusion mode of a complex nanophotonic medium," *New J. Phys.* **18**, 043032 (2016).
 - [161] H. A. Haus, L. Molter-Orr, and F. J. Leonberger, "Multiple waveguide lens," *Appl. Phys. Lett.* **45**, 19 (1984).
 - [162] P. B. Catrysse, V. Liu, and S. Fan, "Complete power concentration into a single waveguide in large-scale waveguide array lenses," *Sci. Rep.* **4**, 6635 (2014).
 - [163] A. Yariv, Y. Xu, R. K. Lee, and A. Scherer, "Coupled-resonator optical waveguide: a proposal and analysis," *Opt. Lett.* **24**, 711 (1999).
 - [164] L. Zhuang, C. G. H. Roeloffzen, M. Hoekman, K. -J. Boller, and A. J. Lowery, "Programmable photonic signal processor chip for radiofrequency applications," *Optica* **2**, 854 (2015).
 - [165] A. S. Solntsev, F. Setzpfandt, A. S. Clark, C. W. Wu, M. J. Collins, C. Xiong, A. Schreiber, F. Katzschmann, F. Eilenberger, R. Schiek, W. Sohler, A. Mitchell, C. Silberhorn, B. J. Eggleton, T. Pertsch, A. A. Sukhorukov, D. N. Neshev, and Y. S. Kivshar, "Generation of Nonclassical Biphoton States through Cascaded Quantum Walks on a Nonlinear Chip," *Phys. Rev. X* **4**, 031007 (2014).
 - [166] C. S. Hamilton, R. Kruse, L. Sansoni, C. Silberhorn, and I. Jex, "Driven Quantum Walks," *Phys. Rev. Lett.* **113**, 083602 (2014).
 - [167] S. Barkhofen, T. J. Bartley, L. Sansoni, R. Kruse, C. S. Hamilton, I. Jex, and C. Silberhorn, "Driven Boson Sampling," *arXiv:1605.08570* (2016).
 - [168] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels," *Phys. Rev. Lett.* **70**, 1895 (1993).
 - [169] D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu, "Experimental Realization of Teleporting and Unknown Pure Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels," *Phys. Rev. Lett.* **80**, 1121 (1998).
 - [170] D. Bouwmeester, J. -W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, "Experimental quantum teleportation," *Nature* **390**, 575 (1997).
 - [171] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, "Event-ready-detectors" Bell experiment via entanglement swapping," *Phys. Rev. Lett.* **71**, 4287 (1993).

Summary

Multiphoton quantum correlations are crucial for quantum information processing and quantum communication protocols in linear optical networks. For large-scale implementation of quantum information processing, such as quantum simulators, boson sampling or programmable quantum logic gates, a programmable functionality of a large multichannel network is required. In this thesis, we describe and demonstrate programmable quantum interference between multiple single-photon states in massively multichannel networks.

Using a theoretical analysis we first show that losses in optical networks, which are unavoidable in experiments, introduce new freedom, in that the functionality of the network, and thus also quantum interference in there, is programmable to an extent not possible with lossless networks. By implementing losses in the form of uncontrolled and unmonitored channels of a massively multichannel network, it is possible to construct a fully programmable linear optical network, without actively tuning the network itself. In this way one can induce programmable multiphoton correlations, which can be applied to a variety of useful quantum information processing and simulation protocols.

We introduce a method to program the functionality of general multichannel linear optical networks in opaque scattering media by phase modulation of incident wavefronts. We demonstrate our method by programming linear optical networks with multiple inputs and multiple outputs of arbitrary functionality in an opaque scattering medium, and verify their functionality using interferometric techniques. This method to program linear optical networks of arbitrary functionality is not restricted to opaque scattering media, but can also be applied to integrated optics. As a first step to this end, we show control over the propagation of light through an array of evanescently coupled waveguides. By adaptive phase modulation of the incident wavefront, we direct light to a targeted output waveguide. Due to its high throughput, integrated optics offers an attractive platform to program quantum interference between a large number of channels.

To demonstrate quantum interference in massively multichannel networks we require a source of multiple indistinguishable single-photon states. Therefore, we have constructed and characterized a versatile quantum light source based on spontaneous parametric down-conversion, whose output can be easily tuned from pure single-photon states to quantum states with a high photon number.

For the first time, we demonstrate two-photon quantum interference in a massively multichannel linear optical network realized in an opaque scattering medium. Using adaptive phase-modulation of the incident photons, the scattering medium is transformed to behave as a fully programmable beam splitter. Since the selected channels stem from a manifold of millions of channels, the programmed network need not fulfil energy conservation and is thus freely tunable in functionality. Exploiting this freedom, we not only show the well-known Hong-Ou-Mandel bunching of photons, but also demonstrate that this bunch-

ing can be made to vanish, or be transformed into antibunching. Our results establish opaque scattering media as a platform for massively multichannel linear optical networks with programmable quantum correlations, which is notably relevant for boson sampling and physical-key-based authentication.

Finally, the high number of available channels offered by opaque scattering media can directly be employed for authentication of secure communication. We present an authenticated protocol for quantum key distribution that removes the need of an initial shared secret for authentication. Moreover, we introduce and demonstrate the first protocol for authenticated and asymmetric quantum communication, based on the quantum-secure readout of a physical unclonable function.

Samenvatting

Kwantumcorrelaties tussen meerdere fotonen zijn van groot belang voor de verwerking van kwantuminformatie en protocollen voor kwantumcommunicatie in lineaire optische netwerken. Voor implementaties van kwantuminformatieverwerking op grote schaal, in de vorm van kwantumsimulators, boson samplers of programmeerbare logische kwantumpoorten, is het nodig de functionaliteit van grote meerkanaalsnetwerken te kunnen programmeren. In dit proefschrift beschrijven en demonstreren we programmeerbare kwantuminterferentie tussen meerdere éénfotontoestanden in netwerken met myriaden kanalen.

Via een theoretische analyse laten we eerst zien dat verliezen in optische netwerken, die in experimenten niet te vermijden zijn, een nieuwe vrijheid introduceren: de functionaliteit van het netwerk, en daarmee ook de kwantuminterferentie in het netwerk, wordt vrij programmeerbaar in een mate die niet mogelijk is in verliesvrije netwerken. Door de verliezen te implementeren in de vorm van kanalen die niet beheerst en niet geobserveerd worden is het mogelijk om een volledig programmeerbaar lineair optisch netwerk te construeren zonder het netwerk zelf te verstellen. Op deze wijze kan men programmeerbare correlaties opwekken tussen meerdere fotonen, wat toegepast kan worden op verscheidene nuttige protocollen voor kwantuminformatieverwerking en kwantumsimulaties.

We introduceren een methode om de functionaliteit van algemene lineaire optische meerkanaalsnetwerken te programmeren in ondoorzichtige verstrooiende materialen door middel van fasemodulatie van de inkomende golffronten. We laten de werking van onze methode zien door lineaire optische netwerken met meerdere in- en uitgangen en een vrij te kiezen functionaliteit te programmeren in een verstrooiend materiaal. De functionaliteit van deze netwerken verifiëren we met behulp van interferometrische technieken. Deze methode om lineaire optische netwerken met willekeurige functionaliteit te programmeren beperkt zich niet tot verstrooiende materialen, maar kan ook toegepast worden op geïntegreerde optica. Als eerste stap in deze richting tonen we beheersing over de voortplanting van licht in een rij van evanescentgekoppelde golfgeleiders. Door middel van adaptieve fasemodulatie van het inkomende golffront kunnen we licht sturen naar een geselecteerde uitgangsgolfgeleider. Omdat zij een hoge transmissie kent, vormt geïntegreerde optica een interessant platform voor het programmeren van kwantuminterferentie tussen een groot aantal kanalen.

Om programmeerbare kwantuminterferentie aan te tonen in netwerken met myriaden kanalen hebben we een bron van meerdere ononderscheidbare éénfotontoestanden nodig. Daarom hebben we een veelzijdige kwantumlichtbron op basis van spontane parametrische downconversie geconstrueerd en gekarakteriseerd. Deze bron kan eenvoudig ingesteld worden voor het genereren van zowel pure éénfotontoestanden als kwantumtoestanden met een groot aantal fotonen.

Voor het eerst laten we programmeerbare kwantuminterferentie tussen twee fotonen zien in een lineair optisch netwerk met myriaden kanalen, dat gerealiseerd is in een verstrooiend materiaal. Door middel van adaptieve fasemodu-

latie van de inkomende fotonen wordt het verstrooiende materiaal zo getransformeerd dat het zich gedraagt als een volledig programmeerbare bundeldealer. Omdat de geselecteerde kanalen voortkomen uit een collectie van miljoenen kanalen hoeft het geprogrammeerde netwerk niet te voldoen aan behoud van energie en is het dus vrij instelbaar in functionaliteit. Gebruikmakend van deze vrijheid laten we niet alleen het samenklonteren van fotonen zien, welbekend als het Hong-Ou-Mandeleffect, maar tonen we ook aan dat dit klonteren kan worden opgeheven, of kan worden omgezet naar antiklonteren. Door onze resultaten bewijzen verstrooiende materialen zich als platform voor grote lineaire optische meerkanaalsnetwerken met programmeerbare kwantumcorrelaties. Dit is in het bijzonder relevant voor boson samplen en authenticatie met fysieke sleutels.

Tenslotte kan het grote aantal aan beschikbare kanalen dat verstrooiende materialen bieden direct worden ingezet voor de authenticatie van beveiligde communicatie. We presenteren een geauthentiseerd protocol voor kwantumsleutel-distributie dat de noodzaak van een eerder gedeeld geheim voor authenticatie wegneemt. Bovendien introduceren en demonstreren we het eerste protocol voor geauthentiseerde en asymmetrische kwantumcommunicatie, dat gebaseerd is op de kwantumveilige uitlezing van een fysieke onkloonbare functie.

List of publications

Journal articles

- T. B. H. Tentrup, T. Hummel, T. A. W. Wolterink, R. Uppu, A. P. Mosk, and P. W. H. Pinkse, "Transmitting more than 10 bit with a single photon," (submitted).
- R. Uppu, T. A. W. Wolterink, T. B. H. Tentrup, and P. W. H. Pinkse, "Quantum optics of lossy asymmetric beam splitters," *Opt. Express* **24**, 16440 (2016).
- T. A. W. Wolterink, R. Uppu, G. Ctistis, W. L. Vos, K. -J. Boller, and P. W. H. Pinkse, "Programmable two-photon quantum interference in 10^3 channels in opaque scattering media," *Phys. Rev. A* **93**, 053817 (2016).
- J. P. Couperus, A. Köhler, T. A. W. Wolterink, A. Jochmann, O. Zarini, H. M. J. Bastiaens, K. -J. Boller, A. Irman, and U. Schramm, "Tomographic characterisation of gas-jet targets for Laser Wakefield Acceleration," *Nucl. Inst. Meth. Phys. Res. A* **830**, 504 (2016).
- S. R. Huisman, T. J. Huisman, T. A. W. Wolterink, A. P. Mosk, and P. W. H. Pinkse, "Programmable multiport optical circuits in opaque scattering materials," *Opt. Express* **23**, 3102 (2015).

Conference proceedings

- T. A. W. Wolterink, G. Ctistis, S. R. Huisman, T. J. Huisman, A. P. Mosk, and P. W. H. Pinkse, "Programming Quantum Interference in Scattering Materials," in *2015 European Conference on Lasers and Electro-Optics - European Quantum Electronics Conference* (Optical Society of America, 2015), p. EA_3_2.
- P. W. H. Pinkse, T. J. Huisman, S. R. Huisman, T. A. W. Wolterink, and A. P. Mosk, "Programming Single-Photon Wavefronts for Quantum Authentication," in *Research in Optical Sciences* (Optical Society of America, 2014), p. QTu3B.4.
- S. R. Huisman, T. J. Huisman, T. A. W. Wolterink, A. P. Mosk, and P. W. H. Pinkse, "Programming quantum interference with multiple scattering," in *2013 Conference on Lasers and Electro-Optics - International Quantum Electronics Conference* (Optical Society of America, 2013), p. IA_P_3.

