Generation, Transformation, and Application of Quantum States of Photons: Quantum Entanglement, Quantum Coherence, and Oblivious Transfer

a Ph.D. thesis

by

Nikola Horová

Faculty of Science | Palacký University

Olomouc
2024

Abstract

This dissertation presents experimental tools for quantum information processing at the level of individual photons and their use for information transmission and processing. We study the generation of entangled photons emitted by quantum dots. We deal with the problem of broken circular symmetry of the quantum dot leading to the generation of distinguishable photons. We apply triaxial stress in the plane to change the shape of the quantum dot electronic structure. This process enables restoring the broken symmetry and generating entangled photon pairs.

We further deal with quantum coherence, which is closely related to quantum entanglement. We introduce the resource theory of coherence as we investigate the protocol for assisted quantum coherence enhancement for a qubit. We deterministically increase the coherence of the target system (one qubit) by reducing the coherence of the control system (multiple copies). We define the concept of mutual coherence and investigate the states that maximize it in different subspaces of the two-qubit Hilbert space. In the 3D subspace, we discover a non-trivial asymmetric state, which we prepare from two factorized photonic qubits.

Finally, we present the specific cryptographic protocol called non-interactive XOR oblivious transfer (XOT). It is a protocol between two participants who do not trust each other. Here, the sender, Alice, has two bits and sends them to the receiver, Bob. He gets either the first bit, the second bit or their XOR. Bob should not learn anything more, and Alice should not know what information Bob received. For the protocol, we also determine the smallest possible cheating probabilities for dishonest parties using pure symmetric states.

Keywords: photon, polarization encoding, quantum dots, quantum coherence, quantum protocol, entanglement, oblivious transfer, quantum tomography

Author:	Mgr. Nikola Horová
Advisor:	prof. Mgr. Jaromír Fiurášek, Ph.D.
Consultant:	Mgr. Robert Stárek, Ph.D.
Study programme:	Optics and Optoelectronics
Institution:	Department of Optics, Faculty of Science, Palacký University
Year:	2024
Pages:	135

Generace, transformace a aplikace kvantových stavů fotonů: kvantově provázané stavy, kvantová koherence a oblivious transfer

Dizertační práce

Nikola Horová

Přírodovědecká fakulta | Univerzita Palackého

Olomouc
2024

Anotace

Dizertační práce se věnuje rozvoji experimentálních nástrojů kvantového zpracování informace na úrovni jednotlivých fotonů a jejich využití pro přenos a zpracování informace. Studována je generaci kvantově provázaných fotonů s využitím zdroje založeného na kvantových tečkách. Zabýváme se problémem narušené kruhové symetrie kvantových teček, která vede ke generaci rozlišitelných fotonů. Na kvantovou tečku aplikujeme tříosé napětí v rovině, abychom změnili tvar její elektronické struktury. Tento proces vede k obnovení její symetrie a následně ke generaci entanglovaných fotonových párů.

Dále se práce zabývá kvantovou koherencí, která s kvantovou provázaností úzce souvisí. Jsou uvedeny definice zdrojové teorie koherence, protože zkoumáme protokol asistovaného vylepšení kvantové koherence u qubitu. Deterministicky navyšujeme koherenci cílového systému (jednoho qubitu) za pomoci snížení koherence řídícího systému (více kopií). Definujeme pojem vzájemné koherence a zkoumáme stavy, které ji maximalizují v různých podprostorech dvouqubitového Hilbertova prostoru. Ve 3D podprostoru objevujeme netriviální asymetrický stav, který připravujeme ze dvou faktorizovaných fotonických qubitů.

V neposlední řadě je v práci prezentován konkrétní kryptografický protokol nazvaný neinteraktivní XOR oblivious transfer, neboli XOT. Jedná se o protokol mezi dvěma účastníky, kteří si navzájem nedůvěřují. Zde odesílatel Alice má k dispozici dva bity a příjemce Bob získá buď první bit, druhý bit, nebo jejich XOR. Bob by se neměl dozvědět nic více a Alice by neměla vědět, jakou informaci Bob obdržel. U protokolu také určujeme nejmenší možné pravděpodobnosti podvádění pro nepoctivé strany využívající symetrické čisté stavy.

Klíčová slova: foton, polarizační kódování, kvantové tečky, kvantová koherence, kvantový protokol, kvantová provázanost, oblivious transfer, kvantová tomografie

Autor:	Mgr. Nikola Horová
Vedoucí práce:	prof. Mgr. Jaromír Fiurášek, Ph.D.
Konzultant:	Mgr. Robert Stárek, Ph.D.
Studijní obor:	Optika a optoelektronika
Instituce:	Katedra Optiky, Přírodovědecká Fakulta, Univerzita Palackého
Year:	2024
Pages:	135

Acknowledgements

First, I would like to thank Jaromír Fiurášek, Michal Mičuda, and Robert Stárek for taking me under their wing. To my supervisor, Jaromír Fiurášek, I am grateful for his support throughout my studies at Palacký University. I remember the first day at the university for my admissions, and the last big fear in the form of the final exams, where you were present. Not only in those days, I got a lot of important information and advice from you. Thank you. Michal and Robert taught me to build and work not only with quantum gates in the laboratory, they shared all their knowledge with me and advised me during my work. I respect you all very much.

I must also not forget the pleasant environment of our faculty. I met a lot of friends here who were and are my support. I won't list you by name because I might forget someone. I am truly grateful to have you in my life. I would like to note that I appreciate the patience and kindness of all my friends who share an office with me. I know it's not always easy :).

And my warmest thanks go to my entire family. I am very grateful for my twin Miška, who has shared all my joys and sorrows with me since the beginning of our lives.

Thank you.

"I declare that I wrote this dissertation on my own under the guidance of my supervisor Prof. Mgr. Jaromír Fiurášek, Ph.D. using the resources which are cited in References. I confirm this Thesis is based on original research and contribution of the author can be found in Preface. I agree with the further usage of this Thesis according to the requirements of Palacký University and the Department of Optics."

In Olomouc

.....

Contents

Preface

This thesis presents the results of my research during PhD studies at the Palacký University in Olomouc. It aims to present advances in experimental methods and their results in the field of quantum entanglement, quantum coherence and quantum protocols. This thesis is based on four publications denoted in References as [A1–A4].

At the very beginning, I would like to note that the results written in this thesis are the efforts of the entire team of researchers. The necessary part of the experiments built in our laboratory was a photon source constructed by Ivo Straka [1]. At the same time, I had some programs created by Robert Stárek, which were able to control the parts of our experiments. Robert Stárek and Michal Mičuda participated in the construction of experiments, data processing and writting manucripts. Our work was supervised by Prof. Jaromír Fiurášek, who participated in the theoretical parts of two publications focused on quantum coherence, checked the results achieved in the experimental parts, considered their improvement and participated in the creation of manuscripts. Prof. Radim Filip and Michal Kolář participated in the theoretical part and calculations of the deterministic enhancement of local quantum coherence protocol and also in writting its manuscript. Prof. Miloslav Dušek ensured all cooperation with colleagues from Great Britain led by Prof. Erika Andersson. He contributed to the theoretical part of the XOT protocol, checked the results of the experiment and participated in writing the manuscript. Now, let me share my contribution.

The first mentioned publication [A1] was the result of the research during a three-month internship when I visited the group of Prof. Rinaldo Trotta at La Sapienza University in Rome, Italy. As part of the internship, under the supervision of colleagues from Rinaldo's group, I learned to work with quantum dots. We measured the degree of linear polarization of the emitted photons by a quantum dot and the lifetime of its quasiparticles. I learned to measure fine-structure splitting. Together with people from the group, we quantified entanglement between emitted photon pairs without influencing the quantum dot. We then applied voltage to the quantum dot and investigated when the fine-structure splitting is reduced and the effect on entanglement. The results in this thesis, thus,

come from my measurements in the laboratory of La Sapienza University.

The next two publications [A2, A3] are based on the experiments created in our laboratory at Palacký University. In this laboratory, I learned to work with quantum bits (qubits), to encode information into the polarization degrees of freedom of photons. I managed to build more than one interferometer and ensure their stability. I learned the importance of two-photon interference in the experiment. I gained experience working with the source of plarization-entangled photon pairs based on spontaneous parametric down-conversion (SPDC) and with entanglement detection. Last but not least, I used the knowledge of quantum tomography to reconstruct the quantum state. During our experiments, I was responsible for building both experimental setups. Together with Robert Stárek and Michal Mičuda, we started both experiments, checked the correct settings, and measured and processed the data. Together with other authors, I contributed to the writing of the manuscript.

The last mentioned publication [A4] arose from our collaboration with Erika Anderson's group in Edinburgh, Great Britain. This group provided the theoretical basis for our experiment regarding oblivious transfer. I participated in setting up the experiment, measuring the results and processing the data. I also helped with the correction of the manuscript.

Olomouc
February 2024

Nikola Horová
horovanikola@outlook.com

Chapter 1

Introduction

The first thoughts about the quantum nature of light appeared around 1900 when Max Planck resolved the ultraviolet catastrophe by considering that the energy of light is absorbed and emitted in quanta - discrete packets of energy [2]. Then in 1905, Albert Einstein, motivated by Max Planck, published a theory of the photoelectric effect, in which he proposed the existence of energy quanta, later called photons [3, 4]. It was during these times when the importance of theory that would connect the wave and the particle nature of light began to emerge. These were the beginnings of quantum mechanics.

Since then, there have been many breakthroughs. For example, photons were previously thought to be independent of each other. However, in 1956, Hanbury Brown and Twiss disproved this theory by an experiment in which they proposed measuring the angular diameters of stars from correlations of intensities in the independent detectors [5]. They observed the bunching correlation for bosons. Later, other experiments were implemented, where fermions were used instead of bosons, and the antibunching effect was observed [6]. This effect has no analogue in classical mechanics. A fully consistent description of the Hanbury Brown and Twiss experiment (HBT) was given by Glauber in his quantum optical coherence theory [7]. It introduces multi-order correlation functions based on those introduced in classical optics.

In the early days of quantum mechanics, there was another breakthrough when Einstein, Podolsky and Rosen introduced a thought experiment known as the EPR paradox [8]. Using this experiment, they tried to prove that the quantum theory is incomplete. They considered a pair of particles prepared in such a quantum state that if, for example, the position (or momentum) of the first particle were measured, it would be immediately possible to predict the position (or momentum) of the second particle as well, which would contradict the theory of relativity. Today, we know that it is possible to generate such states, and we call them entangled. Their existence can be proven, for example, by Bell's

inequalities violation [9]. At the same time, these states do not contradict the theory of relativity since the detected information of one entangled particle cannot be transmitted faster than the speed of light. Entangled states and Bell's work eventually found application in some quantum cryptography protocols [10, 11]. Entangled states are further used for quantum teleportation [12, 13] or in superdense coding [14].

This thesis aims to describe the experiments carried out during my PhD studies. These experiments represent advances in the fields of quantum dots, quantum coherence, and quantum protocols. In this Chapter, in Section 1.1, we present the contemporary state of research. Theory, methodological details and fundamental concepts are included in *Chapter* 2. Specifically, Section 2.1 introduces the quantum bit or qubit, its characterization, and devices that perform logical operations on qubits. At the same time, it explains information encoding using a qubit and describes two-photon interference, quantum state tomography and entanglement. Section 2.2 discusses the generation of entangled photons produced by spontaneous parametric down-conversion and by quantum dots. The description of quantum coherence as a resource theory is in Section 2.3. Subsequently, we introduce the concept of mutual coherence and explain the common traits of coherence and entanglement resource theories. In the last Section 2.4, we describe quantum key distribution and oblivious transfer. We discuss their differences, and we introduce the various protocols that are used to transmit information securely.

Chapter 3 describes the generation of entangled photon pairs inside GaAs quantum dots and a strain tuning method. The generation is dependent on the circular symmetry of a quantum dot. If a quantum dot has reduced symmetry, an effect of fine-structure splitting occurs. The larger this effect is, the more we can distinguish the photons generated by the quantum dot, and thus, the less the photons emitted by a quantum dot are entangled. The purpose of the strain tunning method is the external strain field application, which makes it possible to improve the broken symmetry of the quantum dot. In Section 3.1, we characterize the GaAs quantum dot. We are interested in the degree of linear polarization of the generated photons, the lifetime of quasi-particles inside the quantum dot, from whose recombination we obtain the necessary photons, and last but not least, we are interested in the measurement of fine-structure splitting. In Section 3.2, we describe the application of voltage to the quantum dot using the strain tuning method to reduce the measured value of fine-structure splitting. Subsequently, in Section 3.3, we show the dependence of two entanglement measures on the fine-structure splitting.

In *Chapter* 4, we investigate a remote control and enhancement of quantum coherence. In this protocol, we consider quantum coherence as a resource theory.

We experimentally demonstrate the quantum coherence enhancement using two qubits, one target and one control, with non-zero coherence. We let these two qubits interact in a setup enabling the control of their coupling strength. For a specific coupling strength, we manage to increase the coherence of the target qubit by using several copies of the control qubit. We use a partial SWAP gate (p-SWAP), described in Section 4.1.1, to control the coupling strength between the two qubits. The description of the experiment consisting of the p-SWAP gate is subsequently included in Section 4.1.2.

We stay with quantum coherence as a resource theory in *Chapter* 5 and look at composite systems that consist of multiple qubits. In this case, it is possible to define coherence occurring in the composite system, which, however, is no longer contained in its individual subsystems. We call such a coherence mutual coherence. We investigate quantum states that maximize mutual coherence in various subspaces of the two-qubit Hilbert space.

Finally, in *Chapter* 6, we describe and experimentally implement the proposed non-interactive XOR quantum oblivious transfer protocol. It is a protocol between two participants, Alice and Bob, who do not trust each other. One of the participants sends messages to the other. The recipient should receive only one message without knowing the content of the others and without the sender knowing which message the recipient received. We are interested in all possible cases that may arise, more specifically, they both being honest or when Alice or Bob wants to get more information than they should have. We consider both variants, when Alice sends messages to Bob, as well as when Bob sends messages to Alice.

1.1 Contemporary state of research

Linear optics

Linear optics is a powerful platform for quantum information processing which uses superposition states of photons or atoms for processing or sending information (data). Linear optics is the only choice if we want to connect several nodes of a network for the purpose of quantum communication or quantum computing. It can be used to probe fundamental properties of quantum physics. Individual photons are the carrier of information, and linear optical elements, such as (polarizing) beam splitters, half- and quarter-waveplates or mirrors, are used to transmit and process information.

The importance of linear optics became first apparent in 1984 when the first quantum protocol for secure quantum communication was designed and implemented by Bennett and Brassard [15]. In 2001, Knill, Laflamme, and Mil-

burn showed that scalable quantum computation is possible with linear optics elements, single-photon sources, and detectors, i.e. without nonlinearity [16]. This scheme is an implementation of linear optical quantum computing (LOQC), which enables the creation of universal quantum computers. Even though this scheme is possible in principle, controlling photons moving at the speed of light was challenging at the time. This situation changed with the first experimental demonstrations of two- and three-qubit gates [17–19]. Not long after, there were already various experimental demonstrations of quantum computing [20–22].

Another approach implemented using linear optics that can solve problems beyond the capabilities of classical computers is boson sampling [23]. This method, while not considered universal, could demonstrate the power of quantum computing without realizing a quantum computer. Scalable boson sampling with time-bin encoding has already been implemented [24]. Subsequently, scientists demonstrated three-, four-, and five-boson sampling together with 12-photon entanglement [25] and Gaussian boson sampling on 216 squeezed modes entangled with three-dimensional connectivity using a photonic processor called Borealis [26].

Through boson sampling, we come to the fact that the framework of linear optics also allows the generation of entanglement [27], the associated violation of Bell's inequalities [28] and quantum teleportation [13]. With the constant development of technology, it is possible to realize quantum teleportation even on a photonic chip [29]. Integrated quantum photonics is increasingly used due to its advantages, such as more advanced manufacturing technologies, information transmission and processing at room temperatures, stability and resistance to decoherence. Scientists from Denmark and China managed to assemble a graph-theoretical programmable quantum photonic device in large-scale integrated nanophotonic circuits integrating about 2.500 components fabricated on a silicon-on-insulator wafer [30]. It is also possible to implement an efficient SWAP gate on the chip, which deterministically swaps the photon's polarization qubit for its spatial momentum qubit [31]. A greater challenge in quantum-integrated photonics is the inclusion of (non-classical) light sources and detectors. One of the possible approaches in light sources integration on the chip is a laser cavity with a high-efficiency tunable noise suppression filter and a nonlinear microring for entangled photon pairs generation through spontaneous four-wave mixing [32]. Another solution is using quantum dots, which allows generation of the spin-photon entanglement based on photon-scattering of a quantum dot [33]. As for the detectors, the researchers integrated a superconducting nanowire single-photon detector [34] or mid-infrared photothermoelectric detectors enabling polarization detection [35].

Entangled photon sources

The most widespread way to generate photon entanglement is by spontaneous parametric down-conversion (SPDC). The conservation of energy and momentum in this process leads to the creation of two entangled photons. This phenomenon was first observed by Harris and colleagues in 1967 as parametric fluorescence inside a bulk nonlinear crystal [36]. This observation was followed by experiments generating entanglement in various degrees of freedom, such as polarization [37], time-frequency [38], orbital angular momentum [39], or their numerous combinations [40].

SPDC is not the only way to create entangled photon pairs. Other possible solutions are the use of two neutral atoms and the Rydberg blockade [41] or an entanglement filter, where unwanted states are eliminated, and the outputs are high-fidelity entangled states. The second mentioned procedure is done using strong and controllable photon-photon interaction enabled by Rydberg atoms [42].

Other important sources of entangled photon pairs are quantum dots. Their advantage over SPDC sources lies in the generation of photons "on-demand". In other words, it is not a probabilistic source, where we get the desired output with a certain probability, but a source that, under ideal conditions, creates a photon or entangled photon pairs deterministically when triggered by a laser or electrical impulse. A quantum dot exhibits atom-like properties, such as discrete levels of energy. In a simple model, a quantum dot can be described as a three-level system with ground state, exciton level and biexciton level. Thanks to the Pauli exclusion principle, it is possible to excite a maximum of two electrons to the biexciton level. The recombination of these electrons from the biexciton level through the exciton level to the ground state under certain conditions creates an entangled photon pair. The use of quantum dots enables to generate time-bin entanglement [43, 44], polarization entanglement [45] even on a chip [46], or spatial-dependent quantum dot-photon entanglement [47].

Quantum coherence

Quantum coherence is at the heart of quantum interference and quantum computing and also is a necessary condition for entanglement. It was first described by Glauber [7], Sudarshan [48] in terms of phase space distributions and multipoint correlation functions. However, this theory can be generalized beyond optical fields. Quantum coherence can be present in the quantum superposition of states of quantum system of any type and can be considered an important resource.

A resource theory of quantum coherence was formulated in 2014 by Baumgratz, Cramer, and Plenio [49]. Coherence is a basis-dependent concept, so we must first choose the basis of a defined vector space. This basis can be chosen to suit existing constraints, such as the conditions in the laboratory or different conservation laws. For quantum coherence description, we further need to identify a set of incoherent states and a class of free (incoherent) operations. These operations have been discussed in publications by Chitambar and Gour [50–52].

Possible applications of quantum coherence are in quantum algorithms [53–55]. In Ref. [53], the presented algorithm decides whether the boolean function is constant or balanced. If there is less coherence in this protocol, then the error of this decision increases. Other applications can be found in thermodynamics [56, 57], metrology [58], or in quantum key distribution [59], where authors show that the secure key rate can be quantified by the coherence of the shared bipartite states.

Protocols of quantum cryptography

Quantum cryptography is a technique using principles of quantum mechanics for secret communication over an insecure channel. Its beginnings date back to 1983 when Wiesner proposed using principles of quantum mechanics to create and validate unforgeable banknotes. There are several cryptographic methods including, for example, quantum key distribution (QKD), oblivious transfer (OT), quantum bit commitment [60] or password-based authentication [61].

QKD protocols allow quantum-safe communication and quantum OT-(QOT) protocols allow quantum-safe computation. In QKD, the communication involves participants who trust each other, and thus, the security of the quantum communication channel is determined concerning an unwanted third party. Whereas with OT, even the communication participants do not trust each other, so the security of information transmission must be guaranteed even towards them. The first QKD protocol was created in 1984, and it is the well-known BB84 protocol by Bennett and Brassard [15]. It uses polarization encoding into individual qubits to transmit information. Another QKD protocol is the E91 protocol [10], which uses entanglement to determine the security of information transmission. Among the first OT protocols, we consider 1-2 oblivious transfer [62], 1-n OT [63].

Nowadays, scientists focus on improvements of the protocols security. They try to increase the secure key rate at ever greater distances and reduce the quantum bit error rate (QBER) or cost. Existing QKD and OT protocols work either with discrete variables (DV) [64, 65], where information is encoded into properties of photons, for example, polarization or phase, or protocols working with continuous variables (CV) [66, 67] using the quadrature of coherent or squeezed states of light. CV and DV approaches can also be combined [68]. However,

these different secure communication ways have their own advantages and disadvantages. For example, one of the advantages of CV compared to DV may be a higher secure key rate, but on the other hand, it has complex data processing. To transfer a secret key or message, we can use optical fibers [65, 69], communicate over a free space [70], or a combination of both [71]. Free space communication is affected by diffraction, atmospheric extinction, or turbulence. On the other hand, its advantages are easy mobility and simpler design. There are even protocols with entanglement [72] generated not only by SPDC source [73, 74], but also by quantum dots [75]. Scientists have even come up with satellite-to-ground QKD [76] or (measurement) device-independent protocols [77, 78], where we no longer rely on our detection device being secure.

Chapter 2

Methods

All the experiments presented in this work are based on linear optics and work with individual quantum bits (qubits). Therefore, this entire Chapter is devoted to qubits. We describe what a qubit is and what role it plays in quantum physics. We introduce the elementary quantum gates to demonstrate how we can manipulate qubits. We explain polarization and spatial encoding with qubits, two-photon interference, and the principle of quantum tomography. Subsequently, we introduce the concept of polarization entanglement and present two possible ways to create it among qubits. At the end of this Chapter, we mention quantum coherence and how it is related to entanglement.

2.1 Quantum bits

A quantum bit or a qubit is a two-level system and a basic unit of quantum information. Mathematically, we can describe a qubit by a 2D Hilbert space $\mathcal{H} = \mathbb{C}^2$, which is a complete vector space with a scalar product. The basis of the Hilbert space consists of two orthogonal states, which are written in Dirac notation as $|0\rangle$ and $|1\rangle$. While a classical bit can only be in one of the basis states, $|0\rangle$ or $|1\rangle$, a qubit can also be in a superposition of these two states $\alpha|0\rangle + \beta|1\rangle$ with complex coefficients satisfying $|\alpha|^2 + |\beta|^2 = 1$.

A pure single qubit state can be expressed as

$$|\psi\rangle = \frac{\alpha|0\rangle + \beta|1\rangle}{\sqrt{|\alpha|^2 + |\beta|^2}}. \tag{2.1}$$

The denominator arose from the condition that the state must be normalized, i.e., $|\langle\psi|\psi\rangle|^2 = 1$

Alternatively, a pure single-qubit state $|\psi(\theta, \phi)\rangle$ can be interpreted as an eigenvector of an observable $\hat{\sigma}(\theta, \phi)$ with eigenvalue of 1. Operator $\hat{\sigma}(\theta, \phi)$ can be

expressed as

$$\hat{\sigma}(\theta,\phi) = \sin\theta\cos\phi\hat{\sigma}_x + \sin\theta\sin\phi\hat{\sigma}_y + \cos\theta\hat{\sigma}_z,$$

where $\hat{\sigma}_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $\hat{\sigma}_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$ and $\hat{\sigma}_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ are Pauli spin matrices.

The $\hat{\sigma}(\theta,\phi)$ operator has a second eigenvector, which is perpendicular to the already mentioned eigenvector $|\psi(\theta,\phi)\rangle$ and has an eigenvalue equal to -1. Each of the Pauli matrices also has two eigenvectors with ± 1 eigenvalues

$$\begin{aligned} \hat{\sigma}_x|x^{\pm}\rangle &= \pm|x^{\pm}\rangle, \\ \hat{\sigma}_y|y^{\pm}\rangle &= \pm|y^{\pm}\rangle, \\ \hat{\sigma}_z|z^{\pm}\rangle &= \pm|z^{\pm}\rangle, \end{aligned}$$

where $|x^{\pm}\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$, $|y^{\pm}\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)$, $|z^{+}\rangle = |0\rangle$ and $|z^{-}\rangle = |1\rangle$.

The eigenvectors x^-, y^- and z^- define the axes of a 3D sphere, called the Bloch sphere shown in Figure 2.1, therefore, a measurement in the $\hat{\sigma}_z$ basis can be used as a synonym for projection measurement on a pair of orthogonal vectors $|0\rangle$ and $|1\rangle$. Similarly for measurements in the $\hat{\sigma}_x$ and $\hat{\sigma}_y$ bases.

A single-qubit state can also be written using two angles θ, ϕ in spherical coordinates

$$|\psi(\theta,\phi)\rangle = \cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle, \tag{2.2}$$

where $\theta \in [0,\pi]$ and $\phi \in [0, 2\pi]$. This parametrization allows to represent the qubit by a point on the Bloch sphere.

The Bloch sphere plays an important role in describing quantum states. Pure quantum states lie on the surface of the Bloch sphere. Moreover, points lying inside this sphere can be associated with mixed quantum states representing a statistical ensemble of pure states. They cannot be described by a state vector, but instead, they have to be represented using a density operator (a density matrix after choosing a certain basis)

$$\hat{\rho}_{mix} = \sum_{i=0}^{1} p_i |\psi(\theta_i,\phi_i)\rangle\langle\psi(\theta_i,\phi_i)|, \tag{2.3}$$

with probabilities p_i that must satisfy the conditions $p_i \geq 0$ and $\sum_i p_i = 1$.

Each pure state is also described by a density operator, however, the sum from the previous expression collapses as all p_i except one vanish

$$\hat{\rho}_{pure} = |\psi(\theta,\phi)\rangle\langle\psi(\theta,\phi)|. \tag{2.4}$$

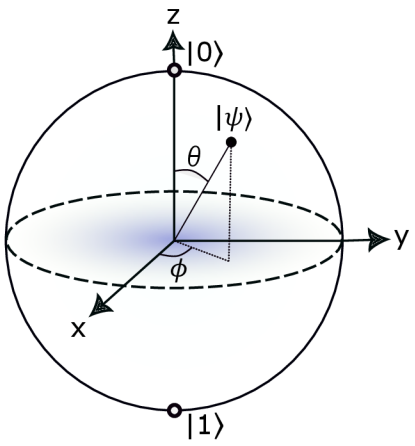


Figure 2.1: Bloch sphere representing qubits. The opposite poles of the sphere usually correspond to the basis vectors $|0\rangle$, $|1\rangle$, but the choice is arbitrary. Points on the surface of the sphere represent pure states, and the points inside the sphere represent mixed states.

Multiqubit states

We can generalize everything presented so far for systems involving two or more qubits. One possible choice of basis states of the two-qubit Hilbert space $\mathcal{H}_2 = \mathbb{C}^4$ is given by the tensor product of the basis states of the single-qubit Hilbert space $\mathcal{H} = \mathbb{C}^2$

$$\begin{aligned} |00\rangle &= |0\rangle \otimes |0\rangle, \\ |01\rangle &= |0\rangle \otimes |1\rangle, \\ |10\rangle &= |1\rangle \otimes |0\rangle, \\ |11\rangle &= |1\rangle \otimes |1\rangle. \end{aligned} \tag{2.5}$$

This basis is called the two-qubit computational basis, just as $\{|0\rangle, |1\rangle\}$ is called the single-qubit computational basis.

A general pure two-qubit state is given by a superposition of basis states

$$|\psi\rangle_{1,2} = C_{00}|00\rangle + C_{01}|01\rangle + C_{10}|10\rangle + C_{11}|11\rangle, \tag{2.6}$$

with complex coefficients that must satisfy $|C_{00}|^2 + |C_{01}|^2 + |C_{10}|^2 + |C_{11}|^2 = 1$.

Analogously for N-qubits, we have a computational basis given by

$$\begin{aligned} |00\ldots0\rangle &= |0\rangle^{\otimes N} = |0\rangle_1 \otimes |0\rangle_2 \otimes \cdots \otimes |0\rangle_N, \\ |00\ldots1\rangle &= |0\rangle_1 \otimes |0\rangle_2 \otimes \cdots \otimes |1\rangle_N, \\ &\vdots \\ |11\ldots1\rangle &= |1\rangle^{\otimes N} = |1\rangle_1 \otimes |1\rangle_2 \otimes \cdots \otimes |1\rangle_N. \end{aligned} \tag{2.7}$$

The N-qubit pure state can be expressed using the relation

$$|\psi\rangle_{1,2,\ldots,N} = \sum_{i_1 i_2 \ldots i_N \in \{0,1\}} C_{i_1 i_2 \ldots i_N} |i_1 i_2 \ldots i_N\rangle, \tag{2.8}$$

with complex coefficients that must satisfy $\sum_{i_1 i_2 \ldots i_N} |C_{i_1 i_2 \ldots i_N}|^2 = 1$.

A mixed N-qubit state is described by a density operator expressed by an incoherent sum of pairwise orthogonal pure states

$$\hat{\rho} = \sum_{i=1}^{2N} p_i |\psi_i\rangle\langle\psi_i|, \tag{2.9}$$

with $p_i \geq 0$ and $\sum_{i=1}^{2N} p_i = 1$.

2.1.1 Single-qubit characterization

There are two important quantities that are frequently used for single-qubit states characterization. The first one is **fidelity** $\mathcal{F}$, which quantifies how close two quantum states are to each other. It is a measure of the distance between two density operators $\hat{\rho}, \hat{\sigma}$ expressed as

$$\mathcal{F}(\hat{\rho}, \hat{\sigma}) = \mathrm{Tr}\left[\sqrt{\sqrt{\hat{\sigma}}\hat{\rho}\sqrt{\hat{\sigma}}}\right]^2 = \mathrm{Tr}\left[\sqrt{\sqrt{\hat{\rho}}\hat{\sigma}\sqrt{\hat{\rho}}}\right]^2 = \mathcal{F}(\hat{\sigma}, \hat{\rho}), \tag{2.10}$$

where Tr denotes the trace, which is the sum of the diagonal terms of the density matrix[1]. If one of the states is pure, i.e., $\hat{\rho} = |\psi\rangle\langle\psi|$, then fidelity takes the form

$$\mathcal{F}(\hat{\rho}, \hat{\sigma}) = \mathrm{Tr}[\hat{\sigma}\hat{\rho}] = \langle\psi|\hat{\sigma}|\psi\rangle. \tag{2.11}$$

The second one is **purity** $\mathcal{P}$, which tells us how close the states are to the surface of the Bloch sphere, i.e., how pure they are. It can be expressed as

$$\mathcal{P}(\hat{\rho}) = \mathrm{Tr}[\hat{\rho}^2]. \tag{2.12}$$

For pure states, the purity is equal to 1, for completely mixed states in the case of a single-qubit d-dimensional system, the purity is $\mathcal{P}_{min} = 1/d$.

[1] The trace of a square matrix that is the product of two real matrices can be rewritten as the sum of the products of their elements $\sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}b_{ij}$.

2.1.2 Quantum gates

Devices that perform operations on qubits are called quantum gates [B1]. In any specific basis, the operators can be represented by square matrices (the chosen one is usually the computational basis). For n qubits, we get $2^n \times 2^n$ matrices. Some quantum logic gates are analogous to classical ones. Unlike classical gates, quantum gates are capable of working with quantum superpositions. In addition, there are quantum gates that do not have a classical counterpart. In the following, we present the elementary unitary[2] quantum logic gates using unitary operators as well as matrix representations in the computational basis.

Identity gate

An identity gate is an identity matrix expressed for a single-qubit as

$$\hat{U}_I = \hat{\mathbb{1}} = |0\rangle\langle 0| + |1\rangle\langle 1| \quad \rightarrow \quad I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \tag{2.13}$$

It does not modify the quantum state. The main importance of this gate lies in the mathematical description of the results of various operations performed with other gates.

Pauli gates

Pauli gates X, Y, Z are given by three Pauli operators $\hat{\sigma}_x$, $\hat{\sigma}_y$, $\hat{\sigma}_z$ and for a single-qubit are expressed as follows

$$\hat{U}_X = \hat{\sigma}_x = |0\rangle\langle 1| + |1\rangle\langle 0| \quad \rightarrow \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \tag{2.14}$$

$$\hat{U}_Y = \hat{\sigma}_y = i|1\rangle\langle 0| - i|0\rangle\langle 1| \quad \rightarrow \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \tag{2.15}$$

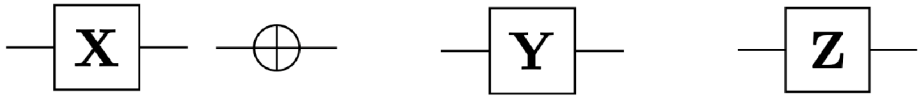
$$\hat{U}_Z = \hat{\sigma}_z = |0\rangle\langle 0| - |1\rangle\langle 1| \quad \rightarrow \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{2.16}$$

Pauli gates are rotations around the x, y, and z axes of the Bloch sphere by π rad. The Pauli X gate is equivalent to the classical logic NOT gate with respect to $\{|0\rangle, |1\rangle\}$ basis. It is also called a *bit-flip* because it maps $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $|0\rangle$. Similarly, the Pauli Y gate maps $|0\rangle$ to $i|1\rangle$ and $|1\rangle$ to $-i|0\rangle$, and the Pauli Z

[2] Any two points on the surface of the Bloch sphere, i.e., two pure qubit states, can be mapped to each other by a reversible operation $\hat{U}$. Such a transformation satisfying the condition $\hat{U}^\dagger\hat{U} = \hat{U}\hat{U}^\dagger = \hat{\mathbb{1}}$ is called unitary.

gate leaves $|0\rangle$ unchanged and maps $|1\rangle$ to $-|1\rangle$, hence it is sometimes called a *phase-flip*.

A quantum circuit using quantum gates can be easily visualized using quantum circuit diagrams. Such diagrams for Pauli operators are shown in Fig. 2.2. And in Fig. 2.3, we can see the circuit diagram for a measurement in a computational basis.



(a) $\hat{\sigma}_x$ gate (NOT gate) **(b)** $\hat{\sigma}_y$ gate **(c)** $\hat{\sigma}_z$ gate

Figure 2.2: Circuit diagrams of Pauli gates.

Pauli operators together with the identity operator satisfy relations

$$\hat{\mathbb{1}} = \hat{\sigma}_x^2 = \hat{\sigma}_y^2 = \hat{\sigma}_z^2, \qquad \mathrm{Tr}[\hat{\sigma}_j \hat{\sigma}_k] = 2\delta_{ij}, \tag{2.17}$$

and since they form an operator basis, we can express any operator $\hat{A}$ as their linear combination

$$\hat{A} = \sum_j a_j \hat{\sigma}_j, \tag{2.18}$$

where $\hat{\sigma}_0 = \hat{\mathbb{1}}$.

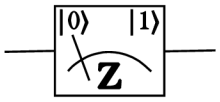


Figure 2.3: Circuit diagram of a measurement in a computational basis.

Phase-shift gates

Single qubit gates mapping $|0\rangle$ to $|0\rangle$ and $|1\rangle$ to $\mathrm{e}^{i\phi}|1\rangle$. The probability of measuring $|0\rangle$ or $|1\rangle$ does not change when applying these gates, but the phase of the given quantum state is modified. More specifically, it is a rotation around the z-axis of the Bloch sphere by ϕ rad, where ϕ is a given phase-shift with a period of 2π. Their matrix has the following general form

$$\hat{U}_{P_\phi} = |0\rangle\langle 0| + \mathrm{e}^{i\phi}|1\rangle\langle 1| \quad \rightarrow \quad P_\phi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix}. \tag{2.19}$$

Depending on the value of ϕ, we get different phase gates. For example, T-gate with $\phi = \pi/4$, S-gate with $\phi = \pi/2$ often used for a SWAP gate, or Pauli Z gate with $\phi = \pi$. All these gates can be expressed together using equation $T = \sqrt{S} = \sqrt[4]{Z}$.

An example circuit diagrams for the S and T gates are shown in Figure 2.4.

(a) S gate **(b)** T gate

Figure 2.4: Circuit diagram of S gate (a) and T gate (b).

Hadamard gate

Hadamard gate H is defined for a single-qubit as

$$\hat{U}_H = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)|0\rangle + \left(\frac{|1\rangle - |0\rangle}{\sqrt{2}}\right)|1\rangle \quad \rightarrow \quad H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{2.20}$$

This gate maps $|0\rangle$ to $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|1\rangle$ to $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$. It means that it creates a balanced superposition of the quantum state if the quantum state is from the computational basis. In Bloch sphere formalism, Hadamard gate performs a rotation around the axis $(x + z)/\sqrt{2}$ by π rad and changes the basis. For example, $HZH = X$ swaps z-basis to x-basis.

Figure 2.5: Circuit diagram of Hadamard gate.

Multi-qubit gates

These gates operate on multiple qubits simultaneously and some enable entanglement creation. They are the basic building blocks for the construction of quantum circuits. Some of them are simple to implement and are composed of single-qubit gates. The more complex gates then use the less complex ones for their construction. Multi-qubit gates include, for example, controlled gates or a SWAP gate. Some of the gates we discuss below.

1) Controlled gates

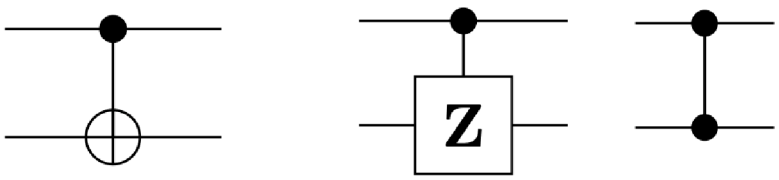
These gates operate on two or more qubits, where at least one qubit plays the role of controlling some operations. For example, a CNOT gate, also known as a CX, operates on two qubits and acts as a NOT operation on the second qubit only when the first qubit is in the state $|1\rangle$. Otherwise, it does nothing.

Since this gate acts on at least two qubits, the minimal computational basis available to us is for two qubits and takes the form $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. Now, we can express the CNOT gate as

$$\hat{U}_{\text{CNOT}} = |0\rangle\langle 0| \otimes \hat{\mathbb{1}} + |1\rangle\langle 1| \otimes \hat{\sigma}_x \quad \rightarrow \quad \text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \tag{2.21}$$

Similarly, the CZ gate introduces a π phase shift if and only if both qubits are in state $|1\rangle$.

$$\hat{U}_{\text{CZ}} = |0\rangle\langle 0| \otimes \hat{\mathbb{1}} + |1\rangle\langle 1| \otimes \hat{\sigma}_z \quad \rightarrow \quad \text{CZ} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}. \tag{2.22}$$



(a) CNOT gate **(b)** CZ gate

Figure 2.6: Circuit diagrams of CNOT gate (a) and CZ gate (b).

In general, unitary operation of controlling gates can be written as $\hat{U}_c = |0\rangle\langle 0| \otimes \hat{\mathbb{1}} + |1\rangle\langle 1| \otimes \hat{U}$ and acts as a $\hat{U}$ operation on the second qubit only when the first qubit is in the state $|1\rangle$. The circuit diagrams of CNOT and CZ gates are shown in Fig. 2.6 and the general circuit diagram for unitary controlled gates is shown in Fig. 2.7

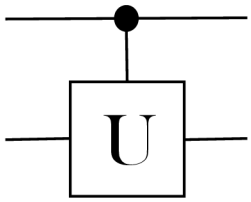


Figure 2.7: Circuit diagram of a general unitary controlled gate.

Toffoli gate

It is a 3-bit entangling gate that is universal for classical computing, but not for quantum computing. A quantum Toffoli gate is defined for three qubits and acts as a CNOT gate with two control qubits and one target qubit. Assuming we only have input qubits in states $|0\rangle$ or $|1\rangle$, then if the first two qubits are in the state $|1\rangle$, a Pauli X gate is applied to the third qubit (CCNOT gate). Otherwise the gate does nothing. Its circuit diagram is shown in Fig. 2.8.

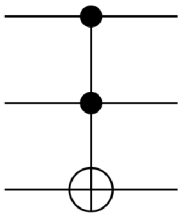


Figure 2.8: Circuit diagram of Toffoli gate.

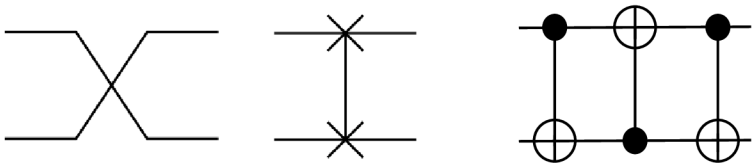
Tomographic characterization of linear optical quantum Toffoli gate implemented by interference of photons on a partially polarizing beam splitter inserted inside a Mach-Zehnder interferometer is reported in Ref. [79]. A simplification and a demonstration of Toffoli gate is in Ref. [19].

2) SWAP gate

SWAP gate operates on two qubits. As its name suggests, when it is used, the given two qubits are swapped. Using the computational basis for two qubits, we can express the SWAP gate as

$$\hat{U}_{\mathrm{SWAP}} = |00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11| \quad \rightarrow \quad \mathrm{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \tag{2.23}$$

We can build the SWAP gate from three consecutive CNOT gates, and an operation that swaps two qubits can then be performed without the need to measure the qubits [B1]. Circuit diagrams of SWAP gate are shown in Fig. 2.9.



(a) **(b)**

Figure 2.9: Two common circuit diagrams of SWAP gate (a), and a circuit diagram of SWAP gate built from three consecutive CNOT gates (b).

The experimental implementation and full tomographic characterization of deterministic high-fidelity SWAP gate for two photonic qubits is reported in Ref. [80]. Implementation of a SWAP gate using linear optics can be found in Ref. [81].

2.1.3 Polarization and spatial encoding

We can implement qubits in many different physical systems. We need an object which exhibits quantum properties. We can use, for example, atoms and ions, other options are NV centres and quantum dots, or superconducting circuits. The most important variant for us is the realization of a qubit using photons. A qubit of information can be encoded in any of several degrees of freedom [82]—polarization, orbital angular momentum [83], time [84] or frequency [85]. Each degree of freedom offers different advantages in solving various problems, be it stability, control or scalability. Encoding a qubit into two modes of a single photon enables long-distance quantum communication. In this thesis, we utilize encoding to polarization and spatial modes.

Polarization encoding

Using the computational basis for one qubit, we can assign a logic value 0 to the horizontal polarization $|H\rangle \equiv |0\rangle$ and a logic value 1 to the vertical polarization

$|V\rangle \equiv |1\rangle$ of a photon. Any other polarization state can be expressed by a linear combination (superposition) of these two mentioned polarization states. The linear combination is given by Eq. (2.1).

When introducing the qubit in Section 2.1, three eigenvectors defining the axes of the Bloch sphere were given, and thus we could determine three different projection measurements on pairs of orthogonal vectors related to each axis. In the case of polarization states, we also have a total of six projections: three pairs of orthogonal vectors related to the individual axes of the Poincaré sphere plotted in Fig. 2.10. In addition to the already mentioned polarization states of horizontal $|H\rangle$ and vertical $|V\rangle$ polarization, we also have diagonal $|D\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$ and anti-diagonal $|A\rangle = (|H\rangle - |V\rangle)/\sqrt{2}$ polarization states, and right-handed circular $|R\rangle = (|H\rangle + i|V\rangle)/\sqrt{2}$ and left-handed circular $|L\rangle = (|H\rangle - i|V\rangle)/\sqrt{2}$ polarization states. These three pairs of states form a set of mutually unbiased bases encoded in polarization.

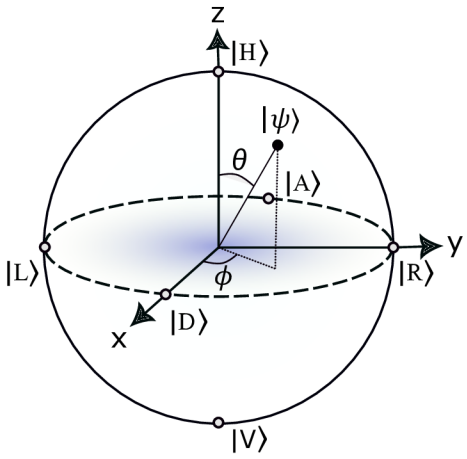


Figure 2.10: Pure polarization states on the surface of the Poincaré sphere. The unplotted partially polarized states lie inside the Poincaré sphere.

To manipulate the polarization state, we generally use birefringent optical components. For example, single-qubit operations can be directly implemented using waveplates, which realize rotation in polarization space. Individual polarization states, their evolution, and the effects of polarization components can be represented by points on the Poincaré sphere. On this sphere, the polarization states are described by vectors in Jones or Stokes formalism (see [B2]- Chapter 6). In this case, the Poincaré sphere is the same object as the Bloch sphere shown in Fig 2.1. The advantages of this encoding in experiments are mainly simple preparation, manipulation and measurement of individual polarization states.

Spatial encoding

While only one spatial mode was used in the polarization encoding, in a spatial encoding, a qubit of information is encoded in a superposition across two spatial modes. We can rewrite the superposition from Eq. (2.1) as

$$|\psi\rangle = \alpha|1,0\rangle + \beta|0,1\rangle, \tag{2.24}$$

where $|i,j\rangle$ is a two-mode state with i (j) photons in the first (second) spatial mode. The Fock state $|1,0\rangle$ ($|0,1\rangle$) corresponding to the state $|0\rangle$ ($|1\rangle$) describes that there is one photon in mode 0 (1) and none in mode 1 (0).

Polarization and spatial encoding can be easily interchanged in experiments using polarizing beam splitters, which separate two orthogonal polarization components into two different spatial modes. We encounter both types of encoding if, for example, we have an interferometer in the experiment. This encoding is well compatible with photonic integrated circuits [86, 87] and, for example, can be used to generate entangled states [88].

2.1.4 Two-photon interference

Two-photon interference is a very important phenomenon that is purely quantum in nature. Its importance lies in the ability to improve the accuracy of measurements, to help overcome the limits of classical computations, to use it in quantum communication or in its possibility to demonstrate the indistinguishability of photons [89]. To describe the effect of two-photon interference, also known as the Hong-Ou Mandel effect [90], we must first look at the behaviour of photons at a beam splitter (BS). BS is a device with two input ports, usually labelled a and b, and two output ports labelled c and d. See Fig. 2.11.

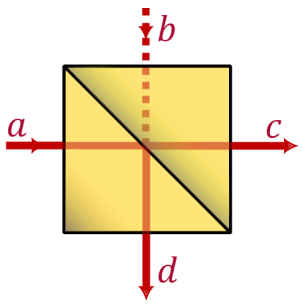


Figure 2.11: Beam splitter with two input (a,b) and two output (c,d) ports.

Now, consider a lossless BS. If the light beam passes through port a or b, it is split according to the given splitting ratio of the BS into two beams that exit

ports c and d. This splitting ratio is described by the complex parameters r and t, known as the BS reflectance and transmittance, which satisfy the condition $|t|^2 + |r|^2 = 1$.

The quantum description of the BS according to the second quantization formalism is given by using a set of bosonic operators known as annihilation $\hat{a}_i$ and creation $\hat{a}_i^\dagger$ operators representing electromagnetic fields in mode i. These operators satisfy the bosonic commutation relation $[\hat{a}_i, \hat{a}_j^\dagger] = \delta_{ij}$, where δ_{ij} is the Kronecker delta. In this approach $\hat{a}, \hat{b}, \hat{c}$, and $\hat{d}$ represent annihilation operators in modes a, b, c, and d of input and output ports of BS, respectively. Now, we can write the BS operation represented by unitary matrix U_{BS} using these field operators

$$\begin{pmatrix} \hat{c} \\ \hat{d} \end{pmatrix} = U_{BS} \begin{pmatrix} \hat{a} \\ \hat{b} \end{pmatrix}, \quad U_{BS} = \begin{pmatrix} \sqrt{T} & e^{i\phi}\sqrt{R} \\ -e^{-i\phi}\sqrt{R} & \sqrt{T}, \end{pmatrix}$$

where $T = |t|^2$, $R = |r|^2$, ϕ is phase shift usually taken as $\pi/2$ or 0.

In this work, we consider $\phi = 0$ and the balanced option where $r = t = 1/\sqrt{2}$. We can express the annihilation operators describing the input ports of the BS by the output ones

$$\hat{a} = \frac{1}{\sqrt{2}}(\hat{c} + \hat{d}), \tag{2.25}$$

$$\hat{b} = \frac{1}{\sqrt{2}}(\hat{c} - \hat{d}). \tag{2.26}$$

Suppose we have two photons at two different BS inputs that are distinguished by polarization, the initial state can be expressed as

$$|\psi_{in}\rangle = |H\rangle_a |V\rangle_b = \hat{a}_H^\dagger \hat{b}_V^\dagger |0\rangle, \tag{2.27}$$

where $|0\rangle$ is a Fock state known as a vacuum state $|vac\rangle$.

The output state changed by the BS transformation can be written using Eq.(2.25) and Eq. (2.26) as

$$\hat{a}_H^\dagger \hat{b}_V^\dagger |0\rangle \xrightarrow{\text{BS}} \frac{1}{2}(\hat{c}_H^\dagger + \hat{d}_H^\dagger)(\hat{c}_V^\dagger - \hat{d}_V^\dagger)|0\rangle = \frac{1}{2}(\hat{c}_H^\dagger \hat{c}_V^\dagger - \hat{c}_H^\dagger \hat{d}_V^\dagger + \hat{c}_V^\dagger \hat{d}_H^\dagger - \hat{d}_H^\dagger \hat{d}_V^\dagger)|0\rangle. \tag{2.28}$$

From this equation we can see that two cases can happen at BS with the same probability:

- Two photons exit the BS together through the same output port c or d. This behaviour is described by the first term and the fourth term in parentheses.

- Two photons exit the BS separately through two different ports c and d. This behaviour is described by the second term and the third term in parentheses.

However, if we assume that we have indistinguishable photons at the BS inputs, the resulting situation will change. The initial state is the same as in Eq. (2.27), only we will no longer write the indices distinguishing the polarization of the photons. The output state has the form

$$\begin{aligned} \hat{a}^\dagger \hat{b}^\dagger |0\rangle &\xrightarrow{\text{BS}} \frac{1}{2}(\hat{c}^\dagger \hat{c}^\dagger - \hat{c}^\dagger \hat{d}^\dagger + \hat{c}^\dagger \hat{d}^\dagger - \hat{d}^\dagger \hat{d}^\dagger)|0\rangle \\ &= \frac{1}{2}((\hat{c}^\dagger)^2 - (\hat{d}^\dagger)^2)|0\rangle \\ &= \frac{1}{\sqrt{2}}(|2\rangle_c - |2\rangle_d), \end{aligned} \tag{2.29}$$

where the last expression arose from the action of the creation operator on the vacuum state $(\hat{a}_i^\dagger)^n|0\rangle = \sqrt{n!}|n\rangle_i$. The result tells us that both photons go together each time either through the output port c or d of the BS. This situation corresponds to a state where there is constructive interference on one BS output port and destructive interference on the other. This phenomenon is called bunching.

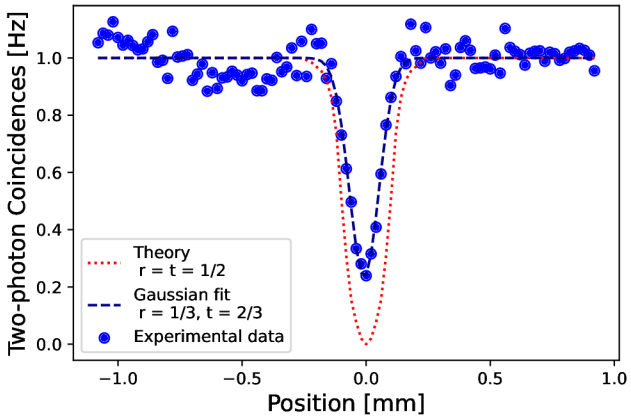


Figure 2.12: HOM dip. The red dotted line is the theoretical dip curve for the balanced beam splitter (BS). We can see that the curve goes from a maximum of 1 to a minimum of 0. For illustration, we plotted a curve for an unbalanced BS. Typical behaviour is shown by the blue points representing directly measured data from our experiment. These data are fitted with a Gaussian function marked by the blue dashed line. In this case, the measured coincidences reach the minimum value at the same position as the theoretical curve for the balanced BS, but the minimum value is no longer zero.

Such behaviour can be experimentally measured by changing the degree of indistinguishability of photons. This can be achieved by changing the polarization state of one input photon or more likely by delaying one photon from a given pair, for example, by extending its path inside the interferometer. Only cases where coincidences were observed, i.e., both detectors detected the arrival of a photon simultaneously, are measured. The resulting graph, also known as HOM dip, is the dependence of the coincidence rate on the temporal delay and it is shown in Fig. 2.12.

2.1.5 Quantum state tomography

Results from experimental measurements in quantum physics are affected by fluctuations. However, knowledge of the quantum state makes it possible to predict the statistical results of a measurement performed on a set of identically prepared systems. To determine the quantum state, we use a method known as quantum state reconstruction or quantum state tomography.

Among the experimenters, from the various proposed algorithms, two approaches came to the fore:

- *Linear inversion*, since the statistics of the measurement results is a linear function of the density matrix $\hat{\rho}$. Thus, the density matrix can be obtained by solving a system of several linear equations.
- *Maximum Likelihood* or simply *MaxLik*, which allows among all possible density matrices to find the one that maximizes the probability of obtaining a given set of experimentally measured data.

Both methods allow the inclusion of experimental imperfections in the calculation, such as the reduced efficiency of the detectors. The disadvantage of linear inversion is that statistical and systematic errors of quantum measurements manifest themselves directly in the density matrix, which can lead to unphysical results. For example, when measuring the polarization state, a density matrix is determined from the measured data, from which it is possible to determine the state purity $\mathcal{P}$ defined in Eq. (2.11). If the source of light fluctuates and we assume $\langle\hat{\sigma}_x\rangle = \langle\hat{\sigma}_y\rangle = 1$, the purity may be greater than one, which is an unphysical result. Such a case does not occur if we use MaxLik. Its other advantage is that it allows the implementation of some additional known information about the density matrix into the reconstruction procedure. In this thesis, we only give a brief description of this method. The theory and mathematical derivation of MaxLik can be found in Refs. [91–93], and the implementation into a Python code is reported in Ref. [94].

Let N be the total number of repeated measurements of a particle (photon) that is detected in one of the j outputs of our experiment. Our measurement is described by a set of positive operators $\hat{\Pi}_j$ known as POVMs for which $\hat{\Pi}_j \geq 0$ and $\sum_j \hat{\Pi}_j = \hat{\mathbb{1}}$. Let f_j be the relative number of occurrences of each measurement result $\hat{\Pi}_j$, where $\sum_j f_j = 1$. The likelihood function of the quantum state $\hat{\rho}$ is given by the relation

$$\mathcal{L}(\hat{\rho}) = \Pi_j p_j^{f_j}, \tag{2.30}$$

where $p_j = \mathrm{Tr}[\hat{\Pi}_j \hat{\rho}]$ is a propability of each outcome. The goal is to find the density matrix that maximizes the likelihood function.

We can consider POVM elements corresponding to measurement $\hat{\Pi}_j = |y_j\rangle\langle y_j|$ and after logarithming Eq. (2.30) we get

$$\ln \mathcal{L}(\hat{\rho}) = \sum_j f_j \ln \langle y_j|\hat{\rho}|y_j\rangle. \tag{2.31}$$

Here we can neglect the multiplicative factors, because they do not affect the maximization of the function.

The density matrix $\hat{\rho}$ that maximizes the likelihood function satisfies the equation [91]

$$\hat{R}\hat{\rho} = \hat{\rho}, \tag{2.32}$$

where $\hat{R} = \sum_j f_j \frac{|y_j\rangle\langle y_j|}{\langle y_j|\hat{\rho}|y_j\rangle}$

It is important to note that the likelihood function maximization may not give a result that correctly describes the quantum system. In general, the relation $\mathrm{Tr}[\hat{\rho}] = 1$ may not hold. This situation is treated using an undetermined Lagrange multiplier λ, where $\hat{R}\hat{\rho} = \lambda\hat{\rho}$. After applying the normalization condition (that is in this text already included in $\hat{R}$), we get $\lambda = 1$ and again Eq. (2.32).

However, it is analytically very difficult or even impossible to solve Eq. (2.32). In addition, the left side of this equation does not represent a Hermitian operator. The solution is to rewrite the equation in the following form [92]

$$\hat{R}\hat{\rho}\hat{R} = \hat{\rho}. \tag{2.33}$$

There are now positive semidefinite operators on both sides of the equation.

Now, we can find the density matrix that maximizes the likelihood function by successive iterations

$$\hat{\rho}_{j+1} = \frac{\hat{R}_j\hat{\rho}_j\hat{R}_j}{\mathrm{Tr}[\hat{R}_j\hat{\rho}_j\hat{R}_j]}, \tag{2.34}$$

where we can start our estimation from $\hat{\rho}_0 = \hat{\mathbb{1}}/2$ and stop when we reach our desired value ϵ, for example using the trace: $\mathrm{Tr}[|\hat{\rho}_{j+1} - \hat{\rho}_j|^2] < \epsilon$.

2.1.6 Entanglement

Quantum entanglement is one of the characteristic features of quantum mechanics that does not occur in classical mechanics. It is also considered an important resource and its use can be found, for example, in quantum teleportation [12, 13, 95], in some protocols of quantum cryptography [10, 75, 96] or in superdense coding [14, 97]. Entanglement occurs between two or more particles. In this work, we only deal with photons. They can be entangled in their polarization [98, 99], frequency [100], momentum [101, 102], time (time bins) [43, 103], orbital angular momentum (OAM) [39], or any combination of all the mentioned options, which is called hyper-entanglement [104–106].

If we consider two or more qubits, then due to the superposition principle, there are quantum states, either pure or mixed, which cannot be expressed simply by a tensor product, as we mentioned in Section 2.1 - Multiqubit States. Thus, for some pure states, we are not able to write

$$|\psi\rangle_{1,2} \neq |\phi\rangle_1 \otimes |\xi\rangle_2, \tag{2.35}$$

and similarly for some mixed states

$$\hat{\rho} \neq \sum_i p_i \hat{\rho}_{1,i} \otimes \hat{\rho}_{2,i}, \tag{2.36}$$

where $p_i \geq 0$. These states are not separable and they are called entangled.

There are different levels of separability. The state may be separable, separable with respect to given subgroups, or inseparable. N-qubit state $\hat{\rho}$ is called k-separable, if it can be written in the following decomposition

$$\hat{\rho} = \sum_i p_i \otimes_{n=1}^{k} (\hat{\rho} S_n)_i,$$

where $\otimes_{n=1}^{k}(\hat{\rho} S_n)_i$ is the tensor product of k density matrices for chosen partition $\{S_1, S_2, \ldots, S_k\}$ into k disjoint nonempty subsets with $k \leq N$.

These different levels of separability give rise to a hierarchy of separable states. For $k = 1$, the states are called genuinely n-partite entangled and $\hat{\rho} \neq \sum_i p_i \otimes_{n=1}^{k} (\hat{\rho} S_n)_i$. For $k > 1$, the states are k-separable and specifically, for $k = 2$, the states are called biseparable and they can be factorized into two subsystems. Finally, for $k = N$, the states are called separable or classical.

A multipartite quantum state can be shared by several parties, which are allowed to act locally on their subsystems by performing measurements and general quantum operations. In order to improve the measurement results, these participants can communicate freely via the classical channel and tell each other, for example, the results of their previous measurements. The whole process is

known as local operations with classical communication (LOCC). It enables the study of quantum correlations and other nonlocal quantum effects. Using LOCC, we can also deterministically transform a maximally entangled bipartite state into any other quantum state when considering a bipartite system [107].

Degradation of entanglement occurs when entangled particles pass through the environment (decoherence), or if at least one of the particles of the entangled pair is detected [108, 109].

The next two Sections in this work deal with some criteria and measures of entanglement, which, together with others, can be found in Ref. [110].

Entanglement detection

If we want to determine that we have an entangled state in an experiment, we need to use one of the entanglement criteria. Such a criterion will tell whether the state is entangled or not. However, it says nothing about how much the systems are entangled.

Historically, the first criterion was *Bell's inequalities*, which originally served to verify the EPR paradox. This criterion makes it possible to decide whether the local hidden variable is consistent with quantum mechanics or whether it is possible to disprove this theory. Measurement statistics (measurement outputs) are bound by Bell's inequalities. These inequalities are violated by entangled states. However, any separable state does not lead to their violation. In addition, not all entangled states lead to Bell's inequalities violation. We can only identify some of them. Among the most famous Bell's inequalities is the Clasuer-Horne-Shimony-Halt (CHSH) inequality [111].

One of the most used criteria is the *positive partial transpose (PPT)* criterion. It serves for detecting entanglement between two qubits. It is based on the partial transposition of the density matrix. Let us have binary parameterized inputs of the density matrix

$$\hat{\rho} = \sum_{i,j\in\{0,1\}} \sum_{k,l\in\{0,1\}} \rho_{ij,kl} |i\rangle\langle j| \otimes |k\rangle\langle l|.$$

Then the partial transpose with respect to the first qubit $\hat{\rho}^{T_1}$ is defined as

$$\hat{\rho}^{T_1} = \sum_{i,j\in\{0,1\}} \sum_{k,l\in\{0,1\}} \rho_{ij,kl} |j\rangle\langle i| \otimes |k\rangle\langle l|.$$

Similarly for $\hat{\rho}^{T_2}$, where we replace the index k with l.

A state is said to have a partial transposition, or to be a PPT if it has **no** negative eigenvalue after partial transposition. But if it has at least one negative eigenvalue, then the given state is entangled.

The main disadvantage of the PPT criterion is that it requires complete information about the quantum state, which is obtained from quantum tomography.

The criterion that does not need full knowledge of the quantum state is an *entanglement witness*. The main idea of the witness lies in the fact that separable states form a convex subset in the state space. The witness is the operator $\hat{W}$, which defines a hyperplane dividing the state space into two half-planes. The first half-plane contains all separable states, and the other one contains entangled states. It holds that $\mathrm{Tr}[\hat{W}\hat{\rho}_{sep}] > 0$ for all separable states and for $\mathrm{Tr}[\hat{W}\hat{\rho}] < 0$ the given $\hat{\rho}$ is entangled, see Fig. 2.13. The theory regarding witnesses and experimental implementation can be found in [112, 113].

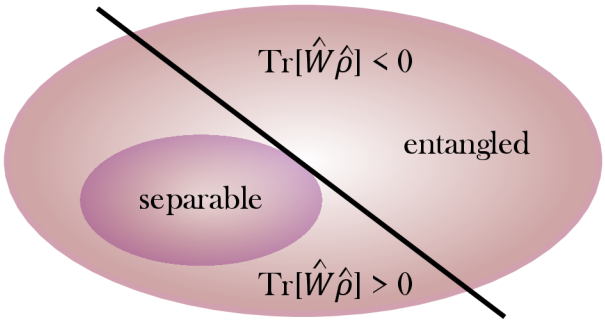


Figure 2.13: An entanglement witness dividing the state space into two half-planes. One contains only entangled states, and the other contains all separable and some entangled states.

Entanglement measures

Measures of entanglement are used to quantify the amount of entanglement of a state defined on a composite Hilbert space $\mathcal{H}$. A quantity can be called the entanglement measure $E(\rho)$ only if it fulfils the following requirements

1. $E(\hat{\rho}_{sep}) = 0$ for all separable states,
2. $E(\hat{\rho})$ cannot be increased using LOCC operations,
3. $E(\hat{\rho})$ is not changed with an action of local unitary operations LU.

Sometimes, due to certain advantages, two more conditions are added, but they are not necessary. These are convexity $E(\sum_k p_k\hat{\rho}_k) \leq \sum_k p_k E(\hat{\rho}_k)$ and additivity $E(\hat{\rho}^{\otimes N}) = NE(\hat{\rho})$, where $\hat{\rho}^{\otimes N}$ represents N-copies of $\hat{\rho}$.

Measures of entanglement include, for example, entanglement of formation, negativity or concurrence.

Entanglement of formation quantifies how many Bell states, i.e., maximally entangled states, are needed to prepare the given state using local quantum operations and classical communications (LOCC). Measures of entanglement include extremizations, which are often difficult to solve analytically. Despite the fact that for pure states the entanglement of formation (EoF) is defined for all bipartite systems of arbitrary dimension, analytic evaluation of EoF for mixed states is known mainly in two-qubit systems [114].

For a bipartite pure state $\hat{\rho}_p$, the EoF is defined as the von Neumann entropy of the reduced state (the subsystem) $\hat{\rho}_1$

$$E_F(\hat{\rho}_p) = S(\hat{\rho}_2) = S(\hat{\rho}_1) = -\mathrm{Tr}[\hat{\rho}_1 \log_2 \hat{\rho}_1] = -\sum_i \lambda_i^{\hat{\rho}_1} \log_2 \lambda_1^{\hat{\rho}_1}, \tag{2.37}$$

where $\hat{\rho}_p = |\phi_{12}\rangle\langle\phi_{12}|$, $\hat{\rho}_1 = \mathrm{Tr}_2[\hat{\rho}_p] = \sum_{m\in\{0,1\}} \sum_{i,j\in\{0,1\}} \sum_{k,l\in\{0,1\}} \rho_{ij,kl} |i\rangle\langle j| \otimes \langle m|k\rangle\langle l|m\rangle$ is a partial trace over the second qubit and $\lambda^{\hat{\rho}_1}$ are eigenvalues of $\hat{\rho}_1$.

For a bipartite mixed state $\hat{\rho}_m$ definition of EoF is based on 'convex-roof extension' and takes form

$$E(\hat{\rho}_m) = \inf_{p_k, |\phi_k\rangle} \sum_k p_k E(|\phi_k\rangle),$$

where $\hat{\rho}_m = \sum_k p_k |\phi_k\rangle\langle\phi_k|$ and infimum is taken over all pure-state decompositions of $\hat{\rho}_m$. Thus, we can write the mixed state using von Neumann entropy

$$E_f(\hat{\rho}) = \inf_{p_k, |\phi_k\rangle} \sum_k p_k S(\hat{\rho}_{1,k}). \tag{2.38}$$

For bipartite system, we can derive this measure directly from concurrence, which will be discussed below.

Another measure is *negativity*, which is close to the PPT criterion. It quantifies how much the PPT criterion is violated. The definition for two qubits is as follows

$$N(\hat{\rho}) = \frac{1}{2}(||\hat{\rho}^{T_1} - 1||) = \sum_{\lambda_i<0} |\lambda_i|, \tag{2.39}$$

where $||A|| = \mathrm{Tr}[\sqrt{A^\dagger A}]$ is a trace norm A and λ_i are eigenvalues of $\hat{\rho}^{T_1}$, which is the state after partial transposition.

The last measure we mention is *concurrence*. For pure states $|\phi\rangle$, it is defined as

$$C(|\phi\rangle) = \sqrt{2(1 - \mathrm{Tr}[(\hat{\rho}_1)^2])}, \tag{2.40}$$

where $\hat{\rho}_1$ is the state after tracing over the second qubit (we consider only two qubits).

Generalizing the concurrence to mixed states is given by

$$C(\hat{\rho}) = \max(0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4), \tag{2.41}$$

where λ_i are eigenvalues of operator $\hat{R} = \sqrt{\sqrt{\hat{\rho}}(\hat{\sigma}_y \otimes \hat{\sigma}_y)\hat{\rho}^*(\hat{\sigma}_y \otimes \hat{\sigma}_y)\sqrt{\hat{\rho}}}$ in descending order.

Concurrence allows us to express entanglement of formation for two qubits

$$E_F(\hat{\rho}) = h\left(1 + \sqrt{1 - (C(\hat{\rho}))^2}/2\right),$$

where $h(x) = x\log_2 x - (1-x)\log_2(1-x)$ is a binary entropy function also known as Shannon entropy.

There are also other measures of entanglement, including the geometric measure of entanglement (witnesses) quintifying the minimum distance between the entangled state and fully separable states.

Based on individual measures of entanglement, we can also define a maximally entangled state that maximizes a certain measure. If we consider the von Neumann entropy of a bipartite state, then the maximally entangled state is the one that leads to a completely mixed state after a partial trace, i.e., the resulting state has a purity equal to 1/2. For a bipartite system, i.e., a system with two qubits, the maximally entangled states are the so-called Bell states. They form the basis of the composite Hilbert space and are expressed as follows

$$|\phi^{\pm}\rangle = \frac{|00\rangle \pm |11\rangle}{\sqrt{2}}, \tag{2.42}$$

$$|\psi^{\pm}\rangle = \frac{|01\rangle \pm |10\rangle}{\sqrt{2}}. \tag{2.43}$$

2.2 Single and entangled photon sources

As quantum information and quantum communication develop, so do the demands on quantum sources. The single-photon generation and correlated (entangled) photon pairs are increasingly required for many applications. Such generation can be achieved either deterministically ("on demand") or probabilistically. Deterministic sources include, for example, quantum dots [115–117], atoms [118], molecules[119, 120], ions [121] or NV centres in diamonds [122, 123]. Probabilistic sources that use a nonlinear optical process to generate photons include spontaneous parametric down-conversion (SPDC) [99, 124, 125] or four-wave mixing (FWM) [126, 127].

In this work, we describe one deterministic and one probabilistic source in more detail. More specifically, we look at the SPDC, which is used in most of our

experiments to generate correlated pairs, but it can also generate heralded single photons. The second source is based on quantum dots, which are excellent single-photon sources, but we look at their ability to generate polarization-entangled pairs.

2.2.1 Spontaneous parametric down-conversion

SPDC is a non-linear process in which the pump photon is converted into two photons - signal and idler, while the energy and momentum are preserved [128]. Since this process starts from the electromagnetic vacuum fluctuations, which are responsible for the photon conversion, it is a purely quantum process, and the photons created in this way have strong quantum properties.

SPDC can be used for single photon generation, where the detection of one photon from a photon pair indicates the existence of a second photon. In other words, the first photon serves to herald the second one. However, this generation is not "on-demand" because it is a probabilistic process where photons are distributed with a Poisson distribution. This implies some nonzero probability of multiphoton emission. The more we increase the source power, the more likely multiphoton emission will occur. There are some efforts to suppress this probability of multiphoton emission, for example, via the photon-blockade effect [129].

Another property of photons generated in SPDC process, which is widely used in experiments, is their indistinguishability. If we control the coherence length of the generated photon pairs as well as their path, we can achieve indistinguishability in the temporal and spatial modes of photons. The indistinguishability of photons leads to the two-photon interference effect discussed in Section 2.1.4.

The most important use of SPDC is to generate entangled pairs. We discussed entanglement in Section 2.1.6. Entanglement can be created between different degrees of freedom of a photon. However, in this thesis we only deal with polarization entanglement, because our experiments require only correlated photon pairs in polarization.

Main principle

The strong input beam (pump) enters the optically nonlinear medium, while the other modes (signal and idler) are in the vacuum states. In this interaction, the vacuum modes are excited and the resulting generated photon pairs are correlated or entangled with each other.

For this interaction, we need an environment that exhibits a second-order nonlinearity described by the susceptibility $\chi^{(2)}$. Such an environment is, for ex-

ample, an anisotropic crystal. The photon conversion into two less energetic photons requires to fulfil the phase-matching condition. This condition expresses the conservation of momentum. If we have a nonlinear anisotropic crystal, it is possible to meet these conservation laws by properly choosing the polarization of the pump beam and tilting the crystal or controlling its temperature.

According to the polarization state of the pump and to the resulting polarization states of the signal and the idler, we distinguish several types of SPDC:

- Type 0: the pump has the same polarization as the signal and idler.
- Type I: the pump has orthogonal polarization with respect to the signal and idler, which both have the same polarization.
- Type II: signal and idler have orthogonal polarization.

However, there are materials for which it is impossible or very difficult to meet the condition of phase matching. For example, in a crystal, this could be due to insufficient or no birefringence to compensate for the dispersion of a material. For shorter wavelengths, this birefringence and dispersion compensation becomes more of a problem. This is due to the refractive index of the material, which tends to increase rapidly with frequency, while the birefringence remains nearly constant [130].

For materials with low birefringence, we can use a method called quasi-phase-matching to improve the efficiency of the nonlinear process. This method is based on creating such a crystal structure that the orientation of one crystal axis is periodically inverted depending on the position in the crystal. This structure is called periodically-poled and the orientation of the crystal axis is inverted after the propagation over the so-called coherence length, i.e., the distance along which the nonlinear process still proceeds constructively.

In this thesis we use the source described in [1]. It is a particular collinear degenerate type II scheme where three waves interact in a nonlinear periodically poled crystal. The pump is polarized and has an extraordinary linear polarization, and two beams of light arising in a nonlinear environment have one ordinary and the other extraordinary polarization, while their spectral and spatial modes are entangled.

2.2.2 Quantum dots

Quantum dots (QDs) are nanocrystals of a semiconducting material with diameters in the range of a few nanometers. Since the dimensions of QDs are very

small, the optical properties, such as the frequency of emitted light, depend on the size of these nanocrystals. If the dimension of the material is larger than the wavelength of the observed particle, then the particle behaves as if it were not constrained by anything. When the dimension of the material decreases, we start to observe a quantum confinement effect, and the energy required to activate electrons inside QDs increases. This effect leads to a blue shift in the emission of radiation, see Fig. 2.14. If the size reduction of particles inside the material reaches a certain limit, the quantum confinement effect becomes more observable and the radiation spectrum changes from continuous to discrete. There are three quantum-confined structures classified by their dimensionality. 1-D confined structures are called quantum wells, 2-D confined structures are known as quantum wires, and the last ones are quantum dots with 3-D confinement. In other words, in a quantum dot case, the motion of electrons and holes is quantized in all three dimensions. This 3-D confinement makes the energy spectrum of a single carrier quantized in discrete-level shells [B3].

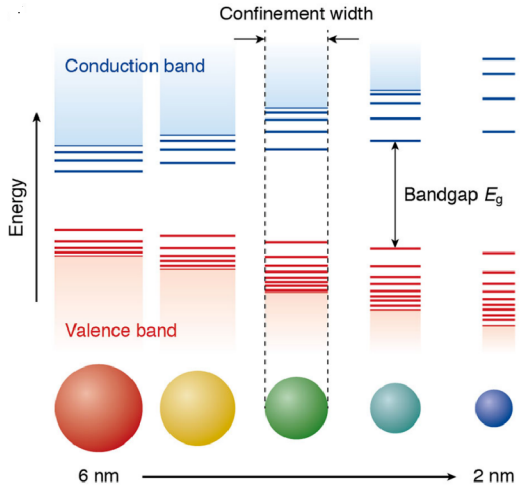


Figure 2.14: Quantum confinment effect. The smaller the QD, the stronger the confinement. The energy required to excite the electron increases and the emission spectrum of the QD shifts to the blue region. This figure is taken from Ref. [131].

Quasiparticles

Absorption of a photon by interband transitions inside QDs creates an electron in the conduction band and a hole in the valence band. The mutual Coulomb interaction between the specific electron and the specific hole can give rise to a new excitation in the QD called exciton (X). This electron-hole pair is bound by

the Coulomb interaction, even though the individual particles are distant from each other. Since the electron-hole pair interaction strength is weak and we can consider QD as a uniform dielectric material, we are in the limit of so-called free excitons, also known as Wannier–Mott excitons [B3]. We can model these quasiparticles by a hydrogen atom and we can apply the Bohr model to calculate, for example, their energy or radius. Analogically to atoms, electrons occupy discrete energy levels and they can be excited to higher energy levels [B3, B4].

The exciton is not the only quasiparticle that can arise from energy absorption. Two excitons can create a quasiparticle called biexciton (XX) or, in some literature, an excitonic molecule, which is the two electron-hole pair state. In addition to these quasiparticles (X, XX) with a neutral charge, there are also charge-carrying excitons, so-called trions ($X^{\pm}$). They consist of two electrons and one hole or vice versa [B5]. The Coulomb interactions among electrons and holes of all mentioned quasiparticles are plotted in Fig 2.15. We will discuss these quasiparticles more in the next section.

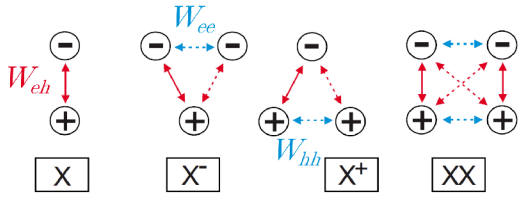


Figure 2.15: Coulomb interaction among electrons and holes. Main forces are marked by solid lines, additional ones by dashed lines. This figure is taken from Ref. [132].

Symmetries and electronic states

A **free** electron-hole pair can not exist inside a QD kept at low temperatures due to quantum confinement. In addition, there can be a maximum of two electrons on individual energy levels inside a QD due to the Pauli exclusion principle. Excitons can be formed when these electrons are excited into higher energy levels.

Conceptually, as mentioned above, an exciton is similar to a hydrogen atom (one electron orbiting one proton, i.e., a hole, bound together by Coulomb interaction) and therefore we can say that a QD with an electron and a hole in the ground state is in the s-shell. The s-shell is an orbital with a spherical symmetry which can contain only two electrons. Excited states of electrons inside the QD, which can be achieved, for example, by a higher temperature or a certain excitation force, are said to be in the higher atomic orbitals: p-shell, d-shell, etc.

Hamiltonian of a single particle (electron or hole) consists of kinetic and potential energy including spin-orbit interaction. The former is invariant under

all unitary operations acting on the spatial coordinates. The latter reflects the symmetry of the QD and thus determines the point group symmetry of the total Hamiltonian. From a theoretical point of view, the QDs are in the high symmetry point group T_d (tetrahedral symmetry, see [B6]), with the total angular momentum $\vec{J}_z = \vec{S}_z + \vec{L}_z$, where $\vec{S}_z$ is the spin angular momentum along the z axis, and $\vec{L}_z$ is the orbital angular momentum along the z axis. Total angular momentum $\vec{J}_z$ is related to the quantum number which describes the shape or type of the orbital.

During the QD formation, an anisotropy arises between the main growth direction and lateral directions. As the anisotropy increases, the group of symmetry points reduces to D_{2d} (dihedral symmetry). The lack of symmetry along the growth axis leads to an even lower group of symmetry points C_{2v} (cyclic symmetry). Additionally, lower symmetry means lifted degeneracy between energy levels. To describe a QD with imperfect symmetry, we can use the restriction on the s-shell for electrons in the conduction band. This restriction implies $\vec{L}^e_z = 0$ and the relation for total angular momentum simplifies to $\vec{J}^e_z = \vec{S}^e_z$. The valence band is more complicated due to spin-orbit interaction. Here, we cannot apply the s-shell restriction like in the case of electrons and thus the spin $\vec{S}_z$ is not enough, because $\vec{L}_z \neq 0$. This spin-orbit interaction splits the valance band into a heavy hole band with total angular momentum[3] $|\vec{J}^h_z| = \pm 1/2$ and a light hole band with total angular momentum $|\vec{J}^h_z| = \pm 3/2$ [133].

The confinement in a QD lifts the degeneracy between the light hole band and the heavy hole band. In consequence, the maximum of the valence band is usually composed only of heavy hole states without mixing the two bands.

What we can do now is to calculate the total angular momentum $\vec{M} = \vec{S}^e_z + \vec{L}^e_z + \vec{S}^h_z + \vec{L}^h_z$ of particles inside of QD, which consists of the total angular momentum of electrons in the conduction band restricted to the s-shell and total angular momentum of heavy holes in the valence band. This procedure leads to seven spin configurations in a QD based on the total angular momentum $\vec{M} = \vec{S}^e_z + \vec{J}^h_z$, see Fig. 2.16. We have four states for exciton, two states for trion, and one spin configuration for biexcition [134]:

- $\|\vec{M}\|$[4]$= 2$ for exciton X. During the recombination of the electron-hole pair, **no** photon is emitted. This effect is called "dark" state[5].
- $\|\vec{M}\| = 1$ for exciton X. During the recombination of the electron-hole

[3] By notation $|\cdot|$ we mean projection.

[4] By notation $\|\cdot\|$ we mean absolute value.

[5] Detailed conditions of the two possible spin configurations of a "dark" state: $|2\rangle = |l, s\rangle = |3/2, 1/2\rangle$ and $|-2\rangle = |-3/2, -1/2\rangle$

pair, a photon is emitted (photoluminescence). This effect is called "bright" state [6].

- $||\vec{M}||$ = 1/2 for trion X^+.
- $||\vec{M}||$ = 3/2 for trion X^-.
- $||\vec{M}||$ = 0 for biexciton XX.

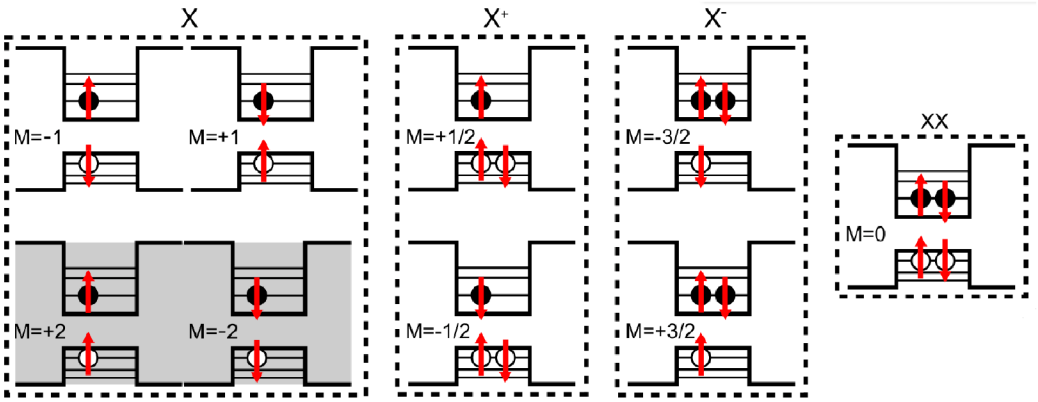


Figure 2.16: Spin configurations of a quantum dot when restricted to the s-shell. There are four configurations for exciton (X), two configurations for each of two trions (X^+, X^-), and one configuration for biexciton (XX), depending on the projection of the total angular momentum M. Electrons are marked with filled circles and holes with empty ones. Two of the exciton configurations are known as "bright" states and the other two as "dark" states, depending on whether or not a photon is emitted during electron-hole pair recombination. Dark states are indicated by a gray background. This figure is taken from Ref. [134].

Entanglement

Exciton and biexciton play significant roles in creating polarization-entangled photon pairs in QDs. In this Section, we describe the quantum dot as a three-level (ladder) system containing the ground level (0), the exciton level (X) and the biexciton level (XX). A two-level system for the QD description is used if we consider only the s-shell restriction. In that case, we are interested in QDs as, for example, single-photon sources. Then, the 0 and X levels are sufficient.

[6] Detailed conditions of the two possible spin configurations of a "bright" state:
$|1\rangle = |l, s\rangle = |3/2, -1/2\rangle$ and $|-1\rangle = |-3/2, 1/2\rangle$

To obtain entangled photon pairs from a QD, we need to populate its XX level. It can be achieved, for example, by shining a laser tuned at half the energy of the $0 - XX$ transition (the $0 - X$ and $X - XX$ transitions generally do not have the same energies). If we have the fully populated XX level, there are two excitons with different spins. Each exciton can decay by radiation emitting a photon with either right (σ^+) or left (σ^-) circular polarization, see Fig. 2.17. More precisely, on the XX level, after the emission of a photon in a specific polarization state created by the recombination of the first electron-hole pair (the first exciton), one more exciton remains on the same energy level. However, this energy level is now labelled as the X level because it has only one exciton left. Energy is now half as in the biexciton case XX. The Fig. 2.17 shows three different levels $0, X, XX$. The excitonic level is, in this case, degenerated. The second electron-hole pair also recombines and emits a photon in a state of orthogonal polarization to the previously emitted photon, which is a consequence of the Pauli exclusion principle. Mathematically, the two-photon state, produced by the described process, can be written as

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}\left(|\sigma^+\rangle_1|\sigma^-\rangle_2 + |\sigma^-\rangle_1|\sigma^+\rangle_2\right), \tag{2.44}$$

which describes a maximally entangled Bell state [135].

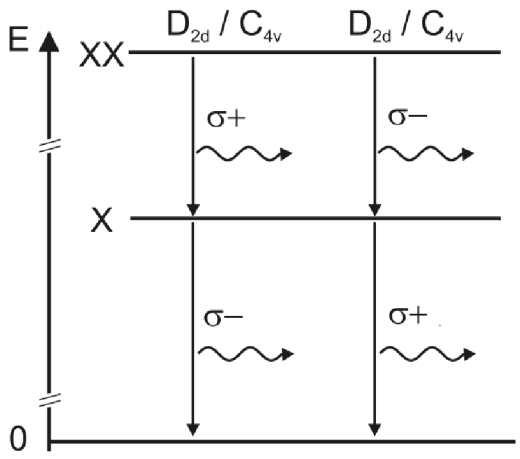


Figure 2.17: The process of two-photon recombination from the biexciton XX level through the degenerate exciton X level to the ground state. During this process, two photons with orthogonal polarizations are generated. If the degeneracy is not lifted, we cannot distinguish which photon comes from which level, and, therefore, the emitted photon pair is entangled in polarization. This Figure is taken from Ref. [136].

Fine-structure splitting

In the previous sections, we described electrons and holes being bound to form an exciton through (their) mutual Coulomb interaction. We mentioned that the exciton has four spin configurations divided into bright and dark states according to the ability to emit a photon. Furthermore, the energy levels of the bright states inside the QD allow the creation of polarization-entangled pairs, but only if they are degenerate. However, the spin-degeneracy of the bright exciton level is usually split due to the spin-orbit interaction and Zeeman interaction between electrons and holes. We call this effect fine-structure splitting (FSS) [136, 137].

The energy level degeneracy is also determined by the QD symmetry mentioned in the previous sections. Its importance is indicated in Fig. 2.18. If the symmetry of the quantum dot is reduced, the FSS increases, and the indistinguishable photon pairs become distinguishable. The entanglement between the photons produced by the X and XX levels decreases and can completely vanish.

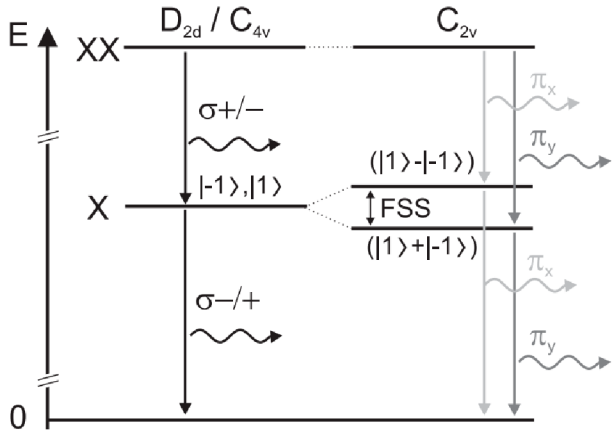


Figure 2.18: Energy scheme illustrating the effect of the exchange interaction on the exciton X bright states. XX denotes the biexciton state. $|M\rangle$ is the exciton total angular momentum, $\sigma^{\pm}$ denotes circularly polarized light, and $\pi_{x/y}$ linearly polarized light. D_{2d}, C_{4v}, and C_{2v} indicate the confinement potential symmetry. This Figure is taken from Ref. [136].

There are many ways to restore higher symmetry in QDs leading to the FSS reduction. These techniques include, for example, annealing [138, 139], application of an external electric [140, 141] or magnetic field [142], structural elongation of the QDs [143], interfacial symmetry lowering and its enhancement by atomistic elasticity[144], or external strain fields [145, 146]. We describe the last mentioned method in more detail in Chapter 3 because we use it to restore the symmetry in QDs to generate entangled photon pairs.

2.3 Quantum coherence as a resource theory

In classical and quantum physics, coherence is at the heart of interference. Quantum coherence arising from quantum superposition describes phenomena that do not occur in classical optics. It is related quantum features, such as quantum correlations (entanglement) [147] or steering [148].

Coherence originates from the fact that all optical fields have some random fluctuations and arises from correlations between some components of the fluctuating electric field at two or more points. Coherence can be described by the sharpness of the fringes in a Young interference experiment [B7]. Mathematically, coherence is introduced in terms of phase space distribution and multipoint correlation functions [7, 48].

The above-mentioned description of coherence is very well developed in both classical and quantum optics. However, the concept can be generalized. To describe quantum coherence beyond optical fields, we can identify a set of incoherent states and a class of free operations that map the set onto itself. Coherence is thus considered a resource that can not be generated or increased within this restricted class of operations. This approach is called *resource theory of coherence*.

It is important to note that resource theory does not exist only for coherence, but resource theories of thermodynamics [149], entanglement [150] or asymmetry [151] were also proposed. In this work, we further deal with coherence as a resource and describe this framework in more detail.

Resource theories aim to describe what tasks or transformations of a physical system an experimenter can achieve when certain constraints exist. Anything that overcomes these limitations is considered a resource.

Since coherence is a basis-dependent concept, we must first choose the so-termed reference basis of our vector space. This basis can be chosen to suit existing constraints, such as the conditions in the laboratory, the difficulty of performing some operations in experiments, or different conservation laws. Subsequently, we can identify a set of incoherent states and a class of free operations. With free states and free operations defined, we can further introduce the maximally coherent state and the coherence measures.

2.3.1 Free states and the set of free operations

Let us have a finite d-dimensional Hilbert $\mathcal{H}$ space and its given reference basis $\{|i\rangle\}_{i=0,\ldots,d-1}$. The density matrices that are diagonal in this basis are called *incoherent*. They form a set denoted as $\mathcal{I} \subset \mathcal{B}(\mathcal{H})$, where $\mathcal{B}(\mathcal{H})$ is the set of all

bounded trace class operators on $\mathcal{H}$. Hence, all incoherent density operators $\hat{\rho}$ can be written as

$$\hat{\rho} = \sum_{i=0}^{d-1} p_i |i\rangle\langle i|, \tag{2.45}$$

where p_i are the probabilities.

In contrast to the mentioned resource theories of entanglement, thermodynamics, or asymmetry, where a set of free operations is clearly given, in the resource theory of coherence the free operations are not unique. There are different classes of these operations. For our purposes, it will be sufficient to mention only three of them. Some other classes of incoherent operations can be found in Ref. [152].

Classes of free (incoherent) operations

First, we define the individual classes of operations, and then we will describe in more detail what the definitions mean and explain how the individual classes differ from each other.

Maximally incoherent operations (MIO): Trace-preserving completely positive and non-selective quantum maps Λ_M: $\mathcal{B}(\mathcal{H}) \mapsto \mathcal{B}(\mathcal{H})$ such that

$$\Lambda_M[\mathcal{I}] \subseteq \mathcal{I}. \tag{2.46}$$

Incoherent operations (IO): A set of trace-preserving completely positive maps Λ_I: $\mathcal{B}(\mathcal{H}) \mapsto \mathcal{B}(\mathcal{H})$ that allows for Kraus representation with corresponding Kraus operators $\{\hat{K}_n\}$, satisfying $\sum_n \hat{K}_n^\dagger \hat{K}_n = \hat{\mathbb{1}}$ (trace preservation), and for all n and $\hat{\rho} \in \mathcal{I}$:

$$\frac{\hat{K}_n \hat{\rho} \hat{K}_n^\dagger}{\mathrm{Tr}[\hat{K}_n \hat{\rho} \hat{K}_n^\dagger]} \in \mathcal{I}. \tag{2.47}$$

IO also fulfils a condition: $\hat{K}_n \mathcal{I} \hat{K}_n^\dagger \subset \mathcal{I}$.

Strictly incoherent operations (SIO): The set of trace-preserving completely positive maps, expressed also as in Eq. (2.47), since it is a subset of IO, but outside the condition $K_n \mathcal{I} K_n^\dagger \subset \mathcal{I}$, they also satisfy a condition $\hat{K}_n^\dagger \mathcal{I} \hat{K}_n \subset \mathcal{I}$. We can also define SIO using the dephasing operator

$$\Delta[\hat{\rho}] = \sum_{i=0}^{d-1} |i\rangle\langle i|\hat{\rho}|i\rangle\langle i|. \tag{2.48}$$

Then SIO can be written using a set of incoherent Kraus operators $\{\hat{K}_n\}$ such that the results measured on the reference basis are independent of the coherence of the input state, i.e.,

$$\langle i|\hat{K}_n\hat{\rho}\hat{K}_n^\dagger|i\rangle = \langle i|\hat{K}_n\Delta[\hat{\rho}]\hat{K}_n^\dagger|i\rangle \tag{2.49}$$

for all n and i.

All these classes are unable to create coherence from incoherent states. MIO is the largest of all the mentioned classes and is also called incoherence preserving operation. IO is a subset of MIO. This representation is not unique, it is determined by the difficulty of the problem being solved. Eq. (2.47) defining IO using the Kraus operators $\hat{K}_n$ guarantees that even if the individual measurement results n are available, coherent states cannot be generated from an incoherent state, not even probabilistically. SIO is a subset of IO, so we can write relations between individual sets: SIO $\subset$ IO $\subset$ MIO. With SIO, it is required that the admissible operations cannot use coherence from the input state (which is therefore not necessarily incoherent). This set has an incoherent Kraus decomposition, i.e., not only $\hat{K}_n$ but also $\hat{K}_n^\dagger$ is incoherent.

Maximally coherent state

For a certain reference basis $\{|i\rangle\}_{i=0,\ldots,d-1}$ of a finite d-dimensional Hilbert space $\mathcal{H}$, we can write the d-dimensional maximally coherent state as

$$|\Psi_d\rangle = \frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|i\rangle. \tag{2.50}$$

Using IO and a maximally coherent state we can generate all other d-dimensional quantum states. The maximally coherent state is analogous to the maximally entangled states expressed in Eq. (2.42) and Eq. (2.43).

2.3.2 Quantum operations

Just as the maximally entangled state in bipartite systems enables the generation of all quantum operations via local operations and classical communication (LOCC) [153], the maximally coherent state enables the generation of all quantum operations via IO [54]. More specifically, if we consume a maximally coherent state via IO, we can implement any quantum operation that acts on Hilbert space $\mathcal{H}$. It is not yet known how much coherence is needed to create any unitary or any quantum operation in general. However, coherence quantifiers are monotonic for incoherent operations, so they can provide lower bounds on the amount of coherence that is needed to realize a quantum operation [49, 154].

2.3.3 Coherence monotones and measures

Coherence monotones and measures are mathematical tools for quantifying coherence. This mathematical approach is based on several postulates. In this work, we will not state the postulates in detail, we will only say what properties a quantity must have to be either monotone or measure. All definitions are given in Ref. [152].

Any quantity C that fulfils *nonnegativity* and either *monotonicity* or *strong monotonicity* (or both) is called a **coherence monotone**. Any quantity C that, in addition to the above-mentioned three conditions, also fulfils *convexity*, *uniqueness*, and *additivity* is called a **coherence measure**. In some literature, a coherence measure is defined as a quantity that satisfies only the first four conditions, i.e., non-negativity, monotonicity, strong monotonicity and convexity. However, with the first-mentioned approach inspired by entanglement theory, we can directly introduce two measures of coherence.

The first one is *distillable coherence* C_d, which is the maximal number of maximally coherent one-qubit states that can be obtained per copy of a given state using IO. The second one is *coherence cost* C_c, which is the minimal rate of maximally coherent single-qubit states required to produce a given state via IO.

In general, the distillable coherence cannot be larger than the coherence cost: $C_d(\hat{\rho}) \leq C_c(\hat{\rho})$. The equality holds only for pure states, and thus the resource theory of coherence is reversible for them.

Coherence monotones include, for example, *geometric coherence*, which is defined using the fidelity of two states [155], or the *relative entropy of coherence* and the l_1*-norm of coherence* C_{l_1}, which are discussed below.

Relative entropy of coherence

Relative entropy of coherence is one of the quantifiers based on finding the infimum of distance that is taken over a set of incoherent states $\mathcal{I}$. For this quantifier, the distance is the quantum relative entropy and is described by the relation

$$C_r(\hat{\rho}) = \min_{\hat{\sigma}\in\mathcal{I}} S(\hat{\rho}\|\hat{\sigma}), \tag{2.51}$$

where $S(\hat{\rho}\|\hat{\sigma}) = \mathrm{Tr}[\hat{\rho}\log_2\hat{\rho}] - \mathrm{Tr}[\hat{\rho}\log_2\hat{\sigma}]$ and $\hat{\rho}$ is an arbitraty state and $\hat{\sigma}$ denotes an incoherent state.

Relative entropy of coherence fulfils nonnegativity, monotonicity and convexity for any MIO, IO or SIO set. For IO, it also fulfils strong monotonicity and, in addition, two other necessary conditions - uniqueness and additivity, which

make it a quantum measure. Specifically, for IO, this coherence measure is equal to the distillable coherence C_d, which leads to a simpler equation

$$C_r(\hat{\rho}) = C_d(\hat{\rho}) = S(\Delta[\hat{\rho}]) - S(\hat{\rho}), \tag{2.52}$$

where $\Delta[\hat{\rho}]$ is the dephasing operator defined in Eq. (2.48) and $S(\hat{\rho}) = -\mathrm{Tr}(\hat{\rho}\log_2\hat{\rho})$. The proof of this equality can be found in Ref. [152].

Relative entropy of coherence can be described as the minimum amount of noise required to obtain a completely decoherent state. The upper bound of this measure on the Hilbert space $\mathcal{H}$ of dimension d is given by the relation

$$C_r(\hat{\rho}) \leq S(\Delta[\hat{\rho}]) \leq \log d. \tag{2.53}$$

Note that $C_r(\hat{\rho}) = S(\Delta[\hat{\rho}])$ if and only if the quantum state $\hat{\rho}$ is a pure state. Pure states satisfying $C_r(\hat{\rho}) = \log d$ are called maximally coherent states, which were defined in Section 2.3.1.

In Chapter 4, we investigate remote control and enhancement of local quantum coherence. We have a bipartite system with two qubits, and we use one as a target and the other as a control. We show that for specific intersystem coupling and using several copies of the second system, we can deterministically enhance the local coherence of the first system while fully preserving its purity. This procedure works for any pure control state with non-zero coherence. We evaluate the amount of coherence in our systems using relative entropy of coherence.

l_1-norm of coherence

Any matrix norm, denoted as $\|\cdot\|$, satisfying the triangle inequality[7] and absolute homogeneity[8] gives rise to a convex coherence quantifier. Such quantifiers include, for example, the l_p-norm, where $p \geq 1$ is a real number. This norm is defined by the relation

$$\|M\|_{l_p} = \left(\sum_{i,j} |M_{ij}|^p\right)^{1/p}. \tag{2.54}$$

For $p = 1$ we get the Taxicab norm also called l_1-norm. For $p = 2$ we have the Euclidean norm[9], and as p goes to infinity, the given norm is called infinity norm.

The l_1-norm of coherence C_{l_1} can be expressed as

$$C_{l_1}(\hat{\rho}) = \min_{\hat{\sigma}\in\mathcal{I}} \|\hat{\rho} - \hat{\sigma}\|_{l_1} = \sum_{i\neq j} |\rho_{ij}|, \tag{2.55}$$

[7] $\|A + B\| \leq \|A\| + \|B\|$, where A and B are matrices.
[8] $\|\lambda A\| = |\lambda| \times \|A\|$, where λ is a real number and A is a matrix.
[9] $\|x\|_2 = \sqrt{\langle x, x\rangle}$

which is the sum of the magnitudes of all off-diagonal terms.

For IO, this coherence quantifier fulfils all four conditions mentioned above (nonnegativity, monotonicity, strong monotonicity and convexity). It is therefore a coherence monotone. However, l_1-norm does not fulfil the other two conditions (uniqueness and additivity), so in our approach, it is not a quantum measure.

Considering maximally coherent state $|\psi_d\rangle$, where d is the dimension of Hilbert space $\mathcal{H}$, the coherence quantifier C_{l_1} takes the form

$$C_{l_1}(|\psi_d\rangle) = d - 1. \tag{2.56}$$

2.3.4 Mutual (correlated) coherence

So far, we have discussed quantum coherence in the context of a simple system that did not contain multiple subsystems. In a composite quantum system, coherence can be distributed in various and non-trivial ways. In addition to the quantum coherence of the composite system (global coherence), we can also consider the coherence of individual subsystems (local coherence). A new form of coherence, which characterizes the amount of quantum coherence in a global composite system that is not contained in the local states of its subsystems, is called mutual coherence. The basis-optimized value of mutual coherence, known as correlated coherence, characterizes new types of quantum correlations of the subsystems that are conceptually different from entanglement [156].

Consider a bipartite quantum system in a composite Hilbert space $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$ with $d = d_A = d_B$ dimensions of the composite system, quantum system A and quantum system B, respectively. The basis of the system AB is given by the tensor product of the reference bases of both subsystems, i.e., $\{|i\rangle_A\}_{i=1}^{d} \otimes \{|j\rangle_B\}_{j=1}^{d}$. Mutual coherence C_M of the bipartite system AB is then defined as a difference between the coherence of the global state $C(\hat{\rho}_{AB})$ and the local coherences of the two subsystems $C(\hat{\rho}_A)$ and $C(\hat{\rho}_B)$

$$C_M(\hat{\rho}_{AB}) = C(\hat{\rho}_{AB}) - C(\hat{\rho}_A) - C(\hat{\rho}_B), \tag{2.57}$$

where $\hat{\rho}_A = \mathrm{Tr}_B[\hat{\rho}_{AB}]$ and $\hat{\rho}_B = \mathrm{Tr}_A[\hat{\rho}_{AB}]$ are the density metrices of subsystems A and B, respectively.

The coherence quantifier in Eq. (2.57) can be chosen to be l_1-norm of coherence C_{l_1} or relative entropy of coherence C_r. If the chosen coherence quantifier is relative entropy of coherence C_r, it is possible to express the mutual coherence as a difference of relative entropies [157]

$$C_M(\hat{\rho}_{AB}) = S(\hat{\rho}_{AB} || \hat{\rho}_A \otimes \hat{\rho}_B) - S(\Delta(\hat{\rho}_{AB}) || \Delta(\hat{\rho}_A) \otimes \Delta(\hat{\rho}_B)), \tag{2.58}$$

where $S(\hat{\rho}\|\hat{\sigma}) = \mathrm{Tr}[\hat{\rho}\log_2\hat{\rho}] - \mathrm{Tr}[\hat{\rho}\log_2\hat{\sigma}]$ and $\Delta[\hat{\rho}]$ is the dephasing operator defined in Eq. (2.48).

As mentioned in Section 2.3.3, relative entropy of coherence is a measure of coherence, which means that is also additive $C_r(\hat{\rho}_A \otimes \hat{\rho}_B) = C_r(\hat{\rho}_A) + C_r(\hat{\rho}_B)$. This condition ensures that the mutual coherence vanishes for any product state $C_M(\hat{\rho}_A \otimes \hat{\rho}_B) = 0$. However, if we choose l_1-norm as the coherence quantifier, then this monotone could lead to a non-zero correlated coherence for a product state. For this reason, we will only use relative entropy of coherence to describe mutual coherence C_M.

In Chapter 5, it is described that care must be taken when considering transformations of various forms of quantum coherence in composite systems. More specifically, we investigated how to maximize mutual coherence C_M in certain subspaces of d-dimensional Hilbert space $\mathcal{H}$ and the connection with maximally entangled states.

2.3.5 Connection of quantum coherence with entanglement

Since both - coherence and entanglement - are significant resources defined by resource theories, it is more than clear that we can find some parallels between these concepts. Considering that we have already defined entanglement in Section 2.1.6, we briefly mention only these similarities point by point.

- The maximally coherent state plays an analogous role in resource theory of coherence, as the maximally entangled state in entanglement resource theory.
- When defining a coherent state, we first introduce an incoherent state. This is similar to introducing a separable state in entanglement theory to define what an entangled state is.
- While in the theory of entanglement the generation of all quantum operations in bipartite systems is possible using the maximally entangled state and local operations and classical communication (LOCC) [153], in the theory of coherence all these operations are generated using the maximally coherent state and IO [54].
- The measures are also defined in both resource theories. In certain cases, some measures of entanglement may be equal to measures of coherence [158].
- A state that has some amount of coherence (i.e., is not incoherent) can be used to generate entanglement via bipartite IOs. In other words, it is

not possible to create an entangled state by any operation if we start from incoherent states [159].

2.4 Quantum cryptography

Ever since humans learned to read and write, there has been an effort to communicate information between two participants in such a way that a third participant can not reach them. Technology has evolved significantly since ancient Egypt, and today, computers and various security protocols are used to communicate information securely. The key is to create an encryption method that can not be broken. However, classical encryption and classical computers already seem insufficient with the development of quantum computers. Therefore, methods based on the principles of quantum mechanics, such as quantum key distribution or oblivious transfer, are increasingly coming to the fore.

2.4.1 Quantum key distribution

Quantum key distribution (QKD) is a secure method that allows an exchange of encryption keys between two participants, usually called Alice and Bob. They have access to two communication channels – one quantum and the other classical. Alice and Bob use the quantum communication channel to securely share keys. The classical channel serves Alice and Bob to communicate such information that they can perform bases reconciliation, error correction, and privacy amplification [160]. In other words, Alice sends information using bits usually encoded into qubits to Bob over a quantum channel. To verify the security of the quantum channel, they communicate certain information over a classical channel to reveal the possible leakage of information to someone else. In QKD, the person trying to get the information shared between Alice and Bob is called Eve, from the word "eavesdropping". Based on the information, which Alice and Bob share over the classical channel, they can determine the amount of noise in the quantum channel. This knowledge allows them to use classical algorithms, which subsequently guarantee that the information Eve has about their secret key is exponentially small. The QKD scheme is shown in Fig. 2.19 (a).

QKD can be described in the following four steps (for more information see the BB84 protocol below):

- *Sifted key creation*, i.e., generation of n random bits encoded into logical values of 0 and 1 using, for example, polarization or phase methods,

- *Channel parameter estimation*, i.e., determining the amount of noise (possible information leakage) present in the quantum channel, which is subsequently included in the privacy amplification algorithm,

- *Error correction*, i.e., using the information communicated over the authenticated classical channel to reconcile the differences between Alice's and Bob's bit strings,

- *Privacy amplification*, i.e., an algorithm applied after error correction for extracting secret random bits from the bit string that still may be partially known to Eve.

The final random secret key, which is known to Alice and Bob, is used to encrypt and decrypt the shared message. Only the key, not the message, is secretly distributed between Alice and Bob over the quantum channel. The message is encrypted with the key and communicated publicly. Eve tries to disrupt both channels, quantum and classical, in such a way that she learns as much information as possible without her presence being detected. The security of QKD is based on the laws of quantum mechanics, unlike classical computing, which relies on the computational difficulty of mathematical tasks.

In QKD, the secret key is distributed over the quantum channel using a variety of quantum protocols. We can divide these protocols into four main categories: The protocols that use discrete variables (DV) [65], the protocols that use continuous variables (CV) [66], hybrid protocols using both [68] and distributed-phase-reference coding [161]. For DV and CV, each bit of information about the key is encoded into a single signal state. However, the difference between the two is that DV uses encoding into discrete variables of the quantum state, such as polarization or phase, while CV encodes information into continuous variables, i.e., quadratures of a coherent or squeezed state. Distributed phase-reference-coding uses the phase difference of two successive signal pulses or the difference in the arrival times of individual photons to encode the information. Some quantum protocols use entanglement which brings certain benefits. It allows, for example, to communicate over a greater distance or it enables determining the security of a given quantum protocol, see the E91 protocol below.

Some important QKD protocols

In this section, we only mention a few quantum protocols to simply explain the principles of QKD. At the same time, we also explain other concepts related to the security of quantum protocols, such as various forms of eavesdropping.

BB84

The first QKD protocol was proposed in 1984 by Bennett and Brassard [15], hence its name BB84. This protocol uses qubits to encode bits of information. It was originally described using photon polarization states, however, other variants, such as the phase encoded states in optical fibers, can be used to transmit information using this protocol. The security of this protocol against eavesdropping (Eve) was proved in Ref. [162].

The protocol consists of choosing two nonorthogonal polarization bases, for example, HV and DA. H (V) is the horizontal (vertical) polarization state assigned to a logical value 0 (1). In the second basis, the two polarization states, diagonal and antidiagonal, are again assigned to the logical values of 0 or 1. The sender, Alice, randomly chooses a basis and thus randomly sends one particular state 0 or 1. This state is sent over a free space or a fiber to the receiver, Bob. He also randomly, independently of Alice, chooses a basis and then detects either 1 or 0. Then they share their settings of bases via the classical communication channel.

If Alice sends $2n$ bits of information encoded into qubits to Bob, then Bob has a 50% chance of choosing the same bases as Alice. Therefore, after sharing the bases choices with Alice over the classical channel, he has at least n bits from the correct guesses. Some random others of these n bits are sacrificed when Alice and Bob exchange information about the logical values they sent/measured. In this way, they try to determine their error rate. Knowledge of the error rate of their quantum channel enables the application of classical protocols, i.e., error correction and privacy amplification. The error rate is caused by a noise in the quantum channel, which is always considered to be caused by Eve. She can disrupt the quantum channel, for example, by taking the qubits sent by Alice and measuring their logical values on the bases she guesses. However, a qubit measurement (detection) destroys the qubit, and because of the no-cloning theorem of quantum mechanics, Eve cannot clone qubits before her measurement. The solution for Eve is to have a device similar to Alice's. She can then send her bits to Bob. But for that, she has to choose her own random bases. Thus, even if Bob agrees on the choices of bases with Alice, he may not agree with Eve, causing Bob to measure different bit logical values than he should, thus revealing the presence of Eve.

Alice and Bob therefore perform error correction. One possible algorithm is based on a parity check [163]. Alice and Bob first agree on a random permutation of the bit positions in their strings because they want to randomly distribute errors. The bit strings are then divided into blocks of the same size k (blocks with the same number of bits), and the parity of each block is calculated by summing the logical values of the bits and dividing the sum by modulo 2. Alice and Bob then exchange these parities. In this way, they can detect the blocks with an odd

number of errors. Alice and Bob can apply a dichotomic search, an algorithm capable of finding and correcting one of the errors, the wrong bit, in the block. However, this bit is not secure for encryption and, therefore, is discarded at the end of the protocol. They can then repeat the process by choosing a different k, recalculate the parity and try to correct the errors. The number of remaining errors decreases with each iteration, and the number of sacrificed bits as well. In this way, Alice and Bob try to match all bit strings and eliminate errors until they reach close to the optimal information rate given by the Shannon limit (the maximum amount of error-free information that can be transmitted per time unit over a communication channel in the presence of noise).

The final step is privacy amplification, where Alice and Bob gain a shorter but secret bit string, their secret key, from a partially secret bit string obtained during the error correction process. For privacy amplification, hash functions are mainly used in practice. These are one-way functions mapping bit strings of arbitrary size to fixed-size ones [164]. After applying both, error correction and privacy amplification, Alice and Bob have a secure bit string, a secret key, where it is guaranteed that the probability that Eve knows the individual bits of the secret key is exponentially small.

E91

In 1991, Artur Ekert proposed a QKD protocol using entanglement [10]. Instead of Alice sending particles with information to Bob, there is another source that creates entangled particles and sends one to Alice and one to Bob. The quantum states used here are called spin singlets[10]. The well-known example of the singlet state is the Bell state $|\psi^-\rangle$ defined in Eq. (2.43). One particle from the entangled pair with either up or down spin travels to Alice, while the other one with the opposite spin travels to Bob. However, one cannot decide which particle has which spin without measuring at least one of these two particles. The spin-up and spin-down states of the particles correspond to bit values 1 and 0, respectively.

Alice and Bob choose one of three coplanar axes to measure their particle. There is a 1/3 probability that Alice and Bob will choose a compatible basis. If this happens, they will always get anti-correlated measurement results. It means that if Alice measures spin up on her particle, Bob's particle has spin down, and vice versa. However, if Alice and Bob choose incompatible bases, then the result of Bob's measurement is random, independent of Alice's measurement. These two-thirds of the results are discarded in this protocol.

[10] A set of particles with spin quantum number $s = 0$, which is evident in a spectrum that has only one spectral line. Then we also have triplet states with $s = 1/2$, in whose spectra we see the threefold splitting of spectral lines.

To discard these measurements, Alice and Bob let each other know via the classical channel in which bases they performed their measurements. The presence of Eve is tested using Bell's theorem. Because, as was already mentioned in Section 2.1.6, Bell's inequalities are violated only if two particles are entangled. If there is Eve in the quantum channel, she will disturb the entanglement by her presence - by measuring one of the entangled particles to obtain information. There may be a situation where Bob does not receive a particle from an entangled pair. But since Alice received hers, this fact already indicates the presence of Eve. Eve can measure Bob's particle in some of her randomly chosen bases, but then she has to send another particle to Bob. In this case, Eve's particle will no longer be entangled with Alice's particle. As a result, Bell's inequalities are not violated.

MSZ96 and others

This QKD protocol was proposed by Mu, Seberry and Zheng in 1996. It uses neither polarizing photons nor entangled particles. It requires four nonorthogonal quantum states described by noncommuting quadrature phase amplitudes of a weak optical field. These states have multiple overlaps (more than 90%), so it is almost impossible to get a definite result by measuring just one state. While the first two protocols use DV, this protocol uses CV.

Some other protocols, such as BBM92 [165] or Decoy state protocol [166], use **decoy states**. These are states with different mean numbers of photons that are used to detect eavesdropping attacks. The main problem with probabilistic sources, such as the SPDC described in Section 2.2.1, is the occurrence of multiphoton emission. The consequence is that there is more than one photon in the pulse. But that is an unwanted case. Eve can steal these extra photons and perform her measurements on them to gain information. Different intensity pulses from different sources transmitted over the same quantum channel help prevent this attack, otherwise known as **photon number splitting** (PNS).

Other invented protocols aim to improve some features of the original ones. For example, SARG04 [167] is a more robust version of BB84 protocol, specifically in PNS attacks. Another example is the Six-state protocol [168], which, as the name suggests, uses all three orthogonal polarization bases. This makes it more resistant to noise.

2.4.2 Oblivious Transfer

In addition to QKD, there are other cryptographic methods such as Oblivious Transfer (OT), quantum bit commitment (QBC) [60] or password-based authentication [61]. OT is the basic building block for all other two-party protocols and

will be discussed in more detail.

In the OT protocol, one communication participant has several messages and sends them to the other communication participant. The receiver should receive only one of the messages and not learn anything about the others. However, the sender should be oblivious to which message the receiver received and whether he received it at all. The OT scheme is shown in Fig. 2.19 (b).

The first OT proposal was introduced by Rabin in 1981[11]. The sender has one bit available, which with a probability of 1/2 is sent to the receiver. However, the sender does not care whether the bit is received or not. This proposal belongs to a form of OT called All-or-nothing. Another form of OT is 1-2 oblivious transfer [62]. It means 1 out of 2, so the sender has two messages, two bits. However, the recipient will only receive one of them. The probabilities of receiving both messages are equal. Again, the sender does not care which message was received, if any at all. There are also several more generalized versions of this protocol. One of them is 1 out of n OT [63], where we have n messages, and the recipient receives only one of them. Or there is also the variant k out of n OT [170]. Another concept of OT is XOR oblivious transfer, or simply XOT [171]. The sender has two bits, which are sent to the receiver. The receiver then receives one of the two bits or their XOR. Apart from our quantum protocol, which is described in Section 6, there is so far only one other XOT quantum protocol, namely KST22 [172].

Just as QKD protocols allow quantum-safe communication, quantum OT-(QOT) protocols allow quantum-safe computation. Unlike QKD, where security is required against an unwanted third party, in (Q)OT, security should be ensured directly against communication participants who do not trust each other. Another difference between QKD and QOT is that we cannot implement QOT with unconditional security. In other words, security is not only determined by the laws of quantum physics. We need to use the restrictions and assumptions discussed below. However, these two approaches, QKD and QOT, also have something in common. Both have quantum protocols for sending encrypted information and may also use similar methods, such as polarization encoding or entanglement.

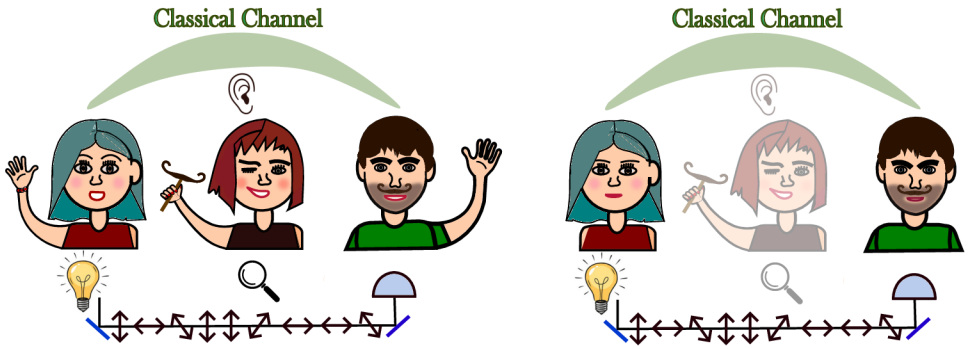
As we already mentioned, QOT security is not determined only by the laws of quantum physics. An unconditionally secure QOT was shown to be impossible in 1997 in Refs. [173, 174], leading the quantum cryptography community to pursue two possible paths:

- The first path was the invention of protocols limited by certain assumptions such as relativistic constrains [175, 176], noise, or bounded quantum storage [177]. Such protocols include, for example, BBCS92 (below) or

[11] However, oblivious transfer was first described by Wiesner [169].

KW16 [178].

- The second path includes protocols which allow communication participants to obtain some information with a certain probability, but we have to calculate the probabilities of cheating for individual participants. This path is referred to in some literature as Weak OT, in which we include protocols, such as CKS13 (see below) or XOT (see Section 6). This approach also leads to the concept of Private Database Query [179].



(a) QKD **(b)** OT

Figure 2.19: Schemes of quantum key distribution (a) and oblivious transfer (b). In QKD, Alice (left) and Bob (right) exchange a secret key and trust each other. Eve (centre) pretends to be Bob (Alice) to Alice (Bob) and tries to get the secret key by eavesdropping and disrupting both channels (classical and quantum) that Alice and Bob use for transmission. In OT, Alice and Bob also communicate with each other, but unlike QKD, they do not trust each other. Here, security is not determined only with Eve in mind, but calculations are made to find out the cheating probabilities of Alice and Bob, who want to get more information than they should.

BBCS92 protocol

This protocol is among the first proposed protocols and reduces quantum OT to quantum bit commitment [180]. Its name, similar to BB84, is formed by the first letters of its inventors, i.e., Bennet, Brassard, Crépeau and Skubiszewska, and at the same time by the year when it was created. This protocol uses weak pulses of polarized light, and the encoding method is very similar to the BB84 protocol.

Alice and Bob initially exchange some information before starting OT, so they can successfully communicate. For example, Bob will tell Alice about the detector's quantum efficiency and their dark count rates. Alice will tell him,

for example, the intensity of the pulses she sends and the security parameter N. Then Alice sends Bob a random sequence of $2N/a$ [12] faint pulses each in one of H, V, D, and A polarization. The following steps are the same as in the BB84 protocol: Bob randomly decides the bases on which he detects pulses. He writes down the choices and the measured results. Alice then tells Bob the bases she used to send each pulse. Unlike the BB84 protocol, Bob does not reveal his choices. He should receive a total of $2N$ pulses, which he divides into good ones and bad ones (depending on his correct choice of bases). With the 50% probability of correct guessing, Bob should now have N correctly measured pulses and N wrongly measured pulses. After further steps with error corrections, two possibilities arise: Either Bob has the correct chain of N pulses, and thus also the necessary information from Alice, or Bob didn't receive anything because his error rate was higher, and, therefore, he doesn't have all the N necessary correct results to gain the information. Alice doesn't know on which bases she and Bob agreed, so she has no idea which information Bob obtained if any at all.

One security issue is immediately apparent. If Bob had some quantum memory where he could store all of his unmeasured photons sent by Alice, then after learning Alice's choice of bases, he would get all the information. For this reason, one possible security assumption of OT is the absence of quantum storage. To verify that Bob does not cheat, Alice can ask about some of his bases choices and the results of his measurements. If Bob is honest, then he passes Alice's test. If not, he only has a certain probability of guessing.

CKS13 protocol

The Chailloux-Kerenidis-Sikora protocol is the first proposed Weak OT protocol. A specific quantum system is sent to the receiver, who performs some quantum operation on it and sends it back to the sender. At the same time, both communication participants work in 3D Hilbert space and do not use conjugate coding, i.e., coding from the BB84 protocol.

It starts by preparing an entangled state on the receiver's side, which depends on the random selection of bits. He keeps one of the three qutrits and sends the other two to the sender. The sender applies a unitary operation according to his random bit selection on these other two qutrits. This subsystem is sent back to the receiver. The receiver now has a state that is either the same as, or orthogonal to, the initially created entangled state. Now, the receiver can make a measurement that perfectly distinguishes between these two cases. One of these cases has the logical value of 1 and the other of 0. This way, the receiver gets only one bit of information without the sender knowing which one [181].

[12] a is a fraction of pulses Alice expects that Bob will detect successfully

Chapter 3

A source of entangled photons based on a GaAs quantum dot

Results presented in this Chapter come from cooperation with the group of Prof. Rinaldo Trotta in Rome, Italy. Rinaldo Trotta et al. devised a method and built an experimental setup (both described below). All our experimental results were measured using their setup directly in the laboratory of La Sapienza University in Rome. This collaboration ended with a joint article [A1]. The results described in this Thesis are based on my own measured data obtained during cooperation with the group of Prof. Trotta.

Quantum dots, as well as SPDCs, can be used as sources of entangled pairs. However, to achieve similar qualities in entanglement generation as probabilistic sources, the quantum dot should have low multiphoton emission probability, high brightness, tunable emission energy, and high fidelity entanglement. The significant advantages of quantum emitters are the Coulomb interaction and the Pauli exclusion principle. Thanks to them, each excited state can be populated only once. Moreover, the simultaneous emission of more than one photon of a given frequency per excitation cycle is reduced to a negligible probability of re-excitation during the same laser pulse.

However, a proof-of-concept demonstration of a quantum dot (QD) device that fulfils all the strict requirements of the ideal entanglement source at the same time is still missing. It is mainly due to several technical difficulties, such as fine structure splitting (FSS) described in Section 2.2.2, which reduces entanglement; the low extraction efficiency which is caused by total internal reflection in the high refractive index semiconductor material; low indistinguishability of the generated pairs due to decoherence and time correlations in the two-photon cascade.

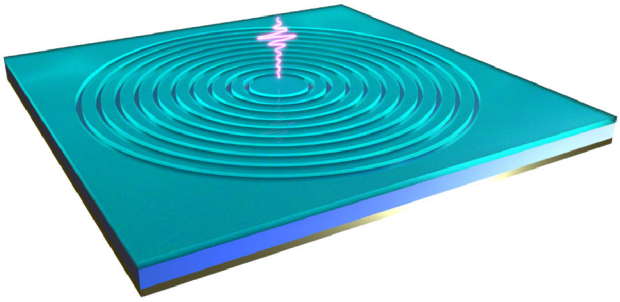


Figure 3.1: Bragg resonator, also called Bullseye cavity. This figure is taken from Ref. [182].

One way to solve some of these problems is to place the QD in the microcavity. Its ability is to redirect the flow of photons, improving the efficiency of photon extraction. Another method is the application of some external fields. We used gallium arsenide (GaAs) QDs embedded in a Bragg resonator and integrated into a micromachined multiaxial piezoelectric actuator that enables voltage tuning. We applied a DC voltage to affect the QDs on this device. More specifically, our goal is to use this voltage to reduce the FSS and thereby improve the entanglement of the generated photon pairs.

The choice of a Bragg resonator (CBR), also called a Bullseye cavity, is best compatible with the strain tuning technique. In the centre of this resonator is a QD surrounded by a circular Bragg grating, see Fig 3.1. This results in a periodic change in the refractive index. The repetition of this structure has a period that satisfies the second-order Bragg condition. Due to this, the light inside the semiconductor is reflected in the direction perpendicular to the plane with the Bragg grating. If, in addition, the Bragg grating is combined with a metallic mirror placed below it, then the result is even better reflectivity of a quasi-Gaussian beam emerging from the top surface of this structure. A further improvement in emission occurs thanks to the Purcell effect, which enables higher repetition rates. By a different Purcell factor, we can also influence the lifetime of quasiparticles such as exciton X and biexciton XX and thus also increase the indistinguishability of photons emitted during the recombination of these quasiparticles (more information below). The extraction efficiency, i.e., the fraction of photons collected by the lens at the surface of the samples in our experiment, is 0.77(5), which was measured with single-photon avalanche photodiodes (SPADs) for the brightest QDs in the sample, excited at the repetition rate of 80 MHz and connected to a multimode fiber.

3.1 QDs characterization

Individual GaAs QDs grown by Al-droplet etching are created by molecular beam epitaxy growth at the Institute for Semiconductor and Solid State Physics of the Johannes Kepler University in Linz (AT). There can be several dozens of them on one created sample. The formed membrane containing GaAs QDs is then placed on the piezoelectric actuator. Next, it is necessary to find the position of each QD and mark them. Therefore, we have to place a marking grid on the membrane. It is done by patterning the mask with electron lithography. Finally, the QDs positions are read again to etch the Bragg cavities. A detailed description of the entire procedure can be found in Ref. [134]. The etched sample is then mounted in a low-temperature (5K) closed-cycle cryostat to characterize the shift of the cavity mode with temperature and to observe any degradation of the QD emission due to the etching process.

Fig. 3.2 shows the reflectivity spectrum of a Bragg cavity with QDs. We can see that the peak corresponding to the QD emission is almost in the centre of the formed cavity, in the dip, so the extraction efficiency is very high. The spectral response of the cavity is analyzed by obtaining its reflectivity spectrum. We used a white halogen lamp, which is a broadband source. The spectrum of the light reflected by the cavity is almost flat, so we plot only the part covering the dip. This dip is created by the light absorption in resonance with the cavity. We also see the emission of the QD inside the dip because the cavity is mode-matched to this QD.

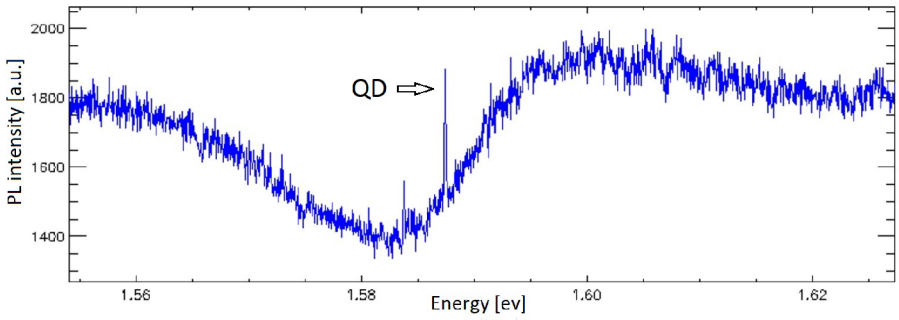


Figure 3.2: A part of the measured reflectivity spectrum of the cavity with a QD. We used a broadband source, it follows that the entire spectrum is almost flat, except for the dip. The dip was created by the absorption of light that is in resonance with the cavity.

Inside the cryostat, the entire sample lies on a mount with linear piezo actuators that control the sample movement in the x, y, and z directions. At the same time, the entire sample is projected onto a computer screen, where the grid and

the location of the individual QDs can be seen, see Fig. 3.3. It is possible to target the position of the desired QD by controlling the piezo actuators. After finding the position, we can start to excite the QD and measure its properties.

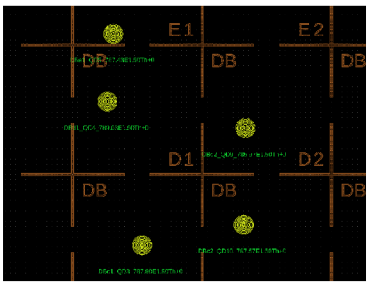


Figure 3.3: Example of an electron lithography grid showing the location of the Bragg resonators surrounding the QDs. This figure is taken from Ref. [134].

3.1.1 Degree of linear polarization

The asymmetry of the QD, the location of the QD in the cavity and also the asymmetry of the cavity in which the QD is located lift the polarization degeneracy into two orthogonal linearly polarized modes. However, we assume that the two emitted photons from the QD, created by the decay of two excitons, will be entangled in polarization, and both will have opposite circular polarizations, see Section 2.2.2. We must therefore determine the degree of linear polarization (DOLP). The smaller the DOLP, the better, as it will not affect our resulting polarization entanglement fidelity measurement.

The measurement starts with cooling the sample with QDs down to 5 K in a cryostat. We use a mode-locked pulsed Ti:Sapphire laser Chameleon Ultra II from Coherent with 680 nm to 1080 nm tuning range. The 200 fs long laser pulses are narrowed in energy with a 4-f pulse shaper to roughly 9 ps temporal width. The QD is excited with a two-photon excitation (TPE) scheme where the laser energy is tuned to half the energy difference of the $0 - XX$ transition (ground state and the biexciton level) and begins to emit light. The laser light is directed to the cryostat using a 10:90 beam splitter with low polarization sensitivity. The radiation from the QD and the scattered laser beam return from the cryostat through the same beam splitter. Scattered radiation from the laser is filtered out by a series of three notch-filters based on volume Bragg gratings (VBG) with a bandwidth of 0.4 nm each. Therefore, we see only two peaks belonging to X and XX on the resulting spectrum. Experimental scheme is shown in Fig. 3.4 (a).

For DOLP measurment, we place a half-wave plate, a linear polarizer and a detector in the path of the light coming from the QD, see Fig. 3.4 (b). If the light

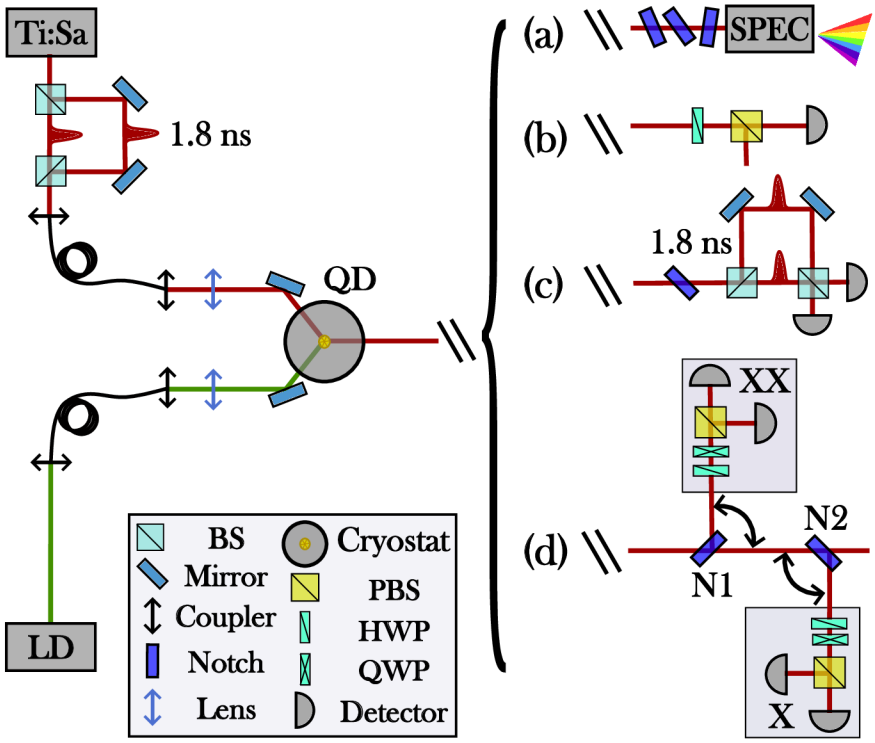


Figure 3.4: Experimental scheme for the characterization of QDs. For simplicity and clarity, we omitted 10:90 BS and sketched the radiation from the lasers going into and out of the cryostat from 3 directions. The red line indicates pulses from the Ti:Sa laser, and the green line represents continuous radiation from the 532 nm laser diode. The diode serves to remove charged excitons. Behind the Ti:Sa laser is a delay line that shifts the pulses by 1.8 ns. All (polarizing) beam splitters have a splitting ratio of 50:50. The figure is further divided into individual schemes according to the measurement of different properties: Scheme for measuring the spectrum of a quantum dot (a), scheme for measuring the degree of linear polarization of photons emitted by a quantum dot (b), scheme for measuring the indistinguishability of photons (c), and scheme for measuring the entanglement of photons (d).

emitted by the QD is not linearly polarized, nothing happens during the rotation of the half-wave plate and the intensity measured by the detector is constant. If, however, the light is linearly polarized, then the intensity at the detector periodically decreases and increases with a typical cosine squared dependence. From this dependence, we can determine the DOLP. Finally, we keep all QDs with low DOLP and write down their positions. We no longer measure with others.

The QD we finally chose for strain tuning and generation of entangled photon pairs has DOLP = 0.05(1).

3.1.2 Lifetime measurement and indistinguishability

Consider a three-level ladder scheme with two decays $XX \rightarrow X \rightarrow 0$. Two photons are emitted in this cascade. The measured photoluminescence spectrum (PL) of X and XX photons is shown in Fig. 3.5. Their wavelength differs by approximately 2 nm. The reason is the Coulomb interaction between the two excitons, which causes XX to have a lower energy, i.e., a longer wavelength. These photons are generally inseparable, but only until the decay rate of the X state vanishes. This nonseparability limits the indistinguishability of photons. The X photon state separability can be quantified by purity $\mathcal{P}$

$$\mathcal{P} = \mathrm{Tr}_{b_{XX\rightarrow X}}\left[\hat{\rho}^2\right] = \frac{\gamma_{XX}}{\gamma_{XX}+\gamma_X}, \tag{3.1}$$

where $\hat{\rho} = \mathrm{Tr}_{b_{X\rightarrow G}}\left[|\psi\rangle\langle\psi|\right] = \int_0^\infty \int_0^\infty \gamma_{XX} e^{i\omega_{XX\rightarrow X}(t'-t)} e^{-\gamma_{XX}(t+t')/2} e^{-\gamma_X|t-t'|/2}$ $b^\dagger_{XX\rightarrow X}(t)|\mathrm{vac}\rangle\langle\mathrm{vac}|b_{XX\rightarrow X}(t')\, dtdt'$ and γ_X (γ_{XX}) is the decay rate of exciton (biexciton), $\omega_{XX\rightarrow X}$ is the frequency of the transition $XX \rightarrow X$, $b^\dagger_{A\rightarrow B}$ ($b_{A\rightarrow B}$) is the time domain creation (annihilation) operator decribing the photonic modes that individual transitions couple (decouple) to. This equation is described in more detail in Ref. [183]. For us, the resulting fraction on the right side of Eq. (3.1) showing the importance of decay rates. It usually holds for QDs that $\gamma_{XX} = 2\gamma_X$. In this case, the maximum purity we can achieve is $\mathcal{P} = 2/3$. At the same time, we can see that the upper bound of photon indistinguishability with maximal coherence for a three-level system in a QD is limited by decay rates of the quasiparticles [183]. We cannot directly measure this theoretical purity value in an experiment. Instead, we measure the two-photon interference and then determine the visibility. Purity and visibility are identical for systems with negligible emission with photon numbers greater than 1 [184].

Two-photon interference is measured using the HOM experiment. Scheme is depicted in Fig. 3.4 (c). We excited the quantum dot with two π-pulses (pulses with the largest population inversion, i.e., creation of a biexciton) delayed by 1.8 ns. This gives us X_E (early) and X_L (late) as well as XX_E and XX_L. These photons then pass through a Mach-Zehnder interferometer with arms of different lengths. This interferometer is equipped with a 1.8 ns delay line. At the output of this interferometer, the photons interfere in a co-polarised configuration and are subsequently detected. The result is a correlation histogram for X and XX containing 5 peaks belonging to all possible combinations of paths that the photons could have taken. If the photons are indistinguishable (we also consider temporal and spatial overlap), there is no peak at zero delay. This result corresponds to the black line in Fig. 3.6. The visibility of the HOM is determined from the values of the intensities in the co- and cross-polarized, and its results

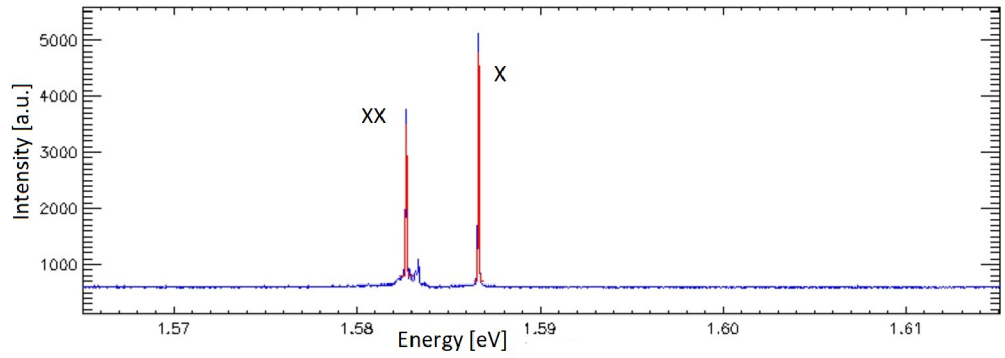
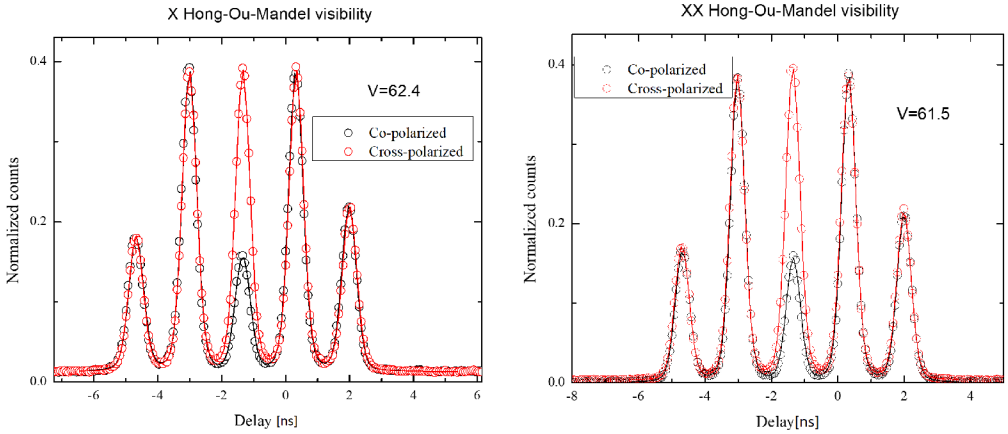


Figure 3.5: Exciton X and biexciton XX photoluminescence (PL) spectrum measured during the experiment. There are no photons from trions or remaining laser beam because they are suppressed by notch-filters.

are $V_{XX} = 61.5\%$ for the biexciton photon and $V_X = 62.4\%$ for the exciton photon, which are values consistent with the theory.



(a) X Hong Ou-Mandel visibility measurement.

(b) XX Hong Ou-Mandel visibility measurement.

Figure 3.6: Measurement of Hong Ou-Mandel visibility of exciton X (a) and biexciton XX (b).

The reduced indistinguishability of the emitted photons is due to the limited visibility that results from the nature of the emission from the three-level QD system. We can also describe this behaviour using finite exciton lifetimes. Biexciton photons are spectrally broadened due to the linewidth of the exciton, which has a finite lifetime. On the other hand, a photon from an exciton has a timing jitter caused by the cascade. Visibility depends on the ratio of lifetimes of both

emitted photons τ_{XX}/τ_X. For large values of this ratio, visibility drops almost to zero [183]. We can influence this ratio with asymmetric Purcell enhancement of these states. This enhancement, influenced by the choice of the cavity, helps achieve near-unity indistinguishability values and entangled photon pairs.

We made measurements of the exciton and the biexciton lifetimes using a spectrometer in which we used a 300g/mm grating. We sent the signal from there to a SPAD with a low time jitter of 70 ps (FWHM) and then to a correlator with a time jitter of 8 ps. The TTL signal from the used photodiode served as a time reference. The instrument response function (IRF) is obtained by sending a 9 ps long laser pulse along the same path. We fitted the data with the model given by the convolution of the IRF with the exponential decay expected from a simple rate equation model of the radiative cascade and extracted the lifetime values. The errors of the obtained lifetimes are determined from a chi-square (χ^2) statistic with a confidence interval enclosed in a 5% increase of the χ^2. In this way, we narrowed down the selection of the remaining QDs, for which we further measured fine-structure splitting.

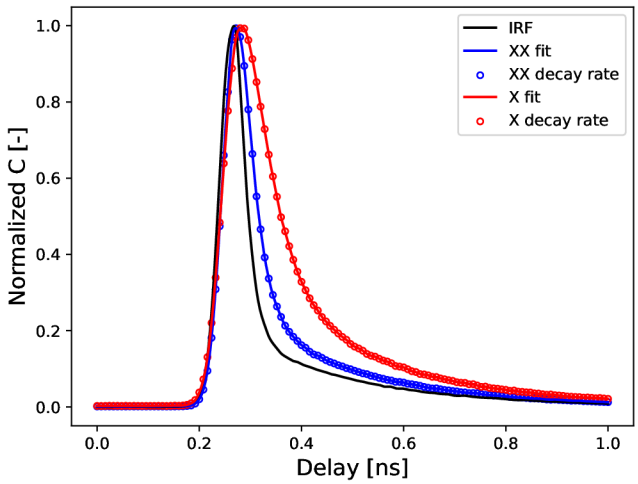


Figure 3.7: Decay rates measurement. We see that the decay rate of the exciton X plotted by red circles and red solid line is larger than that of the biexciton XX plotted by blue dots and blue solid line. For reference, we also plotted the instrument response function (IRF) by solid black line.

The measured lifetimes of the chosen QD are for the exciton $\tau_X = 37(1)$ ps and for the biexciton $\tau_{XX} = 12(1)$ ps. The decay rates of both photons, from which the lifetimes are further determined, are shown in Fig 3.7. To summerize, lifetimes limit the maximum achievable visibility and this is why their measurements are so important. Using different Purcell factors, which are determined

by the properties of the cavity, we can influence the lifetimes of quasi-particles and thus improve the indistinguishability of photons.

3.1.3 Fine-structure splitting measurement

What is fine-structure splitting (FSS) and its undesirable effect on the polarization-entangled photon pairs generation inside QDs was described in Section 2.2.2. Its measurement and subsequent reduction are important for generation of entangled photon pairs from a QD.

The FSS is measured by placing the HWP and linear polarizer in the way of the light emitted by the QD. If the two exitonic levels are degenerate, there is no significant change in their energies during HWP rotation. However, if any FSS exists, the energy values of the two levels are different and are affected by the rotation of the HWP. The larger the FSS, the larger the energy changes difference occurs. Polarization-resolved QD emission spectra are collected at each HWP rotation step using a 1800 g/mm spectrometer grating. The half-amplitude sine fit of the energy difference between the X and XX lines returns the FSS magnitude of the X level. A typical dependence can be seen in Fig. 3.8. The measured FSS values of various QDs reached up to 30 μeV.

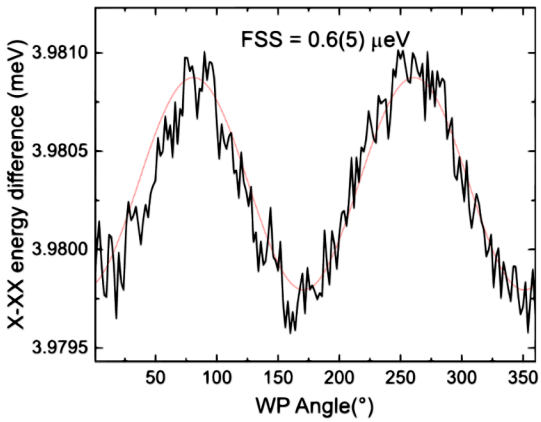


Figure 3.8: Difference of X and XX energy levels depending on HWP rotation. The red line is a fit of the data obtained during the QD measurement. This Figure is taken from the supplementary material of Ref. [185].

3.2 Strain-tuning

After we have characterized the lifetimes of individual quasiparticles of the QD and obtained sufficient extraction efficiency thanks to the Bragg resonator, we still have to solve the FSS that arises from the QD asymmetry. Our method to reduce the FSS is to apply a voltage to the membrane with QDs. Since we only have detectors with finite time resolution, we must reduce the FSS to a value smaller than the natural width of the emission line.

The FSS reduction method in which we can further tune the QD emission was proposed by Trotta et al. in Rome, Italy. A more detailed description is given in Ref. [146]. They designed a device that applies triaxial stress in the plane to change the shape of the QD electronic structure. The idea is as follows: The membrane with QDs is placed on the piezoelectric material. Subsequently, a controlled voltage acting on this membrane causes its volume deformation. In other words, by applying a tunable DC voltage, we can control the amount of stress applied on a particular QD and thus improve its broken symmetry. A mathematical description of this process can be found in Refs. [134, 146].

To achieve voltage tuning, Trotta et al. use a piezoelectric material PMN-PT in which they make three cuts at an angle of 60° with respect to each other. These cuts form six separate areas where we can independently apply voltage with almost no crosstalks. To tune the asymmetry of the QDs, we only need to apply three voltages V_1, V_2, and V_3 on pairs of opposite arms (legs). We choose opposite ones because then the membrane with the QDs cannot move. The six-legged piezoelectric material with QDs membrane is shown in Fig. 3.9.

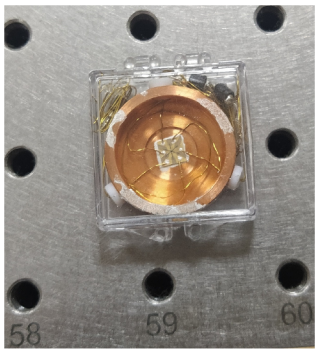


Figure 3.9: Six-legged device made by prof. Trotta et al. in Rome for strain-tuning of the QD.

The measurement of one particular selected QD is shown in Fig 3.10. Here, we used only two channels (two legs) labelled Ch2 and Ch3 with applied voltage to reduce the FSS. We started by measuring the FSS when no voltage was applied.

Subsequently, we left zero values on two of the three channels (Ch1 and Ch2), while on the third (Ch3), we gradually measured the FSS with a step of 50 V. First, we went with the voltage to positive values, and then by reducing the voltage, we returned to zero value. At zero, we continued to decrease the voltage by 50 V. This way we got to negative values. The reason was the fragility of the membrane, which would be destroyed by the application of a larger step. After measuring the voltage on Ch3 from -250 V to 350 V while holding Ch2 and Ch1 at zero values, we came back, as well, with the value of Ch3 at zero. We then changed the voltage on Ch2 by +50V and, leaving Ch1 and Ch2 at zero values, measured the FSS again. Subsequently, we left the value of Ch2 at +50 V and again started to change the voltage of Ch3 from -250V to 350V with the same procedure as in the previous measurement. We repeated this process until we ran the Ch2 scale from -100V to 400V (again slowly returning to zero and only then to negative values).

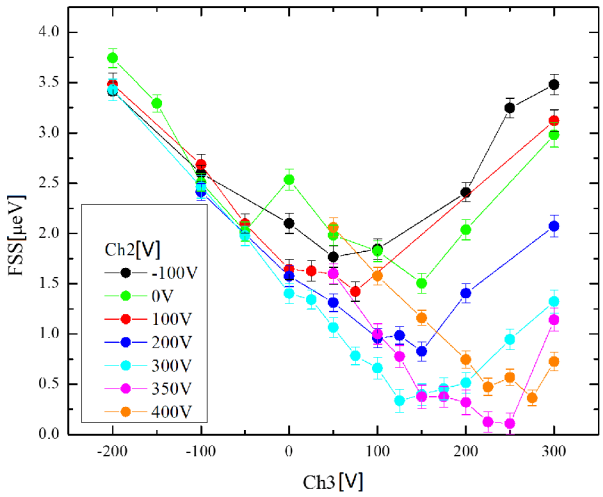


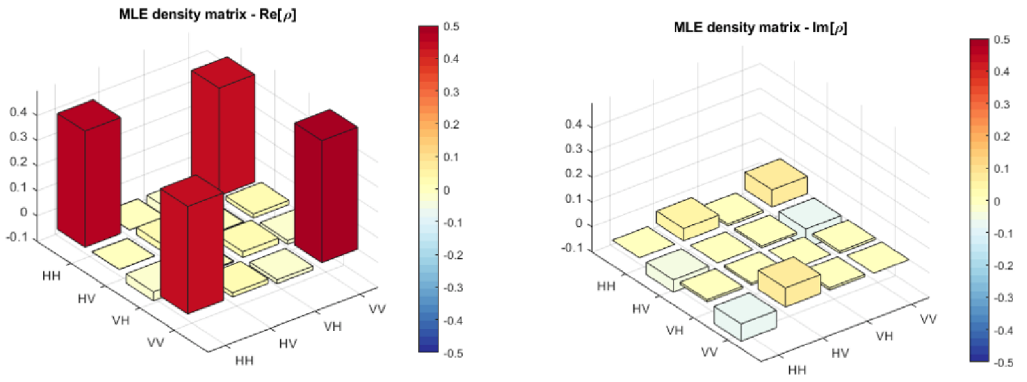
Figure 3.10: Dependence of FSS on the change of two applied voltages on channels Ch2 and Ch3.

We can see from Fig 3.10 that the original FSS value of the selected QD was approximately 2.5 μeV, which corresponds to the green curve with zero voltages on Ch2 and Ch3 channels. By gradually increasing the voltage on both channels through the described process, we achieved the FSS minimal value of 0.2(2) μeV. It corresponds to the purple curve during a set voltage of 350 V on Ch2 and 250 V on Ch3. Furthermore, we see that by further increasing the voltage on Ch2 by 50 V, the FSS value starts to rise again (orange curve).

3.3 Entanglement measures and their measurement

To determine the entanglement of the photons generated during the X and XX recombination process in the QD, we need to reconstruct the two-photon density matrix. Experimental scheme for entanglement measurement is shown in Fig. 3.4 (d). Here, we use notch filters to reflect X (XX) onto the corresponding rotating platform with the polarization tomography measurement components, i.e., polarizing beam splitter (PBS), quarter-wave plate (QWP), and half-wave plate (HWP). The platforms rotate because each QD emits photons with slightly different wavelengths, so the notch filters must be rotated accordingly to these wavelength differences to be able to filter X and XX.

The minimum number of projective measurements on several identical copies of the state for the two-photon density matrix reconstruction is 16. We reconstructed the density matrix by performing 36 projection measurements into different polarization bases states. Subsequently, we applied the maximum likelihood method, MaxLik [93], to obtain the density matrix. Fig. 3.11 shows the real and imaginary parts of the density matrix at the minimum FSS value that we managed to achieve in the experiment. From the knowledge of the density matrix, we can determine the entanglement measure, for example, concurrence defined by Eq. (2.41).



(a) Real part of the density matrix.

(b) Imaginary part of the density matrix.

Figure 3.11: Real (a) and imaginary (b) parts of the density matrix of the entangled photon pair reconstructed using MaxLik during the minimal obtained value of FSS.

Apart from the concurrence, we also evaluate the entanglement fidelity. We use the knowledge that QDs generate a $|\psi^+\rangle$ Bell state (see Section 2.2.2), so we

can determine what overlap our measured state has with this Bell state. Entanglement fidelity F is 1 for perfectly entangled states. Since we know the polarization properties of our setup and we make sure that the radiation emission from the QD is not polarized, we only need a reduced set of 6 co- and cross-polarized coincidence measurements between the two photons of the pair in three polarization bases to determine the entanglement fidelity [186, 187].

From measurements in each polarization basis we can calculate cross-correlation visibilities between the X and XX photons using the relation

$$C_{ij} = \frac{g_{ii}^{(2)}(0) - g_{ij}^{(2)}(0)}{g_{ii}^{(2)}(0) + g_{ij}^{(2)}(0)}, \tag{3.2}$$

where indices i, j represent the two orthogonal polarizations of the chosen basis (HV, DA, RL) and $g^{(2)}(0)$ is the second-order correlation function in $\tau = t_2 - t_1 = 0$. The fidelity of our reconstructed state with the Bell state is then

$$F^{(|\psi^+\rangle)} = \frac{1 + C_{HV} + C_{DA} - C_{RL}}{4}. \tag{3.3}$$

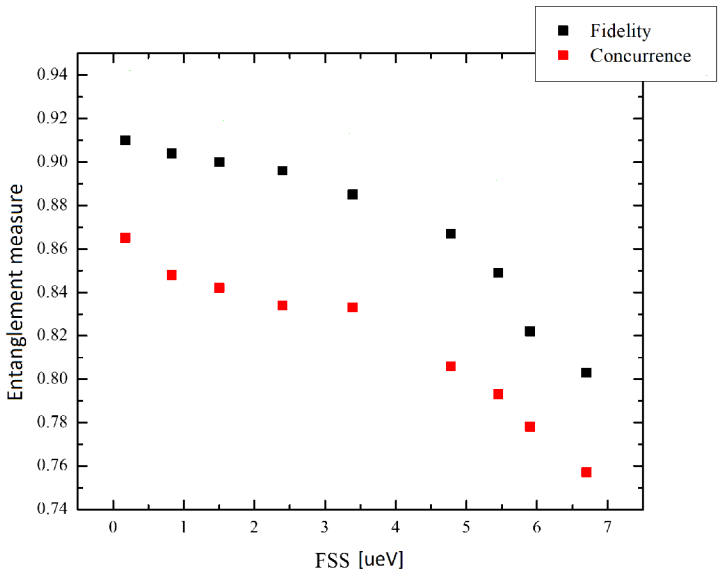


Figure 3.12: Dependence of two different entanglement measures on FSS - concurrence and fidelity. Concurrence is calculated from Eq. (2.41) using the density matrix gained from the full quantum tomography measurement, while fidelity is determined from Eq. (3.3).

The experiment aims to prove that the entanglement measure reaches its maximal value when the FSS is reduced to zero. Measurement results are shown in Fig 3.12. We can see that concurrence and entanglement fidelity are increasing while FSS is decreasing. At the experimentally obtained minimum value of FSS, which is 0.2(2) μeV, the concurrence is maximal and its value is 0.87(1), and the entanglement fidelity reaches also its maximal value, which is 0.91(1).

3.4 Discussion

We have demonstrated a device containing QDs surrounded by an enhanced cavity, i.e., a Bragg resonator, enabling strain-tuning. This device can tune the emission energy of the QD while reducing the FSS between two excitonic levels to almost zero. We managed to increase the extraction efficiency of emitted light to 0.77(5). We measured lifetimes of quasiparticles reaching 12(1) ps for the XX transition and 37(1) ps for the X transition, which corresponds to Purcell factors up to 11. We have shown the effect of different FSSs on the polarization entanglement between the generated photon pairs of the QD. During the experiment, we managed to reduce the FSS value of the QD from 2.5(2) μeV by the applied voltage to 0.2(2) μeV and, thereby, increase the concurrence value to 0.87(1) and the entanglement fidelity value up to 0.91(1). However, considering similar conditions, the probabilities of multiphoton emission are higher if we compare them with the same source type. This could be due to imperfect emission filtering around the XX peak and the remaining poorly filtered backscattered laser beam from the cryostat. The improvement of this device makes it possible to use QDs in the future as sources of entangled pairs used, for example, to demonstrate quantum teleportation or entanglement-based quantum key distribution.

Chapter 4

Deterministic controlled enhancement of local quantum coherence

The resource theory of quantum coherence is gaining more and more interest. Applications range from quantum information processing [53, 188] to metrology [189], thermodynamics [190–192] and even biology [193]. Quantum coherence in terms of resource theory has been described in Section 2.3.

We investigate a remote control and enhancement of quantum coherence. Methods and results described in this Chapter have been published in [A2]. We start from a product state of target system A and control system B, with limited local coherence in each subsystem. The two systems then interact via suitable coupling with a controllable coupling strength, which establishes quantum correlations between A and B. This coupling does not generate any local coherence from input incoherent states. Only incoherent measurements and incoherent operations are allowed locally on systems A and B. We show that for specific intersystem coupling, this procedure can deterministically enhance the local coherence of A while fully preserving its purity, and it works for any pure control state with non-zero coherence. This measurement-based protocol can be iterated and the state of system A can be deterministically steered to a state with maximum coherence. We also show that instead of controlling the coupling strength of the interaction between the two systems, we can consider a fixed coupling strength, and impose a suitable phase shift on the input control system B.

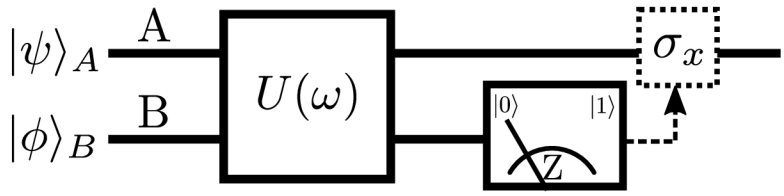


Figure 4.1: Quantum circuit of the measurement-induced quantum coherence enhancement. The target system A and the control system B are coupled by a fixed Hamiltonian and the coupling strength ω can be controlled. Only incoherent operations can be applied locally to the systems A and B. After the interaction with A, the system B is measured in the basis of incoherent states and the measurement outcome is transmitted to A, who can apply a strictly incoherent unitary operation σ_x that flips the basis states $|0\rangle$ and $|1\rangle$.

4.1 Our protocol

We consider the quantum circuit illustrated in Fig. 4.1 with target qubit A and control qubit B initially prepared in pure states

$$|\psi\rangle_A = \cos\alpha|0\rangle + \sin\alpha|1\rangle, \quad |\phi\rangle_B = \cos\beta|0\rangle + \sin\beta|1\rangle, \tag{4.1}$$

where $|0\rangle$ and $|1\rangle$ represent the basis of incoherent states of each qubit. Coherence of pure state $|\psi\rangle$ is quantified by the entropy of probabilities of the basis states $|0\rangle$ and $|1\rangle$,

$$C = h(cos^2\alpha), \tag{4.2}$$

where $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$. The coherence is maximized for balanced superposition state $(|0\rangle + |1\rangle)/\sqrt{2}$, i.e., at $\alpha = \pi/4$ (see Section 2.3.1). As shown in Fig. 4.1, the qubits A and B are coupled via a unitary operation $\hat{U} = \exp(-i\hat{H}t)$ induced by Hamiltonian $\hat{H}$. Subsequently, the control qubit B is measured in the basis of incoherent states and a strictly incoherent operation can be applied to target qubit A depending on the result of measurement on qubit B. The goal of the protocol is to deterministically enhance the coherence of target qubit A while fully preserving its purity. In what follows, we show that this is possible for a non-trivial interaction Hamiltonian $\hat{H}$ that preserves the total population of levels $|1\rangle$, hence it couples only the basis states $|01\rangle$ and $|10\rangle$. Such a Hamiltonian is available for many physical systems including superconducting qubits [194, 195], trapped ions [196] or neutral atoms [197], and thus well motivated. More specifically, we take

$$\hat{H} = ig(|01\rangle\langle 10| - |10\rangle\langle 01|), \tag{4.3}$$

where g is an interaction strength. Consequently, we have

$$\hat{U} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos(gt) & \sin(gt) & 0 \\ 0 & -\sin(gt) & \cos(gt) & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{4.4}$$

This coupling (4.4) does not generate any local coherence if the qubits A and B are initially prepared in incoherent states $\hat{\rho}_A$ and $\hat{\rho}_B$ (i.e., density matrices diagonal in the computational basis). By the local coherence of a system $\hat{\rho}$ we mean a coherence C of its individual qubits, e.g., for an i-th subsystem, the local coherence is $C(Tr_{j\neq i}[\hat{\rho}])$. Although operation in Eq. (4.4) generally introduces correlations between the subsystems, the subsequent partial trace prevents gaining local coherence for initially incoherent states. On the other hand, we will later show that coupling in Eq. (4.4) increases the local coherence of initially partially coherent input qubits.

In our protocol, a nonvanishing coherence of control qubit B represents a resource that can be used to increase the local coherence of qubit A . The protocol requires control of the effective two-qubit coupling strength $\omega = gt$. In practice, this could be achieved, e.g., by choosing the time t when the control system B is measured, thus controlling the effective interaction time. The optimal coupling strength ω can be determined from the requirement that the normalized output states of qubit A $|\psi_0\rangle_A$ and $|\psi_1\rangle_A$, that correspond to projection of qubit B onto $|0\rangle$ or $|1\rangle$, will possess the same coherence. This yields

$$\tan\omega = \frac{\cot\alpha - \tan\alpha}{\tan\beta + \cot\beta}, \tag{4.5}$$

and

$$|\psi_0\rangle_A = \cos\tilde{\alpha}|0\rangle + \sin\tilde{\alpha}|1\rangle, \qquad |\psi_1\rangle_A = \sin\tilde{\alpha}|0\rangle + \cos\tilde{\alpha}|1\rangle, \tag{4.6}$$

where

$$\tan\tilde{\alpha} = \frac{\tan\alpha\cot\beta + \cot\alpha\tan\beta}{\sqrt{\tan^2\beta + \cot^2\beta + \tan^2\alpha + \cot^2\alpha}}. \tag{4.7}$$

The state $|\psi_1\rangle_A$ can be deterministically converted to state $|\psi_0\rangle_A$ by local strictly incoherent unitary operation $\hat{\sigma}_x$ defined in Eq. (2.14). This operation only flips the basis states and cannot increase the coherence of the state.

The above protocol enhances the coherence of target qubit A for any control state $|\phi\rangle_B$ with nonvanishing coherence. Indeed, assuming $0 < \beta < \pi/2$ one can prove the following strict inequalities

$$\min(\tan\alpha, \cot\alpha) < \tan\tilde{\alpha} < \max(\tan\alpha, \cot\alpha), \tag{4.8}$$

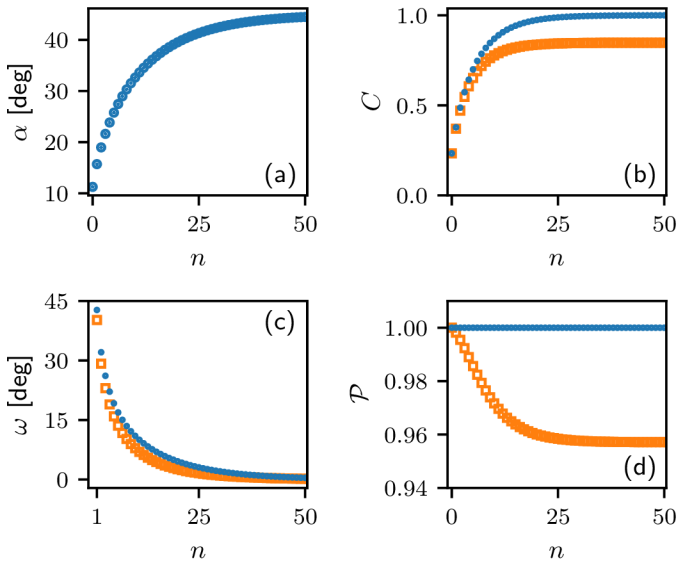


Figure 4.2: Convergence of the deterministic coherence enhancement protocol for $\alpha_0 = \pi/16$ and $\beta = \pi/16$. We plot the parameter α specifying the state of qubit A after n iterations (a), the coherence of qubit A (b), the dependence of the coupling strength ω on the iteration step n (c), and the state purity $\mathcal{P} = \mathrm{Tr}[\hat{\rho}^2]$ (d). Blue circles represent results for the protocol with measurement and feed-forward. For comparison, orange squares indicate results for a scheme without measurement.

which imply $|\tilde{\alpha} - \pi/4| < |\alpha - \pi/4|$. This proves that the coherence of qubit A is enhanced because the angle α gets closer to $\pi/4$. If several copies of control state $|\phi\rangle_B$ are available, we can iterate the protocol and repeatedly apply the map $\alpha \to \tilde{\alpha}$ to asymptotically generate a state with maximal coherence in qubit A. The convergence to $\alpha = \pi/4$ is asymptotically exponentially fast. Assume $\tan\alpha = 1 - \epsilon$ with $\epsilon \ll 1$. Then

$$\tan\tilde{\alpha} \approx 1 + \frac{\cot\beta - \tan\beta}{|\tan\beta + \cot\beta|}\epsilon. \tag{4.9}$$

Since

$$q = \left|\frac{\cot\beta - \tan\beta}{\tan\beta + \cot\beta}\right| < 1$$

we get $\epsilon \to q\epsilon$ and an exponentially fast convergence. We can thus deterministically concentrate the coherence by the measurement and pump it to qubit A starting from several copies of control qubits $|\phi\rangle_B$ with low coherence.

Note that the conditional application of the operation $\hat{\sigma}_x$ to qubit A is not really necessary for deterministic coherence concentration. One can instead keep

track of the measurement outcomes on qubits B and adapt the coupling strength ω at each step accordingly. If the measurement outcome on qubit B is '1', then we instead of $\hat{\sigma}_x$ application select the next $\omega' = -\omega$ where ω is selected using Eq. (4.9). This choice satisfies the condition on equal coherence of output conditional states when the input qubit A has been flipped. The protocol will then deterministically converge to $\alpha = \pi/4$. Typical behaviour of the protocol is illustrated in Fig. 4.2. Note that the coupling strength ω decreases at each iteration of the protocol and asymptotically vanishes.

For comparison, we provide in Fig. 4.2 also results of a simpler protocol that does not involve any measurement and feed-forward. In this latter scheme, we throw away the qubit B after the interaction and we numerically optimize the coupling strength ω at each iteration to maximize the coherence of the output state of qubit A. Note that the state of qubit A becomes mixed in this process as illustrated in Fig. 4.2 (d). Therefore C is evaluated using the general formula for coherence of a mixed state (defined in Eq. (2.52))

$$C(\hat{\rho}) = S(\Delta[\hat{\rho}]) - S(\hat{\rho}), \tag{4.10}$$

where $S(\hat{\rho}) = -\mathrm{Tr}(\hat{\rho}\log_2\hat{\rho})$, and $\Delta[\hat{\rho}] = \rho_{00}|0\rangle\langle 0| + \rho_{11}|1\rangle\langle 1|$ is the density matrix of the completely dephased state. The protocol without measurement does not converge to a maximally coherent state and the coherence saturates at an asymptotic value that is strictly smaller than 1, see Fig. 4.2 (b). This illustrates the importance and usefulness of the measurement and feed-forward that enable us to control and enhance the coherence while fully preserving the purity of the target qubit.

Instead of controlling the coupling strength ω, we can also control the concentration of quantum coherence by applying a phase shift φ to input qubit B, which yields the input control state $\cos\beta|0\rangle + e^{i\varphi}\sin\beta|1\rangle$. This latter approach is less universal, because it works only for a restricted range of input states and coupling strengths, but is appealing because the control of two-qubit interaction is replaced with local control of qubit B. We illustrate this protocol for a maximally entangling two-qubit gate $\hat{U}$ obtained at $\omega = \pi/4$. We again require that the two conditional output states of qubit A $|\psi_{0,1}\rangle$ possess the same coherence. This yields an expression for the phase shift φ,

$$\cos\varphi = \frac{1}{2}\frac{\cot^2\alpha + \cot^2\beta - \tan^2\alpha - \tan^2\beta}{\tan\alpha\tan\beta + \cot\alpha\cot\beta}. \tag{4.11}$$

The condition $|\cos\varphi| \leq 1$ defines the range of α and β for which the protocol works. In particular, this condition is always satisfied if $\alpha = \beta$. Numerical calculations confirm that if the phase shift in Eq. (4.11) exists, then the protocol enhances the coherence of qubit A. Besides the bit flip $\hat{\sigma}_x$ the two conditional

output states of qubit A will differ also by some phase shift δ of the amplitude of state $|1\rangle$ that should be compensated by local strictly incoherent operation $e^{i\delta\hat{\sigma}_z}$, where $\hat{\sigma}_z$ is defined in Eq. (2.16), or tracked and taken into account in the iterative version of the protocol. For $\omega = \pi/4$ we find that the iterative protocol with fixed β and initial point $\alpha_0 = \beta$ will converge to a state with maximum coherence provided that $\pi/8 < \beta < 3\pi/8$.

4.1.1 Experimental realization of a linear opt. partial SWAP gate

We have experimentally tested the proposed protocols with a quantum photonic setup [82, 198], where qubits are encoded into polarization states of single photons. The interaction between the two qubits is provided by a partial-SWAP gate

$$\hat{U}_{\mathrm{PSWAP}} = \hat{\Pi}_+ + e^{i2\omega}\hat{\Pi}_-,$$

where $\hat{\Pi}_- = |\Psi_-\rangle\langle\Psi_-|$ is the projector onto the anti-symmetric singlet Bell state $|\Psi_-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$, $\hat{\Pi}_+ = I - \hat{\Pi}_-$ is projector onto the three-dimensional symmetric subspace of two-qubits, and I denotes the identity operator. Up to unimportant phase shifts of the incoherent basis states, the partial SWAP gate induces the same coupling of states $|01\rangle$ and $|10\rangle$ as the Hamiltonian in Eq. (4.3).

The linear optical partial SWAP gate is schematically illustrated in Fig. 4.3. The gate is formed by a balanced interferometer with additional balanced beam splitter inserted into each of its arms [199]. The coupling strength ω is controlled by the phase shift between the two interferometer arms and is fully tunable. The gate operation is based on two-photon interference at a balanced beam splitter. If the input photons are in a symmetric state, they bunch at the first balanced beam splitter and must propagate through the upper interferometer arm to reach the designated gate outputs. On the other hand, if the photons are initially in the anti-symmetric singlet state, they remain antibunched after interference at BS1 and each photon propagates in one arm of the interferometer, which imposes the phase shift 2ω between the symmetric and antisymmetric states of the two qubits. The gate operates in the coincidence basis and its successful application is heralded by coincidence detection of a single photon in each of the two gate output ports indicated in Fig. 4.3. Similarly to other linear optical quantum gates [198], the gate is probabilistic and its theoretical success probability is $\frac{1}{8}$ irrespective of the coupling strength ω. In the experiment, we automatically post-select the successful events by measuring two-photon coincidences between the two output ports of the gate. Note that this probabilistic nature of the linear optical partial SWAP gate does not preclude testing of our deterministic protocol, because it only reduces the data acquisition rate, but upon success it realizes the

required quantum circuit that could in principle be implemented deterministically on other platforms.

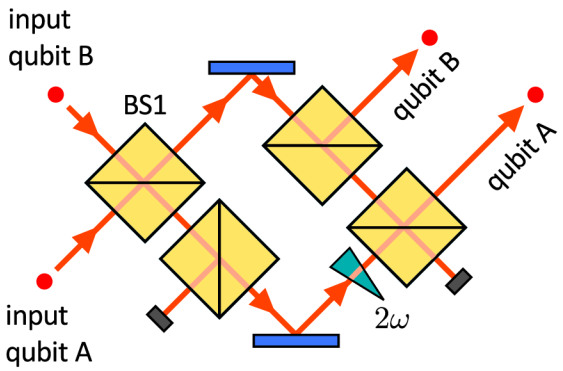


Figure 4.3: Linear optical partial SWAP gate [199]. A Mach-Zehnder interferometer is formed by two balanced beam splitters. Two additional balanced beam splitters are inserted inside the interferometer. The interaction strength ω is determined by the relative phase shift between the interferometer arms. Successful gate operation is indicated by coincidence detection of a single photon in each of the two output gate ports indicated in the figure.

4.1.2 Experimental setup

Detailed experimental setup is depicted in Fig. 4.4. Its core that implements the partial SWAP gate is formed by a displaced Sagnac interferometer, which ensures inherent passive interferometric stability of the setup [200]. Correlated photon pairs are generated in the process of spontaneous parametric down-conversion in a nonlinear crystal pumped by a laser diode (not shown in the figure). The two photons are spatially separated at a polarizing beam splitter and guided to the input ports of the Sagnac interferometer. Polarization states of photons are prepared and controlled with half- and quarter-wave plates and Glan-Taylor prisms. At the output, the photons are detected by single-photon avalanche photodiodes. With this compact and inherently stable setup we have implemented the partial-SWAP gate with unprecedently high gate fidelity that exceeded 0.97 for all tested coupling strengths ω in the interval $[0, \pi/2]$.

The photonic platform employed in our experiment provides a convenient testbed for proof-of-principle demonstration and verifcation of the proposed protocol for controlled enhancement of quantum coherence. Although the coherence of polarization states of single photons could be easily manipulated with the waveplates, we do not use the waveplates for such purpose in the main part of our

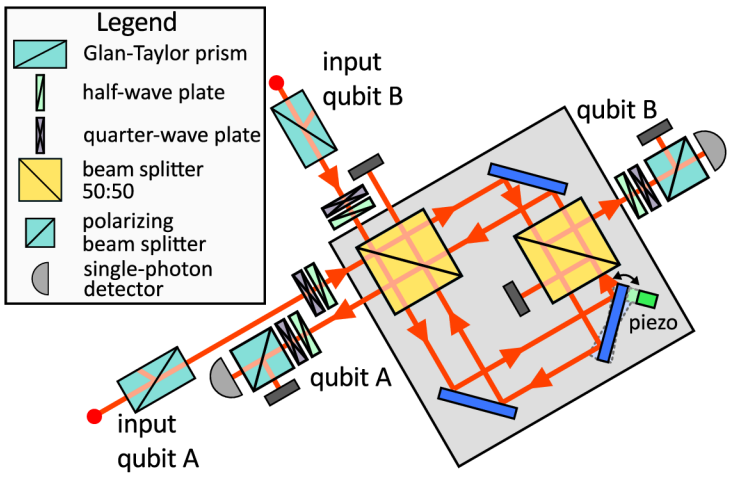


Figure 4.4: Experimental setup. The Mach-Zehnder interferometer is folded into displaced Sagnac interferometer. Polarization states of single photons are controlled and analyzed with the use of wave plates, polarizing beam splitters and Glan-Taylor prisms. Photons are detected by silicon avalanche photodiodes operating in the Geiger mode. The auxiliary detector is used only for the tuning of the interferometric phase.

experiment. We emphasize that we utilize the waveplates solely to prepare the input states and to set the measurement basis for the characterization of the output states. The partial SWAP operation that forms the core of the demonstrated protocol is implemented with a Mach–Zehnder interferometer that does not contain any waveplates. Our results reported below thus confirm the functioning of the protocol, which is applicable to any physical system, including those where the coherence changing-operations can be more experimentally demanding and costly than incoherent operations.

4.1.3 Results

We have first experimentally probed a single step of the coherence enhancement procedure. To compensate for the additional phase shifts induced by the partial SWAP gate, the qubit A was prepared in the state $\cos\alpha|0\rangle + i\sin\alpha|1\rangle$ while the control qubit B was prepared in state $\cos\beta|0\rangle + \sin\beta|1\rangle$. In this measurement, we have probed the symmetric scenario where both qubits A and B initially have the same coherence, $\alpha = \beta$. The two-qubit coupling strength ω is set according to Eq. (4.5). We perform full quantum tomography of the output two-qubit state, reconstruct the density matrix by likelihood maximization [93], and extract from it (non-normalized) density matrices $\hat{\rho}_{A0}$ and $\hat{\rho}_{A1}$ corresponding to the projection of qubit B onto the basis states $|0\rangle$ and $|1\rangle$, respectively. We then apply the

conditional bit flip $\hat{\sigma}_x$ together with a suitable correcting phase shift δ to the reconstructed density matrix $\hat{\rho}_{A1}$ and obtain the overall output state of qubit A, $\hat{\rho}_A = \hat{\rho}_{A0} + e^{i\delta\hat{\sigma}_z}\hat{\sigma}_x\hat{\rho}_{A1}\hat{\sigma}_x e^{-i\delta\hat{\sigma}_z}$.

Alternatively, we can choose only the subset of the two-qubit coincidences that correspond to projections of qubit B onto the computational basis states, and from this restricted data set we directly reconstruct the single-qubit density matrices $\hat{\rho}_{A0}$ and $\hat{\rho}_{A1}$. These two procedures yield very similar results and in what follows we report data obtained with the former procedure.

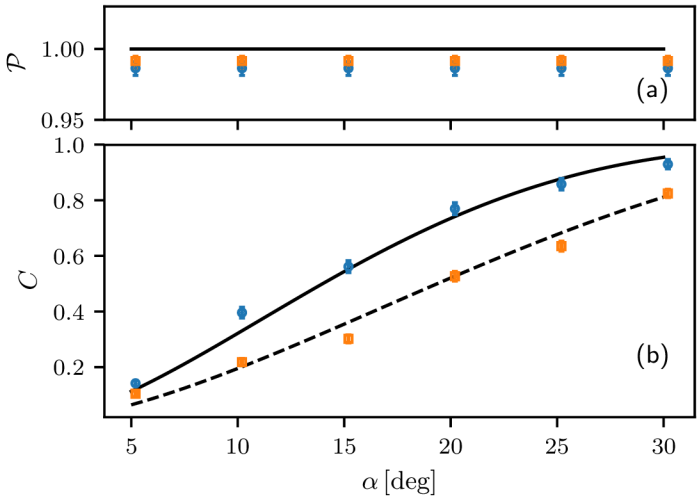


Figure 4.5: Experimental results for a single step of the coherence enhancement protocol with identical input states of qubits A and B, $\alpha = \beta$. The experimentally determined purity $\mathcal{P}$ (a) and coherence C (b) of input (squares) and output (circles) state of qubit A are plotted for 6 different input states. The solid and dashed lines indicate theoretical predictions (they coincide for the purity $\mathcal{P}$).

The experimental results are displayed in Fig. 4.5 for six different values of α. We plot in the figure the coherence of the state C as well as the state purity $\mathcal{P} = \mathrm{Tr}(\hat{\rho}^2)$. Since the experimentally determined states are not exactly pure, we use the general expression for coherence of a mixed state, Eq. (4.10). For reference, the curves in Fig. 4.5 specify the theoretical prediction for an ideal pure-state protocol. We can see that the experimental data closely follow the theoretical expectation. The protocol enhances the local coherence of qubit A while maintaining its very high purity. The input state is practically perfectly pure, with $\mathcal{P} > 0.992$ for all α considered, while the output state becomes slightly mixed. This can be attributed mainly to the imperfections of the two-qubit partial SWAP gate, such as residual phase fluctuations in the interferometer and an imperfect visibility of two-photon interference.

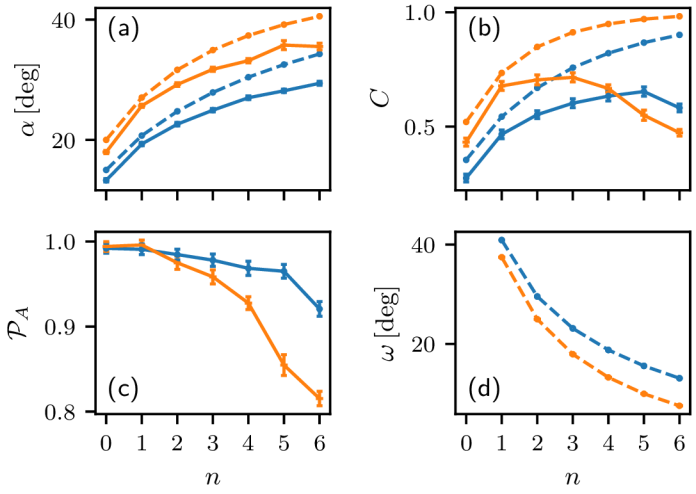


Figure 4.6: Experimental test of iterative coherence enhancement. The effective angle α (a), coherence (b) and purity (c) of qubit A and the coupling strength ω (d) are plotted in dependence on the number n of steps of the protocol. The results are presented for two different inputs $\alpha_0 = \beta = 15^\circ$ (blue) and $\alpha_0 = \beta = 20^\circ$ (orange). Symbols represent experimental data, solid lines guide the eye, and dashed lines indicate theoretical predictions. Data at $n = 0$ represent the reference input state.

Here and in the rest of this Chapter, the error-bars represent one standard deviation and were obtained using parametric bootstrapping. With the knowledge of reconstructed states, measurement operators, mean count-rate in the tomogram, and under the assumption of the Poissonian distribution of measured coincidence numbers, we generated 1000 tomograms, processed them the same way as the original tomograms, obtaining a set for each quantity of interest (e.g. coherence, purity). We evaluated the standard deviation of this set. For quantities of interest near its theoretical boundary, purity in this case, we instead found 0.158 and 0.84 quantiles and used them to plot asymmetrical error-bars, in which lies 68.2% of all samples, equivalently to one standard deviation.

Having verified the functioning of a single step of the protocol, we now proceed to experimental test of the iterative coherence enhancement scheme. At each step, we determine the output density matrix $\hat{\rho}_A$ of qubit A and use it as an input state of the next step of the protocol, while keeping the state of qubit B (i.e., the angle β) fixed at each step. The suitable coupling strength ω is at each step again determined from Eq. (4.5), where the angle α is chosen according to theoretical prediction for ideal pure state protocol, c.f. Fig. 4.2. We prepare a mixed polarization state $\hat{\rho}_A$ of a single photon by preparing a statistical mixture of the two eigenstates of $\hat{\rho}_A$ with weights equal to the corresponding eigenvalues. We

start the iterative protocol from a symmetric input, $\alpha_0 = \beta$. In Fig. 4.6 we plot the experimental results for two different initial coherences, $\alpha_0 = 15^\circ$ and $\alpha_0 = 20^\circ$.

The figure displays the coherence and purity of the state after each step of the protocol, together with the effective angle α determined from the dominant eigenstate of $\hat{\rho}_A$, and the utilized two-qubit coupling strength ω. For $\alpha_0 = 15^\circ$ we observe that the coherence increases up to 5th step of the protocol while for $\alpha_0 = 20^\circ$ the coherence of qubit A reaches its maximum already at the 3rd step and then drops down. The reason for this behavior is that the experimental imperfections accumulate and reduce the purity of $\hat{\rho}_A$ after each step of the protocol, c.f. Fig. 4.6 (d). Therefore, although the effective angle α increases at each step and closely follows the theoretical prediction, as shown in Fig. 4.6 (a), the noise eventually begins to reduce the coherence of the state. These data illustrate the sensitivity of the quantum coherence manipulation protocol to noise and imperfections. Thanks to the very high fidelity of our linear optical partial SWAP gate we were able to observe the improvement of coherence up to 5 iterations of the protocol.

The difference in coherence maxima positions in Fig. 4.6 is related mainly to the partial SWAP gate implementation. Computational basis states $|01\rangle$ and $|10\rangle$ are coupled by the partial SWAP gate, and the coupling strength ω is determined by the interferometric phase $\varphi = 2\omega$. Therefore, the output populations of $|01\rangle$ and $|10\rangle$ are sensitive to φ and vulnerable to phase noise. These populations increase as the parameters α and β get closer to $\pi/4$, and therefore the protocol becomes more vulnerable to dephasing in this limit. Moreover, the phase misalignment breaks the condition $|\psi_0\rangle_A = \hat{\sigma}_x|\psi_1\rangle_A$, which increases the mixedness of the output state. Also, this effect becomes more pronounced when α and β get closer to $\pi/4$, because then the probabilities of the two measurement outcomes on qubit B become more balanced.

Finally, we have experimentally tested the alternative protocol, where the coupling strength ω is fixed and at each step of the protocol we adjust the phase of qubit B to enhance the coherence of qubit A. Experimental results for this protocol are displayed in Fig. 4.7. We set $\omega = \pi/4$ hence we employ the maximally entangling $\sqrt{\text{SWAP}}$ gate as considered in the preceding theoretical analysis. The left panels show results for $\alpha_0 = 20^\circ$, when this protocol cannot be iterated to infinity and terminates after second step, because the phase shift in Eq. (4.11) that should be applied to the control qubit B does not exist anymore. In Fig. 4.7 (b) we present results for $\alpha_0 = 25^\circ$. In this case the protocol can be arbitrarily iterated and in theory should converge to a maximally coherent state. In practice, we observe that the coherence grows up to third iteration and then it begins to moderately decrease again as the noise accumulates.

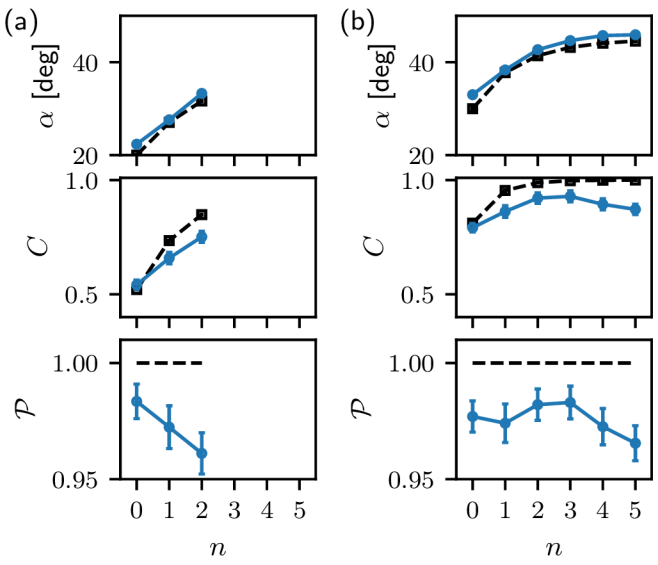


Figure 4.7: Experimental results for iterative protocol with fixed coupling strength $\omega = \pi/4$ and control exercised by phase shifts applied to input qubit B. The coherence, purity and effective angle α of qubit A are plotted for two different inputs $\alpha_0 = \beta = 20^\circ$ (a) and $\alpha_0 = \beta = 25^\circ$ (b). Data at $n = 0$ represent the reference input state. Blue dots are experimental data, black squares show the theoretical prediction for comparison. The lines are to guide the eye.

4.1.4 Coupling strength setting

The coupling strength setting is an important part of our experiment, hence we discuss it in more detail. The coupling strength ω is controlled using a Sagnac interferometer. One of the mirrors inside this interferometer is mounted on a piezoelectric device. By applying a voltage, we can tilt the mirror and thus slightly change the phase φ of the interferometer. By changing the interferometric phase φ, we simultaneously set the two-photon coupling strength ω because they depend on each other by the relation $\varphi = 2\omega$. In Fig 4.8, we see the dependence of the detected counts on the two outputs of our experiment in 0.1 s on the tilting of the mirror. This tilting also changes the coupling efficiency at the individual outputs, resulting in the observation of different local maxima.

We first tried to set the interferometric phase φ to the specific value by measuring the typical behaviour shown in Fig. 4.8. In this way, we found out from the fit which setting of the mirror tilt corresponds to the desired number of counts at the experiment outputs (and therefore the desired coupling strength ω).

When we set the values for the correct mirror tilt determined from the fit, we encountered a problem with the hysteresis of the piezoelectric device. In

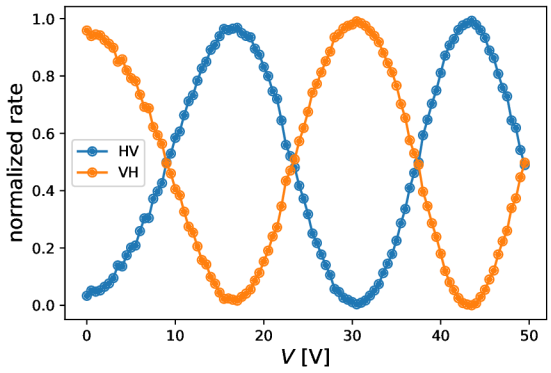


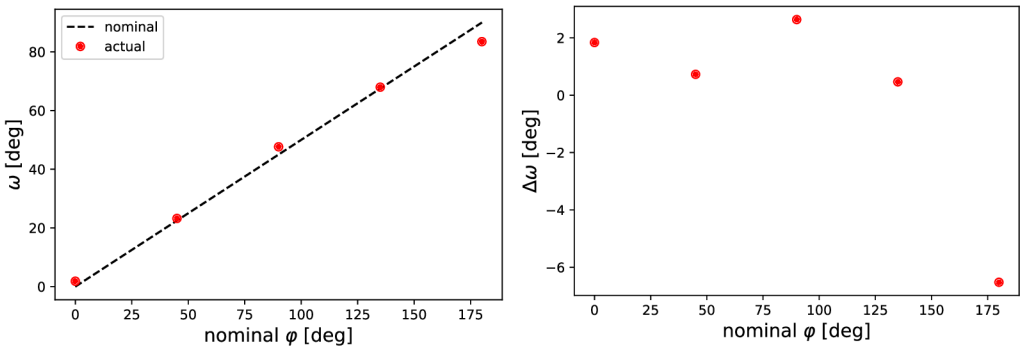
Figure 4.8: A typical interference pattern while the mirror is tilted using a piezoelectric device inside the Sagnac interferometer. We see the number of detections in 0.1 s on the two outputs of the experiment depending on the applied voltage on the piezoelectric crystal. Due to the mirror tilt, the coupling efficiency slightly changes, and we observe different local maxima.

other words, when we repeatedly apply the voltage to the mirror, the number of counts at the outputs change. Therefore, we had to find another solution to the problem. We have separated the mirror tilt settings into several areas. The area with approximately linear dependence, which corresponds to the values $10^\circ \leq |\varphi| \leq 170^\circ$, and two other areas $0^\circ - 10^\circ$ and $170^\circ - 180^\circ$ with nonlinear dependence.

The method with a fit is still sufficient for the first mentioned area. However, we have added a few more steps to improve this method. The procedure is as follows: We fit the scanned interference fringe with a quadratic dependence of the fringe envelope and a quadratic dependence of the phase on the voltage. According to the specific phase, we can calculate from the fit the correct voltage that we set on the piezo, and the setpoint of the normalized intensity I_{tgt}. After this step, we start the method of proportional regulation, where we tune the voltage on the piezo V by a step ΔV according to the relation $\Delta V = \pm k(I - I_{tgt})$, where I is the currently normalized value on the detector, $k = 2$ V is the feedback strength. We choose the sign depending on whether we set the intensity on the rising or the falling edge of the interference fringe and we also take into account the actual value of voltage on the piezo. We terminate the procedure when the change $(I - I_{tgt})$ is smaller than the set threshold. The typical accuracy of setting the phase in this area is approximately $\pm 2^\circ$.

In the $0^\circ - 10^\circ$ and $170^\circ - 180^\circ$ areas, we set the phase using the "scan and stop" method. We can describe this method in this way: 'When you come across the required value plus or minus some minimum value, stop to scan and start to

measure.' We test the accuracy of the phase setting in the interval $0^\circ - 180^\circ$ with the step of 5°. The deviations from the desired phase are plotted in Fig. 4.9. The accuracy of the setting is on average $\pm 2^\circ$. For both methods, we rescan the fringe from time to time to get rid of the effect of slow drift and the gradual appearance of additional hysteresis.



(a) Phase setting **(b)** Phase deviation

Figure 4.9: Interferometric phase setting measurement. The interferometric phase φ is connected to the coupling strength ω by the relation $\varphi = 2\omega$. The black dashed line marks the value that we want to set. Red dots are the measured actual phase settings in the experiment (a). Plotted deviations obtained from (a) by calculating the subtraction of the measured phase values from the expected ones (b).

To verify our methods, we have one more way to determine the phase. It is based on a population ratio where $\varphi = 2\omega = 2\arctan\left(\sqrt{\frac{\langle VH|\hat{\rho}|VH\rangle}{\langle HV|\hat{\rho}|HV\rangle}}\right)$. We try to set the desired phase using the methods mentioned above and estimate the actually set phase with this calculation. The results are in Fig. 4.10 and indicate the presence of both - systematic and random errors.

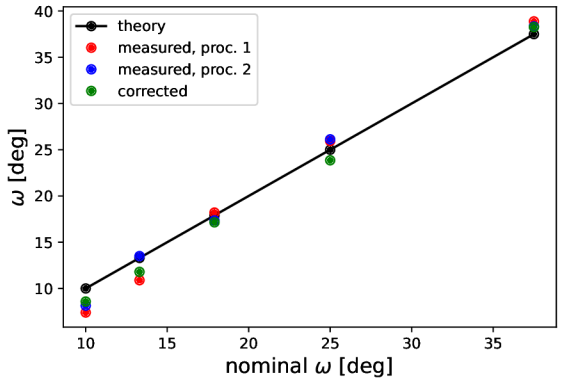


Figure 4.10: Set values of the coupling strength ω. The black points are the desired values. The red and blue points are the two different (measured) values of ω, which are set using the described procedures, and the green points are the measured attempts to correct the ω value setting from population ratio.

4.2 Discussion

We have presented and experimentally tested a novel protocol for control and enhancement of quantum coherence under a restricted set of operations that include local strictly incoherent operations and measurements, feed-forward, and fixed interaction Hamiltonian with tunable coupling strength. We have observed that the quantum coherence of the target system can be remotely deterministically controlled and steered to a maximally coherent state within this setting. The considered set of operations is practically motivated, because the strictly incoherent operations and measurements are usually easy to implement and also the considered interaction Hamiltonian (4.3) is physically well motivated and available for many experimental systems and platforms such as superconducting qubits, trapped ions and neutral atoms [194–197].

While we have presented the protocol for two-dimensional systems (qubits), extension to higher-dimensional systems is possible. Consider interaction Hamiltonian $H_{jk} = ig(|jk\rangle\langle kj| - |kj\rangle\langle jk|)$. Following the above protocol and utilizing a control system B prepared in superposition of states $|j\rangle$ and $|k\rangle$, one can enhance the quantum coherence of target system in a two-dimensional subspace spanned by $|j\rangle$ and $|k\rangle$. One can then apply a unitary permutation operation $\hat{U}_\pi = \sum_j |\pi(j)\rangle\langle j|$ to the target system to address a different subspace and repeat the whole procedure to drive the state of the target system A towards the maximally coherent state. One can also consider variants of this protocol, where one can switch on and off couplings of different pairs of quantum levels $|j\rangle$ and $|k\rangle$ or even simultaneously switch on several such elementary couplings.

Chapter 5

Mutual coherence from separable coherent qubits

The concept of mutual coherence was introduced in Section 2.3.4. This quantum coherence characterizes the amount of quantum coherence in a global composite system that is not contained in the local states of its subsystems. We noted that this type of quantum coherence describes quantum correlations that can differ from entanglement. This Chapter is based on publication [A3].

We investigate quantum states that maximize mutual coherence in various subspaces of the two-qubit Hilbert space. Maximum mutual coherence in different subspaces of the Hilbert space of a pair of qubits cannot always be achieved by using some maximally coherent state. Therefore, we study individual cases with caution. We investigate the characterization of states with maximal mutual coherence in subspaces of dimension $\{2, 3, 4\}$. We quantify the coherence by the relative entropy of coherence, see Section 2.3.3. For this coherence measure, our results reveal a non-trivial structure of the optimal states in dimension 3 of the Hilbert space.

Subsequently, we have generated the optimal states in a linear-optical proof-of-principle experiment. We have realized strictly incoherent two-qubit quantum filters capable of transforming an initial product state of two qubits with a certain amount of local coherence into a state maximizing the mutual coherence. Furthermore, we have also prepared the optimal states via a sequence of unitary operations, which involves single-qubit transformation outside the class of strictly incoherent operations.

5.1 Mutual coherence and subspaces of the Hilbert space

For a pair of d-dimensional quantum systems, the mutual coherence is maximized by a maximally entangled state

$$|\Psi\rangle = \frac{1}{d} \sum_{j,k=0}^{d-1} e^{\frac{2\pi i j k}{d}} |j\rangle|k\rangle, \tag{5.1}$$

where $|j\rangle$ denotes the basis of free states with zero coherence. The state $|\Psi\rangle$ exhibits complete symmetry in the sense of equal probabilities of basis states $|j\rangle|k\rangle$. However, applications may require coherence to be contained in a specific subspace of the full Hilbert space. If we impose a constraint that the state $|\psi\rangle$ can be formed by superposition of N free product states $|jk\rangle$ only, where $N < d^2$, the optimal state that maximizes the mutual coherence in such subspace can become nontrivial and not a maximally entangled state. We investigate this interesting phenomenon for the simplest nontrivial composite Hilbert space of a pair of qubits ($d = 2$) and $N = 3$. In our study, we quantify the coherence by the relative entropy of coherence, Eq.(2.58), which is a well-behaved additive measure of coherence.

We identify the optimal state for the $d = 2$, $N = 3$ setting and find that it exhibits uneven populations of the three basis states and, therefore, does not represent a state with maximum global coherence in the given subspace of the full Hilbert space. We then generate this optimal state experimentally from the easily accessible product state of individual qubits. We aim at the preparation of the optimal state by the free transformation of the resource theory, namely by a probabilistic strictly incoherent operation represented by a single Kraus operator diagonal in the basis of free states [201, 202]. For comparison, we also test an alternative preparation scheme based on a combination of the quantum CZ gate and a local single-qubit unitary operation that couples the basis states $|0\rangle$ and $|1\rangle$.

Our work reveals that care is needed if one considers transformations of different forms of coherence between each other in a compound system. If one aims at gaining maximum mutual coherence, the form shared among subsystems and not being present only locally, one can not directly assume this condition is fulfilled by some maximally coherent state. On the contrary, individual cases should be examined separately with caution.

5.2 Description

Mutual coherence combines together the concepts of coherence and quantum correlations differently from entanglement. Naively, one could conjecture that maximally entangled states maximize the mutual coherence among all pure states in a given considered class. Interestingly, we find that this is not always the case. We focus on a system composed of two qubits and consider pure states that are formed by the superposition of N free basis states $|jk\rangle$, where $j,k \in \{0,1\}$. For $N = 2$ and $N = 4$, we find that the mutual coherence is indeed maximized for maximally entangled states,

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \tag{5.2}$$

and

$$|\psi_4\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle). \tag{5.3}$$

We have $C_M(\psi_2) = 1$ and $C_M(\psi_4) = 2$, which saturates the bound $C_M = \log_2 N$ on mutual coherence of a pure bipartite state formed by the superposition of N free states $|jk\rangle$. By contrast, for $N = 3$, we found by an exhaustive numerical search that the pure state that maximizes C_M is formed by an unbalanced superposition of the three basis states,

$$|\psi_3\rangle = c|11\rangle + \sqrt{\frac{1-c^2}{2}}\,(|01\rangle + |10\rangle)\,, \tag{5.4}$$

where $c \approx 0.277$ and $\sqrt{\frac{1-c^2}{2}} \approx 0.679$.

For this state, we get $C_M(\psi_3) \approx 1.1$, which exceeds the maximum mutual coherence achievable by the superposition of two free basis states. The most interesting feature of the optimal state $|\psi_3\rangle$ is the strong imbalance in absolute values of probability amplitudes, meaning that this state is *not maximally coherent* in the sense of the ordinary coherence C of the total state. In fact, the maximally coherent [201] analog of $|\psi_3\rangle$, $|\phi_3\rangle = 1/\sqrt{3}\ (|11\rangle + |10\rangle + |01\rangle)$, exhibits a suboptimal value of the mutual coherence, $C_M \approx 0.85$. The state $|\psi_3\rangle$ can be seen as a superposition of the maximally entangled state $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ and a product state $|11\rangle$. When we form the linear combination defined in Eq (5.4) and begin to increase the value of c, we increase the coherence of the total state, but we also introduce nonzero local coherences. While the first effect increases the mutual coherence, the other tends to reduce it, and it turns out that the maximum occurs for a specific unbalanced superposition.

Let us conclude this section by noting that the states $|\psi_j\rangle$ are representatives of whole classes of optimal states because local bit flips $\hat{\sigma}_x$ defined by Eq. (2.14)

and phase shifts $\exp(i\theta\hat{\sigma}_z)$, where $\hat{\sigma}_z$ is defined by Eq (2.16), do not change the mutual coherence and also do not change the number of free basis states in the superposition.

5.3 Experimental setup

We next investigate experimental preparation of the optimal states $|\psi_j\rangle$ from input product states $|\varphi_A\rangle|\varphi_B\rangle$ with vanishing mutual coherence. We mainly focus on the non-trivial optimal state $|\psi_3\rangle$, and we generate this state on a quantum photonic platform where qubits are encoded into polarization states of single photons.

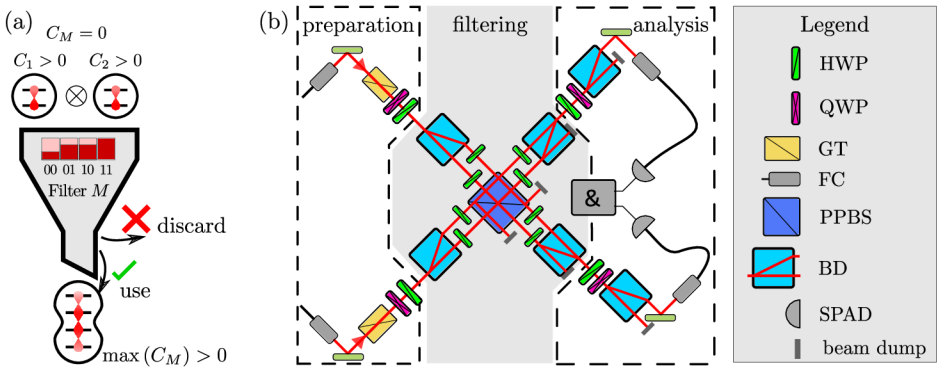


Figure 5.1: Mutual coherence generation by a strictly incoherent quantum filter from input product state with $C_M = 0$. Shown are the conceptual scheme of the protocol (a) and the experimental setup (b). "HWP" is a half-wave plate, "QWP" is a quarter-wave plate, "GT" is the Glan-Taylor polarizer, "PPBS" is a partially polarizing beam-splitter, "BD" is a beam-displacing crystal, "FC" is a fiber coupler, and "SPAD" is a single photon avalanche detector [203].

Our first strategy, illustrated in Fig. 5.1 (a), is based on application of a suitable probabilistic strictly incoherent quantum operation [201] represented by a single Kraus operator $\hat{M}$ diagonal in the basis of free states,

$$\hat{M} = A|00\rangle\langle 00| + B(|01\rangle\langle 01| + |10\rangle\langle 10|) + C|11\rangle\langle 11|, \tag{5.5}$$

and satisfying $\hat{M}^\dagger\hat{M} \leq \mathbb{1}$. This quantum filter transforms a pure input state $|\psi_{\rm in}\rangle$ onto a pure output state $|\psi_{\rm out}\rangle = \hat{M}|\psi_{\rm in}\rangle/\sqrt{P_S}$, with success probability $P_S = \langle\psi_{\rm in}|\hat{M}^\dagger\hat{M}|\psi_{\rm in}\rangle$. Choosing a symmetric product input state

$$|\psi_{\rm in}\rangle = \left(\sqrt{p}|1\rangle + \sqrt{1-p}|0\rangle\right)^{\otimes 2}, \tag{5.6}$$

the optimal state $|\psi_3\rangle$ can be obtained by a filter that completely eliminates the state $|00\rangle$, $A = 0$, and

$$\begin{aligned} \hat{M}_- &= q(|01\rangle\langle 01| + |10\rangle\langle 10|) + |11\rangle\langle 11|, \qquad p \leq p_{\mathrm{th}}, \\ \hat{M}_+ &= |01\rangle\langle 01| + |10\rangle\langle 10| + q^{-1}|11\rangle\langle 11|, \qquad p > p_{\mathrm{th}}. \end{aligned} \tag{5.7}$$

Here $p_{\mathrm{th}} = 2c^2/(1+c^2)$ and $q^2 = p(1-p_{\mathrm{th}})/[p_{\mathrm{th}}(1-p)]$.

In our experiment, time-correlated photon pairs are generated in the process of spontaneous parametric down-conversion in a nonlinear crystal pumped by a CW laser diode [204] and guided to the main setup depicted in Fig. 5.1 (b). Initially, one photon is polarized vertically and the other horizontally, and we associate the H/V basis with the computational basis. Polarization states of single photons are manipulated by a combination of quarter- and half-wave plates. The quantum filter $\hat{M}$ is implemented by two-photon interference in a suitably designed inherently stable multimode interferometer [203, 205] composed of calcite beam displacers, partially polarizing beam splitter and wave plates. Parameters of the filter are determined by the angular positions of wave plates neighbouring the central PPBS. Successful filtering is heralded by the presence of a single photon at each output port of the filter, similarly to linear optical quantum gates operating on a coincidence basis. With our scheme, we can directly implement the quantum filters $\hat{M}_-$. This is not a significant restriction, because for $p > p_{\mathrm{th}}$ the filter $\hat{M}_+$ could be obtained as a combination of easily implementable local single-qubit amplitude attenuations $|0\rangle\langle 0| + q^{-1}|1\rangle\langle 1|$ and an accessible filter $\hat{M}_0 = |01\rangle\langle 01| + |10\rangle\langle 10| + |11\rangle\langle 11|$.

5.3.1 Results

We have applied the quantum filters to a range of input states (5.6). For $p > p_{\mathrm{th}}$ we have employed the filter $\hat{M}_0$ while for $p \leq p_{\mathrm{th}}$ we have applied the optimal filter $\hat{M}_-$ specified in Eq. (5.7). The output two-qubit states were comprehensively characterized by quantum state tomography based on the maximum likelihood reconstruction algorithm, MaxLik [93]. The optical elements in our setup introduce additional single-qubit local phase shifts. These phase shifts do not modify the coherence properties of the state and were compensated in data processing by suitable local single-qubit unitaries $\exp(i\theta_A\hat{\sigma}_{z,A}) \otimes \exp(i\theta_B\hat{\sigma}_{z,B})$ applied to the reconstructed density matrix. The experimentally generated state for $p = 0.125$ is plotted in Fig. 5.2 (c), and the dependence of C_M on p is displayed in Fig. 5.2 (d). Parameters characterizing the prepared state plotted in Fig. 5.2 (c) are summarized in Table 5.1, which displays state fidelity $\mathcal{F}$ with the ideal target state, state

purity $\mathcal{P} = \mathrm{Tr}[\hat{\rho}^2]$, mutual coherence C_M, and the residual population p_{00} of state $|00\rangle$.

preparation	D	$\mathcal{F}$	$\mathcal{P}$	C_M	p_{00}
$\hat{M}_-$	3	0.914(7)	0.92(1)	0.78(2)	0.072(5)
$\hat{V}_B\hat{U}_{CZ}$	3	0.935(6)	0.93(1)	1.18(2)	0.035(3)
$\hat{U}_{CZ}$	4	0.95(1)	0.92(2)	1.70(6)	-

Table 5.1: Fidelity, purity, mutual coherence, and population of state $|00\rangle$ are displayed for two experimentally generated states $|\psi_3\rangle$ and also state $|\psi_4\rangle$. The experimental uncertainties specified in parentheses represent one standard deviation. The first column indicates how the output state was prepared from a suitable input product state. $\hat{M}_-$ is a filter defined in Eq. (5.7), $\hat{V}_B$ is a local unitary operation and $\hat{U}_{CZ}$ is a quantum CZ gate operation.

The observed mutual coherence $C_M = 0.78(2)$ is significantly lower than the theoretical expectation $C_M(\psi_3) \approx 1.1$, which is mainly caused by imperfect filtering that leaves some residual population in state $|00\rangle$, see Fig. 5.2 (e), as well as residual coherence between this state and the other basis states, see Fig. 5.2 (c,e). This leads to higher local coherences, and consequently, the mutual coherence is reduced. As illustrated in Fig. 5.2 (a), the state $|00\rangle$ is initially dominantly populated, which makes the complete elimination of this state particularly experimentally challenging and sensitive to imperfections. To further confirm the origin of the experimentally observed sub-optimal value of C_M, we have artificially eliminated the population of $|00\rangle$ in the reconstructed density matrices and renormalized them. The orange points in Fig. 5.2 (d) show that the resulting mutual coherence is close to the theoretical prediction.

For comparison, we have also pursued an alternative preparation strategy based on unitary transformation of a suitably chosen asymmetric input product state

$$|\psi_{\mathrm{in}}\rangle = (\cos(x)|0\rangle + \sin(x)\|1\rangle) \otimes (\cos(y)|0\rangle + \sin(y)|1\rangle)\,,$$

where

$$\cos(x) = \sqrt{\frac{1-c^2}{2}}, \qquad \sin(2y) = \sqrt{\frac{1-c^2}{1+c^2}}.$$

This state can be transformed to the state (5.4) by a sequence of the maximally entangling quantum CZ gate $\hat{U}_{CZ} = \exp(i\pi|11\rangle\langle 11|)$ followed by local unitary operation $\hat{V}_B = \exp[i(\pi/2 - y)\hat{\sigma}_y]$ on qubit B, where $\hat{\sigma}_y$ is defined by Eq (2.15). We have configured our setup to realize the quantum CZ gate [206–208], which corresponds to the choice $A = B = 1$ and $C = -1$ in Eq. (5.5). The local unitary operation $\hat{V}_B$ was implemented with a half-wave plate. We have experimentally

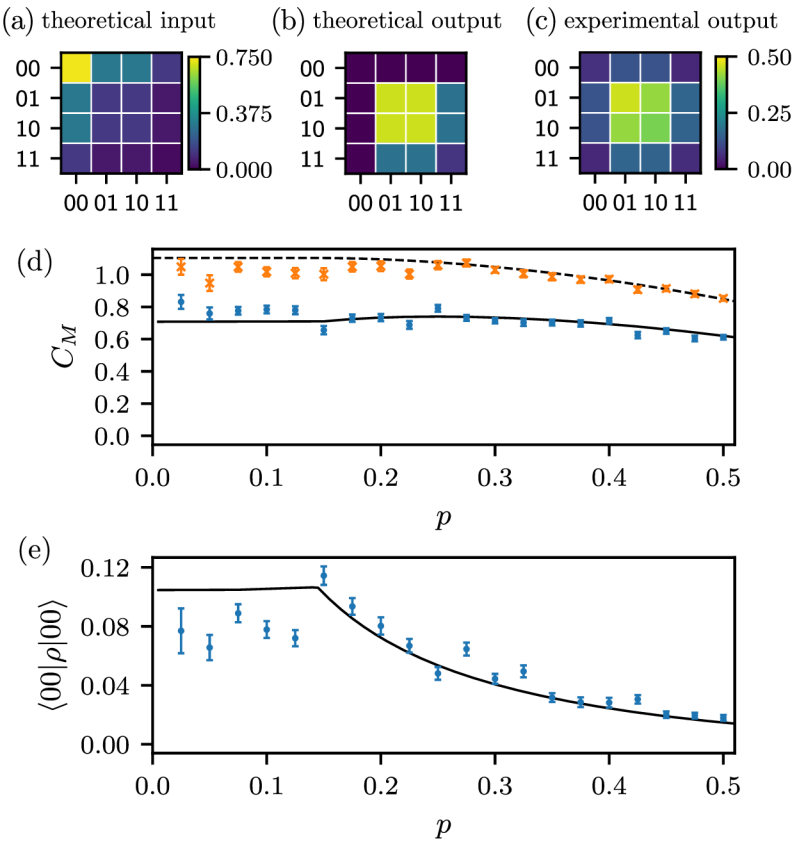


Figure 5.2: Generation of mutual coherence from product two-qubit state. As an example, we plot the real parts of density matrices of the theoretical input product state with $p = p_{\text{th}}$ (a), the corresponding theoretical output state $|\psi_3\rangle$ obtained after application of the filter $\hat{M}_-$ (b), and the actual experimental output state (c). The imaginary parts of the theoretical density matrices vanish. We also display the dependence of the mutual coherence of the output state on the input state excitation probability p (d) and the residual population of the unwanted level $|00\rangle$ (e). Blue dots represent experimental data, and the orange crosses are experimental data after numerical elimination of the level $|00\rangle$ by filter $\hat{M}_0 = \mathbb{1} - |00\rangle\langle 00|$. Solid lines indicate the predictions of a theoretical model of the setup, and the dashed line is the ideal theoretical dependence for a perfect setup. The employed quantum filters are specified in the main text.

probed the generation of the whole single-parametric class of states defined by Eq. (5.4) with $0 < c < 1$.

The experimental results are displayed in Fig. 5.3. As an illustration, we present in Fig. 5.3 (c) the reconstructed experimentally generated state for nominal target value $c = 0.264$, which has the highest fidelity among all generated states with the target state $|\psi_3\rangle$. Note that the actual parameters of the gener-

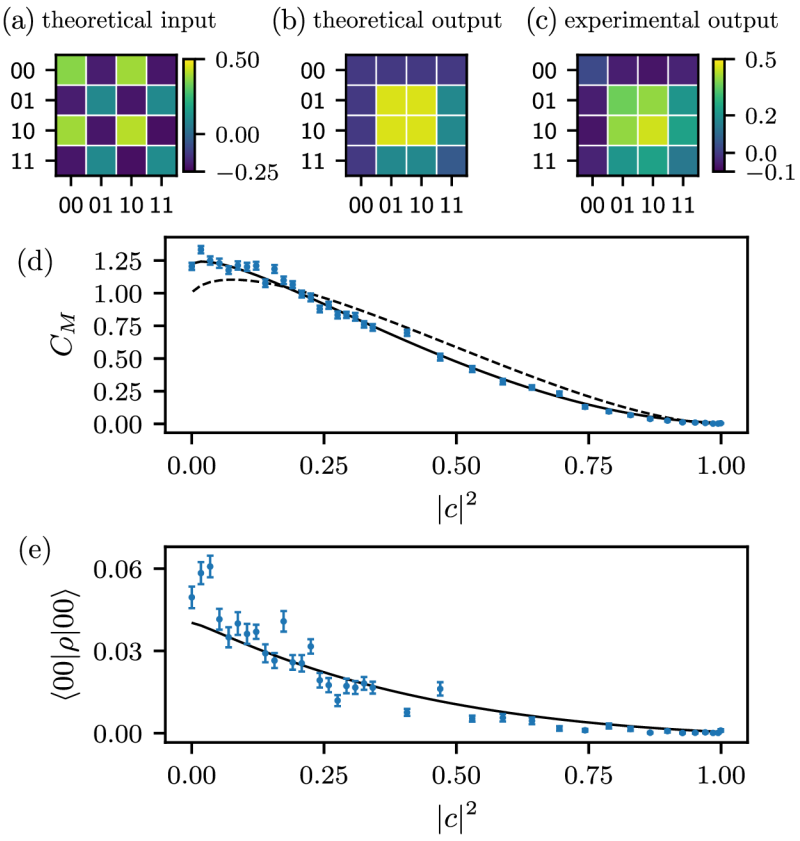


Figure 5.3: Generation of the two-qubit states defined in Eq. (5.4) by unitary operations. As an example we plot the real parts of density matrices of a theoretical asymmetric input product state for $c = 0.277$ (a), the corresponding theoretical output state obtained by application of CZ gate $\hat{U}_{CZ}$ and local unitary operation $\hat{V}_B$ (b), and the actual output experimental state prepared with nominal $c = 0.264$ (c). The imaginary parts of the theoretical density matrices vanish. Also shown is the dependence of the mutual coherence of the output state on $|c|^2$ (d), and the residual population of level $|00\rangle$ in the experimentally prepared states (e). Blue dots represent experimental data, the solid lines indicate predictions of a theoretical model of the setup, and the dashed line shows the ideal theoretical dependence.

ated states slightly differ from the nominal theoretical values, and the presented experimental state is closest to the optimal state $|\psi_3\rangle$ among the whole set of prepared states. In comparison to the filter-based preparation, the purity and fidelity of the state prepared by unitary operations are higher, and the residual population of the state $|00\rangle$ is reduced to 0.035(4), see Table 5.1. The mutual coherence $C_M = 1.18(3)$ slightly exceeds the maximum achievable by superposition of three basis states $|jk\rangle$. The experimental imperfections in this case thus lead to a slight

increase of the mutual coherence. The suppression of the state $|00\rangle$ is generally better than in the filter-based scheme, as illustrated in Fig. 5.3 (d). Our ability to suppress the population of state $|00\rangle$ is mainly limited by imperfect two-photon interference due to the partial distinguishability of the two photons and by the precision of retardance and rotation of wave-plates. To quantify the effect of wave-plate settings, we numerically search for optimal local single-qubit unitary operations that minimize the population of state $|00\rangle$ while keeping C_M above a chosen threshold 1.05. After we apply the optimal single-qubit unitaries to the reconstructed state, the population of $|00\rangle$ drops to $p_{00} = 0.012(2)$, while the mutual coherence of the state remains high, $C_M = 1.05(3)$.

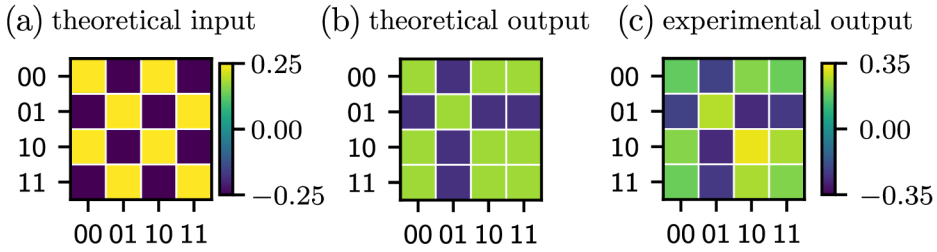


Figure 5.4: Generation of the optimal state $|\psi_4\rangle$ with quantum CZ gate. Shown are the real parts of density matrices of the theoretical input symmetric product state for $p = 0.5$ (a), the theoretical maximally entangled output state $|\psi_4\rangle$ (b), and the experimentally prepared state (c). The imaginary parts of the theoretical density matrices vanish, and the imaginary parts of matrix elements of the experimental state in (c) are smaller than 0.011.

To complete our analysis of preparation of states that maximize the mutual quantum coherence, we have utilized the quantum CZ gate to generate the optimal maximally entangled state $|\psi_4\rangle$ from input product states $|\pm\rangle|\pm\rangle$, where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. Note that for unbalanced input states one could first apply local quantum filters to balance the amplitudes of $|0\rangle$ and $|1\rangle$ and then use the quantum CZ gate. Representative results for input $|+\rangle|-\rangle$ are plotted in Fig 5.4. The purity and fidelity of the generated state read $\mathcal{F} = 0.95(1)$ and $\mathcal{P} = 0.92(2)$ and are for comparison also listed in Table 5.1. The mutual coherence of the state is close to the theoretical maximum, $C_M = 1.70(6)$. The state $|\psi_4\rangle$ simultaneously maximizes also the ordinary global coherence and for the experimentally prepared state we get $C = 1.71(6)$. On the other hand, the local coherences practically vanish, because the state is maximally entangled and each subsystem is locally in a maximally mixed state. The prepared state is not perfectly pure due to the residual distinguishability of the two photons and the amplitudes of the states $|jk\rangle$ are not perfectly balanced due to various experimental imperfections, which explains why the experimental mutual coherence is less than the theoret-

ical maximum $C_M = 2$.

Gate	$\mathcal{P}$	$\mathcal{F}$	$\lvert A\rvert$	$\lvert B_{01}\rvert$	$\lvert B_{10}\rvert$	$\lvert C\rvert$
$\mathbb{1}$	0.985(1)	0.9912(5)	0.950	0.901	1.000	0.957
$\hat{M}_0$	0.963(5)	0.965(3)	0.243	0.949	1.000	0.928
$\hat{U}_{CZ}$	0.927(6)	0.957(3)	0.801	0.951	1.000	0.881

Table 5.2: Purity and fidelity of selected experimental two-qubit quantum operations. The last four columns display the experimentally determined filter parameters that most closely match the experimental data. Since the experimentally implemented operations are not exactly symmetric, we specify separate parameters B_{01} and B_{10} for states $|01\rangle$ and $|10\rangle$.

The observed purities and fidelities of the generated two-qubit states are consistent with the high purities and fidelities of the quantum operations used for their preparation. Note that the input product states for preparation of the optimal states $|\psi_N\rangle$ are superposition states, which are typically more sensitive to gate imperfections than the basis states $|jk\rangle$. We have characterized the experimental two-qubit quantum filters and gates by full quantum process tomography. Each two-qubit quantum operation $\mathscr{E}$ is described by its Choi matrix χ that can be obtained by applying $\mathscr{E}$ to one part of a four-qubit maximally entangled state. This Choi-Jamiolkowski isomorphism between quantum operations and states allows us to conveniently define the purity and fidelity of quantum operation by straightforward extension of definitions for quantum states. In Table 5.2, we summarize experimental results for the filter $\hat{M}_0$ and the unitary gate $\hat{U}_{CZ}$. For reference, we also provide results for the two-qubit identity operation $\mathbb{1}$. The achieved fidelities are fully comparable to the highest fidelities of linear optical two-qubit quantum gates and operations reported in the literature [19, 209–211].

5.3.2 Population suppression

To summarize, we use two different methods for restriction to various subspaces of the Hilbert space in our experiment. The first is the application of a filter by setting specific values of the constants A, B, and C in Eq. (5.5). Specifically, for the 3D subspace of the Hilbert space, which is the most interesting to us, we try not to have any $|00\rangle$ population at all, so we choose $A = 0$. However, with this setting, we failed to completely reduce the $|00\rangle$ population due to partial photon distinguishability, which led to higher mutual coherence than was predicted by theory.

Therefore, we choose another way to reduce the $|00\rangle$ population. We set $A = B = 1$ and $C = -1$, thereby, we get the CZ gate. We then reduce the

population $|00\rangle$ by a local unitary operation on the second output qubit. This method leads to a better reduction of the unwanted population than the first method, but also not to its complete suppression. Since the suppression of the $|00\rangle$ level is a crucial part of the experiment, we describe this second method in more detail.

The input qubits are in a state of generally asymmetric linear polarizations

$$|\psi_{in}\rangle = (\cos(x)|0\rangle + \sin(x)|1\rangle) \otimes (\cos(y)|0\rangle + \sin(y)|1\rangle). \tag{5.8}$$

This state passes through the CZ gate, behind which the second output qubit is rotated using HWP(z). The output state is, therefore, dependent on the parameters x, y, and z and can be written as

$$|\psi_{\text{out}}(x,y,z)\rangle = \begin{pmatrix} \cos(x)\cos(y-z) \\ -\cos(x)\sin(y-z) \\ \cos(y+z)\sin(x) \\ \sin(x)\sin(y+z) \end{pmatrix}. \tag{5.9}$$

We suppress the population $|00\rangle$ by choosing $z = y - \pi/2$ and balance the populations $|01\rangle$ and $|10\rangle$ by choosing $y = -1/2 \arcsin(1/\tan(x))$. The remaining x is our free parameter, which we sample in the interval $(0^\circ - 90^\circ)$. The resulting state should take the form

$$|\psi_{\text{out}}(x)\rangle = \begin{pmatrix} 0 \\ -\cos(x) \\ -\cos(x) \\ -\sqrt{1-\cot^2(x)}\sin(x) \end{pmatrix}. \tag{5.10}$$

With the first sampling iteration, we found the approximate location of mutual coherence C_M maximum, which is around 47°. Therefore, in the next iteration, we chose a step of 1° outside the $45^\circ - 55^\circ$ region, where we proceeded with a finer step of 0.5°. The results are shown in Fig. 5.5 using the blue dots. We compare these results with the theoretical dependence shown by the dashed black line and the dependence determined from the reconstructed process matrix of the CZ gate shown by the solid black line. The prediction from the process matrix and the measured data show a higher mutual coherence C_M than we should get for the states in the 3D subspace of the Hilbert space. The cause is the imperfect suppression of population $|00\rangle$, which we illustrate in Fig. 5.6.

We implement the suppression of the state $|00\rangle$ population by a local unitary operation on the second output qubit. Unfortunately, we only managed to suppress the population of the state $|00\rangle$ to $p_{00} = 0.035$. We came closest to the state with a theoretically optimal population of the state $|11\rangle$ with the values

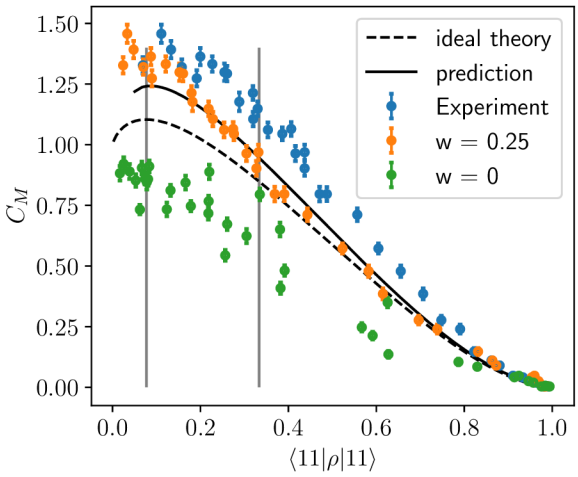


Figure 5.5: Measured mutual coherence C_M of the prepared states depending on the population of the state $|11\rangle$. The dashed line is the ideal theoretical dependence, and the solid line shows the prediction obtained from the measured CZ gate process matrix. The vertical grey lines indicate the theoretical optimal population $p_{11} = |c|^2 = 0.077$ and the population of the balanced superposition where $p_{11} = 1/3$. Error bars show one standard deviation that we obtained by bootstrapping. The blue points are directly measured data. The orange and green points correspond to states to which we applied local unitary operations to suppress the population of the state $|00\rangle$, w is a parameter defining applied local unitary transformations and is discussed below in the text.

$p_{11}^{\text{opt}} = 0.080$, which has a mutual coherence $C_M^{\text{opt}} = 1.33(4)$. The state that most closely corresponds to a balanced superposition has a population $p_{11}^{bal} = 0.330$ and a mutual coherence $C_M^{bal} = 1.15(4)$. The near-optimal state exceeded the mutual coherence of the balanced state by four standard deviations.

To better understand how the mutual coherence depends on the population of levels, we applied local unitary transformations to the reconstructed density matrices to minimize the state population $|00\rangle$ and simultaneously estimate the populations of the states $|01\rangle$ and $|10\rangle$. We formulated the optimal transformations as minimizing $p_{00}^2 + w(p_{01} - p_{10})^2$ and the weight w was set empirically to 0.25. This weight is the compromise between minimizing $|00\rangle$ and balancing $|01\rangle, |10\rangle$. We apply the local unitary transformation found by choosing the w parameter to the density matrix. The mutual coherence of such states is shown in Fig. 5.5 by orange dots, and the resulting populations after adjustment are in Fig. 5.7 (a), (b), (c). This adjustment brought the measured mutual coherence closer to the theoretical prediction obtained from the process matrix of the CZ gate.

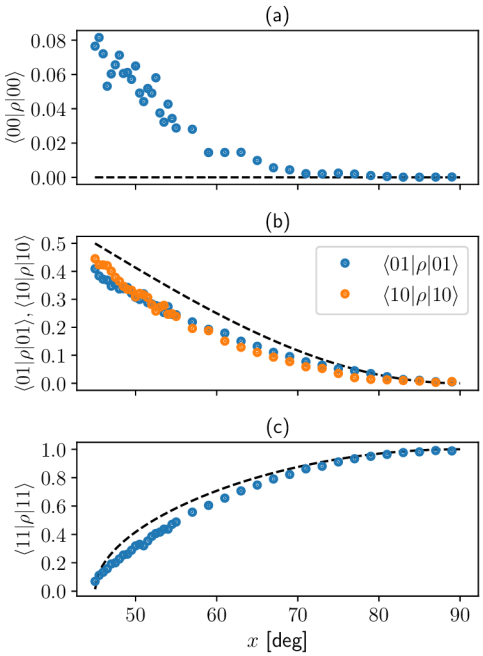
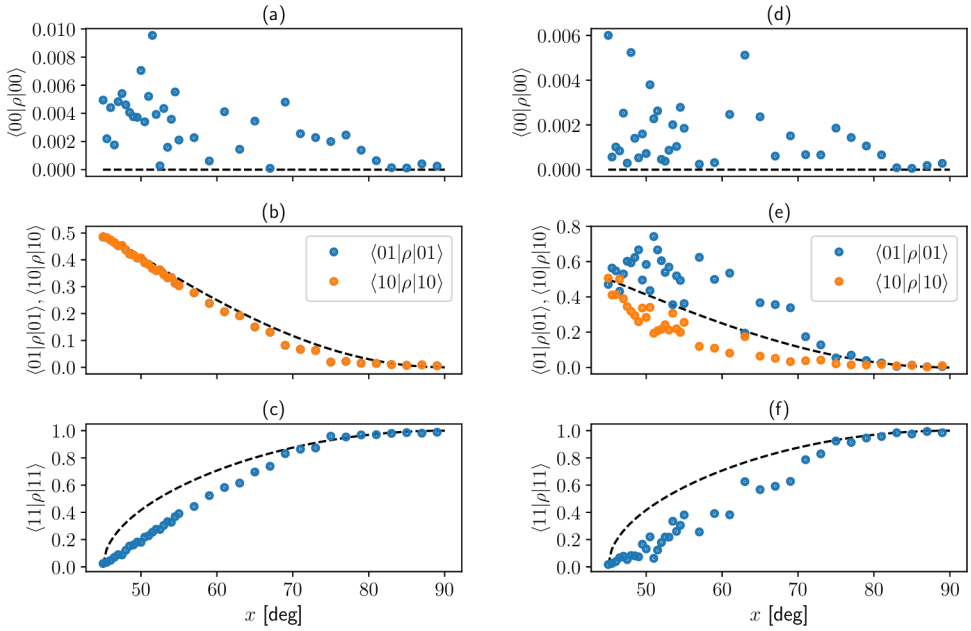


Figure 5.6: The measured population of the prepared state depending on the selected parameter x. The population $|00\rangle$ is plotted in panel (a), the populations $|01\rangle$ and $|10\rangle$, which should theoretically coincide, are plotted for comparison in one panel (b), and the population $|11\rangle$ is plotted in pannel (c).

To obtain the 3D subspace, we have to completely suppress the state population $|00\rangle$. For this, we choose the weight $w = 0$ and repeat the analysis. Populations of individual levels are plottedin Fig. 5.7 (d), (e), (f). The mutual coherence C_M of such states is shown in Fig. 5.5 using green dots and its resulting value together with the suppressed population of the state $|00\rangle$ are in Table 5.1. The mutual coherence is not that large as the corresponding ideal theoretical value, most likely due to the imbalance populations of the $|01\rangle$ and $|10\rangle$ states . Due to the partial mixing of this measured states, the $|00\rangle$ state population plotted in Fig. 5.7 (d), cannot be completely suppressed.

5.4 Discussion

In this Chapter, we have studied the mutual coherence in various subspaces of the Hilbert space of a pair of qubits. First, we have theoretically investigated and characterized states maximizing mutual coherence in the subspaces of dimension $\{2, 3, 4\}$. Our results reveal a non-trivial structure of the optimal states in dimen-



(a) $w = 0.25$. **(b)** $w = 0$.

Figure 5.7: The population of the prepared state, after the application of local unitary transformations with the parameters $w = 0.25$ (a), (b), (c), and $w = 0$ (d), (e), (f). If $w = 0.25$, we have balanced populations of $|01\rangle$ and $|10\rangle$ levels. This behaviour is plotted in panel (b). On the other hand, if w=0, it is no longer the case, which is shown in panel (e). However, by comparing panels (a) and (d), we can see that population suppression of $|00\rangle$ is more successful for the case when $w = 0$.

sion 3, whereas in even-dimensional subspaces, the states show high symmetry. Subsequently, we have generated the optimal states in a linear-optical proof-of-principle experiment. We have realized strictly incoherent two-qubit quantum filters capable of transforming an initial product state of two qubits with a certain amount of local coherence into a state maximizing the mutual coherence. Furthermore, we have also prepared the optimal states via a sequence of unitary operations that involves single-qubit transformation outside the class of strictly incoherent operations. Our experimental results confirm the complex behaviour of mutual coherence in the three-dimensional subspace and show that mutual coherence as a nonlinear quantity is highly sensitive to imperfections.

Chapter 6

Non-interactive XOR quantum oblivious transfer

Presented outcomes result from the cooperation with researchers from Heriot-Watt University in Edinburgh, Great Britain. They devised the protocol mentioned below, including all the necessary calculations. Our group performed an optical experiment confirming their conclusions. The Chapter is based on our joint article [A4].

XOR oblivious transfer (XOT) is a variant where the sender, Alice, has two bits, and a receiver, Bob, obtains either the first bit, the second bit, or their XOR. Bob should not learn anything more, and Alice should not know what Bob has learned. As we mentioned in Section 2.4.2, a perfect quantum OT with information-theoretic security is known to be impossible.

Although we do not consider any other constraints in this protocol, such as limited quantum storage or relativity (see Section 2.4.2), the probabilities of cheating are still limited by the laws of quantum mechanics. The general lower bound of cheating probabilities for sender and receiver in 1-2 OT is 2/3 [181, 212]. When using symmetric states as bit values of the sender, the bound is raised to ≈ 0.749. This shows that protocols using pure symmetric states are not optimal. However, except for 1-2 OT protocols using pure symmetric states, there are no known quantum protocols for quantum oblivious transfer where the lower bounds have been proven to be tight.

We present a protocol that can therefore be said to be optimal among non-interactive protocols using purely symmetric states because it achieves the smallest possible cheating probability for Bob and for Alice considering Bob's cheating probability. Our non-interactive XOT protocol has the same cheating probabilities as the protocol given by Kundu *et al.* [172]. The cheating probabilities are 3/4 for Bob and 1/2 for Alice. That protocol, however, uses entanglement and is

interactive in a way that quantum states are sent back and forth between sender and receiver. Our protocol is easier to implement since it is non-interactive and does not require entanglement. In addition, our protocol can work even if Bob becomes the sender of the quantum state and Alice the receiver who measures it while still implementing an oblivious transfer from Alice to Bob. It is called a reverse protocol. Even though in other OT protocols, the cheating probability for the reverse version may be different than for the non-reversed version, the cheating probabilities for both parties remain the same in both variants of our protocol. However, the reverse version of the protocol is easier to implement.

Determining the cheating probabilities of our XOT quantum protocol, further calculations, comparison with the classical version of XOT, and comparison with the version of the protocol that uses entanglement are described in detail in our article [A4]. In this work, we mainly focus on the experimental implementation of this protocol.

6.1 Quantum XOT with symmetric states

We consider quantum XOT protocols which satisfy certain properties:

1. They are non-interactive protocols, where Alice sends Bob a quantum state $|\psi_{x_0x_1}\rangle$, encoding her bit values x_0, x_1, and Bob measures it.

2. Alice's states $|\psi_{x_0x_1}\rangle$ are pure and symmetric. That is, $|\psi_{01}\rangle = U|\psi_{00}\rangle, |\psi_{11}\rangle = U|\psi_{01}\rangle, |\psi_{10}\rangle = U|\psi_{11}\rangle$, for some unitary U with $U^4 = \hat{1}$.

3. Each of Alice's bit combinations is chosen with probability $1/4$.

4. When measuring each state $|\psi_{x_0x_1}\rangle$, Bob obtains either x_0, x_1, or $x_2 = x_0 \oplus x_1$ with probability $1/3$.

The states $|\psi_{x_0x_1}\rangle$ need to be chosen so that it is possible for Bob to obtain either x_0, x_1 or $x_2 = x_0 \oplus x_1$ correctly. We denote an honest Bob's measurement operators by $\hat{\Pi}_{0*}, \hat{\Pi}_{1*}, \hat{\Pi}_{*0}, \hat{\Pi}_{*1}, \hat{\Pi}_{\mathrm{XOR}=0}, \hat{\Pi}_{\mathrm{XOR}=1}$, corresponding to Bob obtaining $x_0 = 0, x_0 = 1, x_1 = 0, x_1 = 1, x_2 = 0$ and $x_2 = 1$ respectively. Bob should obtain either the first or the second bit, or their XOR, each with probability $1/3$. The probability of obtaining outcome m is

$$p_m = \langle\psi_{jk}|\hat{\Pi}_m|\psi_{jk}\rangle, \tag{6.1}$$

for $m \in \{0*, 1*, *0, *1, \mathrm{XOR} = 0, \mathrm{XOR} = 1\}$. This probability should be equal to $1/3$ when an outcome is possible and otherwise be equal to 0.

Usually, in OT, it is assumed that the sender and receiver are choosing their inputs at random. Here, Bob will obtain either x_0, x_1, or $x_0 \oplus x_1$ at random. Using the terminology in [212], we have a semi-random XOR oblivious transfer (XOT) protocol, defined in general as follows.

Definition 1 (Semi-random XOR oblivious transfer) *Semi-random XOT is a two-party protocol where*

1. *Alice chooses her input bits* $(x_0, x_1) \in \{0, 1\}$ *uniformly at random, thereby specifying also their XOR* $x_2 = x_0 \oplus x_1$*, or she chooses* Abort.

2. *Bob outputs the value* $b \in \{0, 1, 2\}$ *and a bit* y*, or* Abort.

3. *If both parties are honest, then they never abort,* $y = x_b$*, Alice has no information about* b*, and Bob has no information about* $x_{(b+1) \bmod 3}$ *or about* $x_{(b+2) \bmod 3}$.

6.1.1 Bob cheating

We can observe a connection between the cheating probabilities of Alice and Bob. Bob's cheating probability increases if the quantum states are more distinguishable. On the contrary, the cheating probability for Alice decreases. When Bob is cheating, he tries to guess both, x_0 and x_1, bits. He gets one bit from Alice but shouldn't have access to the other, so he can guess. With the knowledge of both bits, he also knows the XOR value. Bob can always cheat in this way with a probability of at least 1/2. The cheating strategy, which maximises Bob's probability of correctly learning both x_0 and x_1 is a minimum-error measurement. His optimal measurement is a square-root measurement [213, 214] since he wants to distinguish between equiprobable, pure and symmetric states.

6.1.2 Alice cheating

A cheating Alice aims to guess whether Bob has obtained x_0, x_1, or $x_2 = x_0 \oplus x_1$. Even if following the protocol, Alice can always cheat at least with probability 1/3 with a random guess. To detect Alice cheating, Bob can test the states he received. If he doesn't, dishonest Alice can send him any state. To prevent Alice's possible cheating, Bob can ask Alice to declare some fraction of the states she sent him. He then checks if his measurement results agree with what Alice declares. Generally, Alice's cheating probability when Bob does not test is at least as high as when he does.

6.2 A non-interactive qutrit XOT protocol

We present a protocol that can thus be said to be optimal among non-interactive protocols using pure symmetric states, since it achieves the smallest possible cheating probability 3/4 for Bob, and the smallest possible cheating probability 1/2 for Alice.

In our protocol, Alice encodes two bit values x_0, x_1 in one of the four non-orthogonal states

$$|\phi_{x_0 x_1}\rangle = \frac{1}{\sqrt{3}}(|0\rangle + (-1)^{x_1}|1\rangle + (-1)^{x_0}|2\rangle). \tag{6.2}$$

These states are symmetric, in the sense that $|\phi_{01}\rangle = \hat{U}|\phi_{00}\rangle$, $|\phi_{11}\rangle = \hat{U}^2|\phi_{00}\rangle$, and $|\phi_{10}\rangle = \hat{U}^3|\phi_{00}\rangle$ for

$$\hat{U} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}, \tag{6.3}$$

for which it holds that $\hat{U}^4 = \mathbb{1}$. The states $|\phi_{x_0 x_1}\rangle$ are selected so that it is possible to unambiguously exclude two of them, meaning that it is possible to learn either x_0, x_1, or $x_0 \oplus x_1$. Because the states are non-orthogonal, it is not possible to unambiguously determine which single state was received. In other words, it is impossible for Bob to perfectly learn both bits x_0, x_1.

After choosing her bits $(x_0, x_1) \in \{0, 1\}$ uniformly at random, Alice sends the respective state to Bob, who makes an unambiguous quantum state elimination measurement to exclude two of the four possible states. There are six different pairs of states he can exclude. Each excluded pair corresponds to learning either x_0, x_1, or $x_0 \oplus x_1$, with either the value 0 or 1. To construct Bob's measurement operators, we need six states, each one orthogonal to a pair of states in Eq. (6.2). The measurement operators are then proportional to projectors onto these six states, normalised so that their sum is equal to the identity matrix. For instance, the measurement operator $\hat{\Pi}_A = (1/4)(|0\rangle + |2\rangle)(\langle 0| + \langle 2|)$ will exclude the states $|\phi_{11}\rangle$ and $|\phi_{10}\rangle$, so Bob's outcome bit will be $x_0 = 0$; similarly for the other operators. Table 6.1 gives the excluded pairs, the corresponding measurement operators, and the deduced output bits for Bob.

Outcome bit	Eliminated states	Measurement operator
$x_0 = 0$	$\|\phi_{11}\rangle$ and $\|\phi_{10}\rangle$	$\hat{\Pi}_A = \frac{1}{4}(\|0\rangle + \|2\rangle)(\langle 0\| + \langle 2\|)$
$x_0 = 1$	$\|\phi_{00}\rangle$ and $\|\phi_{01}\rangle$	$\hat{\Pi}_B = \frac{1}{4}(\|0\rangle - \|2\rangle)(\langle 0\| - \langle 2\|)$
$x_1 = 0$	$\|\phi_{11}\rangle$ and $\|\phi_{01}\rangle$	$\hat{\Pi}_C = \frac{1}{4}(\|0\rangle + \|1\rangle)(\langle 0\| + \langle 1\|)$
$x_1 = 1$	$\|\phi_{00}\rangle$ and $\|\phi_{10}\rangle$	$\hat{\Pi}_D = \frac{1}{4}(\|0\rangle - \|1\rangle)(\langle 0\| - \langle 1\|)$
$x_2 = 0$	$\|\phi_{01}\rangle$ and $\|\phi_{10}\rangle$	$\hat{\Pi}_E = \frac{1}{4}(\|1\rangle + \|2\rangle)(\langle 1\| + \langle 2\|)$
$x_2 = 1$	$\|\phi_{00}\rangle$ and $\|\phi_{11}\rangle$	$\hat{\Pi}_F = \frac{1}{4}(\|1\rangle - \|2\rangle)(\langle 1\| - \langle 2\|)$

Table 6.1: Bob's measurement operators and outcomes.

To summarise, our XOT protocol proceeds as follows:

1. The sender Alice uniformly at random chooses the bits $(x_0, x_1) \in \{0, 1\}$ and sends the corresponding state $|\phi_{x_0 x_1}\rangle$ to the receiver Bob.

2. Bob performs an unambiguous state elimination measurement, excluding two of the possible states with certainty, from which he can deduce either x_0, x_1, or $x_2 = x_0 \oplus x_1$.

A dishonest Bob can cheat with probability $B_{OT} = 3/4$ by applying the square-root measurement [213, 214]. Alice's cheating probability is $A_{OT} = 1/2$, whether or not Bob tests the states she sends.

6.3 Reversed version of the XOT protocol

We will consider non-interactive XOT from Alice to Bob implemented in such a way that Bob sends Alice one of six states depending on his randomly chosen x_0, x_1, or $x_2 = x_0 \oplus x_1$ and its value. Alice learns x_0 and x_1 by performing a measurement on Bob's state. For the reversed non-interactive XOT protocol, Bob's measurement operators given in Table 6.1 become his states, when normalized

to 1, and Alice's states given in (6.2) become her measurement operators, when renormalised so that they sum to the identity operator. The XOT protocol is then performed as follows:

1. Bob randomly chooses one of the six states

$$\begin{aligned}
|\phi_{x_0=0}\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |2\rangle), \quad |\phi_{x_0=1}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |2\rangle), \\
|\phi_{x_1=0}\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |\phi_{x_1=1}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \\
|\phi_{x_2=0}\rangle &= \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle), \quad |\phi_{x_2=1}\rangle = \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle)
\end{aligned} \tag{6.4}$$

   and sends it to Alice. This choice determines the values of b and bit x_b, i.e., Bob's input and output in "standard" non-random XOT.

2. Alice performs a measurement on the state she has received from Bob, learning the bit values (x_0, x_1). Her measurement operators $\hat{\Pi}_{x_0x_1}$ are

$$\begin{aligned}
\hat{\Pi}_{00} &= \frac{1}{4}(|0\rangle + |1\rangle + |2\rangle)(\langle 0| + \langle 1| + \langle 2|), \\
\hat{\Pi}_{01} &= \frac{1}{4}|0\rangle - |1\rangle + |2\rangle)(\langle 0| - \langle 1| + \langle 2|), \\
\hat{\Pi}_{11} &= \frac{1}{4}(|0\rangle - |1\rangle - |2\rangle)(\langle 0| - \langle 1| - \langle 2|), \\
\hat{\Pi}_{10} &= \frac{1}{4}(|0\rangle + |1\rangle - |2\rangle)(\langle 0| + \langle 1| - \langle 2|).
\end{aligned} \tag{6.5}$$

In terms of x_0 and x_1, Alice's measurement operators can be written $\hat{\Pi}_{x_0x_1} = |\Phi_{x_0x_1}\rangle\langle\Phi_{x_0x_1}|$, where $|\Phi_{x_0x_1}\rangle = (1/2)(|0\rangle + (-1)^{x_1}|1\rangle + (-1)^{x_0}|2\rangle)$. As in the unreversed XOT protocol, when both parties act honestly, Alice will have two bits, but will not know whether Bob knows her first bit, her second bit, or their XOR. Bob will have one of x_0, x_1, or $x_2 = x_0 \oplus x_1$, but will not know anything else, since he can only deduce one bit of information with certainty, based on the state he has sent (if he is honest).

6.3.1 Alice cheating

Alice still wants to learn which output Bob has obtained as in the non-reversed version. She cheats by distinguishing between the three mixed states obtained by pairing up the states in (6.4) that correspond to the same output with minimum error, and she can do so with a probability of $A^r_{OT} = 1/2$.

6.3.2 Bob cheating

Bob wants to know exactly which of the four two-bit combinations Alice got. As in the non-reversible protocol, there are two scenarios for the cheating sender of the state, now Bob: The first is when the receiver of the state, now Alice, tests the state, and the second is when she does not. Here again, Bob's probability of cheating is the same for both scenarios and is $B^r_{OT} = 3/4$.

When Alice is not testing, Bob can achieve this probability if he sends an eigenvector corresponding to the largest eigenvalue of one of Alice's measurement operators corresponding to the same output bit. However, if Alice is testing, then to achieve this cheating probability, Bob needs to send a superposition of the states he is supposed to send. In addition, this superposition must be entangled with some system, he keeps.

6.4 Experimental implementation

In our experiment, the quantum states are encoded into spatial and polarization degrees of freedom of a single photon. We generate photon pairs in a type II SPDC with a periodically poled KTP crystal, and their wavelength is 810 nm. In the resulting pair of photons, one is horizontally and the other vertically polarized. Photons with vertical polarization serve as heralding photons and pass through the fiber directly to the detector. Horizontally polarized photons are guided through the fiber into the experiment. The experimental setup is shown in Fig. 6.1.

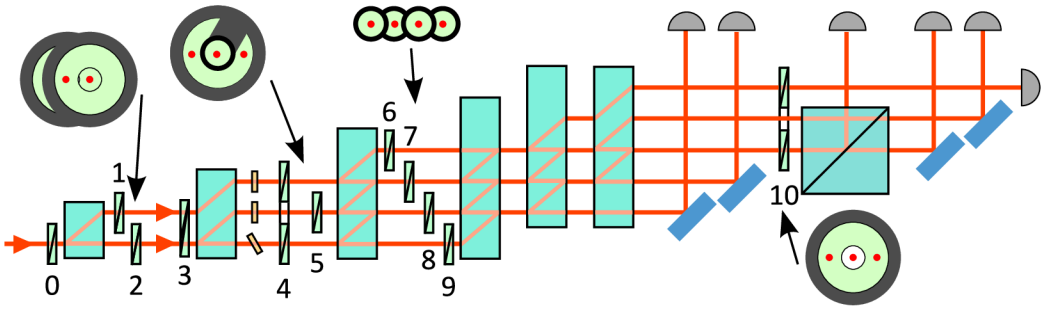


Figure 6.1: Detailed scheme of the experimental setup. Green boxes labelled with black numbers represent half-wave plates (HWP). Small orange rectangles are glass plates which serve for phase compensation. Large semi-transparent cyan boxes represent beam displacers. Next to HWP10, there is a polarizing beam splitter. Note that HWP1, HWP2, HWP4, and HWP10 are ring-shaped and polarization of the central beam is not affected. Insets show the actual arrangement of the half-wave plates.

It contains eleven half-wave plates (HWPs) drawn as green rectangles numbered from 0 to 10. Individual photons pass through the first HWP and then enter the calcite displacer, which is indicated by the cyan rectangle. Here, if the photons are diagonally polarized, they are divided into two possible paths, i.e., the first with horizontal and the second with vertical polarization, 6 mm apart. Vertically polarized photons pass through the calcite directly. However, horizontally polarized photons have a different refractive index inside the calcite and are, therefore, displaced due to the calcite birefringence.

We use these optical components because the protocol requires an interfeqrometric network that allows the coupling of these modes with each other and with the vacuum. Calcite beam displacers serve to construct passively stable interferometers [80] while also allowing us to use spatial and polarization degrees of freedom to encode qutrits. Since we need multiple light propagation paths to implement our protocol, we use HWPs that can address photons in all these propagation paths simultaneously, some paths, or only one path. Therefore, we used standard wave plates (numbers 0 and 3), plates with a hole in the middle (numbers 1, 2, 4, and 10, ring-shaped) and a small plate that is attached only in the centre of its structure (number 5). In addition, we used a custom design for four side-by-side waveplates (numbers 6, 7, 8, 9) in our experiment.

The first HWP addresses all photons. Therefore, we found the most accurate one to minimize errors and losses in later parts of the experiment. First, we adjusted our experiment with a strong signal from a laser diode at 810 nm, and then we used a single-photon source described in [1].

Even though there are multiple optical paths, only four interferometric phases are relevant for the tested protocols. Each of these interferometers shown in Fig. 6.2 consists of two beam displacers. Fig. 6.2 also shows the angles of the HWPs to set the correct interferometric phases. For three of the four interferometers, we placed the beam displacer on the mount with the piezoelectric device. We adjust the first relative optical phase by tilting the second beam displacer using a piezoelectric actuator attached to a prism turn table. We then set the phase of the second interferometer by tilting the third beam displacer. The third interferometric phase is changed by tilting the glass plate, which we place in the bottom arm of the interferometer. Finally, we set the last optical phase by tilting the fourth beam displacer. We have to adjust all these phases in this order because of the optical paths they share.

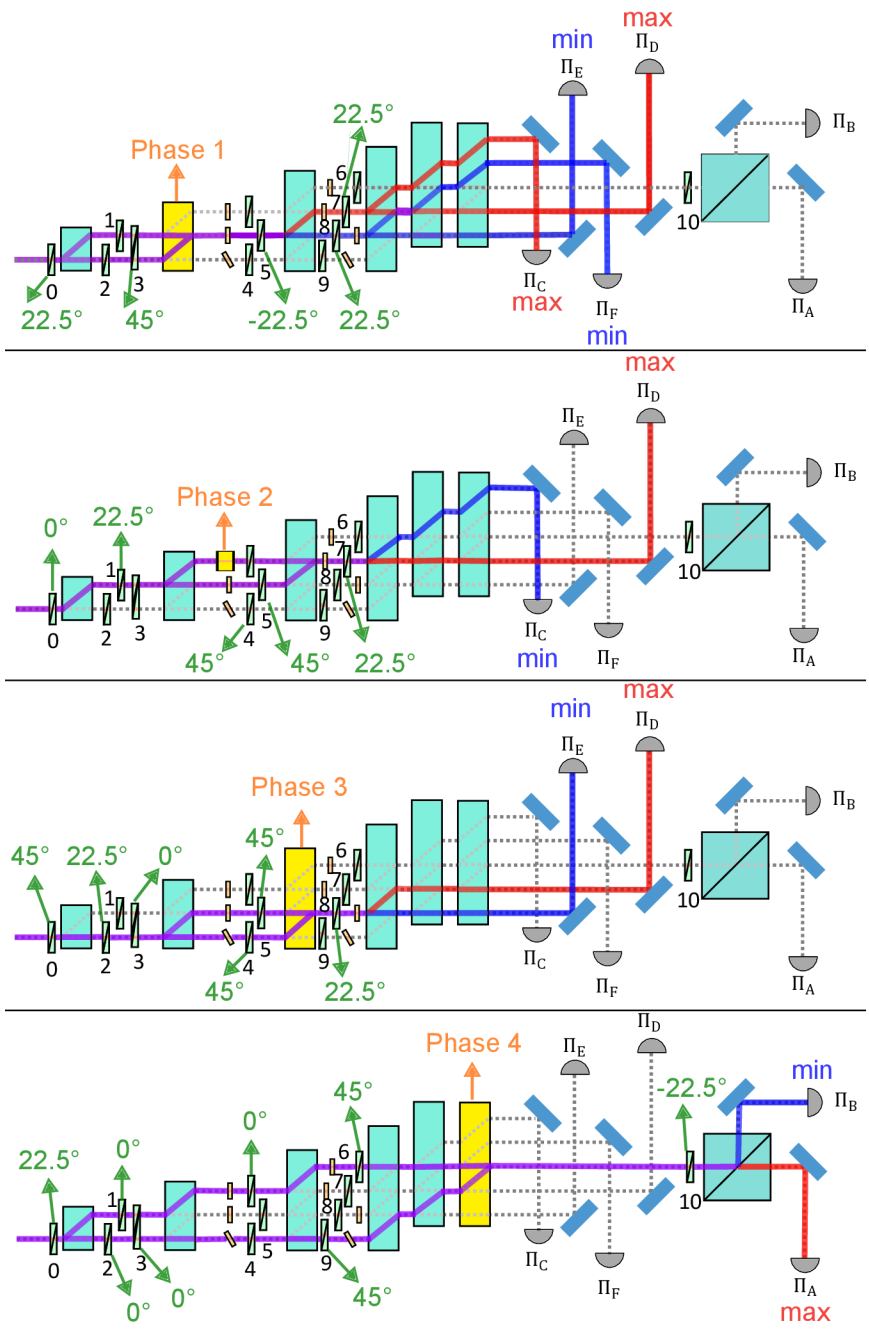


Figure 6.2: Settings of the four relevant phases in the experiment. Calcite beam displacers serve to construct passively stable interferometers while allowing the use of spatial and polarization degrees of freedom to encode qutrits. Calcites that are on mounts with piezoelectric devices are marked in yellow. The red (blue) line corresponds to constructive (destructive) interference.

Single-photon detection is implemented as coincident measurements with a trigger signal heralding photon creation (vertically polarized photons from created photon pairs). The coincidence window used is 2.5 ns. If multiple detectors registered a signal with the trigger signal, only one result is randomly selected and counted. However, such situations occurrs at most once in 2000 measurements.

Using strong laser light, we characterize the phase stability of the largest interferometer formed by the outermost optical paths between the first and the fourth beam displacer, which merge at the sixth displacer. We set the optical phase to roughly $\pi/2$, cover the setup with a cardboard box, and monitor the output intensity for one hour. The observed drift rate is 0.5°/min. The amplitude of the fast phase fluctuations is roughly 5° peak-to-peak.

There are several sources of experimental errors. The most significant of them is the unequal coupling efficiency of the fibers at the output of the interferometric network spanning from 0.75 to 0.85. Furthermore, there are also unequal efficiencies of the used single-photon detectors. The largest relative difference is 0.12. We compensate for these inequalities using detection electronics. The inaccurate retardance of half-wave plates causes a mismatch between the expected and actual coupling ratio for a given angular position. We try to compensate for this imperfection by slightly adjusting the angular positions. We also use wave plates to exchange polarization modes. Imperfect retardance limits the ability to convert horizontal polarization to vertical. In our experiments, it subsequently causes undesired losses and residual coupling.

In addition, a slight difference in the length of the beam displacers causes an imperfect overlap of the optical beams, which reduces the interferometric visibility. The worst observed visibility was 0.85. At the output of our experiment, however, we coupled the light into single-mode optical fibers. They serve as spatial filters and restore interferometric visibility. The worst observed visibility using fibers is 0.99. We also observe that the different optical paths suffered from slightly unequal optical losses (the most significant difference is 0.02), but we did not directly compensate for this imperfection.

Coincidence counts C_{ij} are accumulated during 10 s long measurements for each input state. The relative frequencies are calculated as $f_{ij} = \frac{C_{ij}}{\sum_j C_{ij}}$, where i indexes the input states and j indexes the measurement results. The relative frequency errors shown are determined using the standard error propagation law, assuming that the detection events follow a Poisson distribution, and thus the standard deviations C_{ij} can be estimated as $\sqrt{C_{ij}}$.

6.4.1 Both parties honest

In the case of both honest parties, Alice prepares one of the qutrit states given in (6.2) and sends it to Bob. The basis state $|0\rangle$ is represented by the horizontally polarized mode in the upper output, $|1\rangle$ by the horizontally polarized mode in the lower output, and $|2\rangle$ by the vertically polarized mode in the lower output of the beam displacer. The settings of the angles of wave-plate axes corresponding to all of Alice's states are listed in Table 6.2.

	$\|\phi_{00}\rangle$	$\|\phi_{01}\rangle$	$\|\phi_{10}\rangle$	$\|\phi_{11}\rangle$
HWP0	$-27.37°$	$-27.37°$	$27.37°$	$27.37°$
HWP2	$-25.50°$	$25.50°$	$25.50°$	$-25.50°$

Table 6.2: Wave-plate angles for Alice's state preparation if Alice is honest. The angle of HWP1 is always zero (it only compensates for path differences). These settings also hold for cheating Bob in the reversed protocol.

Bob's six measurement operators are defined in Table 6.1, for unambiguously eliminating pairs of states. This measurement can be implemented by a projective von Neumann measurement $\{|\xi_i\rangle\langle\xi_i|\}_{i=A}^{F}$ in an extended six-dimensional Hilbert space where

$$
\begin{aligned}
|\xi_A\rangle &= \frac{1}{2}\left(|0\rangle + |2\rangle + |3\rangle - |5\rangle\right), \\
|\xi_B\rangle &= \frac{1}{2}\left(|0\rangle - |2\rangle + |3\rangle + |5\rangle\right), \\
|\xi_C\rangle &= \frac{1}{2}\left(|0\rangle + |1\rangle - |3\rangle + |4\rangle\right), \\
|\xi_D\rangle &= \frac{1}{2}\left(|0\rangle - |1\rangle - |3\rangle - |4\rangle\right), \\
|\xi_E\rangle &= \frac{1}{2}\left(|1\rangle + |2\rangle - |4\rangle + |5\rangle\right), \\
|\xi_F\rangle &= \frac{1}{2}\left(|1\rangle - |2\rangle - |4\rangle - |5\rangle\right),
\end{aligned}
\tag{6.6}
$$

are orthogonal states with $|3\rangle, |4\rangle, |5\rangle$ being the basis states in the additional dimensions represented by modes added on Bob's side.

A unitary transformation between states $\{|\xi_i\rangle\}_{i=A}^{F}$ and the computational basis $\{|j\rangle\}_{j=0}^{5}$ can be realized by a symmetric beam-splitter network (consisting of six 50:50 beam splitters), which can be further translated into a setup consisting of half-wave plates and a beam displacer which combines spatial and polarization modes of light. The first beam displacer on Bob's side in Fig. 6.3 just transfers the incoming polarization and spatial modes into three separate paths.

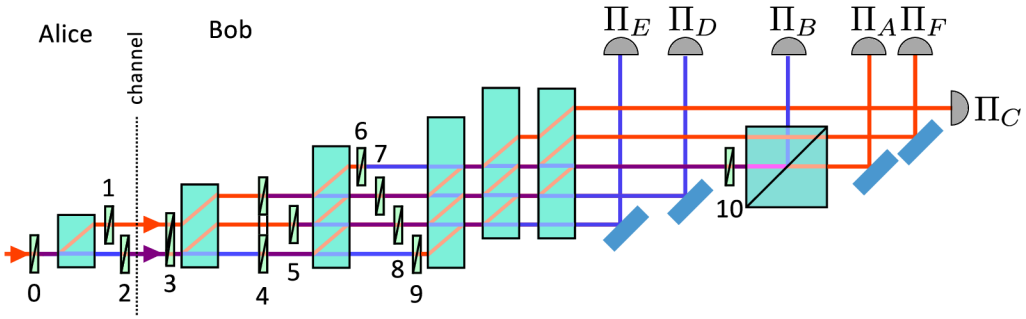


Figure 6.3: Experimental setup for the XOT protocol when both parties are honest. Green boxes labeled with black numbers represent half-wave plates (HWP). Large semi-transparent cyan boxes represent beam displacers. Next to HWP10, there is a polarizing beam-splitter. Note that HWP4 is ring-shaped and polarization of the central beam is not affected. Detectors are labeled according to the corresponding POVM operators. Settings for Alice's half-wave plates are listed in Tab. 6.2 for when she is honest and in Tab. 6.4 for when she is cheating. Settings for Bob's half-wave plates are HWP3= 0°, HWP4=HWP5=HWP7=HWP8=HWP10= 22.5°, HWP6=HWP9= 45°. Beams marked in red have horizontal linear polarization, beams marked in blue have vertical polarization. Purple indicates general polarization states.

The following half-wave plates – "double" HWP4 and HWP5 – turned by 22.5° play the role of "beam splitters", mixing the original three modes with the additional three "empty" (vacuum) modes. Each waveplate mixes two polarization modes. Behind the next beam displacer, there are two half-wave plates turned by 45°, which swap horizontal and vertical linear polarizations, and two half-wave plates turned by 22.5°, which represent the other two "beam splitters". The last "beam splitter" is implemented by a half-wave plate turned by 22.5° followed by a polarizing beam splitter in the right part of the figure.

To prevent the injection of higher-dimensional states into Bob's apparatus (so that Alice only has access to the subspace spanned by her legitimate states), there should be a linear polarizer placed in the upper input port. However, in our proof-of-principle experiment, we have omitted it to simplify the setup.

In Table 6.3, we show the experimental data for the unreversed XOT protocol when both parties are honest. Alice sent states $|\phi_{00}\rangle$, $|\phi_{01}\rangle$, $|\phi_{11}\rangle$, $|\phi_{10}\rangle$ and Bob made an unambiguous quantum state elimination measurement. In Table 6.3, there are the absolute numbers of detector counts, corresponding relative frequencies, and theoretical probabilities for comparison. Digits in parentheses represent one standard deviation at the final decimal place. The states in (6.2) were being prepared with equal probabilities. The average error rate caused by experimental imperfections was 0.01249(8). It was calculated as $\frac{\sum_{i,j\in\mathscr{E}_i} C_{ij}}{\sum_{i,j} C_{ij}}$, where i

indexes input states, j indexes measurement results, C_{ij} are measured numbers of counts, and $\mathscr{E}_i$ denote the sets of erroneous outcomes (outcomes that should not occur).

		Bob					
		$\hat{\Pi}_A$	$\hat{\Pi}_B$	$\hat{\Pi}_C$	$\hat{\Pi}_D$	$\hat{\Pi}_E$	$\hat{\Pi}_F$
Alice		$x_0 = 0$	$x_0 = 1$	$x_1 = 0$	$x_1 = 1$	$x_2 = 0$	$x_2 = 1$
$\|\phi_{00}\rangle$	C	**166443**	5562	**167526**	719	**167691**	1389
	f	0.3268(7)	0.0109(1)	0.3289(7)	0.00141(5)	0.3292(7)	0.00273(7)
	p_t	1/3	0	1/3	0	1/3	0
$\|\phi_{01}\rangle$	C	**167799**	4375	272	**167383**	1001	**166933**
	f	0.3305(7)	0.0086(1)	0.00054(3)	0.3296(7)	0.00197(6)	0.3288(7)
	p_t	1/3	0	0	1/3	0	1/3
$\|\phi_{10}\rangle$	C	4540	**167803**	**167806**	446	1189	**168087**
	f	0.0089(1)	0.3291(7)	0.3291(7)	0.00087(4)	0.00233(7)	0.3297(7)
	p_t	0	1/3	1/3	0	0	1/3
$\|\phi_{11}\rangle$	C	3791	**166615**	317	**166221**	**167797**	1789
	f	0.0075(1)	0.3289(7)	0.00063(4)	0.3282(7)	0.3313(7)	0.00353(8)
	p_t	0	1/3	0	1/3	1/3	0

Table 6.3: Measured counts C, relative frequencies f, and corresponding theoretical probabilities p_t for the situation when both the parties were honest. $x_2 = x_0 \oplus x_1$.

6.4.2 Alice cheating

Bob is honest, so his measurement is the same as in the previous case. To guess which of the three bits Bob will obtain, Alice sends states $|0\rangle, |1\rangle$, or $|2\rangle$. The corresponding angles of the wave-plates are listed in Table 6.4.

	$\|0\rangle$	$\|1\rangle$	$\|2\rangle$
HWP0	0°	45°	45°
HWP2	0°	45°	0°

Table 6.4: Angles for wave plates, for Alice's state preparation if Alice is cheating. The angle of HWP1 is always zero.

Alice's states were being prepared with equal probabilities. Her average probability of correctly guessing which one of the three bits Bob obtained (i.e., his value of b), estimated from the experiment, was 0.4999(3). It was calculated as

$\frac{\sum_{i,j\in\mathscr{C}_i} C_{ij}}{\sum_{i,j} C_{ij}}$, where $\mathscr{C}_i$ denote the sets of correct guesses. The theoretical prediction is $1/2$.

In Table 6.5, we show the experimental data for the case of a dishonest Alice in the unreversed XOT protocol. Alice sent states $|0\rangle$, $|1\rangle$, $|2\rangle$, while Bob honestly made an unambiguous quantum state elimination measurement.

		Bob					
Alice		$\hat{\Pi}_A$ $x_0 = 0$	$\hat{\Pi}_B$ $x_0 = 1$	$\hat{\Pi}_C$ $x_1 = 0$	$\hat{\Pi}_D$ $x_1 = 1$	$\hat{\Pi}_E$ $x_2 = 0$	$\hat{\Pi}_F$ $x_2 = 1$
	C	**126264**	**135006**	**124653**	**121434**	29	30
$\|0\rangle$	f	0.2488(6)	0.2661(6)	0.2457(6)	0.2393(6)	0.00006(1)	0.00006(1)
x_0, x_1	p_t	1/4	1/4	1/4	1/4	0	0
	C	10	189	**127189**	**129235**	**131522**	**121722**
$\|1\rangle$	f	0.000020(6)	0.00037(3)	0.2495(6)	0.2535(6)	0.2580(6)	0.2387(6)
x_1, x_2	p_t	0	0	1/4	1/4	1/4	1/4
	C	**130304**	**124349**	93	26	**119256**	**132601**
$\|2\rangle$	f	0.2572(6)	0.2454(6)	0.00018(2)	0.00005(1)	0.2354(6)	0.2617(6)
x_0, x_2	p_t	1/4	1/4	0	0	1/4	1/4

Table 6.5: Measured counts C, relative frequencies f, and corresponding theoretical probabilities p_t for the situation when Alice is cheating. $x_2 = x_0 \oplus x_1$.

6.4.3 Bob cheating

Alice is honest, so she sends her states exactly as in the described case above, when both parties were honest. To guess all three bits (equivalently, any two bits), Bob applies the square-root measurement consisting of four POVM elements which are actually the same as that expressed in (6.5). This POVM can be implemented by projectors $\{|\xi_i\rangle\langle\xi_i|\}_{i=00}^{11}$ in a four-dimensional Hilbert space spanned by $|0\rangle, |1\rangle, |2\rangle, |3\rangle$, where

$$
\begin{aligned}
|\xi_{00}\rangle &= \frac{1}{2}\left(|0\rangle + |1\rangle + |2\rangle + |3\rangle\right), \\
|\xi_{01}\rangle &= \frac{1}{2}\left(|0\rangle - |1\rangle + |2\rangle - |3\rangle\right), \\
|\xi_{10}\rangle &= \frac{1}{2}\left(|0\rangle + |1\rangle - |2\rangle - |3\rangle\right), \\
|\xi_{11}\rangle &= \frac{1}{2}\left(|0\rangle - |1\rangle - |2\rangle + |3\rangle\right),
\end{aligned}
\tag{6.7}
$$

are orthogonal states. The implementation of this projective measurement is shown in Fig. 6.4. The angles of the wave plates are listed in the figure caption.

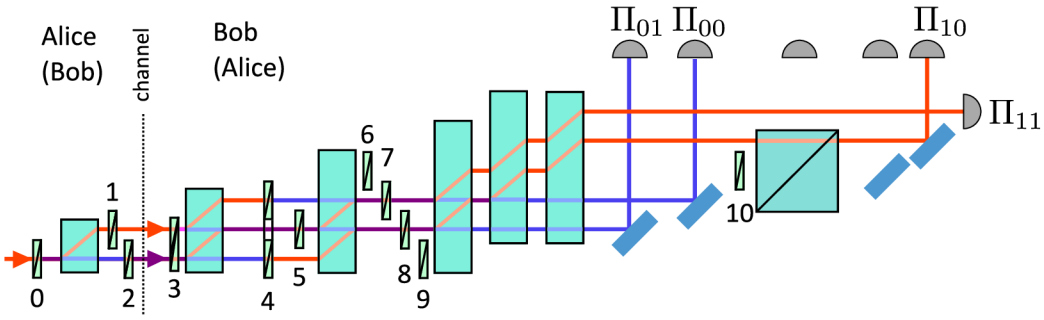


Figure 6.4: Experimental setup for the XOT protocol when Bob is cheating. The notation is the same as in Fig. 6.3. The settings for the reciever's half-wave plates are HWP3=HWP7=HWP8=22.5°, HWP4=45°, HWP5= 90°. The same setup is used for the reversed protocol when Alice is honest. But in that case, Bob is the sender and Alice is the receiver (names in parentheses). The settings of the sender's half-wave plates for honest Alice in the unreversed protocol, or for cheating Bob in the reversed protocol, are listed in Tab. 6.2, and for honest Bob in the reversed protocol in Tab. 6.7.

Alice's states were being prepared with equal probabilities. Bob's average probability of guessing all bits, estimated from the experiment, was 0.7431(3). The theoretical value is 3/4.

Alice (Bob)		Bob (Alice) $\hat{\Pi}_{00}$	$\hat{\Pi}_{01}$	$\hat{\Pi}_{10}$	$\hat{\Pi}_{11}$
$\|\phi_{00}\rangle$	C	**377482**	41178	38173	43299
	f	0.7547(6)	0.0823(4)	0.0763(4)	0.0866(4)
	p_t	3/4	1/12	1/12	1/12
$\|\phi_{01}\rangle$	C	40908	**359828**	52461	41808
	f	0.0826(4)	0.7268(6)	0.1060(4)	0.0844(4)
	p_t	1/12	3/4	1/12	1/12
$\|\phi_{10}\rangle$	C	41904	39478	**378828**	41595
	f	0.0835(4)	0.0787(4)	0.7548(6)	0.0829(4)
	p_t	1/12	1/12	3/4	1/12
$\|\phi_{11}\rangle$	C	50901	42306	38995	**368643**
	f	0.1016(4)	0.0845(4)	0.0779(4)	0.7360(6)
	p_t	1/12	1/12	1/12	3/4

Table 6.6: Measured counts C, relative frequencies f, and corresponding theoretical probabilities p_t for the situation when Bob is cheating. These results also correspond to the reversed protocol with cheating Bob – then the roles of sender and receiver are swapped (see the names in the parentheses).

In Table 6.6, we show the experimental data for the case of a dishonest Bob in the unreversed XOT protocol. While Alice honestly sent the correct states, Bob applied the square-root measurement. In fact, it also shows the experimental data for the reversed XOT protocol with a dishonest Bob, only interchanging the sender and receiver roles, see names in parentheses.

6.4.4 Reversed protocol – Both parties honest

In the reversed protocol, Bob prepares and sends one of the six non-orthogonal qutrit states defined in (6.4). These states can be prepared in a similar way as Alice's states were being prepared in the original protocol. The corresponding angles for the wave-plates are listed in Table 6.7.

	$\|\phi_{x_0=0}\rangle$	$\|\phi_{x_0=1}\rangle$	$\|\phi_{x_1=0}\rangle$	$\|\phi_{x_1=1}\rangle$	$\|\phi_{x_2=0}\rangle$	$\|\phi_{x_2=1}\rangle$
HWP0	-22.5°	22.5°	22.5°	-22.5°	45.0°	45.0°
HWP2	0.0°	0.0°	45.0°	45.0°	-22.5°	22.5°

Table 6.7: Reversed protocol. The wave plate angles for Bob's state preparation, if Bob is honest. The angle of HWP1 is always zero. $x_2 = x_0 \oplus x_1$.

In this case, Alice is the receiver. To learn the bit values she performs a POVM measurement, the components of which are defined in (6.5). We already know how to implement this measurement, because it is exactly the same as the measurement for cheating Bob in the unreversed protocol. So the corresponding higher-dimensional projective measurement consists of the projectors onto the states (6.7). Therefore, the setup for the reversed protocol in the case when both parties are honest is actually the same as the setup for the unreversed protocol when Bob is cheating – see Fig. 6.4 – only the roles of Alice and Bob are interchanged.

Bob's states were being prepared with equal probabilities. The average error rate caused by experimental imperfections was 0.00428(4).

In Table 6.8, we show the experimental data for the reversed XOT protocol when both parties are honest. Bob sent states $|\phi_{x_0=0}\rangle$, $|\phi_{x_0=1}\rangle$, $|\phi_{x_1=0}\rangle$, $|\phi_{x_1=1}\rangle$, $|\phi_{x_2=0}\rangle$, $|\phi_{x_2=1}\rangle$ and Alice performed a POVM measurement.

		Alice			
Bob		$\hat{\Pi}_{00}$	$\hat{\Pi}_{01}$	$\hat{\Pi}_{10}$	$\hat{\Pi}_{11}$
$\|\phi_{x_0=0}\rangle$	C	**249402**	**239442**	1636	1806
	f	0.5066(7)	0.4864(7)	0.00332(8)	0.00367(9)
	p_t	1/2	1/2	0	0
$\|\phi_{x_0=1}\rangle$	C	3028	762	**249215**	**246373**
	f	0.0061(1)	0.00153(6)	0.4991(7)	0.4934(7)
	p_t	0	0	1/2	1/2
$\|\phi_{x_1=0}\rangle$	C	**249097**	802	**246042**	1069
	f	0.5012(7)	0.00161(6)	0.4950(7)	0.00215(7)
	p_t	1/2	0	1/2	0
$\|\phi_{x_1=1}\rangle$	C	1019	**241863**	1840	**246310**
	f	0.00208(6)	0.4926(7)	0.00375(9)	0.5016(7)
	p_t	0	1/2	0	1/2
$\|\phi_{x_2=0}\rangle$	C	**255968**	38	301	**249572**
	f	0.5060(7)	0.00008(1)	0.00060(3)	0.4933(7)
	p_t	1/2	0	0	1/2
$\|\phi_{x_2=1}\rangle$	C	29	**237407**	**264287**	213
	f	0.00006(1)	0.4730(7)	0.5265(7)	0.00042(3)
	p_t	0	1/2	1/2	0

Table 6.8: Reversed protocol - both parties honest. Measured counts C, relative frequencies f, and corresponding theoretical probabilities p_t for the situation when both the parties were honest. $x_2 = x_0 \oplus x_1$.

6.4.5 Reversed protocol – Alice cheating

Bob honestly prepares quantum states, but cheating Alice wants to know which bit Bob has actually learned, the first or the second bit, or their XOR. In this case, however, Alice is the receiver who has to distinguish between three states

$$\begin{aligned}
\hat{\rho}_{x_0} =& \frac{1}{2}|\phi_{x_0=0}\rangle\langle\phi_{x_0=0}| + \frac{1}{2}|\phi_{x_0=1}\rangle\langle\phi_{x_0=1}| \\
=& \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|2\rangle\langle 2|, \\
\hat{\rho}_{x_1} =& \frac{1}{2}|\phi_{x_1=0}\rangle\langle\phi_{x_1=0}| + \frac{1}{2}|\phi_{x_1=1}\rangle\langle\phi_{x_1=1}| \\
=& \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|, \\
\hat{\rho}_{x_2} =& \frac{1}{2}|\phi_{x_2=0}\rangle\langle\phi_{x_2=0}| + \frac{1}{2}|\phi_{x_2=1}\rangle\langle\phi_{x_2=1}| \\
=& \frac{1}{2}|1\rangle\langle 1| + \frac{1}{2}|2\rangle\langle 2|
\end{aligned} \tag{6.8}$$

These mixed states all have prior probability 1/3, since Bob sends each of his six states with probability 1/6. Alice's optimal strategy is to use these measurement operators

$$\begin{aligned}
\hat{\Pi}_{x_0} =& \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|2\rangle\langle 2|, \\
\hat{\Pi}_{x_1} =& \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|, \\
\hat{\Pi}_{x_2} =& \frac{1}{2}|1\rangle\langle 1| + \frac{1}{2}|2\rangle\langle 2|.
\end{aligned} \tag{6.9}$$

This gives Alice a cheating probability A^{r}_{OT} of

$$\begin{aligned}
A^{\mathrm{r}}_{OT} \;=\; & \frac{1}{3}\big[\,\mathrm{Tr}(\hat{\rho}_{x_0}\hat{\Pi}_{x_0}) + \;\mathrm{Tr}(\hat{\rho}_{x_1}\hat{\Pi}_{x_1}) \\
& + \mathrm{Tr}(\hat{\rho}_{x_2}\hat{\Pi}_{x_2})\big] = \frac{1}{2},
\end{aligned} \tag{6.10}$$

which is the same cheating probability as the one Alice can achieve in the unreversed protocol. The POVM operators are actually statistical mixtures of the projectors onto the basis states $|0\rangle, |1\rangle$, and $|2\rangle$. This means that Alice can make a projective measurement followed by classical post-processing. E.g., if she obtains the result corresponding to $|0\rangle\langle 0|$, she knows that Bob has either the value of bit x_0 or the value of bit x_1, each with 50% probability. Bob's states were being prepared with equal probabilities. The average probability of Alice guessing Bob's b, estimated from the experiment, was 0.4992(2).

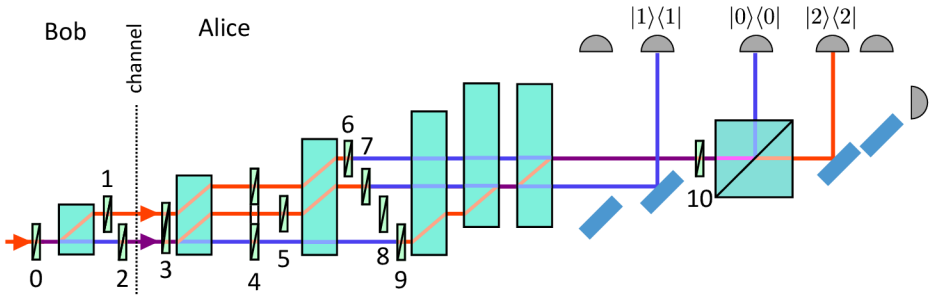


Figure 6.5: Experimental setup for the reversed XOT protocol when Alice is cheating. The notation is the same as in Fig. 6.3. The settings of Alice's half-wave plates are HWP3 = HWP4 = HWP10 = 0°, HWP5 = 90°, HWP6 = HWP7 = HWP9 = 45°.

The setup scheme implementing Alice's measurement when she is cheating is plotted in Fig. 6.5. The angles of the wave plates are listed in the figure caption.

		Alice		
		$\|0\rangle\langle 0\|$	$\|1\rangle\langle 1\|$	$\|2\rangle\langle 2\|$
Bob		x_0, x_1	x_1, x_2	x_0, x_2
$\|\phi_{x_0=0}\rangle$	C	**266828**	23	**260337**
	f	0.5061(7)	0.000044(9)	0.4938(7)
	p_t	1/2	0	1/2
$\|\phi_{x_0=1}\rangle$	C	**266040**	13	**261456**
	f	0.5043(7)	0.000025(7)	0.4956(7)
	p_t	1/2	0	1/2
$\|\phi_{x_1=0}\rangle$	C	**264336**	**255114**	172
	f	0.5087(7)	0.4910(7)	0.00033(3)
	p_t	1/2	1/2	0
$\|\phi_{x_1=1}\rangle$	C	**267393**	**255628**	151
	f	0.5111(7)	0.4886(7)	0.00029(2)
	p_t	1/2	1/2	0
$\|\phi_{x_2=0}\rangle$	C	1240	**257057**	**262665**
	f	0.00238(7)	0.4934(7)	0.5042(7)
	p_t	0	1/2	1/2
$\|\phi_{x_2=1}\rangle$	C	1192	**254941**	**262185**
	f	0.00230(7)	0.4919(7)	0.5058(7)
	p_t	0	1/2	1/2

Table 6.9: Reversed protocol. Measured counts C, relative frequencies f, and corresponding theoret. probabilities p_t for the situation when Alice was cheating. $x_2 = x_0 \oplus x_1$.

In Table 6.9, we show the experimental data for the case of a dishonest Alice in the reversed XOT protocol. While Bob honestly sent the correct states, Alice performed a projective measurement and classical post-processing.

6.4.6 Reversed protocol – Bob cheating

In this case, Alice behaves honestly but cheating Bob wants to obtain the values of both x_0 and x_1 (and thus their XOR). To estimate these values, Bob uses the set of four "fake" states equivalent to the ones in (6.2). Clearly, the experimental setup, as well as the state preparation and measurement, are the same as that for the unreversed protocol with cheating Bob, see Fig. 6.4. Therefore, it was not necessary to repeat the measurement because the results had already been obtained. They are shown in Table 6.6. The average probability of Bob guessing all bits, estimated from the experiment, was 0.7431(3). The theoretical value is 3/4.

6.5 Discussion

We have analysed and realised protocols for quantum XOR oblivious transfer. The protocols are non-interactive, do not require entanglement, and make use of pure symmetric states. We presented particular optimal quantum protocols, showing that they outperform classical XOR oblivious transfer protocols, and obtained cheating probabilities for sender and receiver for general non-interactive symmetric-state protocols. The cheating probabilities for the unreversed protocols are the same as for a previous protocol [172], which is interactive and requires entanglement.

Non-interactive protocols, which do not require entanglement, are simpler to implement. In our protocol, Bob obtains Alice's first bit, her second bit, or their XOR at random. Thus, we introduced the concept of semi-random XOT protocols, analogous to the definition of semi-random 1-2 OT protocols given in [212]. We also introduced the concept of "reversing" a protocol, which means that the sender of the quantum state instead becomes a receiver of quantum states, and vice versa, while keeping their roles in the XOT protocol the same. This is useful if one party only has the ability to prepare and send quantum states while the other party can only measure them.

We optically realised both the unreversed and the reversed version of our optimal non-interactive quantum XOT protocol, including Alice's and Bob's optimal cheating strategies. The achieved experimental data match our theoretical results very well, thus demonstrating the feasibility of both protocols.

Chapter 7

Summary

This thesis covers the generation of entangled photon pairs inside quantum dots, experiments with quantum coherence and applying one specific quantum protocol. We realize these experiments with linear quantum optics. All experiments use encoding a qubit into polarization modes of a photon and quantum state tomography using a maximum likelihood algorithm.

Our first experiment involved a gallium arsenide quantum dot embedded in a ring Bragg resonator and integrated into a multiaxial piezoelectric actuator that enables three-axis mechanical strain tuning. By applying a suitable voltage, we can shape the quantum dot on the given substrate and thus improve its broken circular symmetry. This procedure leads to a greater degeneration of the exciton level and increases entanglement of the generated photon pairs. In this thesis, we demonstrate a device concept that delivers entangled photons with high entanglement, high brightness, tunable emission energy, and low probability of multiphoton emission of photons emitted by the quantum dot. This device enables the implementation of advanced quantum communication protocols, such as entanglement swapping, quantum teleportation, and quantum key distribution based on photon entanglement.

Photon entanglement is closely related to quantum coherence. For example, the secure key rate can be quantified by the coherence of the shared bipartite quantum states [59]. In our second experiment, we investigate the protocol for assisted enhancement of quantum coherence for a qubit. We deterministically increase the coherence of the target system (one qubit) by reducing the coherence of the control system (multiple copies) while fully preserving the purity of the target system. The protocol is based on the control qubit measurement and the two-qubit interaction with a tunable coupling strength, which does not generate local coherence. We experimentally demonstrated this protocol using photonic qubits and observed the enhancement of coherence for up to five iterations of the protocol.

In the following experiment, we stayed with quantum coherence, but this time, we investigate states that maximize the mutual coherence in different subspaces of dimension {2, 3, 4} of the two-qubit Hilbert space. In our study, we quantify the coherence by the relative entropy of coherence. For this coherence measure, We have discovered an optimal non-trivial asymmetric state in a three-dimensional subspace of the Hilbert space. We experimentally prepared this optimal state from two factorized photonic qubits by a strictly incoherent probabilistic quantum operation, which projects this input state into the required three-dimensional subspace. For comparison, we also experimentally tested the preparation of the state with maximum mutual coherence using unitary transformations of the input product states. These theoretical and experimental tests demonstrate the first successful attempts to control mutual quantum coherence in qubit systems. Our results pave the way for further investigations of the properties of mutual coherence in non-trivial subspaces of composite Hilbert spaces.

Last but not least, we study one specific cryptographic protocol called non-interactive XOR oblivious transfer or XOT. It is a protocol between two participants who do not trust each other. Here, the sender, Alice, has two bits available, and the receiver, Bob, gets either the first bit, the second bit, or their XOR. He should not learn anything more, and Alice should not know what information Bob received. Of course, there is the possibility that either the sender or the receiver is not being honest, or even cheating both of them to find out as much information as possible. In the last described experiment of this thesis, we determine the smallest possible cheating probabilities for dishonest parties using symmetric pure states. We also reverse this protocol in such a way that Bob becomes the sender of the quantum state and Alice its receiver, who measures the state, while the oblivious transfer is still implemented in the same direction as in the unreversed case. The cheating probabilities for both parties remain the same as for the original variant of the protocol. This optimal quantum protocol achieves better results than classical XOR oblivious transfer protocols and better probabilistic results when cheating the sender and receiver for generally non-interactive protocols with symmetric states.

References

Articles covering the presented results

A1 M. B. Rota, T. M. Krieger, Q. Buchinger, M. Beccaceci, J. Neuwirth, H. Huet, N. Horová, G. Lovicu, G. Ronco, S. F. C. da Silva, G. Pettinari, M. Moczała-Dusanowska, C. Kohlberger, S. Manna, S. Stroj, J. Freund, X. Yuan, C. Schneider, M. Ježek, S. Höfling, F. B. Basset, T. Huber-Loyola, A. Rastelli and R. Trotta:
'A source of entangled photons based on a cavity-enhanced and strain-tuned GaAs quantum dot',
10.48550/ARXIV.2212.12506 (2022).

A2 N. Horová, R. Stárek, M. Mičuda, M. Kolář, J. Fiurášek and R. Filip:
'Deterministic controlled enhancement of local quantum coherence',
Scientific Reports **12**, 10.1038/s41598-022-26450-1 (2022).

A3 N. Horová, R. Stárek, M. Mičuda, J. Fiurášek, M. Kolář and R. Filip:
'Experimental mutual coherence from separable coherent qubits',
Physical Review A **106**, 10.1103/physreva.106.012440 (2022).

A4 L. Stroh, N. Horová, R. Stárek, I. V. Puthoor, M. Mičuda, M. Dušek and E. Andersson:
'Noninteractive xor Quantum Oblivious Transfer: Optimal Protocols and Their Experimental Implementations',
PRX Quantum **4**, 10.1103/prxquantum.4.020320 (2023).

Books

B1 M. A. Nielsen and I. L. Chuang:
Quantum Computation and Quantum Information,
(Cambridge University Press, 2012).

B2 M. T. B.E.A Saleh:
Fundamentals of photonics,
(John Wiley & Sons, Inc., 2019).

B3 M. Fox:
Optical Properties of Solids,
(Oxford University Press, 2010).

B4 D. W. Snoke:
Solid State Physics: Essential Concepts,
(Phoenix Color Corp., 2009).

B5 C. Klingshirn:
Semiconductor Optics: Second Edition,
(Springer, 2005).

B6 M. Tinkham:
Group Theory and Quantum Mechanics,
(Dover Publications, 2003).

B7 E. Wolf:
Introduction to the Theory of Coherence and Polarization of Light,
(Cambridge University Press, 2007).

Articles, proceedings and theses

1 I. Straka:
'Generation, Detection and Characterization of Photonic Quantum States',
Ph.D. thesis (Faculty of Science, Palacký University, Olomouc, 2019).

2 M. PLANCK:
'On an Improvement of Wien's Equation for the Spectrum',
The Old Quantum Theory, 79–81 (1967).

3 A. Einstein:
'Über einen die Erzeugung und Verwandlung des Lichtes betreffenden heuristischen Gesichtspunkt',
Annalen der Physik **322**, 132–148 (1905).

4 A. Einstein:
'Concerning an heuristic point of view toward the emission and transformation of light',
American Journal of Physics **33**, 367 (1965).

5 R. H. Brown and R. Twiss:
'LXXIV. A new type of interferometer for use in radio astronomy',
The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science **45**, 663–682 (1954).

6 H. Kiesel, A. Renz and F. Hasselbach:
'Observation of Hanbury Brown–Twiss anticorrelations for free electrons',
Nature **418**, 392–394 (2002).

7 R. J. Glauber:
'The Quantum Theory of Optical Coherence',
Physical Review **130**, 2529–2539 (1963).

8 A. Einstein, B. Podolsky and N. Rosen:
'Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?',
Physical Review **47**, 777–780 (1935).

9 J. S. Bell:
'On the Einstein Podolsky Rosen paradox',
Physics Physique физика **1**, 195–200 (1964).

10 A. K. Ekert:
'Quantum cryptography based on Bell's theorem',
Physical Review Letters **67**, 661–663 (1991).

11 B. P. Lanyon, T. J. Weinhold, N. K. Langford, M. Barbieri, D. F. V. James, A. Gilchrist and A. G. White:
'Experimental Demonstration of a Compiled Version of Shor's Algorithm with Quantum Entanglement',
Physical Review Letters **99**, 10.1103/physrevlett.99.250505 (2007).

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

13 D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter and A. Zeilinger:
'Experimental quantum teleportation',
Nature **390**, 575–579 (1997).

14 K. Mattle, H. Weinfurter, P. G. Kwiat and A. Zeilinger:
'Dense Coding in Experimental Quantum Communication',
Physical Review Letters **76**, 4656–4659 (1996).

15 C. H. Bennett and G. Brassard:
'Quantum cryptography: Public key distribution and coin tossing',
Theoretical Computer Science **560**, 7–11 (2014).

16 E. Knill, R. Laflamme and G. J. Milburn:
'A scheme for efficient quantum computation with linear optics',
Nature **409**, 46–52 (2001).

17 J. L. O'Brien, G. J. Pryde, A. G. White, T. C. Ralph and D. Branning:
'Demonstration of an all-optical quantum controlled-NOT gate',
Nature **426**, 264–267 (2003).

18 T. B. Pittman, M. J. Fitch, B. C. Jacobs and J. D. Franson:
'Experimental controlled-NOT logic gate for single photons in the coincidence basis',
Physical Review A **68**, 10.1103/physreva.68.032316 (2003).

19 B. P. Lanyon, M. Barbieri, M. P. Almeida, T. Jennewein, T. C. Ralph, K. J. Resch, G. J. Pryde, J. L. O'Brien, A. Gilchrist and A. G. White:
'Simplifying quantum logic using higher-dimensional Hilbert spaces',
Nature Physics **5**, 134–140 (2008).

20 M. A. Nielsen:
'Optical Quantum Computation Using Cluster States',
Physical Review Letters **93**, 10.1103/physrevlett.93.040503 (2004).

21 P. Walther, K. J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer and A. Zeilinger:
'Experimental one-way quantum computing',
Nature **434**, 169–176 (2005).

22 R. Prevedel, P. Walther, F. Tiefenbacher, P. Böhi, R. Kaltenbaek, T. Jennewein and A. Zeilinger:
'High-speed linear optics quantum computing using active feed-forward',
Nature **445**, 65–69 (2007).

23 S. Aaronson and A. Arkhipov:
'The Computational Complexity of Linear Optics',
10.48550/ARXIV.1011.3245 (2010).

24 K. R. Motes, A. Gilchrist, J. P. Dowling and P. P. Rohde:
'Scalable Boson Sampling with Time-Bin Encoding Using a Loop-Based Architecture',
Physical Review Letters **113**, 10.1103/physrevlett.113.120501 (2014).

25 H.-S. Zhong, Y. Li, W. Li, L.-C. Peng, Z.-E. Su, Y. Hu, Y.-M. He, X. Ding, W. Zhang, H. Li, L. Zhang, Z. Wang, L. You, X.-L. Wang, X. Jiang, L. Li, Y.-A. Chen, N.-L. Liu, C.-Y. Lu and J.-W. Pan:
'12-Photon Entanglement and Scalable Scattershot Boson Sampling with Optimal Entangled-Photon Pairs from Parametric Down-Conversion',
Physical Review Letters **121**, 10.1103/physrevlett.121.250505 (2018).

26 L. S. Madsen, F. Laudenbach, M. F. Askarani, F. Rortais, T. Vincent, J. F. F. Bulmer, F. M. Miatto, L. Neuhaus, L. G. Helt, M. J. Collins, A. E. Lita, T. Gerrits, S. W. Nam, V. D. Vaidya, M. Menotti, I. Dhand, Z. Vernon, N. Quesada and J. Lavoie:
'Quantum computational advantage with a programmable photonic processor',
Nature **606**, 75–81 (2022).

27 S. Stanisic, N. Linden, A. Montanaro and P. S. Turner:
'Generating entanglement with linear optics',
Physical Review A **96**, 10.1103/physreva.96.043861 (2017).

28 B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau and R. Hanson:
'Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres',
Nature **526**, 682–686 (2015).

29 B. J. Metcalf, J. B. Spring, P. C. Humphreys, N. Thomas-Peter, M. Barbieri, W. S. Kolthammer, X.-M. Jin, N. K. Langford, D. Kundys, J. C. Gates, B. J. Smith, P. G. R. Smith and I. A. Walmsley:
'Quantum teleportation on a photonic chip',
Nature Photonics **8**, 770–774 (2014).

30 J. Bao, Z. Fu, T. Pramanik, J. Mao, Y. Chi, Y. Cao, C. Zhai, Y. Mao, T. Dai, X. Chen, X. Jia, L. Zhao, Y. Zheng, B. Tang, Z. Li, J. Luo, W. Wang, Y. Yang, Y. Peng, D. Liu, D. Dai, Q. He, A. L. Muthali, L. K. Oxenløwe, C. Vigliar, S. Paesani, H. Hou, R. Santagati, J. W. Silverstone, A. Laing, M. G. Thompson, J. L. O'Brien, Y. Ding, Q. Gong and J. Wang:
'Very-large-scale integrated quantum graph photonics',
Nature Photonics **17**, 573–581 (2023).

31 X. Cheng, K.-C. Chang, Z. Xie, M. C. Sarihan, Y. S. Lee, Y. Li, X. Xu, A. K. Vinod, S. Kocaman, M. Yu, P. G.-Q. Lo, D.-L. Kwong, J. H. Shapiro, F. N. C. Wong and C. W. Wong:
'A chip-scale polarization-spatial-momentum quantum SWAP gate in silicon nanophotonics',
Nature Photonics **17**, 656–665 (2023).

32 H. Mahmudlu, R. Johanning, A. van Rees, A. Khodadad Kashi, J. P. Epping, R. Haldar, K.-J. Boller and M. Kues:
'Fully on-chip photonic turnkey quantum source for entangled qubit/qudit state generation',
Nature Photonics **17**, 518–524 (2023).

33 M. L. Chan, A. Tiranov, M. H. Appel, Y. Wang, L. Midolo, S. Scholz, A. D. Wieck, A. Ludwig, A. S. Sørensen and P. Lodahl:
'On-chip spin-photon entanglement based on photon-scattering of a quantum dot',
npj Quantum Information **9**, 10.1038/s41534-023-00717-5 (2023).

34 S. Gyger, J. Zichi, L. Schweickert, A. W. Elshaari, S. Steinhauer, S. F. Covre da Silva, A. Rastelli, V. Zwiller, K. D. Jöns and C. Errando-Herranz:
'Reconfigurable photonics with on-chip single-photon detectors',
Nature Communications **12**, 10.1038/s41467-021-21624-3 (2021).

35 M. Dai, C. Wang, B. Qiang, F. Wang, M. Ye, S. Han, Y. Luo and Q. J. Wang:
'On-chip mid-infrared photothermoelectric detectors for full-Stokes detection',
Nature Communications **13**, 10.1038/s41467-022-32309-w (2022).

36 S. E. Harris, M. K. Oshman and R. L. Byer:
'Observation of Tunable Optical Parametric Fluorescence',
Physical Review Letters **18**, 732–734 (1967).

37 P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko and Y. Shih:
'New High-Intensity Source of Polarization-Entangled Photon Pairs',
Physical Review Letters **75**, 4337–4341 (1995).

38 J. Brendel, N. Gisin, W. Tittel and H. Zbinden:
'Pulsed Energy-Time Entangled Twin-Photon Source for Quantum Communication',
Physical Review Letters **82**, 2594–2597 (1999).

39 A. Mair, A. Vaziri, G. Weihs and A. Zeilinger:
'Entanglement of the orbital angular momentum states of photons',
Nature **412**, 313–316 (2001).

40 J. T. Barreiro, N. K. Langford, N. A. Peters and P. G. Kwiat:
'Generation of Hyperentangled Photon Pairs',
Physical Review Letters **95**, 10.1103/physrevlett.95.260501 (2005).

41 T. Wilk, A. Gaëtan, C. Evellin, J. Wolters, Y. Miroshnychenko, P. Grangier and A. Browaeys:
'Entanglement of Two Individual Neutral Atoms Using Rydberg Blockade',
Physical Review Letters **104**, 10.1103/physrevlett.104.010502 (2010).

42 G.-S. Ye, B. Xu, Y. Chang, S. Shi, T. Shi and L. Li:
'A photonic entanglement filter with Rydberg atoms',
Nature Photonics **17**, 538–543 (2023).

43 H. Jayakumar, A. Predojević, T. Kauten, T. Huber, G. S. Solomon and G. Weihs:
'Time-bin entangled photons from a quantum dot',
Nature Communications **5**, 10.1038/ncomms5251 (2014).

44 L. Ginés, C. Pepe, J. Gonzales, N. Gregersen, S. Höfling, C. Schneider and A. Predojević:
'Time-bin entangled photon pairs from quantum dots embedded in a self-aligned cavity',
Optics Express **29**, 4174 (2021).

45 D. Huber, M. Reindl, Y. Huo, H. Huang, J. S. Wildmann, O. G. Schmidt, A. Rastelli and R. Trotta:
'Highly indistinguishable and strongly entangled photons from symmetric GaAs quantum dots',
Nature Communications **8**, 10.1038/ncomms15506 (2017).

46 T. Jin, X. Li, R. Liu, W. Ou, Y. Zhu, X. Wang, J. Liu, Y. Huo, X. Ou and J. Zhang:
'Generation of Polarization-Entangled Photons from Self-Assembled Quantum Dots in a Hybrid Quantum Photonic Chip',
Nano Letters **22**, 586–593 (2022).

47 Y. Delir Ghaleh Joughi and M. Sahrai:
'Spatial-dependent quantum dot-photon entanglement via tunneling effect',
Scientific Reports **12**, 10.1038/s41598-022-11810-8 (2022).

48 E. C. G. Sudarshan:
'Equivalence of Semiclassical and Quantum Mechanical Descriptions of Statistical Light Beams',
Physical Review Letters **10**, 277–279 (1963).

49 T. Baumgratz, M. Cramer and M. B. Plenio:
'Quantifying Coherence',
Physical Review Letters **113**, 10.1103/physrevlett.113.140401 (2014).

50 E. Chitambar and G. Gour:
'Comparison of incoherent operations and measures of coherence',
Physical Review A **94**, 10.1103/physreva.94.052336 (2016).

51 E. Chitambar and G. Gour:
'Critical Examination of Incoherent Operations and a Physically Consistent Resource Theory of Quantum Coherence',
Physical Review Letters **117**, 10.1103/physrevlett.117.030401 (2016).

52 E. Chitambar and G. Gour:
'Erratum: Comparison of incoherent operations and measures of coherence',
Physical Review A **95**, 10.1103/physreva.95.019902 (2017).

53 M. Hillery:
'Coherence as a resource in decision problems: The Deutsch-Jozsa algorithm and a variation',
Physical Review A **93**, 10.1103/physreva.93.012111 (2016).

54 H.-L. Shi, X.-H. Wang, S.-Y. Liu, W.-L. Yang, Z.-Y. Yang and H. Fan:
'Coherence transformations in single qubit systems',
Scientific Reports **7**, 10.1038/s41598-017-13687-4 (2017).

55 A. E. Rastegin:
'On the role of dealing with quantum coherence in amplitude amplification',
Quantum Information Processing **17**, 10.1007/s11128-018-1946-2 (2018).

56 V. Narasimhachar and G. Gour:
'Low-temperature thermodynamics with quantum coherence',
Nature Communications **6**, 10.1038/ncomms8689 (2015).

57 M. Lostaglio, K. Korzekwa, D. Jennings and T. Rudolph:
'Quantum Coherence, Time-Translation Symmetry, and Thermodynamics',
Physical Review X **5**, 10.1103/physrevx.5.021001 (2015).

58 R. Nichols, T. R. Bromley, L. A. Correa and G. Adesso:
'Practical quantum metrology in noisy environments',
Physical Review A **94**, 10.1103/physreva.94.042101 (2016).

59 J. Ma, Y. Zhou, X. Yuan and X. Ma:
'Operational interpretation of coherence in quantum key distribution',
Physical Review A **99**, 10.1103/physreva.99.062325 (2019).

60 G. Brassard and C. Crépeau:
'Quantum Bit Commitment and Coin Tossing Protocols',
Advances in Cryptology-CRYPT0' 90, 49–61 (2007).

61 R. Gennaro and Y. Lindell:
'A Framework for Password-Based Authenticated Key Exchange',
Lecture Notes in Computer Science, 524–543 (2003).

62 S. Even, O. Goldreich and A. Lempel:
'A randomized protocol for signing contracts',
Communications of the ACM **28**, 637–647 (1985).

63 G. Brassard, C. Crepeau and J.-M. Robert:
'Information theoretic reductions among disclosure problems',
27th Annual Symposium on Foundations of Computer Science (sfcs 1986), 10.1109/sfcs.1986.26 (1986).

64 R. Dowsley, F. Lacerda and A. C. A. Nascimento:
'Commitment and Oblivious Transfer in the Bounded Storage Model With Errors',
IEEE Transactions on Information Theory **64**, 5970–5984 (2018).

65 M. F. Ramos, A. N. Pinto and N. A. Silva:
'Polarization based discrete variables quantum key distribution via conjugated homodyne detection',
Scientific Reports **12**, 10.1038/s41598-022-10181-4 (2022).

66 P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier and E. Diamanti:
'Experimental demonstration of long-distance continuous-variable quantum key distribution',
Nature Photonics **7**, 378–381 (2013).

67 F. Furrer, T. Gehring, C. Schaffner, C. Pacher, R. Schnabel and S. Wehner:
'Continuous-variable protocol for oblivious transfer in the noisy-storage model',
Nature Communications **9**, 10.1038/s41467-018-03729-4 (2018).

68 I. B. Djordjevic:
'Hybrid QKD Protocol Outperforming Both DV- and CV-QKD Protocols',
IEEE Photonics Journal **12**, 1–8 (2020).

69 C. Wang, D. Huang, P. Huang, D. Lin, J. Peng and G. Zeng:
'25 MHz clock continuous-variable quantum key distribution system over 50 km fiber channel',
Scientific Reports **5**, 10.1038/srep14607 (2015).

70 S. Pirandola:
'Limits and security of free-space quantum communications',
Physical Review Research **3**, 10.1103/physrevresearch.3.013279 (2021).

71 Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen, S.-L. Han, Q. Yu, K. Liang, F. Zhou, X. Yuan, M.-S. Zhao, T.-Y. Wang, X. Jiang, L. Zhang, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, C.-Y. Lu, R. Shu, J.-Y. Wang, L. Li, N.-L. Liu, F. Xu, X.-B. Wang, C.-Z. Peng and J.-W. Pan:
'An integrated space-to-ground quantum communication network over 4,600 kilometres',
Nature **589**, 214–219 (2021).

72 G. P. He and Z. D. Wang:
'Oblivious transfer using quantum entanglement',
Physical Review A **73**, 10.1103/physreva.73.012331 (2006).

73 S. P. Neumann, A. Buchner, L. Bulla, M. Bohmann and R. Ursin:
'Continuous entanglement distribution over a transnational 248 km fiber link',
Nature Communications **13**, 10.1038/s41467-022-33919-0 (2022).

74 A. Kržič, S. Sharma, C. Spiess, U. Chandrashekara, S. Töpfer, G. Sauer, L. J. González-Martín del Campo, T. Kopf, S. Petscharnig, T. Grafenauer, R. Lieger, B. Ömer, C. Pacher, R. Berlich, T. Peschel, C. Damm, S. Risse, M. Goy, D. Rieländer, A. Tünnermann and F. Steinlechner:
'Towards metropolitan free-space quantum networks',
npj Quantum Information **9**, 10.1038/s41534-023-00754-0 (2023).

75 F. Basso Basset, M. Valeri, E. Roccia, V. Muredda, D. Poderini, J. Neuwirth, N. Spagnolo, M. B. Rota, G. Carvacho, F. Sciarrino and R. Trotta:
'Quantum key distribution with entangled photons generated on demand by a quantum dot',
Science Advances **7**, 10.1126/sciadv.abe6379 (2021).

76 S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang and J.-W. Pan:
'Satellite-to-ground quantum key distribution',
Nature **549**, 43–47 (2017).

77 Y. Cao, Y.-H. Li, K.-X. Yang, Y.-F. Jiang, S.-L. Li, X.-L. Hu, M. Abulizi, C.-L. Li, W. Zhang, Q.-C. Sun, W.-Y. Liu, X. Jiang, S.-K. Liao, J.-G. Ren, H. Li, L. You, Z. Wang, J. Yin, C.-Y. Lu, X.-B. Wang, Q. Zhang, C.-Z. Peng and J.-W. Pan:
'Long-Distance Free-Space Measurement-Device-Independent Quantum Key Distribution',
Physical Review Letters **125**, 10.1103/physrevlett.125.260503 (2020).

78 A. Broadbent and P. Yuen:
'Device-independent oblivious transfer from the bounded-quantum-storage-model and computational assumptions',
New Journal of Physics **25**, 053019 (2023).

79 M. Mičuda, M. Miková, I. Straka, M. Sedlák, M. Dušek, M. Ježek and J. Fiurášek:
'Tomographic characterization of a linear optical quantum Toffoli gate',
Physical Review A **92**, 10.1103/physreva.92.032312 (2015).

80 R. Stárek, M. Miková, I. Straka, M. Dušek, M. Ježek, J. Fiurášek and M. Mičuda:
'Experimental realization of SWAP operation on hyper-encoded qubits',
Optics Express **26**, 8443 (2018).

81 M.-Z. ZHU and L. YE:
'IMPLEMENTATION OF SWAP GATE AND FREDKIN GATE USING LINEAR OPTICAL ELEMENTS',
International Journal of Quantum Information **11**, 1350031 (2013).

82 F. Flamini, N. Spagnolo and F. Sciarrino:
'Photonic quantum information processing: a review',
Reports on Progress in Physics **82**, 016001 (2018).

83 V. D'Ambrosio, E. Nagali, C. H. Monken, S. Slussarenko, L. Marrucci and F. Sciarrino:
'Deterministic qubit transfer between orbital and spin angular momentum of single photons',
Optics Letters **37**, 172 (2012).

84 J. M. Donohue, M. Agnew, J. Lavoie and K. J. Resch:
'Coherent Ultrafast Measurement of Time-Bin Encoded Photons',
Physical Review Letters **111**, 10.1103/physrevlett.111.153602 (2013).

85 J. M. Lukens:
'Quantum information processing with frequency-bin qubits: progress, status, and challenges',
Conference on Lasers and Electro-Optics, 10.1364/cleo_at.2019.jtu4a.3 (2019).

86 Y. Ding, D. Bacco, K. Dalgaard, X. Cai, X. Zhou, K. Rottwitt and L. K. Oxenløwe:
'High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits',
npj Quantum Information **3**, 10.1038/s41534-017-0026-2 (2017).

87 J. Wang, S. Paesani, Y. Ding, R. Santagati, P. Skrzypczyk, A. Salavrakos, J. Tura, R. Augusiak, L. Mančinska, D. Bacco, D. Bonneau, J. W. Silverstone, Q. Gong, A. Acín, K. Rottwitt, L. K. Oxenløwe, J. L. O'Brien, A. Laing and M. G. Thompson:
'Multidimensional quantum entanglement with large-scale integrated optics',
Science **360**, 285–291 (2018).

88 M. Krenn, A. Hochrainer, M. Lahiri and A. Zeilinger:
'Entanglement by Path Identity',
Physical Review Letters **118**, 10.1103/physrevlett.118.080401 (2017).

89 F. Bouchard, A. Sit, Y. Zhang, R. Fickler, F. M. Miatto, Y. Yao, F. Sciarrino and E. Karimi:
'Two-photon interference: the Hong–Ou–Mandel effect',
Reports on Progress in Physics **84**, 012402 (2020).

90 C. K. Hong, Z. Y. Ou and L. Mandel:
'Measurement of subpicosecond time intervals between two photons by interference',
Physical Review Letters **59**, 2044–2046 (1987).

91 Z. Hradil:
'Quantum-state estimation',
Physical Review A **55**, R1561–R1564 (1997).

92 M. Ježek, J. Fiurášek and Z. Hradil:
'Quantum inference of states and processes',
Physical Review A **68**, 10.1103/physreva.68.012305 (2003).

93 Z. Hradil, J. Řeháček, J. Fiurášek and M. Ježek:
'3 Maximum-Likelihood Methods in Quantum Mechanics',
Quantum State Estimation, 59–112 (2004).

94 R. Stárek:
'Experimental implementation of complex multiqubit quantum logic gates on platform of linear optics and their applications',
Ph.D. thesis (Faculty of Science, Palacký University, Olomouc, 2022).

95 X.-M. Hu, Y. Guo, B.-H. Liu, C.-F. Li and G.-C. Guo:
'Progress in quantum teleportation',
Nature Reviews Physics **5**, 339–353 (2023).

96 E. Fitzke, L. Bialowons, T. Dolejsky, M. Tippmann, O. Nikiforov, T. Walther, F. Wissel and M. Gunkel:
'Scalable Network for Simultaneous Pairwise Quantum Key Distribution via Entanglement-Based Time-Bin Coding',
PRX Quantum **3**, 10.1103/prxquantum.3.020341 (2022).

97 F. Zaman, Y. Jeong and H. Shin:
'Dual Quantum Zeno Superdense Coding',
Scientific Reports **9**, 10.1038/s41598-019-47667-7 (2019).

98 M. Müller, S. Bounouar, K. D. Jöns, M. Glässl and P. Michler:
'On-demand generation of indistinguishable polarization-entangled photon pairs',
Nature Photonics **8**, 224–228 (2014).

99 M. Neset:
'Advanced photonic sources and their applications',
Master's thesis (Faculty of Science, Palacký University, Olomouc, 2020).

100 L. Olislager, J. Cussey, A. T. Nguyen, P. Emplit, S. Massar, J.-M. Merolla and K. P. Huy:
'Frequency-bin entangled photons',
Physical Review A **82**, 10.1103/physreva.82.013804 (2010).

101 J. C. Howell, R. S. Bennink, S. J. Bentley and R. W. Boyd:
'Realization of the Einstein-Podolsky-Rosen Paradox Using Momentum- and Position-Entangled Photons from Spontaneous Parametric Down Conversion',
Physical Review Letters **92**, 10.1103/physrevlett.92.210403 (2004).

102 M. Kaur and M. Singh:
'Quantum double-double-slit experiment with momentum entangled photons',
Scientific Reports **10**, 10.1038/s41598-020-68181-1 (2020).

103 C. Simon and J.-P. Poizat:
'Creating Single Time-Bin-Entangled Photon Pairs',
Physical Review Letters **94**, 10.1103/physrevlett.94.030502 (2005).

104 C. Wang, C.-H. Lee, Y. Kim and Y.-H. Kim:
'Generation of hyper-entangled photons in a hot atomic vapor',
Optics Letters **45**, 1802 (2020).

105 S. Ghosh, N. Rivera, G. Eisenstein and I. Kaminer:
'Creating heralded hyper-entangled photons using Rydberg atoms',
Light: Science & Applications **10**, 10.1038/s41377-021-00537-2 (2021).

106 L. Achatz, L. Bulla, S. Ecker, E. A. Ortega, M. Bartokos, J. C. Alvarado-Zacarias, R. Amezcua-Correa, M. Bohmann, R. Ursin and M. Huber:
'Simultaneous transmission of hyper-entanglement in three degrees of freedom through a multicore fiber',
npj Quantum Information **9**, 10.1038/s41534-023-00700-0 (2023).

107 M. A. Nielsen:
'Conditions for a Class of Entanglement Transformations',
Physical Review Letters **83**, 436–439 (1999).

108 P. J. Dodd and J. J. Halliwell:
'Disentanglement and decoherence by open system dynamics',
Physical Review A **69**, 10.1103/physreva.69.052105 (2004).

109 M. P. Almeida, F. de Melo, M. Hor-Meyll, A. Salles, S. P. Walborn, P. H. S. Ribeiro and L. Davidovich:
'Environment-Induced Sudden Death of Entanglement',
Science **316**, 579–582 (2007).

110 R. Horodecki, P. Horodecki, M. Horodecki and K. Horodecki:
'Quantum entanglement',
Reviews of Modern Physics **81**, 865–942 (2009).

111 G. Peruzzo and S. Sorella:
'Entanglement and maximal violation of the CHSH inequality in a system of two spins j: A novel construction and further observations',
Physics Letters A **474**, 128847 (2023).

112 O. Gühne, P. Hyllus, D. Bruß, A. Ekert, M. Lewenstein, C. Macchiavello and A. Sanpera:
'Detection of entanglement with few local measurements',
Physical Review A **66**, 10.1103/physreva.66.062305 (2002).

113 M. Barbieri, F. De Martini, G. Di Nepi, P. Mataloni, G. M. D'Ariano and C. Macchiavello:
'Detection of Entanglement with Polarized Photons: Experimental Realization of an Entanglement Witness',
Physical Review Letters **91**, 10.1103/physrevlett.91.227901 (2003).

114 J. S. Kim:
'Entanglement of formation and monogamy of multi-party quantum entanglement',
Scientific Reports **11**, 10.1038/s41598-021-82052-3 (2021).

115 P. Senellart, G. Solomon and A. White:
'High-performance semiconductor quantum-dot single-photon sources',
Nature Nanotechnology **12**, 1026–1039 (2017).

116 Y. Arakawa and M. J. Holmes:
'Progress in quantum-dot single photon sources for quantum information technologies: A broad spectrum overview',
Applied Physics Reviews **7**, 10.1063/5.0010193 (2020).

117 M. Bozzio, M. Vyvlecka, M. Cosacchi, C. Nawrath, T. Seidelmann, J. C. Loredo, S. L. Portalupi, V. M. Axt, P. Michler and P. Walther:
'Enhancing quantum cryptography with quantum dot single-photon sources',
npj Quantum Information **8**, 10.1038/s41534-022-00626-z (2022).

118 D. B. Higginbottom, L. Slodička, G. Araneda, L. Lachman, R. Filip, M. Hennrich and R. Blatt:
'Pure single photons from a trapped atom source',
New Journal of Physics **18**, 093038 (2016).

119 W. E. Moerner:
'Single-photon sources based on single molecules in solids',
New Journal of Physics **6**, 88–88 (2004).

120 A. Kiraz, M. Ehrl, T. Hellerer, Ö. E. Müstecaplioğlu, C. Bräuchle and A. Zumbusch:
'Indistinguishable Photons from a Single Molecule',
Physical Review Letters **94**, 10.1103/physrevlett.94.223602 (2005).

121 M. Meraner, A. Mazloom, V. Krutyanskiy, V. Krcmarsky, J. Schupp, D. A. Fioretto, P. Sekatski, T. E. Northup, N. Sangouard and B. P. Lanyon:
'Indistinguishable photons from a trapped-ion quantum network node',
Physical Review A **102**, 10.1103/physreva.102.052614 (2020).

122 T. M. Babinec, B. J. M. Hausmann, M. Khan, Y. Zhang, J. R. Maze, P. R. Hemmer and M. Lončar:
'A diamond nanowire single-photon source',
Nature Nanotechnology **5**, 195–199 (2010).

123 N. Mizuochi, T. Makino, H. Kato, D. Takeuchi, M. Ogura, H. Okushi, M. Nothaft, P. Neumann, A. Gali, F. Jelezko, J. Wrachtrup and S. Yamasaki:
'Electrically driven single-photon source at room temperature in diamond',
Nature Photonics **6**, 299–303 (2012).

124 L. A. Rozema, C. Wang, D. H. Mahler, A. Hayat, A. M. Steinberg, J. E. Sipe and M. Liscidini:
'Characterizing an entangled-photon source with classical detectors and measurements',
Optica **2**, 430 (2015).

125 M. V. Jabir and G. K. Samanta:
'Robust, high brightness, degenerate entangled photon source at room temperature',
Scientific Reports **7**, 10.1038/s41598-017-12709-5 (2017).

126 P. Kultavewuti, E. Y. Zhu, X. Xing, L. Qian, V. Pusino, M. Sorel and J. S. Aitchison:
'Polarization-entangled photon pair sources based on spontaneous four wave mixing assisted by polarization mode dispersion',
Scientific Reports **7**, 10.1038/s41598-017-06010-8 (2017).

127 K. Lee, J. Jung and J. H. Lee:
'Optical fiber polarization-entangled photon pair source using intermodal spontaneous four-wave mixing in the visible spectral band',
Laser Physics Letters **20**, 015101 (2022).

128 G. Kulkarni, J. Rioux, B. Braverman, M. V. Chekhova and R. W. Boyd:
'Classical model of spontaneous parametric down-conversion',
Physical Review Research **4**, 10.1103/physrevresearch.4.033098 (2022).

129 J. Tang, L. Tang, H. Wu, Y. Wu, H. Sun, H. Zhang, T. Li, Y. Lu, M. Xiao and K. Xia:
'Towards On-Demand Heralded Single-Photon Sources via Photon Blockade',
Physical Review Applied **15**, 10.1103/physrevapplied.15.064020 (2021).

130 X. P. Hu, P. Xu and S. N. Zhu:
'Engineered quasi-phase-matching for laser techniques [Invited]',
Photonics Research **1**, 171 (2013).

131 F. T. Rabouw and C. de Mello Donega:
'Excited-State Dynamics in Colloidal Semiconductor Nanocrystals',
Topics in Current Chemistry **374**, 10.1007/s41061-016-0060-0 (2016).

132 A. Schliwa, M. Winkelnkemper and D. Bimberg:
'Few-particle energies versus geometry and composition of $In_xGa_{1-x}Ga/GaAs$ self-organized quantum dots',
Physical Review B **79**, 10.1103/physrevb.79.075443 (2009).

133 K. Kowalik:
'Symmetry effects in optical properties of single semiconductor quantum dots',
Ph.D. thesis (Université Pierre et Marie Curie – Paris VI, 2007).

134 M. Rota:
'Quantum Dots for Quantum Networks',
Ph.D. thesis (Sapienza – University of Rome, 2021).

135 O. Benson, C. Santori, M. Pelton and Y. Yamamoto:
'Regulated and Entangled Photons from a Single Quantum Dot',
Physical Review Letters **84**, 2513–2516 (2000).

136 R. Seguin, A. Schliwa, S. Rodt, K. Pötschke, U. W. Pohl and D. Bimberg:
'Size-Dependent Fine-Structure Splitting in InAs/GaAs Self-Organized Quantum Dots',
Physical Review Letters **95**, 10.1103/physrevlett.95.257402 (2005).

137 M. Bayer, G. Ortner, O. Stern, A. Kuther, A. A. Gorbunov, A. Forchel, P. Hawrylak, S. Fafard, K. Hinzer, T. L. Reinecke, S. N. Walck, J. P. Reithmaier, F. Klopf and F. Schäfer:
'Fine structure of neutral and charged excitons in self-assembled In(Ga)As/(Al)GaAs quantum dots',
Physical Review B **65**, 10.1103/physrevb.65.195315 (2002).

138 W. Langbein, P. Borri, U. Woggon, V. Stavarache, D. Reuter and A. D. Wieck:
'Control of fine-structure splitting and biexciton binding in $In_xGa_{1-x}As$ quantum dots by annealing',
Physical Review B **69**, 10.1103/physrevb.69.161301 (2004).

139 E. Margapoti, L. Worschech, A. Forchel, A. Tribu, T. Aichele, R. André and K. Kheng:
'Annealing induced inversion of quantum dot fine-structure splitting',
Applied Physics Letters **90**, 10.1063/1.2737131 (2007).

140 K. Kowalik, O. Krebs, A. Lemaître, S. Laurent, P. Senellart, P. Voisin and J. A. Gaj:
'Influence of an in-plane electric field on exciton fine structure in InAs-GaAs self-assembled quantum dots',
Applied Physics Letters **86**, 041907 (2005).

141 A. Muller, W. Fang, J. Lawall and G. S. Solomon:
'Creating Polarization-Entangled Photon Pairs from a Semiconductor Quantum Dot Using the Optical Stark Effect',
Physical Review Letters **103**, 10.1103/physrevlett.103.217402 (2009).

142 R. M. Stevenson, R. J. Young, P. Atkinson, K. Cooper, D. A. Ritchie and A. J. Shields:
'A semiconductor source of triggered entangled photon pairs',
Nature **439**, 179–182 (2006).

143 G. Bester, S. Nair and A. Zunger:
'Pseudopotential calculation of the excitonic fine structure of million-atom self-assembled $In_{1-x}Ga_x$/GaAs quantum dots',
Physical Review B **67**, 10.1103/physrevb.67.161306 (2003).

144 G. Bester and A. Zunger:
'Cylindrically shaped zinc-blende semiconductor quantum dots do not have cylindrical symmetry: Atomistic symmetry, atomic relaxation, and piezoelectric effects',
Physical Review B **71**, 10.1103/physrevb.71.045318 (2005).

145 R. Trotta, E. Zallo, C. Ortix, P. Atkinson, J. D. Plumhof, J. van den Brink, A. Rastelli and O. G. Schmidt:
'Universal Recovery of the Energy-Level Degeneracy of Bright Excitons in InGaAs Quantum Dots without a Structure Symmetry',
Physical Review Letters **109**, 10.1103/physrevlett.109.147401 (2012).

146 R. Trotta, J. Martín-Sánchez, I. Daruka, C. Ortix and A. Rastelli:
'Energy-Tunable Sources of Entangled Photons: A Viable Concept for Solid-State-Based Quantum Relays',
Physical Review Letters **114**, 10.1103/physrevlett.114.150502 (2015).

147 Z. Xi, Y. Li and H. Fan:
'Quantum coherence and correlations in quantum system',
Scientific Reports **5**, 10.1038/srep10922 (2015).

148 D. Mondal, T. Pramanik and A. K. Pati:
'Nonlocal advantage of quantum coherence',
Physical Review A **95**, 10.1103/physreva.95.010301 (2017).

149 N. H. Y. Ng and M. P. Woods:
'Resource Theory of Quantum Thermodynamics: Thermal Operations and Second Laws',
Fundamental Theories of Physics, 625–650 (2018).

150 E. Chitambar and G. Gour:
'Quantum resource theories',
Reviews of Modern Physics **91**, 10.1103/revmodphys.91.025001 (2019).

151 K. Korzekwa:
'Resource theory of asymmetry',
Ph.D. thesis (Imperial College London, 2013).

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

153 C. Spee, J. I. de Vicente and B. Kraus:
'The maximally entangled set of 4-qubit states',
Journal of Mathematical Physics **57**, 10.1063/1.4946895 (2016).

154 K. Ben Dana, M. García Díaz, M. Mejatty and A. Winter:
'Resource theory of coherence: Beyond states',
Physical Review A **95**, 10.1103/physreva.95.062327 (2017).

155 Z. Zhang, Y. Dai, Y.-L. Dong and C. Zhang:
'Numerical and analytical results for geometric measure of coherence and geometric measure of entanglement',
Scientific Reports **10**, 10.1038/s41598-020-68979-z (2020).

156 Y. Guo and S. Goswami:
'Discordlike correlation of bipartite coherence',
Physical Review A **95**, 10.1103/physreva.95.062340 (2017).

157 X.-L. Wang, Q.-L. Yue, C.-H. Yu, F. Gao and S.-J. Qin:
'Relating quantum coherence and correlations with entropy-based measures',
10.48550/arXiv.1703.00648 (2017).

158 A. Streltsov, U. Singh, H. S. Dhar, M. N. Bera and G. Adesso:
'Measuring Quantum Coherence with Entanglement',
Physical Review Letters **115**, 10.1103/physrevlett.115.020403 (2015).

159 L.-H. Ren, M. Gao, J. Ren, Z. D. Wang and Y.-K. Bai:
'Resource conversion between operational coherence and multipartite entanglement in many-body systems',
New Journal of Physics **23**, 043053 (2021).

160 Y. Watanabe:
'Privacy amplification for quantum key distribution',
Journal of Physics A: Mathematical and Theoretical **40**, F99–F104 (2006).

161 D. Bacco, J. B. Christensen, M. A. U. Castaneda, Y. Ding, S. Forchhammer, K. Rottwitt and L. K. Oxenløwe:
'Two-dimensional distributed-phase-reference protocol for quantum key distribution',
Scientific Reports **6**, 10.1038/srep36756 (2016).

162 P. W. Shor and J. Preskill:
'Simple Proof of Security of the BB84 Quantum Key Distribution Protocol',
Physical Review Letters **85**, 441–444 (2000).

163 J. Martinez-Mateo, C. Pacher, M. Peev, A. Ciurana and V. Martin:
'Demystifying the information reconciliation protocol cascade',
Quantum Information and Computation, 453–477 (2015).

164 C. H. Bennett, G. Brassard and J.-M. Robert:
'Privacy Amplification by Public Discussion',
SIAM Journal on Computing **17**, 210–229 (1988).

165 C. H. Bennett, G. Brassard and N. D. Mermin:
'Quantum cryptography without Bell's theorem',
Physical Review Letters **68**, 557–559 (1992).

166 H.-K. Lo, X. Ma and K. Chen:
'Decoy State Quantum Key Distribution',
Physical Review Letters **94**, 10.1103/physrevlett.94.230504 (2005).

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

168 D. Bruß:
'Optimal Eavesdropping in Quantum Cryptography with Six States',
Physical Review Letters **81**, 3018–3021 (1998).

169 S. Wiesner:
'Conjugate coding',
ACM SIGACT News **15**, 78–88 (1983).

170 C.-K. Chu and W.-G. Tzeng:
'Efficient k-Out-of-n Oblivious Transfer Schemes with Adaptive and Non-adaptive Queries',
Public Key Cryptography - PKC 2005, 172–183 (2005).

171 G. Brassard, C. Crépeau and S. Wolf:
'Oblivious Transfers and Privacy Amplification',
Journal of Cryptology **16**, 219–237 (2003).

172 S. Kundu, J. Sikora and E. Y.-Z. Tan:
'A device-independent protocol for XOR oblivious transfer',
Quantum **6**, 725 (2022).

173 D. Mayers:
'Unconditionally Secure Quantum Bit Commitment is Impossible',
Physical Review Letters **78**, 3414–3417 (1997).

174 H.-K. Lo:
'Insecurity of quantum secure computations',
Physical Review A **56**, 1154–1162 (1997).

175 D. Pitalúa-García:
'Spacetime-constrained oblivious transfer',
Physical Review A **93**, 10.1103/physreva.93.062346 (2016).

176 D. Pitalúa-García and I. Kerenidis:
'Practical and unconditionally secure spacetime-constrained oblivious transfer',
Physical Review A **98**, 10.1103/physreva.98.032327 (2018).

177 I. B. Damgård, S. Fehr, L. Salvail and C. Schaffner:
'Cryptography in the Bounded-Quantum-Storage Model',
SIAM Journal on Computing **37**, 1865–1890 (2008).

178 J. Kaniewski and S. Wehner:
'Device-independent two-party cryptography secure against sequential attacks',
New Journal of Physics **18**, 055004 (2016).

179 P. Chan, I. Lucio-Martinez, X. Mo, C. Simon and W. Tittel:
'Performing private database queries in a real-world environment using a quantum protocol',
Scientific Reports **4**, 10.1038/srep05233 (2014).

180 C. H. Bennett, G. Brassard, C. Crépeau and M.-H. Skubiszewska:
'Practical Quantum Oblivious Transfer',
Advances in Cryptology — CRYPTO '91, 351–366 (2007).

181 A. Chailloux, G. Gutoski and J. Sikora:
'Optimal bounds for semi-honest quantum oblivious transfer',
Chicago Journal of Theoretical Computer Science **22**, 1–17 (2016).

182 S. Kolatschek, C. Nawrath, S. Bauer, J. Huang, J. Fischer, R. Sittig, M. Jetter, S. L. Portalupi and P. Michler:
'Bright Purcell Enhanced Single-Photon Source in the Telecom O-Band Based on a Quantum Dot in a Circular Bragg Grating',
Nano Letters **21**, 7740–7745 (2021).

183 E. Schöll, L. Schweickert, L. Hanschke, K. D. Zeuner, F. Sbresny, T. Lettner, R. Trivedi, M. Reindl, S. F. Covre da Silva, R. Trotta, J. J. Finley, J. Vučković, K. Müller, A. Rastelli, V. Zwiller and K. D. Jöns:
'Crux of Using the Cascaded Emission of a Three-Level Quantum Ladder System to Generate Indistinguishable Photons',
Physical Review Letters **125**, 10.1103/physrevlett.125.233605 (2020).

184 K. A. Fischer, R. Trivedi and D. Lukin:
'Particle emission from open quantum systems',
Physical Review A **98**, 10.1103/physreva.98.023853 (2018).

185 F. Basso Basset, M. B. Rota, C. Schimpf, D. Tedeschi, K. D. Zeuner, S. F. Covre da Silva, M. Reindl, V. Zwiller, K. D. Jöns, A. Rastelli and R. Trotta:
'Entanglement Swapping with Photons Generated on Demand by a Quantum Dot',
Physical Review Letters **123**, 10.1103/physrevlett.123.160501 (2019).

186 A. J. Hudson, R. M. Stevenson, A. J. Bennett, R. J. Young, C. A. Nicoll, P. Atkinson, K. Cooper, D. A. Ritchie and A. J. Shields:
'Coherence of an Entangled Exciton-Photon State',
Physical Review Letters **99**, 10.1103/physrevlett.99.266802 (2007).

187 R. Trotta, J. S. Wildmann, E. Zallo, O. G. Schmidt and A. Rastelli:
'Highly Entangled Photons from Hybrid Piezoelectric-Semiconductor Quantum Dot Devices',
Nano Letters **14**, 3439–3444 (2014).

188 J. Ma, B. Yadin, D. Girolami, V. Vedral and M. Gu:
'Converting Coherence to Quantum Correlations',
Physical Review Letters **116**, 10.1103/physrevlett.116.160407 (2016).

189 P. Giorda and M. Allegra:
'Coherence in quantum estimation',
10.48550/arxiv.1611.02519 (2016).

190 S. Rahav, U. Harbola and S. Mukamel:
'Heat fluctuations and coherences in a quantum heat engine',
Physical Review A **86**, 10.1103/physreva.86.043843 (2012).

191 J. Åberg:
'Catalytic Coherence',
Physical Review Letters **113**, 10.1103/physrevlett.113.150402 (2014).

192 P. Solinas and S. Gasparinetti:
'Full distribution of work done on a quantum system for arbitrary initial states',
Physical Review E **92**, 10.1103/physreve.92.042150 (2015).

193 S. Lloyd:
'Quantum coherence in biological systems',
Journal of Physics: Conference Series **302**, 012037 (2011).

194 B. Foxen, C. Neill, A. Dunsworth, P. Roushan, B. Chiaro, A. Megrant, J. Kelly, Z. Chen, K. Satzinger, R. Barends, F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, S. Boixo, D. Buell, B. Burkett, Y. Chen, R. Collins, E. Farhi, A. Fowler, C. Gidney, M. Giustina, R. Graff, M. Harrigan, T. Huang, S. V. Isakov, E. Jeffrey, Z. Jiang, D. Kafri, K. Kechedzhi, P. Klimov, A. Korotkov, F. Kostritsa, D. Landhuis, E. Lucero, J. McClean, M. McEwen, X. Mi, M. Mohseni, J. Y. Mutus, O. Naaman, M. Neeley, M. Niu, A. Petukhov, C. Quintana, N. Rubin, D. Sank, V. Smelyanskiy, A. Vainsencher, T. C. White, Z. Yao, P. Yeh, A. Zalcman, H. Neven, J. M. Martinis and G. A. Quantum:
'Demonstrating a Continuous Set of Two-qubit Gates for Near-term Quantum Algorithms',
Physical Review Letters **125**, 10.1103/physrevlett.125.120504 (2020).

195 Y. Wu, W.-S. Bao, S. Cao, F. Chen, M.-C. Chen, X. Chen, T.-H. Chung, H. Deng, Y. Du, D. Fan, M. Gong, C. Guo, C. Guo, S. Guo, L. Han, L. Hong, H.-L. Huang, Y.-H. Huo, L. Li, N. Li, S. Li, Y. Li, F. Liang, C. Lin, J. Lin, H. Qian, D. Qiao, H. Rong, H. Su, L. Sun, L. Wang, S. Wang, D. Wu, Y. Xu, K. Yan, W. Yang, Y. Yang, Y. Ye, J. Yin, C. Ying, J. Yu, C. Zha, C. Zhang, H. Zhang, K. Zhang, Y. Zhang, H. Zhao, Y. Zhao, L. Zhou, Q. Zhu, C.-Y. Lu, C.-Z. Peng, X. Zhu and J.-W. Pan:
'Strong Quantum Computational Advantage Using a Superconducting Quantum Processor',
Physical Review Letters **127**, 10.1103/physrevlett.127.180501 (2021).

196 C. Monroe, W. C. Campbell, L.-M. Duan, Z.-X. Gong, A. V. Gorshkov, P. W. Hess, R. Islam, K. Kim, N. M. Linke, G. Pagano, P. Richerme, C. Senko and N. Y. Yao:
'Programmable quantum simulations of spin systems with trapped ions',
Reviews of Modern Physics **93**, 10.1103/revmodphys.93.025001 (2021).

197 D. Barredo, H. Labuhn, S. Ravets, T. Lahaye, A. Browaeys and C. S. Adams:
'Coherent Excitation Transfer in a Spin Chain of Three Rydberg Atoms',
Physical Review Letters **114**, 10.1103/physrevlett.114.113002 (2015).

198 P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling and G. J. Milburn:
'Linear optical quantum computing with photonic qubits',
Reviews of Modern Physics **79**, 135–174 (2007).

199 A. Černoch, J. Soubusta, L. Bartůšková, M. Dušek and J. Fiurášek:
'Experimental Realization of Linear-Optical Partial swap Gates',
Physical Review Letters **100**, 10.1103/physrevlett.100.180501 (2008).

200 M. Mičuda, E. Doláková, I. Straka, M. Miková, M. Dušek, J. Fiurášek and M. Ježek:
'Highly stable polarization independent Mach-Zehnder interferometer',
Review of Scientific Instruments **85**, 10.1063/1.4891702 (2014).

201 K. Fang, X. Wang, L. Lami, B. Regula and G. Adesso:
'Probabilistic Distillation of Quantum Coherence',
Physical Review Letters **121**, 10.1103/physrevlett.121.070404 (2018).

202 Q. Zhao, Y. Liu, X. Yuan, E. Chitambar and X. Ma:
'One-Shot Coherence Dilution',
Physical Review Letters **120**, 10.1103/physrevlett.120.070403 (2018).

203 R. Stárek, M. Mičuda, M. Kolář, R. Filip and J. Fiurášek:
'Experimental demonstration of optimal probabilistic enhancement of quantum coherence',
Quantum Science and Technology **6**, 045010 (2021).

204 M. Ježek, I. Straka, M. Mičuda, M. Dušek, J. Fiurášek and R. Filip:
'Experimental Test of the Quantum Non-Gaussian Character of a Heralded Single-Photon State',
Physical Review Letters **107**, 10.1103/physrevlett.107.213602 (2011).

205 J. Fiurášek, R. Stárek and M. Mičuda:
'Optimal implementation of two-qubit linear-optical quantum filters',
Physical Review A **103**, 10.1103/physreva.103.062408 (2021).

206 N. Kiesel, C. Schmid, U. Weber, R. Ursin and H. Weinfurter:
'Linear Optics Controlled-Phase Gate Made Simple',
Physical Review Letters **95**, 10.1103/physrevlett.95.210505 (2005).

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

208 R. Okamoto, H. F. Hofmann, S. Takeuchi and K. Sasaki:
'Demonstration of an Optical Quantum Controlled-NOT Gate without Path Interference',
Physical Review Letters **95**, 10.1103/physrevlett.95.210506 (2005).

209 H. W. Li, S. Przeslak, A. O. Niskanen, J. C. F. Matthews, A. Politi, P. Shadbolt, A. Laing, M. Lobino, M. G. Thompson and J. L. O'Brien:
'Reconfigurable controlled two-qubit operation on a quantum photonic chip',
New Journal of Physics **13**, 115009 (2011).

210 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**, 711–716 (2015).

211 M. Zhang, L. Feng, M. Li, Y. Chen, L. Zhang, D. He, G. Guo, G. Guo, X. Ren and D. Dai:
'Supercompact Photonic Quantum Logic Gate on a Silicon Chip',
Physical Review Letters **126**, 10.1103/physrevlett.126.130501 (2021).

212 R. Amiri, R. Stárek, D. Reichmuth, I. V. Puthoor, M. Mičuda, L. Mišta Jr., M. Dušek, P. Wallden and E. Andersson:
'Imperfect 1-Out-of-2 Quantum Oblivious Transfer: Bounds, a Protocol, and its Experimental Implementation',
PRX Quantum **2**, 10.1103/prxquantum.2.010335 (2021).

213 P. Hausladen and W. K. Wootters:
'A 'Pretty Good' Measurement for Distinguishing Quantum States',
Journal of Modern Optics **41**, 2385–2390 (1994).

214 M. Ban, K. Kurokawa, R. Momose and O. Hirota:
'Optimum measurements for discrimination among symmetric quantum states and parameter estimation',
International Journal of Theoretical Physics **36**, 1269–1288 (1997).