Efficient Generation of Photonic Entanglement and Multiparty Quantum Communication

Pavel Trojek

München 2007

Efficient Generation of Photonic Entanglement and Multiparty Quantum Communication

Pavel Trojek

Dissertation submitted
for the degree of
Doctor of Philosophy

Faculty of Physics
Ludwig-Maximilians-Universität München
September 2007

Erstgutachter/ First referee: Prof. Dr. Harald Weinfurter
Zweitgutachter/ Second referee: Prof. Dr. Eberhard Riedle
Tag der mündlichen Prüfung/ Day of oral exam: 19.12.2007

Contents

Zusammenfassung vii

Summary ix

1 Introduction 1

1.1 Quantum mechanics . . . 1
1.1.1 The underlying principles . . . 1
1.1.2 EPR paradox and Bell's theorem . . . 2
1.1.3 Clauser-Horne-Shominy-Holt inequality . . . 5
1.2 Quantum information processing and communication . . . 8
1.3 Overview . . . 8

2 Spontaneous parametric down-conversion 11

2.1 Nonlinearity and anisotropy of a dielectric . . . 12
2.2 Simple theoretical model . . . 17
2.3 Multimode description . . . 22
2.3.1 Spectra of down-conversion fields . . . 25
2.3.2 Time distribution of down-conversion fields . . . 30
2.4 Spatial emission distribution of down-conversion photons . . . 32
2.5 Bell state preparation . . . 43
2.5.1 Momentum and energy-time entanglement . . . 43
2.5.2 Polarization entanglement . . . 45

3 Sources of polarization-entangled photon pairs 51

3.1 Photons as information carriers . . . 51
3.1.1 Challenges in quantum communication . . . 52
3.1.2 Quest for high-flux entangled-photon sources . . . 53

3.2 Methods to generate entangled photon pairs . . . 54
3.2.1 SPDC sources . . . 54
3.2.2 Fiber sources . . . 55
3.2.3 Semiconductor sources . . . 56
3.3 Compact non-collinear type-II SPDC source . . . 56
3.3.1 Method . . . 57
3.3.2 Implementation . . . 62
3.3.3 Results . . . 66
3.3.4 Discussion . . . 69
3.4 Compact collinear type-I SPDC source . . . 70
3.4.1 Method . . . 70
3.4.2 Spatial effect . . . 72
3.4.3 Time effect . . . 73
3.4.4 Implementation . . . 82
3.4.5 Results . . . 85
3.4.6 Discussion and outlook . . . 88

4 Single-qubit multiparty quantum communication 91
4.1 Communication complexity . . . 92
4.1.1 Introduction . . . 92
4.1.2 Quantum-assisted communication complexity . . . 92
4.1.3 Communication complexity problems . . . 93
4.1.4 Optimal classical protocol . . . 95
4.1.5 Optimal quantum protocol . . . 97
4.1.6 Implementation . . . 98
4.1.7 Results . . . 100
4.2 Secret sharing . . . 101
4.2.1 Introduction . . . 101
4.2.2 Quantum-assisted secret sharing . . . 102
4.2.3 Entanglement-based protocol . . . 103
4.2.4 Single-qubit protocol . . . 104
4.2.5 Implementation . . . 107
4.2.6 Results . . . 108
4.3 Discussion and outlook . . . 109

5 Conclusions and Outlook 111

Appendices 115

A Sources of polarization-entangled photon pairs 115
A.1 Crystals . . . 115
A.1.1 Beta-barium borate . . . 115

A.1.2 Yttrium vanadate 116
A.2 Historical progress of sources 116
A.3 Photos 118

B Single-qubit multiparty quantum communication 119
B.1 Classical bounds of success probability in communication complexity problems 119
B.2 Photo 121

C Author's publications related to the presented work 123

Bibliography 125

List of figures 137

List of tables 141

Acknowledgments 143

Zusammenfassung

Verschränkte Photonen sind von zentralem Interesse im Bereich experimenteller Quantenphysik. Sie wurden für die ersten fundamentalen Tests der Quantentheorie verwendet und bilden die Grundlage bei der Realisierung vieler neuer Kommunikationsprotokolle die auf quantenmechanischen Effekten basieren, wie zum Beispiel Quantenkryptographie, "dense coding" oder Teleportation. Die effiziente Erzeugung verschränkter Photonen sowie deren genaue Analyse ist folglich von großer Bedeutung, insbesondere im Hinblick auf die Umsetzbarkeit der vielen Quantenkommunikationsanwendungen. Die vorliegende Arbeit behandelt im Wesentlichen das Problem der effizienten Erzeugung von Photon Verschränkung. Das Hauptaugenmerk liegt dabei auf der Entwicklung einer Quelle verschränkter Photonen, die den Anforderungen für einen zuverlässigen und wirtschaftlichen Betrieb in Beispielanwendungen der Quantenkommunikation genügt. Unser Ansatz verwendet die Emission korrelierter Photonen Paare im Prozess der spontanen parametrischen Fluoreszenz. Der Prozess wird mit Licht einer handlichen und billigen blauen Laserdiode gepumpt. Es werden zwei alternative Aufbauten für die Quelle betrachtet. Der erste verwendet das altbewährte Konzept der entarteten nicht-kollinearen Emission in einem einzelnen nichtlinearen Kristall vom Typ II. Der zweite Ansatz basiert auf einer neuen Methode in der die Emission zweier aneinaderliegender, phasenangepasster Kristalle vom Typ I kohärent überlagert wird. Die Phasenanpassung erfolgt dabei im kollinearen nicht-entarteten Zustand. Mit einer Rate von 10^6 Paaren in der Sekunde bei einem Interferenzkontrast der Polarisationskorrelationen von $> 98\,\%$ erwies sich die neue Methode als wesentlich effizienter. Diese Leistungsfähigkeit, in Verbindung mit einem nahezu justagefreien Betrieb, lässt dieses System vielversprechend für zukünftige praktische Anwendungen, wie Quantenkryptographie, Detektorkalibrierung oder Praktikumsversuche für Studenten erscheinen.

Ein weiteres Thema das im Rahmen dieser Arbeit behandelt wird ist die Vereinfachung und Implementierung kommunikationstheoretischer Problemlösungen unter Zuhilfenahme quantenmechanischer Effekte. Während der rasante Fortschritt der letzten Jahre bei der Entwicklung von Quellen zur Erzeugung verschränkter Photonenpaare zu einer großen Anzahl von Veröffentlichungen auf dem Gebiet der Zwei-Parteien-Quantenkommunikation geführt hat, hielt sich die Zahl der Implementierun-

gen von Protokollen mit mehr als zwei Parteien in Grenzen. Dies liegt hauptsächlich daran, dass die benötigten Mehr-Teilchen verschränkten Zustände mit dem heutigen Stand der Technik schwer zu produzieren sind und darüber hinaus hohes Rauschen aufweisen. Wir zeigen, dass Verschränkung nicht die einzige Ressource ist, die Mehrparteien-Quanten-Informationsverarbeitung ihre Stärke verleiht. Im Gegenteil, die sequentielle Kommunikation und Transformation eines einzelnen Qubits kann bereits ausreichend für die Lösung bestimmter Probleme sein. Dies zeigen wir anhand zweier verschiedener informationstheoretischer Problemstellungen, dem "secret sharing" und der Kommunikationskomplexität. Die erste befasst sich mit der Aufteilung eines kryptographischen Schlüssels auf mehrere Parteien in einer Weise, die für dessen Rekonstruktion die Zusammenarbeit aller Parteien erfordert. Die zweite zielt auf die Reduzierung der Kommunikation beim Lösen distributiver Berechnungen ab. Bemerkenswerterweise ist das hier verwendete qubit-basierte Lösungsverfahren mit dem heutigen Stand der Technik umsetzbar, was wir durch dessen Realisierung im Labor für 6 bzw. 5 Personen zeigen. Nach unserem Wissen ist dies die höchste Anzahl an aktiv agierenden Teilnehmern in einem Quantenkommunikationsprotokoll die je implementiert wurde. Die erfolgreiche Lösung und Implementierung von Problemstellungen aus den Bereichen der Kryptographie und der Informatik bringt somit Mehrparteien Quantenkommunikation einen Schritt näher an kommerzielle Anwendungen heran.

Summary

Entangled photons are at the heart of experimental quantum physics. They were used for the first fundamental tests of quantum theory, and became a basic building block for many novel quantum protocols, such as quantum cryptography, dense coding or teleportation. Therefore, the efficient generation of entangled photons, as well as their distribution and accurate analysis are of paramount importance, particularly with regard to the practicability of many applications of quantum communication. This thesis deals largely with the problem of efficient generation of photonic entanglement with the principal aim of developing a bright source of polarization-entangled photon pairs, which meets the requirements for reliable and economic operation of quantum communication prototypes and demonstrators. Our approach uses a correlated photon-pair emission in nonlinear process of spontaneous parametric down-conversion pumped by light coming from a compact and cheap blue laser diode. Two alternative source configurations are examined within the thesis. The first makes use of a well established concept of degenerate non-collinear emission from a single type-II nonlinear crystal and the second relies on a novel method where the emissions from two adjacent type-I phase-matched nonlinear crystals operated in collinear non-degenerate regime are coherently overlapped. The latter approach showed to be more effective, yielding a total detected rate of almost 10^6 pairs/s at $> 98\,\%$ quantum interference visibility of polarization correlations. This performance, together with the almost free of alignment operation of the system, suggest that it is an especially promising candidate for many future practical applications, including quantum cryptography, detector calibration or use in undergraduate lab courses.

The second issue addressed within the thesis is the simplification and practical implementation of quantum-assisted solutions to multiparty communication tasks. While the recent rapid progress in the development of bright entangled photon-pair sources has been followed with ample experimental reports on two-party quantum communication tasks, the practical implementations of tasks for more than two parties have been held back, so far. This is mainly due to the requirement of multiparty entangled states, which are very difficult to be produced with current methods and moreover suffer from a high noise. We show that entanglement is not the only non-classical resource endowing the quantum multiparty information processing its

power. Instead, only the sequential communication and transformation of a single qubit can be sufficient to accomplish certain tasks. This we prove for two distinct communication tasks, secret sharing and communication complexity. Whereas the goal of the first is to split a cryptographic key among several parties in a way that its reconstruction requires their collaboration, the latter aims at reducing the amount of communication during distributed computational tasks. Importantly, our qubit-assisted solutions to the problems are feasible with state-of-the-art technology. This we clearly demonstrate in the laboratory implementation for 6 and 5 parties, respectively, which is to the best of our knowledge the highest number of actively performing parties in a quantum protocol ever implemented. Thus, by successfully solving and implementing a cryptographic task as well as a task originating in computer science, we clearly illustrate the potential to introduce multiparty communication problems into real life.

Acronyms

APD	avalanche photodiode
BBO	beta-barium borate (β-BaB_2O_4)
CCP	communication complexity problem
CW	continuous-wave
CHSH	Clauser-Horne-Shimony-Holt
ECLD	external cavity laser diode
EPR	Einstein-Podolsky-Rosen
FWHM	full width at half maximum
FWM	four-wave mixing
GHZ	Greenberger-Horne-Zeilinger
KLM	Knill-Laflamme-Milburn
KTP	potassium titanyl phosphate ($KTiOPO_4$)
LD	laser diode
MFD	mode field diameter
NIR	near-infrared
PPKTP	periodically poled KTP
QBER	quantum bit error rate
QPM	quasi-phase matching
QSS	quantum secret sharing
SPDC	spontaneous parametric down-conversion
VLPC	visible-light photon counters
WDM	wavelength division multiplexer

Chapter 1

Introduction

1.1 Quantum mechanics

Some discoveries bring answers to questions. Others are so deep, that they cause a radical revolution in our fundamental comprehension of nature. Without any doubt, quantum mechanics has done so.

1.1.1 The underlying principles

From the origin of quantum mechanics at the beginning of twentieth century, scientists struggled to bring its peculiar theoretical frame in accordance with an intuitive view dictated by everyday's experience and common sense. The central tenet of this theory - probabilistic description of physical objects - seriously undermined the dogma of determinism, which was deeply embedded in physical theories over many centuries. In its base the determinism, as distinctly exemplified by Newtonian physics, states that the knowledge of position and momentum of any physical object at one time determines these quantities at all other times, provided, of course, that some other object does not interfere with it. However, in quantum mechanics, the physical objects, such as particles, do not have necessarily well defined positions and momenta. Instead, they are represented by what is called a wave function. It contains all the information we can know about a particle, both its position, and its momentum. The square of the wave function gives the probability that the particle will be found at certain position. The rate, at which the wave function varies from point to point, gives the momentum of the particle.

In 1927 Werner Heisenberg realized one of the major implications of the wave-function description - the uncertainty principle. This principle imposes fundamental limits on a measurement accuracy of two complementary variables, such as position and momentum of a particle. The more precisely the position is determined, the less precisely the momentum is known in this instant, and vice versa. For example, the

wave function with a form of a plane wave, represents a particle with precisely defined momentum, but gives uniform probability of finding particle anywhere in space. On the other hand, a particle whose spatial spread is described by a δ-function is perfectly localized, but there is maximum uncertainty in determination of its momentum. In this way, quantum mechanics introduces its inherent duality: Indeed, we can precisely determine some physical quantities of a physical object, however at the cost of precluding the possibility of ascertaining the other, complementary physical quantities. This concept is in stark contrast with deterministic classical physics, which assumes the precise knowledge of all physical quantities at a given time.

Still, quantum mechanics contains a kind of determinism, but definitely not the one envisaged by Newton. Namely, if a wave function at one time is known, then its evolution to any other time is determined by the so called Schrödinger equation. It allows us to predict future, but somewhat in a "fuzzy" way, when compared to the classical 19^{th} century view.

1.1.2 EPR paradox and Bell's theorem

The success of quantum mechanics in elucidation of known phenomena at atomic-length scales was indisputable. However, the apparent randomness inherent in quantum mechanical description was an eyesore for many physicist, first and foremost for Albert Einstein, who summed up his views in his famous phrase, 'God does not play dice'. He believed there exists an underlying reality, in which all the physical objects have well defined positions and momenta and would evolve according to deterministic laws, in spirit of Newton's classical mechanics. Over the years, he proposed a number of objections to uncover loopholes in the structure of quantum mechanics and to show that its theoretical framework does not say the last word about the function of the universe. His effort culminated by a famous attack on the uncertainty principle, known as EPR paradox, which he devised together with his colleagues Boris Podolsky and Nathan Rosen in 1935 [1]. Their strategy was straightforward: Give a proof that every particle has its certain position and momentum at a given instant, and thereby conclude that the uncertainty principle discloses a fundamental restriction on the quantum-mechanical approach. Simply, if quantum mechanics fails to describe *all* the elements of the reality, such as positions and momenta of particles, it cannot be considered as a complete theory. It cannot be a final link in the chain of physical theories.

Einstein, Podolsky and Rosen were partly inspired in their argumentation by Heisenberg's initial vague explanation of the uncertainty relation: The simultaneous exact determination of position and momentum of a particle cannot be accomplished, because the measurement of one quantity necessarily disturbs the result of the measurement of the other quantity. They cleverly suggested a method how to measure the position and momentum of a particle without disturbing it in any way. The cornerstone of this method is a pair of spatially distant particles (I and II) with perfectly correlated momenta and positions. The wave function of the composed

system (I + II) cannot be written as a product of the wave functions of individual particles. Thus, all the information one can infer about the particles is contained in their mutual correlations and the position or momentum of either particle cannot be predicted, unless a measurement is performed. Such particles later came to be called "entangled", the term introduced by Schrödinger. Now, let's assume the position of "particle I" is measured. By this act, the position of "particle II" is determined, too, due to the existence of tight correlations. Analogously, by measuring the momentum of particle I, the momentum of particle II can be ascertained. Thus, even though we did not disturb particle II in any way[1], its complementary properties can be predicted with certainty. In fact, the EPR paradox does not contradict the uncertainty relation in the first place, because the described measurement procedure does not allow simultaneous determination of the position and momentum of particle II. However, EPR paradox shows that these complementary properties pertaining to particle II do have simultaneous "reality", which was according to Einstein, Podolsky and Rosen sufficient to assert the incompleteness of quantum-mechanical description. The opponents of this interpretation, represented particularly by Niels Bohr, eliminated the raised problem by shifting it to a rather philosophical level. They claimed there is little point to ask whether a particle has defined position and momentum, if they cannot be determined simultaneously. Their conclusion was that any physical theory should deal only with measurable properties of the universe. Since no means seemed to exist to decide which view was right, because the whole issue was essentially an antithetic statement, the question remained open for almost thirty years, until John Bell discovered his famous theorem.

The incompleteness of quantum mechanics concluded from the EPR paradox implies that additional parameters must be supplemented into the description of physical objects, in order to fully account for their properties. These parameters are called hidden and can be considered, in a sense, to provide a program, which predetermines the measurable properties of each particle. Furthermore, they are claimed to be local, since any non-local features were not required to complete quantum-mechanical description according to hidden variables models. In 1964 John Bell proposed a mechanism to test for the existence of these local hidden variables, and proved that entire family of hidden variables models cannot reproduce exactly the quantum-mechanical predictions, forcing us to abandon at least one of the EPR's premises, the reality or locality [2]. He drew this conclusion by investigating the statistical predictions obtained in a simplified version of the EPR experiment, which was proposed by David Bohm [3]. Bohm's version assumes a source emitting pairs of entangled spin-1/2 particles, such as positron-electron pairs, which are freely moving in opposite directions. Two independent observers, each receiving one of the particles, perform measurements of the spin components along a predefined direction using Stern-Gerlach apparatuses. According to the rules of quantum mechanics, the measured spin component can take

[1]Here the locality principle is assumed, i.e., the act of measurement on particle I cannot disturb the other particle (II) due to their sufficient spatial separation.

only two values, for simplicity called spin-up and spin-down[2]. The exact simultaneous determination of spin along more than one direction is forbidden. Thus, in spirit of the original EPR paradox, one may ask a question, whether the spin components along any direction are real, existing quantities, similarly, as it was done before with the position and momentum.

However, Bell extended the idea and studied the experimental scenario, which includes more measurement settings per observer, i.e. the spin of counterpropagating particles is measured along a given set of directions. For example, let's consider the case, where a set containing three directions $(\mathbf{n}_1, \mathbf{n}_2, \mathbf{n}_3)$, perpendicular to the propagation line of particles and separated by 120°, is used. To assure the locality principle the observers are sufficiently separated and they randomly and independently choose the direction to determine spin projection for every measurement run. Assuming the particles are in the singlet state[3], the following two statistical features are predicted by quantum mechanics after repeating the experiment many times: (i) when the same measurement settings are used by the observers, always the anti-correlated, i.e., the opposite results are obtained; (ii) when averaging over all 9 possible combinations of the measurement settings, the observers obtain the anti-correlated results with probability $P_{\mathrm{QM}} = 1/2$, i.e., exactly in half of the runs. To construct a local hidden variable model for the described situation, let's assume that the particles carry for every run a program, which determines the measurement outcomes for all possible settings. For example, the program $(up, down, up)$ means that if the first setting $\mathbf{n}_1$ is chosen, spin-up is measured; for the second setting $\mathbf{n}_2$, spin-down is obtained etc. The statistical feature (i) implies that the entangled particles must carry complementary programs with anti-correlated entries; e.g., for $(up, down, up)$, the complementary program has the form $(down, up, down)$. For this particular example, five combinations of the measurement settings $(\mathbf{n}_1\mathbf{n}_1, \mathbf{n}_2\mathbf{n}_2, \mathbf{n}_3\mathbf{n}_3, \mathbf{n}_1\mathbf{n}_3, \mathbf{n}_3\mathbf{n}_1)$ yield the opposite results and four of them $(\mathbf{n}_1\mathbf{n}_2, \mathbf{n}_2\mathbf{n}_1, \mathbf{n}_2\mathbf{n}_3, \mathbf{n}_3\mathbf{n}_2)$ identical results. Thus, assuming the randomness in choice of measurement settings, each of the cases is equally likely, leading to the probability $P = 5/9$ of obtaining anti-correlated results. Evidently, the same conclusion holds also for all the other programs, which contain two identical entries. The only difference is encountered for the remaining two possible programs, which contain three identical entries, i.e. for (up, up, up) and $(down, down, down)$. For such programs, the results are always anti-correlated for any combination of settings. Thus, the Bell inequality $P > 5/9$ must hold on average, regardless of how the programs are distributed from one measurement run to the other. However, the quantum mechanical prediction violates this inequality, $P_{\mathrm{QM}} = 1/2 \not> 5/9$, leading to a contradiction with the used local hidden variable model. One can show that the considered model is completely general and that there is no other local hidden expla-

[2]The exact values are 1/2 and -1/2. Therefore, electrons are spin-1/2 particles.

[3]The singlet state has a total spin 0 and it is rotationally invariant which means that if we act on both particles with the tensor product of two identical rotations, the resulting state remains unchanged.

nation, which could account for both aforementioned statistical features predicted by quantum mechanics. The presented argument, devised by David Mermin, shows in an intuitive way the nature of Bell's discovery by exemplifying the appropriate local hidden variable model [4].

Interestingly, the conflict between local realism and quantum mechanics exposed by Bell's theorem can be even sharpened using a system of three or more entangled spin-1/2 particles in a so-called Greenberger-Horne-Zeilinger (GHZ) state [5]. For such a system the local realistic model predicts *always* a class of measurement outcomes, which quantum mechanics *never* allows and vice versa. This *always-never* argument against local realism first shown by the GHZ theorem totally eliminates the statistical nature of Bell's theorem and resorts to the requirement of Bell-type inequalities only due to imperfections in practical realizations and finite number of measurement runs.

1.1.3 Clauser-Horne-Shominy-Holt inequality

The most widespread version of Bell's inequality used in experimental tests is the one from Clauser, Horne, Shimony and Holt (hereafter referred to as CHSH) requiring only two measurement settings per observer [6]. Notably, this version was the first, which did not rely upon the assumption of perfect correlations and was therefore perfectly suited for the actual experiments.

Local realistic description. To derive the CSHS-inequality, Bohm's experimental scenario with space-like separated measurements on spin-1/2 particles (I and II) is considered. The measurement results on particles I and II are described using the functions $A(\mathbf{n}_A, \lambda)$ and $B(\mathbf{n}_B, \lambda)$, respectively, with output values ± 1, corresponding to either spin-up or spin-down outcome. To comply with the locality premise, the function A (B) depends only on the orientation of a local Stern-Gerlach measurement apparatus described by a unit vector $\mathbf{n}_A$ ($\mathbf{n}_B$). Moreover, a parameter (or a set of parameters) λ predetermining the measurement outcomes has to be included into the description according to a hidden variable concept. Introducing two alternative orientations $\mathbf{n}'_A$ and $\mathbf{n}'_B$, the following equality holds for any measurement run,

$$[A(\mathbf{n}_A, \lambda) + A(\mathbf{n}'_A, \lambda)]\, B(\mathbf{n}_B, \lambda) + [A(\mathbf{n}_A, \lambda) - A(\mathbf{n}'_A, \lambda)]\, B(\mathbf{n}'_B, \lambda) = \pm 2, \qquad (1.1)$$

since the functions A and B are two-valued; either $[A(\mathbf{n}_A, \lambda) + A(\mathbf{n}'_A, \lambda)] = 0$ and $[A(\mathbf{n}_A, \lambda) - A(\mathbf{n}'_A, \lambda)] = \pm 2$, or $[A(\mathbf{n}_A, \lambda) + A(\mathbf{n}'_A, \lambda)] = \pm 2$ and $[A(\mathbf{n}_A, \lambda) - A(\mathbf{n}'_A, \lambda)] = 0$. Thus, for the average over a statistical ensemble of measurement runs we obtain

$$|\langle A(\mathbf{n}_A) B(\mathbf{n}_B)\rangle + \langle A(\mathbf{n}'_A) B(\mathbf{n}_B)\rangle + \langle A(\mathbf{n}_A) B(\mathbf{n}'_B)\rangle - \langle A(\mathbf{n}'_A) B(\mathbf{n}'_B)\rangle| \leq 2. \qquad (1.2)$$

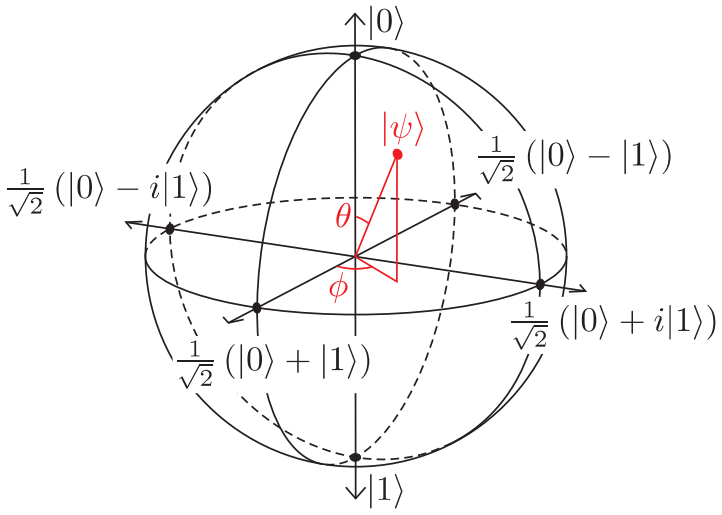

Figure 1.1: Bloch sphere. Any point on the sphere defined by the spherical angles θ and ϕ represents a corresponding spin-1/2 state $|\psi\rangle$.

This is known as the CHSH inequality, giving an upper bound on the correlations between measurement results under the assumption of local realism.

Quantum violation. Quantum mechanics allows to directly calculate the correlation functions in the inequality (1.2). For that, we start with a singlet state:

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_{\rm I}|1\rangle_{\rm II} - |1\rangle_{1}|0\rangle_{\rm II}\right), \tag{1.3}$$

where $|0\rangle$ and $|1\rangle$ represent two orthogonal states of particles I and II, corresponding to two possible spin projections onto an arbitrary direction $\mathbf{n}$; e.g. "0" corresponds to spin-up and "1" to spin-down. The measurement on either particle is represented by the projector operator $\hat{P}(\theta,\phi) = |\psi(\theta,\phi)\rangle\langle\psi(\theta,\phi)|$, where

$$|\psi(\theta,\phi)\rangle = \cos(\theta/2)|0\rangle + \mathrm{e}^{i\phi}\sin(\theta/2)|1\rangle. \tag{1.4}$$

This qubit parametrization assigns each point on a Bloch sphere to a unique pure quantum state, see figure 1.1.

The maximum violation of the CHSH inequality (1.2) occurs for such set of orientations $\{\mathbf{n}_A, \mathbf{n}'_A, \mathbf{n}_B, \mathbf{n}'_B\}$, which obeys the following conditions: angles $\measuredangle(\mathbf{n}_A\mathbf{n}_B) = \measuredangle(\mathbf{n}_B\mathbf{n}'_A) = \measuredangle(\mathbf{n}'_A\mathbf{n}'_B)$ equal $\pi/4$ and the angle $\measuredangle(\mathbf{n}_A\mathbf{n}'_B)$ equals $3\pi/4$. These orientations correspond to the projector operators $\{\hat{P}_A, \hat{P}'_A, \hat{P}_B, \hat{P}'_B\}$, defined as, e.g., $\hat{P}_A = \hat{P}(0,0), \hat{P}'_A = \hat{P}(\pi/2,0), \hat{P}_B = \hat{P}(\pi/4,0)$ and $\hat{P}'_B = \hat{P}(3\pi/4,0)$. Given these forms of observables, the following expectation values can be easily calculated:

$$\langle\Psi^-|\hat{P}_A\hat{P}_B|\Psi^-\rangle = \langle\Psi^-|\hat{P}'_A\hat{P}_B|\Psi^-\rangle = \langle\Psi^-|\hat{P}'_A\hat{P}'_B|\Psi^-\rangle = -\langle\Psi^-|\hat{P}_A\hat{P}'_B|\Psi^-\rangle = \cos(\pi/4). \tag{1.5}$$

Assuming that the above operators reveal in turn the values of the dichotomic func-

tions A and B in (1.2), their substitution can be done,

$$\begin{aligned}&\left|\langle\Psi^-|\hat{P}_A\hat{P}_B|\Psi^-\rangle + \langle\Psi^-|\hat{P}'_A\hat{P}_B|\Psi^-\rangle + \langle\Psi^-|\hat{P}'_A\hat{P}'_B|\Psi^-\rangle - \langle\Psi^-|\hat{P}_A\hat{P}'_B|\Psi^-\rangle\right| \\ &= 4\cos(\pi/4) = 2\sqrt{2} > 2,\end{aligned} \tag{1.6}$$

obtaining the Cirel'son's upper limit on the violation of CHSH inequality [7]. There are three other states leading to the maximal violation:

$$|\Phi^-\rangle = (\mathbb{1}\otimes\hat{\sigma}_x)|\Psi^-\rangle, \quad |\Phi^+\rangle = (\mathbb{1}\otimes i\hat{\sigma}_y)|\Psi^-\rangle, \quad |\Psi^+\rangle = (\mathbb{1}\otimes\hat{\sigma}_z)|\Psi^-\rangle, \tag{1.7}$$

where $\mathbb{1}$ is the identity matrix and

$$\hat{\sigma}_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \hat{\sigma}_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \hat{\sigma}_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{1.8}$$

are well-known Pauli matrices. The three states defined in Eq. (1.7) together with $|\Psi^-\rangle$ form an orthonormal basis to four-dimensional Hilbert space of two qubits and are usually referred to as Bell states.

Experimental tests. Prompted by the derivation of the CHSH inequality, a first series of tests using polarization-entangled photon pairs emitted in an atomic cascade transition were performed in the early 1970s [8, 9], clearly corroborating the quantum predictions. Yet, the local realistic explanation of the obtained results remained at least logically possible, because of the existence of two loopholes arising from the imperfections of the experimental tests.

The first loophole occurs, whenever the communication of the measurement setting from one observer to the other cannot be excluded before completing the actual measurement process. This opens the possibility of establishing the correlations between remote measurement processes, thereby allowing local hidden variable interpretation of the obtained results. The first experiment addressing the locality loophole by Aspect *et al.* [10] employed fast quasi-periodic modulators to select the settings of polarization analyzers only after the entangled photons left the source. This remarkable experiment was further refined in the test of Weihs *et al.* [11], where strict locality conditions were enforced by using fast, random switching of the analyzers that were separated by about 400 meters.

This left only the second loophole, so called detection-efficiency or fair-sampling loophole, open. It arises whenever the detection of particles is inefficient enough so that the detected events may be unrepresentative of the whole ensemble. Even though a significant progress in the area of semiconductor detectors has been made during the last decade, and single-photon detection with close to perfect quantum efficiency has been reported [12], no photonic Bell test eliminating the fair-sampling hypothesis has been presented until now, due to other experimental difficulties. The only Bell test successful in this respect was performed with a pair of entangled beryllium ions

[13]. Regrettably, the actual separation of the ions by a distance of about 3 μm gives no foreseeable chance to close the locality loophole with that system.

Hence, after almost 50 years since Bell's discovery, one must still face the situation that no conclusive experimental test ruling out the local realistic description of nature has been accomplished. The present challenge is to design and perform such an experiment, closing both loopholes at the same time.

1.2 Quantum information processing and communication

Apart from the fundamental motivations, quantum superposition and quantum entanglement are the bedrock on which new paradigms for information transmission, storage, and processing can be built. Current developments eloquently demonstrate that these characteristic quantum phenomena may enable one to perform some tasks of practical interest beyond the capabilities of any other known (classical) method. The preeminent examples of such tasks are quantum cryptography, offering new methods for secure communication with its inviolability ensured by the laws of quantum physics [14, 15]; quantum dense coding, allowing to enhance the capacity of a communication channel [16]; or quantum teleportation, the remote transmission and reconstruction of the state of a quantum system [17]. In the field of quantum computation, novel procedures, as often exemplified by Shor's algorithm to factorize large numbers [18] and Grover's algorithm for searching data bases [19], were shown to lead to a dramatic speed-up over any (known) classical computation.

All these discoveries initiated a worldwide search for new technologies to realize quantum communication and computation systems. The early experiments have highlighted how difficult it will be to build working prototypes, by identifying decoherence in quantum systems as a key issue in practical implementations. In quantum communication the major challenge lies in the error-free transmission of quantum information over noisy and lossy communication channels, followed by efficient recovering of the encoded information. In quantum computation main difficulties stem from the requirement of strong coupling between quantum bits by gates, while at the same time their complete decoupling from external influences, except during write, control and readout the phases when information must flow in and out of the computer.

1.3 Overview

This thesis predominantly focuses on the field of quantum communication. Therein, an impressive progress has been achieved since the entry into the experimental era marked by the first demonstration of single-photon quantum cryptography over the distance of 32 cm in 1989 [20]. Many novel concepts, protocols and methods have been

demonstrated practically, some even outside the ideal lab environment. Nevertheless, there is still a long way to go - the practicality of the systems must be improved, higher bit rates and longer distances must be achieved before any meaningful successes can be claimed. The work presented here contributes to these lines of research by addressing two particular issues.

First, the topic of efficient and practical generation of entangled photon pairs via spontaneous parametric down-conversion (SPDC) is addressed within the thesis. The chapter 2 is intended to cover the theoretical aspects associated with the problem. It brings the detailed theoretical description of the SPDC process and reviews the most common methods of preparation of the emitted photon pairs in maximally-entangled Bell states encoded in different accessible degrees of freedom. Particular attention is devoted to polarization encoding. The subsequent chapter 3 gives the details about the actual design and practical realization of two different compact sources using a blue laser diode as the pump of SPDC. The major parameters of the sources and their output performance are compared to other state-of-the-art implementations.

Second, the chapter 4 deals with two apparently different communication tasks, the secret sharing and the communication complexity. Whereas the goal of the first is to distribute a cryptographic key among several parties in a way that its reconstruction requires the collaboration of the parties, the latter aims at reducing the amount of communication during distributed computation. In common, both tasks were shown to be efficiently solvable via the resource of multi-partite entanglement. This is, however, very difficult to be produced in practice, making the implementation of the tasks technologically very challenging. We show that the quantum-assisted solution to both tasks can be significantly simplified via novel protocols based on sequential communication and transformation of single qubits. This makes the tasks feasible with current experimental methods and above all, scalable in practical applications. These benefits are clearly demonstrated in the proof-of-principle implementations of the tasks described at the end of the chapter.

Chapter 2

Spontaneous parametric down-conversion

In this chapter the theoretical model of spontaneous parametric down-conversion is reviewed, putting a particular emphasis on the analysis of spectral and spatiotemporal characteristics of down-conversion light. In addition, the basic methods for preparation of the emitted photon-pairs in maximally entangled Bell states encoded in the polarization degree of freedom are discussed here.

Parametric processes are widely used in nonlinear optics. In the field of quantum optics they are applied for the generation of quantum fields having no classical analogue. Spontaneous parametric down-conversion is probably the best known example of a simply realizable parametric process manifesting an inherent quantum-mechanical nature of electromagnetic fields. It was first investigated theoretically by Klyshko in late 1960s [21] and experimentally by Burnham and Weinberg few years later [22]. Their pioneering work was followed by a wealth of studies paying a particular attention to nonclassical photon-number statistics [23] and correlation effects of down-conversion fields [24]. Moreover, due to a strong time correlation of the generated fields [25] and output powers in sub-picowatt range, the first applications in the field of metrology were recognized soon [26].

In the SPDC process photons from an intense laser beam interact with a dielectric medium, and split into two lower-frequency photons. This process is forbidden in vacuum by the rules of quantum electrodynamics, but can occur with a small probability in nonlinear crystals having non-zero second-order susceptibility $\chi^{(2)}$, provided that energy and momentum conservation is respected. In the following, the physics of nonlinear $\chi^{(2)}$ media is briefly reviewed.

2.1 Nonlinearity and anisotropy of a dielectric

The presence of electromagnetic fields in a dielectric causes a polarization of the medium. The polarization [dipole moment per unit volume; $P(t)$] induced in the medium can be expanded in power series of instantaneous electric field $E(t)$ [27]:

$$P = \epsilon_0 \left(\chi^{(1)} E + \chi^{(2)} E^2 + \chi^{(3)} E^3 + \ldots \right), \tag{2.1}$$

where $\chi^{(n)}$ are nonlinear dielectric susceptibility coefficients and ϵ_0 is permittivity of vacuum. Under most conditions, the quadratic and higher-order terms can be neglected in the expansion (2.1), which means that the response of the medium to the applied field is linear (linear optics). Nevertheless, for some materials and sufficiently high intensities of the electric field, the quadratic or cubic polarization become significant and the response is nonlinear. Due to the fact that SPDC is a second-order nonlinear process, the series (2.1) can be truncated after the second term for our purposes and the cubic nonlinearity will not be considered any longer.

Suppose, the electric field $E(t) = A\cos(\omega t)$ pumps a medium with nonzero quadratic nonlinearity. Then its response can be written as

$$P(t) = \epsilon_0 \chi^{(1)} A \cos(\omega t) + \frac{1}{2} \epsilon_0 \chi^{(2)} A^2 \big[1 + \cos(2\omega t) \big]. \tag{2.2}$$

The polarization of the medium contains, additionally to the frequency ω of the incident light, a component oscillating at the second harmonic frequency. Dividing the polarization P into its linear $P^{\mathrm{L}} = \epsilon_0 \chi^{(1)} A \cos(\omega t)$ and nonlinear part $P^{\mathrm{NL}} = \frac{1}{2} \epsilon_0 \chi^{(2)} A^2 [1 + \cos(2\omega t)]$, the propagation of electromagnetic fields in a nonlinear medium is described by the wave equation:

$$\nabla^2 E - \frac{1}{c^2} \frac{\partial^2 E}{\partial t^2} = -\mathcal{S} \tag{2.3}$$

$$\mathcal{S} = -\mu_0 \frac{\partial^2 P^{\mathrm{NL}}}{\partial t^2}, \tag{2.4}$$

where c and μ_0 are the speed of light in vacuum and permeability of vacuum, respectively. The function $\mathcal{S}$ represents a source emitting the electromagnetic field: whenever $\frac{\partial^2 P^{\mathrm{NL}}}{\partial t^2}$ is nonzero, charges in the medium are being accelerated, which, according to Larmor's theorem from electromagnetism, leads to generation of electromagnetic radiation. Due to the fact that $\mathcal{S}$ contains a component with frequency 2ω, an electromagnetic field at this frequency is emitted from the medium. Thus, a portion of the incident field is converted to the output at the second harmonic frequency. Thereof, this process is called second harmonic generation.

The SPDC process can, in a sense, be considered as the inverse of second harmonic generation. Whereas in the latter case two incident photons generate one photon at the double frequency, in down-conversion one photon incident on the medium with

nonzero $\chi^{(2)}$ decays into two lower-frequency photons [28], which are for historical reasons often called the signal photon and the idler photon. Denoting the angular frequencies of the interacting fields as ω_p, ω_s and ω_i (pump, signal and idler field, respectively), the energy conservation must hold:

$$\omega_\mathrm{p} = \omega_\mathrm{s} + \omega_\mathrm{i}. \tag{2.5}$$

This condition is not the only, which has to be fulfilled for SPDC to occur. This is due to the fact that the optical materials are dispersive causing the relative drift between the interacting fields. As a result the fields will not be generally in phase over a substantial space region: the signal and idler fields created at one place in a nonlinear medium will interfere destructively with fields created at another place so that no conversion occurs whatsoever. Therefore, the fields have to be phase-matched, which can be expressed by the condition:

$$\boldsymbol{k}_\mathrm{p} = \boldsymbol{k}_\mathrm{s} + \boldsymbol{k}_\mathrm{i}, \tag{2.6}$$

where $\boldsymbol{k}_m$ are the wave vectors of the waves with frequencies ω_m ($m = \mathrm{p}, \mathrm{s}, \mathrm{i}$) and

$$k_m = |\boldsymbol{k}_m| = \frac{\omega_m n_m}{c}. \tag{2.7}$$

Here, the quantities $n_m = n(\omega_m)$ are the refractive indices of the three interacting waves.

In reality, it is often very difficult to fulfill the conditions (2.5) and (2.6). Most materials are normally dispersive, which means that their refractive index is a monotonic increasing function of frequency. Assuming that $\omega_\mathrm{i} \leq \omega_\mathrm{s} \leq \omega_\mathrm{p}$, the effect of normal dispersion implies that $n_\mathrm{i} \leq n_\mathrm{s} \leq n_\mathrm{p}$. As a result, for the collinear geometry of SPDC, where the wave vectors of the interacting fields have the same direction, the condition for perfect phase matching (2.6), rewritten now into the form

$$n_\mathrm{p}\omega_\mathrm{p} = n_\mathrm{s}\omega_\mathrm{s} + n_\mathrm{i}\omega_\mathrm{i}, \tag{2.8}$$

cannot be achieved in normally dispersive materials. To show this the following expressions can be derived with the use of Eqs. (2.5) and (2.8):

$$n_\mathrm{p} - n_\mathrm{s} = \frac{n_\mathrm{s}\omega_\mathrm{s} + n_\mathrm{i}\omega_\mathrm{i}}{\omega_\mathrm{p}} - n_\mathrm{s} = \frac{n_\mathrm{s}(\omega_\mathrm{s} - \omega_\mathrm{p}) + n_\mathrm{i}\omega_\mathrm{i}}{\omega_\mathrm{p}} = (n_\mathrm{i} - n_\mathrm{s})\frac{\omega_\mathrm{i}}{\omega_\mathrm{p}}. \tag{2.9}$$

In the case of normal dispersion, the inequalities $(n_\mathrm{p} - n_\mathrm{s}) > 0$ and $(n_\mathrm{i} - n_\mathrm{s}) < 0$ must hold, and therefore Eq. (2.9) cannot have any solution. The same conclusion can be inferred also for the general case of non-collinear SPDC.

In principle, the phase-matching condition (2.8) can be fulfilled in anomalously dispersive dielectrics, for which the refractive index decreases with increasing frequency near the absorption bands. Nevertheless, this method is only rarely used

in practice because of a high energy absorption. The most common procedure for achieving perfect phase matching is to make use of the birefringence in anisotropic crystals.

In anisotropic crystals, each of the components of the polarization vector $\boldsymbol{P} = (P_1, P_2, P_3)$ is a linear combination of three components of the electric field $\boldsymbol{E} = (E_1, E_2, E_3)$. Assuming that cubic and higher-order nonlinearities vanish, the material equation for isotropic materials (2.1) is rewritten into the form [27]:

$$P_i = \epsilon_0 \sum_j \chi^{(1)}_{ij} E_j + \epsilon_0 \sum_{jk} \chi^{(2)}_{ijk} E_j E_k, \quad (i,j,k) = 1,2,3. \tag{2.10}$$

Here, $\chi^{(1)}_{ij}$ and $\chi^{(2)}_{ijk}$ are the elements of the susceptibility tensors $\boldsymbol{\chi}^{(1)}$ and $\boldsymbol{\chi}^{(2)}$, which correspond to the scalar coefficients $\chi^{(1)}$ and $\chi^{(2)}$ from Eq. (2.1). It can be shown that $\chi^{(1)}_{ij} = \chi^{(1)}_{ji}$ and $\chi^{(2)}_{ijk} = \chi^{(2)}_{ikj}$, i.e., the susceptibility tensors, are symmetric. Consequently, by choosing the appropriate set of coordinate axes, known as principal axes of the medium and denoted here as X, Y and Z, the tensor $\boldsymbol{\chi}^{(1)}$ can be diagonalised, zeroing all the tensor components except $\chi^{(1)}_{11}, \chi^{(1)}_{22}$ and $\chi^{(1)}_{33}$. Furthermore, an alternative notation, d_{ab}, can be used for the elements of quadratic susceptibility $\chi^{(2)}_{ijk}$, where $a = i$ and b varies from 1 to 6 to represent jk values of $11, 22, 33, 23(32), 13(31), 12(21)$[1].

Due to the fact that the linear susceptibility $\boldsymbol{\chi}^{(1)}$ is a tensor, the refractive index $\boldsymbol{n}$ of an anisotropic crystal must be a tensor as well. In the principal coordinate system, the three non-vanishing elements of $\boldsymbol{n}$ can be determined according to the relation:

$$n_i = \left(1 + \chi^{(1)}_{ii}\right)^{1/2}, \tag{2.11}$$

where $i = 1, 2, 3$ represent the axes X, Y and Z of the coordinate system, respectively. In general, $n_1 \neq n_2 \neq n_3$, and the crystals are known as biaxial. Nevertheless, in crystals of certain structures (trigonal, tetragonal and hexagonal), two of the refractive indices are equal, $n_o = n_1 = n_2$, whereas the third is different $n_e = n_3 \neq n_o$. These crystals are uniaxial and the refractive indices n_o and n_e are called ordinary and extraordinary, respectively. If $n_e > n_o$, the crystal is said to be positive; if $n_e < n_o$, it is said to be negative. The difference between the refractive indices, $\Delta n = |n_e - n_o|$, is known as birefringence. For the sake of simplicity, the following description is restricted to uniaxial crystals, but it can be easily extended to the case of biaxial crystals.

In uniaxial crystals an unique direction exists, called the optic axis[2]. Light polarized perpendicular to the plane containing the wave vector $\boldsymbol{k}$ and the optic axis experiences the ordinary refractive index n_o, and therefore it is referred to as ordinary polarized. Light polarized in the plane containing $\boldsymbol{k}$ and the optic axis experiences the extraordinary refractive index n_e; therefore, it is said to be extraordinary polarized.

[1] Usually, d_{ab} is introduced with an extra factor 2 so that $\boldsymbol{d}$ is half of $\boldsymbol{\chi}^{(2)}$: $2d_{ab} = \chi^{(2)}_{ijk}$.

[2] The optic axis coincides with Z axis of the principal coordinate system.

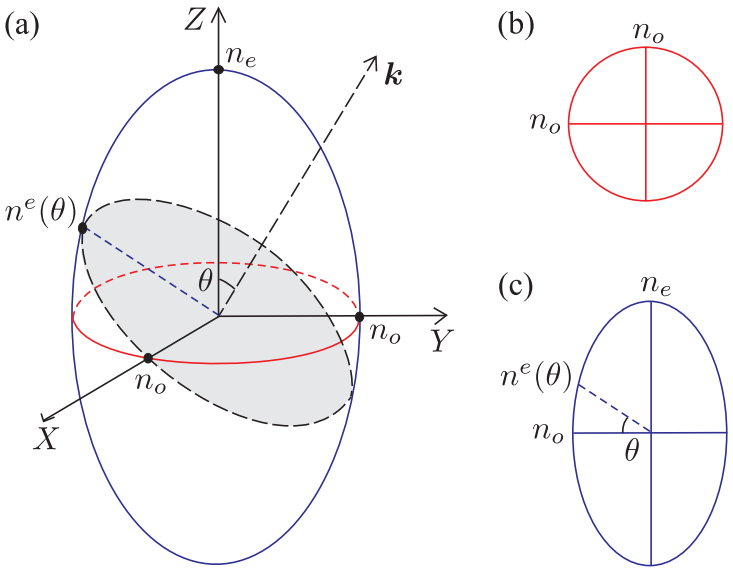

Figure 2.1: Index ellipsoid, the geometrical representation of the orientation and relative magnitude of refractive indices in an anisotropic crystal [29]. (a) In uniaxial crystals the ellipsoid is rotationally symmetric around the optic axis Z. For light propagating under any angle θ with regard to optic axis, we can plot the index ellipse (shaded ellipse), whose semi-minor and semi-major axes define the values n_o and $n^e(\theta)$. (b) Due to rotational symmetry of ellipsoid, one of the semi-axes of the index ellipse always lies in the circular section perpendicular to optic axis, defining the value n_o of ordinary polarized light. (c) The semi-axis of the index ellipse defining the value $n^e(\theta)$ lies in the plane, which contains the optic axis and the wave vector $\boldsymbol{k}$. This plane cuts from the ellipsoid an ellipse. The relation for $n^e(\theta)$ (2.13) is thus given by an equation of ellipse.

The refractive index of the ordinary polarized light does not depend on the propagation direction, whereas for the extraordinary polarized light it does; $n^e = n^e(\theta)$, where θ is the angle between optic axis and vector $\boldsymbol{k}$[3]. This can be illustrated using the geometrical construction called index ellipsoid (or optical indicatrix), which is for uniaxial crystals defined as

$$\frac{x^2 + y^2}{n_o^2} + \frac{z^2}{n_e^2} = 1. \tag{2.12}$$

The index ellipsoid has a rotational symmetry around the optical axis, see Fig. 2.1. To determine the refractive indices, the plane intersecting the ellipsoid center and perpendicular to wave vector $\boldsymbol{k}$ is considered, cutting the ellipsoid in so-called index ellipse. Due to rotational symmetry of ellipsoid, one of the semi-axes of index ellipse always defines the value n_o, which is independent of the direction $\boldsymbol{k}$. The other semi-axis then defines the value $n^e(\theta)$, which can be determined according to the

[3]To avoid confusion with the principal value of the extraordinary refractive index n_e, index e is in this case written as a superscript.

	Positive uniaxial ($n_e > n_o$)	Negative uniaxial ($n_e < n_o$)
Type I	$n_{\mathrm{p}}^o\omega_{\mathrm{p}} = n_{\mathrm{s}}^e\omega_{\mathrm{s}} + n_{\mathrm{i}}^e\omega_{\mathrm{i}}$	$n_{\mathrm{p}}^e\omega_{\mathrm{p}} = n_{\mathrm{s}}^o\omega_{\mathrm{s}} + n_{\mathrm{i}}^o\omega_{\mathrm{i}}$
Type II	$n_{\mathrm{p}}^o\omega_{\mathrm{p}} = n_{\mathrm{s}}^o\omega_{\mathrm{s}} + n_{\mathrm{i}}^e\omega_{\mathrm{i}}$	$n_{\mathrm{p}}^e\omega_{\mathrm{p}} = n_{\mathrm{s}}^o\omega_{\mathrm{s}} + n_{\mathrm{i}}^e\omega_{\mathrm{i}}$

Table 2.1: Phase-matching schemes for uniaxial crystals. No assumptions regarding the relative magnitudes of ω_{s} and ω_{i} are considered in the classification.

relation:

$$\frac{1}{n^e(\theta)^2} = \frac{\sin^2\theta}{n_e^2} + \frac{\cos^2\theta}{n_o^2}. \tag{2.13}$$

Note that $n^e(\theta)$ is equal to the principal value n_e for $\theta = \pi/2$ and is equal to n_o for $\theta = 0$. In practice, the principal refractive indices n_o and n_e are obtained from an empirical relation, known as Sellmeier formula:

$$n_{o,e}^2(\lambda) = A_{o,e} + B_{o,e}/(\lambda^2 - C_{o,e}) + E_{o,e}\lambda^2, \tag{2.14}$$

which specifies the dispersion properties of a certain material for ordinary and extraordinary polarization. The coefficients A, B, C and E are determined experimentally from spectrometric measurements and can be found for most materials in the literature, for example in [30].

In order to achieve phase matching in SPDC, the pump photon has to be polarized in the direction that corresponds to the lower value of the two possible refractive indices [27]. For example, in the case of negative uniaxial crystals, this polarization must be extraordinary. Furthermore, at least one of the lower-frequency photons has to be orthogonally polarized with regard to the pump photon. Two alternatives in the choice of the polarizations of lower-frequency photons arise, referred to as type I and type II phase matching. Whereas, in the first phase matching scheme the signal and idler photons have the same polarization (ordinary or extraordinary), in the latter case their polarizations are orthogonal. All the possibilities are summarized in Table 2.1. For most uniaxial crystals, type I phase matching can be achieved over a broad spectral range; type II phase matching is in general more difficult to achieve. A fine control over refractive indices of the interacting waves is required to drive the SPDC process into perfect phase matching condition $\Delta k = k_{\mathrm{p}} - k_{\mathrm{s}} - k_{\mathrm{i}} = 0$. In practice, the most common technique is angle tuning. It involves a precise adjustment of the angle θ to achieve the desired refractive index/indices $n^e(\theta)$ of the interacting extraordinary polarized wave/waves such that the condition $\Delta k = 0$ is achieved. For some crystals, notably lithium niobate, the amount of birefringence is strongly temperature dependent, allowing the efficient temperature tuning of phase matching.

2.2 Simple theoretical model

The simplest theoretical model of SPDC assumes the coupling of three discrete modes of field oscillations[4]. Even though this model is a rough simplification, and a more adequate treatment including multimode description of interacting fields has to be applied (see the next section 2.3), it allows us to readily calculate basic scaling rules of conversion efficiency and deduce some interesting aspects associated with SPDC.

The dynamics of the mode coupling is described by the time-dependent nonlinear interaction Hamiltonian of the form [31]:

$$\hat{H}_I(t) = \int P_i^{\mathrm{NL}} E_i \mathrm{d}^3 r = \epsilon_0 \int \chi_{ijk}^{(2)} E_i E_j E_k \mathrm{d}^3 r, \tag{2.15}$$

where P_i^{NL} is the nonlinear part of dielectric polarization from Eq. (2.10), and summation on repeated indices is understood. The interacting modes in SPDC must be expressed in the quantized forms in terms of the annihilation $\hat{a}$ and creation $\hat{a}^\dagger$ operators, which obey well-known bosonic commutation relations:

$$\left[\hat{a}_m, \hat{a}_{m'}^\dagger\right] = \delta_{mm'}, \ \left[\hat{a}_m, \hat{a}_{m'}\right] = \left[\hat{a}_m^\dagger, \hat{a}_{m'}^\dagger\right] = 0, \tag{2.16}$$

where m and m' are the mode indices. Consequently, the complex-valued electric fields $\boldsymbol{E}$ in (2.15) are transmuted into field operators $\hat{\boldsymbol{E}}$. In the most elementary form that takes into account only one possible polarization direction and propagation along the z axis, the electric-field operator is expressed as [32],

$$\hat{E}(z,t) = E_0 \left(\hat{a} e^{i(kz-\omega t)} + \hat{a}^\dagger e^{-i(kz-\omega t)}\right), \tag{2.17}$$

where E_0 is a parameter containing all the prefactors emerging from the field quantization. The first term in relation (2.17) corresponds to the positive-frequency part of the field $\hat{E}^{(+)}(z,t)$, which is associated with photon absorption, whereas the second corresponds to the negative-frequency part $\hat{E}^{(-)}(z,t)$, associated with photon emission. Under the assumption of a given phase matching configuration, and considering that Es in (2.15) formally represent the pump-, signal- and idler-mode operators, the interaction Hamiltonian becomes:

$$\begin{aligned}
\hat{H}_I(t) &= 2\epsilon_0 d_{\mathrm{eff}} \int_{-\infty}^{\infty} \delta(z-z') \hat{E}_{\mathrm{p}}^{(+)}(z,t) \hat{E}_{\mathrm{s}}^{(-)}(z,t) \hat{E}_{\mathrm{i}}^{(-)}(z,t)\, \mathrm{d}z + \mathrm{h.c.} \\
&= 2\epsilon_0 d_{\mathrm{eff}} E_{0\mathrm{p}} E_{0\mathrm{s}} E_{0\mathrm{i}} \int_{-\infty}^{\infty} \delta(z-z') e^{i\Delta k z} \mathrm{d}z\, \hat{a}_{\mathrm{p}} \hat{a}_{\mathrm{s}}^\dagger \hat{a}_{\mathrm{i}}^\dagger e^{-i(\overbrace{\omega_{\mathrm{p}} - \omega_{\mathrm{s}} - \omega_{\mathrm{i}}}^{0})t} \\
&\quad + \mathrm{h.c.},
\end{aligned} \tag{2.18}$$

[4]In principle, this situation could be physically realized by the requirements of phase matching for three modes in a cavity.

where d_{eff} is an effective nonlinearity, which can be determined from the tensor $\boldsymbol{d}$ [see definition in the paragraph below Eq. (2.10)] assuming a certain crystallographic structure of the nonlinear medium [30].

The description of the mode coupling using interaction Hamiltonian (2.18) accounts for an effect of pump depletion, due to the quantized form of this field. However, under standard experimental conditions this effect is negligible, because the incident pump field is intense and conversion efficiency in SPDC is very low. The latter can be inferred from closer inspection of the relative magnitudes between the linear and the nonlinear term in the expansion of the dielectric polarization:

$$\frac{\left|\boldsymbol{P}^{\text{NL}}\right|}{\left|\boldsymbol{P}^{\text{L}}\right|} = \frac{2d_{\text{eff}}|E_{\text{s(i)}}|}{n^2-1}, \tag{2.19}$$

where $|E_{\text{s(i)}}|$ represents the strength of the signal (or idler) mode, which emerges as amplification of vacuum fluctuations; $|E_{\text{s(i)}}| \ll 1$ V/m. Assuming the realistic magnitudes of the other quantities, $d_{\text{eff}} \approx 10^{-12}$ m/V, $n^2 \approx 1$–10, this ratio is close to zero, corresponding to the spontaneous nature of SPDC. Therefore, to a good approximation, we can treat the pump mode $\hat{a}_{\text{p}}$ classically as a complex-valued field of a constant amplitude a_{p}.

The total Hamiltonian consists of the term $\hat{H}_0$ describing the energy of a free two-mode field and the interaction term $\hat{H}_I$ from Eq. (2.18) [31]:

$$\hat{H} = \hat{H}_0 + \hat{H}_I = \sum_{m=\text{s,i}} \hbar\omega_m \left(\hat{a}_m\hat{a}_m^\dagger + \frac{1}{2}\right) + \hbar g\left(\hat{a}_{\text{i}}^\dagger\hat{a}_{\text{s}}^\dagger a_{\text{p}} + \text{h.c.}\right), \tag{2.20}$$

where g is the mode coupling parameter describing the strength of nonlinear interaction. It is proportional to the effective nonlinearity d_{eff} and to a factor $e^{i\Delta ktc}$, where we put $t = z'/c$. In Heisenberg representation the time evolution of the field operators is described by the coupled equations of motions [31]:

$$\frac{\mathrm{d}\hat{a}_{\text{s}}}{\mathrm{d}t} = \frac{1}{i\hbar}\left[\hat{a}_{\text{s}}, \hat{H}\right] = -i\omega_{\text{s}}\hat{a}_{\text{s}} - ig\hat{a}_{\text{i}}^\dagger a_{\text{p}}, \tag{2.21a}$$

$$\frac{\mathrm{d}\hat{a}_{\text{i}}}{\mathrm{d}t} = \frac{1}{i\hbar}\left[\hat{a}_{\text{i}}, \hat{H}\right] = -i\omega_{\text{i}}\hat{a}_{\text{i}} - ig\hat{a}_{\text{s}}^\dagger a_{\text{p}}, \tag{2.21b}$$

and their Hermitian conjugates. Note that these equations are identical to equations derived for a classical parametric amplifier, see e.g. [29], provided that the annihilation and creation operators are identified with classical mode amplitudes and their complex conjugates, respectively. Making use of commutation rules (2.16), it follows directly from Eqs. (2.21):

$$\frac{\mathrm{d}}{\mathrm{d}t}\hat{a}_{\text{s}}^\dagger\hat{a}_{\text{s}} = \frac{\mathrm{d}}{\mathrm{d}t}\hat{a}_{\text{i}}^\dagger\hat{a}_{\text{i}}, \tag{2.22}$$

which is equivalent to the commutation relations:

$$\left[\hat{a}_{\mathrm{s}}^{\dagger}\hat{a}_{\mathrm{s}}, \hat{H}\right] = \left[\hat{a}_{\mathrm{i}}^{\dagger}\hat{a}_{\mathrm{i}}, \hat{H}\right], \tag{2.23}$$

so that $\hat{a}_{\mathrm{s}}^{\dagger}\hat{a}_{\mathrm{s}} - \hat{a}_{\mathrm{i}}^{\dagger}\hat{a}_{\mathrm{i}}$ is a constant of motion. Recalling the definition of the number operator $\hat{n}$ [32]:

$$\hat{a}^{\dagger}\hat{a}|n\rangle = \hat{n}|n\rangle = n|n\rangle, \tag{2.24}$$

where n is the number of quanta in a mode and $|n\rangle$ is the corresponding eigenstate, we can finally write:

$$\hat{n}_{\mathrm{s}}(t) - \hat{n}_{\mathrm{s}}(0) = \hat{n}_{\mathrm{i}}(t) - \hat{n}_{\mathrm{i}}(0), \tag{2.25}$$

which is a well known Manley-Rowe relation[5] [33], reflecting the fact that signal and idler photons are always created in pairs.

The equations of motions (2.21) posses the following solution [34]:

$$\hat{a}_{\mathrm{s}}(t) = e^{-i\omega_{\mathrm{s}}t}\Big[\hat{a}_{\mathrm{s}}(0)\cosh\big(\kappa|a_{\mathrm{p}}|\big) - i\hat{a}_{\mathrm{i}}^{\dagger}(0)\sinh\big(\kappa|a_{\mathrm{p}}|\big)\Big], \tag{2.26a}$$

$$\hat{a}_{\mathrm{i}}(t) = e^{-i\omega_{\mathrm{i}}t}\Big[\hat{a}_{\mathrm{i}}(0)\cosh\big(\kappa|a_{\mathrm{p}}|\big) - i\hat{a}_{\mathrm{s}}^{\dagger}(0)\sinh\big(\kappa|a_{\mathrm{p}}|\big)\Big], \tag{2.26b}$$

where we introduced $\kappa(t_I) = \int_{-\infty}^{t_I} g(t)\mathrm{d}t$. In practice, the interaction time t_I may be taken as propagation time through the nonlinear medium of length L, $t_I \approx L/c$, which allows to reduce the integration limits in κ: $\int_{-\infty}^{t} \longrightarrow \int_{0}^{t_I}$. The Eqs. (2.26) can be readily used to calculate certain expectations on photon number statistics. To this end we first express the number operators in terms of the field operators at $t = 0$:

$$\begin{aligned}\hat{n}_{\mathrm{s}}(t) = \hat{a}_{\mathrm{s}}^{\dagger}(t)\hat{a}_{\mathrm{s}}(t) = \hat{a}_{\mathrm{s}}^{\dagger}(0)\hat{a}_{\mathrm{s}}(0)\cosh^2\big(\kappa|a_{\mathrm{p}}|\big) + \big[1 + \hat{a}_{\mathrm{i}}^{\dagger}(0)\hat{a}_{\mathrm{i}}(0)\big] \\ \times \sinh^2\big(\kappa|a_{\mathrm{p}}|\big) - \frac{1}{2}i\big[\hat{a}_{\mathrm{s}}^{\dagger}(0)\hat{a}_{\mathrm{i}}^{\dagger}(0) - \hat{a}_{\mathrm{s}}(0)\hat{a}_{\mathrm{i}}(0)\big]\sinh\big(2\kappa|a_{\mathrm{p}}|\big),\end{aligned} \tag{2.27a}$$

$$\begin{aligned}\hat{n}_{\mathrm{i}}(t) = \hat{a}_{\mathrm{i}}^{\dagger}(t)\hat{a}_{\mathrm{i}}(t) = \hat{a}_{\mathrm{i}}^{\dagger}(0)\hat{a}_{\mathrm{i}}(0)\cosh^2\big(\kappa|a_{\mathrm{p}}|\big) + \big[1 + \hat{a}_{\mathrm{s}}^{\dagger}(0)\hat{a}_{\mathrm{s}}(0)\big] \\ \times \sinh^2\big(\kappa|a_{\mathrm{p}}|\big) - \frac{1}{2}i\big[\hat{a}_{\mathrm{i}}^{\dagger}(0)\hat{a}_{\mathrm{s}}^{\dagger}(0) - \hat{a}_{\mathrm{i}}(0)\hat{a}_{\mathrm{s}}(0)\big]\sinh\big(2\kappa|a_{\mathrm{p}}|\big).\end{aligned} \tag{2.27b}$$

Next, assuming that the initial state at $t = 0$ is $|n_{\mathrm{s}}(0), n_{\mathrm{i}}(0)\rangle$, the time evolution of the average photon-number $\langle n_{\mathrm{s}}\rangle$ ($\langle n_{\mathrm{s}}\rangle$) at frequency ω_{s} (ω_{i}) can be easily evaluated:

$$\langle n_{\mathrm{s}}(t)\rangle = n_{\mathrm{s}}(0)\cosh^2\big(\kappa|a_{\mathrm{p}}|\big) + [1 + n_{\mathrm{i}}(0)]\sinh^2\big(\kappa|a_{\mathrm{p}}|\big), \tag{2.28a}$$

$$\langle n_{\mathrm{i}}(t)\rangle = n_{\mathrm{i}}(0)\cosh^2\big(\kappa|a_{\mathrm{p}}|\big) + [1 + n_{\mathrm{s}}(0)]\sinh^2\big(\kappa|a_{\mathrm{p}}|\big). \tag{2.28b}$$

[5] Since the number of photons n is related to the optical power P by $P = n\hbar\omega$, we can rewrite expression (2.25) in the form $P_{\mathrm{s}}/\omega_{\mathrm{s}} = P_{\mathrm{i}}/\omega_{\mathrm{i}}$, in accordance with the original formulation from Manley and Rowe.

Due to the commutation rules (2.16), the second terms in Eqs. (2.28a) and (2.28b) contain an extra 1, which gives under any initial conditions a nonzero contribution $\sinh^2\left(\kappa|a_\mathrm{p}|\right)$ to the average photon number. Thus, even if the signal and idler modes are initially in vacuum states, i.e. $n_\mathrm{s}(0) = n_\mathrm{i}(0) = 0$, after a time period t_I long enough there will be photons in these modes. This purely quantum-mechanical effect elucidates the possibility of spontaneous emission in parametric down-conversion, which emerges as an amplification of the vacuum fluctuations associated with the noncommutation of the field operators. Let us note that the presence of the input signal field stimulates the emission of photons in the idler field and vice versa. That is, the initial conditions $n_\mathrm{s}(0) \neq 0$ or $n_\mathrm{i}(0) \neq 0$ correspond to the effect of stimulated emission, which is fully accounted for by the classical theory of the parametric amplifier.

The interaction time t_I is extremely short for realistic crystal lengths ($\sim$ mm), so that generally we can consider the short-time limit condition, $\kappa|a_p| \ll 1$, to be valid. Then, the photon flux emitted from SPDC is given by

$$\langle n_\mathrm{s}(t)\rangle = \langle n_\mathrm{i}(t)\rangle = \sinh^2\left(\kappa|a_\mathrm{p}|\right) \approx \left(\kappa|a_\mathrm{p}|\right)^2. \tag{2.29}$$

The average photon numbers in the signal and idler mode are proportional to the intensity of the pump field $I_\mathrm{p} \sim |a_\mathrm{p}|^2$. As I_p gives the rate at which pump photons fall on the nonlinear medium, the parameter $|\kappa|^2$ is a dimensionless number determining the fraction of incident pump photons to be converted into lower-frequency photons. The following scaling behavior can be inferred by closer inspection of the parameter κ, see the definition below Eqs. (2.26):

$$\kappa \propto d_\mathrm{eff} L \mathrm{sinc}\left(\frac{\Delta k L}{2}\right), \tag{2.30}$$

where sinc function, $\mathrm{sinc}(x) = \sin(x)/x$, accounts for the impact of phase mismatch Δk on the efficiency of SPDC. As illustrated in Fig. 2.2(a), for a given L the phase mismatch Δk corresponds to a decrease in efficiency by a factor, which is inversely proportional to L. The quadratic scaling of the photon flux with L for the case of perfect phase matching is therefore generally reduced to a linear dependence $\propto L$ if $\Delta k \neq 0$, see Fig. 2.2(b). Furthermore, it follows from (2.30) that the yield of down-conversion photons grows quadratically with the effective nonlinearity d_eff. Due to the fact that signal and idler photons are always created in pairs, the afore-mentioned scaling rules do not apply only for photon emissions into an individual mode, but also for simultaneous double-photon emissions into both modes.

Notably, the above simple theoretical model is sufficient to prove the nonclassical statistics of down-conversion light [31]. To that end, the mathematical steps leading to Eqs. (2.28) are again applied here to evaluate the second moment $\langle : \hat{n}_\mathrm{s,i}^2 : \rangle$ and the

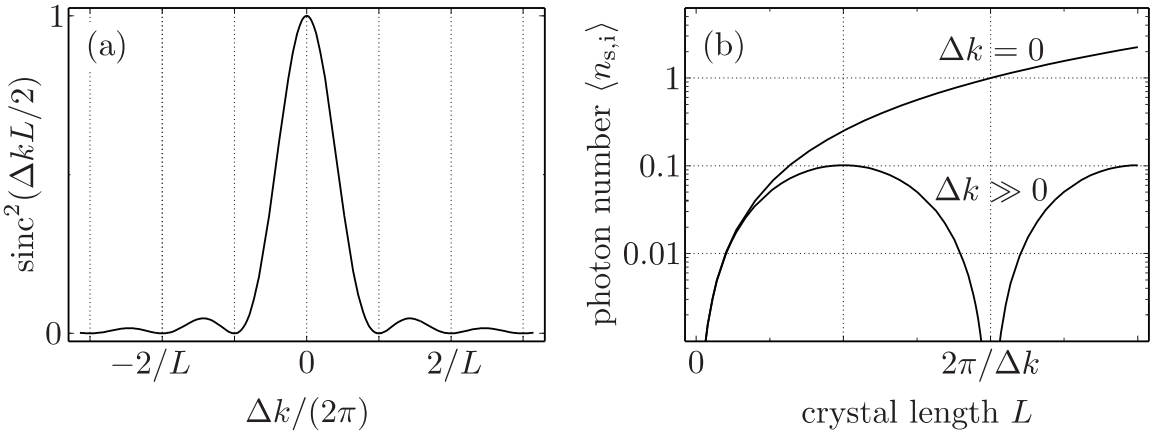

Figure 2.2: Effect of phase mismatch on the efficiency of SPDC. (a) The phase mismatch Δk leads to a decrease of the conversion efficiency in the SPDC process by a factor $\mathrm{sinc}^2(\Delta kL/2)$. For $\Delta k = 0$ this factor equals to 1, but with growing Δk the factor decreases till it reaches 0 at $\Delta k = 2\pi/L$. The width of the sinc function is inversely proportional to L, hence clarifying why the condition of phase matching is more restrictive for longer interaction lengths L. (b) The evolution of the average photon number for the case of perfect phase matching, $\Delta k = 0$ and no-phase matching at all, $\Delta k \gg 0$, is shown. For real situations including a continuous range of possible values $\Delta k \geq 0$, the integration over this range has to be performed to observe the scaling behavior of the photon flux.

cross-correlation $\langle : \hat{n}_{\mathrm{s}} \hat{n}_{\mathrm{i}} : \rangle$[6]:

$$\langle : \hat{n}_m^2(t) : \rangle = \langle 0,0|\hat{a}_m^{\dagger 2}(t)\hat{a}_m^2(t)|0,0\rangle = 2\sinh^4\left(\kappa|a_{\mathrm{p}}|\right), \quad m = \mathrm{s},\mathrm{i}, \tag{2.31a}$$

$$\langle : \hat{n}_{\mathrm{s}}(t)\hat{n}_{\mathrm{i}}(t) : \rangle = \langle 0,0|\hat{a}_{\mathrm{s}}^{\dagger}(t)\hat{a}_{\mathrm{i}}^{\dagger}(t)\hat{a}_{\mathrm{i}}(t)\hat{a}_{\mathrm{s}}(t)|0,0\rangle = 2\sinh^2\left(\kappa|a_{\mathrm{p}}|\right)\left[1+\sinh^2\left(\kappa|a_{\mathrm{p}}|\right)\right], \tag{2.31b}$$

so that the following inequality must hold :

$$\langle : \hat{n}_{\mathrm{s}}(t)\hat{n}_{\mathrm{i}}(t) : \rangle > \frac{1}{2}\big(\langle : \hat{n}_{\mathrm{s}}^2(t) : \rangle + \langle : \hat{n}_{\mathrm{i}}^2(t) : \rangle\big). \tag{2.32}$$

This is however at variance with the analogical classical inequality:

$$\langle I_1 I_2 \rangle \leq \frac{1}{2}\big(\langle I_1^2 \rangle + \langle I_2^2 \rangle\big), \tag{2.33}$$

which evidently has to be fulfilled for any arbitrary classical intensities I_1 and I_2, because $0 \leq \langle (I_1 - I_2)^2 \rangle = \langle I_1^2 \rangle + \langle I_2^2 \rangle - 2\langle I_1 I_2 \rangle$. Ample experimental corroboration of the non-classical character of down-conversion light has been achieved [35, 36].

[6]The colons denote the normal order of operators, in which all the creation operators stand to the left from all the annihilation operators, such that the vacuum expectation value of the normally ordered product is zero.

2.3 Multimode description

In the previous, the theoretical description of SPDC process has been introduced, assuming that just two monochromatic modes of the lower-frequency fields become excited. This treatment could account for some phenomena associated with SPDC, but fails in most cases, where the correlation effects start to be prominent. Therefore, more realistic models are needed, decomposing the down-conversion fields into an infinite set of modes, which is eventually treated as continuum [24, 37]. This treatment conceptualizes the signal and idler photons as short wave packets rather than monochromatic waves, even though the sum of their frequencies has a sharp value.

The down-conversion fields are described as a superposition of modes represented by plane waves, so that each mode is characterized by a wave vector $\boldsymbol{k}$ and a polarization index. The rules of birefringent phase matching dictate that all modes belonging to the signal or the idler field, respectively, have to have the same polarization - either ordinary or extraordinary. This greatly simplifies the situation and allows to omit the polarization indexing in the course of the following derivation. It will be just sufficient to assign certain polarization directions to interacting fields in the final formulas, provided that a certain phase matching scheme will be considered, see Table 2.1. The electric-field operator of the down-conversion field can be thus written as

$$\hat{E}_m(\boldsymbol{r},t) = \sum_{\boldsymbol{k}_m} e_m(\omega_{\boldsymbol{k}_m})\hat{a}_m\left[\boldsymbol{k}_m(\omega_{\boldsymbol{k}_m})\right] e^{i\boldsymbol{k}_m(\omega_{\boldsymbol{k}_m})\boldsymbol{r}-i\omega_{\boldsymbol{k}_m}t} + \text{h.c.}, \quad m = \text{s},\text{i}, \tag{2.34}$$

where $e_m(\omega_{\boldsymbol{k}_m}) = \sqrt{\hbar\omega_{\boldsymbol{k}_m}/2\epsilon_0 V}$ is the amplitude per photon of the mode with a wave vector $\boldsymbol{k}_m$ and a frequency $\omega_{\boldsymbol{k}_m}$. Similarly as in the previous section, the parametric approximation is applied here, treating the pump as a classical, undepleted field. Further, the pump field is assumed to be linearly polarized and propagating in z direction, so that we can write:

$$E_{\text{p}}(z,t) = \mathcal{E}_{\text{p}}^{(+)}(z,t)e^{-i\omega_{\text{p}}^0 t} + \text{h.c.}, \tag{2.35}$$

where ω_{p}^0 is the central frequency and $\mathcal{E}_{\text{p}}^{(+)}(z,t)$ is the positive-frequency part of the complex pump-field envelope, expressed in the form [38]:

$$\mathcal{E}_{\text{p}}^{(+)}(z,t) = \int_{-\infty}^{\infty} \mathrm{d}\nu_{\text{p}}\, \mathcal{E}_{\text{p}}^{(+)}(0,\nu_{\text{p}})e^{ik_{\text{p}}(\omega_{\boldsymbol{k}_{\text{p}}})z-i\nu_{\text{p}}t}, \tag{2.36}$$

where $\nu_{\text{p}} = \omega_{k_{\text{p}}} - \omega_{\text{p}}^0$ and $\mathcal{E}_{\text{p}}^{(+)}(0,\nu_{\text{p}})$ is the spectrum of the field envelope $\mathcal{E}_{\text{p}}^{(+)}(0,t)$ at $z = 0$, defined through the Fourier transformation:

$$\mathcal{E}_{p}^{(+)}(0,\nu_{\text{p}}) = \frac{1}{2\pi}\int_{-\infty}^{\infty} \mathrm{d}t\, \mathcal{E}_{\text{p}}^{(+)}(0,t)e^{i\nu_{\text{p}}t}. \tag{2.37}$$

In the majority of real experimental scenarios, the down-conversion fields are emitted close to the forward direction. Therefore, in the following derivation, we can adopt a reasonable assumption that the transverse $\boldsymbol{k}$-vector components of the down-conversion modes are negligible and put $\hat{E}_m(\boldsymbol{r},t) \equiv \hat{E}_m(z,t)$, $(m = \mathrm{s},\mathrm{i})$. This approximation will substantially simplify the following consideration, but, needles to say, prohibits to gain any information on the spatial characteristics of down-conversion emission. The total Hamiltonian of the system can be expressed as a sum of two terms - the energy in the free uncoupled fields:

$$\hat{H}_0 = \sum_{k_\mathrm{s}} \hbar\omega_{k_\mathrm{s}} \left(\hat{a}_\mathrm{s}^\dagger(k_\mathrm{s})\hat{a}_\mathrm{s}(k_\mathrm{s}) + \frac{1}{2} \right) + \sum_{k_\mathrm{i}} \hbar\omega_{k_\mathrm{i}} \left(\hat{a}_\mathrm{i}^\dagger(k_\mathrm{i})\hat{a}_\mathrm{i}(k_\mathrm{i}) + \frac{1}{2} \right) \tag{2.38}$$

and the energy arising from the interaction of the fields, see Eq. (2.15):

$$\hat{H}_I(t) = C_I \int_{-L}^{0} \mathrm{d}z \int_{-\infty}^{\infty} \mathrm{d}\nu_\mathrm{p} \sum_{k_\mathrm{s}} \sum_{k_\mathrm{i}} \mathcal{E}_\mathrm{p}^{(+)}(0,\nu_\mathrm{p}) \times \hat{a}_\mathrm{s}^\dagger(k_\mathrm{s})\hat{a}_\mathrm{i}^\dagger(k_\mathrm{i}) e^{i(k_\mathrm{p}-k_\mathrm{s}-k_\mathrm{i})z - i(\omega_{k_\mathrm{p}}-\omega_{k_\mathrm{s}}-\omega_{k_\mathrm{i}})t} + \mathrm{h.c.}, \tag{2.39}$$

where C_I includes the effective nonlinearity d_eff and the slowly varying functions $e_\mathrm{s}(\omega_{\boldsymbol{k}_\mathrm{s}})$ and $e_\mathrm{i}(\omega_{\boldsymbol{k}_\mathrm{i}})$. The first integration in (2.39) extends over the length L of the nonlinear crystal in z direction; the origin of the coordinates is assumed to be at the output plane of the crystal. The expressions (2.38) and (2.39) should be compared to the Hamiltonian from Eq. (2.20) describing the discrete three-mode SPDC process.

The splitting of the Hamiltonian into a free unperturbed part $\hat{H}_0$ and an interaction part $\hat{H}_I$, which can be treated as a perturbation, suggests that we can take an advantage of a quantum-mechanical description in the interaction representation, where the time evolution of an arbitrary state vector $|\psi(t)\rangle$ is defined as [32]

$$|\psi(t)\rangle = \exp\left(\frac{1}{i\hbar} \int_{t_0}^{t_0+t_I} \hat{H}_I(t) \right) |\psi(0)\rangle = |\psi(0)\rangle + \sum_{n=1}^{\infty} \left(\frac{1}{i\hbar} \right)^n \times \int_{t_0}^{t_0+t_I} \mathrm{d}t_1 \int_{t_0}^{t_0+t_I} \mathrm{d}t_2 \cdots \int_{t_0}^{t_0+t_I} \mathrm{d}t_n \, \hat{H}_I(t_1)\hat{H}_I(t_2)\cdots\hat{H}_I(t_n)|\psi(0)\rangle. \tag{2.40}$$

Here, t_I is the time of interaction and $|\psi(t=t_0)\rangle = |\psi(0)\rangle$ represents the state at t_0, when the interaction has not been started yet. In the SPDC process there is no input radiation in any signal and idler mode, so that the initial state $|\psi(0)\rangle$ is the multimode vacuum state $|\mathrm{vac}\rangle$. Furthermore, the spontaneous nature of the process implies that the perturbation $\hat{H}_I$ is very small compared to $\hat{H}_0$, which means that the series from Eq. (2.40) must converge fast. Under most experimental conditions only the first term in the series is relevant, corresponding to the emission of a photon pair from SPDC. Thus, the two-photon state of down-conversion photons $|\psi^{(2)}(0,t)\rangle$

at the output of the nonlinear medium ($z = 0$) can be written as

$$|\psi^{(2)}(0,t)\rangle = \frac{1}{i\hbar}\int_{-\infty}^{\infty} \mathrm{d}t\, \hat{H}_I(t)|\mathrm{vac}\rangle. \tag{2.41}$$

By extending the limits of integration in (2.41) to infinity we explicitly assume that the interaction Hamiltonian approaches zero for times before t_0 and after $t_0 + t_I$. Substituting for the interaction Hamiltonian and evaluating the time integral, the two-photon state becomes:

$$|\psi^{(2)}(0,t)\rangle = \frac{C_I}{i\hbar}\int_{-L}^{0}\mathrm{d}z\int_{-\infty}^{\infty}\mathrm{d}\nu_\mathrm{p}\sum_{k_\mathrm{s}}\sum_{k_\mathrm{i}}\mathcal{E}_\mathrm{p}^{(+)}(0,\nu_\mathrm{p})\hat{a}_\mathrm{s}^\dagger(k_\mathrm{s})\hat{a}_\mathrm{i}^\dagger(k_\mathrm{i}) \\ \times e^{i(k_\mathrm{p}-k_\mathrm{s}-k_\mathrm{i})z+i(\omega_{k_\mathrm{s}}+\omega_{k_\mathrm{i}})t}\,\delta(\omega_{k_\mathrm{p}}-\omega_{k_\mathrm{s}}-\omega_{k_\mathrm{i}})|\mathrm{vac}\rangle, \tag{2.42}$$

For the further consideration we expand the wave numbers of interacting fields about their carrier frequencies ω^0 [38]:

$$k_m(\omega_{k_m}) = k_m^0\left(\omega_m^0\right) + \frac{1}{v_m}\left(\omega_{k_m}-\omega_m^0\right) + \frac{1}{2}\mathcal{D}_m\left(\omega_{k_m}-\omega_m^0\right)^2 = k_m^0 + \epsilon k_m, \tag{2.43}$$

where $m = \mathrm{p,s,i}$ and the higher-order terms are dropped. The central wave numbers of the fields $k_m^0\,(\omega_m^0)$ are given by Eq. (2.7). The symbol v_m is the group velocity of the field m, expressed in terms of the refractive index $n(\lambda_m)$ as

$$\frac{1}{v_m} = \left.\frac{\mathrm{d}k_m}{\mathrm{d}\omega_{k_m}}\right|_{\omega_{k_m}=\omega_m^0} = \frac{1}{c}\left[n(\lambda_m) - \lambda_m\frac{\mathrm{d}n(\lambda_m)}{\mathrm{d}\lambda_m}\right], \tag{2.44}$$

and $\mathcal{D}$ is the group velocity dispersion parameter:

$$\mathcal{D}_m = \left.\frac{\mathrm{d}^2k_m}{\mathrm{d}^2\omega_{k_m}}\right|_{\omega_{k_m}=\omega_m^0} = \left.\frac{\mathrm{d}}{\mathrm{d}\omega_{k_m}}\frac{1}{v_m}\right|_{\omega_{k_m}=\omega_m^0} = \frac{\lambda^3}{2\pi c^2}\frac{\mathrm{d}^2n(\lambda_m)}{\mathrm{d}\lambda_m^2}. \tag{2.45}$$

Applying the above expressions in Eq. (2.42) and assuming that the carrier frequencies ω_m^0 and the central wave numbers k_m^0 of the interacting fields fulfill energy- and momentum-conservation conditions from Eqs. (2.5) and (2.6), respectively, we arrive at the following form of the two-photon state [39]:

$$|\psi^{(2)}(0,t)\rangle = \frac{C_I e^{i(\omega_\mathrm{s}^0+\omega_\mathrm{i}^0)t}}{i\hbar}\int_{-L}^{0}\mathrm{d}z\int_{-\infty}^{\infty}\mathrm{d}\nu_p\int_{-\infty}^{\infty}\mathrm{d}\nu_\mathrm{s}\int_{-\infty}^{\infty}\mathrm{d}\nu_\mathrm{i}\,\mathcal{E}_\mathrm{p}^{(+)}(0,\nu_\mathrm{p}) \\ \times\exp\left[i\left(\frac{\nu_\mathrm{p}}{v_\mathrm{p}}-\frac{\nu_\mathrm{s}}{v_\mathrm{s}}-\frac{\nu_\mathrm{i}}{v_\mathrm{i}}\right)z\right]\exp\left[\frac{i}{2}\left(\mathcal{D}_\mathrm{p}\nu_\mathrm{p}^2-\mathcal{D}_\mathrm{s}\nu_\mathrm{s}^2-\mathcal{D}_\mathrm{i}\nu_\mathrm{i}^2\right)z\right] \\ \times\delta(\nu_\mathrm{p}-\nu_\mathrm{s}-\nu_\mathrm{i})e^{i(\nu_\mathrm{s}+\nu_\mathrm{i})t}|\nu_\mathrm{s}\rangle|\nu_\mathrm{i}\rangle, \tag{2.46}$$

where $\nu_m = \omega_{k_m} - \omega_m^0$ is the detuning frequency from the central frequency and $|\nu_m\rangle$ is a one-photon Fock state; $m = \mathrm{s}, \mathrm{i}$. The output two-photon state from SPDC is represented by a continuous superposition of states in which the signal and idler photons have frequencies ν_s and ν_i, respectively. The energy-conservation law, leading to strong correlations of the frequencies ν_s and ν_i, is explicitly displayed in $|\psi^{(2)}(0,t)\rangle$ by the delta function. By evaluating the spatial integral in (2.46) we obtain $\mathrm{sinc}\,[(\epsilon k_\mathrm{p} - \epsilon k_\mathrm{s} - \epsilon k_\mathrm{i})L/2]$, which accounts for the momentum correlation of the down-conversion photons. In the limit of very long crystals, $L \to \infty$, the sinc function approaches delta function $\delta(\epsilon k_\mathrm{p} - \epsilon k_\mathrm{s} - \epsilon k_\mathrm{i})$. That is, in such a limiting case, a down-conversion event is allowed only, if the momenta of the lower-frequency photons sum to the momentum of the pump. Note that the delta functions preclude the possibility of factorization $|\psi^{(2)}(0,t)\rangle$ into a product state of the signal and the idler photon, i.e., $|\psi^{(2)}(0,t)\rangle$ from Eq. (2.46) is an EPR-type entangled state.

2.3.1 Spectra of down-conversion fields

The knowledge of the two-photon state $|\psi^{(2)}(0,t)\rangle$ allows us to readily evaluate the spectral properties of the individual down-conversion fields. The spectrum of the signal (idler) field behind the nonlinear crystal is defined as follows [39, 40]:

$$\mathcal{S}_{\mathrm{s(i)}}(\nu_{\mathrm{s(i)}}) = \langle\psi^{(2)}(0,t)|\hat{a}^\dagger_{\mathrm{s(i)}}(\nu_{\mathrm{s(i)}})\hat{a}_{\mathrm{s(i)}}(\nu_{\mathrm{s(i)}})|\psi^{(2)}(0,t)\rangle. \tag{2.47}$$

Using the state $|\psi^{(2)}(0,t)\rangle$ from (2.46), the expression for the signal field becomes

$$\mathcal{S}_\mathrm{s}(\nu_\mathrm{s}) = \frac{|C_I|^2}{\hbar^2}\int_{-\infty}^{\infty}\mathrm{d}\nu_\mathrm{p}\,\left|\mathcal{E}_\mathrm{p}^{(+)}(0,\nu_\mathrm{p})\right|^2 L^2 \times \mathrm{sinc}^2\left[\frac{L}{2}\left(u_\mathrm{pi}\nu_\mathrm{p} - u_\mathrm{si}\nu_\mathrm{s} + \frac{D_\mathrm{pi}}{2}\nu_\mathrm{p}^2 - \frac{D_\mathrm{si}}{2}\nu_\mathrm{s}^2 + \mathcal{D}_\mathrm{i}\nu_\mathrm{p}\nu_\mathrm{s}\right)\right], \tag{2.48}$$

in which we introduced the following parameters:

$$u_{\mathrm{p}m} = \frac{1}{v_\mathrm{p}} - \frac{1}{v_m}, \qquad D_{\mathrm{p}m} = \mathcal{D}_\mathrm{p} - \mathcal{D}_m, \quad m = \mathrm{s}, \mathrm{i}, \tag{2.49}$$

$$u_\mathrm{si} = \frac{1}{v_\mathrm{s}} - \frac{1}{v_\mathrm{i}}, \qquad D_\mathrm{si} = \mathcal{D}_\mathrm{s} + \mathcal{D}_\mathrm{i}, \tag{2.50}$$

The spectrum of the idler field is obtained from (2.48) by substituting the dispersion parameters u_pi, D_pi and $\mathcal{D}_\mathrm{i}$ for u_ps, D_ps and $\mathcal{D}_\mathrm{s}$, respectively. In the limiting case of the continuous-wave (CW) pumping at the frequency ω_p^0, the complex spectrum of the pump-field envelope $\mathcal{E}_\mathrm{p}^{(+)}(0,\nu_\mathrm{p})$ is put as the delta function $\delta(\nu_p)$ multiplied by

the amplitude ξ_p, and the expression (2.48) reduces to the following analytical form:

$$\mathcal{S}_\mathrm{s}^{(\mathrm{cw})}(\nu_\mathrm{s}) = \frac{|C_I \xi_\mathrm{p}|^2}{\hbar^2} L^2 \mathrm{sinc}^2 \left[\frac{L}{2} \left(u_\mathrm{si} \nu_\mathrm{s} + \frac{D_\mathrm{si}}{2} \nu_\mathrm{s}^2 \right) \right]. \tag{2.51}$$

The spectral profiles of the emitted photon wave packets are determined by a sinc^2 function, which appears in the expression (2.48) due to the double integration over the finite length L of the crystal. Note that the idler spectrum will be given by the formula identical to (2.51), because none of the dispersion parameters from (2.49) are contained therein. That is, the spectra of the two generated fields are always the same in CW-pumped SPDC. This is explained by perfect anti-correlation of the signal and idler frequencies: The two frequencies always sum up to the pump frequency ω_p^0, which ensures that the output two-photon state $|\psi^{(2)}(0,t)\rangle$ will be symmetric in the frequencies of signal and idler photon wave packets.

A further simplification of the expression (2.51) for down-conversion spectra in the CW-pumping limit might be attained, when assuming a certain phase matching scheme. This also allows to investigate the scaling behavior of the spectral width on the relevant parameters, showing remarkably different results for type I and type II phase matching. Unless specified otherwise, the spectral width is defined here as the full width at half maximum (FWHM) of the sinc^2 profile.

We start with type II phase matching scheme. There, signal and idler wave packets are orthogonally polarized, and therefore they are necessarily subjected to distinct material dispersion in the nonlinear crystal due to its anisotropy, see section 2.1. Consequently, the difference in the group velocities of photons reaches considerable values; for standard materials u_si is roughly $\approx 10^{-10}$ s/m. The parameter D_si reaches usually $\approx 10^{-25}$ s^2/m in case of type-II phase matching, so that the second term in sinc^2 function of Eq. (2.51) can be neglected for the realistic values of the detuning frequencies $\nu_\mathrm{s}, \nu_\mathrm{i} \approx 10^{13} - 10^{14}$ s^{-1}. The phase-matched spectral width of the down-conversion fields is thus solely determined by the difference in group velocities u_si and the thickness of the crystal L, and it scales as $\propto 1/(u_\mathrm{si} L)$. That is, the longer the crystal L and the higher the difference in group velocities $|v_\mathrm{s} - v_\mathrm{i}|$, the narrower the resultant spectrum will be.

For type I phase matching a markedly different situation is encountered. The emitted photons have the same polarization and therefore they propagate through the nonlinear crystal with identical group velocities. Consequently, the dispersion parameter u_si vanishes and it is now the second term in the sinc^2 function of Eq. (2.51), which will determine the spectral characteristics of down-conversion light. Due to the fact that this term is smaller by 1–2 orders of magnitude than the term, which was previously dominant for type II phase matching, significantly broader spectra might be expected in case of type I phase matching. Moreover, the spectral width now scales as $\propto 1/\sqrt{(D_\mathrm{si} L)}$. This means that the width shrinks only with the square root of crystal length.

Note that the above discussion implicitly assumed degenerate central output fre-

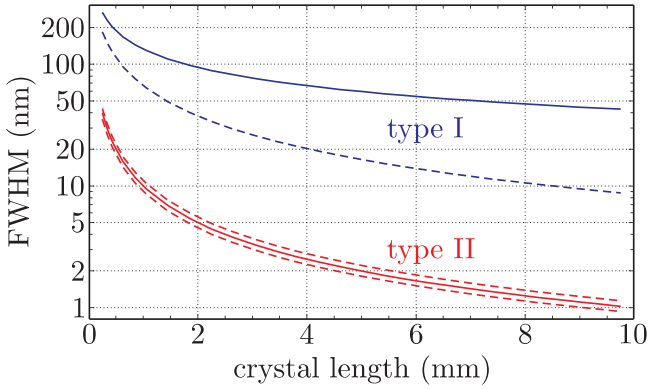

Figure 2.3: Scaling of down-conversion spectral width with the crystal length for different phase-matching configurations. The widths are for degenerate type I and type II SPDC represented by blue and red solid curves, respectively. The first scales as $\propto 1/\sqrt{L}$ and the latter as $\propto 1/L$. The dashed curves in corresponding colors show the widths for non-degenerate type I and type II phase matching, assuming a 100 nm separation between central down-conversion wavelengths. In the plot SPDC in a BBO crystal and pumped at a wavelength $\lambda_{\mathrm{p}}^0 = 403$ nm is assumed.

quencies, i.e. the condition $\omega_{\mathrm{p}}^0 = 2\omega_{\mathrm{s}}^0 = 2\omega_{\mathrm{i}}^0$. If non-degenerate central frequencies ($\omega_{\mathrm{s}}^0 \neq \omega_{\mathrm{i}}^0$) are phase-matched in type I SPDC, the parameter u_{si} does not vanish any longer due to the dispersive nature of the nonlinear crystal, and both terms in the sinc^2 function have to be taken into account. As a result, the spectral width shrinks compared to the degenerate case, and approaches the type-II phase-matched width as the non-degeneracy increases. In contrast to type I phase matching, there is only a little effect on the width of phase-matched spectra in type II SPDC when going away from the non-degeneracy point. The resultant width might slightly increase or decrease depending on whether the higher central non-degenerate frequency corresponds to extraordinary or ordinary polarization.

The general conclusions drawn above for the CW-pumped SPDC are quantitatively demonstrated in the Fig. 2.3, showing the dependencies of spectral width on the crystal lengths for different phase matching configurations. An example of SPDC in a beta-barium borate nonlinear crystal (β-BaB_2O_4 or BBO, the basic characteristics are given in appendix A.1.1) is considered therein.

While the idler and signal wave packets produced in narrow-band pumped SPDC are perfectly anti-correlated in their frequencies, the broadband pumping of SPDC entails more complex spectral correlation of the wave packets. For the latter case, the energy-conservation condition is relaxed, because a down-conversion event is permitted, whenever the frequencies of the daughter photons sum to some frequency found in the pump. As a finite range of pump frequencies is available for the nonlinear process, the phase matching condition is fulfilled for more signal and idler frequencies and consequently, their natural spectra are broadened in comparison with CW-pumping case. Moreover, for type II SPDC the broadband pumping causes a symmetry break-

ing between the spectra of ordinary- and extraordinary-polarized wave packets [41]. They are no longer identical, which is attributed to the distinct influence of material dispersion on the two polarizations.

To quantitatively estimate the effect of broadband pumping on the down-conversion spectra, we conveniently represent the pump field as a gaussian pulse with a duration τ_{p}. Then, the following form of the pump-field envelope from Eq. (2.35) applies [38]:

$$\mathcal{E}_{\mathrm{p}}^{(+)}(0,t) = \xi_{\mathrm{p}} \exp\left(-\frac{1+ia_{\mathrm{p}}}{\tau_G^2}t^2\right), \tag{2.52}$$

where ξ_{p} is the amplitude and a_{p} represents the linear chirp of the pulse. The parameter τ_G determines the pulse duration τ_{p} (measured as the full width at half maximum of the intensity profile) via the following relation:

$$\tau_{\mathrm{p}} = \sqrt{2\ln 2}\tau_G. \tag{2.53}$$

The Fourier transformation of (2.52) according to the definition in Eq. (2.37) into the frequency domain gives:

$$\mathcal{E}_{\mathrm{p}}^{(+)}(0,\nu_{\mathrm{p}}) = \xi_{\mathrm{p}} \frac{\tau_G}{2\sqrt{\pi}\sqrt{1+ia_{\mathrm{p}}}} \exp\left[-\frac{\tau_G^2}{4(1+ia_{\mathrm{p}})}\nu_{\mathrm{p}}^2\right], \tag{2.54}$$

which might be directly substituted into the expression (2.48) to find the down-conversion spectra. The results of a numerical evaluation are presented in Fig. 2.4, assuming a specific example of SPDC in a 2 mm long BBO nonlinear crystal. For short pump-pulse durations, a significant broadening of spectra is observed for both type I and type II SPDC. Moreover, as expected, the spectrum of the ordinary polarized wave packet is broader than that of the extraordinary-polarized photon in case of type II SPDC.

It is important to bear in mind that the above theoretical model is built upon two approximations, which limit the general validity of the inferred results. First, it treats the pump field as a superposition of plane waves, which all propagate in z direction, see Eq. (2.36). Thus, the effect of pump-beam focusing is not included in the model whatsoever. We might expect, that this effect will be completely analogous to that of spectral broadening of the pump. Because a wider range of pump-wave vectors is available for the nonlinear process in case of tight focusing, the phase matching condition is fulfilled for more signal and idler frequencies/momenta and consequently, their natural spectra will be broadened. Indeed, it was shown that the tight focusing of the pump to waist sizes of $\ll 100$ μm leads to a significant increase of down-conversion spectral width [42] (provided that crystals with lengths in $\sim$ mm range are used). A second limitation arises from the assumption of the collinear geometry of the nonlinear process, which was adopted in the model. This implies that the faithful results are obtained only for the emission of down-conversion photons close enough to the direction of the pump beam. A more sophisticated treatment is required, if

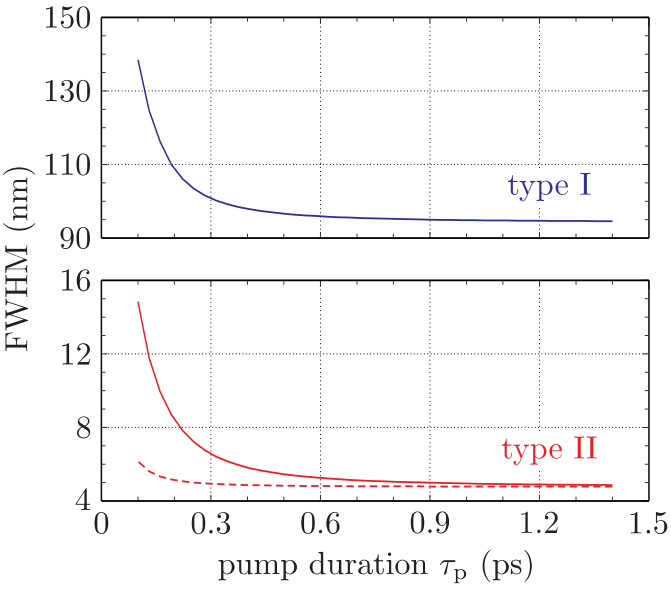

Figure 2.4: Effect of the broadband pumping on the phase-matched spectral width. The upper plot shows the results obtained for type I SPDC and the lower for type II SPDC. In the latter plot the solid and dashed curves correspond to ordinary and extraordinary polarization, respectively. The evaluation assumes SPDC in a 2 mm long BBO crystal pumped at a wavelength of $\lambda_p^0 = 403$ nm.

the directions of down-conversion photons deviate significantly from the pump-beam direction [42].

Finally, we emphasize again that the formula (2.47) provides the spectral characteristics of the natural phase matching in SPDC. I.e., in fact, it determines the spectral widths of the photon wave packets right behind the nonlinear crystal. Nevertheless, it is straightforward to elaborate the theoretical frame and incorporate the effect of frequency filtering, which is commonly used in the experimental arrangements. In practice, frequency filtering is realized by interference filters or by restricting the angular distribution of the emitted down-conversion fields. In either case it can be modelled to a good approximation by a spectral transmission function with a gaussian profile centered around the carrier frequency ω_m^0:

$$\mathcal{F}_m(\nu_m) = \exp\left(-\frac{2\nu_m^2}{\sigma_m^2}\right), \quad m = \mathrm{s}, \mathrm{i}. \tag{2.55}$$

The FWHM of the profile is defined as $\sqrt{2\ln 2}\sigma_m$. Frequency filtering is then included in the theoretical frame by inserting the term $\sqrt{\mathcal{F}_\mathrm{i}\mathcal{F}_\mathrm{s}}$ in the two-photon state $|\psi^{(2)}(0,t)\rangle$ defined in Eq. (2.46). Consequently, the signal (idler) spectra evaluated according to Eq. (2.47) account not only for a trivial effect of spectral filtering performed directly on signal (idler) photons, but also for a non-local effect, which might be loosely referred to as cross-filtering. It means, e.g., if a frequency filtering is performed on the signal photon, then the corresponding idler-photon spectra, which effectively contribute to the two-photon state, will be altered as well due to entanglement of photon pairs in the frequency domain.

2.3.2 Time distribution of down-conversion fields

The joint time distribution of down-conversion fields is conveniently described in terms of the two-photon amplitude, which is sometimes referred to as biphoton amplitude. It is defined as a matrix element for the transition of the down-conversion fields from a two-photon state $|\psi^{(2)}(0,t)\rangle$ into a vacuum state $|\mathrm{vac}\rangle$ [39, 40],

$$\mathcal{A}(\tau_\mathrm{s},\tau_\mathrm{i}) = \langle \mathrm{vac}|\hat{E}_\mathrm{s}^{(+)}(0,t_0+\tau_\mathrm{s})\hat{E}_\mathrm{i}^{(+)}(0,t_0+\tau_\mathrm{i})|\psi^{(2)}(0,t_0)\rangle. \tag{2.56}$$

That is, $\mathcal{A}$ defines the amplitude that two separated ideal detectors of negligible sizes record the signal and idler photons at the times τ_s and τ_i, respectively. This interpretation comes directly from standard quantum field theory, see e.g. [43]. It becomes then obvious that the square of the two-photon amplitude determines the second-order correlation function $G^{(2)}(\tau_\mathrm{s},\tau_\mathrm{i}) = |\mathcal{A}(\tau_\mathrm{s},\tau_\mathrm{i})|^2$, which is proportional to the probability of coincidence detection of the down-conversion photons at the times τ_s and τ_i. Integrating the correlation function $G^{(2)}(\tau_\mathrm{s},\tau_\mathrm{i})$ over a time interval T gives the average coincidence count rate R_c of the two detectors during T, which might be written as [44]:

$$\begin{aligned} R_c \propto \frac{1}{T}\int_0^T \mathrm{d}\tau_\mathrm{s}\int_0^T \mathrm{d}\tau_\mathrm{i}\ \langle\psi^{(2)}(0,t_0)|\hat{E}_\mathrm{i}^{(-)}(0,t_0+\tau_\mathrm{i})\hat{E}_\mathrm{s}^{(-)}(0,t_0+\tau_\mathrm{s}) \\ \times \hat{E}_\mathrm{s}^{(+)}(0,t_0+\tau_\mathrm{s})\hat{E}_\mathrm{i}^{(+)}(0,t_0+\tau_\mathrm{i})|\psi^{(2)}(0,t_0)\rangle. \end{aligned} \tag{2.57}$$

The above formula directly relates the measurable quantity - the coincidence count rate - to the two-photon amplitude.

In general, the two-photon amplitude determines all the measurable joint characteristics of the down-conversion fields [40]. I.e., $\mathcal{A}(\tau_\mathrm{s},\tau_\mathrm{i})$ plays a role of a wavefunction, which describes the effective field of the two-photon wave packet (biphoton). Since we are primarily interested in the time characterization of the two-photon wave packet, the spatial dependency of the amplitude $\mathcal{A}(\tau_\mathrm{s},\tau_\mathrm{i})$ is completely omitted in the above description. Substituting for the electric-field operators and the two-photon state, Eq. (2.56) becomes [39]

$$\begin{aligned} \mathcal{A}(\tau_\mathrm{s},\tau_\mathrm{i}) =& \frac{C_I}{i\hbar}e_\mathrm{s}(\omega_\mathrm{s}^0)e_\mathrm{i}(\omega_\mathrm{i}^0)e^{i(\omega_\mathrm{s}^0\tau_\mathrm{s}+\omega_\mathrm{i}^0\tau_\mathrm{i})}\int_{-L}^{0}\mathrm{d}z\int_{-\infty}^{\infty}\mathrm{d}\nu_p\int_{-\infty}^{\infty}\mathrm{d}\nu_\mathrm{s}\int_{-\infty}^{\infty}\mathrm{d}\nu_\mathrm{i}\,\mathcal{E}_\mathrm{p}^{(+)}(0,\nu_\mathrm{p}) \\ &\times\exp\left[i\left(\frac{\nu_\mathrm{p}}{v_\mathrm{p}}-\frac{\nu_\mathrm{s}}{v_\mathrm{s}}-\frac{\nu_\mathrm{i}}{v_\mathrm{i}}\right)z\right]\exp\left[\frac{i}{2}\left(\mathcal{D}_\mathrm{p}\nu_\mathrm{p}^2-\mathcal{D}_\mathrm{s}\nu_\mathrm{s}^2-\mathcal{D}_\mathrm{i}\nu_\mathrm{i}^2\right)z\right] \\ &\times\delta(\nu_\mathrm{p}-\nu_\mathrm{s}-\nu_\mathrm{i})e^{i(\nu_\mathrm{s}\tau_\mathrm{s}+\nu_\mathrm{i}\tau_\mathrm{i})}\mathcal{T}_\mathrm{s}(\nu_\mathrm{s})\mathcal{T}_\mathrm{i}(\nu_\mathrm{i})|\nu_\mathrm{s}\rangle|\nu_\mathrm{i}\rangle. \end{aligned} \tag{2.58}$$

The newly introduced symbols $\mathcal{T}_\mathrm{s}$ and $\mathcal{T}_\mathrm{i}$ represent the optical transfer functions [29], which describe the effect of any linear optical system (or series of linear optical systems) on signal and idler photons. This allows us to evaluate the effective two-photon amplitude at any place of a real experimental set-up. E.g., putting $\mathcal{T}_m(\nu_m) \equiv$

$\sqrt{\mathcal{F}_m(\nu_m)}$ [see Eq. (2.55)], the expression (2.58) defines the amplitude $\mathcal{A}$ of the two-photon down-conversion wave packet after passing through frequency filters.

For CW-pumped SPDC [$\mathcal{E}_{\mathrm{p}}^{(+)}(0,\nu_{\mathrm{p}}) = \xi_{\mathrm{p}}\delta(\nu_{\mathrm{p}})$], the expression for the two-photon amplitude simplifies to

$$\mathcal{A}(\tau_{\mathrm{s}},\tau_{\mathrm{i}}) = \frac{C_I}{i\hbar} e_{\mathrm{s}}(\omega_{\mathrm{s}}^0) e_{\mathrm{i}}(\omega_{\mathrm{i}}^0) \xi_{\mathrm{p}} e^{i(\omega_{\mathrm{s}}^0\tau_{\mathrm{s}} + \omega_{\mathrm{i}}^0\tau_{\mathrm{i}})} \int_{-\infty}^{\infty} \mathrm{d}\nu_{\mathrm{s}}\, e^{-i\nu_{\mathrm{s}}(\tau_{\mathrm{s}}-\tau_{\mathrm{i}})} \times \mathcal{T}_{\mathrm{s}}(\nu_{\mathrm{s}}) \mathcal{T}_{\mathrm{i}}(-\nu_{\mathrm{s}}) \exp\left[-i\frac{L\nu_{\mathrm{s}}}{2}\left(u_{\mathrm{si}} + \frac{D_{\mathrm{si}}}{2}\nu_{\mathrm{s}}\right)\right] \mathrm{sinc}\left[\frac{L\nu_{\mathrm{s}}}{2}\left(u_{\mathrm{si}} + \frac{D_{\mathrm{si}}}{2}\nu_{\mathrm{s}}\right)\right], \quad (2.59)$$

where the dispersion parameters u_{si} and D_{si} are defined in (2.50). In order to grasp the basic physics of (2.59), we put, for simplicity, $\mathcal{T}_{\mathrm{s}}(\nu_{\mathrm{s}}) = \mathcal{T}_{\mathrm{i}}(-\nu_{\mathrm{s}}) = 1$, and analyze the two-photon amplitude right after the nonlinear crystal. The two photon-amplitude is conveniently studied in the rotated coordinate system with the axes $\tau_+ = (\tau_{\mathrm{s}} + \tau_{\mathrm{i}})/2$ and $\tau_- = \tau_{\mathrm{s}} - \tau_{\mathrm{i}}$. We may interpret τ_- as the difference in the arrival times of the signal and idler photon at the output face of the crystal. If it is positive, the signal photon arrives after the idler photon and vice versa. The value of τ_+ may be regarded as the time at which the center of the two-photon wave packet arrives at the output face of the crystal. The origin for the τ_+ axis is defined by the arrival time of the pump.

We immediately recognize that the expression (2.59) is independent of the time τ_+ except for an irrelevant phase factor. This must be clearly right for the case of CW pumping, because an SPDC event can occur in principle at any time, so that all the values τ_+ are equally probable. In general, the two-photon amplitude is determined along the τ_+ direction by the temporal characteristics of the pump field and the group velocity mismatch between the pump and the two-photon down-conversion wavepacket. Apparently, for very short crystals, the time profile of the pump will be directly transferred to the τ_+-profile of $|\mathcal{A}(\tau_+,\tau_-)|$. For long enough crystals the broadening of the τ_+-profile due to the effect of the group velocity mismatch will become significant.

By closer inspection of (2.59), the distinct profiles of the two-photon amplitudes might be recognized along the τ_- axis for type I and type II SPDC, see Fig. 2.5. This is evidently a consequence of different effects, which lead to time mismatch in arrivals of signal and idler photons at the output face of the nonlinear crystal. For type II SPDC, it is the difference in group velocities, which causes a rectangular-shaped asymmetric profile. This profile stretches from 0 to the value of $u_{\mathrm{si}}L$, which corresponds to the difference in time required for ordinary- and extraordinary-polarized photon to cross the full length of the crystal. For degenerate type I SPDC the group velocities are identical and it is the next order in the expansion of the wave numbers [see Eq. (2.43)], i.e. the effect of group velocity dispersion, which determines the width of biphoton in τ_- direction. Consequently, a narrow symmetric triangular-shaped profile is observed.

The above description together with the results from Fig. 2.5 suggest that the

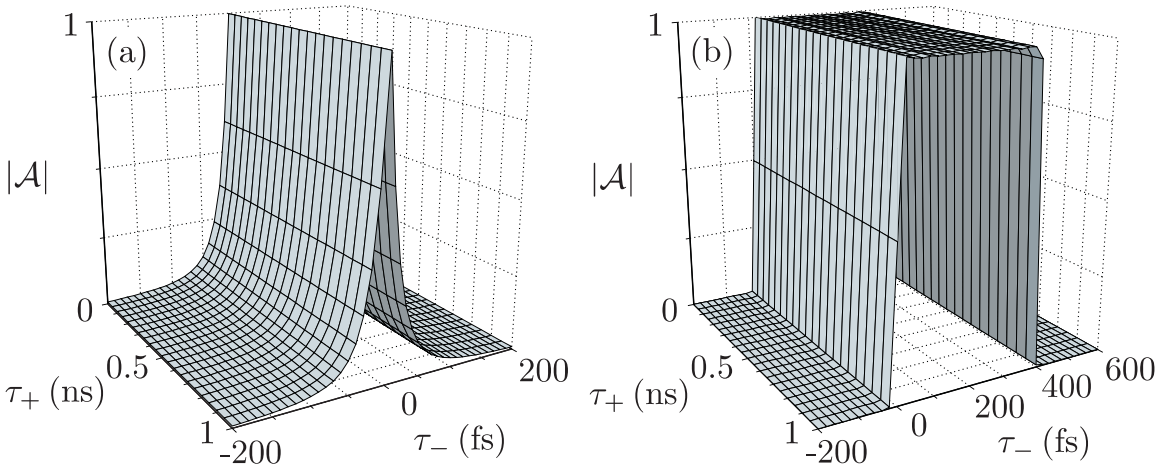

Figure 2.5: Absolute value of the normalized two-photon amplitude, $|\mathcal{A}(\tau_+, \tau_-)|$, for CW-pumped (a) type I and (b) type II SPDC. Whereas a narrow triangular-shaped profile is observed for type I phase matching in the τ_- direction, type II is characterized by a wide rectangular profile, which is asymmetric to $\tau_- = 0$. In the graphs, SPDC in a 2 mm long BBO pumped at $\lambda_p^0 = 403$ nm is considered; the signal (idler) is identified with ordinary (extraordinary) polarization.

width of $|\mathcal{A}(\tau_+, \tau_-)|$ in the τ_- direction is inversely proportional to the phase-matched spectral width of down-conversion photons in case of CW pumped SPDC[7]. This clarifies, why the spectral bandwidth of down-conversion photons is incomparably broader for type I phase matching. For non-degenerate type I phase matching or for increasing crystal lengths, the amplitude $|\mathcal{A}(\tau_+, \tau_-)|$ spreads in the τ_- direction. This behavior is in accordance with the observation from the subsection 2.3.1 that the phase-matched spectral width shrinks in such cases.

2.4 Spatial emission distribution of down-conversion photons

In the foregoing sections the spectral and temporal characteristics of the down-conversion fields have been investigated. To keep the theoretical frame on a manageable level, the spatial properties of the fields interacting in SPDC have been ignored. This section addresses the issue of the spatial properties of these fields and derives the emission characteristics of down-conversion photons. The emission characteristics are derived from the analysis of the energy and momentum conservation conditions. For a fixed pump wave vector and a fixed wavelength of one down-conversion photon

[7]Indeed, for the FWHM values of 28.2 fs (type I phase matching) and 388.9 fs (type II phase matching) inferred for the parameters used in Fig. 2.5, we find the related "Fourier" spectral widths of 76.8 nm and 5.5 nm, respectively, which fit well to results plotted in Fig. 2.3.

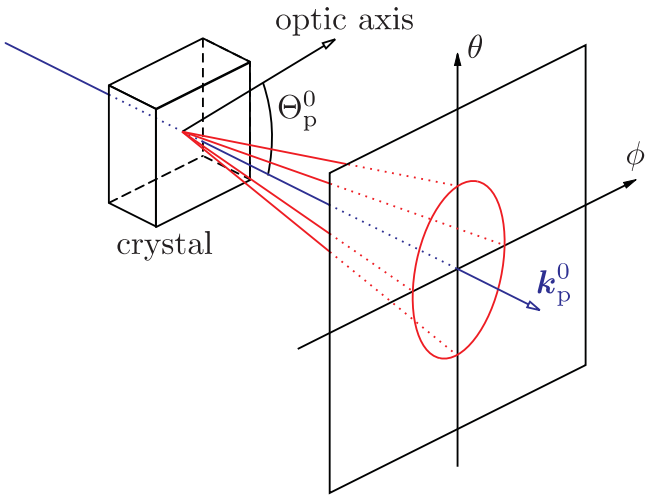

Figure 2.6: General geometrical setting to analyze the angular distribution of down-conversion light. The distribution is defined in terms of the external emission angles θ and ϕ, which are measured with respect to the central pump wave vector $\boldsymbol{k}_{\mathrm{p}}^{0}$. This vector forms an angle Θ_{p}^{0} with optic axis of the nonlinear crystal.

from the pair, all emission directions allowed by conservation laws can be calculated.

In practical experiments, a gaussian beam of a certain divergence is usually used for pumping of the nonlinear crystal. To account for this feature, the pump is decomposed into a representative set of plane waves, each characterized by a wave vector[8]. The allowed emission directions are then searched for each vector separately. To include the effect of finite spectral bandwidth, which is always phase-matched in SPDC, the wavelengths of down-conversion photons are varied within the relevant ranges during the evaluation. The angular distribution of down-conversion light inside the crystal is then evaluated as a weighted superposition of all the found solutions. Finally, Snell's law is applied to determine the distribution outside the crystal. This external angular distribution is obtained in terms of the angles θ and ϕ, which are defined with regard to the central pump wave vector $\boldsymbol{k}_{p}^{0}$, see Fig. 2.6.

This relatively simple approach to the problem, based on the analysis of phase-matching conditions, determines the emission pattern related to the single-photon count rate [45], rather than the coincidence count rate, which has to be considered in the context of two-photon imaging or other spatial correlation effects (see e.g. [46]). In practice, the single-photon pattern can be experimentally captured by imaging the down-conversion emission onto an intensified charge coupled device array. The knowledge of this pattern is sufficient to understand the spectral and spatial characteristics of the parametric down conversion process for the purpose of maximizing the yield of available photon pairs in common experiments.

In the following, we shall discuss the elements of the method at length. We start the analysis by decomposing the phase matching condition (2.6) into a linear set of equations associated with momentum conservation along the principal axes of the

[8]The justification of this approach is addressed later in this section.

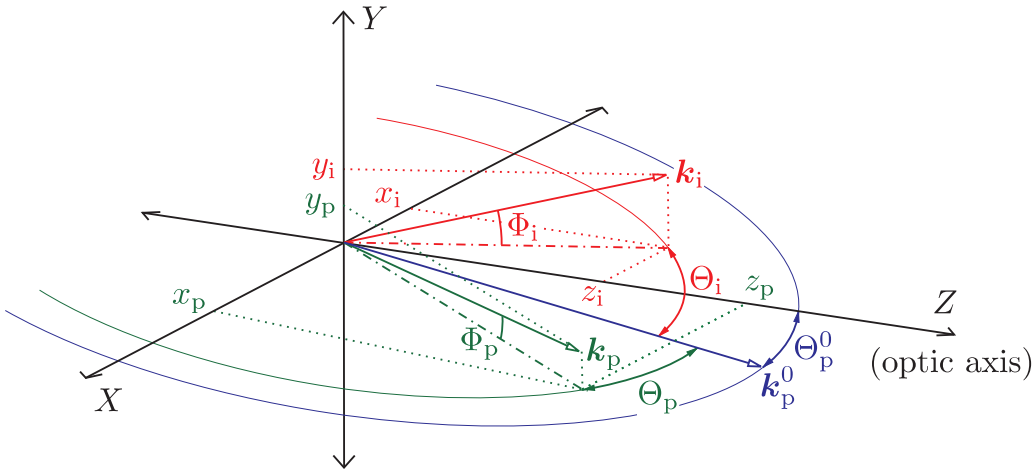

Figure 2.7: Principal coordinate system of the crystal with the definitions of unit wave vectors of the three interacting fields in SPDC. Each of the vectors is specified by an internal azimuth angle Θ_m and an internal polar angle $\Phi_m, (m = \mathrm{p}, \mathrm{s}, \mathrm{i})$. These angles are measured with respect to central pump wave vector $\boldsymbol{k}_\mathrm{p}^0$. For clarity, only the wave vectors $\boldsymbol{k}_\mathrm{p}$ and $\boldsymbol{k}_\mathrm{i}$ of pump and idler photons, respectively, are displayed in the figure; the signal vector is defined analogously.

crystal. Using the relation (2.7), we write these equations in the form:

$$\begin{aligned} \omega_\mathrm{s} n_\mathrm{s} x_\mathrm{s} + \omega_\mathrm{i} n_\mathrm{i} x_\mathrm{i} &= \omega_\mathrm{p} n_\mathrm{p} x_\mathrm{p}, \\ \omega_\mathrm{s} n_\mathrm{s} y_\mathrm{s} + \omega_\mathrm{i} n_\mathrm{i} y_\mathrm{i} &= \omega_\mathrm{p} n_\mathrm{p} y_\mathrm{p}, \\ \omega_\mathrm{s} n_\mathrm{s} z_\mathrm{s} + \omega_\mathrm{i} n_\mathrm{i} z_\mathrm{i} &= \omega_\mathrm{p} n_\mathrm{p} z_\mathrm{p}, \end{aligned} \tag{2.60}$$

where $x_m, y_m, z_m, (m = \mathrm{p}, \mathrm{s}, \mathrm{i})$ are the projections of the unit wave vectors onto the axes of the principle coordinate system, which is identified with the crystallographic structure of the crystal, see Fig. 2.7. The choice of this coordinate system shows to be preferable for the analysis of phase matching because it allows fairly direct definition of the wave vectors in question and avoids any confusions in the calculation of refractive indices. Applying the energy conservation law (2.5) and the normalization condition, $x_m^2 + y_m^2 + z_m^2 = 1$, the Eqs. (2.60) can be combined into a single equation of the form [45]:

$$\begin{aligned} &\left(\omega_\mathrm{p} n_\mathrm{p} \sqrt{1 - y_\mathrm{p}^2 - z_\mathrm{p}^2} - \omega_\mathrm{i} n_\mathrm{i} \sqrt{1 - y_\mathrm{i}^2 - z_\mathrm{i}^2}\right)^2 \\ &\qquad + \left(\omega_\mathrm{p} n_\mathrm{p} y_\mathrm{p} - \omega_\mathrm{i} n_\mathrm{i} y_\mathrm{i}\right)^2 + \left(\omega_\mathrm{p} n_\mathrm{p} z_\mathrm{p} - \omega_\mathrm{i} n_\mathrm{i} z_\mathrm{i}\right)^2 = n_\mathrm{s}^2 \left(\omega_\mathrm{p} - \omega_\mathrm{i}\right)^2, \end{aligned} \tag{2.61}$$

where all the variables related to the wave vector of the signal photon were eliminated. Orientations of the pump and idler wave vectors, expressed using the projections $y_\mathrm{p}, z_\mathrm{p}$ and $y_\mathrm{i}, z_\mathrm{i}$, respectively, can be conveniently redefined with the help of Fig. 2.7

in terms of the azimuthal angles $\Theta_{\rm p}, \Theta_{\rm i}$ and polar angles $\Phi_{\rm p}, \Phi_{\rm i}$ as follows

$$y_{\rm i} = \sin\left(\Phi_{\rm i}\right), \qquad z_{\rm i} = \cos\left(\Theta_{\rm p}^0 - \Theta_{\rm i}\right)\sqrt{1-\sin^2\left(\Phi_{\rm i}\right)}, \tag{2.62}$$

$$y_{\rm p} = \sin\left(\Phi_{\rm p}\right), \qquad z_{\rm p} = \cos\left(\Theta_{\rm p}^0 + \Theta_{\rm p}\right)\sqrt{1-\sin^2\left(\Phi_{\rm p}\right)}. \tag{2.63}$$

Assuming type I phase matching in a negative uniaxial crystal, such as beta-barium borate, the classification of Table 2.1 asserts the pump photon to be extraordinary polarized, whereas both signal and idler photons to be ordinary polarized. Accordingly, the following refractive indices have to substituted into Eq. (2.61):

$$\begin{gathered} n_{\rm p} \equiv n^e(\lambda_{\rm p}; \Theta_{\rm p}^0, \Theta_{\rm p}, \Phi_{\rm p}) = \frac{n_e(\lambda_{\rm p}) n_o(\lambda_{\rm p})}{\sqrt{n_o^2(\lambda_{\rm p}) + \left[n_e^2(\lambda_{\rm p}) - n_o^2(\lambda_{\rm p})\right] z_{\rm p}^2}}, \\ n_{\rm s} \equiv n_o(\lambda_{\rm s}), \quad n_{\rm i} \equiv n_o(\lambda_{\rm i}). \end{gathered} \tag{2.64}$$

The first expression (for extraordinary refractive index) is deduced from Eq. (2.13). In type II phase matching, the idler photon is co-polarized with the extraordinary pump photon, whereas the signal photon remains ordinary polarized as in type I phase-matching. Consequently, the following triad of refractive has to be used in Eq. (2.61):

$$\begin{gathered} n_{\rm p} \equiv n^e(\lambda_{\rm p}; \Theta_{\rm p}^0, \Theta_{\rm p}, \Phi_{\rm p}) = \frac{n_e(\lambda_{\rm p}) n_o(\lambda_{\rm p})}{\sqrt{n_o^2(\lambda_{\rm p}) + \left[n_e^2(\lambda_{\rm p}) - n_o^2(\lambda_{\rm p})\right] z_{\rm p}^2}}, \\ n_{\rm s} \equiv n_o(\lambda_{\rm s}), \quad n_{\rm i} \equiv n^e(\lambda_{\rm i}; \Theta_{\rm p}^0, \Theta_{\rm i}, \Phi_{\rm i}) = \frac{n_e(\lambda_{\rm i}) n_o(\lambda_{\rm i})}{\sqrt{n_o^2(\lambda_{\rm i}) + \left[n_e^2(\lambda_{\rm i}) - n_o^2(\lambda_{\rm i})\right] z_{\rm i}^2}}. \end{gathered} \tag{2.65}$$

For a fixed pair of pump and idler wavelengths, $\lambda_{\rm p}$ and $\lambda_{\rm i}$, the corresponding signal-photon wavelength is known, $\lambda_{\rm s} = \lambda_{\rm i}\lambda_{\rm p}/(\lambda_{\rm i} - \lambda_{\rm p})$, and the refractive indices given by Eqs. (2.64) and (2.65) can be easily determined using the Sellmeier formula (2.14). Consequently, Eq. (2.61) assigns to every pump orientation a continuous set of idler emission directions defined in terms of internal angles $\Theta_{\rm i}$ and $\Phi_{\rm i}$. The corresponding signal emission angles $\Theta_{\rm s}$ and $\Phi_{\rm s}$, meeting the momentum conservation condition (2.60), can be readily determined, bearing in mind the following equivalence formulas:

$$y_{\rm s} = \sin\left(\Phi_{\rm s}\right), \qquad z_{\rm s} = \cos\left(\Theta_{\rm p}^0 - \Theta_{\rm s}\right)\sqrt{1-\sin^2\left(\Phi_{\rm s}\right)}. \tag{2.66}$$

The last step in the evaluation procedure entails the calculation of the emission directions outside the crystal. We shall consider a general arrangement of pumping the nonlinear crystal under a non-normal direction, which is often required to achieve perfect phase matching in angle-tuned crystals. In case of uniaxial crystals the technique of angle-tuning involves a precise adjustment of the angle $\Theta_{\rm p}^0$, as explained at

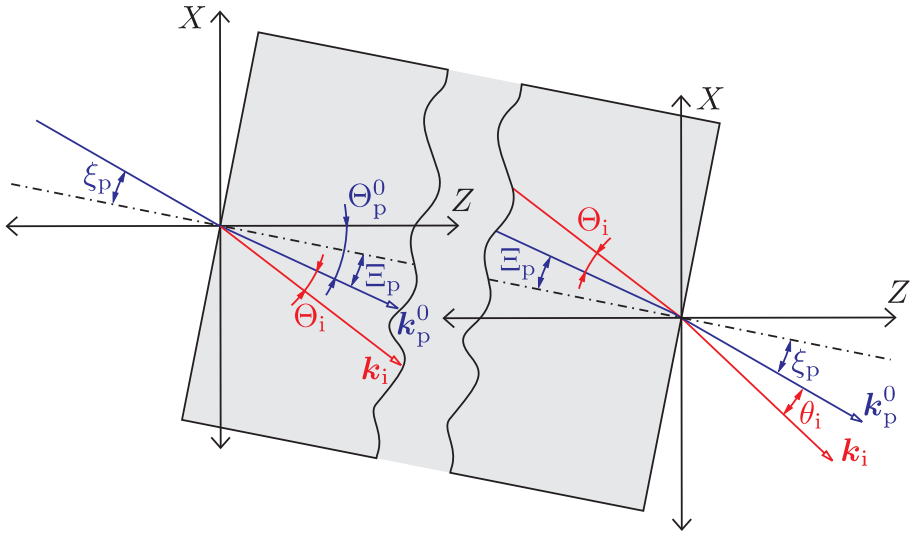

Figure 2.8: Refraction of the relevant wave vectors on the faces of the crystal; the attention is restricted only to the XZ-plane containing the central pump wave vector and the optic axis of the crystal. The internal and external angles of the pump incidence, Ξ_p and ξ_p, have to be taken into account when calculating the emission angles θ_s and θ_i of down-conversion light outside the crystal. For clarity, only the central pump wave vector $\boldsymbol{k}_p^0$ and the projection of idler wave vector $\boldsymbol{k}_i$ on the afore-mentioned plane are displayed in the figure; the definitions for the signal vector are analogous.

the very end of section 2.1. Therefore, we can confine the non-normal incidence of the pump on the crystal only to the plane containing the optic axis and the pump direction, i.e. to the XZ-plane of the principle coordinate system depicted in Fig. 2.7.

The refraction of the central pump wave vector $\boldsymbol{k}_p^0$ at the dielectric-air interface is described by Snell's law, relating the internal angle of incidence Ξ_p to the external angle of incidence ξ_p:

$$n^e(\lambda_p; \Theta_p^0, \Theta_p, \Phi_p) \sin \Xi_p = \sin \xi_p. \tag{2.67}$$

Here, we have directly set the pump polarization to the extraordinary one, in accordance with the assumptions put into force above. Due to the fact that the down-conversion emission directions are defined with respect to the central pump wave vector $\boldsymbol{k}_p^0$, the angles ξ_p and Ξ_p will play the roles of offsets in the calculation of the emission angles outside the crystal; see also Fig. 2.8. That is, the external emission angles θ_s and θ_i of the down-conversion light along the XZ-plane are given by

$$n_m \sin(\Theta_m + \Xi_p) = \sin(\theta_m + \xi_p), \quad m = s, i. \tag{2.68}$$

Obviously, the external emission angles ϕ_s and ϕ_i along the YZ-plane of the prin-

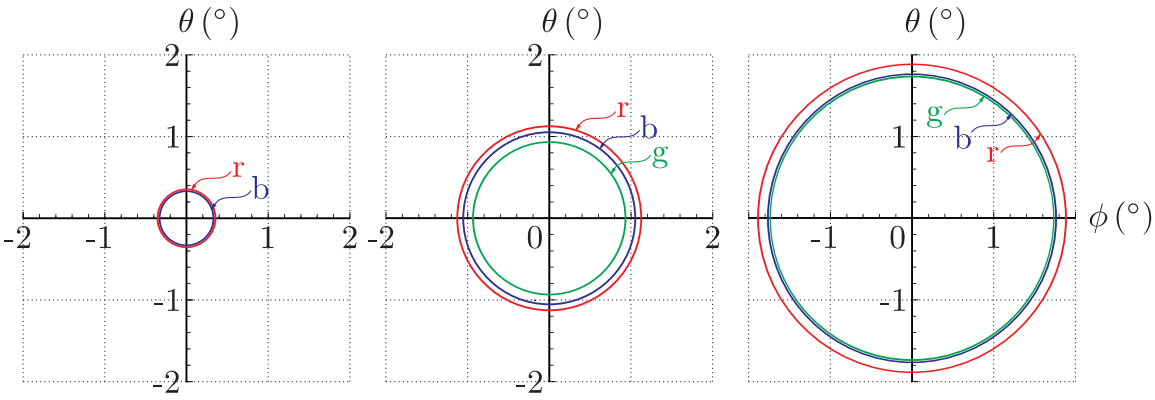

Figure 2.9: Angular distribution of down-conversion light in type I phase matching. The characteristic emission rings centered around the pump direction (determined by an angle $\phi = \theta = 0°$) at the wavelengths 780 nm (blue, "b"), 806 nm (green, "g") and 834 nm (red,"r") are shown. The three patterns from the left to the right correspond in turn to pump angles of $\Theta_p^0 = 28.95°$, $\Theta_p^0 = 29.0°$ and $\Theta_p^0 = 29.1°$. The missing green ring in the left pattern signifies that no phase-matched output at 806 nm is obtained in this configuration. The plot shows the expected emission patterns from a BBO crystal pumped at a wavelength of $\lambda_p = 403$ nm.

ciple coordinate system are given by the standard Snell's formula:

$$n_m \sin \Phi_m = \sin \phi_m, \quad m = \mathrm{s}, \mathrm{i}, \tag{2.69}$$

due to the normal incidence of the central pump wave vector on the crystal.

It is well known that the emission pattern of down-conversion light is formed by cones, which result in the characteristic rings in the plane perpendicular to the pump direction. In type I phase matching the cones are concentric around the pump direction, as illustrated in Fig. 2.9. This is, needles to say, a consequence of the equal polarization of the down-conversion photons. For the degenerate case, the signal and idler are absolutely indistinguishable and their emission patterns overlap, forming effectively a single cone. The transverse momentum conservation requires that the photons have to emerge from the crystal along the directions lying always on exactly opposite sides of this cone. For the non-degenerate emission, the cones of signal and idler photons do not overlap in general. The opening angles of the emission cones thus depend on the wavelengths of signal and idler photons, but also on the angle Θ_p^0 between the pump direction and the optic axis. The smaller the angle Θ_p^0, the smaller the opening angle of a cone. At a certain limiting angle, the momentum and energy conservation conditions are satisfied only in the collinear direction. In this case we might imagine the cones to "collapse" into a single line coinciding with the pump direction. Interestingly enough, with decreasing values of Θ_p^0 this collapse appears first for the cone representing the emission at degenerate wavelengths (compare the first two patterns in Fig. 2.9). This allows to tune the emission into a configuration,

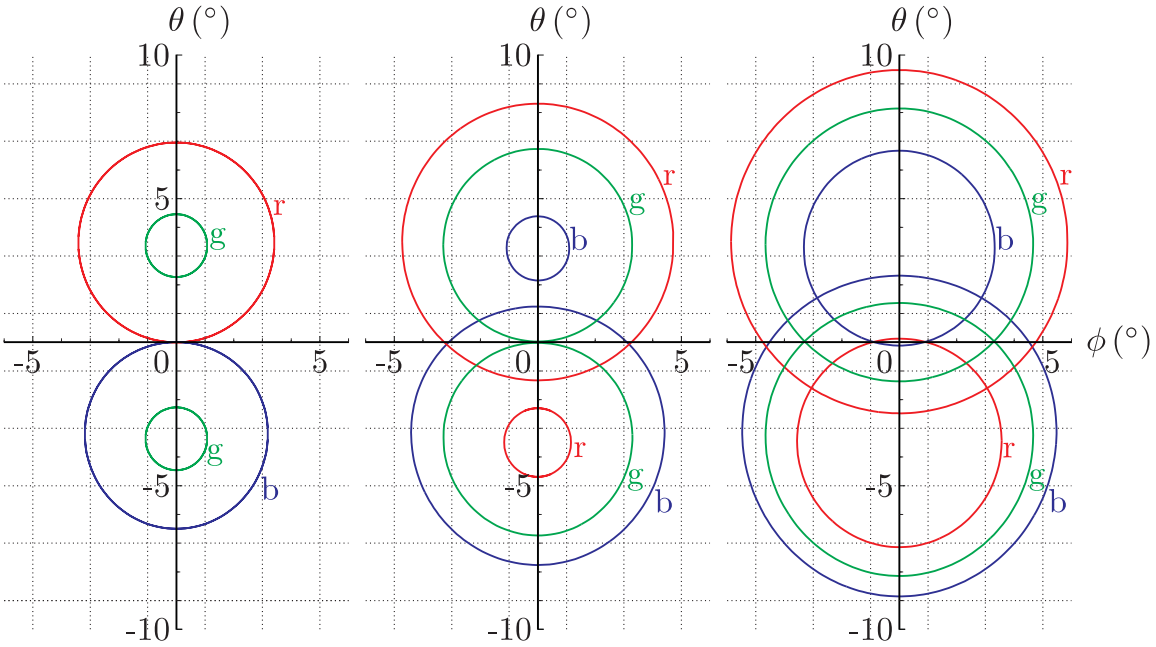

Figure 2.10: Angular distribution of down-conversion light in type II phase matching. The emission rings of extraordinary-polarized idler photons are shifted along the axis $\phi = 0°$ towards positive values of angle θ, whereas the ordinary-polarized rings of signal photons are shifted in the opposite direction. The three patterns from the left to the right correspond in turn to pump angles of $\Theta_p^0 = 41.2°$, $\Theta_p^0 = 42.0°$ and $\Theta_p^0 = 42.9°$. The blue ("b"), green ("g") and red ("r") colors show the emission at the wavelengths of 780 nm, 806 nm and 834 nm, respectively. The plot shows the expected emission patterns from a BBO crystal pumped at a wavelength of $\lambda_p = 403$ nm.

where signal and idler photons at any desired non-degenerate wavelengths emerge from the crystal collinearly with the pump light.

In type II phase matching the emission cones (or corresponding rings in far field) of extraordinary photons split from those of ordinary polarized photons and are displaced in the direction defined by $\phi = 0°$, see Fig. 2.10. This guarantees the mirror symmetry of the emission rings around this line. The emission pattern is, however, asymmetric to the axis $\theta = 0°$. In type II phase matching, the tuning of phase-matched wavelengths λ_s and λ_i or tuning of angle Θ_p^0 produce not only a change in ring radii but also a shift of ring centers along the axis $\phi = 0°$. At a specific angle Θ_p^0, the collinear situation is obtained and the signal and idler cones at given wavelengths λ_s and λ_i touch each other along the pump direction corresponding to the angle $\phi = \theta = 0°$. If the angle Θ_p^0 is decreased, the two emission cones get separated entirely. However, if the angle Θ_p^0 increases, the cones will overlap to some extent, intersecting each other along two directions.

The above discussion of the emission patterns for both type I and type II phase matching dealt with an oversimplified case of pumping the crystal with a plane wave

and the down-conversion emission at fixed wavelengths λ_s and λ_i.

As can be readily deduced from rainbow-type emission rings depicted in Figs. 2.9 and 2.10, the finite spectral bandwidths of down-conversion photons around λ_s and λ_i will manifest themselves by an angular spread of the cones to certain widths $\Delta\alpha_s$ and $\Delta\alpha_i$, respectively. Due to the concentricity and perfect circular shape of emission rings in type I phase matching, the angular widths $\Delta\alpha_s$ and $\Delta\alpha_i$ will possess radial symmetry. This cannot be, however, the case in type II phase matching, where the wavelength tuning of down-conversion photons causes a change in both, ring radius and ring center. Thus, the angular widths $\Delta\alpha_s$ and $\Delta\alpha_i$ will be a function of a radial orientation in general. Nevertheless, the effect of asymmetric broadening of emission rings is expected to be hardly visible in view of the fact that a spectral bandwidth of only several nanometers is usually phase-matched in type II SPDC (see Fig. 2.3).

We note at this point that the adopted approach to calculate the down-conversion angular distribution confines one to the case of perfect phase-matching, which assigns a unique sharp emission ring to every output frequency. The breakdown of perfect phase matching will cause the down-conversion photons at a fixed frequency to be emitted in a wider set of directions, resulting in a natural width of emission rings[9]. This natural width is, however, small in comparison to the width $\Delta\alpha_m, (m = \mathrm{s}, \mathrm{i})$ of angular spread of the phase-matched frequencies. Therefore, for standard experimental scenarios, where a finite spectral bandwidth (often natural phase-matched bandwidth) is detected, the assumption of perfect phase-matching does not pose any considerable limitation in the study of down-conversion emission characteristics.

A large wave-vector spread, which is associated with focused pumping, causes the broadening of emission rings to certain widths $\Delta\alpha'_s$ and $\Delta\alpha'_i$. Whereas for type I phase matching the radial symmetry of the angular width can be expected due to the concentricity of the cones, for type II the emission distribution acquires a spatial asymmetry. In this sense, the transition from plane-wave to focused pumping is analogous to the transition from a single down-conversion wavelength to a finite bandwidth of wavelengths. Nevertheless, the effects of focused pumping on SPDC-emission pattern, particularly the effect of asymmetric broadening, are expected to be much stronger.

For a better insight into the origin of the asymmetric broadening of type II emission rings, it is useful to investigate the effects of pump focusing in YZ-plane and XZ-plane separately, see Fig. 2.11. Focusing the pump in YZ-plane, a range of input pump angles Φ_p has to be considered, corresponding to a continuous shift of the emission ring in the ϕ direction. Consequently, a roughly uniform broadening of the rings in this direction is observed, as illustrated in Fig. 2.11(a). In the latter case, the change of the input pump angle Θ_p associated with focusing in XZ-plane, causes the twofold effect on the SPDC-emission pattern: the center of the ring is shifted in the θ direction, while the radius of the ring increases (for the shift of the ring towards

[9]The natural angular spread of a given output frequency is given by a sinc function, $\mathrm{sinc}(\Delta L/2)$, where the function Δ determines the magnitude of phase-mismatch (see e.g. [47]).

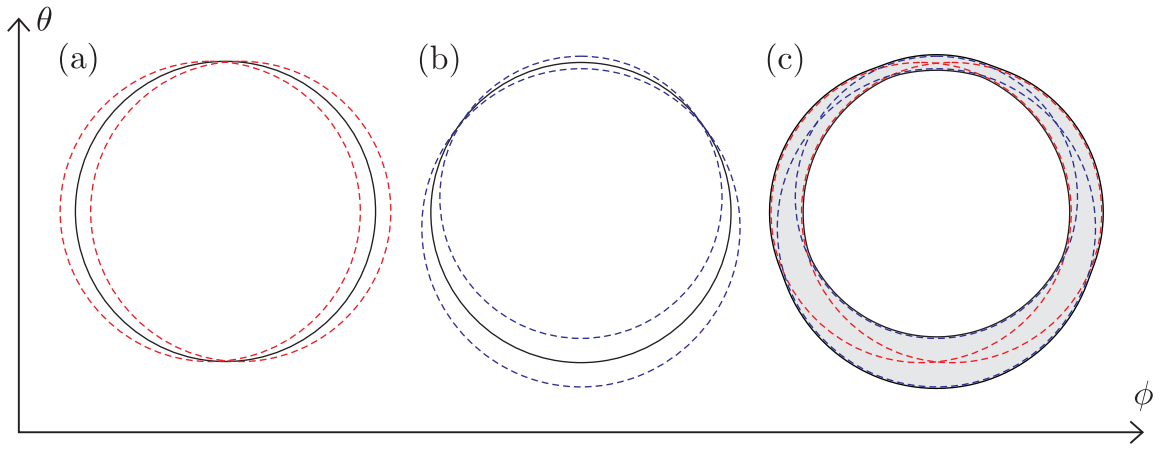

Figure 2.11: The effect of pump focusing on SPDC emission pattern. While a focusing in YZ-plane causes a roughly uniform broadening of the ring in the ϕ direction (a), the twofold effect of focusing in XZ-plane - ring shift in the θ direction and change of ring radius - is responsible for the radial asymmetry of the ring (b). The overlap (shaded area) of the patterns shows the resultant emission distribution for symmetrically focused pump (c). For a better clarity, only one of the type II emission cones is shown.

lower values of θ) or decreases (for the shift of the ring towards higher values of θ). The angular broadening is thus nonuniform over the emission rings, see Fig. 2.11(b). Combining the two cases, a strongly asymmetric emission distribution is obtained [Fig. 2.11(c)].

The origin of the described spatial asymmetry can be clarified by a more physical, but completely equivalent, argumentation [48]. Suppose the case of near-forward type II phase matching in a negative uniaxial crystal, such as BBO. Due to the anisotropy of the crystal, the ordinary (signal) photon propagates in a direction close to the pump wave vector, whereas the extraordinary photons (pump and idler) do not - they deviate from this direction by what is called a walk-off angle. The situation is graphically represented in Fig. 2.12. As a result, the idler photons emerge at the end face of the crystal from a region approximately the same size as that of the pump. The signal photons are due to lateral displacement of the pump emitted from a region, which is considerably elongated in the XZ-plane of principal coordinate system. The diffraction then dictates that the idler photons have to acquire a bigger divergence than the signal photons in the θ direction. For a near-forward emission, this implies the strong broadening of the bottom side of the emission ring, while hardly affecting the other side, in accordance with the conclusion drawn in the previous paragraph [compare Figs. 2.11(c) and 2.12].

The above phase matching argumentation served to qualitatively predict the emission distributions in different configurations including the effects of focused pump and finite down-conversion bandwidth. To study the interplay between these effects in determining the emission pattern and to quantitatively estimate the angular diver-

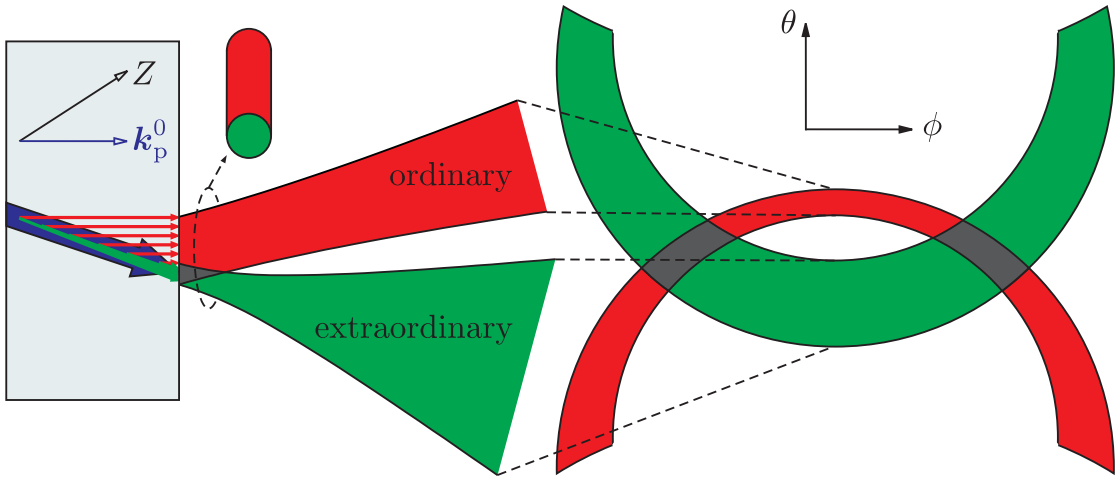

Figure 2.12: Spatial walk-off as a cause of asymmetric broadening of type II emission pattern. Assuming near-forward emission, ordinary (red) photons propagate through the crystal in the direction close to $\boldsymbol{k}_p^0$, whereas extraordinary (green) photons deviate in conjunction with the pump (represented by blue arrow). In this way extraordinary photons acquire a spatial distribution similar to that of the pump, becoming strongly divergent, when the pump is tightly focused. The angular distribution of ordinary photons is barely affected by focusing of the pump beam.

gence of down-conversion photons along a certain emission direction, the evaluation elements discussed step by step in this section are simply combined into a single procedure. In short, this procedure repeats the calculation of internal emission angles [Eq. (2.61)] and subsequent application of Snell's law [Eqs. (2.68) and (2.69)] for an array of input pump wave vectors and a range of phase-matched down-conversion wavelengths. The down-conversion emission distribution is then obtained as a weighted sum of the results from all executed evaluation runs.

The representation of the pump as an array of characteristic wave vectors is perfectly justified by the measurement of the transverse coherence area of signal (idler) field, demonstrating the spatial incoherence of the down-conversion source [49]. This was later corroborated by the theoretical analysis of second-order (amplitude) and fourth-order (intensity) coherence functions at pairs of spatially-resolved points within the signal (idler) field [50], showing that there is no spatial coherence in the source other than the limits for the angular distribution defined by the conditions of energy and momentum conservation. This suggests that the down-conversion emission from every point within the pump can be treated independently. Accordingly, the transverse cross-section of pump beam inside the crystal can be decomposed into a representative set of virtual fields, each characterized by its position $\{x, y\}$ and a wave vector $\boldsymbol{k}_p^{(x,y)}$, as illustrated in Fig. 2.13. Moreover, a weight associated with the pump intensity $I^{(x,y)}$ at the point $\{x, y\}$ is assigned to each of the fields. The allowed emission directions from each field are calculated and finally superposed with corresponding weights to simulate the effect of a gaussian pump beam.

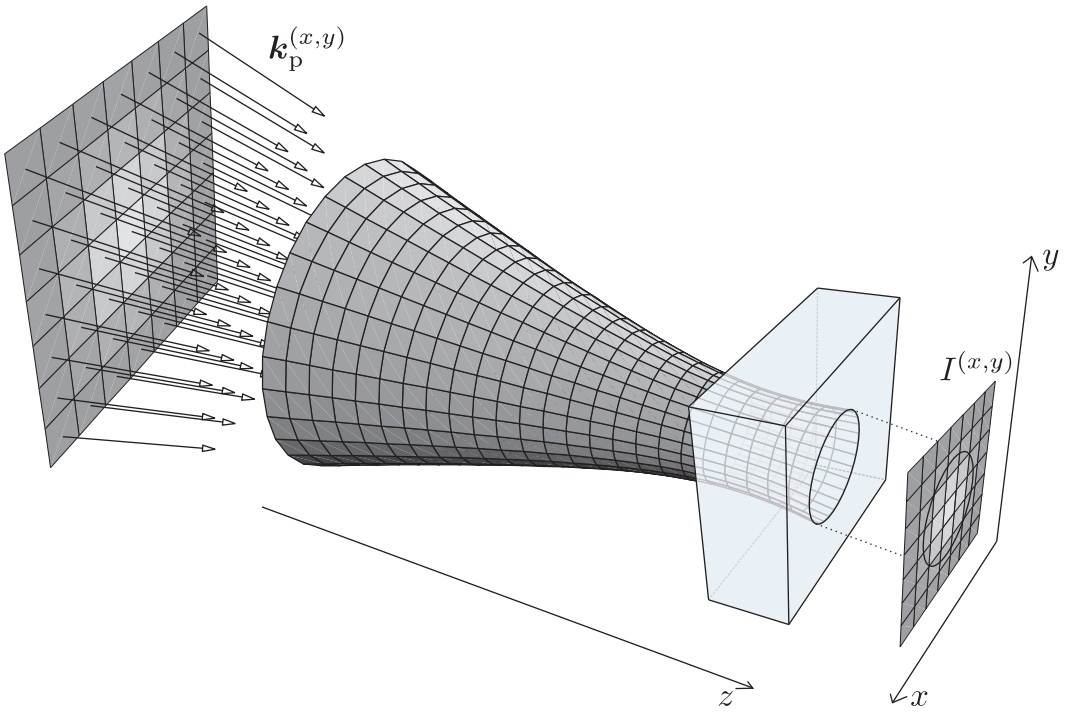

Figure 2.13: Representation of the pump beam in the study of down-conversion emission distribution. The cross-section of the pump beam in the crystal is decomposed into an array of virtual fields (represented by squares in the 2D density plot), each characterized by a position $\{x, y\}$, a wave vector $\boldsymbol{k}_{\mathrm{p}}^{(x,y)}$ and an integrated intensity $I^{(x,y)}$. The vectors $\boldsymbol{k}_{\mathrm{p}}^{(x,y)}$ are determined in the far region from the beam waist position using simple geometrical arguments. Each of the virtual fields can be treated separately in the evaluation, assuming the spatial incoherence of the down-conversion source.

Apparently, in the far field, i.e. for substantial distances from the emission plane, the source might be treated as dimensionless[10], thereby allowing the definition of the emission distribution in the phase space using the angles θ and ϕ, as already shown in Figs. 2.9 and 2.10. However, in the near field the transverse dimension of the down-conversion source cannot be neglected when determining the emission pattern. Consequently, the results have to be given for a fixed distance z from the source in the real space. In this case, we might imagine the angular distribution to be projected on an observation plane positioned at a distance z from the nonlinear crystal. Nevertheless, in either case it is straightforward to extract from the pattern the angular divergence of the down-conversion photons along any emission direction. Examples of simulated emission distributions from type II SPDC in BBO nonlinear crystal are presented in the next chapter.

[10] A condition $\rho^2/(z\lambda_{\mathrm{s,i}}) \ll 1$, where $\rho^2 = x_{\max}^2 + y_{\max}^2$ is the maximum distance of an emission point from the center of the pump beam and z is the distance from the source, can be applied in accordance with the diffraction theory to guarantee the validity of this approximation.

Finally, we add that the presented method to evaluate the emission characteristics, does not include effects arising from the depth of the nonlinear process. For substantial interaction lengths the spatial walk-off or the transverse deviation of down-conversion light in the crystal might influence to some extent the emission pattern, when determining it in the near field.

2.5 Bell state preparation

The preparation of a photon pair in one of the four possible Bell states requires that there has to be only two discrete ways of creating and/or observing such a pair. Regardless of a concrete physical embodiment, e.g., both photons must be in state $|0\rangle$ or in state $|1\rangle$. Moreover, the two alternative ways have to coherently add up to form the entangled state of the form displayed in Eq. (1.4). To achieve that, the wave functions associated with the superposed terms in the entangled state have to be made indistinguishable. Only then, the perfect correlations between the outcomes of the independent measurements on the two photons in any common basis (for example, $\{(|0\rangle + |1\rangle)/\sqrt{2}, (|0\rangle - |1\rangle)/\sqrt{2}\}$) can be always observed, thereby allowing the violation of Bell's inequalities.

It is the simultaneous emission of the two photons together with energy and momentum conservation that make the creation of entanglement in SPDC process possible [51]. Nevertheless, to observe the entanglement in various accessible degrees of freedom, such as momentum, time, polarization etc., the proper spatial and temporal selection of down-conversion photon pairs has to be always accomplished. In the following, the most common examples of entanglement encoding are concisely discussed, pointing out the advantages or drawbacks of the individual approaches.

2.5.1 Momentum and energy-time entanglement

Due to energy and momentum conservation the signal and idler photons emitted from SPDC are strongly correlated in these two continuous degrees of freedom. This is directly manifested in the presence of the functions $\delta(\nu_\mathrm{p} - \nu_\mathrm{s} - \nu_\mathrm{i})$ and $\mathrm{sinc}\,[(\epsilon k_\mathrm{p} - \epsilon k_\mathrm{s} - \epsilon k_\mathrm{i})L/2]$ in the two-photon state $|\psi^{(2)}\rangle$ [see Eq. (2.46)], thereby precluding its factorization into a product of the states corresponding to signal and idler photons. To prepare the down-conversion photons in the momentum or the energy-time Bell state, the continuous spectrum of existing creation/observation possibilities has to be reduced to just two alternatives, as it was mentioned above.

Considering first the case of momentum encoding, this can be practically achieved by selecting the two spatial mode pairs (emission directions) using pinholes [52], see Fig. 2.14. If carried out properly, the pairs of selected spatial modes, denoted here as $a1$, $b2$ and $a2$, $b1$, carry the two photons at slightly non-degenerate wavelengths

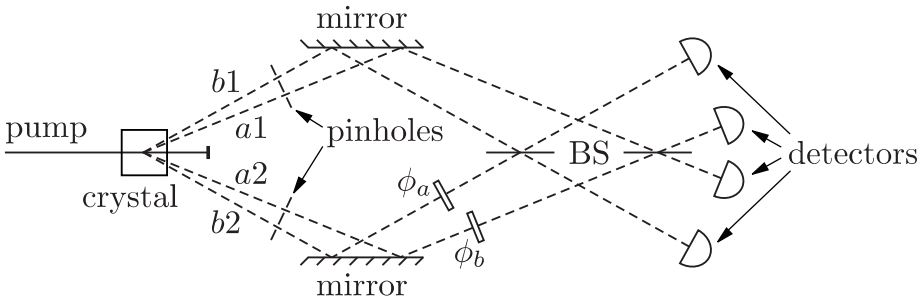

Figure 2.14: Schematic set-up of the experiment to demonstrate momentum entanglement from a down-conversion source.

λ_a and λ_b. Thus, the state of the photon pair behind the pinholes can be written as

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\Big[e^{i\phi_a}|\lambda_a\rangle_{a1}|\lambda_b\rangle_{b2} + e^{i\phi_b}|\lambda_a\rangle_{a2}|\lambda_b\rangle_{b1}\Big]. \tag{2.70}$$

This state is not entangled at this stage, yet, because the spatial modes are evidently distinguishable. If this spatial information is erased, e.g. by recombining the a-modes and b-modes at beam-splitters, the momentum entanglement manifests itself in a sinusoidal dependence of the coincidence count rate on the difference of the phases ϕ_a and ϕ_b, which can be easily controlled with a pair of phase plates inserted in the modes before the beam-splitter.

In case of the energy-time encoding, the two alternatives contributing to the Bell state can be realized by the two possible creation/detection times of down-conversion photons. This can be physically implemented by detecting the down-conversion photons behind the identical unbalanced interferometers, having their short (S) and long (L) paths [53], see Fig. 2.15. Since the path-length difference of the interferometers is designed to be much greater than the coherence length of the photons, no interference is seen in a single-detector count rate. Nevertheless, due to energy-time entanglement, the interference is observable in the rate of coincidence detections as we vary the phase difference, $\phi_1 - \phi_2$, in either interferometer. This can be understood, when closely inspecting the state of the photons within the interferometers. Due to energy conservation in SPDC the emission of any pair is uncertain within the coherence time of the pump (which is supposed to be very long) and therefore, the state can be expressed as a coherent sum of the four combinations of the passage of the down-conversion photons through the interferometers:

$$|\Psi\rangle = \frac{1}{2}\Big[|S\rangle_1|S\rangle_2 + e^{i(\phi_1+\phi_2)}|L\rangle_1|L\rangle_2 + e^{i\phi_2}|S\rangle_1|L\rangle_2 + e^{i\phi_1}|L\rangle_1|S\rangle_2\Big]. \tag{2.71}$$

The simultaneous emissions of the photons from CW-pumped SPDC in a nonlinear crystal ensures that only the first two terms in Eq. (2.71), i.e. short-short (S_1S_2) and long-long (L_1L_2) detections, are truly coincident. In practice, they can be filtered from the remaining contributions with a proper coincidence gating. We thus end up

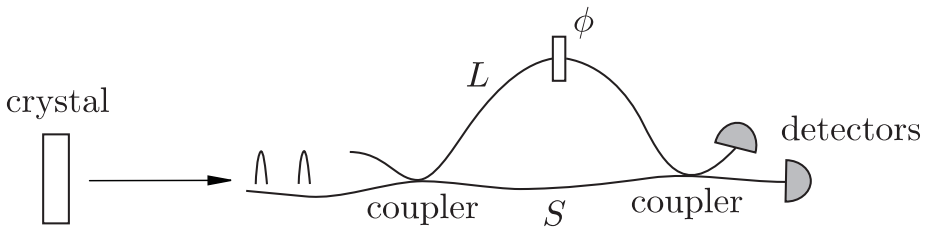

Figure 2.15: Schematic set-up of the unbalanced interferometer to analyze energy-time entanglement. In a pulsed version of energy-time entanglement, which is usually referred to as time-bin entanglement, the unbalanced interferometer serves as a pump preparation device, too. Then, the emission time of the photon pair from SPDC is given by a coherent superposition of only two discrete terms (time-bins), instead of a continuous range bounded only by the coherence length of the pump laser as in the case of energy-time entanglement.

with the maximally entangled Bell state encoded in the time basis $\{|S\rangle, |L\rangle\}$.

A notable variation of energy-time entanglement, often referred to as time-bin entanglement, has been proposed [54], avoiding the need for a CW pump laser having long coherence time. Instead, a pulsed laser is employed followed by the unbalanced interferometer, identical to those used for the analysis of energy-time entanglement, see Fig. 2.15. Here, it serves as preparation device, transforming the state of the pump photon into the superposition $\alpha|S\rangle_\mathrm{p} + \beta|L\rangle_\mathrm{p}$, provided that the pump duration is short compared to the path length difference. With such pump preparation, the emission time of the photon pair from SPDC is given by a coherent superposition of only two discrete terms (time-bins), instead of a continuous range bounded only by the coherence length of the pump laser as in the previous case. Thus, the down-conversion photons are directly created in the Bell state:

$$|\Psi\rangle = \alpha|S\rangle_1|S\rangle_2 + \beta|L\rangle_1|L\rangle_2, \tag{2.72}$$

where $|S\rangle$ and $|L\rangle$ form again the basis of our qubit space. The values of α and β can be controlled by varying the coupling ratio and phase of the unbalanced pump interferometer. Hence any two-qubit entangled state can be prepared with the method.

Although its analysis using interferometers is rather demanding, the coding of entanglement in the time basis found undeniably its practical use in fiber-based realizations of certain communication protocols, such as entanglement-based quantum key distribution or secret sharing. This is due to the inherent robustness of such a coding against birefringence of fibres, which, e.g., poses a serious problem in case of polarization encoding, that is discussed in the next part.

2.5.2 Polarization entanglement

Arguably the most illustrative and also the most popular encoding of entanglement is in polarization degree of freedom. Contrary to energy-time entanglement provided directly by SPDC process, the achievement of polarization entanglement between the

down-conversion photons necessitates an additional effort. In particular, it is the emission of the identically polarized photons from the type I phase matching and the spatiotemporal characteristics of the type II emission that do not allow for a direct extraction of polarization entanglement from either phase matching configuration. Consequently, an additional optics has to be always supplied to bring the initially separable polarization state of down-conversion photons into an entangled state.

The first experimentally examined method for producing polarization entanglement used type-I emission from SPDC [55]. The degenerate pairs of momentum correlated photons have been selected and the polarization of one of them rotated by $\pi/2$, before being superposed with the other photon on a beam-splitter. Conditioned upon the detection of one photon in either output mode of the beam-splitter (denoted as "1" and "2") the maximally entangled polarization state is obtained:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\big[|H\rangle_1|V\rangle_2 + e^{i\phi}|V\rangle_1|H\rangle_2\big], \tag{2.73}$$

where $|H\rangle$ and $|V\rangle$ stand for horizontal and vertical polarization, respectively. This method, however suffers from a necessary postselection by coincidence measurement. In fact, the total state of photons behind the beam-splitter is not entangled and it is the act of postselection of only the half of the total states, which approximates an entangled state.

To avoid this problem, two basic methods have been suggested and experimentally demonstrated. The first uses non-collinear type-II phase matching in a single crystal [56], whereas the other relies on the coherent spatial overlap of the emissions from two adjacent type-I phase-matched nonlinear crystals [57]. Nowadays, these two methods are widely used in sources of polarization-entangled photon pairs and as such deserve a good deal of attention.

Type-II source. The use of type-II phase matching for the generation of the photon pairs in polarization Bell states appears to be a natural solution. Recall just the corresponding angular emission distribution [see Fig. (2.10)]. Considering the degenerate case, the down-conversion photons are emitted along the two (orthogonally polarized) cones, which intersect each other for certain orientations of the nonlinear crystal. This intersections define two directions ("1" and "2"), along which the polarization of each emitted photon is undefined, but perfectly anti-correlated with the polarization of the other one. Therefore, it might seem that the photon pairs in the polarization-entangled state (2.73) are directly produced in this configuration. However, this is not yet true, because in the birefringent crystal the ordinary and the extraordinary photons will propagate at different group velocities and under different directions[11].

[11] Historically, it was exactly the lack of understanding of spatiotemporal properties of the type-II emission, which delayed the demonstration of the polarization entanglement in this configuration

For example, if one uses a negative uniaxial crystal, such as BBO, the extraordinary-polarized photons propagate faster than the ordinary-polarized photons inside the crystal. Identifying the horizontal (vertical) direction with ordinary (extraordinary) polarization, this causes that the detector 1 positioned in the mode "1" would fire first in a $|V\rangle_1|H\rangle_2$ term, whereas the detector 2 in the second mode would fire first in the other $|H\rangle_1|V\rangle_2$ term. Thus, the two terms are, at least in principle, distinguishable. The propagation of ordinary and extraordinary polarization under different directions in the crystal has a two-fold effect on the spatial characteristics of down-conversion emission, see Fig. 2.12. First, the extraordinary-polarized photons are emitted from a spot approximately the same size as that of the pump, whereas the emission region of ordinary photons is considerably elongated in the direction of the transverse walk-off. Second, the emission spot of the extraordinary photons is laterally displaced with respect to that of the ordinary photons. As a result, this two-fold spatial effect provides the partial label of the terms in (2.73), too.

The optimum compensation of the described spatiotemporal effect in the down-conversion crystal is achieved by inserting identical crystals of half the length in each of the two down-conversion modes [56]. If the polarization of the down-conversion light is rotated by $\pi/2$ before passing the crystals, the spatial overlap of ordinary and extraordinary emission modes is restored, thereby effectively erasing the spatial label of the $|V\rangle_1|H\rangle_2$ and $|H\rangle_1|V\rangle_2$ terms in (2.73). Analogously, the temporal retardation of the ordinary and extraordinary are exchanged in this way, introducing the temporal indistinguishability of the terms in question.

To prove the latter, we can apply the evaluation tools of section 2.3.2 to determine the joint time distributions $\mathcal{A}(\tau_+, \tau_-)$ of the biphoton associated with the terms $|V\rangle_1|H\rangle_2$ and $|H\rangle_1|V\rangle_2$. Assuming CW pumping of SPDC for convenience, the amplitude $\mathcal{A}(\tau_+, \tau_-)$ is independent of $\tau_+ = (\tau_1 + \tau_2)/2$, where τ_1 and τ_2 are individual detection times of the photon at the first and the second detector, respectively. Therefore, the analysis can be restricted only to the dependence on the time $\tau_- = \tau_1 - \tau_2$, which is interpreted as the difference in the time of the two detections. Due to the rectangular shape of $\mathcal{A}(\tau_-)$ in type II phase matching, and its asymmetry to $\tau_- = 0$ [see Fig. 2.5(b)], the two distributions do not overlap whatsoever, unless a proper compensation is applied. The temporal distribution of $|H\rangle_1|V\rangle_2$ stretches from 0 to $u_{\rm si}L$, where the dispersion parameter $u_{\rm si}$ is defined in Eq. (2.50) and L is the length of the crystal. I.e, the horizontally-polarized photon arrives at the detector 1 always after registering of the vertically-polarized photon at the detector 2, $\tau_1 > \tau_2$. Applying the analogous arguments to the term $|V\rangle_1|H\rangle_2$, it is straightforward to deduce that the corresponding distribution stretches from $-u_{\rm si}L$ to 0, as illustrated in Fig. 2.16. This proves the complete temporal distinguishability of the two terms in question. In order to achieve the perfect overlap, both distributions has to be shifted by $|u_{\rm si}L/2|$ in the proper direction. Obviously, this is exactly realized by the suggested half-length crystals, which are rotated by $\pi/2$ with respect to down-conversion crystal.

by approximately a decade, to the mid-90s.

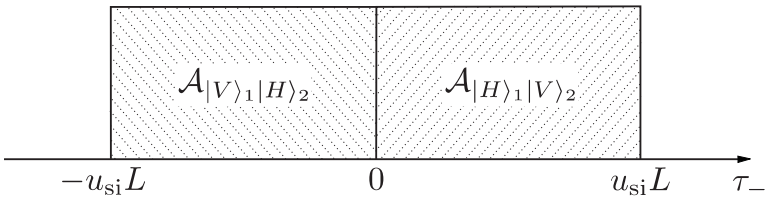

Figure 2.16: Explanation of the temporal distinguishability of the $|H\rangle_1|V\rangle_2$ and $|V\rangle_1|H\rangle_2$ terms in Eq. (2.73). Whereas, the temporal distribution of the first term stretches in $\tau_-(=\tau_1-\tau_2)$ direction from 0 till $u_{\rm si}L$, the distribution of the latter is the mirror image of the first one about $\tau_-=0$. Consequently, no polarization entanglement can be observed unless a proper compensation is applied.

The described compensation method completely erases any possible spatial and timing information of the two terms and therefore the true polarization-entangled photons in the state (2.73) are produced. Furthermore the compensation crystals can be exploited to set the relative phase ϕ in the state. If an additional half-wave plate in one of the two modes is inserted, we can prepare any of the four maximally-entangled Bell states [see Eqs. (1.3) and (1.7)] in the polarization basis.

Double crystal type I source. The second widely used method to prepare polarization-entangled photon pairs relies on the coherent spatial overlap of the two non-collinear type I emissions. Consider two adjacent nonlinear crystals, both operated in type-I phase-matching configuration and pumped with linearly polarized light. The otherwise identical crystals are oriented such that their optic axes lie in mutually perpendicular planes. For example, let the optic axis of the first (second) crystal define together with the pump direction the vertical (horizontal) plane. Due to the type-I coupling, the down-conversion process occurs only in the crystal, where the pump photon is extraordinary polarized, emitting the ordinary polarized down-conversion photons into a characteristic cone. That is, with the vertically-polarized pump the down-conversion process occurs only in the first crystal, whereas with the horizontally-polarized pump it occurs only in the second crystal. By pumping the crystals with light, linearly polarized at 45° with regard to horizontal and vertical direction, there is an equal probability that a pump photon will be down-converted in either crystal. Provided that the two emission processes are coherent with one another, which is fulfilled as long as there is no way of ascertaining whether a photon pair was produced in the first or the second crystal, the following entangled state is automatically produced:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\big[|H\rangle_1|H\rangle_2 + e^{i\phi}|V\rangle_1|V\rangle_2\big]. \tag{2.74}$$

The labels "1" and "2" again correspond to the two spatial modes, which are experimentally selected with e.g. pinholes or fibres. The relative phase ϕ is determined by the details of the phase matching and thickness of the crystals, but can be controlled

by adjusting the relative phase between the horizontal and vertical components of the pump light.

The distinguishing information, which might possibly label the emission processes and thereby reduce their mutual coherence, can be either of temporal or spatial character. The first type is usually precluded by using CW pumping. Nevertheless, if pumping with (pulsed) light of short coherence length is required, e.g. for timing purposes, the two processes could be at least in principle distinguished by the detection times. Therefore, in such a case a proper compensation is required to restore the temporal coherence of the emission processes [58, 59]. The analysis of the joint time distributions associated with the two emissions might be applied, similarly as in the previous case of the type-II source, in order to determine the suitable compensation. A particular example of such analysis is presented in the next chapter and therefore it is not discussed here further. The second possibility, which can lead to the loss of coherence between the two terms, occurs whenever the emission modes from the two crystals are spatially distinguishable. To avoid this situation, the nonlinear crystals have to be thin enough. Only then, the emission cones at certain wavelength overlap to a great extent and very pure polarization-entangled photon pairs can be obtained [57].

A remarkable feature of this source is that by a plain rotation of the linear pump polarization, any non-maximally entangled state, i.e of the form $|H\rangle_1|H\rangle_2 + \epsilon|V\rangle_1|V\rangle_2, |\epsilon| \neq 1$, can be prepared without degrading a production rate of the photon pairs. In other sources this is often possible only by manipulating the down-conversion light, thereby affecting significantly the accessible yield of the photon pairs.

Chapter 3

Sources of polarization-entangled photon pairs

This chapter describes the design and implementation of two different compact sources of polarization-entangled photon pairs using a blue laser diode as a pump source for spontaneous-parametric down conversion. Whereas the first source uses a well established concept of degenerate non-collinear emission from a single type-II nonlinear crystal, the other features a fully collinear geometry where the photon pairs at non-degenerate wavelengths emitted from two adjacent type-I down-converters are collected to one single-mode fibre and subsequently split using a wavelength division multiplexer.

3.1 Photons as information carriers

Photons are natural carriers of quantum information due to their easy distribution and the fairly weak interaction with the environment. The other non-photonic systems, such as atoms and ions, do not offer such potential, which significantly lowers their applicability for information transfer, leaving photons as the only practical alternative for the foreseeable future.

The first quantum communication schemes were based on the exchange of single photons [14]. Nevertheless, the vast majority of novel quantum communication protocols, including quantum dense coding [16], quantum state teleportation [17] or entanglement-enhanced classical communication [60] uses as a resource the photonic entanglement. Also quantum key distribution, the most advanced application of quantum communication, significantly profits when applying the entanglement-based schemes [15]. With regard to further extension of bridgeable distances in quantum communication, it even appears mandatory to apply entanglement in the quantum repeater [61] (or quantum relay [62]) architectures, where the communication channel is divided into shorter segments connected via entanglement swapping. The technology

of the generation of photonic entanglement, its distribution and detection, together with the methods of controlling and recovery of the encoded data, are therefore vital for the further progress in the field of quantum communication.

3.1.1 Challenges in quantum communication

To ensure the high-level performance of any application with entangled photons, the selection of the proper operating wavelength must be done carefully. In this context two communication systems are being currently under intensive development (for a review, see e.g. [63, 64, 65]).

The first type, which is undeniably the most promising for future terrestrial quantum communication, utilizes the transport of photons in single-mode optical fibres. To take full advantage of today's telecommunication technology, the most advantageous wavelengths turn out to be at $\lambda = 1.31$ μm and $\lambda = 1.55$ μm, i.e., at the low-dispersion and low-absorption spectral windows of fibres. The distortion of polarization due to birefringence and polarization mode dispersion in the fibres pose the crucial obstacle for the use of any kind of polarization-encoding scheme. Hence, in fiber-based communication systems energy-time or time-bin encodings of entangled photons are usually employed. They offer a good stability for long-distance applications since they are not sensitive to polarization fluctuations in optical fibers; and chromatic dispersion can be passively compensated using linear optics. Efficient and practical down-conversion sources of time-bin entangled photons at the telecom wavelengths have been developed [54], [66], however, the only applicable single-photon photodiodes made from germanium or InGaAs/InP semiconductor material show low efficiencies (typically ranging from 10% to 25 %), and high dark count noise (over 10 kHz). The combination of the poor detection and the attenuation in optical fibres[1] limit the communication distances to the order of 100 km. Without a major breakthrough in the fiber and/or detector technology or the demonstration of the working quantum repeater architecture, whose development is still in its infancy, no further extension of communication reach by an order of magnitude is to be expected.

The second type of the communication system utilizes the transmission of the photons over free space. The increase of atmosphere transmission towards infrared wavelengths, together with the peak detection efficiencies of silicon avalanche photodiodes (APD; typically up to 70%) in the visible red and the near-infrared (NIR) spectral region, suggest that the optimal operating wavelengths lie within the 700–900 nm range. Furthermore, the atmosphere is only weakly dispersive and essentially non-birefringent, allowing the use of polarization encoding, for which simple and efficient control elements and analyzers are standardly available. The terrestrial communication using free-space links suffers from many problems, which are not encountered in

[1]The minimum attenuations in standard telecom fibers at $\lambda = 1.31$ μm and at $\lambda = 1.55$ μm are of the order of 0.35 dB/km and 0.20 dB/km, respectively, corresponding in turn to the 99% loss after about 57 and 100 km.

fiber-based systems, e.g. requirement of line-of-sight path between the communicating parties, dependence of the system's performance on the weather, pollution and other atmospheric conditions etc. This generally limits the communication reach of the terrestrial free-space links to the same order as the fiber links. To fully exploit the advantages of free-space communication, it is necessary to use space and satellite technology. Quantum communication via satellites appears to be feasible even with today's technology, thereby allowing to bridge distances on a global scale. Ultimately, this solution holds a promise for establishing the global quantum communication network.

3.1.2 Quest for high-flux entangled-photon sources

One of the major challenges to successfully implement free-space communication systems is the development of practical, polarization-entangled photon sources with sufficient performance[2]. The performance of sources can be conveniently quantified in terms of their brightness, measured as a number of detected pairs per second and miliwatt of pump power and the quantum-interference visibility of polarization-entanglement. Besides reaching a high performance, the practical source has to fulfill additional criteria regarding compactness and robustness of the design, as well as low operation costs or turn-key operation requiring minimum alignment.

The development of the compact high-flux sources of (polarization-entangled) photon pairs is not important only for quantum communication, but has undeniably a great impact on the progress in the other research areas of quantum optics. Optical quantum computing, particularly with KLM (Knill, Laflamme and Milburn) architecture [68], involves as one of the key ingredients an efficient single-photon and entangled-photon generation. The tight correlations of entangled photon pairs are also of great benefit in the field of quantum metrology, e.g., for distant clock synchronization [69] or for absolute calibration of detectors without the need for a reference system [26, 70]. Other possible applications include quantum imaging with a fascinating perspective of remote sensing; or quantum lithography (and microscopy), where entangled photons are applied to write (and observe) structures at a resolution exceeding that imposed by classical diffraction theory [71]. Finally, the majority of today's multi-photon entangled sources, which are essential for advanced multi-party communication or cluster state quantum computing, rely on the interference of independently created entangled photon pairs.

Sources of polarization-entangled photon pairs made a rapid progress in the recent years. The detected photon-pair flux increased tremendously - an empirical observation suggests that the brightness doubles approximately every 12 months, see Fig. 3.1. Keeping the present pace of the brightness growth, we might expect that the

[2]For example, the preliminary feasibility studies of the space quantum experiments estimate the minimum required production rate of 10^6 pairs per second and quantum-interference visibility of at least 98 % [67].

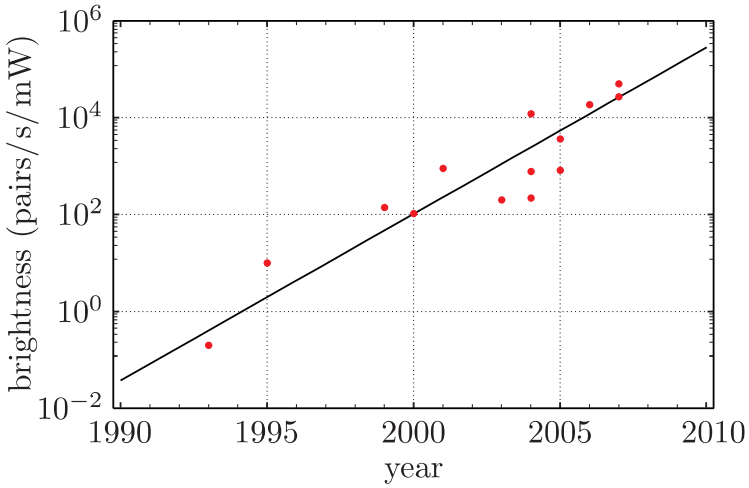

Figure 3.1: Growth of the source brightness over the recent years. The exponential fit suggests that the brightness doubles approximately every 12 months. Parameters of the sources used in the plot are listed in appendix A.2.

production rate reaches the gigahertz level before 2015. Also the practicality of the sources increases steadily. Only five years ago, large-frame ion lasers were used commonly for pumping the SPDC process. Nowadays, the new generation of blue and violet laser diodes (LDs) starts to be widely utilized, making sources more compact and economical.

3.2 Methods to generate entangled photon pairs

Since the first demonstration of a source producing polarization-entangled photon pairs based on an atomic decay, a wealth of theoretical proposals and experimental prototypes have been reported. Nowadays, the generation of entangled photon pairs is a routine lab work and the development of sources focuses largely on their simplification and/or optimization of their performance. The most widely spread way how to generate entangled photon pairs relies on the emission from the SPDC. Nevertheless, novel techniques of photon-pair generation based on the four-wave mixing process in nonlinear optical fibres or on the decay processes in semiconductor structures have been suggested, offering a great potential to outperform the traditional approaches eventually, and thus to be once widely integrated in practical applications. In the following the most common methods are briefly described, pointing out their strengths and/or weaknesses and possible future prospects.

3.2.1 SPDC sources

Presently, the two most established methods to generate polarization-entangled photon pairs utilize spontaneous parametric down conversion. The first makes use of type-II phase-matching in a single crystal [56], whereas the second relies on the coherent spatial overlap of the emissions from two adjacent type-I phase-matched nonlinear crystals [57]; (for further details see section 2.5.2). Usually, due to the

non-collinear geometry of the methods, the nonlinear crystal must be relatively short (typically in the range from 0.5 mm to 3 mm), thereby limiting strongly the potential brightness of the methods to the order of only hundreds of coincidence counts per second. Many variations of the two original proposals including confinement of the nonlinear crystal in a cavity [72] or phase-compensated collection of a wider solid angle of the emitted light [73] were reported over the past few years enhancing the yield of down-conversion photons by roughly an order of magnitude.

Birefringent phase matching in materials with a relatively high nonlinearity, such as beta-barium borate or lithium iodate ($LiIO_3$), is regularly applied for the SPDC process. However, this method fails, when the material does not exhibit sufficient birefringence at the interacting wavelengths. As an alternative, quasi-phase matching in periodically poled structures can be used, opening the possibility to noncritically phase match almost any combination of wavelengths within the transparency range of the nonlinear materials. This enables to access the highest nonlinear coefficients of many materials, such as lithium niobate ($LiNBO_3$), lithium tantalate ($LiTaO_3$) or potassium titanyl phosphate ($KTiOPO_4$), thereby enhancing the overall conversion efficiency of the SPDC process.

Different configurations of sources using bulk periodically poled crystals were investigated over the recent few years. The best results were reported in collinear geometry using bi-directional pumping of a single periodically poled crystal [74, 75] or coherent overlap of the emissions from two crystals [76, 77, 78]. This way, the brightness increased by at least one order of magnitude in comparison to sources using BBO crystals, reaching values above 10^4 detected pairs/s/mW, while at the same time keeping the high purity of polarization entanglement. A further boost of photon-pair yield might be expected, when exchanging bulk crystals for nonlinear periodically poled waveguides. Due to the field confinement, waveguides provide an improved mode overlap of the interacting waves, leading to an enhancement of the conversion efficiency. Conversion efficiencies of up to 10^{-6}, roughly 4 orders of magnitude more than that obtained with BBO crystal, were already demonstrated, though without the possibility for direct generation of polarization entanglement [79, 80].

3.2.2 Fiber sources

Four-wave mixing (FWM) via the third-order ($\chi^{(3)}$) nonlinearity of optical fibers can be utilized to generate correlated photon pairs at unequal wavelengths [81]. The generated pairs are predominantly co-polarized with the pump, which can be exploited for obtaining polarization entanglement by bi-directional pumping of a fiber Sagnac loop [82]. This geometry has the advantage that the counter-propagating pairs remain in a coherent superposition without the need for any phase or path adjustments. Substantial interaction lengths together with the strong mode confinement lead to unprecedented brightness [83]. However, the occurrence of significant spontaneous Raman background makes the actual production of high-purity polarization entanglement complicated. Usually, pumping at very low powers, a careful filtering of

true correlated photon pairs and an operation at liquid nitrogen temperatures is required, to reach near-to-unity quantum-interference visibility [84]. This problem can be somewhat avoided by pumping the fiber in normal dispersion regime generating photons at widely spaced wavelengths (typically by hundreds of nanometers) outside the Raman scattering region. In either case, the need of mode-locked picosecond lasers for pumping the FWM process together with the difficulties in extracting high-purity polarization entanglement make today's fiber sources less suitable for practical applications. Nevertheless, the achieved high production rates suggest their possible future applicability in multi-photon quantum information experiments [85].

3.2.3 Semiconductor sources

Semiconductor quantum dots became widely utilized as optically and electrically driven sources of single photons on demand. Few years ago, the biexciton decay in a single quantum dot via an intermediate exciton level was proposed to provide a source of triggered, entangled photon pairs [86]. In contrast to afore-mentioned methods based on SPDC and FWM processes, which generate probabilistic numbers of photons pairs, the biexciton decay produces no more than two photons per excitation cycle. This makes such a compact and integrated device a favorable alternative to other sources, with the additional benefit of being easily implemented using simple, LED-like technologies.

Practically, structure asymmetries lead to polarization dependent splitting of the intermediate exciton level, resulting in only polarization correlated photons. However, two schemes to eliminate the polarization splitting by control of growth or application of magnetic field, have enabled the recent observation of polarization-entangled photons, although at very poor quality [87]. Many tremendous engineering challenges still remain in order to realize a practical quantum dot source of entangled photons. Improvements must be made to the efficiency of the device, to the frequency of operation, and, most importantly, to the degree of entanglement.

3.3 Compact non-collinear type-II SPDC source

To generate photon pairs in the NIR spectral region compatible with high-efficient silicon APDs and the low-absorption window of the atmosphere, the pump-beam wavelength for SPDC has to be shorter than 450 nm. This requirement generally led to the use of large-frame ion lasers, which, due to their complexity and high operating costs are not suitable for practical applications. Hence, a great deal of attention has been recently devoted to replace these cumbersome and expensive lasers. The first step towards this goal have been undertaken by Volz *et al.* [88], who successfully demonstrated the generation of polarization-entangled photon pairs in NIR using a frequency doubled, red LD. The advent of a new generation of gallium nitride based blue LDs promised a further simplification of the system. The first

reported implementation, however, did not reach the expected brightness and high-purity polarization entanglement [89]. It was therefore our goal to demonstrate that the performance of sources using low-cost LDs can be comparable to those using CW ion lasers [90].

3.3.1 Method

For the generation of polarization-entangled photons we use a well-established technique based on SPDC emission from a single type II phase-matched nonlinear crystal. For closer details of this method, addressing particularly the issue of entanglement production, we refer to section 2.5.2. Since in many applications a well-defined spatial mode is highly desirable, in our source single-mode fibres are used for coupling of the down-conversion light. To increase the yield of photon pairs we aim at optimizing the photon-pair collection efficiency into single-mode fibres. Due to a limited laser-diode pump power available for SPDC, this issue is of particular importance in our source.

The problem of maximizing the coupling efficiency is investigated at length for type-I phase matching in both CW and pulsed pumping regime [91, 92]. The fibre coupling of type-II emission is less explored mainly due to difficulties in determining the angular distribution of SPDC light along the intersection of the output rings. The first work along this line was reported by Kurtsiefer *et al.* [93], who suggested a simple hands-on method for determining the optimum parameters of the pump and the collection optics. The method involves adjusting the crystal orientation till the perpendicular intersection of the SPDC rings is provided. Then, emission modes along the intersection lines might be approximated by gaussian profiles with a divergence, which can be easily determined from the fixed relation between the emission direction and the output wavelength. To maximize the yield of fibre-coupled photon pairs, collection modes with the same divergence are chosen. Furthermore, the pump beam waist size is suggested to match the size of the target collection mode in the crystal. Later Bovino *et al.* [94] presented a more rigorous approach to the problem based on maximizing the overlap between the two photon amplitude $\mathcal{A}$ of the entangled photon state and the field distribution of single-mode fibres. This allowed to study the interplay of the major experimental parameters, including crystal length, magnification of the coupling system or fibre mode field diameter, in determining the coupling efficiency. Both approaches have been verified experimentally, demonstrating a high net coupling efficiency.

Here we propose yet another approach to the problem. Even though it resembles the method proposed in [93] to some extent, it avoids using therein applied simplifications, including rotational symmetry of the down-conversion rings or plane-wave pumping. Using the evaluation tools introduced in section 2, our approach takes fully into account the focusing geometry of all three interacting fields. Contrary to [93], our results suggest that the maximum yield of fibre-coupled pairs is not achieved if the pump beam waist size matches the size of the target collection mode in the nonlinear crystal; see also [94].

Our fibre-coupling strategy might be divided into a few successive steps: (i) determination of the optimum pump beam divergence; (ii) evaluation of the emission characteristics; and (iii) determination of the collection mode. In the following the individual steps are discussed in more detail.

Pump-beam dependencies. The first important observation relevant to the determination of the optimum pump beam divergence α_{p} for SPDC is the spatial incoherence of the down-conversion source. If the transverse width of the source is too large, the collective emission will be spatially multimode. This explains the impossibility of efficient fibre-coupling of the photons in this regime.

The need of a focused pump for successful collection of down-conversion photons has been demonstrated in several theoretical and experimental works [48, 93, 94, 95]. The only theoretical model predicting the opposite, i.e., achieving high coupling efficiencies if the pump-beam waist size w_{p} and the collection-mode divergence α_C are chosen large enough, has been suggested recently [96]. To disprove this hypothesis and show that indeed the size of the emission region has to be sufficiently small, we apply the evaluation steps described in section 2.4 and calculate the distribution of down-conversion light with a certain spectral bandwidth. Similarly as in Kurtsiefer's optimization method [93], we analyze the configuration for a perpendicular intersection of the SPDC rings. This appears to be a convenient choice for achieving efficient fibre-coupling due to an approximate rotational symmetry of the emission modes. Next, from the calculated distributions of the two intersection regions we single out only emission directions restricted within a small interval of polar angles ϕ (or, alternatively within a small interval of azimuth angles θ). From a physical perspective this step corresponds to a selection of down-conversion light from the intersection regions using a very narrow vertical (or horizontal) slit apertures. Using this procedure, we obtain a representative set of light rays, which are to be coupled into a single-mode fibre. To this end, the collection optics has to be designed first, matching the angular width of the emission modes to a gaussian distribution of the receiving modes. This distribution can be easily determined from a mode field diameter (MFD) of single-mode fibres. To investigate the actual process of fibre-coupling, a standard ray-tracing method allowing us to track the path of down-conversion photons through the collection lens is applied[3]. This way, we arrive at clearly different regimes of fibre coupling for a focused and collimated pump [compare Figs. 3.2(a) and 3.2(b)]. In the first case, the coupling lens concentrates the down-conversion rays to a spot of several microns in diameter, which is compatible to the core sizes of standard fibres with single-mode operation in NIR spectral region [for the parameters in Fig. 3.2(a) the focused spot has the diameter of ≈ 5.5 μm]. However, for the second case, a roughly one order of magnitude larger diameter of the focus is observed, suggest-

[3]We note that even though the methods of geometric optics approach cannot be used for a rigorous investigation of fibre-coupling efficiencies [97], the ray-tracing approach clearly demonstrates the feasibility of coupling the down-conversion light into single-mode fibres.

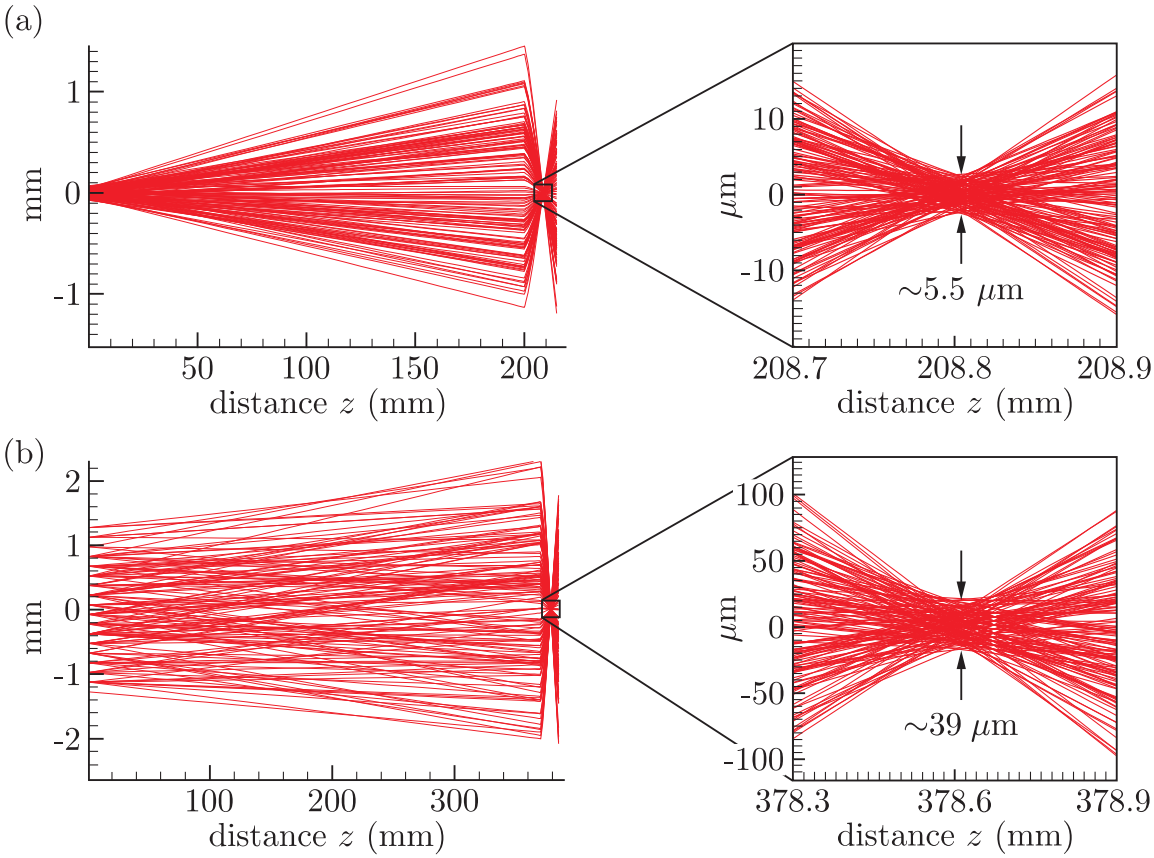

Figure 3.2: Ray tracing of representative set of down-conversion emissions ($\lambda = 806$ nm, $\Delta\lambda = 5$ nm) through the aspheric coupling lens in different regimes of pumping: (a) for focused pump with the divergence of $\alpha_p = 1.9$ mrad and (b) for almost collimated pump with $\alpha_p \approx 0.1$ mrad. An aspheric lens with effective focal length of $f = 7.5$ mm at a distance of $z = 210$ mm and $z = 370$ mm from the crystal is used in (a) and (b), respectively. The distances were determined to optimally match the calculated down-conversion angular divergence to the numerical apertures of the receiving mode defined by the MFD $= 5.2$ μm of a single-mode fibre. SPDC emission from BBO crystal cut at $\Theta_p^0 = 42.9°$ and pumped at a wavelength of $\lambda_p = 403$ nm is assumed in the plots.

ing a transverse multi-mode character of the emission modes [for the parameters in Fig. 3.2(b) the spot diameter is ≈ 39 μm]. One has to face the same situation, if a nonlinear-crystal is moved well beyond the Rayleigh range of the focused pump - it is the size of the pump cross-section inside the nonlinear crystal, which predetermines the feasibility of efficient fibre-coupling of down-conversion light.

Notably, the results of ray-tracing also suggest that if down-conversion photons are collected into spatially multi-mode channels[4], such as a pair of circular apertures

[4]In multi-mode collection channels the emission angles of down-conversion photons are resolvable. This is in contrast to single-mode channels, where all the information on emission angles is erased.

in the far zone of the source, a collimated pump might be even preferred [56]. Due to the reduced divergence of the emission modes in this regime, an increased collection rate of down-conversion photons is achieved for a given opening of the apertures. Thus, a collimated pump should yield a higher degree of polarization entanglement for a given detected photon-pair flux than a focused pump [48, 98].

The rule of increasing fibre-coupling efficiency with decreasing size of pump-beam waist inside the nonlinear crystal, however, fails below certain critical waist sizes. Recall that a large wave-vector spread, which is associated with tight focusing causes the asymmetric broadening of the emission rings [for further explanation see section 2.4]. As a result, the intensity distribution within the intersection of the rings loses its approximate rotational symmetry and becomes elongated in one direction, see Fig. 2.12. Thus, it can be mapped to the receiving modes of optical fibres only with a limited efficiency. We note, that the integration of tailored cylindrical optical elements into coupling optics can restore a high fibre-coupling efficiency. This is, however, experimentally demanding and not practical.

To determine the critical pump beam waist size, which still leads to a tolerable emission-mode asymmetry, a series of down-conversion emission distributions have been evaluated for different values of pump-beam divergence α_{p}, see Fig. 3.3. As expected, the gradual transition of the ring intersection distribution from an initially circular shape towards an elongated elliptical profile is observed. For the input divergence of 2 mrad, the aspect ratio of the elliptical profile reaches the value of about 0.58[5]. This corresponds to the maximum overlap between the emission modes and the receiving modes of above 0.9, which we still consider as a tolerable value. For the input divergence of 3 mrad, the aspect ratio is reduced to ≈ 0.42, resulting in a maximum overlap of 0.85, which is below the set limit.

The asymmetry of the emission mode does not lead only to a reduction of fibre-coupling efficiencies, but also limits the maximum accessible degree of polarization, eventually. The effect arises, if the collection modes are dissimilar, resulting in fibre coupling of one predominant polarization state and consequently, the detection of nonmaximal entanglement [48]. Furthermore, the increase of pump-beam divergence far beyond 1–2 mrad (provided that crystals with lengths in $\sim$ mm range are used) was shown to be accompanied with a significant broadening of down-conversion spectra [42], which is unwanted with regard to practical applications as well. In summary, all the above argumentation suggests that the best regime of source operation is obtained for pump-beam divergence α_{p}, ranging between 1 and 2 mrad.

SPDC emission dependencies. The fixed relation between the emission direction and the output down-conversion wavelength allows a pure geometrical definition of the fibre-coupled spectral bandwidth $\Delta\lambda$ by properly designing the collection modes. In principle, any bandwidth $\Delta\lambda$ (of course, below the naturally phase-matched width

[5]The obtained values of aspect ratios are independent of the considered down-conversion spectral width. Thus, any reasonable value can be entered in the evaluation of the emission distributions.

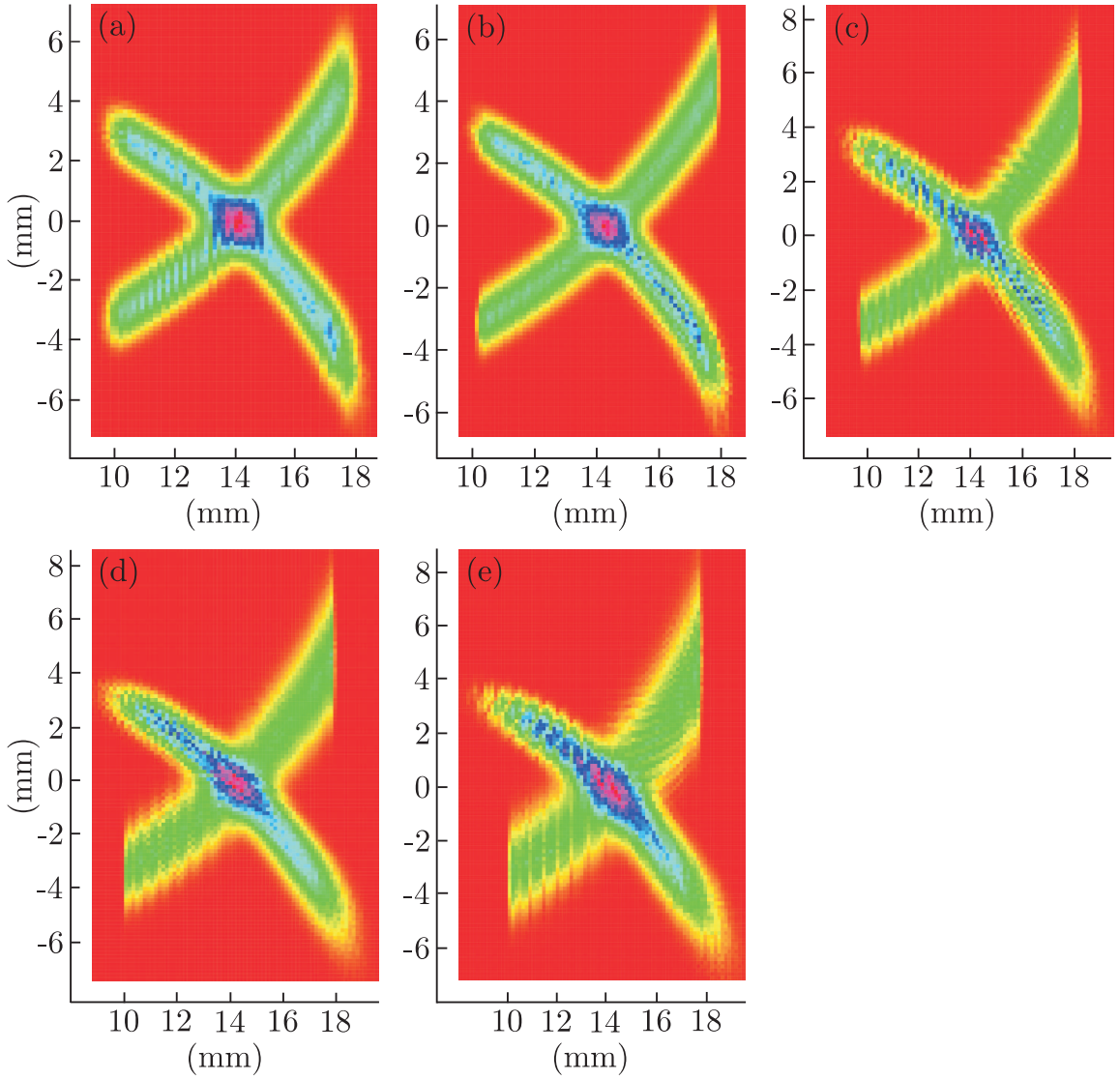

Figure 3.3: Simulated down-conversion emission distributions restricted to the immediate vicinity of the intersection of the rings as a function of the pump-beam divergence: (a) $\alpha_p = 0.1$ mrad, (b) $\alpha_p = 1.0$ mrad, (c) $\alpha_p = 2.0$, (d) $\alpha_p = 3.0$ mrad, and (e) $\alpha_p = 4.0$ mrad. The patterns show the distributions determined at a distance of $z = 250$ mm from the BBO crystal ($\Theta_p^0 = 42.9°$); the size of one pixel corresponds to 140 μm in real space and the zero of the coordinate system is given by the position of the pump beam ($\lambda_p = 403$ nm).

for a given crystal length, see Fig. 2.3) can be freely chosen in this way and thus, no interference filters reducing the resultant efficiency of the source are required.

Fixing the parameters of the pump beam, the corresponding emission distribution can be calculated at any distance from the nonlinear crystal for a given spectral bandwidth $\Delta\lambda$, which is aimed to be collected into the single-mode fibre. The eval-

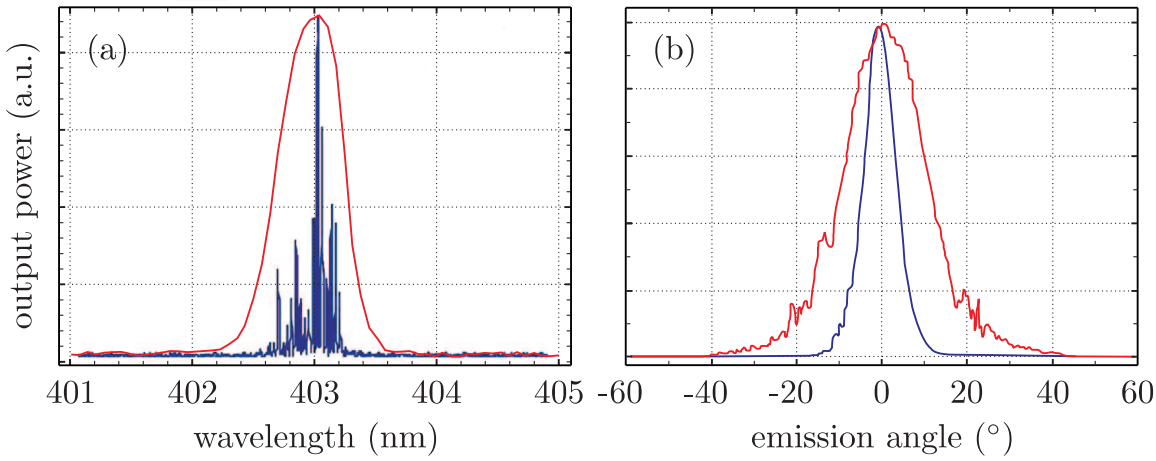

Figure 3.4: Basic emission properties of violet LDs. (a) The spectrum exhibits multiple-peak structure (blue line; taken from [99]) with an aggregate FWHM bandwidth of roughly 0.5 nm (red line; measured). The broadening of measured spectral profile due to a spectrometer resolution of 0.15 nm is subtracted from FWHM. (b) The angular emission distributions in the two main planes show nearly ideal Gaussian profiles; taken from [99]. FWHM divergences reach typically the values of $\sim 8°$ (blue; plane parallel to the diode junction) and $\sim 22°$ (red; plane perpendicular to the diode junction).

uation is repeated several times at different distances and the geometrical width of the emission mode is determined by fitting the ring-intersection distribution with a gaussian profile at each of them. This way, we can readily infer the divergence of the emission mode α_E.

Collection mode. We now define Gaussian collection modes, which are aligned with the intersection directions of the emission rings. In order to maximize the fibre-collection efficiency of down-conversion light with a desired bandwidth $\Delta\lambda$, the divergence of collection modes must match that of the emission modes [93], i.e. we set $\alpha_C = \alpha_E$. This determines the waist size of a Gaussian collection mode of $w_0 = \lambda_{\mathrm{s(i)}}/(\pi\alpha_C)$, which is optically mapped using a coupling lens to the MFD of the collection fibre.

3.3.2 Implementation

Pump-beam preparation. The pump beam for SPDC is provided by a violet transverse single-mode LD (Nichia, No. NDHV310ACA) with a maximum optical output power of 30 mW at about 60 mA driving current. Alternatively, a 60 mW LD (Nichia, No. NDHV310APC) is applied as the pump. The diode is mounted in an aluminium housing, which is temperature stabilized with a Peltier element to about 20 °C. Both types of diodes operate at $\lambda_{\mathrm{p}} = 403$ nm and exhibit multiple-peak spectra with an aggregate FWHM ranging from $\Delta\lambda_{\mathrm{p}} = 0.4$ nm to $\Delta\lambda_{\mathrm{p}} = 0.6$ nm, depending on the particular LD [see Fig. 3.4(a)]. This spectral bandwidth corresponds to a coherence

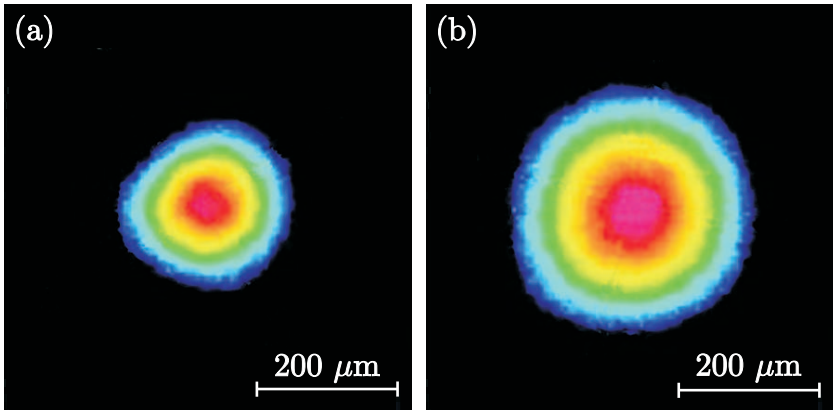

Figure 3.5: A typical example of the beam-shaped violet-LD output captured with a CCD camera. The snapshots of the beam profile at (a) beam waist position, and at (b) 240 mm distance from the waist position are shown. Using cylindrical lenses a nearly circular beam is achieved, exhibiting the ellipticity factor of > 0.95 in a wide region around the beam waist position.

time of roughly 1 psec. Besides, a weak broadband in-line emission centered in the visible red spectral range is observed.

The angular emission distributions of the laser-diode light show nearly ideal Gaussian profiles [see Fig. 3.4(b)], suggesting that no mode filters are required to improve the quality of the beam. The FWHM beam divergences typically reach $\theta_{\parallel} = 7-10^{\circ}$ and $\theta_{\perp} = 20-26^{\circ}$ in the directions parallel (usually termed as slow axis) and perpendicular (fast axis) to the diode junction. A quality factor, M^2, defining the deviation of the laser beam from a theoretical Gaussian ($M^2 = 1$) was measured along the slow and fast axes using the four-cuts method [100], yielding the values of $M^2_{\parallel} \sim 1.3$ and $M^2_{\perp} \sim 2.3$, respectively. The radial asymmetry of the angular divergence, together with the mismatch of the M^2 factors along the slow and fast axes make the laser-diode beam highly astigmatic. To correct the astigmatism, usually an adjustable anamorphic prism pair or cylindrical lenses are utilized. The latter technique delivered better results in our case and permitted complete removal of the astigmatism inherent to the laser-diode light. This is simply accomplished by proper focussing of the lenses in each direction. First, a pair of lenses, a positive aspheric lens (focal length $f = 4.6$ mm) and a negative singlet lens (typically $f = -15$ to -30 mm), forming a Galilean-type telescope is used to focus the slow axis to the desired size. Then, a cylindrical lens or lens pair (typically $f = 150$ to 350 mm) is used to match the size and the position of the beam waist in the plane of the fast axis. This way we are able to focus the laser beam to waist radii between 50 μm and 300 μm at a distance of 180–240 mm from the laser diode. The smaller focal length of the negative lens results in a shortening of this distance, however at the expense of stiffening the positioning tolerances. A typical example of the achieved beam profiles of the focused laser-diode beam is shown in Fig. 3.5. For the operation of the non-

collinear type II source we choose the waist radius of $w_\mathrm{p} = 75$ μm, corresponding to a pump-beam divergence of $\alpha_\mathrm{p} = 1.7$ mrad. In accordance with the conclusions drawn above, such a divergence should allow an efficient coupling of down-conversion photons into single-mode fibres.

Nonlinear crystal and SPDC emission. We use beta-barium borate (β-BaB_2O_4 or BBO; basic characteristics are given in appendix A.1.1) as a nonlinear material for SPDC. The crystal with dimensions $7 \times 7 \times 2$ mm^3 is cut for type II collinear phase matching at an angle of $\Theta_c = 42.0°$ ($\Phi_c = 29.0°$). The perpendicular intersection of the emission cones at the degenerate wavelengths of $\lambda_\mathrm{s} = \lambda_\mathrm{i} = 806$ nm is obtained for a pump orientation of $\Theta_\mathrm{p}^0 = 42.9°$ with respect to the optical axis (see green rings in the altogether right pattern of Fig. 2.10). The corresponding intersection lines form an external angle of $\phi = 3.26°$, measured with regard to the pump direction.

For the crystal length of $L = 2$ mm the output phase-matched spectral width is expected to reach $\Delta\lambda \approx 5$ nm, according to Fig. 2.3. The finite pump-beam coherence time of ≈ 1 psec contributes to a broadening of this width only negligibly, see Fig. 2.4. Aiming for all the phase-matched bandwidth of 5 nm to be collected into the fibres, the emission-mode divergence of $\alpha_E \approx 0.30°$ is determined from the down-conversion distributions calculated at different distances from the BBO crystal [see Fig. 3.6]. The pumping of the crystal by a Gaussian beam with a waist radius of $w_\mathrm{p} = 75$ μm is assumed in the evaluation. The fibre-coupling optimization method requires $\alpha_C = \alpha_E$, which fixes the waist size of the Gaussian collection mode to $w_0 = 59$ μm.

The non-collinear geometry of the nonlinear process puts the constraints on the maximum depth L_max of the down-conversion emission, which is still possible to collect into single-mode fibres. The increase of the crystal length beyond L_max brings no further gain in the number of collected photon pairs. Using simple geometrical arguments one can show that the maximum depth equals to $L_\mathrm{max} = 2w_0/\sin\phi$, see Fig. 3.7. For the parameters of $w_0 = 59$ μm and $\phi = 3.26°$ this implies the maximum usable crystal length of about $L_\mathrm{max} = 2.1$ mm. This agrees well with the actually chosen crystal length of $L = 2$ mm.

Compensation and fiber coupling. Due to birefringent nature of BBO material the horizontally- and vertically- polarized down-conversion photons propagate at different group velocities and under different directions. This provides a spatiotemporal distinguishability of the two created polarization states[6] and thus leads to non-maximal entanglement [for further explanation see section 2.5.2]. To compensate the effect and to obtain polarization-entanglement for all wavelengths in the acceptance spectrum

[6]The maximum time delay and the maximum lateral displacement of down-conversion photons at the output face of a 2-mm-long crystal amount to 382 fs and 145 μm, respectively. This has to be compared to the photon coherence time and coherence width to estimate the extent of the distinguishability.

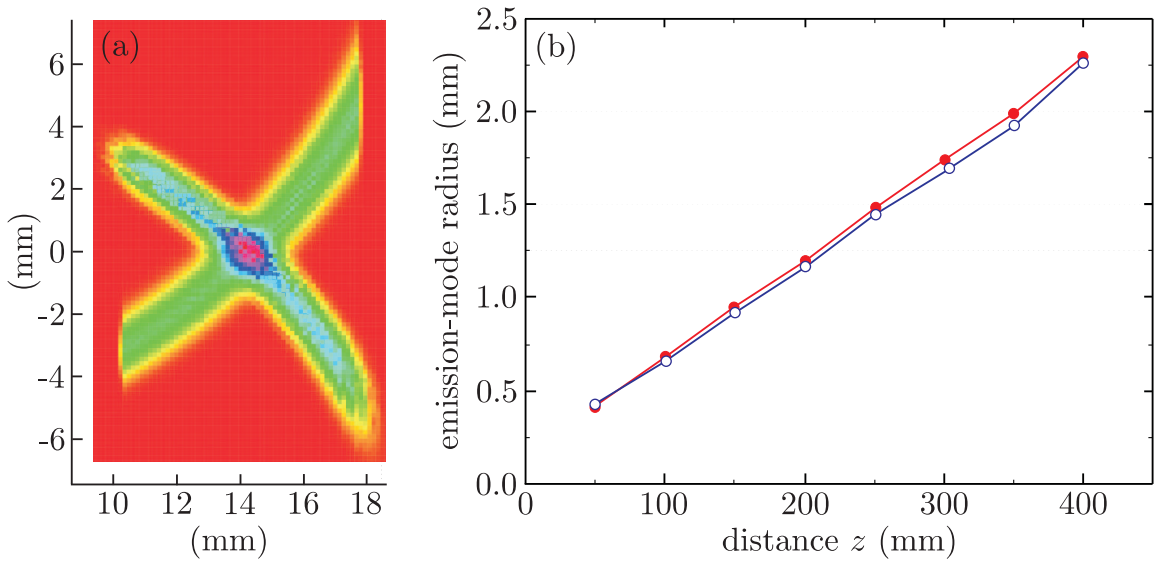

Figure 3.6: Emission characteristics of SPDC light calculated for the actual parameters of the source. Figure (a) shows the intensity distribution of SPDC light with the central wavelength of 806 nm and the bandwidth of 5 nm, which is determined at the distance of 250 mm from the BBO crystal. The size of one pixel corresponds to 140 μm in real space and the zero of the coordinate system is given by the position of the pump beam; the parameters of the pump are: $w_{\mathrm{p}} = 75$ μm, $\lambda_{\mathrm{p}} = 403$ nm. Figure (b) shows the linear increase of the emission-mode radius with the distance from the crystal in the horizontal (red full points) and in the vertical (blue open points) directions. The data are obtained by fitting the ring-intersection distributions with gaussian functions.

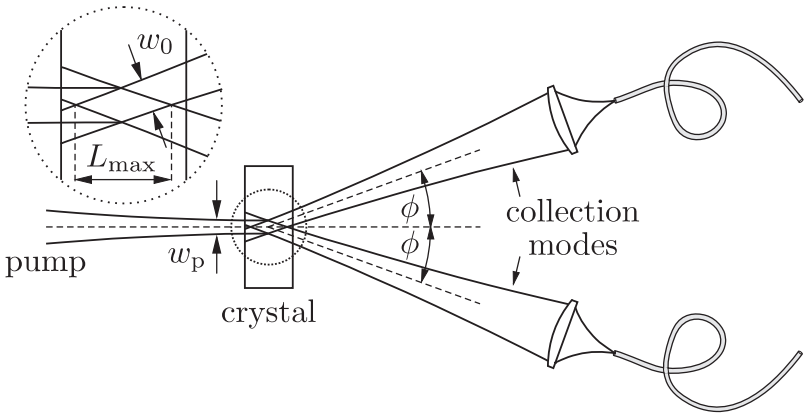

Figure 3.7: The sketch of the non-collinear geometry of SPDC process. The waist size w_0 and the relative orientation (determined by the angle ϕ) of the collection modes define the maximum depth L_{max} of the down-conversion emission, which is possible to collect with fibres. Thus, the depth L_{max} limits the practically usable crystal length.

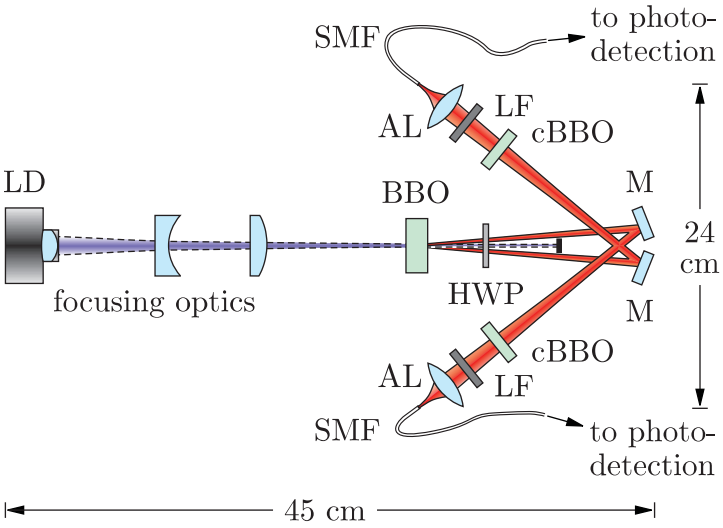

Figure 3.8: Schematic set-up of the compact non-collinear type-II SPDC source: half-wave plate (HWP), mirror (M), compensation BBO crystal (cBBO), longpass filter (LF), aspheric lens (AL), single-mode fibre (SMF).

of down conversion photons, additional BBO crystals of length 1 mm preceded by a half-wave plate are inserted into the emission modes of the photons.

The photons are coupled into single-mode fibres at a distance of about 270 mm from the emission point. This spacing is determined by the aspheric coupling lenses with focal length of $f = 11.0$ mm, the calculated waist size of the collection modes of $w_0 = 59$ μm, and the MFD of the used optical fibres of 5.2 μm.

Set-up overview. The sketch of the source set-up is shown in Fig. 3.8 (the photo of the tested source is included in appendix A.3). The laser beam of a free-running LD at 403 nm is focused into the type II phase-matched BBO crystal and produces pairs of polarization-entangled photons at the degenerate wavelength of 806 nm, which are collected into single-mode fibres. Two long-pass filters with a cut-off wavelength at 715 nm are used to block the residual violet light. For compensation of the walk-off, two additional BBO crystals preceded by a half-wave retarder are used. To keep the source compact, two mirrors are used to fold the paths of the down-conversion photons.

3.3.3 Results

The two essential parameters characterizing the performance of sources are the quality of the produced polarization entanglement and the brightness. The first is usually determined as a visibility of correlation curves in complementary bases and the latter as a number of detected pairs per second and milliwat of pump power. With regard to some applications requiring a supply of narrow-band photons, such as for addressing atoms, a better figure of merit is spectral brightness, which includes in its definition the spectral bandwidth of the photons. A further benchmark quantifying the performance of sources is the degree of violation of the CHSH inequality in a fixed measurement period. Large speed of violation is possible only if both the

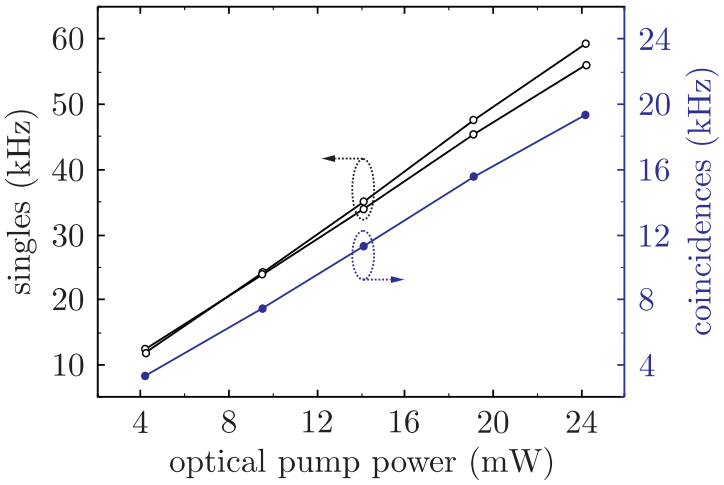

Figure 3.9: Detected single (black) and coincidence (red) count rates depending on the pump power, measured at the crystal position.

brightness and the entanglement-purity reaches a high level. Additional parameters, which show to be important in many applications, are the spectral bandwidth of the down-conversion photons and the coupling efficiency.

Brightness. In order to determine the brightness and the coupling efficiency, the output single-mode optical fibers are directly connected to two actively quenched silicon APDs (Perkin Elmer, No. SPCM-AQ4C). Their detection efficiency is estimated to be ≈ 51 % at 800 nm using a calibration method relying on the photon-pair emission from SPDC [70] and a conventional measurement technique with a strong reference beam. We detect a flux of roughly $B = 800$ pairs per second and milliwatt of pump power, see Fig. 3.9. For the maximum LD output power of 25 mW measured at the crystal position, this implies a coincidence count rate of about 20000 s^{-1}. The estimated accidental coincidences are negligible for the observed single-count rates of ≈ 60000 and the gate time of $\tau_c = 5.8$ ns. The coincidence to single count ratio, characterizing the quality of coupling, reaches values of up to $\mu \approx 0.34$. Taking into account the limited detection efficiency and other losses in the set-up, such as the reflection at the tips of the fibers (together $> 10\,\%$) and the optics in the path of down-conversion photons ($> 2\,\%$), the estimate of the net coupling efficiency reaches values as high as 75%.

Entanglement quality. To verify the entanglement of fibre-coupled photon pairs, their polarization correlations in two complementary bases are measured. This is done by directing the down-converted light into adjustable polarization analyzers, each consisting of a polarizing beamsplitter cube preceded by a rotatable half-wave plate. After passing through the analyzers, the light is re-coupled into multi-mode fibres and detected with APDs. Fig. 3.10 shows the expected $\sin^2$ dependence of the measured coincidence rates on the rotation angle φ_1 of one half-wave plate, while keeping the other one at fixed orientation of $\varphi_2 = 0°$ or $\varphi_2 = 22.5°$, respectively. For the setting of $\varphi_2 = 0°$, corresponding to a detection of photons in H/V linear

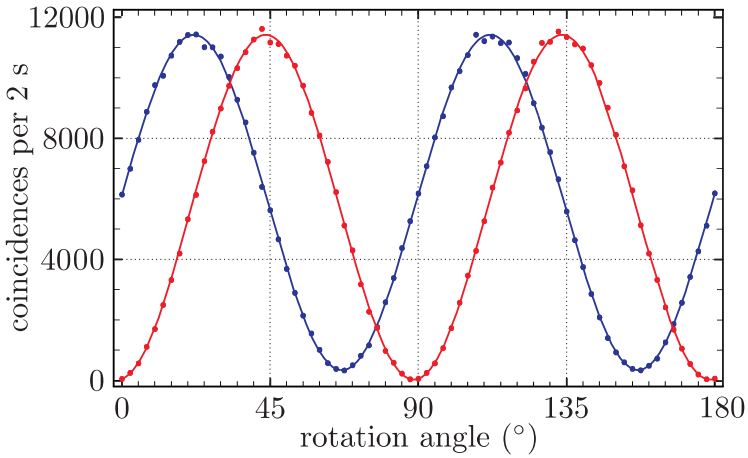

Figure 3.10: Polarization correlations between photons measured in the H/V (red points) and +45/-45 (blue points) polarization bases. The visibilities obtained from $\sin^2$ fits (solid lines) to the measured data are $99.6 \pm 0.3\,\%$ and $94.2 \pm 0.3\,\%$, respectively.

polarization basis, a visibility of $\mathcal{V}_{\mathrm{H/V}} = 99.55 \pm 0.31\,\%$ is observed. For the second investigated setting of $\varphi_2 = 22.5°$, i.e., a detection of photons in +45/-45 linear polarization basis, we obtain a visibility of $\mathcal{V}_{45} = 94.20 \pm 0.30\,\%$.

CHSH-inequality violation. The high-visibility sinusoidal coincidence fringes obtained by measuring the polarization correlations of photon pairs suggest a violation of a suitable Bell's inequality. Particularly, according to the most frequently used inequality in the CHSH formulation, any local-hidden variable theory is bound by the correlation coefficient $|S| \leq 2$, whereas, according to quantum mechanics, $|S|$ reaches the value of $2\sqrt{2}$ for maximally-entangled state with unit visibility. If the two-photon polarization state decoheres equally in all polarization bases, a minimum violation implies a visibility larger than 71 %. In the actual measurement, we recorded the coincidence count rates for 16 combinations of analyzer settings $\varphi_1 = \{0, \pi/2, \pi/4, 3\pi/4\}$ and $\varphi_2 = \{\pi/8, 5\pi/8, 3\pi/8, 7\pi/8\}$. In section 1.1.3 this particular set of settings is proved to be optimal. The chosen integration time per one measurement run is $T_I = 5$ s. Following the procedure of, e.g., [10], the obtained data are combined, yielding the value $S = 2.743 \pm 0.006$. This corresponds to a violation of the classical bound by 124 standard deviations. To unify results obtained from the measurements of CHSH-inequality violation over different integration times and to allow for a direct comparison of sources, the parameter "normalized speed of CHSH violation" has been suggested recently in [77]. It is defined as the number of standard deviations σ_S by which the correlation coefficient S is violated per $\sqrt{\mathrm{s}}$. For the measured values we infer the speed of violation of $(S-2)/(\sigma_S\sqrt{T_I}) \approx 55\,\sigma_S\ \mathrm{s}^{-1/2}$.

Spectrum. In order to spectrally analyze the parametric down-conversion light coupled into single-mode fibres, the fibres are individually connected to a grating spectrometer with single-photon sensitivity. We determine its wavelength resolution to be about 1.2 nm at a wavelength of 785 nm. As shown in Fig. 3.11, the measured spectral distributions are centered around the degenerate wavelength of 806 nm, with

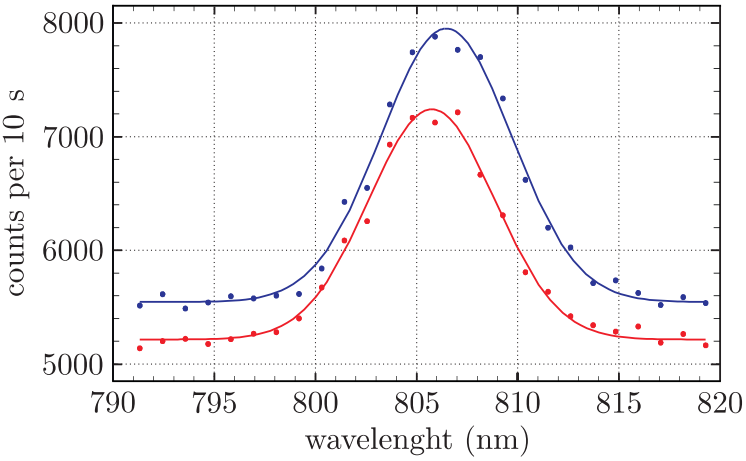

Figure 3.11: Spectral distributions of down-conversion light collected into single-mode fibres. The solid lines show Gaussian fits to measured data. The offset of ≈ 5400 counts is due to dark counts of the APDs.

the separation of ≈ 0.7 nm due to residual misalignment of the fiber coupler positions. The full widths at half maxima are found from the gaussian fits to be 6.24 ± 0.17 nm and 6.47 ± 0.19 nm. Correcting the inferred widths for the finite wavelength resolution of the spectrometer, a reasonable agreement with the design parameters of the coupling-optimization method is obtained.

3.3.4 Discussion

The brightness and the degree of polarization entanglement reached in the described LD-pumped source are comparable to conventional systems utilizing ion lasers [93]. Also, the achieved coupling efficiency appears to be at the level of the best reported values, indicating a successful implementation of the proposed fibre-coupling strategy. These traits make the LD-based systems a compact and cheap alternative for a variety of quantum-optics experiments. Moreover, the source shows to be a very suitable tool to practically demonstrate the phenomenon of entanglement in undergraduate laboratories [89, 101].

Nevertheless, no dramatic improvement of the present system, particularly regarding its brightness, is to be expected in future. This is due to the geometry of non-collinear type-II emission, which has some disadvantages. First, only a small fraction of the total SPDC output flux is polarization-entangled. Second, the overlap of the intensity distribution of the emission modes with the guiding mode of single-mode fibres is limited, lowering thus the accessible coupling efficiency to some extent. Finally, the practically applicable length of nonlinear crystals is restricted within only a few mm range. These drawbacks and the associated limitations certainly lower the usability of this type of source in future demanding applications of quantum information processing and communication and highlight the need for novel methods of entangled photon-pair generation.

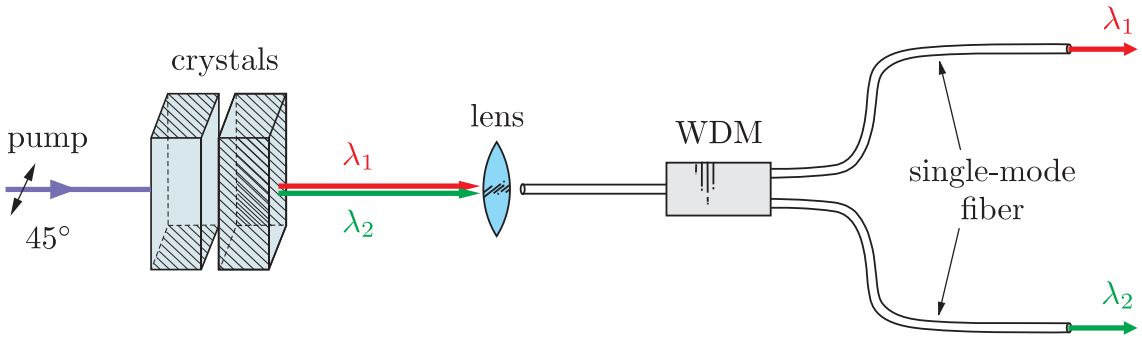

Figure 3.12: Conceptual layout of the method to generate entangled photon pairs using collinear geometry of SPDC operated in type I non-degenerate configuration.

3.4 Compact collinear type-I SPDC source

The concept of non-collinear SPDC entails several inevitable shortcomings. Besides those linked to the output performance of the source, purely practical problems arise as well. This is due to the use of two separate spatial collection modes defined by the coupling optics and single-mode fibres. High-purity polarization entanglement can be obtained only, if the divergences of these modes, as well as their mutual spatial orientations, are perfectly matched. Consequently, a careful alignment is always required, making such type of sources rather impractical for applications.

The following section introduces a novel method to generate entangled photon pairs using a collinear geometry of SPDC operated in type I non-degenerate configuration [102]. As will be demonstrated in the following, the proposed method overcomes many deficiencies of the prior art, including those outlined above.

3.4.1 Method

The conceptual layout of the method is shown in Fig. 3.12. The photon pairs at non-degenerate wavelengths are generated collinearly with respect to the pump light via SPDC and collected into one single-mode fiber. The spectral information is exploited to split the photons into two distinct spatial modes using a wavelength division multiplexer (WDM). To achieve a successful operation of the method, the wavelengths of the down-conversion photons have to be such that, first, their propagation in the same single-mode optical fiber, and second, their splitting with a high isolation ratio is possible.

For the actual generation of the photon pairs, SPDC in a simple two-crystal geometry is applied. Consider two adjacent nonlinear crystals, both operated in type-I phase-matching configuration and pumped with linearly polarized light. The orientation of otherwise identical crystals is adjusted such, that the optic axes of the first and second crystal lie in vertical and horizontal plane, respectively. With a 45°-polarized pump light, SPDC occurs equally likely in either crystal, producing

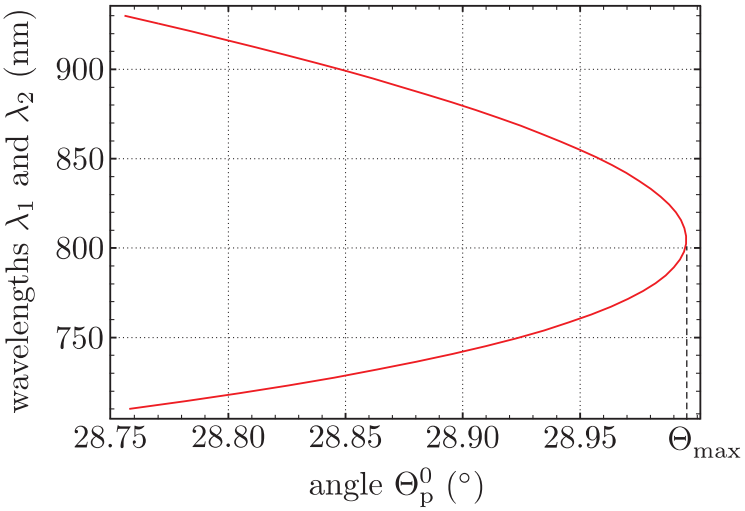

Figure 3.13: Collinearly phase-matched output wavelengths of down-conversion photons as a function of the angle Θ_p^0 between the pump and the optic axis. The calculation assumes SPDC in a BBO crystal pumped at $\lambda_p = 403$ nm.

pairs of horizontally polarized ($|H\rangle|H\rangle$) or vertically polarized ($|V\rangle|V\rangle$) photons due to type-I coupling. For further details on the method, which was originally suggested for non-collinear configuration of SPDC in [57], we refer to the section 2.5.2.

By angle tuning the crystals, down-conversion is driven to a collinear phase-matching configuration, emitting pairs of photons at non-degenerate wavelengths [58]. This mode of operation has been proved to be feasible in section 2.4. Fig. 3.13 shows the calculated tuning curve of collinearly phase-matched SPDC assuming the particular case of emission from BBO crystal. There are two clearly different regions above and below a limiting angle Θ_{max}, which corresponds to the degenerate emission of photons at the double wavelength of the pump light. In the region above Θ_{max} no collinearly phase-matched output is obtained whatsoever. Yet, tuning the angle in the regime of $\Theta_p^0 < \Theta_{max}$, the photons at any desired conjugate non-degenerate wavelengths λ_1 and λ_2 are phase matched in the nonlinear crystal .

Provided that the two emission processes are coherent with one another, which is fulfilled as long as there is no way of ascertaining whether a photon pair was produced in the first or the second crystal, the entangled state

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left[|H\rangle_{\lambda_1}|H\rangle_{\lambda_2} + e^{i\phi}|V\rangle_{\lambda_1}|V\rangle_{\lambda_2}\right] \tag{3.1}$$

is automatically produced. The relative phase ϕ is determined by the details of phase matching. The non-degenerate wavelengths are mapped onto two distinct spatial modes (labelled as usual by "1" and "2") using a WDM, thereby finally arriving at the state in the form:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left[|H\rangle_1|H\rangle_2 + e^{i\phi}|V\rangle_1|V\rangle_2\right]. \tag{3.2}$$

This way, the method produces polarization entangled photon pairs directly, with-

out a need for any post-selection [103] or beam overlap [75], which is often required in sources utilizing collinear geometry of SPDC. The fully collinear configuration of the method utilizing only one spatial mode for collecting down-conversion photons brings numerous advantages. First, it minimizes the complexity of the source and thereby enhances its inherent robustness. Second, it precludes the occurrence of any intrinsic spatial effect limiting the quantum-interference visibility, while at the same time allows the use of long down-conversion crystals yielding a higher photon-pair flux. From a practical point of view, the technical requirements and the demand for alignment are enormously reduced. The only evident drawback of the method lies in the restriction to non-degenerate wavelengths of the photons. Although this poses no limitation for a practical realization of a majority of quantum-communication protocols, some applications, e.g. those involving the overlap of down-conversion photons, cannot be accomplished with the proposed source.

The generation of non-degenerate photons using SPDC in a two-crystal geometry is accompanied with a detrimental spatiotemporal effect, which results in a poor fibre-coupling efficiency and also low-quality polarization entanglement. In the following we discuss this issue in detail and show, how to design an optimum compensation.

3.4.2 Spatial effect

It is well known that due to crystal birefringence the extraordinary wave gets spatially deflected from the ordinary wave by a walk-off angle γ. This leads to a lateral displacement of the two waves at the output surface of the crystal by $\delta = L \tan \gamma$. One has to face the same situation in case of the SPDC process in the two crossed type-I non-linear crystals. The down-conversion photons from the first crystal have the extraordinary polarization in the second crystal and therefore they are laterally displaced with regard to ordinary polarized photons created there. The situation is somewhat more complex, because the ordinary and extraordinary components of the pump wave undergo a birefringent spatial separation as well. This is schematically summarized in Fig. 3.14(a). There, one can see that the spatial walk-off has a two-fold effect on the emission characteristics. First, elliptical shapes are obtained for the horizontally- and vertically-polarized down-conversion emission spots at the output face of the second crystal. Second, the spots are laterally displaced with regard to each other, thereby reducing their mutual overlap. The resulting down-conversion emission region has an L-shaped profile. The spatial separation of the photons precludes the possibility of efficient fibre-coupling. Either the photons originating in the first crystal can be collected into the single-mode fibre or those originating in the second crystal, but never both together. Using simple geometrical arguments one can show that optimum compensation includes the same pair of crystals, but only half as long. This is graphically illustrated in Fig. 3.14(b).

We note that the described lateral displacement between the horizontally- and vertically-polarized photons does not impair the resultant purity of polarization entanglement. This is due to the fact that the single-mode nature of the collection fibre

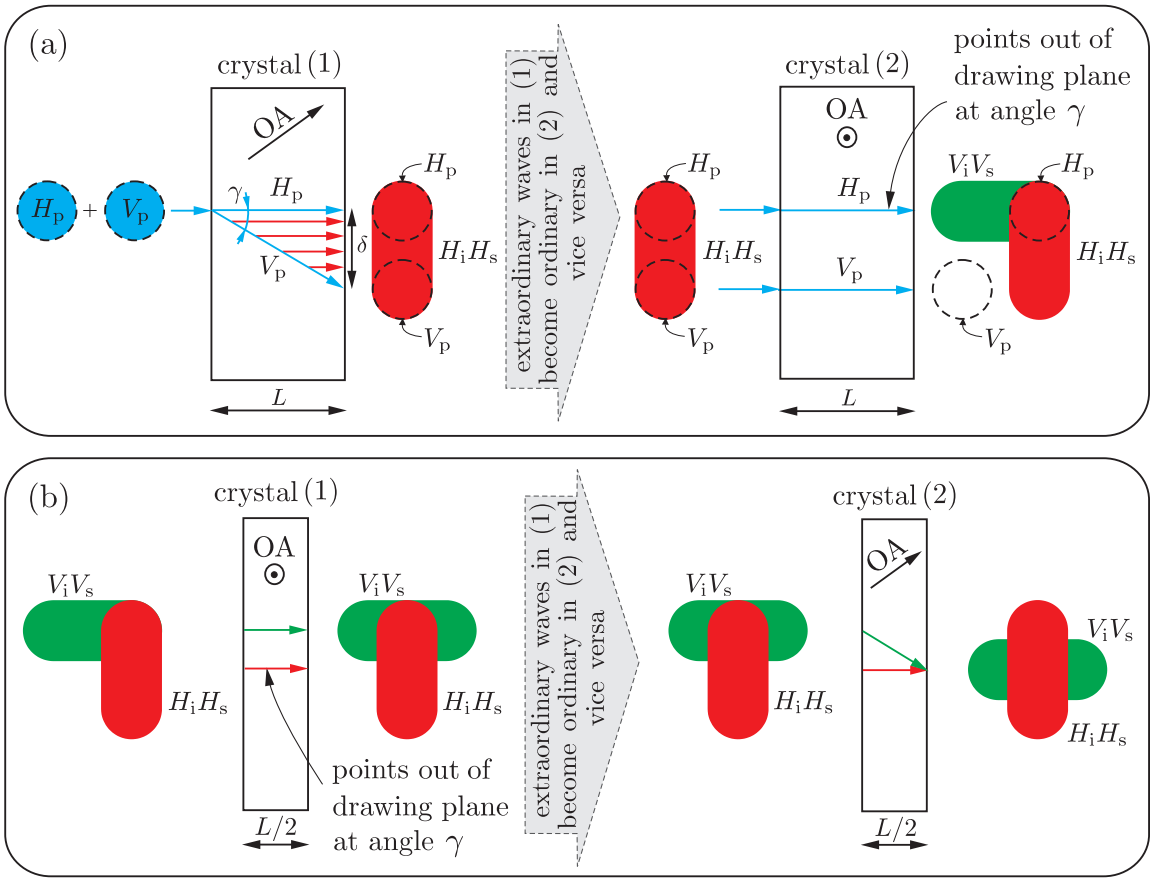

Figure 3.14: Schematic explanation of the detrimental spatial effect inherent to SPDC emission in two-crystal geometry. (a) The vertically- (V_p; blue) and horizontally-polarized (H_p; blue) components of the pump down-convert in the first and second crystal, respectively, producing pairs of horizontally- (H_sH_i; red) and vertically-polarized (V_sV_i; green) photon pairs due to type I nonlinear coupling. The orientation of the first (second) crystal with its optic axis (OA) in the vertical (horizontal) plane implies that vertically-polarized (horizontally-polarized) waves will deviate from the normal propagation direction. This effectively leads to, first, elliptical shapes of down-conversion emission spots at the output face of the crystals, and second, to a lateral displacement between the horizontally- and vertically- polarized down-conversion photons. (b) An optimal compensation involves two crystals identical to the down-conversion crystals, but only half as long.

removes all the spatial information the photons may have carried before entering the fibre.

3.4.3 Time effect

In the time domain, the crystal birefringence in combination with dispersion lead to an unwanted effect as well. The arrival times of photons at the output face of the second crystal depend on their wavelengths and polarizations, which reveal the

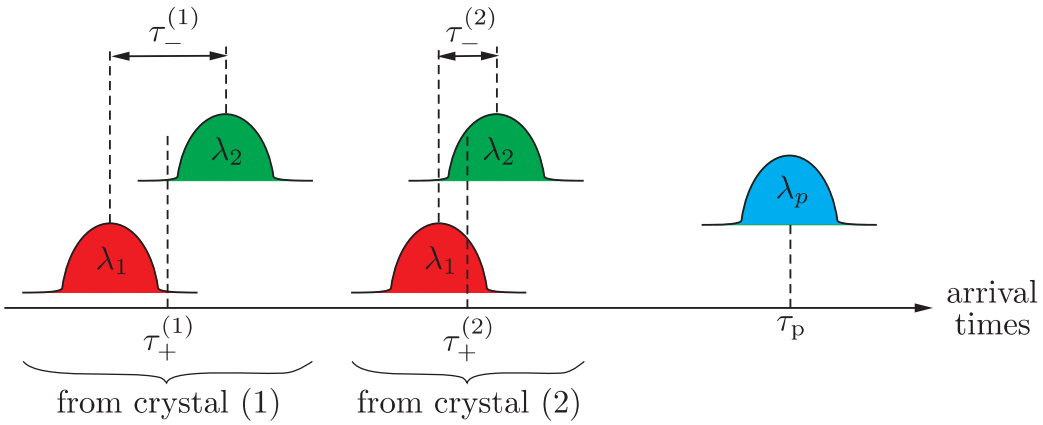

Figure 3.15: Explanation of the detrimental time effect inherent to SPDC emission in a two-crystal geometry. Due to crystal birefringence and dispersion, the arrival times of photons at the output face of the second crystal differ in general for the two emission possibilities. Consequently, a compensation erasing their temporal distinguishability has to applied.

actual position of the photon-pair's origin. This leads to a partial loss of the coherence between the two emission processes, and thus to a reduced entanglement. The detrimental temporal effect is two-fold, which is illustrated in a simplified fashion in Fig. 3.15. First, it is primarily the group-velocity mismatch between the pump and the down-conversion light, which causes that the photon pairs born in the first crystal are advanced with regard to those originating in the second crystal. Second, the dispersive delay of the down-conversion photons at the non-degenerate wavelengths is different for the two emission possibilities, because the photons generated in the first crystal acquire an extra spread by propagating through the second crystal.

To investigate the time effect and to find the optimum compensation, the evaluation tools introduced in section 2.3.2 are applied to determine the joint time distributions of the two-photon wave-packets $\mathcal{A}_1(\tau_+, \tau_-)$ and $\mathcal{A}_2(\tau_+, \tau_-)$, associated with the down-conversion emission in the first and second crystal, respectively. Since the non-degenerate wavelengths effectively label the photons of the emitted pair, we may define $\tau_+ = (\tau_{\lambda_1} + \tau_{\lambda_2})/2$ and $\tau_- = \tau_{\lambda_1} - \tau_{\lambda_2}$, where τ_{λ_1} and τ_{λ_2} are individual arrival times of the photons at λ_1 and λ_2 to the output face of the second crystal. Putting $\lambda_1 < \lambda_2$ for convenience, the two-photon amplitudes will be constrained only to the region of positive values of τ_- due to $\tau_{\lambda_1} > \tau_{\lambda_2}$ in normally dispersive materials.

The two-photon amplitudes are evaluated using Eq. (2.58). To find $\mathcal{A}_1(\tau_+, \tau_-)$ originating in the first crystal, we put $\mathcal{T}_{\lambda_1} \equiv \exp[ik_1^e(\lambda_1)L]$ and $\mathcal{T}_{\lambda_2} \equiv \exp[ik_2^e(\lambda_2)L]$. This way, the propagation of the photons through the second crystal is automatically accounted for. In the calculation the wave numbers $k_1^e(\lambda_1)$ and $k_2^e(\lambda_2)$ of the extraordinary polarized photons at non-degenerate wavelengths have to be expanded into a power series according to Eq. (2.43). The correct form of $\mathcal{A}_2(\tau_+, \tau_-)$ is obtained when putting $\mathcal{T}_{\lambda_1} \equiv \mathcal{T}_{\lambda_2} \equiv 0$. In this case we must insert a function $\exp[ik_\mathrm{p}^o(\lambda_\mathrm{p})L]$ into

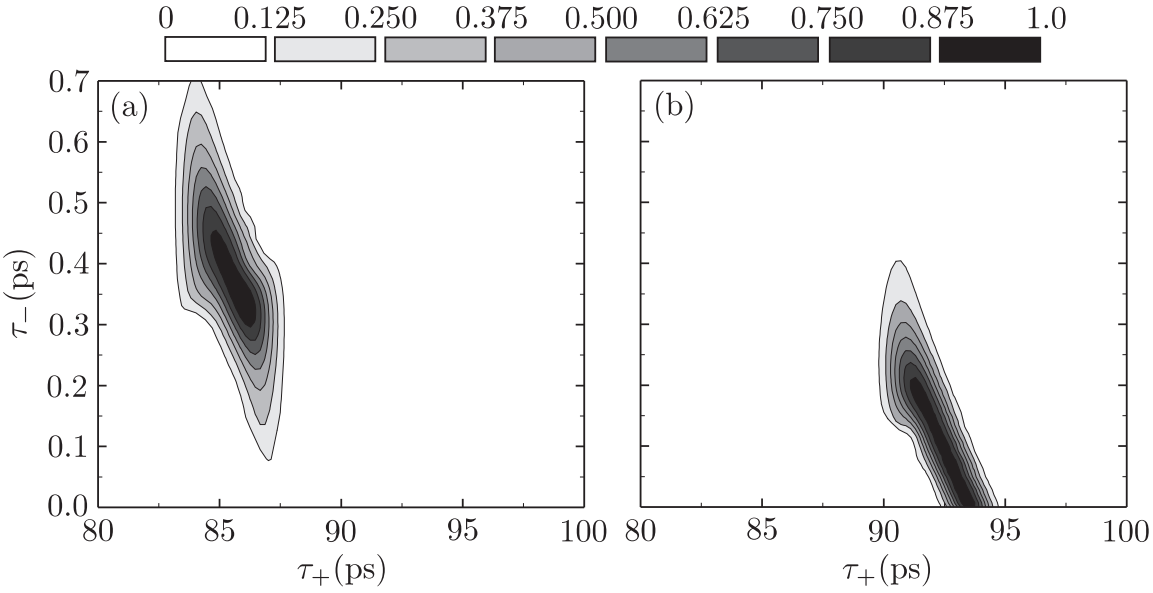

Figure 3.16: Absolute value of the normalized two-photon amplitudes (a) $\mathcal{A}_1(\tau_+, \tau_-)$ and (b) $\mathcal{A}_2(\tau_+, \tau_-)$ revealing the time distribution of photon wave-packets originating from the first and second crystal, respectively. The evaluation assumes SPDC in the pair of BBO crystals, each $L = 15.76$ mm long and cut at $\Theta_{\rm p}^0 = 28.95°$, corresponding to collinear phase matching of the wavelengths $\lambda_1 \approx 765$ nm and $\lambda_2 \approx 850$ nm (see Fig. 3.13). The parameters of the pump are: $\lambda_{\rm p} = 403$ nm, $\tau_{\rm p} = 1$ ps.

Eq. (2.58) to include the effect of the pump propagation through the first crystal[7].

Fig. 3.16 shows the time distributions of the numerically calculated amplitudes assuming type I SPDC in the pair of BBO crystals, each with the length of $L = 15.76$ mm. The limited extent of the amplitudes in the τ_+ direction signifies that a pump with a finite coherence time has been used for the evaluation (compare to two-photons amplitudes obtained in CW-pumped regime, see Fig. 2.5). In particular, we assumed the pump with a duration of 1 psec, which roughly corresponds to the coherence time of the used blue LDs. The distribution of $\mathcal{A}_2(\tau_+, \tau_-)$ is shifted towards larger values of τ_+ in comparison to $\mathcal{A}_1(\tau_+, \tau_-)$. From a physical point of view this corresponds to a time delay of the photons created in the second crystal with regard to those created in the first. The time distributions of amplitudes in the τ_- direction is determined by the extent of the chromatic dispersion: a huge difference of group velocities v_{λ_1} and v_{λ_2} at non-degenerate wavelengths will manifest itself by a large spread of the amplitudes in this direction and vice versa. Whereas the distribution of $\mathcal{A}_2$ is constrained to roughly $0 < \tau_- < L(1/v^o_{\lambda_1} - 1/v^o_{\lambda_2})$, the amplitude $\mathcal{A}_1$ stretches

[7]Note that the polarization of the pump photon, which eventually down-converts in the second crystal, has to be ordinary in the first crystal. Analogously, when evaluating $\mathcal{A}_1$ we have to take into account that the down-conversion photons generated in the first crystal become extraordinary polarized in the second crystal.

in a range of $L(1/v^e_{\lambda_1} - 1/v^e_{\lambda_2}) < \tau_- < L(1/v^e_{\lambda_1} - 1/v^e_{\lambda_2}) + L(1/v^o_{\lambda_1} - 1/v^o_{\lambda_2})$. The offset $L(1/v^e_{\lambda_1} - 1/v^e_{\lambda_2})$ is due to the passage of the photons originating in the first crystal through the second crystal. For the present parameters we calculate $L(1/v^o_{\lambda_1} - 1/v^o_{\lambda_2}) = 285$ fs and $L(1/v^e_{\lambda_1} - 1/v^e_{\lambda_2}) = 258$ fs. A slight broadening of the amplitudes in Fig. 3.16 compared to these calculated values is due to the finite phase-matched bandwidth of the photons. The tilt of both amplitudes in the τ_+/τ_- plane expresses the fact that the photons created at the very end of either crystal are always delayed with regard to those created at the beginning. This is again caused by the group-velocity mismatch between the pump and the generated down-conversion photons.

The overlap of the amplitudes $\mathcal{A}_1$ and $\mathcal{A}_2$ provides a measure of the maximum accessible quantum-interference visibility $\mathcal{V}$ in polarization correlation measurements. To understand that, the overlap might be interpreted from the perspective of mutual distinguishability of two paths (or Feynman alternatives) leading to a coincidence detection [39, 104]. No overlap signifies the paths being totally distinguishable. Consequently, no quantum interference can be observed whatsoever. When the overlap is complete, the interference pattern has a maximum visibility. Mathematically, the overlap $\mathcal{O}_{12}$ of the amplitudes $\mathcal{A}_1$ and $\mathcal{A}_2$ is expressed in the form

$$\mathcal{O}_{12} = \int_{-\infty}^{\infty} \mathrm{d}\tau_+ \int_{-\infty}^{\infty} \mathrm{d}\tau_- \, \mathrm{Re}\big[\mathcal{A}_1(\tau_+, \tau_-)\mathcal{A}_2^*(\tau_+, \tau_-)\big], \tag{3.3}$$

where the symbol Re denotes the real part of its argument. Normalizing the overlap $\mathcal{O}_{12}$ to the modulus squared of the amplitudes, $\mathcal{D}$, which is defined as

$$\mathcal{D} = \int_{-\infty}^{\infty} \mathrm{d}\tau_+ \int_{-\infty}^{\infty} \mathrm{d}\tau_- \, \big|\mathcal{A}_1(\tau_+, \tau_-)\big|^2 = \int_{-\infty}^{\infty} \mathrm{d}\tau_+ \int_{-\infty}^{\infty} \mathrm{d}\tau_- \, \big|\mathcal{A}_2(\tau_+, \tau_-)\big|^2, \tag{3.4}$$

we directly obtain the quantum-interference visibility $\mathcal{V}$ (i.e., $\mathcal{V} = \mathcal{O}_{12}/\mathcal{D}$).

Without a further evaluation it is directly apparent from Fig. 3.16 that the amplitudes $\mathcal{A}_1$ and $\mathcal{A}_2$ do not overlap whatsoever. The detrimental distinguishing information has to be eliminated by temporal engineering of the two-photon amplitudes [58, 104]. This is physically achieved by including additional special birefringent elements in front and/or behind the nonlinear crystals. They effectively redistribute the amplitudes and, if designed properly, they allow restoring of their complete overlap.

First, we investigate the effect of a birefringent crystal placed in the path of the down-conversion photons. As a material we conveniently choose yttrium orthovanadate (YVO_4; basic characteristics are given in appendix A.1.2) due to its very high birefringence of $\Delta n = |n_e - n_o| > 0.2$ at NIR wavelengths. For this crystal the slope of chromatic dispersion, which was shown to determine the projected distribution of the amplitudes onto the τ_- axis, is higher for the extraordinary polarization. Thus, if we adjust the crystal orientation such that the photons born in the second BBO crystal have extraordinary polarization within the compensation YVO_4, the overlap of $\mathcal{A}_1$ and $\mathcal{A}_2$ becomes larger in the τ_- direction. For a certain length of the crystal, which is calculated to be $l = 8.20$ mm in the considered example, the overlap reaches

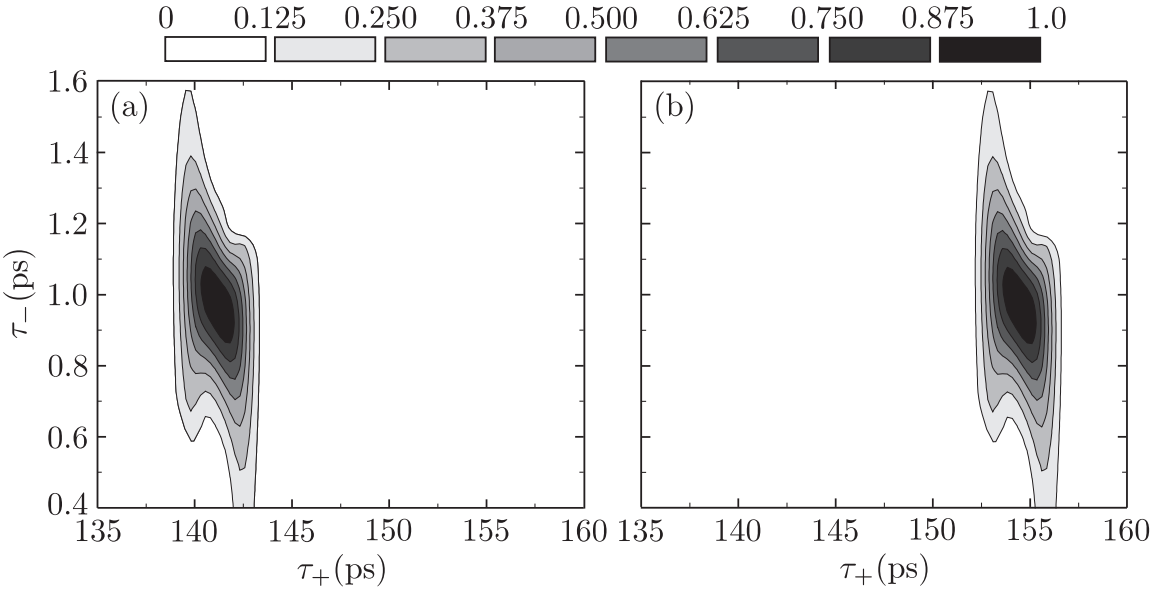

Figure 3.17: Absolute value of the normalized two-photon amplitudes (a) $\mathcal{A}_1(\tau_+, \tau_-)$ and (b) $\mathcal{A}_2(\tau_+, \tau_-)$, revealing the time distribution of photon wave-packets originating from the first and second crystal, respectively. The plots show the amplitudes after passage through the compensation element YVO_4 with a length of $l = 8.20$ mm positioned behind the down-conversion crystals. All the other parameters are the same as in Fig. 3.16.

its maximum. In this case the temporal spread of photons at non-degenerate wavelengths inside the YVO_4 reaches $l(1/g^o_{\lambda_1} - 1/g^o_{\lambda_2}) = 585$ fs for ordinary polarization and $l(1/g^e_{\lambda_1} - 1/g^e_{\lambda_2}) = 843$ fs for extraordinary polarization. Here g_{λ_1} and g_{λ_2} denote the corresponding group velocities in YVO_4. That is, passing through the YVO_4 crystal, the amplitude $\mathcal{A}_1$ is confined within the range

$$\begin{aligned} 0.843 \text{ ps} = l\left(\frac{1}{g^o_{\lambda_1}} - \frac{1}{g^o_{\lambda_2}}\right) + L\left(\frac{1}{v^e_{\lambda_1}} - \frac{1}{v^e_{\lambda_2}}\right) < \tau_- \\ < l\left(\frac{1}{g^o_{\lambda_1}} - \frac{1}{g^o_{\lambda_2}}\right) + L\left(\frac{1}{v^e_{\lambda_1}} - \frac{1}{v^e_{\lambda_2}}\right) + L\left(\frac{1}{v^o_{\lambda_1}} - \frac{1}{v^o_{\lambda_2}}\right) = 1.128 \text{ ps}, \end{aligned} \quad (3.5)$$

which perfectly matches the limits found for the amplitude $\mathcal{A}_2$:

$$0.843 \text{ ps} = l\left(\frac{1}{g^e_{\lambda_1}} - \frac{1}{g^e_{\lambda_2}}\right) < \tau_- < l\left(\frac{1}{g^e_{\lambda_1}} - \frac{1}{g^e_{\lambda_2}}\right) + L\left(\frac{1}{v^o_{\lambda_1}} - \frac{1}{v^o_{\lambda_2}}\right) = 1.128 \text{ ps}. \quad (3.6)$$

The calculated amplitudes are shown in Fig. 3.17.

Although the suggested compensation provides an optimum overlap of the amplitudes in the τ_- direction, it makes them more distinguishable along the τ_+ axis at the same time. This is due to the fact that YVO_4 is a positive birefringent crystal, in

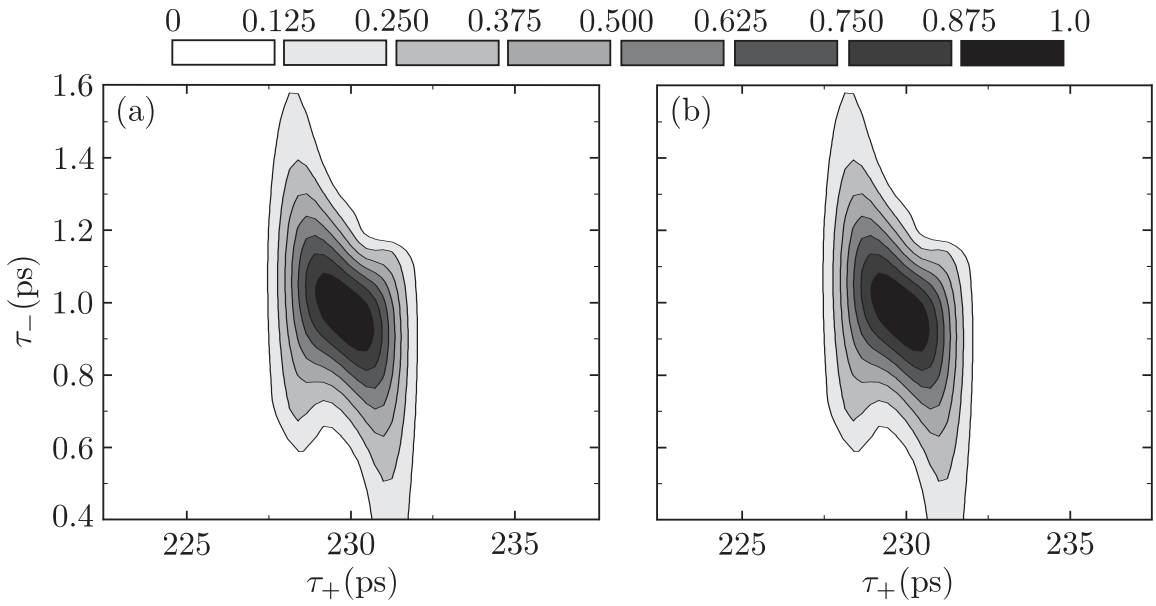

Figure 3.18: Absolute value of the normalized two-photon amplitudes (a) $\mathcal{A}_1(\tau_+, \tau_-)$ and (b) $\mathcal{A}_2(\tau_+, \tau_-)$ revealing the time distribution of photon wave-packets originating from the first and second crystal, respectively. The plots show the amplitudes after complete compensation using two tailored birefringent elements with lengths of $l_\mathrm{p} = 9.03$ (in the path of the pump light) mm and $l = 8.20$ mm (in the path of the down-conversion light). All the other parameters are the same as in Fig. 3.16.

which the ordinary-polarized light propagates always faster than the extraordinary-polarized light. This way, the total temporal retardation of down-conversion photons originating from the second crystal relative to those from the first crystal increases to $\Delta\tau_+ = 13.28$ ps. To counteract the effect, the respective delay between the horizontally- and vertically-polarized pump components has to be introduced[8]. This shows to be very convenient, because the birefringent delay in the pump does not cause any relative change of the amplitudes in the τ_- direction. The desired delay of $\Delta\tau_+ = 13.28$ ps is achieved using $l_p = \Delta\tau_+/(1/g^o_{\lambda_\mathrm{p}} - 1/g^o_{\lambda_\mathrm{p}}) = 9.03$ mm long YVO_4 crystal. After the compensation, the two-photon amplitudes $\mathcal{A}_1$ and $\mathcal{A}_2$, which are associated with the $|H\rangle_{\lambda_1}|H\rangle_{\lambda_2}$ and $|V\rangle_{\lambda_1}|V\rangle_{\lambda_2}$ terms, show to be temporally indistinguishable (see Fig. 3.18), so that the resultant state takes the form of (3.1).

The necessary temporal indistinguishability between the terms $|H\rangle_{\lambda_1}|H\rangle_{\lambda_2}$ and $|V\rangle_{\lambda_1}|V\rangle_{\lambda_2}$ can be built using the pump with a sufficient coherence length as well. This effectively leads to elongation of the amplitudes $\mathcal{A}_1$ and $\mathcal{A}_2$ in the τ_+ direction, and thus to their overlap. No birefringent element introducing a relative delay between the two orthogonal polarization components of the pump is then needed. Fig. 3.19

[8]Particularly, we need to delay the pump-polarization component which down-converts in the first BBO crystal.

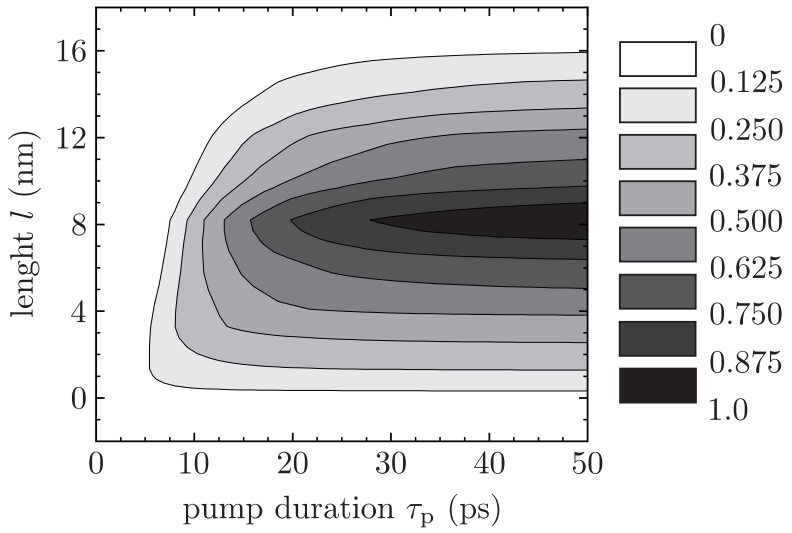

Figure 3.19: The map of maximum accessible quantum-interference visibility $\mathcal{V}$ as a function of the length l of the compensation YVO_4 crystal and the pump duration τ_{p}. If a laser light with a sufficiently long coherence length is applied for pumping SPDC, no birefringent compensation element preceding the down-conversion crystals is required for achieving a high visibility. Values of the parameters are the same as in Fig. 3.16.

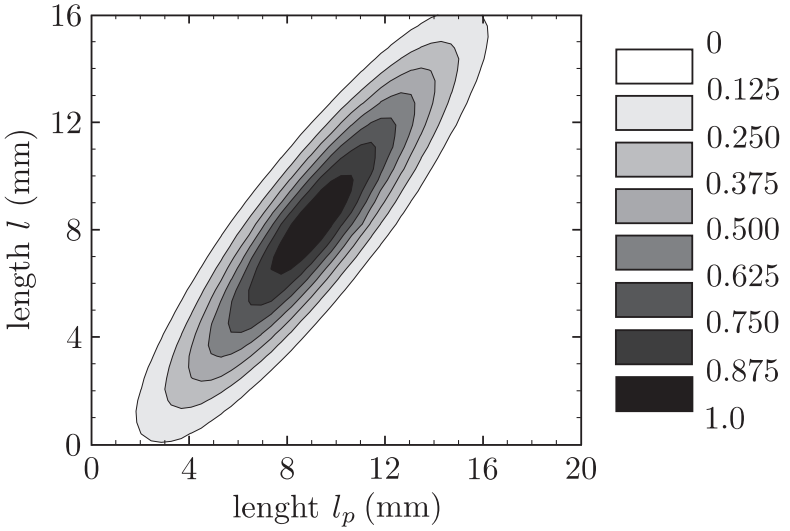

Figure 3.20: The map of maximum accessible quantum-interference visibility $\mathcal{V}$ as a function of the lengths l and l_p of the compensation YVO_4 crystals. Values of the parameters are the same as in Fig. 3.16.

illustrates the issue in a quantitative way. It shows the map of visibility $\mathcal{V}$ as a function of the length l of the compensation YVO_4 crystal and the pump duration τ_{p}. To achieve the quantum-interference visibility of at least $\mathcal{V} = 90\,\%$ the pump duration has to be longer than $\tau_{\mathrm{p}} \approx 31$ ps in the considered example of the temporal retardation of $\Delta\tau_+ = 13.28$ ps.

Finally, Fig. 3.20 shows the density plot of visibility $\mathcal{V}$ evaluated in dependence on the lengths l and l_p of either YVO_4 compensation crystal. It demonstrates that

a deviation of several hundreds of microns from the determined optimum values of l and l_p might be accompanied by a notable drop in the achieved quantum-interference visibility. The suggested compensation method using a pair of birefringent elements works equally efficient for even shorter pump-coherence lengths than the one investigated. Yet, we must be aware of the substantial stiffening of the tolerances imposed on the lengths l and l_p when very short pump pulses, such as with fs duration, are used.

The described time effect can be understood from another, but completely equivalent perspective, which is based on the investigation of the relative phase ϕ in the state (3.2). This phase generally depends on the particular wavelengths of pump and down-conversion photons being considered. The following argument might be used to determine this dependence: both $|H\rangle_1|H\rangle_2$ and $|V\rangle_1|V\rangle_2$ terms in (3.2) receive an equal ordinary phase in the crystals, where they are created. Therefore, these phases can be neglected as a global phase. Besides, the $|H\rangle_1|H\rangle_2$ term originating in the first crystal[9] acquires an additional extraordinary phase in the second crystal equal to

$$\frac{2\pi L}{\lambda}\, n^e(\lambda, \Theta_{\mathrm{p}}^0) + \frac{2\pi L(\lambda - \lambda_{\mathrm{p}})}{\lambda\lambda_{\mathrm{p}}}\, n^e\left(\frac{\lambda\lambda_{\mathrm{p}}}{\lambda - \lambda_{\mathrm{p}}}, \Theta_{\mathrm{p}}^0\right), \tag{3.7}$$

and the $|V\rangle_1|V\rangle_2$ term originating in the second crystal acquires an additional ordinary phase,

$$\frac{2\pi L}{\lambda_{\mathrm{p}}}\, n_o(\lambda_{\mathrm{p}}), \tag{3.8}$$

which is given by the propagation of the pump photon in the first crystal. In the expression (3.7) λ denotes the wavelength of one of the down-conversion photons. The difference of the phases (3.7) and (3.8) determines the relative phase $\phi = \phi(\lambda, \lambda_{\mathrm{p}})$, up to irrelevant constant phase factors. As demonstrated in Fig. 3.21(a), a strong variation of $\phi(\lambda, \lambda_{\mathrm{p}})$ over a relevant spectral region is observed for the parameters considered above, which corresponds to an effective dephasing of photon-pair polarization state. Consequently, no interference pattern can be observed in the polarization-correlation measurements.

The distinct dispersive delay between the down-conversion photons at the non-degenerate wavelengths for the two emission possibilities, results in a dependence of the phase map $\phi(\lambda, \lambda_{\mathrm{p}})$ on the wavelength λ. Previously, it was shown to be a cause of different distributions of two-photon amplitudes $\mathcal{A}_1(\tau_+, \tau_-)$ and $\mathcal{A}_2(\tau_+, \tau_-)$ in the τ_- direction, which could be compensated using a tailored YVO_4 crystal with the length of $l = 8.20$ mm inserted in the path of down-conversion photons. Such a crystal has an effectively reverse phase characteristics to $\phi(\lambda)$ and therefore, after the compensation the relative phase ϕ becomes independent of the down-conversion wavelength λ, see Fig. 3.21(b).

[9] Here, without any loss of generality we assume a particular setting, where the optic axis of the first crystal defines, together with the pump direction, the vertical plane, and the optic axis of the second crystal the horizontal plane.

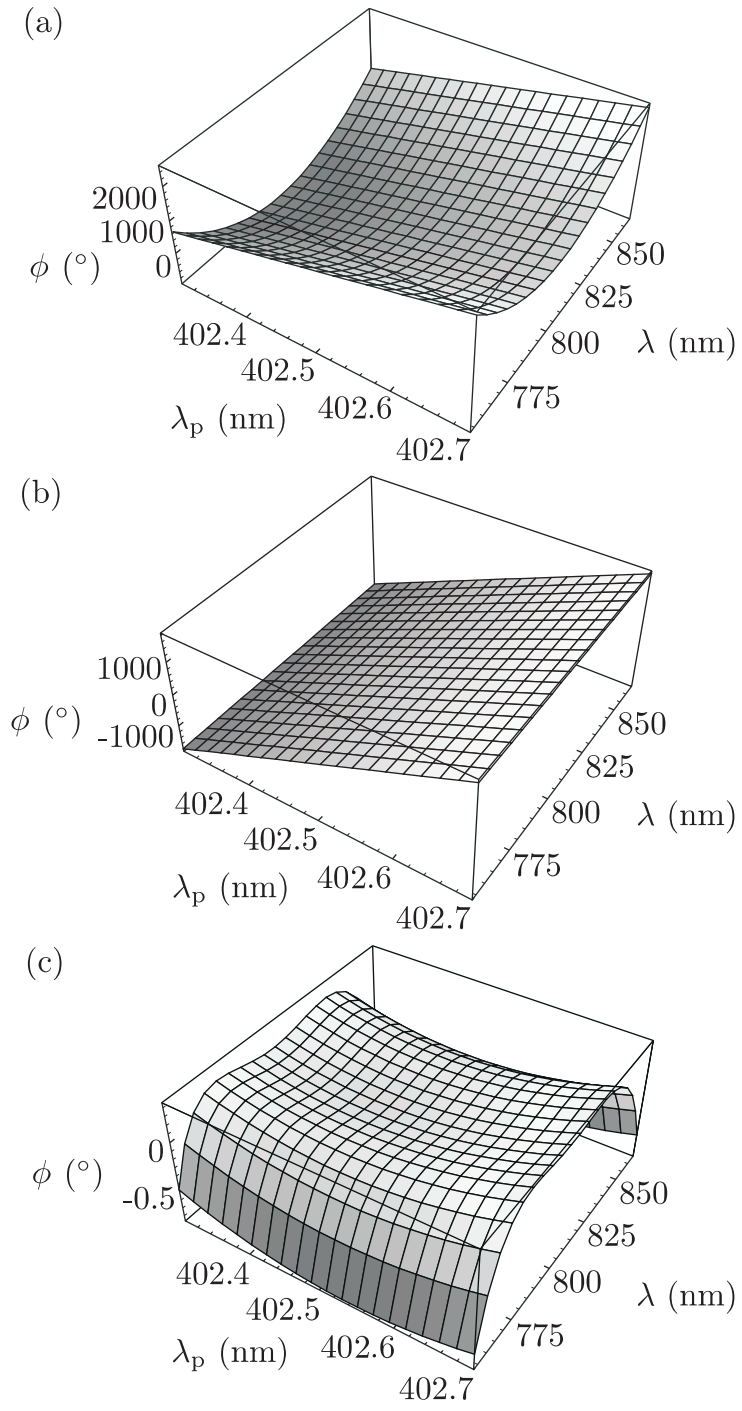

Figure 3.21: Calculated dependence of the relative phase ϕ on the wavelengths of pump λ_p and one of the down-conversion photons λ for different configurations: (a) Uncompensated configuration. (b) With the birefringent YVO_4 element of length $l = 8.20$ mm included in the path of down-conversion photons. (c) Ideally compensated configuration using a pair of YVO_4 with lengths of $l_p = 9.03$ mm (in the path of pump light) mm and $l = 8.20$ mm (in the path of down-conversion light). After compensation, the initially strongly varying phase map $\phi(\lambda, \lambda_p)$ becomes flat over the relevant spectral region (note the change in the vertical scale), which signifies that all the detected photon pairs are described by essentially the same polarization state.

The group-velocity mismatch between the pump and the down-conversion light, which causes the delay of the photons born in the second crystal with regard to those originating in the first crystal, manifests itself as a finite slope of the phase map $\phi(\lambda, \lambda_p)$ in the λ_p direction. This effect can be simply precluded using the narrowband pump, which effectively corresponds to a selection of a particular phase value

from the phase map in Fig. 3.21(b). If a short-coherence-length source is used instead, a special birefringent compensation crystal has to be inserted into the path of the pump, introducing a proper temporal retardation between its horizontally- and vertically-polarized component, and thus effectively compensating the predicted slope. The YVO_4 thickness of $l_p = 9.03$ mm was proved to be optimal in the previous analysis of the two-photon amplitudes. In this way, the initially strongly varying phase map $\phi(\lambda, \lambda_p)$ becomes flat after the compensation [see Fig. 3.21(c)], representing the complete temporal indistinguishability of the emission processes. Consequently, all detected photons will be described with essentially the same polarization state.

3.4.4 Implementation

Some of the tools or techniques required for the implementation of the source, including LD or pump-beam shaping and focusing, were already discussed in section 3.3.2. Here we describe only the parts of the set-up not introduced therein.

Nonlinear crystal and SPDC emission. As a nonlinear medium for SPDC we use a pair of BBO crystals, both cut for type-I phase matching at an angle of $\Theta_c = 29.0°$ ($\Phi_c = 0.0°$). The crystals, each with dimensions of $6 \times 6 \times 15.76$ mm^3, are oriented with their optic axes aligned in perpendicular (horizontal and vertical) planes and cemented together. Tilting the crystal assembly in horizontal and vertical direction, the output phase-matched wavelengths are tuned for either crystal separately. We choose the operation at non-degenerate wavelengths centered on $\lambda_1 \approx 765$ nm and $\lambda_2 \approx 850$ nm. Alternatively, two other BBO pairs with lengths of $L = 7.88$ mm and $L = 3.94$ mm are tested with the aim to experimentally determine the dependence of the output photon-pair flux and the output spectral width on the crystal length.

For the crystal length of $L = 15.76$ mm and the wavelength non-degeneracy of $\lambda_2 - \lambda_1 \approx 85$ nm the phase-matched spectral width is expected to reach $\Delta\lambda_1 = \Delta\lambda_2 = 6.42$ nm for narrow-band pumping [for reference see also Fig. 2.3]. Nevertheless, the spectral characteristics of the non-degenerate type-I phase-matching shows to be very dependent on the coherence length of the pump. Reducing the coherence length to 1 ps, corresponding to the value inferred for the blue LDs, the output spectral widths of the down-conversion light at λ_1 and λ_2 are roughly doubled to $\Delta\lambda_1 = 11.86$ nm and $\Delta\lambda_2 = 12.85$ nm. Note that for the coherence length of 1 ps almost no broadening was observed in the case of degenerate type I and type II phase matching, see Fig. 2.4. Similarly as in the type II phase matching, the broadband pumping results in a weak asymmetry of the spectra at non-degenerate wavelengths. Fig. 3.22 shows the numerically simulated down-conversion spectra for different coherence lengths of the pump and different crystal lengths. Particularly interesting is the observation that extending the crystal length beyond a certain boundary brings only a negligible reduction of the output spectral width for a given coherence length of a broadband

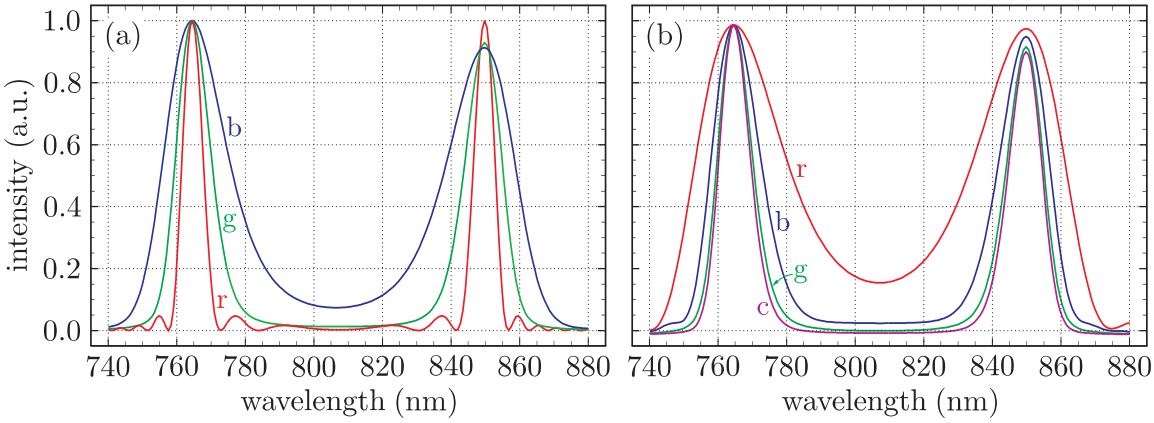

Figure 3.22: Calculated non-degenerate spectra centered on $\lambda_1 \approx 765$ nm and $\lambda_2 \approx 850$ nm obtained from type I phase-matched BBO crystal for (a) different coherence lengths of pump light: CW pumping, i.e. $\tau_p = \infty$ (red,"r"), $\tau_p = 1.0$ ps (green, "g"), $\tau_p = 0.5$ ps (blue, "b"); and (b) for different crystal lengths: $L = 3.94$ mm (red,"r"), $L = 7.88$ mm (blue, "b"), $L = 15.76$ mm (green, "g"), $L = 31.52$ mm (cyan, "c"). In plot (a) the crystal length of $L = 15.76$ mm is assumed and in plot (b) a coherence length of the pump light of $\tau_p = 1.0$ ps is assumed.

pump. In such a case the only possibility to achieve narrower spectral distributions is to enlarge the pump-beam coherence length.

Wavelength division multiplexer. The collinearly emitted photons at the wavelengths of $\lambda_1 = 765$ nm and $\lambda_2 = 850$ nm are coupled into a single-mode fibre using an aspheric lens. The fibre is pigtailed to the custom made visible WDM (Fiber Optic Network Technology Co.), which demultiplexes the two wavelengths into output single-mode fibres each carrying one wavelength. The WDM was characterized using a broadband light source, yielding the spectral dependence of the insertion loss and isolation into both outputs, see Fig. 3.23. The isolation of > 17 dB is obtained in the bandpass of 15 nm around the operating wavelengths of 765 nm and 850 nm. The peak isolation reaches nearly 22 dB. The insertion loss was found to be about 0.35 dB in 765 nm output port and 0.3 dB in 850 nm port. A separate measurement of the internal polarization effects at the operating wavelengths determined the maximum polarization-dependent loss to be below 0.1 dB.

Set-up overview. The schematic set-up of the source is shown in Fig. 3.24 (the photo of the experimental source is included in appendix A.3). The linearly polarized pump light is provided by a 60 mW free-running laser diode. The light is reflected several times at dichroic mirrors to remove the background broadband laser emission and passes through a half-wave plate rotating the angle of polarization to 45° with regard to the horizontal direction. A triad of lenses is used to focus the pump beam

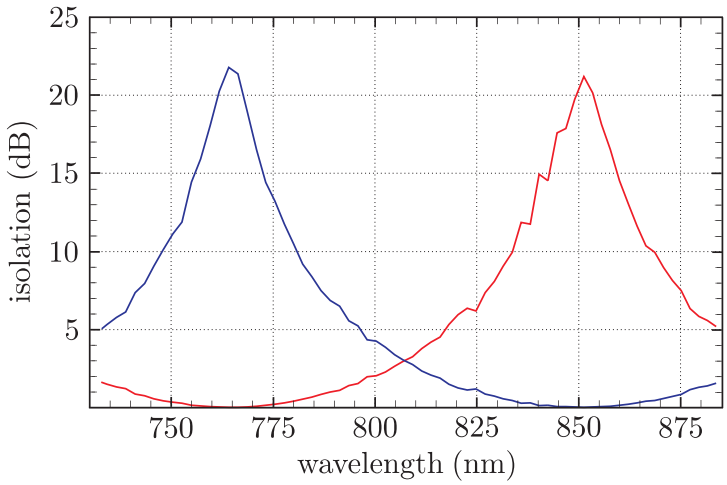

Figure 3.23: Spectral dependence of the isolation in the 765 nm (blue curve) and 850 nm (red curve) output ports of the WDM.

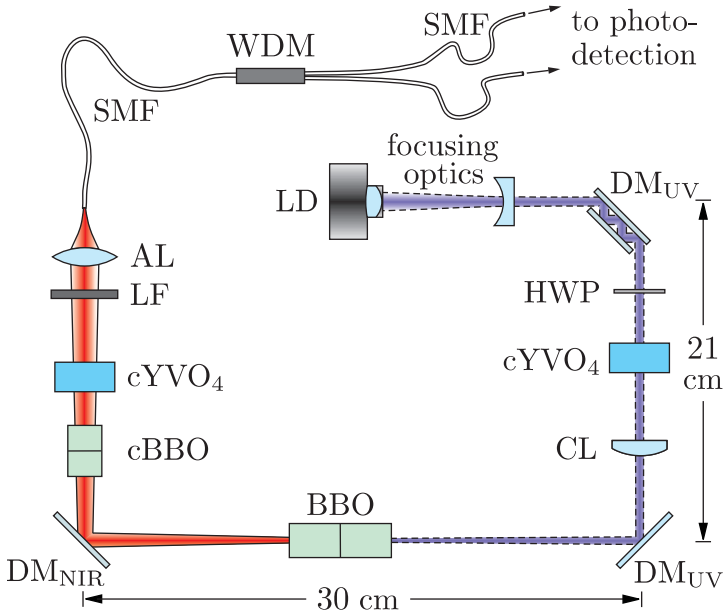

Figure 3.24: Schematic setup of the compact collinear type-I SPDC source: dichroic mirror (DM_{UV} and DM_{NIR}), half-wave plate (HWP), cylindrical lens (CL), compensation YVO_4 crystal ($cYVO_4$), compensation BBO crystal (cBBO), longpass filter (LF), aspheric lens (AL), single-mode fibre (SMF).

to a diameter of ≈ 200 mm within the two BBO crystals[10], oriented for a collinear emission of photons at the non-degenerate wavelengths of $\lambda_1 = 765$ nm and $\lambda_2 = 850$ nm. The emitted photons are separated from the pump light using a dichroic mirror and a long-pass filter, and are collected into a single-mode fiber guiding the photons to the WDM, which splits the non-degenerate wavelengths into two single-mode fibers with a probability higher than 99 %. To reach high collection efficiency, the lateral displacement of the orthogonally polarized down-conversion photons is compensated using the same pair of BBO crystals, but only half as long. The detrimental time

[10]No theoretical investigation of optimum focusing of the pump mode was performed. The exceptional simplicity of the source and its alignment allowed the efficient optimization directly in the experiment. This way, the optimum regime of focusing was found when reaching the values of ≈ 2 in the ratio between the Rayleigh range of the mode and the double-crystal length.

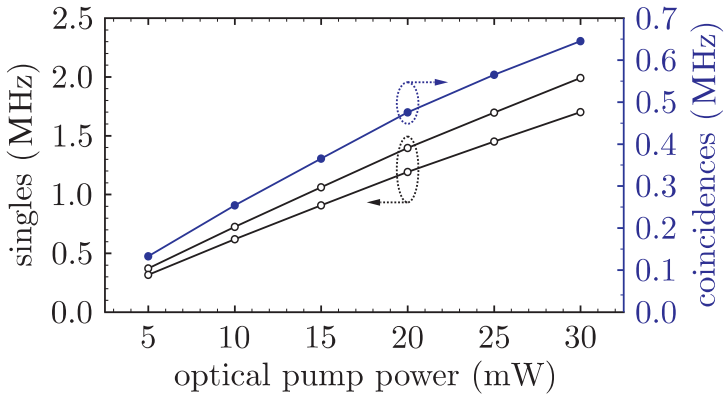

Figure 3.25: Detected single and coincidence count rates depending on the pump power measured at the position of BBO crystals. To avoid failure of the detectors, the peak count rate was electronically regulated to $\approx 2 \times 10^6$ detections per second, thereby limiting the directly observed pair rate to $\approx 6.5 \times 10^5$ per second. We note that the measured LD maximum pump power of 57 mW was reduced to 38 mW at the crystal position, mainly due to attenuation in the compensation YVO_4 crystal (length $l_p = 9.03$), which was estimated to be above 2 % per one mm of the crystal.

effect is compensated with a pair of tailored YVO_4 crystals; one of them (length $l_p = 9.03$ mm) is put into the path of the pump, whereas the another ($l = 8.20$ mm) is included in the path of the down-conversion photons, in accordance with the explanation given above. The cut of both YVO_4 crystals is at 90° with regard to pump- and down-conversion-light direction, thus precluding the occurrence of any unwanted spatial walk-off effects.

3.4.5 Results

Since the measurement techniques follow those already applied for the compact non-collinear type-II SPDC source, a minimum of technical details about the performed measurements is given here. For more information we refer to section 3.3.3.

Brightness. For the detection of the down-conversion photons two actively quenched silicon APDs with a measured efficiency of $\approx 51\,\%$ at 800 nm were used. Balancing the photon-pair flux obtained from either crystal by aligning the focus position of the collection mode to the contact plane of the crystals, we detected $B \approx 27000$ pairs per second and milliwatt of pump power, see Fig. 3.25. This is somewhat lower than the maximum rate of up to $B = 37000$ pairs/s/mW observed after rotating the pump polarization to horizontal or vertical direction such that the emission from only one crystal is collected, and after refocusing the collection mode to the mid of the

respective crystal[11].

The output photon-pair flux was measured also for shorter BBO crystals with $L = 7.88$ mm and $L = 3.94$ mm. In the first case we detected about $B = 25000$ pairs/s/mW in the balanced configuration and up to $B \approx 28000$ pairs/s/mW when the collection from one crystal was optimized. In the latter case no apparent difference in the output rates was observed in both configurations; the brightness was $B \approx 23000$ pairs/s/mW. This clearly suggests that we cannot take full advantage of higher photon-pair fluxes converted in longer crystals, because of the impossibility to optimally collect photons from both crystals at the same time. Furthermore, from the detected rates we can infer that the fibre-coupled photon pair flux scales maximally with the square root of the crystal length ($\propto \sqrt{L}$). This is in agreement with the conclusions drawn in [95].

The impossibility of optimum simultaneous collection of photons from long crystals, however, does not preclude achieving of a high coincidence/single ratio μ. This can be explained by the perfect rotational symmetry of the collinear emission mode: if one of the photons from the pair is emitted within the acceptance angular region of the single-mode fibre, the other photon must occupy this region as well, even in the case of non-optimum focusing of the collection mode. This hypothesis is evidently verified in the experiment, where we measured $\mu \approx 0.38$ for crystals with the length of $L = 15.76$ mm. Taking into account the limited detection efficiency and other losses in the set-up, such as the reflection at the tips of the fibers (together $> 10\,\%$) and the optics in the path of down-conversion photons ($> 3\,\%$) or the insertion loss of the WDM ($> 5\,\%$), the moderate estimate of the net coupling efficiency reaches values as high as $90\,\%$.

Entanglement quality. To verify the entanglement of photon pairs, the degree of polarization correlations in two complementary bases was measured using a pair of polarizers. After correction for accidental coincidences, we obtain a visibility of $\mathcal{V}_{\mathrm{H/V}} = 98.85 \pm 0.11\,\%$ in the horizontal/vertical basis and $\mathcal{V}_{45} = 98.48 \pm 0.13\,\%$ in the basis rotated by 45°, see Fig. 3.26. The corrected visibilities are, within errors, consistent with those obtained at low pump power of about 1 mW, where accidental coincidences are negligible. The gap between the measured value and the maximum quantum-interference visibility is attributed to polarization-dependent loss inside the WDM rather than to the state preparation.

We note that the removal of one of the compensation YVO_4 elements from the set-up was accompanied with a dramatic drop of quantum-interference visibility. In order to confirm that high-purity polarization entanglement can be achieved in the narrow-

[11] The applied divergence of the collection mode was optimized with regard to maximum photon-pair flux obtained in the balanced configuration. Although the reduction of collection-mode divergence results in a relaxation of the tolerances imposed on the positioning of its focus, the reduced angular range implies a coupling of a smaller proportion from the total SPDC emission and thus smaller detected rate.

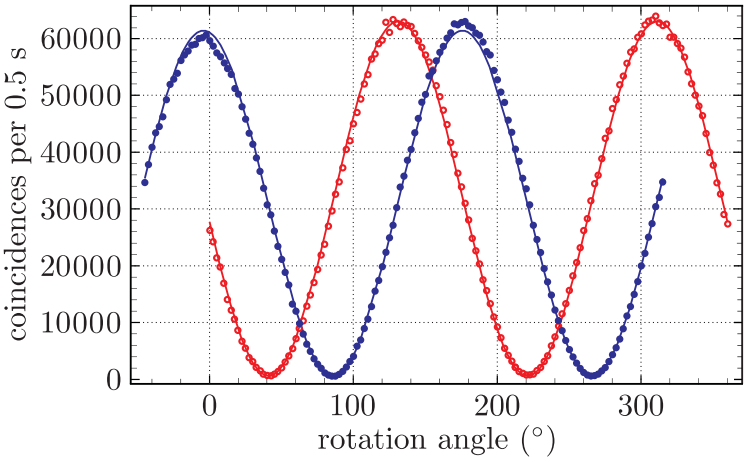

Figure 3.26: Polarization correlations between photons measured in the H/V (red points) and +45/-45 (blue points) polarization bases. The solid lines in corresponding colors are $\sin^2$ fits to the measured coincidence count rates, yielding visibilities of about 98.5 % in both bases.

band pumping regime even without YVO_4 crystal preceding the down-conversion BBO crystals (for explanation see section 3.4.2), the external cavity laser diode with the spectral line-width of < 50 MHz was applied as the pump. The measurement of polarization correlations yielded the visibility of above 98 % also without a compensation in the pump beam, thereby supporting the conclusions of the theoretical model.

CHSH-inequality violation. The measurement of CHSH-type Bell inequality was accomplished at the maximum pump power of LD using a pair of polarizers. By performing the whole measurement within 16 s (i.e., $T_I = 1$ s per angle setting), we obtained the value of the correlation coefficient of $S = 2.80399 \pm 0.00125$. This corresponds to a violation of the inequality by 694 standard deviations. The specified values assume the correction of raw data for accidental coincidences. Note that an even higher violation should be possible with the present source if one employs the optimized polarization analysis with high-transmission elements. The corresponding speed of CHSH violation $[= (S-2)/(\sigma_S\sqrt{T_I})]$ is $694\,\sigma_S$ s$^{-1/2}$.

Spectrum. The fibre-coupled down-conversion light was spectrally analyzed using the grating spectrometer with single-photon sensitivity and a measured resolution of about 1.2 nm. The bandwidths of photons determined from the gaussian fits to the measured data were found to be $\Delta\lambda_1 = 14.56 \pm 0.72$ nm and $\Delta\lambda_2 = 15.38 \pm 1.23$ nm at the non-degenerate wavelengths of $\lambda_1 = 762.8 \pm 0.4$ nm and $\lambda_1 = 849.4 \pm 0.6$ nm, see Fig. 3.27. Taking into account the given wavelength resolution of the spectrometer, the measured values are consistent with the theoretical widths of $\Delta\lambda_1 = 11.86$ nm and $\Delta\lambda_2 = 12.85$ nm.

The spectra of down-conversion photons were measured for shorter BBO crystals with $L = 7.88$ mm and $L = 3.94$ mm as well. In the first case we obtained the widths of $\Delta\lambda_1 = 18.65 \pm 1.74$ nm and $\Delta\lambda_2 = 22.37 \pm 2.23$ nm, which are again in a reasonable agreement with the theoretically inferred values of $\Delta\lambda_1 = 16.21$ nm and $\Delta\lambda_2 = 16.94$

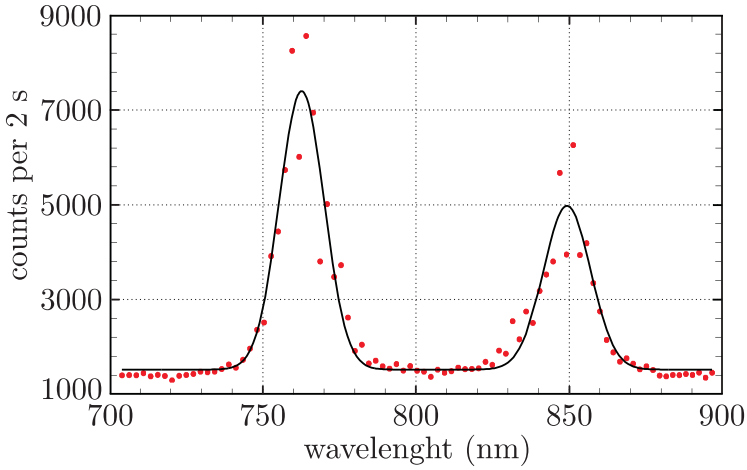

Figure 3.27: Spectral distribution of down-conversion light collected into a single-mode fibre. The solid line shows a Gaussian fit to the measured data. The photons of the pair are centered on the wavelengths of $\lambda_1 = \approx 763$ nm and $\lambda_2 = \approx 849$ nm, which agree well with the operation wavelengths of WDM. The lower peak number of counts at λ_2 is attributed to a reduced efficiency of the spectrometer towards NIR wavelengths and the offset of ≈ 1100 counts is due to dark counts of the APDs.

nm. For $L = 3.94$ mm we measured $\Delta\lambda_1 = 31.21 \pm 1.68$ nm and $\Delta\lambda_2 = 40.33 \pm 1.91$ nm. This has to be compared to theoretically determined widths of $\Delta\lambda_1 = 30.75$ nm and $\Delta\lambda_2 = 31.03$ nm.

Spectral brightness. From the afore-mentioned results we infer that the spectral brightness of the source increased from the initial rate of $B^{(s)} \approx 650$ s^{-1}nm^{-1}mW^{-1} for $L = 3.94$ mm to $B^{(s)} \approx 1220$ s^{-1}nm^{-1}mW^{-1} for $L = 7.88$ mm and finally to $B^{(s)} \approx 1800$ s^{-1}nm^{-1}mW^{-1} for the crystal length of $L = 15.76$ mm. Fitting the experimentally recorded growth of brightness in dependence on the crystal length, we obtain the scaling of $B^{(s)} \propto L^{0.72}$. This is considerably slower than the theoretically assumed dependence of $B^{(s)} \propto L$ for degenerate phase-matching. Due to the fact that at a high non-degeneracy the phase-matched down-conversion width approaches that obtained in type II phase matching (see also Fig. 2.3), it seems that even faster scaling of up to $B^{(s)} \propto L\sqrt{L}$ should be obtained in such a case. The slower increase of the experimentally inferred scaling of $B^{(s)}(L)$, compared to that inferred theoretically, is due to the two-crystal geometry of the SPDC emission, which does not allow the optimum simultaneous coupling of photons from both crystals.

3.4.6 Discussion and outlook

The recorded performance of the source shows to be extraordinarily high. To the best of our knowledge, the achieved brightness is the highest using a conventional crystal [73] and at the level of the best results obtained with quasi-phase matched

periodically poled crystals [75, 105]. Together with the purity of the polarization entanglement, which appears to be only limited by a weak depolarization effect in WDM, we could measure the violation of CHSH inequality as high as $694\,\sigma_S$ $\mathrm{s}^{-1/2}$. This exceeds even the speed of $468\,\sigma_S$ $\mathrm{s}^{-1/2}$, inferred from the results reported using an ultra-bright source, where almost 10 times higher pump power was applied to the down-conversion crystals [73]. The only shortcoming in the source characteristics lies in the down-conversion spectra, which might appear to be rather broad with regard to certain applications. Nevertheless, we have theoretically shown that a substantial reduction of the spectral widths should be feasible when applying a pump light with sufficiently long coherence length. This was also verified experimentally to some extent, by observing a reduction of spectral widths by about 6 nm in narrow-band pumping regime for BBO crystals with the length of $L = 3.94$ mm.

The use of other materials with higher nonlinearity, such as bismuth triborate (BiB_3O_6), or the use of quasi-phase matched periodically poled crystals, such as periodically poled potassium titanyl phosphate ($KTiOPO_4$), will lead to further immense improvement of the source parameters regarding the bandwidth of down-conversion photons and its brightness. For example, the relative magnitude between the effective nonlinearities of BiB_3O_6 ($d_{\mathrm{eff}} = 3.41$ pm/V) and BBO ($d_{\mathrm{eff}} = 1.93$ pm/V) implies an increase in photon-pair yield by a factor ≈ 3. At the same time the calculation predicts the reduction of the phase-matched spectra to below 3 nm for narrow-band pumping (for $L = 15.76$ mm) and to about 10 nm, when the pump source is a free-running blue laser diode. In case of quasi-phase matched $KTiOPO_4$ ($d_{\mathrm{eff}} \approx 9.5$ pm/V, [106]), an even higher relative ratio of the effective nonlinearities of ≈ 5 is reached, which suggests that an increase of the brightness by a factor of 15–25 should be certainly feasible. Remarkably, this potential brightness is at the level of the best results reported using four-wave mixing process in the optical fibres [83]. The already demonstrated performance and the future prospects for its improvement, along with the simple configuration requiring minimum alignment, make this type of source an especially promising candidate for integration into future practical applications.

Apart from the practical motivations, the described source might find its relevance also in fundamental tests of quantum mechanics. Particularly, to eliminate the fair-sampling hypothesis in photonic Bell tests, high detection and collection efficiencies of entangled photon pairs are indispensable; for a brief introduction into the problem see also section 1.1.3. The lower bound on the overall coincidence/single ratio necessary to close detection loophole has been proven to be $2(\sqrt{2}-1) \approx 0.83$ (assuming all other aspects of the experiment to be ideal) [107], which, in the limit of no background noise, reduces to $2/3 \approx 0.67$ [108]. Whereas high detection efficiencies in the visible spectral region of up to $\eta = 90$ % have been reported with visible-light photon counters (VLPC) [12], the experimental demonstration of the required collection efficiency of entangled photon pairs is missing. With our source we achieved the coincidence/single ratio of $\mu \approx 0.38$ (detection efficiency $\eta \approx 0.51$), to our knowledge the highest value ever reported (for comparison see appendix A.2). Scaling our result to a VLPC detection efficiency of $\eta = 90$ %, we arrive at the overall coincidence/single ratio of

0.67, i.e. exactly at the theoretical limit for successful detection loophole-free Bell test for no background. The further increase of this ratio to ≈ 0.8 should be possible after eliminating the current inefficiencies inherent in the source, including the reflection at the tips of the single-mode fibers or absorption in other optical elements placed in the path of the down-conversion photons. Our results are very encouraging and indeed, move the feasibility of a loophole-free photonic Bell test into the realm of state-of-the-art technologies.

Chapter 4

Single-qubit multiparty quantum communication

This chapter deals with two distinct multiparty communication tasks, the secret sharing and communication complexity. Whereas the goal of the first is to split a secret among several parties in a way that its reconstruction requires their collaboration, the latter aims at reducing the amount of communication during distributed computational tasks. We describe the simple and practical quantum-assisted solutions of both tasks and show their proof-of-principle experimental implementations.

The use of quantum resources leads to a speed-up in solving many communication tasks or even achieving goals which are classically not possible at all. Probably the best-known example is quantum key distribution, the first commercialized application of quantum information science. While there is already quite a number of other two-party tasks demonstrated in the lab, there is hardly anything for more than two parties. This is due to the fact that most of such tasks require as a resource multiparty entangled states, which are very difficult to be produced with current methods and moreover suffer from a high noise.

In the following it is shown that entanglement is not the only non-classical resource giving quantum information processing its power. Instead, only sequential communication and transformation of a single qubit can be sufficient to accomplish certain tasks. Such simplification makes multiparty communication tasks feasible and, most importantly, technologically comparable to quantum key distribution. This we demonstrate for two distinct multiparty communication tasks, communication complexity [109] and secret sharing [110].

The chapter is subdivided into two parts. The first part is concerned with communication complexity. After it, the section analyzing secret sharing follows.

4.1 Communication complexity

4.1.1 Introduction

Complexity theory addresses the problem of reduction of inherent costs required for solving information processing tasks. In its most widespread branch, computational complexity, the inherent costs are traditionally measured by the number of operations required and/or the amount of memory spent during a large-scale computation. Here, we deal with yet another type of problems - communication complexity problems (CCPs) - where the resource under investigation and aimed to be minimized is the amount of communication during distributed computation.

The notion of communication complexity was introduced by Andrew Yao [111], who investigated the following two-party scenario: The parties $\mathcal{P}_1$ and $\mathcal{P}_2$ receive each an n-bit string X_1 and X_2 with the common goal to compute the value of a given function $T(X_1, X_2)$. Before distribution of the strings, the parties are allowed to communicate freely and prepare themselves jointly in any way, e.g., by sharing classically correlated random variables, agreeing on a common strategy etc. However, once received, they must communicate as little as possible. The question is how many bits of information exchange then is enough to compute $T(X_1, X_2)$, or alternatively how high is the probability to reach the correct value of $T(X_1, X_2)$ under a specific communication restriction.

In general terms CCPs are aimed at finding the communication protocols minimizing the amount of information that parties, performing some *local* computation, have to exchange in order to accomplish some *globally* defined goal. This abstract problem finds its relevancy in many contexts: First and foremost in distributed computing, where enhancing the communication efficiency among the local computers, processing in parallel a large-scale computational task, leads to a speed-up. Besides, the problem finds its practical use in optimizing the design of Very Large Scale Integrated (VLSI) circuits or computer networks as well as in studies of data structures (for survey of the field, see [112]).

4.1.2 Quantum-assisted communication complexity

The pioneer of communication complexity, Andrew Yao, was also the first who introduced a *qubit-communication* model, where the parties are allowed to exchange qubits rather than bits [113]. It is not immediately clear whether this variation might bring some savings in communication, given a fundamental theorem in quantum information theory by Holevo [114]. The theorem implies that the mutual information between two unentangled parties cannot increase by more than one bit per qubit of communication between them. This still holds even if the communication is not restricted to be one-way [115]. More generally, if the parties share a prior entanglement the information capacity of communication increases to maximally two bits per exchanged qubit [16].

The first example that quantum-assisted protocols enhance the communication efficiency compared to any known classical ones, was given by R. Cleve *et al.* [116]. They considered a different model than that of Yao, the *entanglement* model, where in addition to the classical communication we allow the parties to perform measurements on previously shared set of qubits in an entangled state. As with the qubit model, there are no trivial communication advantages in this model, because entanglement alone cannot be used to signal information. Even though, R. Cleve *et al.* showed that entanglement can act as a substitute for communication, when the goal is to compute inner product function with the data distributed among three parties.

Since then, it was theoretically proven that entanglement or qubit communication can help to solve a range of tasks more efficiently compared to the best classical scenarios [115, 117, 118, 119, 120]. For some tasks even an exponential separation in efficiency between quantum and classical protocols was demonstrated [121, 122]. Moreover, the generic link between the classical/quantum conflict exposed by Bell's theorem and the advantage of quantum communication complexity protocols over the classical ones, was shown in [123, 124]. It was established there that the violation of Bell's inequality is the criterion of the advantage of the quantum protocols over the classical ones.

Despite many theoretical results, to date no experiment showing a genuine quantum advantage in solving CCPs has been reported; see also feasibility studies [125, 126]. The only laboratory demonstrations corrected the measured results for the experimental inefficiencies [127, 128], and thus did not provide the conclusive and unambiguous practical manifestation of the superiority of quantum-assisted protocols in distributed computations.

4.1.3 Communication complexity problems

In general, one can distinguish two types of CCPs, related to the following two questions: (i) What is the minimal amount of communication for the parties to determine the value of a searched function T with the success probability of $P = 1$, that is with certainty [115, 118, 119]? (ii) What is the highest possible probability of success P if only a restricted amount of communication is allowed [119, 123, 124, 125]? The particular tasks might further differ according to whether all the parties or only one of them are required to determine the value of T, whether they are restricted to a certain communication architecture (such as sequential or tree-like communication), etc.

In the following we consider only the second class of problems. This choice is motivated primarily by the goal of performing a fair comparison between the optimum classical protocol and the quantum-assisted protocol in a realistic experiment, which is inherent of many inefficiencies. Whereas the inefficiencies are directly reflected in the reduction of the measured success probability P_{exp}, which is readily compared to the classically allowed value, it is not directly obvious how to deal with the issue of experimental imperfections in the first class of problems. Let us now introduce the

two CCPs analyzed and implemented here [109].

Problem A. The problem A is the so-called *modulo-4 sum* problem. It was first defined for three parties by Buhrman *et al.* [119] and later generalized to N parties in [118]. The problem in the setting with restricted communication is stated as follows: Imagine N separated partners $\mathcal{P}_1, \ldots, \mathcal{P}_N$. Each of them receives a two-bit input string X_k, $(X_k = 0, 1, 2, 3; k = 1, \ldots, N)$. The X_ks are distributed such that their sum is even, i.e., $(\sum_{k=1}^{N} X_k) \mathrm{mod} 2 = 0$. No partner has any information whatsoever on the values received by the others. Next, the partners communicate with the goal that one of them, say $\mathcal{P}_N$, can tell whether the sum modulo-4 of all inputs is equal 0 or 2. That is, $\mathcal{P}_N$ should announce the value of a dichotomic function[1] $T(X_1, \ldots, X_N)$ given by $T_A = 1 - (\sum_{k=1}^{N} X_k \mathrm{mod} 4)$. The total amount of communication is restricted to only $N-1$ bits (classical scenario). The partners can freely choose a communication protocol as long as it does not depend on input data[2]. Such a dependence would imply a violation of the communication restriction.

An alternative description of the task A, simplifying the calculation of the maximum classical success probability and making the connection with the task B more visible, can be introduced. It puts the probability distribution for local data as

$$p_A(X_1, \ldots, X_N) = \frac{1}{2^{2N-1}} \left| \cos\left(\frac{\pi}{2} \sum_{k=1}^{N} X_k \right) \right|, \tag{4.1}$$

and the global task function as

$$T_A(X_1, \ldots, X_N) = \cos\left(\frac{\pi}{2} \sum_{k=1}^{N} X_k \right). \tag{4.2}$$

Problem B. Problem B has a similar structure as A, but now N *real* numbers $X_1, \ldots, X_N \in [0, 2\pi)$ with probability density

$$p_B(X_1, \ldots, X_N) = \frac{1}{4(2\pi)^{N-1}} \left| \cos(X_1 + \ldots + X_N) \right| \tag{4.3}$$

are distributed to the partners. Their task is to compute whether $\cos(X_1 + \ldots + X_N)$ is positive or negative, i.e. to give the value of the dichotomic function

$$T_B = S\left[\cos\left(\sum_{k=1}^{N} X_k \right) \right], \tag{4.4}$$

[1] A dichotomic function is a function with a range restricted to two values of ± 1.

[2] E.g. they can choose between sequential communication from one to the other, or any arbitrary tree-like structure ending at the last party $\mathcal{P}_N$.

where $S(x) = x/|x|$. The communication restriction is the same as for problem A, i.e., only $N-1$ bits are allowed to be exchanged.

4.1.4 Optimal classical protocol

To find the best performing protocols for these two CCPs, it is convenient to first rewrite the random inputs X_ks. For the task A we put $X_k = (1-y_k) + x_k$, where $y_k \in \{-1, 1\}$, $x_k \in \{0, 1\}$. For the task B we write $X_k = \pi(1-y_k)/2 + x_k$, with $y_k \in \{-1, 1\}$, $x_k \in [0, \pi)$. Accordingly, the task function T can now be reformulated in a common form: $T = f(x_1, \ldots, x_N) \prod_{k=1}^{N} y_k$ and $p(X_1, \ldots, X_N) = 2^{-N} p'(x_1, \ldots, x_N)$[3]. Specifically, for the task A we have $f = f_A = \cos(\frac{\pi}{2} \sum_{k=1}^{N} x_k)$ with $p' = p'_A = 2^{-N+1} |\cos(\frac{\pi}{2} \sum_{k=1}^{N} x_k)|$, and for the task B, $f = f_B = S[\cos(\sum_{k=1}^{N} x_k)]$ with $p' = p'_B = 2^{-1}\pi^{-N+1} |\cos(\sum_{k=1}^{N} x_k)|$.

We note that the dichotomic variables y_k are not restricted by the probability distributions, p, for the X_ks. Thus, they are completely random. Furthermore, since T is proportional to the product of *all* y_ks, the answer $e_N = \pm 1$ of $\mathcal{P}_N$ is completely random with respect to T, if it does not depend on *every* y_k. Thus, an unbroken communication structure is necessary: the information from all $N-1$ partners must directly or indirectly reach $\mathcal{P}_N$. Due to the restriction to $N-1$ bits of communication each of the partners, $\mathcal{P}_k$, where $k = 1, \ldots, N-1$, sends only an one-bit message, which for convenience will be denoted as $e_k = \pm 1$.

The task function T as well as the answer e_N of $\mathcal{P}_N$ takes only two values, ± 1. If the answer is correct, then $T = e_N$ and thus $Te_N = 1$; otherwise, $Te_N = -1$. Therefore, following [124] we can quantify the average success of the protocol with the fidelity $F = \sum_{X_1, \ldots, X_N} pTe_N$, or equivalently

$$F = \frac{1}{2^N} \sum_{x_1, \ldots, x_N = 0,1} p'(x_1, \ldots, x_N) f(x_1, \ldots, x_N) \times \sum_{y_1, \ldots, y_N = \pm 1} \prod_{k=1}^{N} y_k e_N(x_1, \ldots, x_N; y_1, \ldots, y_N) \quad (4.5)$$

For the problem B integrations replace summations ($\sum_{x_k} \to \int_0^\pi \mathrm{d}x_k$); the probability of success reads $P = (1+F)/2$.

In any classical protocol the answer e_N given by $\mathcal{P}_N$ can depend on y_N, x_N, and on the messages, $e_{i_1}, \ldots, e_{i_\ell}$, received directly from partners $\mathcal{P}_{i_1}, \ldots, \mathcal{P}_{i_\ell}$. That is, $e_N = e(x_N, y_N, e_{i_1}, \ldots, e_{i_\ell})$. Let us fix x_N, and treat e as a function e_{x_N} of the remaining $\ell + 1$ dichotomic variables, $y_N, e_{i_1}, \ldots, e_{i_\ell}$. In the $2^{\ell+1}$ dimensional space of such functions one has an orthogonal basis given by $V_{jj_1 \ldots j_\ell}(y_N, e_{i_1}, \ldots, e_{i_\ell}) = y_N^j \prod_{k=1}^{\ell} e_{i_k}^{j_k}$,

[3]This reformulation enables one to adopt the mathematical formalism developed for entanglement-assisted communication complexity models in [123, 124].

where $j, j_1, \ldots, j_\ell = 0, 1$. Thus, one can expand e_{x_N}:

$$e_{x_N} = \sum_{j,j_1,\ldots,j_\ell=0,1} c_{jj_1\ldots j_\ell}(x_N) y_N^j \prod_{k=1}^{\ell} e_{i_k}^{j_k}, \tag{4.6}$$

where

$$c_{jj_1\ldots j_\ell}(x_N) = \frac{1}{2^{\ell+1}} \sum_{y_N, e_{i_1},\ldots,e_{i_\ell}=\pm 1} e_{x_N} V_{jj_1\ldots j_\ell}.$$

Since $|e_{x_N}| = |V_{jj_1\ldots j_\ell}| = 1$, one has $|c_{jj_1\ldots j_\ell}(x_N)| \leq 1$. We put the expansion to Eq. (4.5). As, $\sum_{y_N=\pm 1} y_N y_N^0 = 0$, and $\sum_{y_k=\pm 1} y_k e_k^0 = 0$, only the term with $j, j_1, \ldots, j_\ell = 1$ in expansion (4.6) can give a non-zero contribution to F_c. Thus, without changing the result of Eq. (4.5), e_N in (4.5) can be replaced by a function $e'_N = y_N c_N(x_N) \prod_{k=1}^{\ell} e_{i_k}$, where $c_N(x_N)$ stands for $c_{11\ldots1}(x_N)$. Next, notice that, e.g., e_{i_1}, which is in the formula for e'_N, can depend only on x_{i_1}, y_{i_1} and the messages obtained by $\mathcal{P}_{i_1}$ from a subset of partners: $e_{p_1}, \ldots, e_{p_m}$ (this set does not contain any e_{i_k}). In analogy with (4.6), e_{i_1}, for a fixed x_{i_1}, can be expanded in terms of orthogonal basis functions:

$$e_{i_1} = \sum_{j,j_1,\ldots,j_m=0,1} c'_{jj_1\ldots j_m}(x_{i_1}) y_{i_1}^j \prod_{k=1}^{m} e_{p_k}^{j_k}. \tag{4.7}$$

Again, $|c'_{jj_1\ldots j_m}(x_{i_1})| \leq 1$. If one puts this into e'_N one obtains for the fidelity

$$F_c = \frac{1}{2^{N-2}} \sum_{x_1,\ldots,x_N} g(x_1, \ldots, x_N) c_N(x_N) c_{i_1}(x_{i_1}) \sum_{y'} \prod_{k\neq N, i_1} y_k \prod_{r=1}^{m} e_{p_r} \prod_{k=2}^{\ell} e_{i_k}, \tag{4.8}$$

where $g = p' f$, $c_{i_1}(x_{i_1}) = c'_{11\ldots1}(x_{i_1})$, and $\sum_{y'}$ represents summation over $y_1, \ldots, y_{i_1-1}$, $y_{i_1+1}, \ldots, y_{N-1} = \pm 1$. Note that each message appears in the product only once. We continue this procedure of expanding the messages, till it halts (i.e., till we reach the level of those partners who do not receive any messages). The end result is

$$F_c = \sum_{x_1,\ldots,x_N} g(x_1, \ldots, x_N) \prod_{n=1}^{N} c_n(x_n), \tag{4.9}$$

with $|c_n(x_n)| \leq 1$. Since F_c in Eq. (4.9) depends on the product of local functions $c_n(x_n)$, it has to be bounded from above, i.e., $|F_c| \leq \mathcal{B}(N)$, where $\mathcal{B}(N)$ is the maximum classical fidelity. The reasoning is similar to that leading to Bell inequalities[4] [123, 124]. The extrema of F_c are at the limiting values $c_n(x_n) = \pm 1$, because F_c is linear in every $c_n(x_n)$. It becomes apparent now that the class of protocols, in which the partners $\mathcal{P}_1$ to $\mathcal{P}_{N-1}$ calculate $e_k = y_k c_k(x_k)$, with $c_k(x_k) = \pm 1$, and send

[4] As a matter of fact the inequality $|F_c| \leq \mathcal{B}(N)$, where F_c is defined in (4.9), is an algebraic version of a general Bell inequality for N observers.

the result, encoded in e_k, to $\mathcal{P}_N$, who puts $e_N = \prod_{k=1}^{N} y_k c_k(x_k)$, contains an optimal protocol of fidelity $\mathcal{B}(N)$.

The specific forms of the bound $\mathcal{B}(N)$ for our problems A and B are calculated in appendix B.1. In both cases the fidelity decreases exponentially with the number of parties N. For the task A we found $F_{c,A} \leq 2^{-K+1}$, where $K = N/2$ and $K = (N+1)/2$ for even and odd numbers of parties, respectively. This analytic result confirms the numerical simulations of [125] for small N. For the task B we derived $F_{c,B} \leq (2/\pi)^{N-1}$.

4.1.5 Optimal quantum protocol

For the quantum protocols, we note that the Holevo bound [114] limits the information storage capacity of a qubit to no more than one classical bit. Thus, we must now restrict the communication to $N-1$ qubits, or alternatively, to $N-1$-fold exchange of a *single* qubit.

The optimal solution of the task A starts with a qubit in the state $|\psi_0\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle)$. Parties then sequentially act on the qubit with the phase-shift transformation $|0\rangle\langle 0| + e^{i\pi X_k/2}|1\rangle\langle 1|$, in accordance with their local data X_k. After all N phase shifts the state takes the form:

$$|\psi_N\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\pi(\sum_{k=1}^{N} X_k)/2}|1\rangle). \tag{4.10}$$

Since the sum over X_k is even, the phase factor $e^{i\pi(\sum_{k=1}^{N} X_k)/2}$ is equal to the dichotomic function T_A to be computed. Thus, a measurement of the qubit in the basis $(|0\rangle \pm |1\rangle)/\sqrt{2}$ reveals the value of T_A with fidelity $F_{q,A} = 1$, that is, *always* correctly.

Task B starts also with a qubit in the state $|\psi_0\rangle$. Each party performs according to his/her local data a unitary transformation $|0\rangle\langle 0| + e^{iX_k}|1\rangle\langle 1|$, leading to

$$|\psi_N\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\sum_{k=1}^{N} X_k}|1\rangle). \tag{4.11}$$

The last party makes the same measurement as in the task A. The probability for the detection of state $1/\sqrt{2}(|0\rangle \pm |1\rangle)$, which we associate with the result $r = \pm 1$, is given by $P(\pm) = [1 \pm \cos(\sum_{k=1}^{N} X_k)]/2$. The expectation value for the final answer $e_N = r$ is $E = P(+) - P(-)$, and reads $\cos(\sum_{k=1}^{N} X_k)$. The fidelity of e_N, with respect to T_B is

$$F_{q,B} = \int_0^{2\pi} \mathrm{d}X_1 \ldots \int_0^{2\pi} \mathrm{d}X_N p_B(X_1, \ldots, X_N) T_B(X_1, \ldots, X_N) E(X_1, \ldots, X_N). \tag{4.12}$$

With the actual forms of p_B, T_B, and E, one gets $F_{q,B} = \pi/4$, i.e., the protocol gives the correct value of T_B with probability $P_{q,B} = (1 + \pi/4)/2 \approx 0.892$.

For both problems the classical fidelity F_c or the probability of success P_c decreases

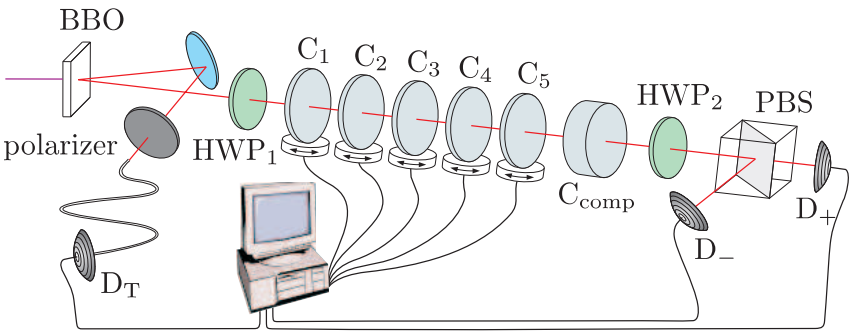

Figure 4.1: Experimental set-up for qubit-assisted CCPs. Pairs of orthogonally polarized photons are emitted from a BBO crystal via the type-II SPDC process. The detection of one photon by the trigger detector D_T indicates the existence of the protocol photon. The polarization state is prepared with a half-wave plate (HWP_1) and a polarizer, placed in the trigger arm. Each of the parties introduces a phase-shift by the rotation of a birefringent YVO_4 crystal (C_1 to C_5). The last party performs the analysis of a photon-polarization state using a half-wave plate (HWP_2) followed by a polarizing beam-splitter (PBS).

exponentially with growing N to the value corresponding to a random guess by $\mathcal{P}_N$. I.e., communication becomes useless. In contrast, P_q does not change with N. For the task A it equals 1, and for B we have ≈ 0.892. The simple, one qubit assisted quantum protocol, without any shared multi-particle entanglement, clearly outperforms the best classical protocols.

4.1.6 Implementation

We implemented the quantum protocols for $N = 5$ parties [109], using a heralded single photon as the carrier of the qubit communicated sequentially by the partners. The qubit was encoded in the polarization, so that the computational basis, "0" and "1", corresponds to horizontal H and vertical V linear polarization, respectively. The data X_k of each party was encoded on the qubit via a phase shift, using birefringent materials. The last party performed a measurement in the basis $1/\sqrt{2}(|H\rangle \pm |V\rangle)$ to obtain the answer e_N.

The experimental set-up is shown in Fig. 4.1. Time-correlated photon pairs are produced via non-collinear SPDC process in a 2-mm-long BBO crystal pumped by a blue LD ($\lambda_p = 402.5$ nm) with the output optical power of about 10 mW. The detection of one photon by the trigger detector D_T heralds the existence of the other one used in the protocol. The narrow gate window of 4 ns for coincidence detection between these two photons, along with the single-count rates of ≈ 140000 s^{-1} at the detectors D_+ and D_-, warrant that the recorded data are due to single photons only[5].

[5]The probability of having more than one photon per heralding signal and during time corresponding to the gate window is estimated to 2×10^{-3}, assuming the given parameters and the Poissonian photon-number statistics of SPDC photons.

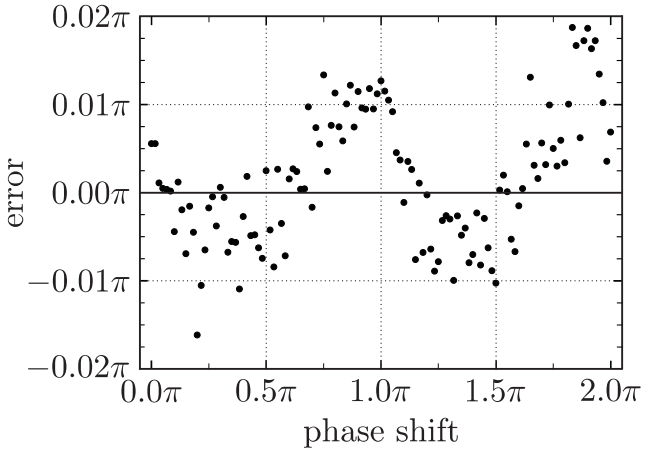

Figure 4.2: Deviation of the phase shift by an YVO_4 crystal from the expected value, measured over the full range $[0, 2\pi]$ in steps of $\pi/60$.

Since a type II degenerate phase-matching scheme is used, the emitted photon pairs at $\lambda = 805$ nm ($\Delta\lambda \approx 6$ nm) are orthogonally polarized. Filtering of the vertical polarization for the trigger photons, ensures that the protocol photon has horizontal polarization initially. A half-wave plate (HWP_1) transforms the qubit to the initial state $1/\sqrt{2}(|H\rangle + |V\rangle)$ as required by the optimal quantum protocol.

The individual phase shifts of parties are implemented using a 200 μm thick Yttrium-Vanadate (YVO_4) birefringent uniaxial crystals (C_i). The crystals, cut with their optic axes parallel to the surface, are aligned in such a way that H and V polarization states correspond to their normal modes. In this configuration the difference between optical paths of horizontal and vertical polarization can be continuously tuned using motor-driven rotations of the crystals along their optic axes, thereby allowing to set any desired phase-shift from 0 to 2π independently from the incoming polarization state. The precision in applying an arbitrary phase shift was measured to be better than 0.02π over the full phase range, see Fig. 4.2. An additional YVO_4 crystal (C_{comp},1000 μm long), aligned with its optic axis in the plane perpendicular to the direction defined by the optic axes of the previous crystals, is used to compensate dispersion effects (for details, see [129]). To analyze the polarization state of photons in the basis $(|0\rangle \pm |1\rangle)/\sqrt{2}$, a half wave-plate ($HWP_2$) at an angle of 22.5° followed by polarizing beam-splitter (PBS) is used.

For a fair comparison of the quantum protocols with the classical ones, no heralded events are discarded, even if the detection of the protocol photon fails. In such a case one can still guess the value of T, but with success rate of only 1/2. Therefore, a high detection efficiency η of the heralded photons, i.e. high coincidence/single ratio for our set-up, is essential for an unambiguous demonstration of the superiority of the qubit-assisted protocol[6]. To minimize the cases with no detection of the photon, the yield of heralded photons was maximized by adopting an unbalanced SPDC scheme. We select a restricted spatial mode with well defined polarization of the trigger photons by

[6]E.g., in a realistic implementation of the five-party problem A, the efficiency of $\eta \gtrsim 0.33$ was estimated to be sufficient to beat the optimum classical protocol, see [125].

coupling them into a single-mode fiber behind a polarizer, whereas no spatial filtering is performed on the protocol photons. As a result, we observed ≈ 5000 trigger events per second at the detector D_T with ≈ 2400 coincident events per second of protocol detections, i.e. an overall detection efficiency of $\eta \approx 0.48$, close to the limit given by the detector efficiency of our silicon APDs (measured to be about $\approx 55\,\%$).

The protocols were run many times, to obtain sufficient statistics. Each run took about one second. It consisted of generating a set of pseudorandom numbers obeying the specific distribution, subsequent setting of the corresponding phase shifts, and opening detectors for a collection time window τ. The limitation of communicating one qubit per run requires that only these runs, in which exactly one trigger photon is detected during τ, are selected for the evaluation of the probability of success P_{exp}. To maximize the number of such runs, n, the length of τ was optimized to 200 μs, assuming a Poissonian photon-number distribution of SPDC photons.

We merely remark that essentially the same set-up could be used to solve the CCPs using bright polarized pulses. However, in such a case, a suitable polarization measurement of the pulses reveals all the encoded input data of any party: two bits for the task A, and arbitrarily many for the task B. Thus, the communication restriction to $N-1$ bits is violated. Attenuation of the pulses to the single-photon level does not help either. The efficiency of the protocol is significantly lowered in such a case, due to many non-detection events, forcing one to guess the answer most of the time.

4.1.7 Results

In order to determine the probability of success from the data acquired during the runs we have to distinguish the following two cases. First, the heralded photon is detected, which happens with probability η, given by the coincidence/single ratio. Then, the answer e_N can be based on the measurement result. However, the answer is correct only with a probability γ, due to experimental imperfections in the preparation of the initial state, the setting of the desired phase shifts, and the polarization analysis. This must be compared with the theoretical limits given by $P_{q,A}$ and $P_{q,B}$ for the task A and B, respectively. Second, with the probability $1-\eta$ the detection of the heralded photon fails. Forced to make a random guess, the answer is correct in half of the cases. This leads to an overall success probability $P_{exp} = \eta\gamma + (1-\eta)0.5$, or a fidelity of $F_{exp} = \eta(2\gamma - 1)$.

Due to a finite measurement sample, our experimental results for the success probability are distributed around the value P_{exp} as shown in Fig. 4.3 for both tasks. The width of the distribution is interpreted as the error in the experimental success probability. For the task A we obtain a quantum success probability of $P_{exp,A} = 0.711 \pm 0.005$. The bound $P_{c,A} = 5/8$ of the optimal classical protocol for $N = 5$ parties is violated by 17 standard deviations. For the task B we reached $P_{exp,B} = 0.669 \pm 0.003$, whereas the classical bound is $P_{c,B} \approx 0.582$. The violation is by 29 standard deviations. Expressing the final results in terms of fidelities, we obtain

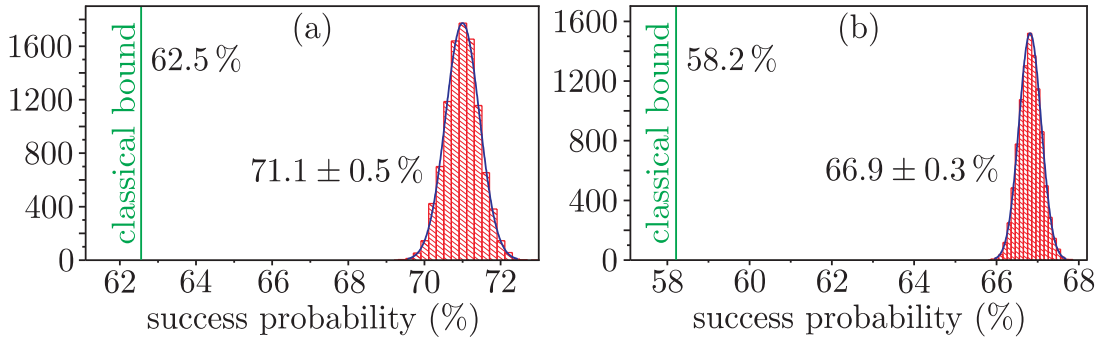

Figure 4.3: Histograms of measured quantum success probabilities (a) for the task A and (b) for task B. The bounds for optimum classical protocols are displayed, too.

	n	η	γ
task A	6692	0.452 ± 0.010	0.966 ± 0.003
task B	18169	0.471 ± 0.006	0.858 ± 0.004

Table 4.1: Relevant experimental parameters in the implementation of communication complexity problems A and B: n - number of correct runs, η - overall detection efficiency of heralded photons, and γ - success rate of the protocol for the fraction of the runs with detected heralded photon.

$F_{exp,A} = 0.421 \pm 0.010$ for the task A, and $F_{exp,B} = 0.337 \pm 0.006$ for the task B. This must be compared to the performance of the best classical protocol for $N = 5$ parties reaching $F_{c,A} = 0.25$ for A and $F_{c,B} \approx 0.164$ for B. Table 4.1 summarizes the relevant experimental parameters for both tasks.

4.2 Secret sharing

4.2.1 Introduction

Splitting a secret in a way that a single player or an unauthorized subset of players is not able to reconstruct it, is a common task in information processing and especially, in high security applications. Suppose, for example that a launch sequence of a nuclear missile is protected by a secret code. Yet, it has to be ensured that a single lunatic is not allowed to activate it, as well as two are not. At least three out of five officers are required to be lethal lunatics before the missile launch can be initiated. This problem, together with its many possible variations and generalizations, is called secret sharing.

The secret sharing problems are extensively studied in the framework of classical cryptography [130]. The classical solution usually involves a randomized encoding of

a secret into an n-tuple, the coordinates of which are each distributed to n different players. The encoding, i.e the partitioning of the secret into so-called shares given to players, has to be such that the reconstruction of the secret requires a specified level of concurrence by the players. This can be expressed in the majority of cases by a single number - the so-called concurrence threshold k - which means that (i) knowledge of any k or more shares makes the secret easily computable and (ii) knowledge of any $k-1$ or fewer shares leaves the secret completely undetermined in the sense that all its possible values are equally likely[7].

The two classic examples of the algorithms for the general (k, n) threshold secret sharing scheme are due to A. Shamir [131] and G. R. Blakley [132]. Shamir's technique relies on the fact that k points in an $\mathbb{R}^2$ space uniquely determine a $(k-1)^{\text{th}}$ degree polynomial, but there are infinitely many polynomials of degree $k-1$ defined by $k-1$ points. Clearly, k or more players, each knowing the coordinates of one point, are then able to recover the polynomial by interpolation of their values. The Blakley's scheme is geometric in nature. The secret is defined as a point in a k dimensional space and the shares distributed among n players are the equations of $(k-1)$-dimensional hyperplanes comprising that point. Moreover, the intersection of the hyperplanes defines the coordinates of the point. Analogously to Shamir's version, any collusion of $k-1$ or fewer players will not be able to obtain a unique point by intersecting their hyperplanes. Thus, they have no better chance of recovering the secret than an outsider who does not hold any of the shares. On the other hand, as soon as any k players concur, they can easily compute the coordinates of the point and retrieve thus the secret.

That is, both schemes are unconditionally secure in the sense that the security they provide is independent of the computing time or power that the cheater may bring to bear on subverting the system; or put in another way, even with infinite computing power the cheater can do no better than guess the secret.

4.2.2 Quantum-assisted secret sharing

So far we did not address the issue of distribution of the shares among the players. Obviously, if the shares are accessed during this phase by an eavesdropper or even by some dishonest player (i.e. by a cheater), the security of the system is ruined[8].

Unfortunately, classical and conventional cryptographic solutions offer no tools to guarantee the security of the shares during their communication to the players. They are vulnerable to eavesdropping attacks. The only provable way how to defeat eavesdropping is provided by quantum cryptography [14, 15]. Unlike the conven-

[7] In view of this definition the example with the missile launch is a $(k = 3, n = 5)$ threshold scheme.

[8] By eavesdropping we refer to an attack from an outsider, that is from a person who is not involved with the group of players whatsoever, whereas by cheating we refer to an attack from one of the players.

tional cryptography with its security relying only on computational assumptions, the security of quantum cryptography is based upon the laws of quantum mechanics, which ultimately guarantee that distributed keys cannot be captured without being irretrievably altered and therefore rendered useless - a process that is provably detectable. Therefore, quantum cryptography has to be integrated into secret sharing protocols with the principal motivation of discovering whether an eavesdropper or cheater has been active during the protocol. The most obvious way how to achieve this goal is to establish a mutual secret key with each of the players separately via a standard two-party quantum key distribution protocol and then implement a classical secret sharing procedure, such as in the Shamir's or Blakley's version. This solution is however not efficient and scalable with regard to the number n of the participating players.

An elegant way how to achieve the task of secret sharing via the resource of multiparty entanglement was outlined by Żukowski *et al.* [133][9] and later discussed in more depth by Hillery *et al.* [134]. They showed that a shared maximally-entangled GHZ-state allows the information splitting and the protection against eavesdropping simultaneously. But, due to lack of efficient and stable entangled multi-photon sources, an experimental demonstration of a working quantum secret sharing (QSS) shows to be very challenging. Till now, solely the in-principle feasibility of was shown in an experimental realization using pseudo-GHZ states [135] and very recently the scenario for three players was implemented [136].

In the following we propose a general protocol for n players, in which a sequential single qubit communication between them is used with no need for GHZ-states [110]. As our protocol requires only single qubits it is realizable with the current state-of-the-art technologies, and above all, scalable with respect to the number of participating players. These merits made the experimental demonstration of our protocol for six players possible. To grasp the essential elements in the construction of QSS let us first briefly describe the entanglement-based protocol using a multiparty GHZ state [134, 137].

4.2.3 Entanglement-based protocol

Consider a group of n players, each having a particle from the maximally-entangled n particle GHZ-state

$$|GHZ\rangle = \frac{1}{\sqrt{2}}\left(|\underbrace{00\ldots0}_{n}\rangle + |\underbrace{11\ldots1}_{n}\rangle\right), \tag{4.13}$$

[9] To be perfectly accurate the task being discussed in [133] is a bit different from secret sharing. It is often termed as "Third-Man" cryptography, and its goal is the generation of the cryptographic key between the players in such a way that its activation can be controlled by the Third Man. Nevertheless, as a matter of fact both tasks in question are very similar and their quantum-assisted solutions are closely inter-linked.

where $|0\rangle$ and $|1\rangle$ are orthogonal states in an arbitrary Hilbert space. Next, the partners randomly and independently choose the value of a local parameter $\phi_j = 0$ or $\phi_j = \pi/2$ and perform a measurement on the local particle of the observable

$$\widehat{\sigma}_j(\phi_j) = \sum_{k_j=\pm 1} k_j \, | \, k_j, \phi_j \, \rangle \langle \, k_j, \phi_j \, | , \tag{4.14}$$

with the eigenstates $|k_j, \phi_j\rangle = 1/\sqrt{2}(|0\rangle + k_j \exp(i\phi_j)|1\rangle)$, $(j = 1, 2, \ldots, n)$ associated with eigenvalues $k_j = \pm 1$. The correlation function for an n-particle GHZ state, defined as the expectation value of the product of n local results, is given by

$$E(\phi_1, \ldots, \phi_n) = \langle \prod_{j=1}^{n} \widehat{\sigma}_j(\phi_j) \rangle \; = \; \cos\left(\sum_{j=1}^{n} \phi_j \right). \tag{4.15}$$

After the measurement each player publicly announces her/his choice of ϕ_j, but keeps the result k_j secret. Then all of them know whether this procedure leads to perfect correlations, i.e. when $|\cos(\sum_j^n \phi_j)| = 1$. This happens in half of the runs. In these instances, on the basis of the perfect correlations, any subset of $n-1$ players is able to infer the measurement result of the dealer, $\mathcal{P}_D$, if and only if the players collaborate. Thereby they achieve the principal task of secret sharing in the particular setting with the threshold of $k = n - 1$[10]. One can prove that the entanglement-based scheme is unconditionally secure in the sense of the aforementioned definitions; security issues are analyzed in references [134, 139, 140].

4.2.4 Single-qubit protocol

An n party scheme [see Fig. 4.4(a)] for the *same* task, where only the sequential communication of a single qubit is used, runs as follows. The qubit is initially prepared in the state

$$|+x\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big). \tag{4.16}$$

During the protocol the qubit is sequentially communicated from one player to the other, each acting on it with the unitary phase operator

$$\widehat{U}_j(\varphi_j) = \begin{cases} |0\rangle \rightarrow |0\rangle \\ |1\rangle \rightarrow e^{i\varphi_j}|1\rangle, \end{cases} \tag{4.17}$$

[10]The efficient construction of all threshold schemes is given in [138]. It is also shown therein that for a certain class of threshold schemes the secret *must* be distributed in a globally mixed state.

with the randomly chosen value of $\varphi_j \in \{0, \pi, \pi/2, 3\pi/2\}$. Therefore, having passed all parties, the qubit will end up in the state

$$|\chi_N\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i(\sum_j^n \varphi_j)}|1\rangle\right). \tag{4.18}$$

The last party performs a measurement on the qubit in the basis $|\pm x\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ leading to the result ± 1. As it will be clarified later, for her/him it suffices to choose only between $\varphi_n = 0$ or $\varphi_n = \pi/2$. The probability that she/he detects the state $|+x\rangle$ reads

$$p_+(\varphi_1, \ldots, \varphi_n) = \frac{1}{2}\left[1 \pm \cos\left(\sum_j^n \varphi_j\right)\right], \tag{4.19}$$

whereas the probability to detect the state $|-x\rangle$ is

$$p_-(\varphi_1, \ldots, \varphi_n) = \frac{1}{2}\left[1 \pm \cos\left(\sum_j^n \varphi_j\right)\right]. \tag{4.20}$$

That is, the expectation value of the measurement is

$$E'(\varphi_1, \ldots, \varphi_n) = p_+(\varphi_1, \ldots, \varphi_n) - p_-(\varphi_1, \ldots, \varphi_n) = \cos\left(\sum_j^n \varphi_j\right). \tag{4.21}$$

Note that this expectation value (Eq. 4.21) has the same structure like the correlation function (Eq. 4.15) and can therefore also be used to obtain a shared secret. For this purpose each participant divides his action for every run into two classes: a class X corresponding to the choice of $\varphi_j \in \{0, \pi\}$ and a class Y corresponding to $\varphi_j \in \{\pi/2, 3\pi/2\}$. Following this classification they broadcast the class of their action for each run, but keep the particular value of φ_j secret. This corresponds in the GHZ scheme to the announcement of ϕ_j while keeping k_j secret. The order in which they announce the classification is each time randomly chosen. From that procedure they can determine which runs lead to a deterministic measurement result, i.e. when $\cos(\sum_j^n \varphi_j)$ equals to either 1 or -1, or equivalently, to either $p_+ = 1$ or $p_- = 1$, respectively. Such sets of φs occur on average in half of the runs. These are valid runs of the protocol. In such cases any subset of $n-1$ players is able to infer the choice of phase φ_D of the dealer, if and only if, they concur and reveal among themselves their values of φ_j. In case that this subset contains the last partner, he/she must reveal the measurement result[11]. The task of secret sharing in the particular setting

[11]Note that although doing different things in practice (measurement/phaseshift) all parties are equal as far as the amount of information is concerned. In fact the state preparation and detection could be formally separated from the parties and be performed by some higher instance etc. Yet we do not think this is in any way of practical importance.

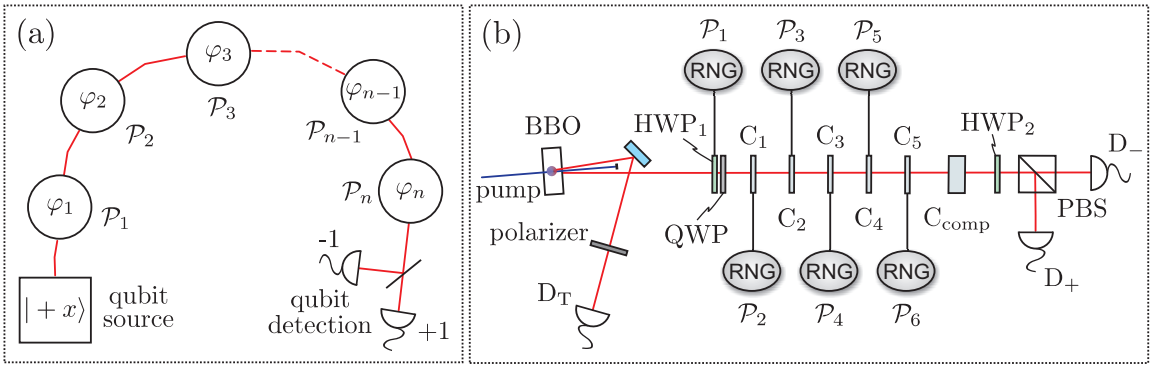

Figure 4.4: (a) Scheme for n party single qubit secret sharing. A qubit is prepared in an initial state and sequentially communicated from one player to the next, each applying a randomly chosen phase φ_j from a preselected set. The last player performs a measurement on the qubit leading to the result ± 1. In half of the cases the phases add up such that the measurement result is deterministically depending on the sum of phases. These instances can be used to achieve the aim of secret sharing. (b) Experimental set-up. Pairs of orthogonally polarized photons are generated via type II SPDC. The detection of one photon by D_T heralds the existence of the other one used in the protocol. The initial polarization state is prepared using a polarizer in the trigger arm. Each of the players $(\mathcal{P}_1, \ldots, \mathcal{P}_6)$ introduces one out of four phase shifts, according to the output of a pseudo random number generator (RNG), using a half- and quarter-wave plate (HWP_1, QWP) or YVO_4 crystals (C_1,...,C_5), respectively. The last party analyzes additionally the final polarization state of the photon by detecting it behind a half-wave plate (HWP_2) and a polarizing beam splitter (PBS).

with the threshold of $k = n - 1$, is now achieved via local manipulation of phases on a communicated single qubit, and no multi-particle entangled GHZ state is required anymore.

Security of the protocol. In order to ensure the security of the protocol against eavesdropping or cheating, the dealer $\mathcal{P}_D$ of the secret arbitrarily selects a certain subset (the size depends on the degree of security requirements) of valid runs. For these runs the value of φ_D is compared with the one inferred by the players. To this end each of the players sends, in a random order, the value of his/her phase φ_j. The comparison reveals any eavesdropping or cheating strategy. That can be easily seen by discussing the following intercept/resend eavesdropping attacks.

Imagine for instance the first player $\mathcal{P}_j$ who follows directly after the dealer $\mathcal{P}_D$ tries to infer the secret on her/his own, i.e. without the required level of concurrence $k = n - 1$, by measuring the qubit, *before* acting on it with $\widehat{U}_j(\varphi_j)$ and afterwards sending it to the next player $\mathcal{P}_{j+1}$. For convenience, let us assume $\mathcal{P}_j$ chooses for this measurement one of the two protocol bases $|\pm x\rangle$ or $|\pm y\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)$. The choice of these bases appears to be natural because at any stage of the protocol the qubit is in one of these four states. As $\mathcal{P}_D$ applies randomly one of four different phase shifts, the probability that the qubit is an eigenstate of the measurement chosen by $\mathcal{P}_j$ is 1/2

and thus in half of the cases the measurement result of $\mathcal{P}_j$ will be completely bitwise random, because $|\langle \pm y \mid \pm x \rangle|^2 = 1/2$. Thus, the cheater $\mathcal{P}_j$ gets no information about the secret. Furthermore, such cheating causes an overall error of 25 % in the final measurement results. Simply, if $\mathcal{P}_j$ chooses the wrong basis, the final state of the qubit after all the introduced phase shifts will not always be of the form (4.18).

An eavesdropper following such a strategy faces a similar situation. The usage of the bases x and y for an intercept/resend attack is the optimal with regard to the information gain on the valid runs. One might also consider using the intermediate (or so-called Breidbart) basis $|\pm b\rangle = \frac{1}{\sqrt{2+\sqrt{2}}}(|\pm x\rangle + |\pm y\rangle) = \frac{1}{\sqrt{2}}(|0\rangle \pm e^{i\pi/4}|1\rangle)$ which gives the eavesdropper maximum information on all exchanged bits [141]. But even here the error rate goes necessarily up to 25 %. The security of the presented protocol against a general eavesdropping attack follows from the proven security of the well known BB84 protocol [14, 63]. Each communication step between two successive parties can be regarded as a BB84 protocol using the bases x and y. Any set of dishonest players in our scheme can be viewed as an eavesdropper in BB84 protocol.

4.2.5 Implementation

The single-qubit protocol for secret sharing was experimentally implemented for $n = 6$ players with a threshold of $k = n - 1 = 5$, thereby clearly demonstrating the practicality of the scheme [110]. The implementation exploits numerous tools already applied in the experimental set-up to solve CCPs. Therefore, the following description is rather cursory; for more details we refer to section 4.1.6.

The experimental set-up for single-qubit secret sharing is shown in Fig. 4.4(b); (photo of the set-up is included in appendix B.2). The protocol qubit is encoded in a polarization state (the computational basis states $|0\rangle$ and $|1\rangle$ correspond to the horizontal $|H\rangle$ and vertical $|V\rangle$ polarization states) of a single photon provided by the heralded single photon source based on a correlated photon pair emission from type II SPDC. Filtering of the vertical polarization of the trigger photon by a polarizer, ensures that the protocol photon has horizontal polarization initially.

The first player $\mathcal{P}_1$ is equipped with a motorized half-wave plate (HWP_1) followed by a quarter-wave plate (QWP) at an angle of 45°. By rotating of HWP_1 to the angles 0°, 45° and 22.5°, −22.5° he transforms the horizontally polarized photons coming from the source to $|\pm y\rangle$ and $|\pm x\rangle$. This corresponds to applying the phase-shifts $\varphi \in \{\pi/2, 3\pi/2\}$ and $\varphi \in \{0, \pi\}$, respectively. As the phase-shifts of the other players $(\mathcal{P}_2, \ldots, \mathcal{P}_6)$ have to be applied independently of the incoming polarization state, the usage of standard wave plates is not possible. Therefore the unitary phase operator is implemented by rotating 200 μm long YVO_4 birefringent crystals (C_i) along their optic axis, oriented perpendicularly to the beam. An additional YVO_4 crystal (C_{comp}) compensates dispersion effects. The last party performs the measurement behind a half-wave plate (HWP_2) at an angle of 22.5° followed by polarizing beam-splitter (PBS).

	z_{total}	z_{raw}	z_{val}	QBER (%)
$\vert \pm x\rangle$	27501	883	452	25.22 ± 2.04
$\vert \pm y\rangle$	24993	784	409	30.32 ± 2.27
$\vert \pm b\rangle$	38174	1137	588	30.27 ± 1.89

Table 4.2: Results of the simulation of an intercept/resend eavesdropping strategy in the protocol bases as well as in the intermediate bases. The attack was done by inserting a polarizer between the first two players. In each case the quantum bit error rate (QBER) rises up to more than 25 % and by this blows the eavesdropper's cover.

The photons are detected at D_+/D_- and D_T by passively quenched silicon APDs with a measured efficiency of about 35 % at our operating wavelength. At the typical single-count rates of ≈ 35000 s^{-1} both in D_+ and D_- and about 5000 s^{-1} in D_T we obtained a coincidence rate of 1200 s^{-1}. Together with a chosen coincidence gate window of 4 ns this implies the communication of single photons only. Accidental coincidences or multi-coincidences were negligible.

4.2.6 Results

The protocol was repeated $z_{\text{total}} = 25000$ times. One run consisted of generating pseudo-random variables, rotating the crystals accordingly and opening the detectors for a collection time window $\tau = 200$ μs, what took all together about 1 s. The requirement of communicating a single photon imposes that only those runs were included into the protocol in which just one coincidence between D_T and either D_+ or D_- was detected during τ. In these runs a single coincidence detection happened $z_{\text{raw}} = 2107$ times which provided us with the raw key. From this we extracted $z_{\text{val}} = 982$ valid runs where $|\cos(\sum_j^n \varphi_j)| = 1$ [506 times $\cos(\sum_j^n \varphi_j) = 1$ and 476 times $\cos(\sum_j^n \varphi_j) = -1$] with a quantum bit error rate (QBER) of 2.34 ± 0.48 %. To calculate the error on the QBER the experiment is considered to be a sequence of Bernoulli trials implying a binomial distribution of error events. The error correction protocols (like, e.g., parity check) could be used exactly like in conventional quantum cryptography to further reduce the errors.

In order to show that the QBER increases significantly by an eavesdropping attack we simulated an intercept/resend strategy by inserting a polarizer between the first two players. The attack was done in the protocol bases $\vert \pm x\rangle, \vert \pm y\rangle$ as well as in the intermediate bases $\vert \pm b\rangle$. For the latter two the polarizer was additionally sandwiched by two quarter-wave plates. The angular settings {1st QWP, polarizer, 2nd QWP} were $\{45°, 0°, -45°\}$ and $\{-45°, 22.5°, 45°\}$. For every choice of the basis the QBER went up to at least 25 % (or even higher due to other experimental imperfections). The results are summarized in Table 4.2.

A different eavesdropping/cheating strategy could be of a Trojan Horse type. One of the players could pass polarized light through the devices of the other play-

ers and therefore attempt to gain information on local phase shifts. However, such action might be easily discovered by the players by checking the nature of light passing through their devices from time to time. Note further that any excess photons, i.e. those not in coincidence with the trigger, cannot be utilized for eavesdropping/cheating as they do not have a defined polarization[12]. Only higher-order emissions, i.e. two pairs emitted within the coherence time (≈ 360 fs), are useful for beam-splitting attacks; this is just the same as in entanglement-based quantum cryptography, see e.g. [142, 143, 144]. The probability for such a opportunity, however, for our parameters is as low as 7.1×10^{-8} per run.

We merely remark that the use of weak coherent pulses of light containing much less than one photon on average, instead of a heralded single photon source, is possible and further reduces the required experimental resources. However, this would be at the expense of the concept of communicating strictly one qubit and can be also disadvantageous for the practical performance of the protocol [145, 146]. While we have realized our secret sharing protocol using photons and polarization encoding, alternative schemes, like proposed or realized in BB84-type protocols can be adopted as well.

4.3 Discussion and outlook

We introduced new schemes for solving the multiparty communication tasks of communication complexity and secret sharing. Unlike other quantum-assisted methods employing multi-particle entangled states, our protocols involve only the sequential communication and transformation of a single qubit. As single-qubit operations using linear optical elements and the analysis of photon polarization states are efficiently realizable with today's technology, we were therefore able to present the first successful experimental demonstrations of the protocols for as many as five and six parties, respectively. This is to our knowledge the highest number of actively performing parties in a quantum protocol ever implemented. In principle, we see no experimental barrier to extend the performed protocols to even significantly higher number of participants.

From theoretical point of view, our work unambiguously demonstrates the power of qubit communication in multiparty tasks. Even though a qubit can be used to communicate only one bit of information between two unentangled parties [114], the full continuous nature of the quantum state still helps when performing some quantum information tasks. The trick is not to require that the information encoded in a qubit is actually read out, but rather substituted for a large amount of classical

[12]The initial polarization of the heralded photons is fixed in the experiment by putting the polarization filter in the path to the trigger detector, see Fig. 4.4(b). Since the photons form polarization entangled EPR pairs, detection of a trigger photon behind a polarization filter collapses the initially undefined polarization state of the heralded one to the required $|+x\rangle$. All other photons, since no trigger event accompanies them, remain unpolarized.

information, which is sequentially processed by every party.

(i) In CCPs with restricted amount of communication this allows to achieve the exponential separation between the quantum/classical performance with increasing number of parties. The performance of the quantum protocol and of its implementation is so high that even without any correction for detector efficiency, loss in the set-up etc., our experimental results significantly outperform the best classical protocols for both studied tasks.

(ii) In QSS this allows to induce among the players the GHZ-like correlations, which are essential for achieving secret sharing task. Still, due to the different architectures of the GHZ-assisted and single-qubit schemes one has to be aware of possibly new security dangers. Since eavesdropper might have an access to input and output ports of the partners, particulary the attacks of Trojan Horse type have to be carefully analyzed in our scheme. Yet, they can be precluded by the players with a reasonable technological effort like, e.g., discussed in [147]. Also, very recently it was shown that by using a quantum memory and a teleportation protocol the cheater/eavesdropper can learn a minor random part of the key (the size depends on her/his position in the communication chain) in our protocol [148]. To close this subtle security loophole various classical methods, like e.g. hash functions, have to be applied or the quantum protocol has to be further refined [149].

Interestingly, our single-qubit communication protocols for CCPs and QSS can be considered as a direct adaptation of the corresponding entanglement-based protocols using GHZ states. While the entanglement-based protocols use a non-local quantum phase, which can be operated on locally by each party, the single-qubit protocols use a quantum phase of a qubit to sequentially encode local information as it flies by the parties towards the last party, who performs a suitable measurement. The expectation value of such a measurement has the same structure as a correlation function of GHZ state (defined as the expectation value of the product of the local measurement results by parties). This explains why the tasks of secret sharing and communication complexity are efficiently solvable with protocols involving only the communication of a single qubit. It appears rather plausible that our single-qubit approach may be a practical solution for many other problems, which were believed to be possible only with the use of multiparty entangled states until now.

In summary, by successfully solving and implementing a cryptographic task as well as a task originating in computer science, we clearly illustrate the potential to introduce multiparty communication problems into real life.

Chapter 5

Conclusions and Outlook

The work presented in this thesis addresses two topics related primarily to the development of technologies and systems for practical quantum communication. The first topic is the efficient generation of photonic entanglement and the second is the simplification and implementation of quantum-assisted solutions to multiparty communication tasks.

Generation of photonic entanglement. In the last decade we witnessed a dramatic progress of photon pair sources in terms of the output flux and the practicality of systems. It appears safe to say that some of the concepts have come to reach an upper bound, forcing one to develop novel methods and techniques for the generation of photonic entanglement. This gradual progress is also clearly perceptible in this thesis, which describes the work on two distinct sources of polarization-entangled photon pairs, spanning the period of over four years.

The first type of source was designed and implemented using the well established concept of degenerate non-collinear emission from a single type-II nonlinear crystal. With a blue laser diode as a pump source of SPDC, this configuration yields maximally hundreds of detected pairs per second and mW of pump power. More importantly, no substantial increase of the brightness is to be expected in the future. This is due to the limitation of the crystal length to a few mm range and due to the fact that only a small fraction of the total SPDC output flux is polarization-entangled. However, the main goal of this design, to demonstrate the feasibility of sources using blue laser diodes as replacement of costly large frame ion lasers, was achieved. Moreover, based on this design, a setup for a lab course on entanglement and the EPR-Bell-problem could be built.

Deficiencies of the first setup are overcome in the second type of source, which features a novel configuration with only a single spatial mode for collecting non-degenerate photon pairs generated via SPDC in a double-crystal geometry. This fully collinear configuration greatly enhances the practicality of the source. Particularly, it allows one to use very long nonlinear crystals, resulting in a highly increased photon-

pair flux. With a pair of 16-mm-long crystals we observed almost two order of magnitudes higher photon-pair flux compared to the non-collinear type II source. The usage of the only spatial mode for coupling of the photons also precludes the occurrence of any intrinsic spatial effect limiting the quantum-interference visibility. Applying a tailored dispersion compensation, we were thereby able to reach nearly 99 % quantum-interference visibility, even though a free-running laser diode as a pump of SPDC was used and no filtering of generated photons was applied. These merits, together with almost free-of-alignment operation, suggest that this type of source is an especially promising candidate for many future practical applications, including quantum cryptography, detector calibration or use in undergraduate lab courses. Apart from the practical applicability, the source might find its relevance also in fundamental tests of quantum mechanics. Particularly, a measured net coupling efficiency of photons pairs of about 90 % offers a unique chance to accomplish a photonic Bell test excluding a fair sampling hypothesis for the first time.

There is a multitude of future research directions following on from the work on photon pair sources presented in this thesis. As the technology for manufacturing quasi-phase-matched materials have progressed, periodically poled crystals like PPKTP have become commonly available, offering a greater freedom in the choice of wavelengths and an access to the highest nonlinear coefficients. Their integration into the collinear type I source should bring a higher output brightness, reduction of photon bandwidth, and possibly, complete suppression of the spatial walk-off effect, which has to be compensated in the current realization using additional birefringent crystals. Another issue deserving more attention is the usage of ultrashort (fs to ps range) pulse pumped SPDC. The precise timing information inherent to such type of pumping showed to be very useful for the realization of certain experiments in quantum optics including generation of multi-photon entangled states, quantum teleportation or other advanced communication protocols. Although the theoretical model developed in the thesis suggests that the concept of collinear type I source works equally efficient for ultrashort pulse pumping, the experimental verification has to be accomplished.

Turning to applications, it is the next goal for the source of non-degenerate entangled photon pairs to be used for a real world experiment such as a demonstration of long-distance quantum cryptography; see also [150]. The preliminary steps in this direction have been already taken by testing the source outside an ideal lab environment, showing no impairment of the output performance and an overall long-term stability of the system. Concerning the applicability of the source for future applications a great deal of effort has to be also made to miniaturize the system, to further minimize the necessary adjustment, and to use a design with superior (thermo-)mechanical stability such as, for example, using fixed components.

Multiparty communication tasks. The use of quantum resources leads to a speed-up in solving many communication tasks or even achieving goals which are classically

not possible at all. While the recent rapid progress in the development of bright entangled photon-pair sources has been followed with ample experimental reports on two-party quantum communication tasks, the practical implementations of tasks for more than two parties have been quite rare, so far. This is primarily due to the requirement of multiparty entangled states, which are very difficult to be produced with current methods and, moreover, suffer from high noise and (depending on the number of partners) exponentially decreasing output yield. We show that entanglement is not the only non-classical resource endowing the quantum multiparty information processing its power. Instead, only the sequential communication and transformation of a single qubit can be sufficient to accomplish certain tasks in a highly efficient way. This we prove for two distinct communication tasks, communication complexity and secret sharing.

Quantum communication complexity addresses the problem of communication reduction for distributed computation tasks by the utilization of quantum effects. In the thesis we study two CCPs, in which N separated partners with local random data must determine in common the correct value of a globally defined Boolean function with the highest possible probability of success. In these tasks the parties can communicate only $N-1$ bits (classical scenario) or $N-1$ qubits (quantum scenario). We theoretically show that for such tasks with restricted communication the advantage of single-qubit assisted protocols over the corresponding classical ones may increase even exponentially with the number of partners. Furthermore, we successfully implement the quantum protocols for $N = 5$ partners using a heralded single photon from parametric down-conversion as the carrier of the qubit communicated from one partner to the other. For a fair comparison with the classical scenario, no correction for imperfections of the state-of-the-art set-up was done whatsoever. The performance of the protocol and of its implementation is so high that even without any correction for detector efficiency, loss in the set-up etc., we significantly outperform the best classical protocols for both studied tasks.

Secret sharing is a cryptographic task with the aim of distributing a secret in such a way that its reconstruction requires the collaboration of the participating partners. Classically the problem is solved by splitting the information using some mathematical algorithms and distributing the resulting pieces to the legitimate parties. However, classical communication is not secure and thus integration of quantum cryptography to secret sharing was proposed. In this protocol a shared GHZ-state allows the information splitting and the eavesdropper protection simultaneously. We propose a protocol for N partners, in which only single-qubit communication is used with no need for GHZ-states. As our protocol requires only single qubits it is realizable with the current state-of-the-art technologies and, above all, scalable with respect to the number of participating partners. These merits enabled us to accomplish the first experimental proof-of-principle demonstration of secret sharing for as many as six partners. This is to our knowledge the highest number of actively performing parties in a quantum protocol ever implemented.

By successfully solving and implementing a cryptographic task as well as a task

originating in computer science, we clearly illustrate the potential to introduce multiparty communication problems into real life. Yet, a great deal of effort need to be spent for this to succeed. It was our aim to provide proof-of-principle realizations of single-qubit protocols. Further work should be focused on the demonstration of more elaborate implementations and on the design of optimum system architectures. Also, many theoretical issues remain open. As concerns quantum communication complexity, the following questions of considerable significance should be answered: Do all entanglement-based protocols with higher-than-classical performance have single-qubit counterparts? Can one use the single-qubit approach to solve a broader class of CCPs? Does the higher-dimensional encoding (qudits) bring an increased performance of quantum protocols? Turning to secret sharing, first and foremost, the security of the single-qubit protocol has to be inspected in more detail. The next issue to be investigated is the usage of other types of qubit encoding (in particular time-bin encoding, which is suitable for fiber-based systems). Finally, on a more general note, it appears rather plausible that our single-qubit approach may be a practical solution for many other problems, which were believed to be possible only with the use of multiparty entangled states until now. The quest for such problems should certainly not be left out from the future research.

Appendix A

Sources of polarization-entangled photon pairs

A.1 Crystals

A.1.1 Beta-barium borate

Beta-barium borate (β-BaB_2O_4 or BBO) is a common non-linear optical material. Its useful characteristics include transparency over a large bandwidth from ultraviolet through infrared wavelengths, wide phase-matching capabilities, high nonlinear coefficient and damage threshold, and low hygroscopic susceptibility. Table A.1 lists basic optical properties of BBO crystal.

Crystal type	Negative uniaxial ($n_o > n_e$)	
Crystal structure	Trigonal, point group 3m	
Transparency range	0.198–2.6 μm	
Nonlinear coefficients	$d_{22} = \pm(2.22 \pm 0.09)$ pm/V $d_{31} = \pm(0.16 \pm 0.08)$ pm/V	
Effective nonlinearity	$d_{\text{eff}} = d_{31} \sin\theta - d_{22} \cos\theta \sin 3\phi$ (type I) $d_{\text{eff}} = d_{22} \cos^2\theta \cos 3\phi$ (type II)	
Sellmeier coefficients	$A_o = 2.7359$	$A_e = 2.7353$
	$B_o = 0.01878\ \mu\text{m}^2$	$B_e = 0.01224\ \mu\text{m}^2$
	$C_o = -0.01822\ \mu\text{m}^{-2}$	$C_e = -0.01667\ \mu\text{m}^{-2}$
	$E_o = -0.01354\ \mu\text{m}^{-2}$	$E_e = -0.01516\ \mu\text{m}^{-2}$

Table A.1: Basic nonlinear optical properties of BBO crystal according to [30] and references therein.

A.1.2 Yttrium vanadate

Undoped yttrium orthovanadate (YVO_4) is widely used in optical polarization components due to its very high birefringence of $\Delta n > 0.2$ within its entire transparency range and due to its superior physical and mechanical characteristics. Basic optical properties of YVO_4 crystal are given in Table A.2.

Crystal type	Positive uniaxial ($n_o < n_e$)	
Crystal structure	Tetragonal, point group $I4_1/\mathrm{amd}$	
Transparency range	0.4–5.0 μm	
Sellmeier coefficients	$A_o = 3.77834$	$A_e = 4.59905$
	$B_o = 0.06974\ \mu\mathrm{m}^2$	$B_e = 0.11053\ \mu\mathrm{m}^2$
	$C_o = -0.04724\ \mu\mathrm{m}^{-2}$	$C_e = -0.04813\ \mu\mathrm{m}^{-2}$
	$E_o = -0.01081\ \mu\mathrm{m}^{-2}$	$E_e = -0.01227\ \mu\mathrm{m}^{-2}$

Table A.2: Basic structural and optical properties of YVO_4 crystal according to [151].

A.2 Historical progress of sources

The parameters of the sources reported over the recent 15 years have been collected into the Table A.3 and used to quantify the historical growth of the achieved photon pair fluxes. To make a fair comparison, only sources emitting photon pairs in the visible and the near-infrared spectral region compatible with today's high-efficiency silicon APDs, and exhibiting at least 90 % quantum-interference visibility, have been selected.

The following data are listed in the columns: (*i*) reference and year of publication; (*ii*) method used for the generation of entangled photon pairs and wavelengths of the pump, signal and idler; (*iii*) type of nonlinear crystal and pump laser; (*iv*) type of detectors and their efficiencies; (*v*) quantum-interference visibility $\mathcal{V}$ of polarization correlations; (*vi*) brightness B (detected pairs/sec/mW) and spectral brightness $B^{(s)}$ (detected pairs/sec/mW/nm); (*vii*) detected coincidence/single ratio μ.

Ref. (year)	method/ wavelengths	laser/ medium	detectors (efficiency)	$\mathcal{V}$	B/ $B^{(s)}$	μ
[103] (1993)	SPDC (type II)/ $351 \rightarrow 702 + 702$	Ar^+/ BBO	Si APD (30-60%?)	$\sim 99\%$	0.2 ?/ 0.2 ?	?
[56] (1995)	SPDC (type II)/ $351 \rightarrow 702 + 702$	Ar^+/ BBO	Si APD (30-60%?)	97.8%	10/ 2	?
[57] (1999)	SPDC (type I)/ $351 \rightarrow 702 + 702$	Ar^+/ BBO	Si APD (65%)	$\sim 95\%$	140/ 28	0.05

continues on the next page...

. . . continued from the previous page

Ref. (year)	method/ wavelengths	laser/ medium	detectors (efficiency)	visibility	$B/$ $B^{(s)}$	μ
[72] (2000)	SPDC (type II)/ $351 \rightarrow 702 + 702$	Ar^+/ BBO	Si APD (30-60%?)	92.2%	105/ ?	?
[93] (2001)	SPDC (type II)/ $351 \rightarrow 702 + 702$	Ar^+/ BBO	Si APD (30-60%?)	96.3%	900/ 210	0.28
[94] (2003)	SPDC (type II)/ $415 \rightarrow 830 + 830$	Ti:Sapp/ BBO	Si APD (50%)	97.2%	~ 200/ ~ 20	0.3
[90] (2004)	SPDC (type II)/ $402 \rightarrow 805 + 805$	LD/ BBO	Si APD (36%)	94.3%	220/ 37	0.19
[152] (2004)	SPDC (type II)/ $407 \rightarrow 815 + 815$	Kr^+/ BBO	Si APD (45-60%?)	96.0%	775/ 16	0.26
[76] (2004)	QPM (type II)/ $398 \rightarrow 797 + 797$	Ti:Sapp PPKTP	Si APD (45-60%?)	90.0%	12000/ 4000	0.18
[73] (2005)	SPDC (type I)/ $351 \rightarrow 702 + 702$	Ar^+/ BBO	Si APD (65%)	$\sim 95\%$?	3640/ 146	> 0.3
[153] (2005)	QPM (type II)/ $398 \rightarrow 797 + 797$	Ti:Sapp PPKTP	Si APD (45-60%?)	96.0%	820/ 820	?
[75] (2006)	QPM (type II)/ $405 \rightarrow 810 + 810$	ECLD/ PPKTP	Si APD (45-60%?)	96.6%	18600/ 18600	?
[a] (2007)	SPDC (type I)/ $402 \rightarrow 805 + 805$	LD/ BBO	Si APD (51%)	98.5%	27000/ 1800	0.38
[105] (2007)	QPM (type II)/ $405 \rightarrow 810 + 810$	LD/ PPKTP	Si APD (45-60%?)	97.3%	28000/ ?	0.15
[105] (2007)	QPM (type II)/ $405 \rightarrow 810 + 810$	ECLD/ PPKTP	Si APD (45-60%?)	99.5%	50000/ 80500	0.28

[a] This work (section 3.4).

Table A.3: Comparison of sources of polarization entangled photons pairs. Exponential growth of the brightness with time can be deduced from the parameters. Moreover, in a few last years the gradual exchange of ion lasers (Ar^+ and Kr^+) for blue laser diodes, and the exchange of conventional crystals (typically BBO) for quasi-phase matched (QPM) periodically poled crystals (typically KTP), can be observed.

A.3 Photos

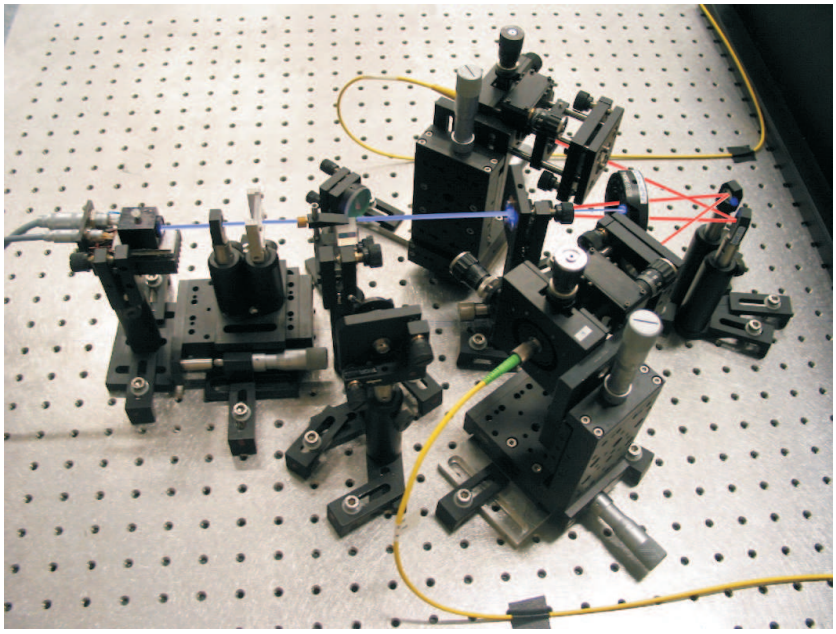

Figure A.1: Photo of the compact non-collinear type-II SPDC source of polarization-entangled photon pairs pumped with a blue laser diode.

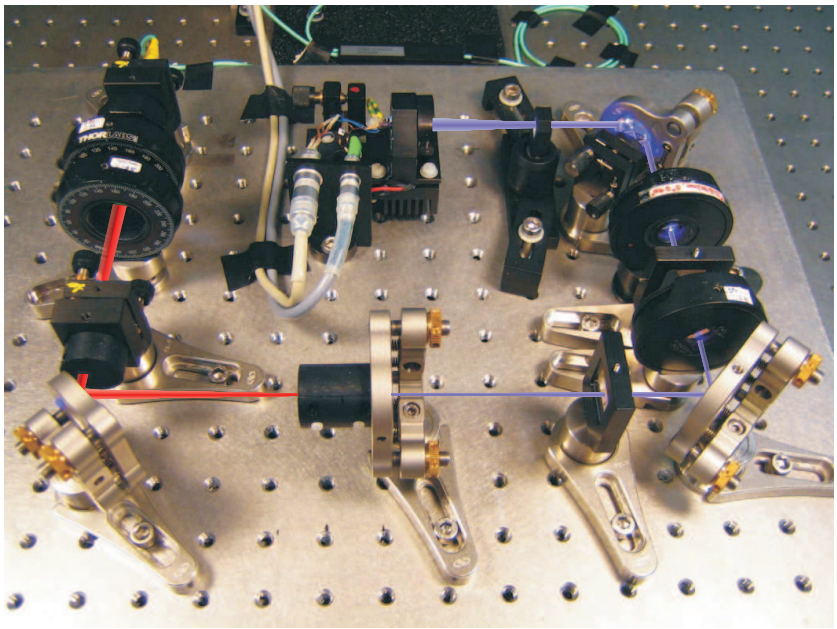

Figure A.2: Photo of the compact collinear type-I SPDC source of polarization-entangled photon pairs pumped with a blue laser diode.

Appendix B

Single-qubit multiparty quantum communication

B.1 Classical bounds of success probability in communication complexity problems

In the following we calculate the classical fidelity bounds $\mathcal{B}(N)$ for the problems A and B defined in section 4.1.3.

The bound $\mathcal{B}(N)$ is found as the maximum of the fidelity F_c expressed in (4.9). With the use of formulas (4.1) and (4.2) we obtain for the specific problem A the following form of $F_{c,A}$:

$$\begin{aligned} F_{c,A} &= \frac{1}{2^{N-1}} \sum_{x_1,\ldots,x_N} \cos\left(\frac{\pi}{2}\sum_{k=1}^{N} x_k\right) \prod_{k=1}^{N} c_k(x_k) \\ &= \frac{1}{2^{N-1}} \mathrm{Re}\left[\prod_{k=1}^{N}\sum_{x_k} \exp\left(i x_k \frac{\pi}{2}\right) c_k(x_k)\right]. \end{aligned} \tag{B.1.1}$$

Each of the numbers $x_1, \ldots, x_N$ takes only the values 0 and 1, so the sum in (B.1.1) reduces to

$$\sum_{x_k} \exp\left(i x_k \frac{\pi}{2}\right) c_k(x_k) = c_k(0) + i c_k(1). \tag{B.1.2}$$

Since c_k are dichotomic functions of spectrum ± 1, the possible values of (B.1.2) are

$$\pm 1 \pm i = \sqrt{2}\exp\left(i\frac{\pi}{4} + in\frac{\pi}{2}\right), \tag{B.1.3}$$

where n is an integer. Considering an even number N of parties, i.e. $N = 2K$, K being an integer ≥ 1, the expression in (B.1.1) is maximized by using pairs of

conjugate values (B.1.3). Thus the maximum is given by

$$\mathcal{B}(N=2K)=\max(F_{c,A})=\frac{1}{2^{2K-1}}\mathrm{Re}\left[\prod_{i=1}^{K}\sqrt{2}\exp\left(i\frac{\pi}{4}+in\frac{\pi}{2}\right)\sqrt{2}\exp\left(-i\frac{\pi}{4}-in\frac{\pi}{2}\right)\right] \tag{B.1.4}$$

and one can easily show that the bound for even number of parties is

$$\mathcal{B}(N=2K)=2^{-K+1}. \tag{B.1.5}$$

Analogously, for odd number of parties, i.e. $N=2K-1$, we can find the bound

$$\mathcal{B}(N=2K-1)=2^{-K+1}. \tag{B.1.6}$$

For the problem B, the fidelity $F_{c,B}$ is given by

$$F_{c,B}=\frac{1}{2\pi^{N-1}}\int_0^{\pi}\mathrm{d}x_1\ldots\int_0^{\pi}\mathrm{d}x_N\,\cos\left(\sum_{k=1}^{N}x_k\right)S\left[\cos\left(\sum_{k=1}^{N}x_k\right)\right]\prod_{k=1}^{N}c_k(x_k). \tag{B.1.7}$$

Since $|y|\cdot S[y]=y$ and $|c_k(x_k)|=1$, one can derive the following inequality [154]:

$$\int_0^{\pi}\mathrm{d}x_1\ldots\int_0^{\pi}\mathrm{d}x_N\,\cos\left(\sum_{k=1}^{N}x_k\right)\prod_{k=1}^{N}c_k(x_k)\leq 2^N \tag{B.1.8}$$

Therefore, the classical bound $\mathcal{B}(N)$ for the task B involving any number of parties N is given by

$$\mathcal{B}(N)=\max(F_{c,B})=\frac{1}{2\pi^{N-1}}2^N=\left(\frac{2}{\pi}\right)^{N-1}. \tag{B.1.9}$$

B.2 Photo

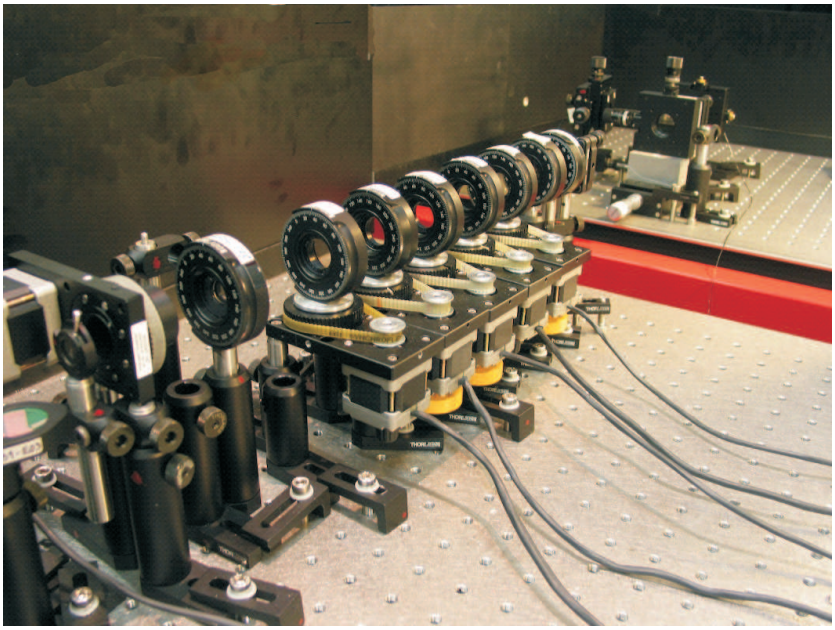

Figure B.1: Photo of the demonstration of single-qubit quantum secret sharing for 6 players. Each of them uses a rotatable birefringent crystal to introduce a relative phase shift to the qubit encoded in polarization state of a single photon, which is provided by a heralded single photon source.

Appendix C

Author's publications related to the presented work

Articles

- P. Trojek, C. Schmid, M. Bourennane, C. Kurtsiefer, and H. Weinfurter. Compact source of polarization-entangled photon pairs. *Opt. Express* **12**, 276–281 (2004).
- P. Trojek, C. Schmid, M. Bourennane, Časlav Brukner, M. Żukowski, and H.Weinfurter. Experimental quantum communication complexity. *Phys. Rev. A* **72**, 050305(R) (2005).
- C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Żukowski, and H. Weinfurter. Experimental single qubit quantum secret sharing. *Phys. Rev. Lett.* **95**, 230505 (2005).
- C. Schmid, P. Trojek, S. Gaertner, M. Bourennane, C. Kurtsiefer, M. Żukowski, and H. Weinfurter. Experimental quantum secret sharing. *Fortschr. Phys.* **54**, 831–839 (2006).
- C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, Marek Żukowski, and H. Weinfurter. Schmid *et al.* reply. *Phys. Rev. Lett.* **98**, 028902 (2007).
- R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger: Entanglement-based quantum communication over 144 km. *Nature Physics* **3**, 481–486 (2007).
- P. Trojek and H. Weinfurter. Collinear source of polarization-entangled photon pairs at nondegenerate wavelengths. *Appl. Phys. Lett.* **92**, 211103 (2008).

Proceedings and book contributions

- C. Schmid, P. Trojek, S. Gaertner, M. Bourennane, C. Kurtsiefer, M. Żukowski, and H. Weinfurter. Experimental quantum secret sharing. In: *Elements of Quantum Information*, 303–314 (Wiley-VCH, Weinheim, 2007).
- M. Bourennane, C. Schmid, P. Trojek, C. Kurtsiefer, Č. Brukner, M. Żukowski, and H. Weinfurter. Experimental single qubit quantum multiparty communication. In: *Quantum Communication and Security*, 22–30 (IOS Press, Amsterdam, 2007).

Patents

- Inventors: M. Bourennane, C. Kurtsifer, C. Schmid, P. Trojek, H. Weinfurter, and M. Żukowski. Single-particle quantum-enhanced secret sharing. Publication No. **WO/2006/074153** (2006).
- Inventors: P. Trojek and H. Weinfurter. Gerät oder Methode zur Erzeugung von quantenkorrelierten und/oder polarisationsverschränkten Photonenpaaren. Application No. **PCT/IB2008/050815** (2008).

Bibliography

[1] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.* **47**, 777–780 (1935).

[2] J. S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics* **1**, 195–200 (1964).

[3] D. Bohm. *Quantum Theory.* Prentice-Hall, Englewood Cliffs, New York, 1951.

[4] N. D. Mermin. Is the moon there when nobody looks? Reality and the quantum theory. *Phys. Today* **38**, 38–47 (1985).

[5] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger. Bell's theorem without inequalities. *Am. J. Phys.* **58**, 1131–1143 (1990).

[6] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.* **23**, 880–884 (1969).

[7] B. S. Cirel'son. Quantum generalizations of Bell's inequality. *Lett. Math. Phys.* **4**, 93–100 (1980).

[8] S. J. Freedman and J. F. Clauser. Experimental test of local hidden-variable theories. *Phys. Rev. Lett.* **28**, 938–941 (1972).

[9] J. F. Clauser and A. Shimony. Bell's theorem: experimental tests and implications. *Rep. Prog. Phys.* **41**, 1881–1927 (1978).

[10] A. Aspect, J. Dalibard, and G. Roger. Experimental test of Bell's inequalities using time-varying analyzers. *Phys. Rev. Lett.* **49**, 1804–1807 (1982).

[11] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger. Violation of Bell's inequality under strict Einstein locality conditions. *Phys. Rev. Lett.* **81**, 5039–5043 (1998).

[12] S. Takeuchi, J. Kim, Y. Yamamoto, and H. H. Hogue. Development of a high-quantum-efficiency single-photon counting system. *Appl. Phys. Lett.* **74**, 1063–1065 (1999).

[13] M. A. Rowe, D. Kielpinsky, V. Meyer, C. A. Sacket, W. M. Itano, C. Monroe, and D. J. Wineland. Experimental violation of a Bell's inequality with efficient detection. *Nature* **409**, 791–794, (2001).

[14] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In: *Proceedings of IEEE International Conference on Computers Systems and Signal Processing*, 175–179 (Bangalore, India, 1984).

[15] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661–663 (1991).

[16] C. H. Bennett and S. J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Phys. Rev. Lett.* **69**, 2881–2884 (1992).

[17] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* **70**, 1895–1899 (1993).

[18] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Sci. Statist. Comput.* **26**, 1484–1509 (1997). [Preliminary version appeared in: *Proceedings of 35th Annual Symposium on Foundations of Computer Science*, 124–134 (IEEE Press, Los Alamitos, 1994).]

[19] L. K. Grover. Quantum mechanics helos in searching for a needle in a haysteck. *Phys. Rev. Lett.* **79**, 325–328 (1997).

[20] C. H. Bennett and G. Brassard. The dawn of a new era for quantum cryptography: The experimental prototype is working! *Sigact News* **20**, 78–82 (1989).

[21] D. N. Klyshko. Coherent decay of photons in a nonlinear medium. *Pis'ma Zh. Eksp. Teor. Fiz.* **6**, 490–492 (1967) [Translation: *Sov. Phys. JETP Lett.* **6**, 23–25 (1967)].

[22] D. C. Burnham and D. L. Weinberg. Observation of simultaneity in parametric production of optical photon pairs. *Phys. Rev. Lett.* **25**, 84–87 (1970).

[23] D. N. Klyshko and B. Y. Zel'dovich. Statistics of field in parametric luminescence. *Pis'ma Zh. Eksp. Teor. Fiz.* **9**, 69–74 (1969) [Translation: *Sov. Phys. JETP Lett.* **9**, 40–44 (1969)].

[24] B. R. Mollow. Photon correlation in the parametric frequency splitting of light. *Phys. Rev. A* **8**, 2684–2694 (1973).

[25] C. K. Hong, Z. Y. Ou, and L. Mandel. Measurement of subpicosecond time intervals between two photons by interference. *Phys. Rev. Lett.* **59**, 2044–2046 (1987).

[26] D. N. Klyshko. On the use of two-photon light for absolute calibration of photodetectors. *Kvantovaya Electron.* **7**, 1932–1940 (1980) [Translation: *Sov. J. Quantum Electronics* **10**, 1112–1116 (1980)].

[27] R. W. Boyd. *Nonlinear optics*. Academic Press, San Diego (2002).

[28] D. N. Klyshko. *Photons and Nonlinear Optics*. Nauka, Moscow (1980) [Translation: Gordon & Breach, New York (1988)].

[29] B. E. A. Saleh and M. C. Teich. *Fundamentals of photonics*. John Wiley & Sons, Inc., New York (1991).

[30] V. G. Dmitriev, G. G. Gurzadyan, and D. N. Nicogosyan. *Handbook of nonlinear optical crystals*. Springer Verlag, Berlin (1999).

[31] L. Mandel and E. Wolf. *Optical Coherence and Quantum Optics*. Cambridge Univ. Press, Cambridge (1995).

[32] M. O. Scully and M. S. Zubairy. *Quantum optics*. Cambridge Univ. Press, Cambridge, (1997).

[33] W. H. Louisell, A. Yariv, and A. E. Siegman. *Coupled mode and parametric electronics*. John Wiley & Sons, Inc., New York (1960).

[34] W. H. Louisell, A. Yariv, and A. E. Siegman. Quantum fluctuations and noise in parametric processes. I. *Phys. Rev.* **124**, 1646–1654 (1961).

[35] S. Friberg, C. K. Hong, and L. Mandel. Intensity dependence of the normalized intensity correlation function in parametric down-conversion. *Opt. Commun.* **54**, 311–316 (1985).

[36] X. Y. Zou, L. J. Wang, and L. Mandel. Violation of classical probability in parametric down-conversion. *Opt. Commun.* **84**, 351–354 (1991).

[37] C. K. Hong and L. Mandel. Theory of parametric frequancy down conversion of light. *Phys. Rev. A* **31**, 2409–2418 (1985).

[38] J.-C. Diels and W. Rudolph. *Ultrashort laser pulse phenomena*. Academic Press, Inc., San Diego (1996).

[39] J. Peřina Jr. Properties of pulsed entangled two-photon fields. *Eur. Phys. J. D* **7**, 235–242 (1999).

[40] A. V. Belinsky and D. N. Klyshko. Two-photon wave packets. *Laser Phys.* **4**, 663–689 (1994).

[41] W. P. Grice and I. A. Walmsley. Spectral distinguishability in type-II down-conversion with a broadband pump. *Phys. Rev. A* **56**, 1627–1634 (1997).

[42] S. Carrasco, A. V. Sergienko, B. E. A. Saleh, M. C. Teich, J. P. Torres, and L. Torner. Spectral engineering of entangled two-photon states. *Phys. Rev. A* **73**, 063802 (2006).

[43] R. J. Glauber. The quantum theory of optical coherence. *Phys. Rev.* **130**, 2529–2539 (1963).

[44] Y. Shih. Entangled biphoton source – property and preparation. *Rep. Prog. Phys.* **66**, 1009–1044 (2003).

[45] C. Kurtsiefer, M. Oberparleiter, and H. Weinfurter. Generation of correlated photon pairs in type-II parametric down conversion – revisited. *J. Mod. Opt.* **48**, 1997–2007 (2001).

[46] T. B. Pittman, D. V. Strekalov, D. N. Klyshko, M. H. Rubin, A. V. Sergienko, and Y. H. Shih. Two-photon geometric optics. *Phys. Rev. A* **53**, 2804–2815 (1996).

[47] M. H. Rubin. Transverse correlation in optical spontaneous parametric down-conversion. *Phys. Rev. A* **54**, 5349–5560 (1996).

[48] R. S. Bennink, Y. Liu, D. D. Earl, and W. P. Grice. Spatial distinguishability of photons produced by spontaneous parametric down-conversion with a focused pump. *Phys. Rev. A* **74**, 023802 (2006).

[49] P. H. S. Ribeiro, C. H. Monken, and G. A. Barbosa. Measurement of coherence area in parametric downconversion luminescence. *Appl. Opt.* **33**, 352–355 (1993).

[50] A. Joobeur, B. E. A. Saleh, T. S. Larchuk, and M. C. Teich. Coherence properties of entangled beams generated by parametric down-conversion: Theory and experiment. *Phys. Rev. A* **53**, 4360–4371 (1996).

[51] Editors: D. Bouwmeester, A. Ekert, and A. Zeilinger. *The physics of quantum information. Quantum cryptography, quantum teleportation, quantum computation.* Springer Verlag, Berlin (2000).

[52] J. G. Rarity and P. R. Tapster. Experimental violation of Bell's inequality based on phase and momentum. *Phys. Rev. Lett.* **64**, 2495–2498 (1990).

[53] J. D. Franson. Bell inequality for position and time. *Phys. Rev. Lett.* **62**, 2205–2208 (1989).

[54] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden. Pulsed energy-time entangled twin-photon source for quantum communication. *Phys. Rev. Lett.* **82**, 2594–2597 (1999).

[55] Y. H. Shih and C. O. Alley. New type of Einstein-Podolsky-Rosen-Bohm experiment using pairs of light quanta produced by optical parametric down conversion. *Phys. Rev. Lett.* **61**, 2921–2924 (1988).

[56] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih. New high-intensity source of polarization-entangled photon pairs. *Phys. Rev. Lett.* **75**, 4337–4341 (1995).

[57] P. G. Kwiat, E. Waks, A. G. White, I. Appelbaum, and P. H. Eberhard. Ultrabright source of polarization-entangled photons. *Phys. Rev. A* **60**, R773–R776 (1999).

[58] Y. H. Kim, S. P. Kulik, and Y. Shih. High-intensity pulsed source of space-time and polarization double-entangled photon pairs. *Phys. Rev. A* **62**, 011802(R) (2000).

[59] Y. Nambu, K. Usami, Y. Tsuda, K. Matsumoto, and K. Nakamura. Generation of polarization-entangled photon pairs in a cascade of two type-I crystals pumped by femtosecond pulses. *Phys. Rev. A* **66**, 033816 (2002).

[60] C. H. Bennett, C. A. Fuchs, and J. A. Smolin. Entanglement-enhanced classical communication on a noisy quantum channel. In: *Quantum Communication, Computing and Measurement*, 79–88 (Plenum, New York, 1997).

[61] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller. Quantum repeaters: The role of imperfect local Operations in quantum communication. *Phys. Rev. Lett.* **81**, 5932–5935 (1998).

[62] B. C. Jacobs, T. B. Pittman, and J. D. Franson. Quantum relays and noise suppression using linear optics. *Phys. Rev. A* **66**, 052307 (2002).

[63] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145–195 (2002).

[64] M. Dušek, N. Lütkenhaus, and M. Hendrych. Quantum Cryptography. In: *Progress in Optics* **49**, 381–454 (Elsevier, 2006).

[65] A. V. Serginko. (Ed.) *Quantum communications and cryptography.* CRC Press, Taylor & Francis Group, New York (2005).

[66] S. Tanzilli, W. Tittel, H. De Riedmatten, H. Zbinden, P. Baldi, D. B. Ostrowsky, and N. Gisin. PPLN waveguide for quantum communication. *Eur. Phys. J. D* **18**, 155–160 (2002).

[67] M. Pfennigbauer, M. Aspelmeyer, W. R. Leeb, G. Baister, T. Dreischer, T. Jennewein, G. Neckamm, J. M. Perdigues, H. Weinfurter, and A. Zeilinger. Satellite-based quantum communication terminal employing state-of-the-art technology. *J. Opt. Netw.* **4**, 549560 (2005).

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

[69] A. Valencia, G. Scarcelli, and Y. Shih. Distant clock synchronization using entangled photon pairs. *Appl. Phys. Lett.* **85**, 2655–2657 (2004).

[70] A. Migdall. Correlated-photon metrology without absolute standards. *Physics Today* **January**, 41–46 (1999).

[71] M. D'Angelo, M. V. Chekhova, and Y. Shih. Two-photon diffraction and quantum lithography. *Phys. Rev. Lett.* **87**, 013602 (2001).

[72] M. Oberparleiter and H. Weinfurter. Cavity-enhanced generation of polarization-entangled photon pairs. *Opt. Comm.* **183**, 133–137 (2000).

[73] J. B. Altepeter, E. R. Jeffrey, and P. G. Kwiat. Phase-compensated ultra-bright source of entangled photons. *Opt. Express* **13**, 8951–8959 (2005).

[74] F. König, E. J. Mason, F. N. C. Wong, and M. A. Albota. Efficient and spectrally bright source of polarization-entangled photons. *Phys. Rev. A* **71**, 033805 (2005).

[75] F. N. C. Wong, J. H. Shapiro, and T. Kim. Efficient generation of polarization-entangled photons in a nonlinear crystal. *Laser Phys.* **16**, 1517–1524 (2006).

[76] M. Fiorentino, G. Messin, C. E. Kuklewicz, F. N. C. Wong, and J. H. Shapiro. Generation of ultrabright tunable polarization entanglement without spatial, spectral, or temporal constraints. *Phys. Rev. A* **69**, 041801(R) (2004).

[77] D. Ljunggren, M. Tengner, P. Marsden, and M. Pelton. Theory and experiment of entanglement in a quasi-phase-matched two-crystal source. *Phys. Rev. A* **73**, 032326 (2006).

[78] S. Sauge, M. Swillo, S. Albert-Seifried, G. B. Xavier, J. Waldebäck, M. Tengner, D. Ljunggren, and A. Karlsson. Narrowband polarization-entangled photon pairs distributed over a WDM link for qubit networks. *Optics Express* **15**, 6926–6933 (2007).

[79] S. Tanzilli, H. De Riedmatten, W. Tittel, H. Zbinden, P. Baldi, M. De Micheli, D. B. Ostrowsky, and N. Gisin. Highly efficient photon-pair source using a periodically poled lithium niobate waveguide. *Electron. Lett.* **37**, 26–28 (2001).

[80] A. B. U'Ren, C. Silberhorn, K. Banaszek, and I. A. Walmsley. Efficient conditional preparation of high-fidelity single photon states for fiber-optic quantum networks. *Phys. Rev. Lett.* **93**, 093601 (2004).

[81] L. J. Wang, C. K. Hong, and S. R. Friberg. Generation of correlated photons via four-wave mixing in optical fibers. *J. Opt. B: Quantum Semiclass. Opt.* **3**, 346–352 (2001).

[82] X. Li, P. L. Voss, J. E. Sharping, and P. Kumar. Optical-fiber source of polarization-entangled photons in the 1550 nm telecom band. *Phys. Rev. Lett.* **94**, 053601 (2005).

[83] J. Fulconis, O. Alibart, W. Wadsworth, P. Russell, and J. Rarity. High brightness single mode source of correlated photon pairs using a photonic crystal fiber. *Opt. Express* **13**, 7572–7582 (2005).

[84] C. Liang, K. F. Lee, M. Medic, P. Kumar, R. H. Hadfield, and S. W. Nam. Characterization of fiber-generated entangled photon pairs with superconducting single-photon detectors. *Opt. Express* **15**, 1322–1327 (2007).

[85] J. Fulconis, O. Alibart, W. J. Wadsworth, J. G. Rarity. Quantum interference with photon pairs using two micro-structured fibres. *ArXiv:* quant-ph/0701129 (2007).

[86] O. Benson, C. Santori, M. Pelton, and Y. Yamamoto. Regulated and entangled photons from a single quantum dot. *Phys. Rev. Lett.* **84**, 2513–2516 (2000).

[87] 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).

[88] J. Volz, C. Kurtsiefer, and H. Weinfurter. Compact all-solid-state source of polarization-entangled photon pairs. *Appl. Phys. Lett.* **79**, 869–871 (2001).

[89] D. Dehlinger and M. W. Mitchell. Entangled photon apparatus for the undergraduate laboratory. *Am. J. Phys.* **70**, 898–902 (2002).

[90] P. Trojek, C. Schmid, M. Bourennane, C. Kurtsiefer, and H. Weinfurter. Compact source of polarization-entangled photon pairs. *Opt. Express* **12**, 276–281 (2004).

[91] A. Dragan. Efficient fiber coupling of down-conversion photon pairs. *Phys. Rev. A* **70**, 053814 (2004).

[92] R. Andrews, E. Pike, and S. Sarkar. Optimal coupling of entangled photons into single-mode optical fibers. *Opt. Express* **12**, 3264–3269 (2004).

[93] C. Kurtsiefer, M. Oberparleiter and H. Weinfurter. High-efficiency entangle photon pair collection in type-II parametric fluorescence. *Phys. Rev. A* **64**, 023802 (2001).

[94] F. A. Bovino, P. Varisco, A. M. Colla, G. Castagnoli, G. Di Giuseppe, and A. V. Sergienko. Effective fiber-coupling of entangled photons for quantum communication. *Opt. Comm.* **227**, 343–348 (2003).

[95] D. Ljunggren and M. Tengner. Optimal focusing for maximal collection of entangled narrow-band photon pairs into single-mode fibers. *Phys. Rev. A* **72**, 023802 (2005).

[96] S. Castelletto, I. P. Degiovanni, A. Migdall, and M. Ware. On the measurement of two-photon single-mode coupling efficiency in parametric down-conversion photon sources. *New J. Phys.* **6**, 87, (2004).

[97] E.-G. Neumann. *Single-mode fibers: Fundementals.* Springer-Verlag, Berlin, 1988.

[98] C. H. Monken, P. H. Souto Ribeiro, and S. Pádua. Optimizing the photon pair collection efficiency: A step toward a loophole-free Bell's inequalities experiment. *Phys. Rev. A* **57**, R2267–R2269 (1998).

[99] Nichia corporation. *Spec. Sheet NDHV310APC*, `http://www.nichia.co.jp/product/laser-main.html`.

[100] T. F. Johnston. Beam propagation (M^2) measurement made as easy as it gets: The four-cuts method. *Appl. Opt.* **37**, 4840–4850 (1998).

[101] D. Dehlinger and M. W. Mitchell. Entangled photons, nonlocality, and Bell inequalities in the undergraduate laboratory. *Am. J. Phys.* **70**, 903–910 (2002).

[102] P. Trojek and H. Weinfurter. Collinear source of polarization-entangled photon pairs at nondegenerate wavelengths. *Appl. Phys. Lett.* **92**, 211103 (2008).

[103] T. E. Kiess, Y. H. Shih, A. V. Sergienko, and C. O. Alley. Einstein-Podolsky-Rosen-Bohm experiment using pairs of light quanta produced by type-II parametric down-conversion. *Phys. Rev. Lett.* **71**, 3893–3897 (1993).

[104] Y.-H. Kim, W. P. Grice. Generation of pulsed polarization entangled two-photon state via temporal and spectral engineering. *J. Mod. Opt.* **49**, 2309–2323 (2002).

[105] A. Fedrizzi. Private communication.

[106] A. Arie, G. Rosenman, V. Mahal, A. Skliar, M. Oron, M. Katz, and D. Eger Green and ultraviolet quasi-phase-matched second harmonic generation in bulk periodically-poled $KTiOPO_4$. *Opt. Commun.* **142**, 265–268 (1997).

[107] N. D. Mermin. The EPR experiment – thoughts about the 'loophole'. In: *New techniques and Ideas in Quantum Measurement Theory* **480**, 422–427, (New York Academy of Sciences, New York, 1986).

[108] P. H. Eberhard. Background level and counter efficiencies required for a loophole-free Einstein-Podolsky-Rosen experiment. *Phys. Rev. A* **47**, R747–R750 (1993).

[109] P. Trojek, C. Schmid, M. Bourennane, Časlav Brukner, M. Żukowski, and H.Weinfurter. Experimental quantum communication complexity. *Phys. Rev. A* **72**, 050305(R) (2005).

[110] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Żukowski, and H. Weinfurter. Experimental single qubit quantum secret sharing. *Phys. Rev. Lett.* **95**, 230505 (2005).

[111] A. C.–C. Yao. Some complexity questions related to distributed computing. In: *Proceedings of the 11th Annual ACM Symposium on Theory of Computing*, 209–213 (ACM Press, NewYork, 1979).

[112] E. Kushilevitz and N. Nisan. *Communication complexity.* (Cambridge University Press, England, 1997).

[113] A. C.–C. Yao. Quantum circuit complexity. In: *Proceedings of the 34th Annual IEEE Symposium on Foundations of Computer Science*, 352–361 (IEEE Press, Los Alamitos, 1993).

[114] A. S. Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Probl. Peredachi Inf.* **9**, 3–11 (1973) [Translation: Probl. Inf. Transm. **9**, 177–183 (1973)].

[115] R. Cleve, W. van Dam, M. Nielsen, and A. Tapp. Quantum entanglement and the communication complexity of the inner product function. *Lecture Notes in Computer Science* **1509**, 61–74 (Springer–Verlag, London, 1999).

[116] R. Cleve and H. Buhrman. Substituting quantum entanglement for communication. *Phys. Rev. A* **56**, 1201–1204 (1997).

[117] L. Hardy and W. van Dam. Quantum communication using a nonlocal Zeno effect. *Phys. Rev. A* **59**, 2635–2640 (1999).

[118] H. Buhrman, W. van Dam, P. Høyer, and A. Tapp. Multiparty quantum communication complexity. *Phys. Rev. A* **60**, 2737–2741 (1999).

[119] H. Buhrman, R. Cleve, and W. van Dam. Quantum entanglement and communication complexity. *Siam J. Comput.* **30**, 1829–1841 (2001).

[120] T. Rudolph, and L. Grover. Quantum communication complexity of establishing a shared reference frame. *Phys. Rev. Lett.* **91**, 217905 (2003).

[121] H. Buhrman, R. Cleve, and A. Wigderson. Quantum vs. classical communication and computation. In: *Proceedings of the 30th Annual ACM Symposium on Theory of Computing*, 63–68 (ACM Press, New York, 1998).

[122] R. Raz. Exponential separation of quantum and classical communication complexity. In: *Proceedings of the 31th Annual ACM Symposium on Theory of Computing*, 358–367 (ACM Press, New York, 1999).

[123] Č. Brukner, M. Żukowski, and A. Zeilinger. Quantum communication complexity protocol with two entangled qutrits. *Phys. Rev. Lett.* **89**, 197901 (2002).

[124] Č. Brukner, M. Żukowski, J.-W. Pan, and A. Zeilinger. Bell's inequalities and quantum communication complexity. *Phys. Rev. Lett.* **92**, 127901 (2004).

[125] E. F. Galvão. Feasible quantum communication complexity protocol. *Phys. Rev. A* **65**, 012318 (2002).

[126] A. Cabello and J. López-Tarrida. Proposed experiment for the quantum "Guess My Number" protocol. *Phys. Rev. A* **71**, 020301(R) (2005).

[127] P. Xue, Y.-F. Huang, Y.-S. Zhang, C.-F. Li, and G.-C. Guo. Reducing the communication complexity with quantum entanglement. *Phys. Rev. A* **64**, 032304 (2001).

[128] R. T. Horn, S. A. Babichev, K.-P. Marzlin, A. I. Lvovsky, and B. C. Sanders. Single-qubit optical quantum fingerprinting. *Phys. Rev. Lett.* **95**, 150502 (2005).

[129] C. Schmid. Kompakte Quelle verschränkter Photonen und Anwendungen in der Quantenkommunikation. Master's thesis, Ludwig-Maximilians-Universität München, 2004.

[130] B. Schneier. *Applied Cryptography.* John Wiley & Sons, Inc., New York (1996).

[131] A. Shamir. How to share a secret. *Communications of the ACM* **22**, 612–613 (1979).

[132] G. R. Blakley. Safeguarding cryptographic keys. In: *Proceedings of the American Federation of Information Processing 1979 National Computer Conference* **48**, 313–317 (American Federation of Information Processing, Arlington, 1979).

[133] M. Żukowski, A. Zeilinger, M. A. Horne, and H. Weinfurter. Quest for GHZ states. *Acta Phys. Pol.* **93**, 187–195 (1998).

[134] M. Hillery, V. Bužek, and A. Berthiaume. Quantum secret sharing. *Phys. Rev. A* **59**, 1829–1834 (1999).

[135] W. Tittel, H. Zbinden, and N. Gisin. Experimental demonstration of quantum secret sharing. *Phys. Rev. A* **63**, 042301 (2001).

[136] Y.-A. Chen, A.-N. Zhang, Z. Zhao, X.-Q. Zhou, C.-Y. Lu, C.-Z. Peng, T. Yang, and J.-W. Pan. Experimental quantum secret sharing and third-man quantum cryptography. *Phys. Rev. Lett.* **95**, 200502 (2005).

[137] A. Karlsson, M. Koashi, and N. Imoto. Quantum entanglement for secret sharing and secret splitting. *Phys. Rev. A* **59**, 162–168 (1999).

[138] R. Cleve, D. Gottesman, and H.-K. Lo. How to share a quantum secret. *Phys. Rev. Lett.* **83**, 648–651 (1999).

[139] V. Scarani and N. Gisin. Quantum key distribution between N partners: Optimal eavesdropping and Bell's inequalities *Phys. Rev. A* **65**, 012311 (2001).

[140] A. Sen(De), U. Sen, and M. Żukowski. Unified criterion for security of secret sharing in terms of violation of Bell inequalities. *Phys. Rev. A* **68**, 032309 (2003).

[141] B. Huttner and A. Ekert. Information gain in quantum eavesdropping. *J. Mod. Opt.* **41**, 2455–2466 (1994).

[142] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger. Quantum cryptography with entangled photons. *Phys. Rev. Lett.* **84**, 4729–4732 (2000).

[143] D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund, and P. G. Kwiat. Entangled state quantum cryptography: Eavesdropping on the Ekert protocol. *Phys. Rev. Lett.* **84**, 4733–4736 (2000).

[144] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin. Quantum cryptography using entangled photons in energy-time Bell states. *Phys. Rev. Lett.* **84**, 4737–4740 (2000).

[145] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders. Limitations on practical quantum cryptography. *Phys. Rev. Lett.* **85**, 1330–1333 (2000).

[146] N. Lütkenhaus. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A* **61**, 052304 (2000).

[147] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy. Trojan-horse attacks on quantum-key-distribution systems. *Phys. Rev. A* **73**, 022320 (2006).

[148] G. P. He. Comment on "Experimental single qubit quantum secret sharing". *Phys. Rev. Lett.* **98**, 028901 (2007).

[149] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, Marek Żukowski, and H. Weinfurter. Schmid *et al.* reply. *Phys. Rev. Lett.* **98**, 028902 (2007).

[150] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger. Entanglement-based quantum communication over 144 km. *Nature Physics* **3**, 481–486 (2007).

[151] Casix, Inc. *Properties of Yttrium Vanadate (YVO_4) Crystal* `http://www.casix.com`.

[152] P. S. K. Lee, M. P. van Exter, and J. P. Woerdman. Increased polarization-entangled photon flux via thinner crystals. *Phys. Rev. A* **70**, 043818 (2004).

[153] M. Fiorentino, C. E. Kuklewicz, and F. N. C. Wong. Source of polarization entanglement in a single periodically poled $KTiOPO_4$ crystal with overlapping emission cones. *Opt. Express* **13**, 127–135 (2004).

[154] M. Żukowski. Bell theorem involving all settings of measuring apparatus. *Phys. Lett. A* **177**, 290–296 (1993).

List of Figures

1.1 Bloch sphere 6

2.1 Index ellipsoid 15
2.2 Effect of phase mismatch on the efficiency of SPDC 21
2.3 Scaling of down-conversion spectral width with the crystal length for different phase-matching configurations 27
2.4 Effect of the broadband pumping on the phase-matched spectral width 29
2.5 Absolute value of the normalized two-photon amplitude, $|\mathcal{A}(\tau_+, \tau_-)|$, for CW-pumped type I and type II SPDC 32
2.6 General geometrical setting to analyze the angular distribution of down-conversion light 33
2.7 Principal coordinate system of the crystal with the definitions of unit wave vectors of the three interacting fields in SPDC 34
2.8 Refraction of the relevant wave vectors on the faces of the crystal . . 36
2.9 Angular distribution of down-conversion light in type I phase matching 37
2.10 Angular distribution of down-conversion light in type II phase matching 38
2.11 The effect of pump focusing on SPDC emission pattern 40
2.12 Spatial walk-off as a cause of asymmetric broadening of type II emission pattern 41
2.13 Representation of the pump beam in the study of down-conversion emission distribution 42
2.14 Schematic set-up of the experiment to demonstrate momentum entanglement from a down-conversion source 44
2.15 Schematic set-up of the unbalanced interferometer to analyze energy-time entanglement 45
2.16 Explanation of the temporal distinguishability of down-conversion photons arising in type II phase-matching of SPDC 48

3.1 Growth of the source brightness over the recent years 54
3.2 Analysis of fibre coupling of down-conversion emission from a type-II phase-matched crystal in different regimes of pump focusing. 59

3.3 Simulated down-conversion emission distributions as a function of the divergence of the pump beam. 61
3.4 Basic emission properties of violet laser diodes 62
3.5 A typical example of the beam-shaped violet-LD output captured with a CCD camera 63
3.6 Emission characteristics of SPDC light calculated for the actual parameters of the source 65
3.7 The sketch of the non-collinear geometry of SPDC process 65
3.8 Schematic set-up of the compact non-collinear type-II SPDC source . 66
3.9 Photon-pair flux obtained from the compact non-collinear type-II SPDC source 67
3.10 Polarization correlation measurement of the photons emitted from non-collinear type-II source 68
3.11 Spectra of down-conversion light obtained in non-collinear type II source 69
3.12 Conceptual layout of the method to generate entangled photon pairs using collinear geometry of SPDC operated in type I non-degenerate configuration 70
3.13 Nonlinear phase-matching diagram for collinear type-I SPDC process 71
3.14 Schematic explanation of the detrimental spatial effect inherent to SPDC emission in the two-crystal geometry 73
3.15 Explanation of the detrimental time effect inherent to SPDC emission in a two-crystal geometry 74
3.16 Theoretical time distributions of photon wave packets originating from SPDC process in a two-crystal geometry 75
3.17 Theoretical time distributions of photon wave packets originating from SPDC process in a two-crystal geometry after passing through compensation crystal 77
3.18 Theoretical time distributions of photon wave packets originating from SPDC process in a two-crystal geometry after complete compensation using two tailored birefringent elements 78
3.19 The map of visibility $\mathcal{V}$ as a function of the length l of the compensation YVO_4 crystal and the pump duration τ_{p} 79
3.20 The map of visibility $\mathcal{V}$ as a function of the lengths l and l_p of the compensation YVO_4 crystals 79
3.21 Calculated dependence of the relative phase on the wavelengths of pump and one of the down-conversion photons for uncompensated and compensated configuration 81
3.22 Numerically simulated down-conversion spectra in type I non-degenerate phase matching for different coherence lengths of pump light and different crystal lengths 83
3.23 Spectral dependence of the isolation in two output ports of the WDM 84
3.24 Schematic set-up of the compact collinear type-I SPDC source 84

3.25 Photon-pair flux obtained from the compact collinear type-I SPDC source 85
3.26 Polarization correlation measurement of the photons emitted from collinear type-I source 87
3.27 Spectra of down-conversion light obtained in collinear type I source . 88

4.1 Experimental set-up for solving qubit-assisted communication complexity problems 98
4.2 Deviation of the phase shift by an YVO_4 crystal from the expected value 99
4.3 Histograms of measured quantum success probabilities for the two implemented communication complexity problems 101
4.4 General scheme for n party single-qubit secret sharing and the experimental set-up for $n = 6$ 106

A.1 Photo of the compact non-collinear type-II SPDC source 118
A.2 Photo of the compact collinear type-I SPDC source 118

B.1 Photo of the demonstration of single-qubit quantum secret sharing . . 121

List of Tables

2.1 Phase-matching schemes for uniaxial crystals 16

4.1 Relevant experimental parameters in the implementation of communication complexity problems 101
4.2 Results of the simulation of intercept/resend eavesdropping strategy in single-qubit secret sharing protocol 108

A.1 Basic nonlinear optical properties of BBO crystal 115
A.2 Basic optical properties of YVO_4 crystal 116
A.3 Comparison of sources of polarization entangled photons pairs 117

Acknowledgments

My Ph.D. study was exciting as well as challenging period of my life. What makes it an exceptional experience are fascinating people from whom I have learned not only professionally, but who also shaped (for the better) my personality. This thesis is a direct result of their helpful influence, for which I am very thankful.

First and foremost, I would like to express my deep and sincere gratitude to my supervisor Harald Weinfurter for giving me the opportunity to come to his group and for guiding me from the stage of being a novice to the stage where I can hopefully say interesting and new things about physics. His constant support, enthusiasm and insightful advice always provided a perfect basis for succeeding in many experiments.

I also thank Mohamed Bourennane and Christian Kurtsiefer for co-supervising me at the initial stages of the study. They have been always generous in their thoughts, time and advices. Marek Żukowski for the clear and to-the-point explanations of theoretical problems, and stimulating discussions resulting in several publications.

In particular, a great deal of gratitude goes to Chris, Manfred, Nikolai and Witlef for the encouragement and countless discussions, which always helped to overcome physical (and sometimes non-physical) problems. It has truly been a pleasure working with them for the last almost five years here in Garching. One of the pleasures of doing my Ph.D. was enjoying time with other friends and colleagues from MPQ and University: Daniel, Reinhold, Roland, Sascha, Uli, Yousef, and Carsten, Chunlang, Daniel, Florian, Gerhard, Henning, Jürgen, Magdalena, Markus, Martin, Oliver, Patrick, Sebastian, Tobias, Wenjamin. I thank them for their help whenever I needed and for their friendship.

The first year of my study would not be possible without the financial support of Marie Curie Fellowships, which I greatly appreciate as well. I also would like to thank Miloslav Dušek and Jan Peřina, Jr., who helped me very much with the smooth transition to Munich.

I am grateful to my parents and brother for their unwavering support and understanding throughout all the years. Finally, in a very special way, I thank to dear Monika: for her endless patience, encouragement, and healthy amount of distraction from the work. Without her I would never overcome plenty of difficult and unexpected situations and truly enjoy all the joys around us. I am her debtor.