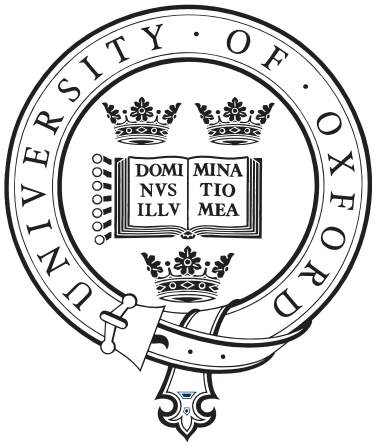
Towards Single Photon Quantum Key Distribution with Continuous Variables

Lijian Zhang
Wolfson College, Oxford



Submitted for the degree of Doctor of Philosophy
Hilary Term 2009

Supervised by
Prof. Ian A. Walmsley

Clarendon Laboratory
University of Oxford
United Kingdom

To my parents.

Abstract

Photons have a rich structure associated with their continuous variable (CV) degrees of freedom: spectral (time-frequency) and spatial (momentum-position). This modal structure offers a new degree of freedom for quantum information processing based on photons. In this thesis we study a quantum cryptography (QKD) scheme based on the spatial correlations of the photon pairs generated from parametric downconversion (PDC), and several major factors of the experimental implementation.

We study the methods to tailor the PDC state for different quantum information processing purposes. In particular, we derive the conditions to generate highly correlated photon pairs in continuous variable (spatial or spectral) degrees of freedom, as well as spatio-temporally factorable state. The latter allows the generation of heralded single photons in pure states without filtering. We show that the spatially highly correlated PDC state can be used to violate a Bell inequality constructed from a measurement of the transverse wavevector Wigner function. This reveals the potential of this kind of state for transferring secure informations. We further analyse the performance of a specific QKD protocol using this kind of state. The information content is derived for a realistic source, which demonstrates a boosted key distribution rate. We show that due to the non-Gaussian character of the experimental imperfections, standard measures of security known for quadrature-based CV-QKD are inadequate for single-photon CV-QKD. A specific simple eavesdropping attack, known as the intercept-resend attack, is analysed to illuminate how secret information may be distilled well beyond the bounds of the usual CV-QKD measures.

To access the full potential offered by the spatial degree of freedom of single photons or entangled photon pairs, a detector array that can well distinguish single-photon events is required. As a potential candidate, an electron multiplying charge coupled device (EMCCD) camera is experimentally characterized. The camera exhibited single-photon sensitivity, good quantum efficiency and relatively low noise. However, it is possible that imperfect charge transfer efficiency broadens the effective pixel size and reduces the spatial resolution.

Acknowledgements

The work presented in this thesis was made possible with the help, guidance and support from those around me. I owe them more thanks than can be fitted in merely few pages. Still, I would like to make the effort with my clumsy words.

First and formost, I need to express my sincere gratitude to my supervisor, Professor Ian Walmsley for offering me the opportunity to work in his research group. For sure I need to thank Ian for his professional guidance throughout my study. Ian's vast knowledge of physics never cease to amaze and inspire me. Working with him is not only academically challenging but also enjoyable. The last five years has been such a great learning experience that it will undoubtedly influence my whole academic career.

Secondly, I would like to thank all the postdocs I have worked with during my D.Phil. study. It was a true pleasure to work with them. Christine Silberhorn had been a mentor to me since I joined the group. She helped me to start the project. I kept getting assistance from her even after she left the group. In the later stage, Jeff Lundeen taught me a lot in developing my experiment skills as well as gave me invaluable suggestions on my work. Leonardo Neves was a steadfast work companion throughtout the experiment on the EMCCD camera, though it is a mystery to me how he could enjoy the weather in oxford. Brian Smith gave me enthusiastic advice on everything and moreover, spent a lot of time helping me to correct the mistakes in this thesis. I must also thank Piotr Wasylczyk for sharing his fantastic experiment experience, Rob Davis for the assistance in the double slit experiment, and Graciana Puentes for inspiring conversations.

Upon my arrival in oxford, it was my first time to live in an environment with totally different culture than I had been used to. No doubt there were many uncertainties in front of me which made me slightly nervous. Fortunately the group is so friendly that they help me to get over the difficulties and be adapted to the new life. I thank all the group members for their kind assistance throughtout my degree. Firstly the Rochester students, especially Alfred U'ren for teaching me downconversion and collaborations on factorable states, Manuel de la Cruz for the invitation to the Christmas dinner and being as my first lab mentor, as well as the first Oxford Ultrafast students Matthijs Branderhorst and Daryl Achilles. I would like to thank Peter Mosley for organizing pub tours which helped me to develop my capacity for liquor, Adam Wyatt for the BBQs and puntings, Alex Dicks for helping me moving house, Josh Nunn for those cups of tea (though I am not a big fan of tea, still, thanks for asking me every time). I also need to thank David McCabe, Ben Sussman, KC

Lee, Huga Marty, Phil Bustard, Hendrik Coldenstrodt-Ronge, Nick Thomas-Peter, Jovana Petrovic, Gina Lorenz, Melissa Friedman, Dane Austin, Tobias Witting, Offir Cohen, Duncan England, Klaus Reim, Xiaodan Yang, Antoine Monmayrant, Laura Corner and Felix Waldermann for the favors I received from them.

I would like to thank Sue Gardner and Agnieszka Borkowska for helping me to sort out all the documents problems.

I wish to acknowledge the support from K. C. Wong scholarship for funding received for my first three years study, and to Ian Walmsley for funding during the remainder of the time.

Finally, I would like to express my sincere gratitude to my parents. Thanks for everything you have done for me. This thesis is dedicated to you.

List of Publications

Journal publications

1. L. Zhang, A. B. U'ren, R. Erdmann, K. A. O'Donnell, Ch. Silberhorn, K. Banaszek and I. A. Walmsley, *Generation of Highly Entangled Photon Pairs for Continuous Variable Bell Inequality Violation*, Journal of Modern Optics, **54**, 707-719, 2007.

   See chapter 3.

2. L. Zhang, Ch. Silberhorn, and I. A. Walmsley, *Secure Quantum Key Distribution using Continuous Variables of Single Photons*, Physical Review Letters, **100**, 110504, 2008.

   See chapter 4.

3. L. Zhang, L. Neves, J. S. Lundeen and I. A. Walmsley, *A Characterization of the Single-Photon Sensitivity of an Electron Multiplying Charge-Coupled Device*, Journal of Physics B: Atomic, Molecular and Optical Physics, **42**, 114011, 2009.

   See chapter 5.

Miscellaneous

1. L. Zhang, E. Mukamel, I. A. Walmsley, Ch. Silberhorn, A. B. U'ren and K. Banaszek, *Continuous Variable for Single Photons*, Quantum Information with Continuous Variables of Atoms and Light, eds N.J. Cerf, G. Leuchs and E.S. Polzik, World Scientific, 367-388, 2007

Contents

List of Figures

Chapter 1

Introduction

1.1 Quantum information processing with continuous variables

Quantum information processing (QIP), the combination of quantum mechanics, computer science and information theory, not only promises technical capabilities beyond classical computing and communication systems, but also yields several new insights into physics and profound understandings of the workings of nature. Inspired by classical information theory, the early stages of QIP focused on discrete quantum systems, especially on two-level systems, called quantum bits or qubits. System with discrete and finite Hilbert spaces are also amenable to rigorous mathematical treatment. However there are important quantum degrees of freedom which take on a continuum of values, *e.g.*, position and momentum, time and freqency, quadrature amplitudes of the electromagnetic field *etc.* a straightforward way to

employ these continuous variables in QIP is to split the continuous variables (CVs) into discrete bins or resort to filtering one or the other discrete values[1,2]. Thus some of the results for discrete variables (DVs) can be applied to the discretized CVs. But these methods have limitations, since the evolution of continuous quantum variables has some intrinsic differences from that of DV[3], which cannot be removed by the artifical discretization. An alternative way is to keep the continuous nature of the Hilbert space in preparing, manipulating and measuring the quantum state. Here the only discretization is due to the finite resolution of a practical detection system.

The most commonly studied CV-QIP schemes consider the quadrature amplitudes of the electromagnetic field, denoted as $\hat{X}$ and $\hat{P}$, which are defined by

$$\hat{X} = \frac{1}{2}(\hat{a}^\dagger + \hat{a}) \tag{1.1}$$

$$\text{and} \quad \hat{P} = \frac{1}{2}i(\hat{a}^\dagger - \hat{a}) \tag{1.2}$$

where $\hat{a}^\dagger$ and $\hat{a}$ are the creation and annihilation operators of a single mode of the quantized field. The expectation values of $\hat{X}$ and $\hat{P}$ take on a continuum of values, and may not be precisely determined simultaneously, due to the Heisenberg Uncertainly Principle. The quantum state of the mode of the electromagnetic field is usually described in terms of quasi-probability distributions, such as the Wigner function $W(X, P)$, in the phase space of the two quadratures.

The feasibility of CV-QIP with the quadrature amplitudes has been widely studied and experimentally demonstrated in quantum teleportation[4–7], quantum dense

coding[8,9], quantum cryptography[10–14] and quantum computation[3]. So far most of the CV-QIP applications deal with Gaussian states, *e.g.* coherent states and squeezed states, whose phase space representations, *i.e.* Wigner functions, are Gaussian functions. The operations involved in most applications are Gaussian as well. Operations such as phase shifting, beam splitting, squeezing, phase space displacement, homodyne detection, heterodyne detection are Gaussian operations that map Gaussian states onto Gaussian states. For more sophisticated applications, such as universal CV quantum computation and CV entanglement distillation, Gaussian operations on Gaussian states are not enough[3]. One must employ either non-Gaussian states (Fock states, Schrödinger cat states, *etc*) or non-Gaussian operations (Kerr interaction[3], photon-subtraction, photon number quantum nondemoliton measurement[15], *etc.*) for such applications.

From a technical point of view continuous variables potentially enable one to encode, transfer and process more information per quantum system than dichotomic variables associated with a qubit. This has been demonstrated in CV dense coding[8,9], quantum cryptography[10–12,14] and quantum computation[3]. Moreover, CV-QIP implementations using quadrature amplitudes normally have high efficiency due to their *unconditionalness*[3], which means that the quantum resources are generated in a deterministic manner, and no heralding or postselection conditions such as those used in the generation of single-photon states, are required. On the other hand, these implementations have the drawback that quantum characteristics of such states are sensitive to loss, and usually require a phase reference, *i.e.* local

oscillator, to carry out measurements.

1.2 Quantum entanglement

Best possible knowledge of a whole does not include best possible knowledge of its parts – and this is what keeps coming back to haunt us.

E. Schrödinger [16]

Entanglement is one the most important concepts in quantum mechanics, and one the of the features that distinguish quantum formalism from classical formalism. Moreover, it is a key resource for quantum information processing [17–20]. In addition to the well-known quantum communication applications, like quantum teleportation and quantum dense coding, entanglement can help to reduce the communication complexity [21], or increase the transmission distance of quantum states by entanglement swapping in quantum repeaters [22]. In quantum cryptography it turns out that entanglement plays an important role in the security analysis [23–25]. Although it is unclear whether the quantum computation speed-up benefits from entanglement, entanglement is a crucial ingredient for linear optical quantum computation with feedforward [26] or with cluster states [27]. Manipulation, characterization and quantification of entanglement are very broad topics and a multitude of research has been done in this field (for a comprehensive review, see [28]). This section will concentrate on the results related to the work in this thesis.

1.2.1 Definition and properties

The original definition of entanglement was given in a passive way: *a global state of composite system which cannot be written as a product of the states of individual subsystems*[28]. To formulate in the language of quantum mechanics, consider a multipartite system consisting of n subsystems, the total Hilbert space $\mathcal{H}$ is a tensor product of the subsystem spaces $\mathcal{H} = \otimes_{l=1}^{n}\mathcal{H}_l$. Then a state $|\psi\rangle$ is an entangled state if for any state $|\psi_l\rangle$ in $\mathcal{H}_l$

$$|\psi\rangle \neq \otimes_{l=1}^{n} |\psi_l\rangle \,. \tag{1.3}$$

Due to noise and decoherence in most practical situations a general quantum state will be a mixed state ρ instead of a pure state $|\psi\rangle$. The definition of entangled state is modifed such that the density operator ρ cannot be written as a convex combination of product states[28,29]:

$$\rho \neq \sum_i P_i \left(\otimes_{l=1}^{n} \rho_l^i\right). \tag{1.4}$$

Recently there has been an active definition of entanglement proposed by L. Masanes *et al*[30]: *entangled states are the ones that cannot be simulated by classical correlations.* This defines the entanglement from its behavior instead of the preparation of the state, and emphasize the entanglement as a signature of quantum coherence.

In fact, entanglement is more than correlations. As first pointed by Schrödinger,

entanglement involves the nonclassical relation between the information about the whole system and the information between subsystems [16,28]. This is formulated into the following entropic inequality: the von Neumann entropy of a subsystem can be greater than the entropy of the whole system only when the state is entangled [31]. This allows negative quantum information (more precisely, partial quantum information) to exist, which can be used for future quantum communication applications, *e.g.*, quantum teleportation [32].

The work of this thesis only involves bipartite entangled states, so the following discussions will be restricted to this kind of states.

1.2.2 Characterization of entanglement

A fundamental problem in quantum mechanics is to distinguish entangled states from separable states. This is also a necessary step for QIP applications based on entanglement. Moreover, for some applications it is required to quantify the entanglement contained in the state. Unfortunately there are usually no simple answers to such questions. Numerous criteria have been suggested for different situations. This section will discuss several of them related to the content of this thesis.

Schmidt decomposition

The simplest situation is to characterize the entanglement of pure states. Any bipartite pure state $|\psi_{AB}\rangle \in \mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$ of subsystems A and B can be

written as

$$|\psi_{AB}\rangle = \sum_j \sum_k a_{jk} |j_A\rangle \otimes |k_B\rangle \tag{1.5}$$

where $|j_A\rangle$ and $|k_B\rangle$ are arbitrary orthonormal bases of $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively. Then there exist unitary transformations U and V, such that $|i_A\rangle \equiv U|j_A\rangle = \sum_j u_{ji}|j_A\rangle$ and $|i_B\rangle \equiv V|k_A\rangle = \sum_k v_{ik}|k_B\rangle$, which allow the joint state $|\psi_{AB}\rangle$ to be written in a diagonal form[33]

$$|\psi_{AB}\rangle = \sum_i \sqrt{\lambda_i} |i_A\rangle \otimes |i_B\rangle \tag{1.6}$$

Hhere the λ_i are non-negative real numbers satisfying $\sum_i \lambda_i = 1$ known as Schmidt numbers. From Eq. 1.6 it is clear that $|\psi_{AB}\rangle$ is an entangled state if and only if there is more than one nonzero Schmidt number in $\{\lambda_i\}$. Then the entanglement entropy

$$E = -\sum_i \lambda_i \log \lambda_i \tag{1.7}$$

and the Schmidt number[34,35]

$$K = \frac{1}{\sum_i \lambda_i^2} \tag{1.8}$$

can be used to quantify the degree of entanglement. For separable states, we have $E = 0$ and $K = 1$.

Schmidt decompostion can also be used to analyse the entanglement of bipartite

continuous variable states, which can be written as

$$|\psi_{AB}\rangle = \int dx_A dx_B \mathcal{A}(x_A, x_B) |x_A\rangle \otimes |x_B\rangle \tag{1.9}$$

Here $\mathcal{A}(x_A, x_B)$ is the joint probability amplitude which satisfies the normalization condition $\int dx_A dx_B |\mathcal{A}(x_A, x_B)|^2 = 1$. It has been shown that $\mathcal{A}(x_A, x_B)$ can be decomposed as[36]

$$\mathcal{A}(x_A, x_B) = \sum_i \sqrt{\lambda_i} \phi_i(x_A) \varphi_i(x_B) \tag{1.10}$$

where $\{\phi_i\}$ and $\{\varphi_i\}$ are two sets of orthonormal modes. The state $|\psi_{AB}\rangle$ can then be written as

$$|\psi_{AB}\rangle = \sum_i \sqrt{\lambda_i} |\phi_i\rangle |\varphi_i\rangle \tag{1.11}$$

where $|\phi_i\rangle = \int dx_A \phi_i(x_A) |x_A\rangle$ and $|\varphi_i\rangle = \int dx_B \varphi_i(x_B) |x_B\rangle$. The subsequent discussions hold for both discrete variable and continuous variable states. The Schmidt decomposition has been used to analyse the entanglement of the bi-photon state generated from parametric downconversion[35,37]. However this method can only be used to analyse the entanglement of pure states. The analysis of the entanglement of mixed states needs other tools, which we discuss next.

Negative partial transpose

As shown in Eq. 1.4, a mixed bipartite separable state can be written as

$$\rho_{AB} = \sum_i P_i \left(\rho_A^i \otimes \rho_B^i \right). \tag{1.12}$$

As suggested in[38], applying a transposition to one of the subsystems, say B, yields another valid state, *i.e.*, another legitimate non-negative density operator

$$\rho_{AB}^{T_B} = \sum_i P_i \left(\rho_A^i \otimes \left(\rho_B^i \right)^T \right). \tag{1.13}$$

If ρ_{AB} is not a separable state, $\rho_{AB}^{T_B}$ is usually not a physical density operator any more, and could have negative eigenvalues[38]. Checking the positivity of $\rho_{AB}^{T_B}$ allows one to tell a separable state from an entangled state. It turns out that the negative partial transposition condition is necessary and sufficient condition for the entanglement of composite systems with dimensions $2 \otimes 2$ and $2 \otimes 3$. Moreover, a quantity called *Negativity* is defined as[39]

$$\mathcal{N}(\rho) \equiv \frac{\left|\left|\rho_{AB}^{T_B}\right|\right| - 1}{2} \tag{1.14}$$

where $||X|| \equiv \mathrm{Tr}\sqrt{X^\dagger X}$ is the trace norm. There is also a modified version called *Logarithmic Negativity*

$$E_{\mathcal{N}}(\rho) \equiv \log \left|\left|\rho_{AB}^{T_B}\right|\right| = \log \frac{2\mathcal{N}(\rho) + 1}{2} \tag{1.15}$$

Both the *Negativity* and *Logarithmic Negativity* can be used to quantify the degree of entanglement. For a separable state, $\mathcal{N}(\rho) = E_{\mathcal{N}}(\rho) = 0$. Only entangled states can give positive values for this quantity[40].

However, there are also entangled states that can have a positive partial trans-

postion, *i.e.*, $\mathcal{N}(\rho) = E_{\mathcal{N}}(\rho) = 0$. This is related to the issues of entanglement distillation and bound entanglement[41,42].

Negativity analysis can also be applied to continuous variable states. This will be discussed in Sec. 4.3.4.

Entanglement witnesses

Many approaches to entanglement characterization have the difficulty that they require the full information about the state, *i.e.*, quantum tomography of the state is required, which is difficult to implement for arbitrary states. Therefore a more economic way to detect the presence of entanglement has been proposed, which is called an entanglement witness[43–46]. An entanglement witness is an observable or Hermitian operator W that (i) has at least one negative eigenvalue and (ii) has nonnegative expectation value on every product state

$$\langle\phi_A|\langle\varphi_B|W|\phi_A\rangle|\varphi_B\rangle \geq 0 \tag{1.16}$$

for all pure product states $|\phi_A\rangle|\varphi_B\rangle$[28]. Then if a state ρ_{AB} is separable, it should have non-negative mean value for W:

$$\mathrm{Tr}(W\rho_{AB}) \geq 0 \tag{1.17}$$

Therefore a state is entangled as long as $\mathrm{Tr}(W\rho_{AB}) < 0$. This is schematically demonstrated in Fig. 1.1, where the separable states form a convext set, and the

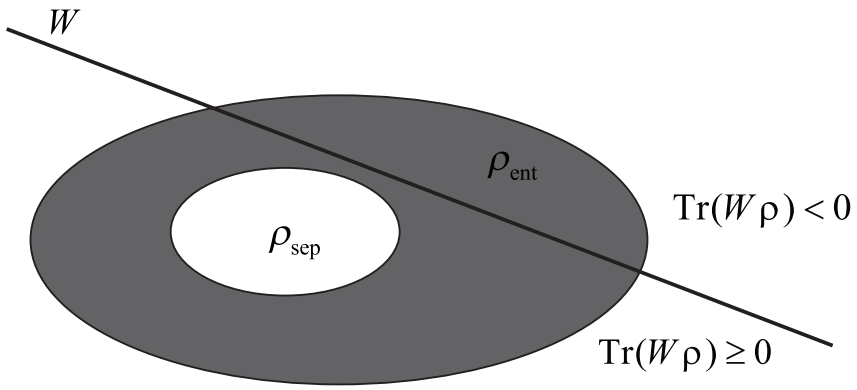


Figure 1.1 Schematic representation of entanglement witnessing. The separable states form a convex set, while the entanglement witness, or the observable, W is a hyperplane. All the states located to the left of the hyperplane, including the separable states, yield a nonnegative mean value for $\mathrm{Tr}(W\rho)$. Only entangled states can have a negative mean value and are located to the right of the hyperplane.

entanglement witness W represents a hyperplane [28,47].

Usually entanglement witnessing is much weaker than the positive map conditions, *e.g.*, partial transpose, in the sense that a single map is equivalent to a set of witnesses [28]. On the other hand, an entanglement witness represents an observable that can be directly measured. So it plays an important role in the experimental detection of entanglement [48–50]. Moreover, when considering entanglement based quantum communication applications, *e.g*, quantum cryptography, it is necessary to decompose the witness into locally measurable observables, since it requires one to detect the entanglement between spatially separated systems. This issue is studied in Refs [51,52].

1.2.3 Entanglement and nonlocality: Bell's theorem

Although entanglement is one of the most nonclassical features of quantum mechanics, its first explicit notion was in the famous paper by Einstein, Podolsky and Rosen [53] as an objection to quantum mechanics because it implies a 'spooky action-at-a-distance', or nonlocality [1]. Therefore they suggest quantum mechanics is incomplete ("the wave function does not provide a complete description of the physical reality" [53]) and must be supplemented by some local hidden variables.

In 1964 John Bell accepted the conclusions of EPR as a working hypothesis, and formulated it into a local hidden variable model [54]. The model assumes the measurement results (α and β) on the spacelike separated subsystems (A and B) are predetermined by the local measurement settings ($\mathbf{a}$ and $\mathbf{b}$) and the properties (hidden parameters λ) the systems carry prior to, and independent of, the measurements. The joint probability of the measurement results conditioned on the measurement settings can be written as

$$P(\alpha,\beta|\mathbf{a},\mathbf{b}) = \int d\lambda\ \rho(\lambda) P^A(\alpha|\mathbf{a},\lambda) P^B(\beta|\mathbf{b},\lambda) \tag{1.18}$$

where $\rho(\lambda)$ is the probability distribution of λ, $P^A(\alpha|\mathbf{a},\lambda)$ and $P^B(\beta|\mathbf{b},\lambda)$ are the probabilities of measurement results on A and B conditioned on the local measurement settings and λ. Bell proved this condition would impose some constraints on the statistical correlations of α and β in the form of Bell inequalities. Then he

[1] In fact, the 'action-at-a-distance' did not appear explicitly in the orgininal EPR paper. Instead, they assume that two subsystems separated at a distance can not interact with each other. In particular the measurment result of one subsystem will not affect the state of the other

showed that properly prepared bipartite entangled states can violate this inequality. In this sense the local hidden variable model can not be consistent with quantum mechanics. Inspired by Bell's work, Clauser, Horne, Shimony and Holt modified Bell's result to accommodate the imperfections of practical experiments[55]. Since then, different experimental demonstrations of the violation of CHSH inequality have been reported[56–60], which confirms the predictions of quantum discription.

However, the relation between entanglement and nonlocality is nontrivial. It has been shown that any pure bipartite entangled state can violate a CHSH inequality for suitably chosen variables[61,62]. While for mixed states this is not necessarily the case. Generally speaking, Bell inequalities are entanglement witnesses[44]. Recently, it has been shown that each entangled state σ can display some hidden nonlocality in the sense that there exists another state ρ not violating the CHSH inequality such that $\rho \otimes \sigma$ violates a CHSH inequality[30]. So in principle Bell inequalities can be used for two tasks: testing quantum formalism against local hidden variable models, and detection of entanglement within quantum formalism.

1.3 Quantum cryptography

Cryptography usually involves the transmission of secret messages between two or more parties (for two parties, they are usually called Alice and Bob). The message is rendered such that only the authorized parties can read it. To achieve this goal, the message is combined with some additional information, or the 'key', with some encryption algorithm. Without knowing the key, one can not extract the original

message from the encrypted information. Therefore a crucial issue is to distribute the key between the legitimate parties. Classical cryptography can usually be divided into public key cryptosystems and private key cryptosystems. The security of classical cryptography is usually based on computational complexity. For example, the security of a well known clan of public key systems, the RSA cryptosystem, is based on the fact that factoring a large integer is computationally difficult on classical computers. However, it turns out that a quantum computer can overcome this problem with the use of Shor's algorithm [63]. This presents a great challenge to public key systems. Private key systems usually offers better security. But it has a severe problem in how to distribute the key, which is vulnerable to eavesdropping.

Fortunately, although quantum information processing poses a threat to classical cryptography, it also offers a completely new way to solve the key distribution problem. This quantum solution is called quantum cryptography, or quantum key distribution (QKD). The basic idea of QKD is to employ a quantum state to deliver the secret key. Due to a fundamental principle of quantum mechanics: *every measurement perturbs the state* (unless the state is compatible with the measurement). Therefore the presence of eavesdropping (usually denoted by the protagonist, Eve) will appear as a disturbance of the communication channel and thus be detected by Alice and Bob. According to the variables that carries the information, QKD schemes can be divided into two major categories: discrete variable QKD (DVQKD) and continuous variable QKD (CVQKD).

1.3.1 Discrete variable quantum key distribution: BB84 and Ekert91

The idea of QKD was first proposed by Wiesner[64] and the first protocol was proposed in 1984 by C.H. Bennett and G. Brassard[65], which is known as the BB84 protocol. In this protocol the information, or the key to be distributed between Alice and Bob, is encoded into the polarization of photons. Alice chooses randomly between two bases $\oplus$ (the eigenstates of Pauli σ_x operator) and $\otimes$ (the eigenstates of the Pauli σ_z operator) to prepare the quantum states and sends them to Bob. In $\oplus$ basis, the vertically polarized state $|V\rangle$ is assigned the value '1' and the horizontally polarized $|H\rangle$ is assigned '0', while in $\otimes$ basis, the $+45°$ polarized state $|+\rangle$ represents '1' and the $-45°$ polarized $|-\rangle$ represents '0'. Since σ_x and σ_z do not commute with each other, their eigenstates are nonorthogonal. In fact

$$|+\rangle = \frac{|H\rangle + |V\rangle}{\sqrt{2}} \tag{1.19}$$

$$|-\rangle = \frac{|H\rangle - |V\rangle}{\sqrt{2}} \tag{1.20}$$

and $|\langle H|+\rangle|^2 = |\langle H|-\rangle|^2 = |\langle V|+\rangle|^2 = |\langle V|-\rangle|^2 = 1/2$. When Bob receives the states he also also randomly chooses the basis to perform the measurements. If Alice and Bob use the same basis, they get perfectly correlated results, otherwise they get totally uncorrelated results. Hence, without other disturbance, Bob gets a string of bits with on average a 25% error rate, which is called the *raw key*. Alice and Bob then tell each other the bases they used over an authenticated public

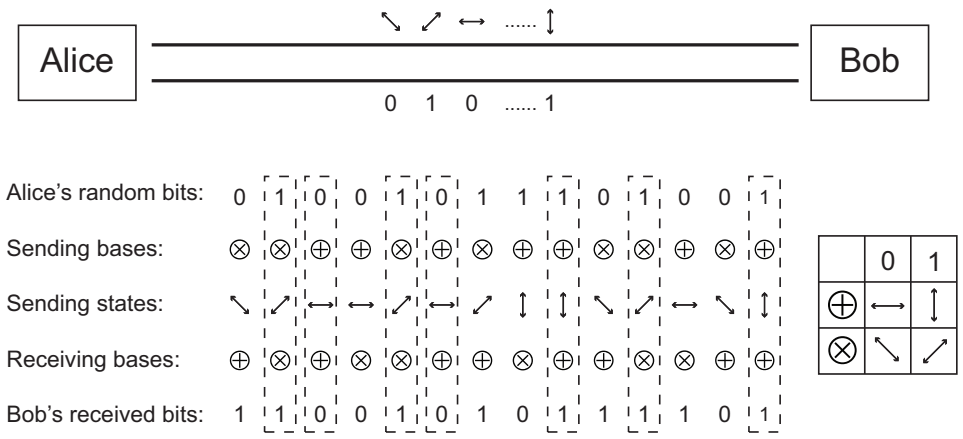


Figure 1.2 An example of key distribution process of BB84. Alice generates a string of random bits and encode it on photons in a randomly chosen basis ($\otimes$ and $\oplus$. The mapping between the bits and the photon states is shown to the right. When Bob receives a photon, he random chooses a basis to perform the measurement. The bits that Alice and Bob use the same basis (in the dashed lines) are the sifted key.

channel, and keep only the bits corresponding to the same bases, the *sifted key*. Fig. 1.2 shows an example of the key distribution process. If Eve wants to listen to the quantum states that Alice sent to Bob, there are two principles of quantum mechanics that get in her way. The first is the *No Cloning theorem*: one can not duplicate an unknown quantum state, therefore the only option that Eve has is to interact with the original state. The second is the *Heisenberg Uncertainty Principle*, which prevents her to measure, no matter whether directly or not, the polarization in two bases simultaneously. So she needs to choose one basis for her measurement, and if her choice is not compatible with those of Alice and Bob, she will introduce disturbance and unveil herself.

In fact, Eve can employ very powerful attacks. For example, she could entangle

her ancillas with the photons that is passed between Alice and Bob, and with the aid of a quantum memory, she can even apply joint manipulation and measurement of her ancillas[66–68]. Fortunately, no matter what she does, she can not avoid the disturbance to the states shared by Alice and Bob. However, in practical systems, Alice and Bob usually will not have a perfect quantum channel. Losses and various noise should be take into account, which will also appear as disturbance to the states transmitted. This gives an opportunity to Eve: she can exchange the channel with a lossless and noiseless one (for example, with quantum relay[69] or even quantum memory), and apply her attack. Since it is hard to distinguish between the disturbance introduced by the channel and by Eve, Alice and Bob need to consider the worst situation where all the disturbances are due to Eve. From the disturbance, or the error rate in BB84, they can estimate the maximum information that Eve may have acquired. Then they can apply error correction and privacy amplification[70,71] to lower Eve's information down to zero.

Since the BB84 protocol was proposed, there has been a large collection of variations, including QKD with 2 nonorthogonal states[72], QKD with 6 states[73], QKD with blind polarization bases[74], QKD based on the relative phases of single-photon superpostion states[75,76], *etc.* Among them one of particular interest is the QKD scheme proposed by Ekert in 1991[77], which is based on entangled photon pairs. In that work, Ekert suggested using the violation of a Bell's inequality as a measure of security. Since Bell's inequalities are entanglement witnesses, Ekert's work actually set connection between entanglement and security, which has later been discussed

in a lot of works[23–25,78]. A concrete connection between Bell's theorem and the security of QKD has been proved recently[79].

Almost all of these schemes employ single-photon state as the information carriers. So, as discussed in Sec. 1.1 in principle they are not sensitive to the channel loss. But in practice, perfect single-photon sources are hard to get using current technology, so usually Alice and Bob should have to compromise and use an attenuated coherent state as the photon source. This severely limit the performance of the scheme. Since the coherent state contains the multiphoton ($n > 1$) component, Eve can apply a photon-number-splitting (PNS) attack[80–82]. To understand this consider a pulsed laser source with 10% probability of a single photon in a pulse, and 90% probability for multiphoton events. If the channel loss is 90% or higher, Eve could switch the channel with a lossless one, block all the single photon events and split a photon from each multiphoton event, sending the residue to Bob. Bob will not notice the change of the channel loss since he still receives 10% of the pulses, as he expected. However, Eve has an identical copy of the signal that Bob possesses, and the security of QKD is compromised. To simply the analysis, for this example we ignore the events that a pulse contains no photon, *i.e.* vacuum state. Actually the ratio of this event can play an important role in the detection of the presence of Eve[83].

From the description of PNS attack, one can imagine that if Alice and Bob could monitor the losses of pulses with different photon numbers, they could easily detect the presence of Eve. But this requires a perfect photon-number-resolving detector,

which is also not currently available. An alternative way is to randomly adjust the intensity of the coherent state. Since the transmission (or yield) of the coherent state is decided by its intensity in a definite way if there is no eavesdropper, by monitoring the yield of different coherent state amplitude, it is possibly to reveal Eve. This is called the *decoy state quantum key distribution* [83–86]. It has been experimentaly demonstrated that this greatly improves the performance of practical QKD systems, even close to the limit of the theoretical prediction [87–91].

There is another scheme against the PNS attack called SARG04 [92], which modifies the classical sifting procedure of BB84 protocol. A comparison of the performance of decoy state QKD and SARG04 was given by C.F. Fung *et al* [92].

1.3.2 Continuous variable quantum key distribution

QKD schemes based on BB84 encode the quantum information on dichotomic variables, *e.g.* polarizations, thus the maximum information transfer rate is intrinsically limited to one bit per signal. As mentioned in Sec. 1.1, there are numerous QIP schemes based on quantum continuous variables. So it is not suprising that there are suggestions about employing continuous variables in quantum key distribution [10,13,93,94]. Most of these schemes utilize the quadrature amplitudes of either coherent states [95] or squeezed states [11,12] as the information carrier. Another approach is to encode the information on the choice of the quadrature while using the value of the quadratures to test the correlations [13]. This scheme in principle possess as similar advantages as the other CV-QIP schemes, *e.g.*, deterministic generation

of the signal and a potentially high key distribution rate.

Similar to DVQKD schemes, the security of quadrature-based CVQKD is guaranteed by the basic principles of quantum mechanics: uncertainty principle, no-cloning theorem, no-measurement theorem, *etc.* However, due to the features of the quantum state involved as the information carrier, the detailed security analysis of practical systems requires special treatment. Since the signals are encoded on multi-photon states, security is sensitive to the channel loss and this opens a loophole for the beam splitter attack: Eve replaces the lossy channel with a perfect one and uses a beam splitter to mimic the channel loss, so that she possesses a copy of the state that Bob received with a fidelity depending on the beam splitter transmission. In the previous works, it was suggested that the channel loss should be below 50% (3dB)[95]. This severely limits the available communication distance. Fortunately it has been shown that limit could be overcome by postselection[96,97] or reverse reconciliation protocols[14]. An experimental demonstration of CVQKD with reverse reconciliation was done by F. Grosshans *et al* in 2003[14]. The security of CVQKD against more powerful attacks, including non-Gaussian attack and collective attack, has been shown in[98,99]. S. Pirandola *et al* showed that a CVQKD with two-way quantum communication can improve the performance even further[100].

1.4 Continuous variables for single photons

It is well known that according to non-relativistic quantum mechanics, position and momentum are canonical conjugate variables. Similar to quadrature amplitudes,

they may take a continuum of values, but due to the Heisenberg Uncertainty Principle cannot both have a definite value at the same time. So intuitively, one expects that in principle the position and momentum of single photons could play a similar role in QIP as the quadrature amplitudes of the electromagnetic field. However this is not trivial consideration. As a spin-1 particle with no rest mass or charge, photons cannot be localized in coordinate space[101], *i.e.*, there is no position operator $\hat{r}$ defined for photons. One cannot define a probability density for the position of photons, or in terms of quantum mechanics, the photon number operator $\hat{n}_{V,t}$ in a specific space-time region $\{V, t\}$ is not an integral of photon density operator over V[102], and the photon number operators $\hat{n}_{V_1,t_1}$ and $\hat{n}_{V_2,t_2}$ for two disjoint region $\{V_1, t_1\}$ and $\{V_2, t_2\}$ do not strictly commute[103]. However it has been shown by Mandel[103] that one may approximately localize a photon in a volume V larger than its cubic wavelength. Moreover, it has been shown that the energy density, and so the photodetection rates, of photons is localized in space with an exponential falloff[104]. All these results suggest that it is possible to introduce a photon wave function in coordinate representation $\vec{\psi}(\vec{r}, t)$ which satisfies the equation[105–107]

$$i\frac{\partial\vec{\psi}(\vec{r},t)}{\partial t} = \pm c\nabla\times\vec{\psi}(\vec{r},t), \tag{1.21}$$

where $\pm$ corresponds to the helicity of the photon. Instead of being a probability amplitude, $\vec{\psi}(\vec{r}, t)$ is the energy amplitude, *i.e.*, the energy of the photon in a volume

$d\vec{r}$ about $\vec{r}$ is

$$\vec{\psi}^*(\vec{r},t)\cdot\vec{\psi}(\vec{r},t)d\vec{r}.$$

This result can be derived from quantum field theory as well as from Einstein kinematics[105–107]. From viewpoint of practical applications this definition also has the benefit that $|\vec{\psi}(\vec{r},t)|^2$ gives the photodetection rates of photon counting, *i.e.*, the probability density that a photon being registered by a detector at $\vec{r}$, up to a proportionality constant.

Since the photon momentum operator $\hat{p}$ is well defined, there is no problem with defining the momentum-space photon wave function $\vec{\varphi}(\vec{p},t)$, which is the probability amplitude of the photon in the momentum space. Here $|\vec{\varphi}(\vec{p},t)|^2 d\vec{p}(2\pi\hbar)^{-3}$ gives the probability of finding a photon with momentum in the volume $d\vec{p}$ around $\vec{p}$. Then the relation between $\vec{\psi}(\vec{r},t)$ and $\vec{\varphi}(\vec{p},t)$ is[106,107]

$$\vec{\psi}(\vec{r},t)=\int\frac{d\vec{p}\sqrt{cp}}{(2\pi\hbar)^{3/2}}\vec{\varphi}(\vec{p},t)\exp\left[i(\vec{p}\cdot\vec{r}-cpt)/\hbar)\right], \tag{1.22}$$

where $p=|\vec{p}|$. Since there is a factor $\sqrt{cp}$, $\vec{\psi}(\vec{r},t)$ and $\vec{\varphi}(\vec{p},t)$ are not Fourier transform pairs. So in principle, the momentum and position (or more precisely, the 'position where the photon is detected') are not conjugate variables. Fortunately, Eq. 1.22 can be simplified for quasi-monochromatic photons, *i.e.*, the spectral bandwidth of the photon is narrow compared to its central frequency

$$\Delta\omega\ll\bar{\omega} \tag{1.23}$$

Since the magnitude of the momentum of the photon is related to its frequency by

$$p = \frac{\hbar\omega}{c} \tag{1.24}$$

for a narrowband photon, the magnitude of the momentum can be approximated as a contant $\bar{p}$, and the $\sqrt{p}$ term can be moved out of the integration in Eq. 1.22[108]. Then the relation between $\vec{\psi}(\vec{r},t)$ and $\vec{\varphi}(\vec{p},t)$ is a Fourier transform, and in this context the position and momentum can be considered as conjugate variables. For most of the photon states considered in this thesis, interference filters are used to ensure Eq. 1.23 is satisfied. Therefore it is safe to treat the momentum and position of the photons as those of non-relativistic particles.

Similarly, the time (the 'time' at which a photon is registered by a detector) and frequency of a quasi-monochromatic photon can be considered as conjugate variables as well. So in principle the continuous variables of (quasi-monochromatic) single photons can play a similar role to the quadrature amplitudes. Moreover, the phase-space representation now takes a new meaning as a way to represent the wave function of the photon. This parallelism allows one to consider the operations, *e.g.* QIP application, on the continuous variables of individual photons. There have been several demonstrations employing the spatial (position-momentum) or spectral (time-frequency) degree of freedom for the transfer of secure informations, *i.e* quantum cryptography[2,109,110]. QIP with continuous variables of single photons removes the requirement of an ancillary phase reference (local oscillator) for measurement,

and is more robust against loss than quadrature amplitudes [2]. Even without employing a continuum of values, the spatial and spectral properties of individual photons offer additional degrees of freedom for information encoding, which together with the polarization allows the generation of hyperentangled states[111,112]. This state offers several advantages in quantum communcations. For example, it enables 100%-efficient Bell state analysis[112], which is a crucial part of dense coding[20]. It has also been shown that the hyperentangled states allow for quantum key distribution without the need of a shared reference frame[113].

1.5 Outline

In this thesis, we study the spatial correlations of the entangled photon pairs and its applications in quantum communications, especially in QKD. The spatial correlations we mention here and later in the thesis mean the correlations in the spatial degree of freedom, *i.e.* momentum and position. As we mentioned in Sec. 1.4, the study of continuous variables (spatial or spectral) of single photons has kept increasing over last few years. There have been several works on employing this degree of freedom for QKD purposes. Yet most of these works artificially discretize the variables that carry information, therefore not use the full potential of the continuum of values. Moreover, a complete analysis of the security performanc of this scheme is still missing. Here we propose a QKD protocol that utilizes the continuum of

[2] If there is no extra noise, losses will only affect the detection rates of the photons, but cannot change the distribution of the continuous variables of the photon, while the quadrature amplitudes of electromagnetic field will accumulate noise from losses themselves

the spatial degree of freedoms of photons, and experimentally investigate the key elements for the implementation of this protocol. A security analysis taking into account of experimental imperfections of practical systems is also presented. The results lie between the conventional dichotomic and continuous variable QKDs and highlight the differences between these alternative approaches.

This thesis is presented in six chapters, including this introduction. Chapter 2 introduces a scheme of entangled photon pair generation. This scheme is called parametric downconversion (PDC). The properties of the spatial degree of freedom of the PDC state are discussed. To demonstrate the ability of the spatially-entangled PDC state for transfering secure information, chapter 3 shows a Bell inequality violation with such state without resort to spatial filtering. An experimental setup is also proposed. Chapter 4 presents a QKD protocol based on the spatial degree of freedom of the PDC state. The security performance of this protocol is analysed taking into account the experimental imperfections of practical systems. The relation between the key rate and the transmission distance is given. A key element for the implementation of this protocol is a single-photon detector array. Chapter 5 experimentally characterizes a possible candidate of such a detector array, the electron-multiplying charge coupled device (EMCCD), and reveals the capabilities and limits of this device. The conclusions and an outlook of future work are given in chapter 6.

Chapter 2

Parametric Downconversion and its Spatial Properties

2.1 Introduction

Before discussing any applications of the continuous variables of single-photon states, it is necessary to first understand the continuous variables characteristics. This requires the knowledge of the photon generation process. This thesis considers photons generated by means of parametric downconversion (PDC)[114–116]. PDC is a three wave mixing process in which a pump photon (p) incident on a non-centrosymmetric nonlinear optical crystal splits with a small probability into a pair of lower frequency photons, usually called signal (s) and idler (i) (see Fig. 2.1). Since the process is

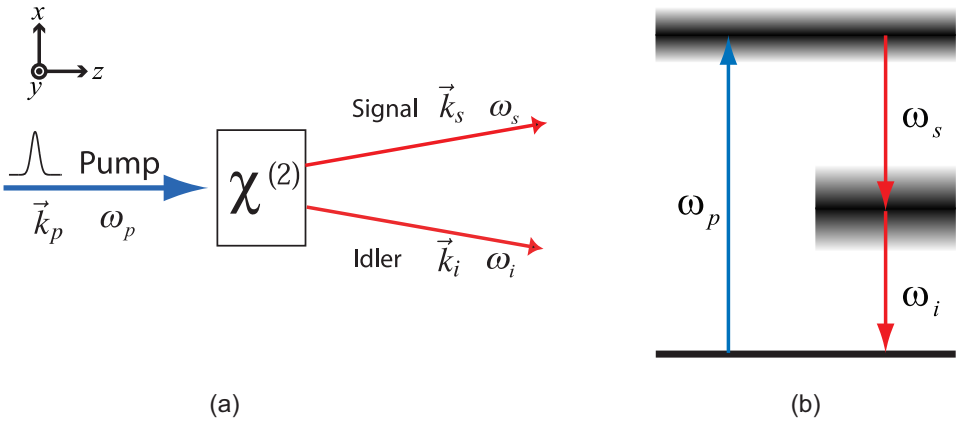


Figure 2.1 (a) Schematic of parametric downconversion. A pump photon is incident on a nonlinear crystal and decays into two photons with less energy, known as signal and ilder photons. (b) The energy diagram of parametric downconversion. The upper gray-scale band represents the pump bandwidth, and the lower gray-scale band represents the spectral spread allowed by the phase matching constraints.

parametric, energy and momentum should be conserved [117]

$$\omega_s + \omega_i = \omega_p, \qquad \mathbf{k}_s + \mathbf{k}_i = \mathbf{k}_p. \tag{2.1}$$

The latter equation is also known as the phase matching condition. The energy conservation and phase matching conditions are not independent due to dispersions of the material.

PDC has a number of merits that are of use in quantum optics. First, the downconverted photons are always emitted in pairs. Hence there is always photon number correlation between the signal and idler beams. Moreover, the emissions are simultaneous within the coherence time of the photons (see later discussion in this chapter). Thus detection of one photon will reveal the generation of its sibling.

This enables PDC to be used as a heralded single-photon source. According to the phase matching condition, the two photons are highly correlated in the spatial and spectral degrees of freedoms, and can also be correlated in the polarizations[58,118]. As shown in this chapter, the spatially-correlated PDC state can approach asympotically the famous EPR state[53]. Therefore the PDC state is a useful prototype for a general bipartite entangled state, which has been widely used in the applications of quantum imaging[119–122], quantum communications[17,123–125], and tests of Bell inequalities[58,126,127].

Usually the polarization dependence of the PDC process and the polarization correlations resulting from it can be divided into two categories called type-I and type-II. In type-I PDC, the signal and ider photons have the same polarization, and are orthogonal to that of the pump. In type-II PDC, one of the downconverted photons has polarization parallel to the pump and the other has polarization orthogonal to it. Recently another type of configuration, type-0 PDC, that pump, signal and idler photons have the same polarization, has been increasingly studied. This kind of configuration allows to access larger nonlinear coefficients, but it usually requires periodically-poled nonlinear crystal to support quasi-phase matching conditions[128].

2.2 Theory of parametric downconversion

The theoretical description of PDC has been studied in several works[116,119,129,130]. This section follows the procedures provided in Ref.[116] to present a derivation of the two-photon PDC state in the perturbative regime, where probability of more

than one photon pairs generated within one pump pulse is negligible. This will be serve as a foundation for the following discussions. The derivation can be applied to either Type-I or Type-II PDC process.

In quantum mechanics, given the initial state at time t_0 is $|\Psi_0\rangle$, then at some later time t, the state is

$$|\Psi(t)\rangle = \exp\left\{\mathcal{T}\left[\frac{1}{i\hbar}\int_{t_0}^{t} dt' \hat{H}_I(t')\right]\right\}|\Psi_0\rangle\,, \tag{2.2}$$

where $\hat{H}_I(t)$ is the interaction Hamiltonian of the system, and $\mathcal{T}$ is the time-ordering operator[131]. For practical PDC setup, the interaction strength is usually small, so the perturbative approximation is applicable

$$|\Psi(t)\rangle \approx \left[1 + \frac{1}{i\hbar}\int_{t_0}^{t} dt' \hat{H}_I(t')\right]|\Psi_0\rangle\,. \tag{2.3}$$

The interaction Hamilotonian for PDC can be written as[116]

$$\hat{H}_I(t) = \frac{1}{2}\int_V d\mathbf{r}\, \hat{\mathbf{E}}(\mathbf{r},t)\cdot\hat{\mathbf{P}}^{(2)}(\mathbf{r},t), \tag{2.4}$$

where the integration volume V is the entire interaction region, $\hat{\mathbf{E}}(\mathbf{r},t)$ is the quantized electric field operator, while $\hat{\mathbf{P}}^{(2)}(\mathbf{r},t)$ is the second-order polarization operator, which can be written as

$$\hat{\mathbf{P}}^{(2)}(\mathbf{r},t) = \chi^{(2)}\hat{\mathbf{E}}(\mathbf{r},t)\hat{\mathbf{E}}(\mathbf{r},t). \tag{2.5}$$

The nonlinear susceptibility $\chi^{(2)}$ is in general a rank 3 tensor. The permutation symmetry of the elements and the symmetry of uniaxial crystals can largely reduce the number of independent elements in $\chi^{(2)}$. For a particular configuration of the PDC setup, it is possible to reduce Eq. 2.5 to a scalar form[132,133]. The electric field in the crystal consists the pump, the signal and the idler

$$\hat{\mathbf{E}}(\mathbf{r},t) = \hat{E}_p(\mathbf{r},t)\mathbf{e}_p + \hat{E}_s(\mathbf{r},t)\mathbf{e}_s + \hat{E}_i(\mathbf{r},t)\mathbf{e}_i. \tag{2.6}$$

where $\mathbf{e}_\mu$ are unit vectors of the pump, signal and idler, respectively. The pump field is usually a strong laser field, and is assumed to propagate undepleted through the crystal. The allows the pump to be treated classically and written as

$$\hat{E}_p(\mathbf{r},t) \rightarrow E_p(\mathbf{r},t) = A_p \int d\mathbf{k}_p\, \alpha(\mathbf{k}_p) \exp\left[i\left(\mathbf{k}_p \cdot \mathbf{r} - \omega_p t\right)\right] + c.c. \tag{2.7}$$

where $\mathbf{k}$ and ω represent the wave vector and frequency respectively, A_p is the pump amplitude and $\alpha(\mathbf{k}_p)$ is the profile of the pump in the momentum space. The field operators of the signal and idler modes can be written as

$$\hat{E}_\mu(\mathbf{r},t) = A_\mu \int d\mathbf{k}_\mu \sqrt{\frac{\omega_\mu}{n_\mu^2(\mathbf{k}_\mu)}}\hat{a}_\mu(\mathbf{k}_\mu) \exp\left[i\left(\mathbf{k}_\mu \cdot \mathbf{r} - \omega_\mu t\right)\right] + c.c. \tag{2.8}$$

where n_μ is the refractive index of the medium, $\hat{a}_\mu$ is the annihilation operator of mode μ ($\mu = s, i$), and A_μ is a constant.

Substituting Eqns. 2.5 - 2.8 into Eq. 2.4, and neglecting all the terms that do

not satisfy the energy conservation condition, the Hamiltonian can be written as

$$\hat{H}_I(t) = A \int d\mathbf{k}_p \int d\mathbf{k}_s \int d\mathbf{k}_i \sqrt{\frac{\omega_s \omega_i}{n_s^2(\mathbf{k}_s) n_i^2(\mathbf{k}_i)}} \alpha(\mathbf{k}_p) \exp\left[-i\Delta\omega t\right] \hat{a}_s^\dagger(\mathbf{k}_s) \hat{a}_i^\dagger(\mathbf{k}_i) \times \int_V dV \exp\left[i\Delta\mathbf{k} \cdot \mathbf{r}\right] \tag{2.9}$$

where $A = A_p A_s A_i \chi^2/2$, $\Delta\omega$ represents the frequency mismatch

$$\Delta\omega = \omega_p - \omega_s - \omega_i, \tag{2.10}$$

and $\Delta\mathbf{k}$ represents the phase mismatch

$$\Delta\mathbf{k} = \mathbf{k}_p - \mathbf{k}_s - \mathbf{k}_i \tag{2.11}$$

Substituting Eq. 2.11 into Eq. 2.2, with the initial state of the signal and idler modes is vacuum state $|\Psi_0\rangle = |\text{vac}\rangle$, the PDC state is

$$|\Psi\rangle = |\text{vac}\rangle + \frac{A}{i\hbar} \int d\mathbf{k}_p \int d\mathbf{k}_s \int d\mathbf{k}_i \sqrt{\frac{\omega_s \omega_i}{n_s^2(\mathbf{k}_s) n_i^2(\mathbf{k}_i)}} \alpha(\mathbf{k}_p) \left\{ \int_{t_0}^{t} dt' \exp\left[-i\Delta\omega t'\right] \right\} \times \left\{ \int_V dV \exp\left[i\Delta\mathbf{k} \cdot \mathbf{r}\right] \right\} \hat{a}_s^\dagger(\mathbf{k}_s) \hat{a}_i^\dagger(\mathbf{k}_i) |\text{vac}\rangle \tag{2.12}$$

The temporal integration in the first curly brackets of Eq. 2.12 is proportional to, negelecting an overall phase factor, $\text{sinc}[\Delta\omega\Delta t/2]$, where $\Delta t = t - t_0$ is the interaction time and

$$\text{sinc}(x) = \frac{\sin x}{x}. \tag{2.13}$$

For PDC pumped with laser pulses, one is usually interested in the state after the pulse has turned off. Thus the sinc function can be approximated in the limit $\Delta t \to \infty$ as a Dirac delta function, $\delta(\Delta\omega)$. To carry out the volume integration over the interaction volume in the second curly brackets, we define the propagation direction of the pump to be the z-axis, and assume the crystal is normal to the pump, so its surface is in the xy-plane (see Fig. 2.1(a)), and the transvere dimension of the crystal is usually larger than the transverss profile of the pump, so the limits of the integrations in x and y direction can be taken to infinity. The integration can then be written as (with overall phase factors neglected)

$$\begin{aligned}\int_V dV \exp\left[i\Delta\mathbf{k}\cdot\mathbf{r}\right] &= \int_{-\infty}^{\infty} dx e^{i\Delta k_x x}\int_{-\infty}^{\infty} dy e^{i\Delta k_y y}\int_0^L dz e^{i\Delta k_z z} \\ &= 8\pi^2 L\delta(\Delta k_x)\delta(\Delta k_y)\mathrm{sinc}\left[\frac{\Delta k_z L}{2}\right] \end{aligned} \tag{2.14}$$

where L is the length of the crystal in the z direction. Depending on the relative position between the pump and the crystal, there might be a phase factor.

The next step involves the integration over the pump wave distribution $\alpha(\vec{k}_p)$. Although this seems to depend only on the pump wave vectors, which is a spatial property, it also implicitly includes the spectral properties of the pump. This arises through the dispersion relation

$$k = \frac{\omega n(\omega)}{c}. \tag{2.15}$$

where $k = |\mathbf{k}| = \sqrt{k_x^2 + k_y^2 + k_z^2}$. So the complete description of the pump field can be done with either the distribution of $\mathbf{k}_p$ (k_{px}, k_{py} and k_{pz}), or the distribution of

$\mathbf{k}_p^\perp$ (k_{px}, k_{py}) and ω_p. For the following calculations it is favorable to use the spectral contribution explicitly. Thus we use the transformation

$$\int d\mathbf{k}_p\, \alpha(\mathbf{k}_p) = \int d\omega_p \int d\mathbf{k}_p^\perp\, v(\mathbf{k}_p^\perp, \omega_p) \tag{2.16}$$

where $\alpha(\omega_p)$ is the spectral profile of the pump, and $v(\mathbf{k}_p^\perp, \omega_p)$ is the transvers momentum amplitude at frequency ω_p.

Substituting Eqns. 2.14 and 2.16 into Eq. 2.12, and noting that the term $\sqrt{\omega_s\omega_i/n_s^2(\mathbf{k}_s)n_i^2(\mathbf{k}_i)}$ varies slowly over the frequencies and wavevectors considered in most situations, and may be approximated as a constant, the PDC state is given by

$$\begin{aligned} |\Psi\rangle = |\mathrm{vac}\rangle + \eta \quad & \int d\omega_s \int d\omega_i \int d\mathbf{k}_s \int d\mathbf{k}_i v(\mathbf{k}_s^\perp + \mathbf{k}_i^\perp, \omega_s + \omega_i) \\ & \times \mathrm{sinc}\left[\tfrac{\Delta k_z L}{2}\right] \hat{a}_s^\dagger(\mathbf{k}_s^\perp, \omega_s)\hat{a}_i^\dagger(\mathbf{k}_i^\perp, \omega_i)\,|\mathrm{vac}\rangle\,. \end{aligned} \tag{2.17}$$

where Δk_z is a function of ω_s, ω_i, $\mathbf{k}_s^\perp$ and $\mathbf{k}_i^\perp$:

$$\begin{aligned} \Delta k_z &= k_p^z - k_s^z - k_i^z \\ &= \sqrt{k_p^2(\omega_s+\omega_i) - |\mathbf{k}_s^\perp + \mathbf{k}_i^\perp|^2} - \sqrt{k_s^2(\omega_s) - |\mathbf{k}_s^\perp|^2} \\ &\quad - \sqrt{k_i^2(\omega_i) - |\mathbf{k}_i^\perp|^2} \end{aligned} \tag{2.18}$$

Eq. 2.17 shows the complex correlation between the spectral and spatial degrees of freedom of PDC states. This makes it very difficult to manipulate both of the degrees

of freedom independently. Usually experiments with PDC resort to filtering to decouple this correlation or even eliminate one degree of freedom. This thesis mainly deals with the spatial properties of the PDC state, so for the current discussion, we restrict our attention to frequencies of the signal and idler $\omega_{s0} = \omega_{i0} = \omega_{p0}/2$, where ω_{p0} is the central frequency of the pump. This eliminates the spectral degree of freedom. Experimentally this situation is achieved by means of interference filters in the signal and idler beams. The required bandwidth of the filters depends on the PDC configuration and the spatial collection aperture[134].

2.3 Spatial distribution of parametric downconversion in momentum domain

In this thesis, the spatial distribution or spatial property of photons is the distribution or property of photons in the spatial degree of freedom, *i.e.* position or momentum. By applying a narrow-band filter to the PDC state in Eq. 2.17, the state can be written as

$$|\Psi\rangle = |\text{vac}\rangle + \lambda \int d\mathbf{k}_s^{\perp} \int d\mathbf{k}_i^{\perp}\, f(\mathbf{k}_s^{\perp}; \mathbf{k}_i^{\perp}) \left|\mathbf{k}_s^{\perp}; \mathbf{k}_i^{\perp}\right\rangle \tag{2.19}$$

with the joint probability amplitude

$$f(\mathbf{k}_s^{\perp}; \mathbf{k}_i^{\perp}) = v(\mathbf{k}_s^{\perp} + \mathbf{k}_i^{\perp}) \text{sinc}\left[\frac{\Delta k_z L}{2}\right] \tag{2.20}$$

where $v(\mathbf{k}_s^\perp + \mathbf{k}_i^\perp)$ originates from the pump envelope and transverse phase-matching function, while $\mathrm{sinc}\,[\Delta k_z L/2]$ is the longitudinal phase-matching function. Here $\left|\mathbf{k}_s^\perp; \mathbf{k}_i^\perp\right\rangle$ is a two-photon state with the signal photon having the transverse momentum $\mathbf{k}_s^\perp$ and the idler photon having transverse momentum $\mathbf{k}_i^\perp$.

2.3.1 Pump envelope

For practical experiment setup, the transverse pump envelope can be approximated by a Gaussian function, so that

$$v(\mathbf{k}_s^\perp + \mathbf{k}_i^\perp) \propto \exp\left(-\frac{w_0^2}{4}\left|\mathbf{k}_s^\perp + \mathbf{k}_i^\perp\right|^2\right) \tag{2.21}$$

where w_0^2 is the beam waist (mininum spot size) of the pump.

2.3.2 Longitudinal phase matching function

For experimental source considered in this thesis, the downconverted modes are usually close to the z-axis (paraxial regime), *i.e.*, $|\mathbf{k}_s^\perp| \ll k_s$ and $|\mathbf{k}_i^\perp| \ll k_i$. Then the expression for Δk_z can be simplified

$$\begin{aligned}\Delta k_z &= \sqrt{k_{p0}^2 - |\mathbf{k}_s^\perp + \mathbf{k}_i^\perp|^2} - \sqrt{k_{s0}^2 - |\mathbf{k}_s^\perp|^2} - \sqrt{k_{i0}^2 - |\mathbf{k}_i^\perp|^2} \\ &\approx k_{p0} - \frac{|\mathbf{k}_s^\perp + \mathbf{k}_i^\perp|^2}{2k_{p0}} - k_{s0} + \frac{|\mathbf{k}_s^\perp|^2}{2k_{s0}} - k_{i0} + \frac{|\mathbf{k}_i^\perp|^2}{2k_{i0}},\end{aligned} \tag{2.22}$$

where $k_{p0} = k_p(\omega_{p0})$, $k_{s0} = k_s(\omega_{s0})$ and $k_{i0} = k_i(\omega_{i0})$. For degenerate type-I PDC, $k_{s0} = k_{i0} = K$, so that Eq. 2.22 can be simplified to give

$$\Delta k_z = \Delta k + \frac{\Delta k}{4k_{p0}K}|\mathbf{k}_s^\perp + \mathbf{k}_i^\perp|^2 + \frac{1}{4K}|\mathbf{k}_s^\perp - \mathbf{k}_i^\perp|^2, \tag{2.23}$$

with $\Delta k = k_{p0} - 2K$.

If the crystal is cut for collinear phase matching, then $\Delta k = 0$. Therefore Δk_z can be simplified further as[135]

$$\Delta k_z = \frac{|\vec{k}_s^\perp - \vec{k}_i^\perp|^2}{4K}. \tag{2.24}$$

Even for type-II PDC, if the collinear phase matching conditions $\Delta k = 0$ are satisfied, and the birefrigence of the crystal is not too big, *i.e.* $|k_{s0} - k_{i0}| \ll k_{s0} + k_{i0}$, one can make the approximation that $k_{s0} \approx k_{i0} \approx k_{p0}/2$. Thus Eq. 2.24 can also be applied to Type-II collinear PDC[135].

For noncollinear phase matching condition $\Delta k \neq 0$, the situation is more complex. In principle all the terms in Eq. 2.23 should be taken into account. But for certain configurations the equation can be simplified. Recall the Gaussian pump envelope function in Eq. 2.21, this indicates that $|\mathbf{k}_s^\perp + \mathbf{k}_i^\perp|$ should be of the same order of magnitude as $1/w_0$, therefore the second term can be evaluated as

$$\frac{\Delta k}{4k_{p0}K}|\mathbf{k}_s^\perp + \mathbf{k}_i^\perp|^2 \quad \approx \quad \frac{1}{4k_{p0}K}\frac{1}{w_0^2}\Delta k. \tag{2.25}$$

When the pump, signal and idler modes are in the optical regime, the wave vectors $k_{p0} = 1/\lambda_{p0}$ and $K = 1/\lambda_{s0}$ (λ is the wavelength) have the magnitudes of μm^{-1}, while unless the pump is strongly focused, the beam waist w_0 considered in this thesis is normally from hundreds of micrometers to several millimeters, so

$$\frac{\Delta k}{4k_{p0}K}|\mathbf{k}_s^\perp + \mathbf{k}_i^\perp|^2 \quad \approx \quad 10^{-6}\Delta k \quad \ll \quad \Delta k, \tag{2.26}$$

the second term of Eq. 2.23 is much smaller than the first term, and can then be ignored. When the pump is focused close to the Rayleigh limit, this approximation may not work any longer. It will be shown in chapter 4 and 5 that keeping the pump as spatially broad as possible has several advantages for the issues discussed in the thesis. So it is safe to remove the second term of Eq. 2.23.

Finally the joint probability amplitude of the two-photon state in the transverse spatial domain can be written as

$$f(\mathbf{k}_s^\perp;\mathbf{k}_i^\perp) = C\exp\left(-\frac{w_0^2}{4}\left|\mathbf{k}_s^\perp + \mathbf{k}_i^\perp\right|^2\right)\text{sinc}\left[\frac{L}{2}\left(\Delta k - \frac{\left|\mathbf{k_s}^\perp - \mathbf{k_i}^\perp\right|^2}{4K}\right)\right]. \tag{2.27}$$

The function $f(\mathbf{k}_s^\perp;\mathbf{k}_i^\perp)$ describes the main features of the correlation of the two-photon state in the momentum domain. The joint probability distribution of $\mathbf{k}_s^\perp$ and $\mathbf{k}_i^\perp$ is given by $P(\mathbf{k}_s^\perp;\mathbf{k}_i^\perp) = |f(\mathbf{k}_s^\perp;\mathbf{k}_i^\perp)|^2$.

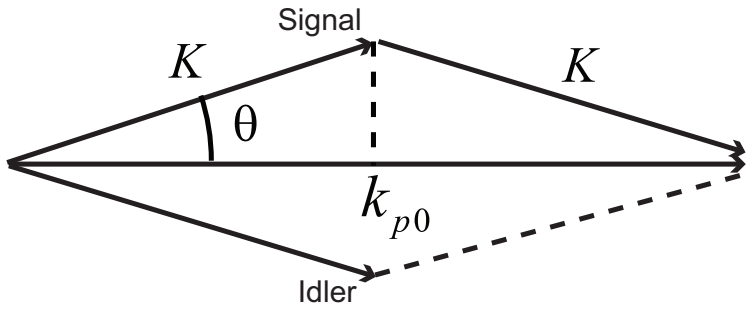


Figure 2.2 Noncollinear phase matching conditions for degenerate type-I PDC.

2.3.3 Marginal distribution

From the joint probability distribution $P(\mathbf{k}_s^\perp;\mathbf{k}_i^\perp)$, it is possible to obtain other quantities of interests. One would be the marginal distribution of the signal and idler modes $\bar{P}(\mathbf{k}_s^\perp)$ and $\bar{P}(\mathbf{k}_i^\perp)$. Due to the symmetry of the degenerate type-I PDC, the marginal distributions should be the same, *i.e.*, $\bar{P}(\mathbf{k}_s^\perp) = \bar{P}(\mathbf{k}_i^\perp)$, and

$$\bar{P}(\mathbf{k}_s^\perp) = \int d\mathbf{k}_i^\perp \; P(\mathbf{k}_s^\perp;\mathbf{k}_i^\perp). \tag{2.28}$$

For the integration, $\mathbf{k}_s^\perp$ can be considered as a parameter, while $\mathbf{k}_i^\perp$ is the argument. The first term in $P(\mathbf{k}_s^\perp;\mathbf{k}_i^\perp)$ (the Gaussian function) has the width of approximately $1/w_0$, while the second term (the sinc function) has the width of roughly $\sqrt{\frac{K}{\Delta k}}\frac{1}{L}$. For a practical PDC setup, both the pump beam waist w_0 and the crystal length L are on the mm - cm scale. As shown in Fig. 2.2

$$\frac{K}{\Delta k} = \frac{K}{2K - k_{p0}} = \frac{K}{2K - 2K\cos\theta} = \frac{1}{1-\cos\theta}. \tag{2.29}$$

In the paraxial regime, the angle between the downconverted modes and the pump, θ, is small. Expanding Eq. 2.29 in θ, we have

$$\sqrt{\frac{K}{\Delta k}} \approx \sqrt{\frac{1}{1-(1-\theta^2/2)}} = \frac{\sqrt{2}}{\theta} \gg 1. \tag{2.30}$$

Therefore it is reasonable to assume

$$\frac{1}{w_0} \ll \sqrt{\frac{K}{\Delta k}} \frac{1}{L}. \tag{2.31}$$

For the integration in Eq. 2.28, the Gaussian function can be approximated as a Dirac delta function $\delta(\mathbf{k_s^\perp} + \mathbf{k_i^\perp})$ (ignoring an overall normalization constant), and the marginal distribution is given by

$$\bar{P}(\mathbf{k}_s^\perp) \propto \left| \mathrm{sinc}\left[\frac{L}{2} \left(\Delta k - \frac{\left|\mathbf{k_s^\perp}\right|^2}{K} \right) \right] \right|^2. \tag{2.32}$$

In principle this equation is sufficient to describe the distribution of each individual mode of the PDC state. To show the characteristics of the modes more clearly, this equation can be simplified further using several approximations. First, the sinc function can be approximated as a Gaussian with the same full width at half maximum (FWHM). This approximation keeps the central peak of the sinc function, ignoring all secondary peaks. This is acceptable for a rough description of the PDC

states. This approximation can be expressed as

$$\mathrm{sinc}\,(x) \approx \exp(-\gamma x^2), \tag{2.33}$$

with $\gamma = .193$.

In this approximation the marginal distribution can be written as

$$\begin{aligned} \bar{P}(\mathbf{k}_s^{\perp}) &\propto \exp\left[-\frac{\gamma L^2}{2}\left(\Delta k - \frac{|\mathbf{k}_\mathbf{s}^{\perp}|^2}{K}\right)^2\right] \\ &\propto \exp\left[-\frac{\gamma L^2}{4K^2}\left(\sqrt{K\Delta k} - |\mathbf{k}_\mathbf{s}^{\perp}|\right)^2\left(\sqrt{K\Delta k} + |\mathbf{k}_\mathbf{s}^{\perp}|\right)^2\right]. \end{aligned} \tag{2.34}$$

According to Eq. 2.34, $\bar{P}(\mathbf{k}_s^{\perp})$ achieves its maximum value at $|\mathbf{k}_\mathbf{s}^{\perp}|_{mp} = \sqrt{K\Delta k}$. In degenerate type-I PDC, the signal and idler modes have the same polarization and wavelength. But for practical applications, it is usually required to distinguish these two modes. The only way is to make them well separated in the spatial domain, *i.e.*, they cannot overlap in space with each other. Mathematically this means $|\mathbf{k}_\mathbf{s}^{\perp}|_{mp} \gg \sqrt{\mathrm{var}\{|\mathbf{k}_{s(i)}^{\perp}|\}}$, where $\mathrm{var}\{|\mathbf{k}_{s(i)}^{\perp}|\}$ is variance of $|\mathbf{k}_{s(i)}^{\perp}|$. So the following approximation can be applied

$$\sqrt{K\Delta k} + |\mathbf{k}_\mathbf{s}^{\perp}| \approx 2\sqrt{K\Delta k}, \tag{2.35}$$

and Eq. 2.34 can be simplified as

$$\bar{P}(\mathbf{k}_s^{\perp}) \propto \exp\left[-\frac{2\gamma L^2 \Delta k}{K}\left(\sqrt{K\Delta k} - |\mathbf{k}_\mathbf{s}^{\perp}|\right)^2\right], \tag{2.36}$$

which is a ring with a radius $\sqrt{K\Delta k}$ and width $\sim \sqrt{\frac{K}{\gamma\Delta k}}\frac{1}{L}$.

Fig. 2.3 compares the experimental measurements of $\bar{P}(\mathbf{k}_s^\perp)$ (left column) and the theoretical predictions from Eq. 2.36 (right column). The experiment measurements were done with a 2-f imaging system and a charge coupled device (CCD) camera. The details of the setup are discussed in chapter 5. This comparison is done for the PDC state generated from a β-barium borate (BBO) crystal with two different lengths $L = 1$ mm (upper row) and $L = 0.5$ mm (lower row). It could be seen that the theoretical fits of the experiment results are better for longer crystals. This is due to the increased variance of $|\mathbf{k}_\mathbf{s}^\perp|$ for $L = 0.5$ mm making the approximation in Eq. 2.35 less accurate.

2.3.4 Conditional distribution

The conditional distribution of the transverse momentum of the PDC state can also be calculated from the joint probability distribution and the marginal distribution

$$P(\mathbf{k}_i^\perp|\mathbf{k}_s^\perp) = \frac{P(\mathbf{k}_s^\perp;\mathbf{k}_i^\perp)}{\bar{P}(\mathbf{k}_s^\perp)} \tag{2.37}$$

With the same approximations applied in Sec. 2.3.3, it can be shown that

$$P(\mathbf{k}_i^\perp|\mathbf{k}_s^\perp) \propto \exp\left(-\frac{w_0^2}{4}\left|\mathbf{k}_s^\perp + \mathbf{k}_i^\perp\right|^2\right), \tag{2.38}$$

which shows the anticorrelation between the signal and idler photon transverse momenta.

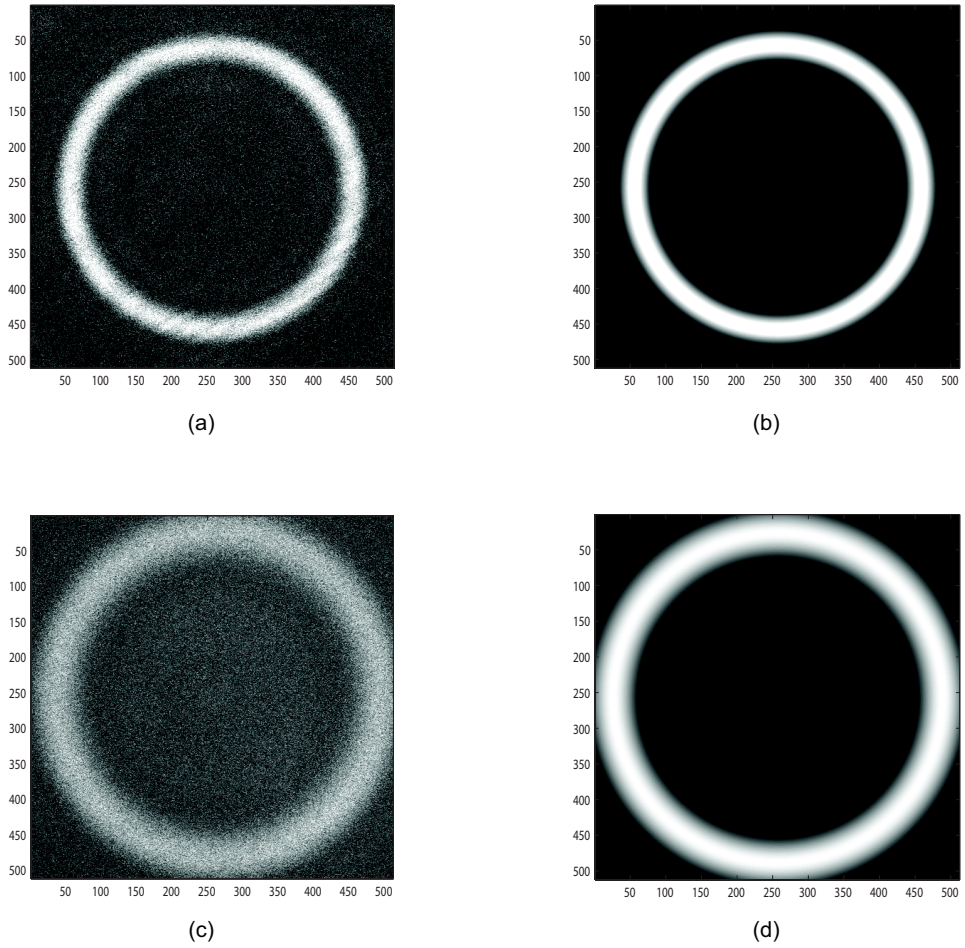


Figure 2.3 Comparision between the experimental measurement and theoretical predictions of $\bar{P}(\mathbf{k}_s^{\perp})$. The axes are the pixel numbers of the CCD camera. Figures on the left are the experiment results, and those on the right are the theoretical results according to Eq. 2.36. For (a) and (b), $L = 1$mm, while for (c) and (d) $L = 0.5$mm. The pump wavelength is 405 nm. The estimated $K = 12.88\ \mu\text{m}^{-1}$ and $\Delta k = 17.27\ \text{mm}^{-1}$.

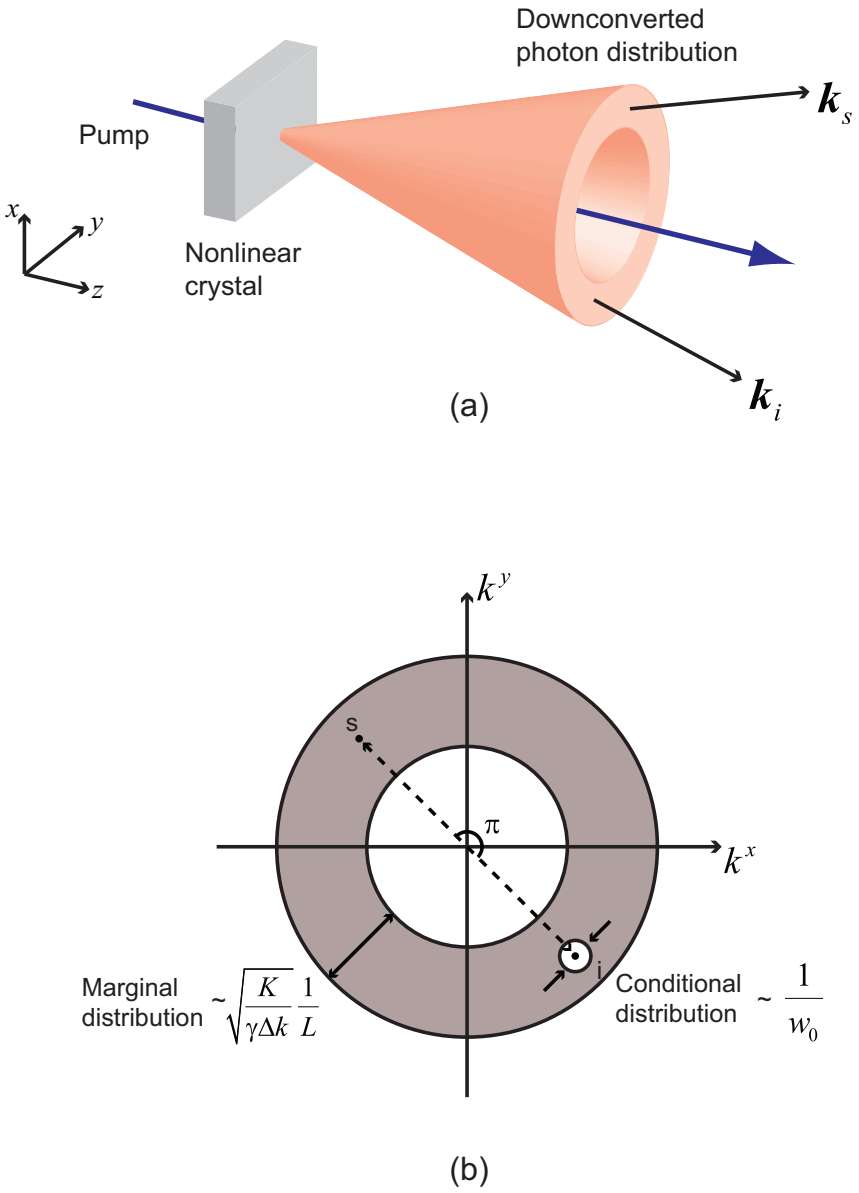


Figure 2.4 Schematic of the degenerate type-I PDC. (a) The 3D figure shows how the downconverted photons are emitted in cones. The cross section is shown in (b). The circular section is the marginal distribution of signal and idler photons, which has a width of $\sqrt{K/\gamma\Delta k}/L$. On the detection of one photon, the conjugate photon will be found within a diametrically opposing area with radius $1/w_0$.

In type-I noncollinear PDC, the photon pairs are emitted in directions defined by two angles, the polar and azimuthal angles, about the pump propagation axis, z. The azimuthal angle is random for each pair, while the polar angle is determined by the phase matching conditions. Thus the downconverted photons are distributed around cones centered on the z axis, and the apertures of the cones are specified by the polar angle. In the degenerate case, the cross sections of the cones are circular and have the same radius for the signal and idler photons (Fig. 2.4(a)), which creates, after the accumulation of a lot of pairs, a ring structure like Fig. 2.3(a) and Fig. 2.3(c). Inside this region, the photon pairs are anticorrelated. If this anticorrelation is perfect, the photons will be found in diametrically opposing points inside the ring. However due to the uncertainty in the transverse momentum, introduced by the finite pump beam spatial distribution (w_0), each photon is located inside the correlation area with radius $1/w_0$. This is summaried in Fig. 2.4(b).

2.4 Distribution of parametric downconversion in position domain

As discussed in Chapter 1, for the spectrally filtered photon pairs, the transverse position can be considered as the conjugate variable of the transverse momentum. Therefore the joint probability amplitude for the transverse positions of the PDC state can be defined as the Fourier transform of the joint momentum probability

amplitude:

$$f(\mathbf{r}_s^\perp;\mathbf{r}_i^\perp)=\mathcal{F}\{f(\mathbf{k}_s^\perp;\mathbf{k}_i^\perp)\}=\int d\mathbf{k}_s^\perp d\mathbf{k}_i^\perp\ f(\mathbf{k}_s^\perp;\mathbf{k}_i^\perp)e^{i(\mathbf{k}_s^\perp\cdot\mathbf{r}_s^\perp+\mathbf{k}_i^\perp\cdot\mathbf{r}_i^\perp)}. \tag{2.39}$$

Substituting Eq. 2.27 into Eq. 2.39, we have

$$f(\mathbf{r}_s^\perp;\mathbf{r}_i^\perp)\propto\tilde{v}(\mathbf{r}_s^\perp+\mathbf{r}_i^\perp)\tilde{\Delta}(\mathbf{r}_s^\perp-\mathbf{r}_i^\perp) \tag{2.40}$$

where

$$\tilde{v}(\mathbf{r}_s^\perp+\mathbf{r}_i^\perp)=\exp\left(-\frac{1}{4w_0}\left|\mathbf{r}_s^\perp+\mathbf{r}_i^\perp\right|^2\right) \tag{2.41}$$

and

$$\tilde{\Delta}(\mathbf{r}_s^\perp-\mathbf{r}_i^\perp)=\int d\mathbf{k}_v\,\mathrm{sinc}\left[\frac{L}{2}\left(\Delta k-\frac{\left|\mathbf{k}_\mathbf{v}^\perp\right|^2}{4K}\right)\right]e^{i\mathbf{k}_v^\perp\cdot\frac{\mathbf{r}_s^\perp-\mathbf{r}_i^\perp}{2}} \tag{2.42}$$

which can only be calculated numerically.

With the approximations in Sec. 2.3.3, it can be shown that $\tilde{v}(\mathbf{r}_s^\perp+\mathbf{r}_i^\perp)$ determines the marginal distribution of the downconverted photons, which has the widths $\sim w_0$. This is easy to understand since the photons can only be generated in the area defined by the width of the pump profile. While $\tilde{\Delta}(\mathbf{r}_s^\perp-\mathbf{r}_i^\perp)$ determines the conditional distribution of the PDC state, which has the width about $L\sqrt{\frac{\Delta k}{K}}$. This could be seen from Fig. 2.5. The downconverted photons generated inside the crystal travel in different directions due to the noncollinear phase matching condition. The maximum separation between the signal and idler photon when they emerge

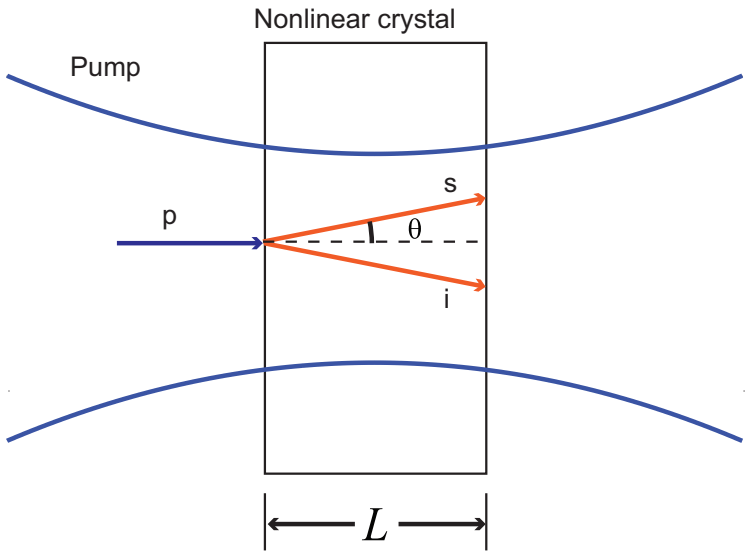


Figure 2.5 Position correlation of PDC. The downconverted photons generated inside the crystal travel in direction separated by 2θ due to the noncollinear phase matching condition. The maximum separation when they emerge from the back surface of the crystal is $2L\theta$.

from the surface of the crystal is

$$|\mathbf{r}_s^{\perp} - \mathbf{r}_i^{\perp}|_{\max} = 2L\tan\theta \approx 2L\theta = \sqrt{2}L\sqrt{\frac{\Delta k}{K}}. \tag{2.43}$$

where Eq. 2.30 is used.

2.5 Entanglement of the PDC state

The Schmidt decomposition has been used to analyse the spatial correlations of a collinear PDC state[35]. It has been shown that this method can also be generalized to quantify the entanglement of noncollinear PDC states with spatial filtering[136]. The Schmidt decomposition can be applied numerically to any bipartite joint prob-

ability amplitude using the method of singular value decomposition (SVD)[137], including the noncollinear PDC state discussed in this section. This thesis will not go into the details of this calculation. With Gaussian approximations, the Schmidt number (see Sec. 1.2.2 for definition) is given by the ratio of the width of the marginal distribution to the width of the conditional distribution, *i.e.*, $\sim \sqrt{\frac{K}{\Delta k}}\frac{w_0}{L}$.

As dicussed in Sec. 1.2.2, there are many ways to characterize entanglement other than by direct quantification, *e.g.*, by use of an entanglement witness. For bipartite continuous variable system, a family of the widely used entanglement witness is[138–141]

$$\Delta^2(|a_s\mathbf{k}_s^\perp + a_i\mathbf{k}_i^\perp|)\Delta^2(|b_s\mathbf{r}_s^\perp + b_i\mathbf{r}_i^\perp|) \leq \frac{(|a_sb_s| + |a_ib_i|)^2}{4}. \tag{2.44}$$

where $\Delta^2(x)$ is the variance of x, $a_{s(i)}$ and $b_{s(i)}$ are real coefficients, $\mathbf{k}_{s(i)}$ and $\mathbf{r}_{s(i)}$ are transverse momenta and positions, respectively.

Due to the expression of the joint probability amplitude of the PDC state in Eq. 2.27, it is convenient to choose $a_s = a_i = b_s = 1$ and $b_i = -1$. The variance product on the left side of Eq. 2.44 can be estimated as

$$\Delta^2(|\mathbf{k}_s^\perp + \mathbf{k}_i^\perp|)\Delta^2(|\mathbf{r}_s^\perp - \mathbf{r}_i^\perp|) \approx \frac{L}{w_0}\sqrt{\frac{\Delta k}{K}}, \tag{2.45}$$

which is, as shown in the previous discussions, much less than unity. This shows the transverse spatial entanglment between the signal and idler photons.

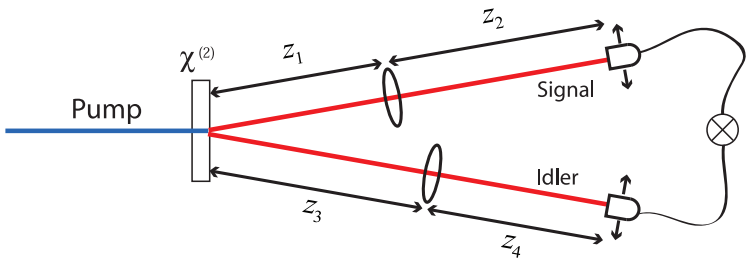


Figure 2.6 The experimental setup to measure the spatial correlations of the PDC state. Different imaging systems are used for measuring different variables (momentum or position). By measuring the coincidence rate of the two single-photon detectors, we can estimate the joint distribution of the PDC state in different domain.

2.6 Experimental setup to measure the spatial correlations of the PDC state

To measure the spatial correlations (joint probability) of the PDC state, imaging systems as shown in Fig. 2.6 should be used. Assume the focal length of the imaging lens (we assume same lenses are used in the two arms) is f, then to measure the momentum correlation of the photon pair, we should have

$$z_2 = z_4 = f. \tag{2.46}$$

Usually, though not necessarily, one also choose $z_1 = z_3 = f$ to remove the additional phase factor. This imaging system is known as 2-f imaging system. Two single-photon detectors are used to scan the distribution of each photon. By measuring the coincidence rate the detectors, we can estimate the joint distribution of the photon pair.

To measure the position correlation of the photon pair, we should have

$$\frac{1}{z_1} + \frac{1}{z_2} = \frac{1}{f}, \tag{2.47}$$

$$\frac{1}{z_3} + \frac{1}{z_4} = \frac{1}{f}. \tag{2.48}$$

As a special example, we can choose $z_1 = z_2 = z_3 = z_4 = 2f$, which is called the 4-$f$ imaging system.

Fig. 2.6 is only the simplest setup for measuring the correlations of photon pairs in the spatial degree of freedom. In implementations with long distance links, more complicated optical systems should be used to reduce the spread of the beam. Moreover, different imaging systems may be used on each arm to measure different variables.

2.7 Engineering the PDC state for quantum information processing

A useful feature to produce photon pairs via parametric downconversion (PDC) is that it offers well-developed techniques to modify the modal structure of the downconverted photons. With the combination of a variety of lasers (with different spectrum, spatial mode, *etc.*) and nonlinear crystals, the photons can be tailored in numerous ways. Most importantly, the correlations of the spatio-temporal degrees of freedom can be modified. Many quantum communication applications, including the quantum cryptography scheme discussed in thesis, require the highly correlated

PDC state. Therefore in this thesis we mainly study the generation and application of this kind of state. There are other quantum information processing applications that will benifit from the spatio-temporally factorable PDC state, which is studied in Appendix A.

Chapter 3

Violation of a Bell Inequality Based on the Spatial Wigner Function

As mentioned in Sec. 1.2.3, the Bell inequality provides a measure of the nonclassicality of a composite quantum system, by testing whether a local realistic model can describe the results of joint measurements on the system. Moreover, the Bell inequality provides a way to verify entanglement. Of special interest for the issues discussed in this thesis is the fact that the Bell inequality plays an important role in the security of quantum key distribution protocols[77,142,143]. In particular, it has been proved that the correlations shared by Alice and Bob must violate a generalized Bell inequality, known as CHSH inequality[55], otherwise Alice and Bob's measurement results could be produced by the quantum measurements on the seperable

state of larger dimensions, which cannot be used for secure key generation[79].

In this section, we show that the spatial correlations of the PDC state can be used to violate a CHSH inequality. Although this is not part of the QKD protocol proposed in Chapter 4, it confirms the potential for the spatial correlations of the PDC state to be used in the secure distribution of information.

3.1 CHSH inequality and experimental loopholes

The original Bell theorem assumed perfect correlations between two different subsystems[54]. This situaiton is difficult to achieve in realistic experiments due to practical imperfections. Clauser, Horne, Shimony and Holt refined Bell's work and derived an equation that is applicable to real experiments[55]. Their result, known as the CHSH inequality, is formualted in the following way: consider a bipartite system with spacelike separated subsystems labelled as A and B. We denote $\mathbf{a}$ and $\mathbf{b}$ as the local measurement settings on each subsystem, with α and β being the measurement results each with only two possible values ± 1. The joint probability of α and β for measurement settings $\mathbf{a}$ and $\mathbf{b}$ is denoted by $P(\alpha, \beta|\mathbf{a}, \mathbf{b})$. We define the correlation function

$$E(\mathbf{a}, \mathbf{b}) = \sum_{\alpha,\beta} \alpha\beta \, P(\alpha, \beta|\mathbf{a}, \mathbf{b}). \tag{3.1}$$

which describes correlations between subsystems A and B. Then for a local realistic hidden variable model $P(\alpha, \beta|\mathbf{a}, \mathbf{b})$ should be able to be written in the form of Eq.

1.18, and the measurement results must satisfy

$$|E(\mathbf{a}_1, \mathbf{b}_1) + E(\mathbf{a}_1, \mathbf{b}_2) + E(\mathbf{a}_2, \mathbf{b}_1) - E(\mathbf{a}_2, \mathbf{b}_2)| \leq 2. \tag{3.2}$$

This inequality gives a bound on any local realistic hidden variable model. It is shown that quantum mechanics allows the combination on the left side of Eq. 3.2 to achieve a maximum value of $2\sqrt{2}$[144].

Since the publication of CHSH inequality, there have been numerous experimental demonstrations violating this type of inequalities (see, for example, Refs[56–58]), supporting the predictions of quantum theory. However there are two major experimental loopholes which make the experiment results less convincing[145].

The first loophole is called the locality loophole[146]. An ideal experimental test for a Bell inequality should prohibit communications between the two different measurement apparatus to speeds less than or equal the speed of light, *i.e.*, the measurement apparatus must be space-like separated. This requires the spatial separation between the measurement apparatus to be sufficiently large and switching of measurement settings to be fast, *i.e.*, the switching time of the measurement settings is smaller than the flight time of the detected particles so that the choice of the measurement settings are made during the flight of particles (see Fig.3.1). There have been many experimental efforts to close this loophole[146]. Finally the experiment reported in Ref[60] achieved this goal by detecting correlations of photon pairs generated by type-II PDC with polarizers separated by a distance of over 400

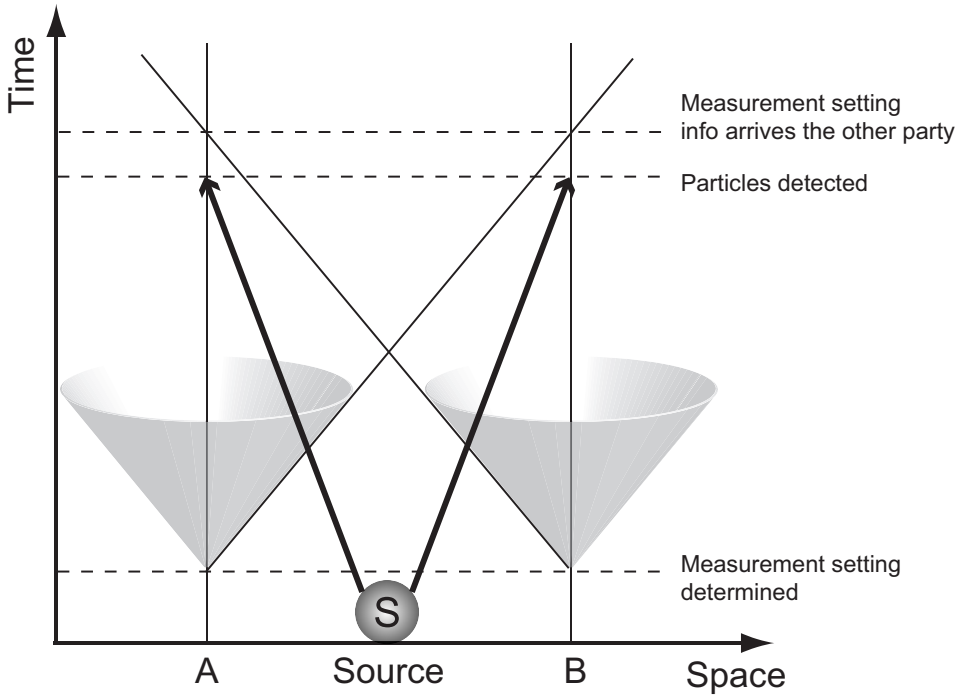


Figure 3.1 A schemetic describes the locality loophole in the experimental test of Bell inequality. The gray cone shows the spread of the information on the measurement settings of each party. This information must arrive the other party after the detection of the particle to ensure the localilty loophole closed.

m.

The other main loophole is known as the detection loophole. This impediment arises from the non-unit efficiency of the signal detection. In most experiments only a small fraction of the quantum objects are detected due to low detection efficiency, making a supplementary assumption necessary. This assumption is that the detected quantum objects are good candidates of the whole ensemble, that is, they faithfully represents the ensemble. In defense of local realism, one can argue that correlations that violate the Bell inequality are only possessed by the particles detected in pairs,

and all the others are rejected. It was proven that unless the detection efficiency exceeds a certain threshold of 83%[147], the violation of a Bell inequality does not necessarily imply a contradiction with a local realistic description of the data[147–149]. There have been several efforts to improve detection efficiency in experiments with entangled photon pairs[150,151]. However this turns out to be very difficult, not only due to the efficiency of single-photon detectors, but also due to the large emission angle of photons from PDC which makes high collection efficiency difficult to achieve. Another option is to perform measurements on correlated, more localized, massive particles, for example, atoms, ions *etc.* Ref[152] reported an experiment to measure the correlations between two trapped ions with near perfect efficiency, closing the detection loophole. Although the two major loopholes have been closed in different experiments, there is still no single experiment that closes both of the loopholes simulataneously.

As mentioned above, for the experiment with photon pairs, due to the detection efficiency, the violation of a Bell inequality is usually not a decisive disproof of local realism, but rather a signature of entanglement between the measured photons.

3.2 Violation of a Bell inequality with the spatial correlations of PDC

The original Bell inequality (and the CHSH inequality as well) relies on dichotomic outcomes of measurements made on each subsystem. Although there have been

discussions on the generalization of Bell inequalities to N-value observables with $N \geq 3$ [123,153], as N increases the number of detectors increases as well, which makes it challenging for experimental realizations. In this chapter we restrict our attention to Bell inequalities based on dichotomous observables. Therefore it is necessary to identify a way in which a given state may yield only two possible results for a specified measurement.

The first Bell inequality violation was shown with a singlet state of two spin-1/2 particles [54], which differs from the original EPR state. Since then, the question of whether it is possible to violate a Bell inequality using the original, continuous-variable entangled EPR state [53] with the wave function

$$\psi(p_1, p_2) = \int_{-\infty}^{\infty} e^{(2\pi i/h)(p_1+p_2)x} dx \tag{3.3}$$

has arisen. Here p_1 and p_2 are the momenta of the two particles. The actual form of the state in Ref [53] was defined in terms of the particle positions, which is the Fourier transform of Eq. 3.3). Although this state has some mathematical problems due to its singularity, since the joint distribution amplitude is a delta function and is not square integrable, it can be regarded as the limit of an appropriate class of smooth normalizable states [1] to overcome this difficulty. In particular, the EPR state is the limit of the collinear phase-matched PDC state shown in Sec. 2.3 (for

simplicity, we only consider the 1D distribution)

$$\begin{aligned} f(k_s^{\perp};k_i^{\perp}) &= C\exp\left[-\frac{w_0^2}{4}\left(k_s^{\perp}+k_i^{\perp}\right)^2\right]\operatorname{sinc}\left[\frac{L}{8K}\left(k_s^{\perp}-k_i^{\perp}\right)^2\right] \\ &= C\exp\left[-\frac{\left(k_s^{\perp}+k_i^{\perp}\right)^2}{\sigma_+^2}\right]\operatorname{sinc}\left[\frac{\left(k_s^{\perp}-k_i^{\perp}\right)^2}{\sigma_-^2}\right] \end{aligned} \tag{3.4}$$

When $w_0 \to \infty$ and $L \to 0$ this amplitude approaches that of an ideal EPR state in $k_s^{\perp}$ and $k_i^{\perp}$. Although John Bell argued that the original EPR state, and its Gaussian approximations, are consistent with a local realistic description due to the positivity of their joint Wigner functions (see the following discussions for the definition) [154], it has been shown that the positivity or negativity of the Wigner function has a very weak relation to the locality problem [155]. Since an arbitrary system can be separated into dichotomous observables, the realistic states that approach the EPR state *can* be used to demonstrate violations of Bell-inequalities. An easier approach is to operate on only one two-dimensional subspace of the continuous space, and discard the photons that do not fall into it. For example, Cohen [1] shows that a Bell state can be produced by selecting two pairs of correlated space-time modes from the continuum occupied by each EPR particle. This allows the momentum-entangled photons to be treated exactly like polarization-entangled photons. However, this procedure works by throwing away nearly all the amplitude of the EPR state, creating a spin-like state by projecting onto a dichotomic subspace of the original, continuous Hilbert space. This idea was, in fact, the basis for a practical realization by Tapster and Rarity of Bell inequality violations using frequency and momentum entanglement

of photon pairs[126]. In these experiments, pinholes were used to select just two pairs of correlated modes, thus discarding most of the correlated particles produced by the quantum source (PDC). This severely limits the signal-to-noise ratio of the experiments, and suffers from the detection loophole as well.

Therefore it would be a significant achievement to demonstrate that a Bell inequality is violated with continuous degrees of freedom, without discarding any of the photons used to provide the information. For the issues discussed in this thesis this is of particular importance since we aim to employ the continuum of the spatial correlations without spatial filtering or projecting onto a discrete subspace of the PDC state for quantum key distribution. Interestingly, it turns out that a Bell inequality violation can be achieved by measuring the joint Wigner function of the PDC state and applying the method suggested in Ref[155].

3.2.1 Wigner function and spatial parity

As mentioned in Sec. 1.1, the Wigner function[156] is a phase-space representation of contiunuous variable quantum states, and is usually considered as a quasi-probability distribution. For a pure single-particle state

$$|\Psi\rangle = \int dk\, f(k)|k\rangle \tag{3.5}$$

with a momentum-space wave function $f(k)$, the Wigner function is defined as

$$\begin{aligned} W(x,k) &= \int dk'\, f^*\left(k+k'\right) f\left(k-k'\right) e^{i2k'x} \\ &= \frac{1}{2\pi}\int dx'\, \tilde{f}^*\left(x+x'\right) \tilde{f}\left(x-x'\right) e^{-i2kx'} \end{aligned} \tag{3.6}$$

where $\tilde{f}(x)$, the Fourier transform of $f(k)$, is the coordinate-space wave function. Wigner function has many convenient properties. For example, its integration over one variable gives the probability distribution of the other variable. The Wigner function can be considered as the expectation value of a displaced parity operator[157]. To see, we follow the analysis in Ref[157] and rewrite the Wigner function in a more quantum-mechanical way

$$W(x,k) = \langle\Psi|\hat{\Pi}_{x,k}|\Psi\rangle \tag{3.7}$$

where

$$\begin{aligned} \hat{\Pi}_{x,k} &= \int dk'\, e^{i2k'x}|k+k'\rangle\langle k-k'| \\ &= \int dx'\, e^{-i2kx'}|x+x'\rangle\langle x-x'|. \end{aligned} \tag{3.8}$$

From Eq. 3.7 it is obvious that $W(x,k)$ is the expectation value of the displaced parity operator $\hat{\Pi}_{x,k}$. It is easy to check that

$$\left(\hat{\Pi}_{x,k}\right)^2 = \hat{I} \tag{3.9}$$

where $\hat{I}$ is the identity operator. Therefore $\hat{\Pi}_{x,k}$ has two eigenvalues ± 1, *i.e.*, each measurement of $\hat{\Pi}_{x,k}$ will yield either 1 or -1, although the eigenstates of $\hat{\Pi}_{x,k}$ are highly degenerate. So the Wigner function is the expectation value of a measurement with dichotomic outcomes, which is similar to the measurement of polarization or particle spin. Thus we can construct a CHSH inequality using this measurement operator.

Before we move on to the Bell inequality violation, it is worthwhile to examine the operator $\hat{\Pi}_{x,k}$ more closely. It is shown in Ref[157] that $\hat{\Pi}_{x,k}$ is a diplaced parity operator

$$\hat{\Pi}_{x,k} = \hat{D}(x,k)\hat{\Pi}\hat{D}^{\dagger}(x,k) \tag{3.10}$$

where

$$\begin{aligned} \hat{\Pi} = \hat{\Pi}_{0,0} &= \int dk' |k'\rangle\langle -k'| \\ &= \int dx' |x'\rangle\langle -x'| \end{aligned} \tag{3.11}$$

is the parity operator about the origin: it changes $f(k)$ to $f(-k)$ and $\tilde{f}(x)$ to $\tilde{f}(-x)$, and $\hat{D}(x,k)$ is the phase-space displacement operator, which shifts the position and momentum operator by x and k respectively. It can be shown that $\hat{\Pi}_{x,k}$ changes $x'-x$ to $x-x'$ and $k'-k$ to $k-k'$ when applied to a wave function $f(k')$. Therefore $\hat{\Pi}_{x,k}$ reflects the state around the point (x,k) and is the the parity operator around

that point[157]. This can also be seen by rewriting the Wigner function in the form

$$W(x,k) = \frac{1}{2\pi}\int dx' \left[e^{ikx'} f(x+x')\right]\left[e^{-ikx'} f(x-x')\right]^*. \tag{3.12}$$

The term in the first square brackets, $f_{x,k}(x') = e^{ikx'} f(x+x')$, is the wave function $f(x')$ shifted by (x,k) in phase space, $e^{-ikx'} f(x-x')$ is acquired by applying the transformation $x' \to -x'$ on $f_{x,k}(x')$. Therefore the Wigner function measures the overlap of $f(x')$ with its mirror image around (x,k), or how much $f(x')$ is centered on (x,k). This also suggests a way to experimentally measure the spatial Wigner function[158,159].

Until now we have discussed the Wigner function of a single-particle state. For a bipartite state

$$|\Psi\rangle = \int dk_a \int dk_b\, f(k_a,k_b)|k_a,k_b\rangle \tag{3.13}$$

a joint Wigner function can be defined in a similar way

$$\begin{aligned} W(x_a,k_a;x_b,k_b) &= \int dk'_a \int dk'_b\, f^*\left(k_a+k'_a,k_b+k'_b\right) f\left(k_a-k'_a,k_b-k'_b\right) \\ &\quad \times e^{i2(k'_a x_a + k'_b x_b)} \\ &= \langle\Psi|\hat{\Pi}_{x_a,k_a}\hat{\Pi}_{x_b,k_b}|\Psi\rangle. \end{aligned} \tag{3.14}$$

From Eq. 3.14, it can be seen that $W(x_a,k_a;x_b,k_b)$ is the correlation function of $\hat{\Pi}_{x_a,k_a}$ and $\hat{\Pi}_{x_b,k_b}$, which is exactly the same as that defined by Eq. 3.1, with (x_a,k_a) and (x_b,k_b) taking the place of the local measurement settings **a** and **b** respectively.

Thus a CHSH inequality with the form in Eq. 3.2 can be easily constructed with different pairs of (x_a, k_a) and (x_b, k_b).

3.2.2 A CHSH inequality with the Wigner function of PDC state

For the joint two-photon transverse spatial state from PDC we can construct a CHSH inequality following Eq. 3.2 and discussions in Sec. 3.2.1

$$|W(x_{a1}, k_{a1}; x_{b1}, k_{b1}) + W(x_{a1}, k_{a1}; x_{b2}, k_{b2}) + W(x_{a2}, k_{a2}; x_{b1}, k_{b1}) \\ -W(x_{a2}, k_{a2}; x_{b2}, k_{b2})| \leq 2. \tag{3.15}$$

Then the problem is to find proper settings (x_{a1}, k_{a1}), (x_{a2}, k_{a2}), (x_{b1}, k_{b1}) and (x_{b2}, k_{b2}) that will allow a given state to violate this inequality. Here we first consider the combinations that are suggested in Ref.[155]: $k_{a1} = k_{a2} = k_{b1} = k_{b2} = 0$, $x_{a1} = x_{b1} = 0$, $x_{a2} = \sqrt{J}$ and $x_{b2} = -\sqrt{J}$. It is unclear whether this is the optimal selection in the sense that whether it allows the maximal violation of Eq. 3.15, but we will show that this is adequate for the PDC state.

It is straightforward to calculate the Wigner function of the PDC state with Eqns. 3.4 and 3.14. However due to the sinc function in the PDC wave function, it is not possible to give an analytical expression for the Wigner function, and we need to resort to numerical calculations. It is always useful tohave an analytical expression, even with approximations, since it can give insight to the mechanisms

at work. Therefore we start with a Gaussian state with the wave function

$$f(k_a, k_b) = \frac{2}{\sqrt{\pi\sigma_+\sigma_-}} \exp\left[-\frac{(k_a+k_b)^2}{\sigma_+^2}\right] \exp\left[-\frac{(k_a-k_b)^2}{\sigma_-^2}\right]. \tag{3.16}$$

Note this state is not the Gaussian approximation of the collinear PDC state in Eq. 3.4, since the Gaussian approximation of $\mathrm{sinc}(x^2)$ is $\exp(\gamma x^4)$. However it has several characteristics similar to the PDC state, *e.g.*, the Schmidt numbers (Eq. 1.8) for this state and the PDC state vary in a similar way when the same parameters are used, and both achieve the minimum Schmidt number at $\sigma_+/\sigma_- = 1$.

The Wigner function of the Gaussian state in Eq. 3.16 is given by

$$\begin{aligned} W(x_a, k_a; x_b, k_b) &= \exp\left[-\frac{\sigma_+^2(x_a+x_b)^2}{8}\right] \exp\left[-\frac{\sigma_-^2(x_a-x_b)^2}{8}\right] \\ &\quad \times \exp\left[-\frac{2(k_a+k_b)^2}{\sigma_+^2}\right] \exp\left[-\frac{2(k_a-k_b)^2}{\sigma_-^2}\right]. \end{aligned} \tag{3.17}$$

The combination for testing the CHSH inequality is

$$\begin{aligned} \mathcal{B} &= W(0,0;0,0)+W(\sqrt{J},0;0,0)+W(0,0;-\sqrt{J},0)-W(\sqrt{J},0;-\sqrt{J},0) && (3.18) \\ &= 1 + 2\exp\left[-\frac{\sigma_+^2+\sigma_-^2}{8}J\right] - \exp\left[-\frac{\sigma_-^2}{2}J\right] && (3.19) \end{aligned}$$

We define the ratio of the Gaussian widths

$$r = \frac{\sigma_-}{\sigma_+}. \tag{3.20}$$

When σ_+ goes to infinity (r goes to 0), we have spatially anti-correlated photons ($k_a = -k_b$), while for σ_- going to infinity (r goes to infinity), we have spatially correlated photons ($k_a = k_b$).

With Eq. 3.20, the combination in Eq. 3.19 can be rewritten as

$$\mathcal{B} = 1 + 2\exp\left[-\frac{1+r^2}{8}\sigma_+^2 J\right] - \exp\left[-\frac{r^2}{2}\sigma_+^2 J\right]. \tag{3.21}$$

Thus the maximum value of $\mathcal{B}$ is not determined by the specific values of σ_+ and σ_-, but rather by their ratio r. This is similar to the Schmidt number analysis of the state[35]. The corresponding shift in position $\sqrt{J}_{\max}$ is inversely proportional to σ_+. This offers some convenience in the proposed experiment. As will be shown in Sec. 3.2.3, $\sqrt{J}$ is achieved by moving the position of a mirror which has a finite resolution. Therefore it is convenient to make σ_+ small and keep r a constant such that $\sqrt{J}_{\max}$ is large enough to tolerate errors due to the experimental precision.

Fig. 3.2(a) shows the calculated $\mathcal{B}$ as a function of r and $\sigma_+^2 J$. It can be seen that for certain values of r and J, $\mathcal{B}$ exceeds the classical limit 2. Since $\mathcal{B} \geq 0$, the extremum (maximum or minimum) value of $|\mathcal{B}|$ is the extremum of $\mathcal{B}$, which can be found by solving the condition

$$\frac{\partial \mathcal{B}}{\partial J} = 0 \tag{3.22}$$

Thus we have the extremum is achieved at

$$J_m = \frac{1}{\sigma_+}\frac{8}{3r^2-1}\log\left(\frac{2r^2}{1+r^2}\right). \tag{3.23}$$

A more careful examination shows that where $r \leq 1$, $\mathcal{B}$ achieves its minimum value at J_m, and its maximum is 2, while for $r > 1$, $\mathcal{B}$ achieves its maximum at J_m. Therefore we have

$$\mathcal{B}_{\max} = \begin{cases} 2 & \text{when } r \leq 1 \\ 1 + 2\left(\frac{2r^2}{1+r^2}\right)^{-\frac{1+r^2}{3r^2-1}} - \left(\frac{2r^2}{1+r^2}\right)^{-\frac{4r^2}{3r^2-1}} & \text{when } r > 1 \end{cases} \tag{3.24}$$

Fig. 3.2(b) shows $\mathcal{B}_{\max}$ as a function of r. It can be seen that when $r > 1$, the violation of a CHSH inequality can be achieved. Note that when $r \to \infty$, the Gaussian state in Eq. 3.16 approaches the EPR state (Eq. 3.3), and $\mathcal{B}_{\max}$ achieves its maximum value of 2.19. This shows that the EPR state *can* demonstrate some nonlocality. This is exactly the same result in Ref[155], althought we use a slightly different state for our analysis. A interesting point about this result is that although the amount of the entanglement contained in the state can be made arbitrarily large by letting $r \to \infty$, $\mathcal{B}$ can never exceed Tsirelson's bound $2\sqrt{2}$[144]. This shows that entanglement does not exhaust the full potential of nonlocality[28].

An interesting point of Fig. 3.2 is that the CHSH inequality is only violated when $r > 1$. It has been shown that when $r \ll 1$, the state also exhibits a significant amount of entanglement[35], but it cannot be used to violate the CHSH inequality in combination with Eq. 3.19. This confirms that a specific Bell inequality is an entanglement witness, *i.e.*, not every entangled stated can violate a given Bell inequality.

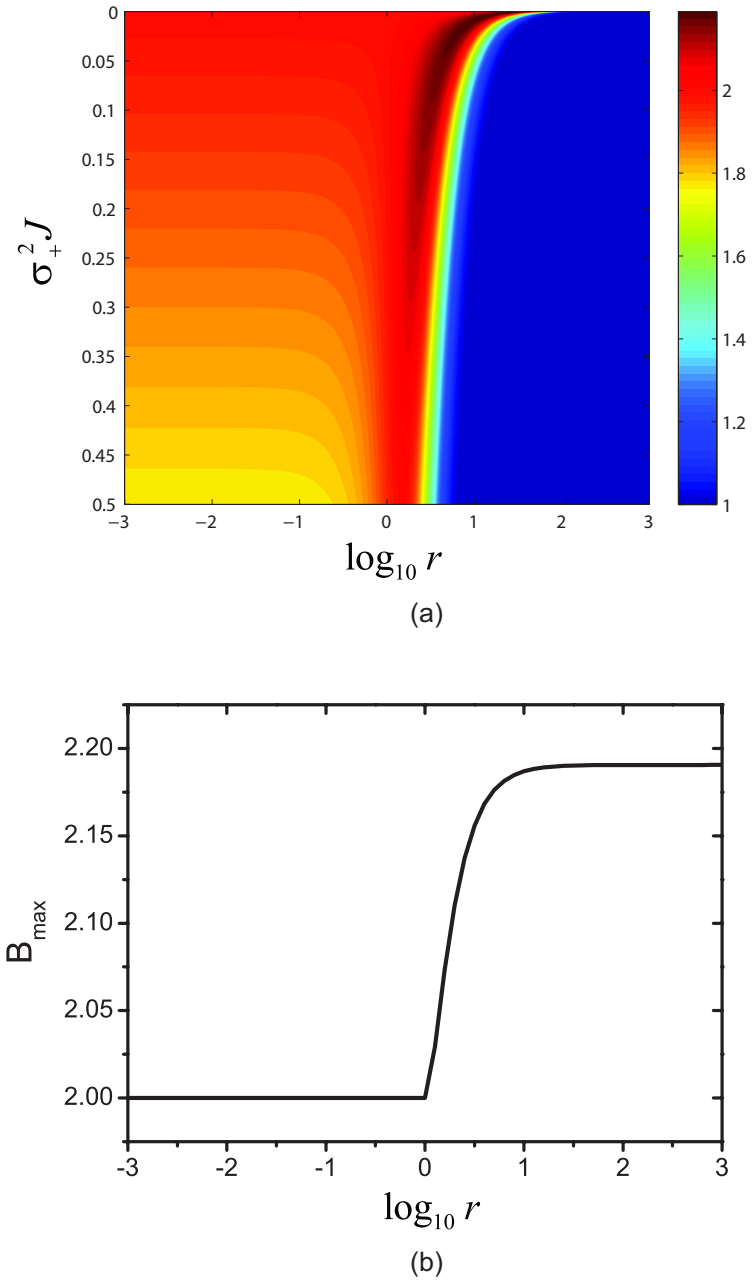


Figure 3.2 (a) $\mathcal{B}$ defined in Eq. 3.19 versus r and J. When $\mathcal{B}$ exceeds 2, the violation of a CHSH inequality can be achieved. (b) The maximum value of $\mathcal{B}$ versus r. When $r \to \infty$, $\mathcal{B}_{\max}$ approaches its limit 2.19.

In fact, we can construct another combination

$$\mathcal{B} = W(0,0;0,0) + W(0,\sqrt{J};0,0) + W(0,0;0,-\sqrt{J}) - W(0,\sqrt{J};0,-\sqrt{J}) \quad (3.25)$$

which means instead of applying shift in position of the particle wave function, we apply the shift in momentum. A similar analysis implies that the combination in Eq. 3.25 can be used to violate the CHSH inequality if and only if when $r < 1$, and achieves the maximum value 2.19 when $r \to 0$. Therefore the combinations for violating a Bell inequality should be carefully selected according the state used in the setup.

Now we calculate $\mathcal{B}$ for a realistic PDC source. We consider the degenerate collinear type-II PDC photon pairs generated by pumping a $L = 3$ mm thick β-barium borate (BBO) crystal with a monochromatic pump at 400nm with beam waist $w_0 = 2$ mm. The estimated wave vector of the downconverted photon is $K = 12.9\ \mu\text{m}^{-1}$. Then the ratio between σ_- and σ_+ in Eq. 3.4 is

$$r = \frac{\sigma_-}{\sigma_+} = w_0\sqrt{\frac{2K}{L}} = 185 \gg 1. \quad (3.26)$$

The value of r is proportional to $(L_{\text{dif}}/L)^{1/2}$, where L_{dif} is the diffraction length of the pump beam. The result of Eq. 3.26 is the normal situation unless the pump beam is strongly focused. Therefore we choose $\mathcal{B}$ of the form in Eq. 3.18. As mentioned previously, this calculations is done numerically with the two-photon wave function shown in Eq. 3.4. We should indicate that in contrast to the Gaussian correlated

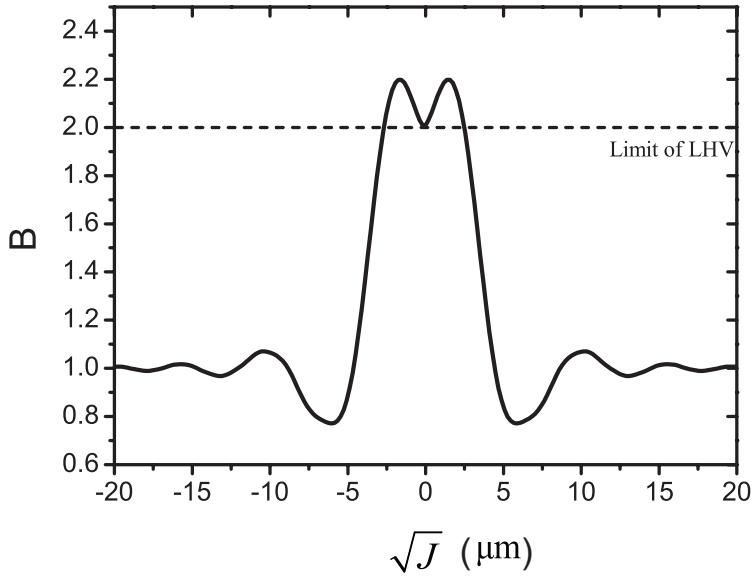


Figure 3.3 The numerically calculated $\mathcal{B}$ versus $\sqrt{J}$ for a practical PDC source. It can be seen that with a proper shift $\sqrt{J}$ (1.76 μm), a CHSH inequality is violated.

state, the Wigner function of the PDC state has negative values at some points due to the sinc function. The numerically calculated $\mathcal{B}$ versus $\sqrt{J}$ is shown in Fig. 3.3. At $\sqrt{J} = 1.76$ μm, $\mathcal{B}$ reaches its maximum value 2.2, a clear violation of the CHSH inequality. This number is also slight larger than the limit of the Gaussian states, 2.19, indicating a stronger violation.

Therefore it is possible to violate the Bell inequality using the correlations of continuous spatial variables of a realistic PDC source. Rather than manipulating the input state using a projection in order to obtain a Bell state, we construct a dichotomic observable that is non-zero for any biphoton state. Although the idea is similar to the CHSH inequality violations with the entanglement in field quadratures suggested in Ref[155,160], the use of the spatial degree of freedom of the

entangled photon pairs overcomes one of the main obstacles of the entanglement in field quadratures: the degradation of quantum correlations due to inevitable optical losses and inefficiencies in real systems. Experiments using photon pairs are not hampered by losses, since the photon number is decoupled from the observed correlated variables such that viable results can be postselected.

3.2.3 The proposed experiment setup

Another advantage of using the spatial Wigner function of photons is that it can be measured directly using Sagnac interferometers[158,159]. Recall the Wigner function expression in Eq. 3.12, the Wigner function $W(x,k)$ is the overlap of the wave function $f(x')$ with its mirror around (x,k), which can be acquired by a spatial integration of the overlap between $e^{ikx'}f(x+x')$ and a complex conjugate of its replica rotated by 180°. For the electromagnetic field, or photons, translation of the transverse spatial state $f(x')$ by x, giving $f(x+x')$, can be realized by displacement of $f(x')$ in space by x, and the added transverse phase factor $e^{ikx'}$ can be achieved by changing the transverse propagation direction by k. Thus the transverse spatial Wigner function of a single photon $W(x,k)$ can be measured by the Sagnac interferometer depicted in Fig. 3.4(b)[158]. Before entering the interferometer, the photon is steered by a mirror (M1 in the figure). The displacement and tilt of the mirror determines x and k respectively. The interferometer includes an image rotator (a Dove prism[158] or a three-mirror setup[159] to rotate the geometric phase of the photon), which acts as the spatial inversion of the photon. The output signal of the

interferometer is collected by a focusing lens and directed to a large area detector to perform the spatial integration.

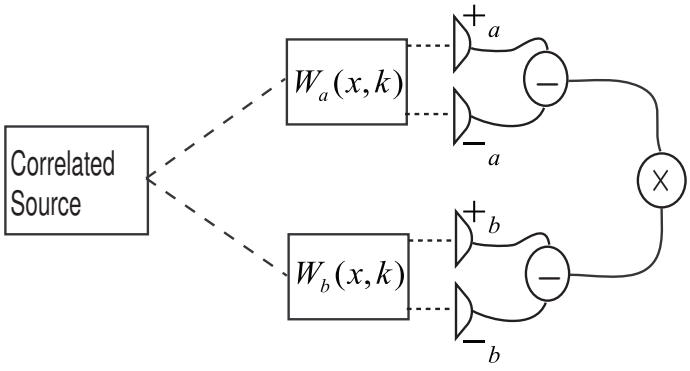
The two output ports of the Sagnac interferometer correspond to two possible measurement results (+ and −, or symmetric and anti-symmetric) of the spatial parity operator $\Pi_{x,k}$. Since the Wigner function is the expectation value of $\Pi_{x,k}$, it should be proportional to the difference between the signal intensities of the two detectors. For the measurement of the joint Wigner function, an apparatus consisting two separate Sagnac interferometers should be employed (Fig. 3.4(a)). The coincidence events between different detectors ($+_a+_b$, $+_a-_b$, $-_a+_b$ and $-_a-_b$) corresponds to four possible measurement results of $\hat{\Pi}_{x_a,k_a}\hat{\Pi}_{x_b,k_b}$, therefore the joint Wigner function is given by

$$W(x_a,k_a;x_b,k_b)=\frac{C(+_a+_b)-C(+_a-_b)-C(-_a+_b)+C(-_a-_b)}{C(+_a+_b)+C(+_a-_b)+C(-_a+_b)+C(-_a-_b)} \tag{3.27}$$

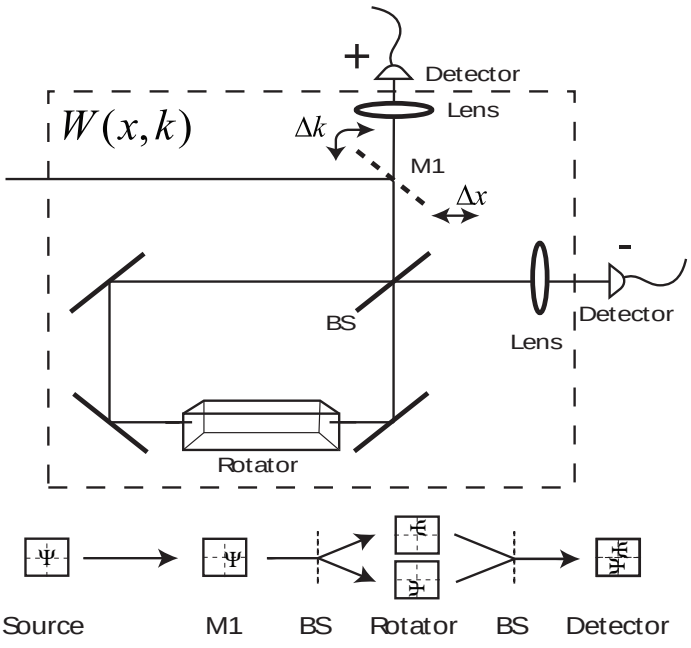
where $C(\cdot)$ is the number of coincidence events.

By selecting appropriate configurations of the PDC source and displacements of the mirrors, the results of measurements can violate local realism. Nevertheless, there will likely be some restrictions on the possible states testable in this way due to the finite numerical aperture of the Sagnac interferometer.

Recently another experimental violation of a Bell inequality with spatial parity has been reported[161]. This experiment also employs an appropriately tailored PDC state. Instead of measuring the parity of the wave function in the phase space



(a)



(b)

Figure 3.4 (a) Apparatus for measuring the spatial joint Wigner function of the PDC source. Each arm consists of a Sagnac interferometer shown in (b). The displacement and tilt of the mirror M1 determine the point (x, k) for measuring the Wigner function.

$(x_1, k_1; x_2, k_2)$ with Wigner function, they concentrate on the parity in position. This is achieved by local parity analysers, which change the geometric phases of the photons by θ_a and θ_b respectively. With properly selected combinations of (θ_a, θ_b), a Bell inequality violation is demonstrated.

3.3 Detection loophole revisited

The proposed scheme for examining Bell's theorem with spatial parities has a significant benefit: it allows one to employ the full continuum of the joint wave function of the two photon state from PDC, without any spatial filtering. This can drastically reduce the optical loss, though improvement of the detector efficiency is still required to close the detection loophole. However, recall the spatial correlation in Eq. 3.4 is only applicable for the degenerate PDC state, *i.e.* spectral filtering is required, which introduces remarkable loss as well. To fix this problem it is necessary to study whether the correlation of a PDC state in the spatial degree of freedom, without any spectral filtering, is able to violate a Bell inequality. This requires to study entanglement in a larger Hilbert space[134], and Bell inequalities should be adapted to this new Hilbert space. An alternative approach is to find a PDC state that decouples the spatial degree of freedom from the spectral degree of freedom, some ideas of which were presented in Appendix A.

Chapter 4

Quantum Key Distribution Using Continuous Variables of Single Photons

The distribution of secret information via optical channels, *e.g.* quantum key distribution (QKD) (see Sec. 1.3 for the introduction), provides an important example of the technological capability of quantum correlations. As discussed in Sec. 1.3, current QKD schemes can usually be divided into two major categories. One is the Bennett-Brassard (BB84) protocol[65] and a large collection of its variations[162], which employ dichotomic variables, *e.g.* the polarization or relative phase[75], of single photons or entangled photon pairs to transfer information securely. Thus the maximum achievable information transfer rate is intrinsically limited to one bit per photon. The other QKD category utilizes continuous variable (CV) multi-photon

systems[10,13,94] where the amplitude and phase quadratures of coherent states[14,95] or squeezed state[11,12] serve as the information carriers. While CV-QKD systems potentially enable higher key distribution rate, since measurment results can have a continuum of values instead of two, they appear to be much more sensitive to losses[93], restricting the security for longer distances. Entanglement purification, postselection[96] or reverse reconciliation protocols[14] can enhance the range of secure communications in this approach.

As shown in Sec. 1.4, the spatial (position and momentum) and spectral (time and frequency) degrees of freedom of quasi-monochromatic single photons can play a similar role as the quadrature amplitudes of the electromagnetic field. Therefore it is possible to implement quantum information processing applications with these variables. For example, experimental demonstrations of encoding qudits ($d > 4$) on the spatial degree of freedom of entangled photons generated with parametric downconversion (PDC) process have been reported[163,164], which demonstrates the potential of continuous variables of single photons for quantum communications. Recently there have been several considerations to employ these variables for distributing secret information. These schemes, *i.e.* single-photon CV-QKD, have been suggested as a means to increase the information transfer rate by coding more than one bit per photon. Compared to quadrature-based CV-QKD, single photon CV-QKD eliminates the local oscillators required for homodyne detection, and as we will show in this chapter, decouple the channel loss from the quantum correlations. Experimental implementations have demonstrated the feasibility of these schemes

by utilizing the spatial [2,109] or spectral [110] degree of freedom of single photons or entangled photon pairs generated by PDC. Yet, the security of such schemes has not been analysed in a thorough way, and as we show here, this is not a trivial extension of either BB84 or the conventional CV-QKD security proofs.

In this chapter, we evaluate the potential of the spatial properties of PDC for QKD by considering a realistic PDC source with practical detectors and a lossy quantum channel. The analysis here also works for CV-QKD employing the correlations of time-frequency entangled photon pairs [110]. Although the spectral degree of freedom of a properly engineered PDC state can demonstrate a large entanglement [165], which is extremely benificial for quantum communications, to make use of this correlation, one requires nonstationary optical elements, such as shutters, phase modulators and especially detectors whose response time is in the femtosecond-picosecond range, or alternatively, devices with very high spectral resolution, on the order of the pump bandwidth. These devices are difficult or impossible to build with current technology. Spatial correlations are, however, easier to manipulate with current technology, therefore allowing more complete assessment of the channel security.

4.1 Information content of the parametric downconversion state

Analysis of the amount of information shared between different parties (Alice, Bob and Eve) plays an important role in quantum cryptography. It determines the transfer rate of secret keys. Therefore we start with an analysis of the information content in the PDC state.

There are several ways to quantify information. The most well-known definition was given by C. E. Shannon: the amount of information is defined by the reduction of uncertainty[166]. A key concept in the quantification of information is *entropy*. The entropy of a random variable X measures the uncertainty about X before we know the exact value of X. Assume the value of X has a probability distribution $p(x)$ (here we consider the situation that X is a continuous variable), then the entropy is defined as[166] (in units of 'bits').

$$H(X) = -\int_{-\infty}^{\infty} dx\, p(x) \log_2 p(x). \tag{4.1}$$

Entropy also measures the amount of information that one can gain after learning the value of X. Consider a communication process with a perfect channel, *i.e.* lossless, no noise, no distortion *etc.*, the sender (Alice) transmits the value of X to the receiver (Bob) along this channel. Then $H(X)$ quantifies the amount of information that is transfered from Alice to Bob.

In practical systems, due to the imperfections of the transfer channel (losses,

noises, distortions *etc*), Alice and Bob may have different variables X and Y, *i.e.* $X \neq Y$. Suppose Alice tries to send X to Bob and Bob receives Y. X and Y are not perfectly correlated in the sense that the conditional probability distribution

$$p(x|y) \neq \delta(x-y), \tag{4.2}$$

where $\delta(\cdot)$ is the Dirac delta function. In this situation the conditional entropy is defined as

$$H(X|Y) = -\int_{-\infty}^{\infty} dy \int_{-\infty}^{\infty} dx\, p(x,y) \log_2 p(x|y), \tag{4.3}$$

where $p(x,y)$ is the joint probability distribution of X and Y. $H(X|Y)$ quantifies Bob's uncertainty in X after he receives Y. Recalling information is quantified as the reduction of uncertainty, the amount of information that is transfered from Alice to Bob is

$$I(X;Y) = H(X) - H(X|Y), \tag{4.4}$$

which is also known as the *mutual information* of X and Y. Substituting Eq. 4.1 and Eq. 4.3 into Eq. 4.4, we have

$$I(X;Y) = \int_{-\infty}^{\infty} dy \int_{-\infty}^{\infty} dx\, p(x,y) \log_2 \frac{p(x,y)}{p(x)p(y)}, \tag{4.5}$$

where $p(x)$ and $p(y)$ are the marginal distributions of X and Y, respectively.

Eq. 4.5 has a symmetric form between X and Y. Therefore it is not necessary to assume that X is the variable being sent and Y the variable being received. $I(X;Y)$

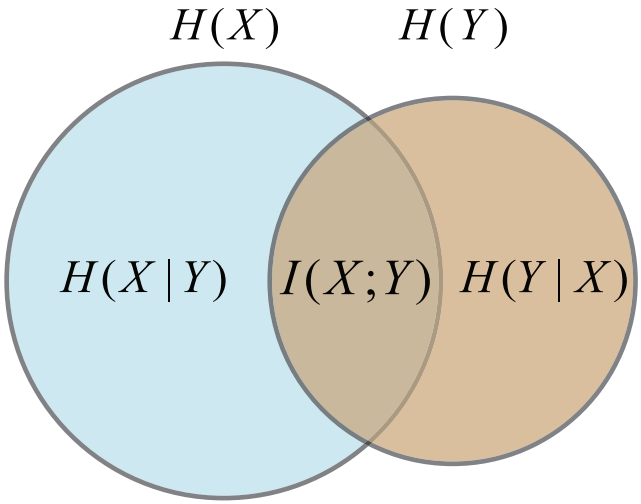


Figure 4.1 A Venn-diagram depicting the relations between $H(X)$, $H(Y)$, $H(X|Y)$, $H(Y|X)$ and $I(X;Y)$.

is the amount of information shared between the two communicating parties, *i.e.*, it is the amount of information that X has about Y, and Y has about X as well. This is reflected by the fact that $I(X;Y)$ has another form

$$I(X;Y) = H(Y) - H(Y|X). \tag{4.6}$$

The relations between $H(X)$, $H(Y)$, $H(X|Y)$, $H(Y|X)$ and $I(X;Y)$ are depicted in Fig. 4.1. In some sense $I(X;Y)$ can be considered as a quantification of the correlation between X and Y.

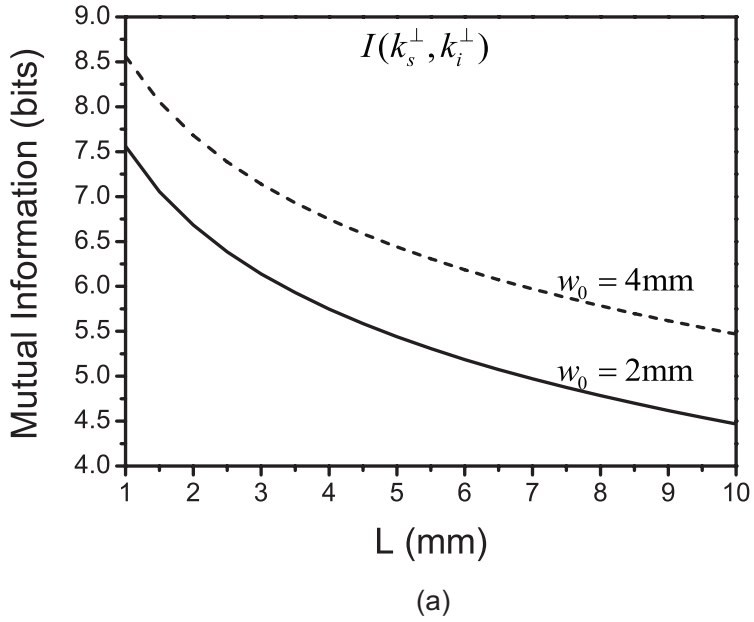
With this introduction to information theory, we can apply this idea to calculate the information content of the spatial correlations of two-photon PDC states. Here we consider a degenerate type-I PDC state, the joint amplitude $f(\mathbf{k}_s^\perp;\mathbf{k}_i^\perp)$ of which is give in Eq. 2.27, and the joint probability distribution of $\mathbf{k}_s^\perp$ and $\mathbf{k}_i^\perp$ is given

by $p(\mathbf{k}_s^\perp;\mathbf{k}_i^\perp) = |f(\mathbf{k}_s^\perp;\mathbf{k}_i^\perp)|^2$. Previous treatment of this problem[2] ignores the longitudinal phase-matching function ($\mathrm{sinc}(\Delta kL/2)$ in Eq. 2.27), by assuming the phase-matching spatial bandwidth is much broader than the pump function $\alpha(\mathbf{k}^\perp)$. In this case the joint probability distribution is approximated as

$$p(\mathbf{k}_s^\perp;\mathbf{k}_i^\perp) \approx \exp\left(-\frac{w_0^2}{2}\left|\mathbf{k}_s^\perp + \mathbf{k}_i^\perp\right|^2\right). \tag{4.7}$$

This gives an uniform marginal distribution of $\mathbf{k}_s^\perp$ and $\mathbf{k}_i^\perp$, which is unphysical and will give infinite mutual information $I(\mathbf{k}_s^\perp;\mathbf{k}_i^\perp)$. Therefore retaining the longitudinal phase-matching function is critical to bounding the shared information from above. Unfortunately, with the the longitudinal phase-matching function the mutual information can not be estimated analytically, even with the Gaussian approximation given in Eq. 2.33. In order to make progress we must resort to numerical calculations. For the numerical analysis we model our practical source of entangled photon pairs by considering degenerate Type-I PDC in a BBO crystal with a phase-matching angle of 3°, pumped at 400 nm wavelength. Fig. 4.2(a) shows the calculated mutual information between the transverse momemta of signal and idler photons $I(\mathbf{k}_s^\perp;\mathbf{k}_i^\perp)$. Similarly, the Fourier transform of Eq. 2.27 gives the joint amplitude of the transverse positions of the photons $f(\mathbf{r}_s^\perp;\mathbf{r}_i^\perp)$, which determines the mutual information $I(\mathbf{r}_s^\perp;\mathbf{r}_i^\perp)$ between the transverse positions of the two photons.

The graph illustrates the information transfer gain for CV single photon systems. It is shown that for a practical PDC state, over 8 bits of information can be



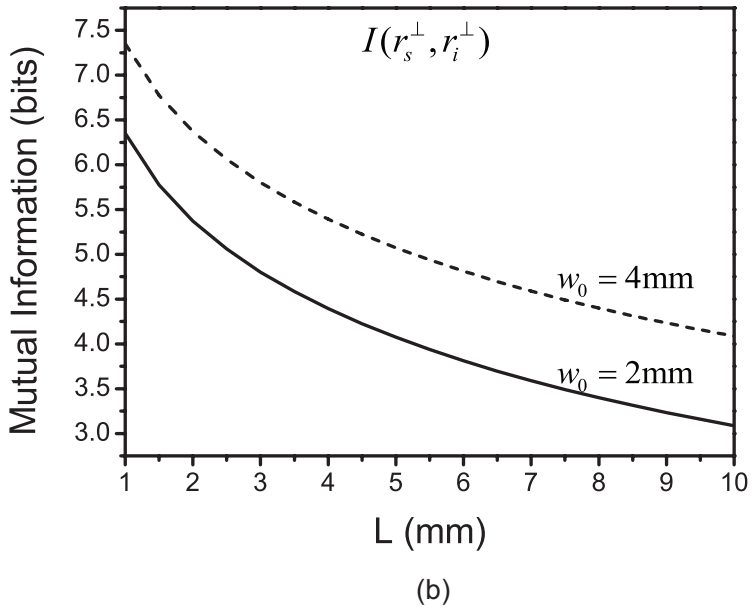


Figure 4.2 Mutual information for spatially entangled photon pairs generated by Type-I PDC in BBO crystal in the (a) momentum and (b) position. This figure shows how the crystal length and the pump waist affects the averaged mutual information in momentum and position.

transfered through the spatial degree of freedom of one photon pair. This should be compared with binary coding, for which a maximal value of one bit is obtained. The amount of shared information between the transverse spatial state of PDC photons may be increased by increasing the pump waist w_0 and decreasing the crystal length L, though the penalty for these changes is a reduced efficiency of photon pair generation, resulting in low signal rates. This is an expected result since increasing w_0 makes the conditional distribution of the transverse momenta of the PDC state ($P(\mathbf{k}_s^{\perp}|\mathbf{k}_i^{\perp})$ in Eq. 2.38) narrower, while decreasing L makes the marginal distribution of the transverse momentum of the PDC state ($\bar{P}(\mathbf{k}_s^{\perp})$ in Eq. 2.36) broader. Therefore the reduce of the uncertainty in the transverse momentum of the signal photon after the measurement of the transverse momentum of the idler photon becomes larger. We should mention that if we continue increasing the length of the crystal, the mutual information will meet a minimum and goes up again. This is because the photon pair generated from the PDC state is changed from anti-correlated to correlated. The turning point is where the photon pair is separable or quasi-separable[35]. This situation is beyond the scope of this thesis. The entanglement of the two-photon state in our analysis is reflected by considering the correlations or the mutual information for direct measurements of a pair of conjugate continuous variables, namely the position and momentum of the photons. Alternatively, one may quantify the entanglement contained in this degree of freedom by decomposing the state into its Schmidt modes[35], and evaluating the corresponding concurrence (the Schmidt number defined in Eq. 1.8). We verified that this approach yields

the same asymptotic behavior, which confirms the consistency of our results with more general entanglement measures. However the difference between the values of $I(\mathbf{k}_s^{\perp};\mathbf{k}_i^{\perp})$ and $I(\mathbf{r}_s^{\perp};\mathbf{r}_i^{\perp})$ indicates that mutual infomation analysis is not a universal way to quantify entanglement. QKD further requires that the measurements of non-corresponding variables do not exhibit correlations; our calculations show that the mutual information between momentum and position ($I(\mathbf{k}_s^{\perp};\mathbf{r}_i^{\perp})$ and $I(\mathbf{r}_s^{\perp};\mathbf{k}_i^{\perp})$) is negligible (less than 0.01 bits).

4.2 The QKD protocol utilizing the spatial correlations of the PDC state

To analyse the performance of a single-photon CV-QKD system we need to specify the protocol. The proposed CV-QKD protocol is depicted in Fig. 4.3. The six basic steps of the scheme are:

1. *Transmission of raw key.* Pairs of entangled photons are generated in a nonlinear crystal and transmitted to Alice and Bob separately via a quantum channel. The two parties choose randomly to detect either the transverse position ($\mathbf{r}^{\perp}$) or momentum ($\mathbf{k}^{\perp}$) of each photon they receive. The outcome values registered by Alice and Bob are the raw keys.

2. *Key sifting.* Alice and Bob announce by an authenticated public channel the basis in which they measured for each photon (position or momentum) and drop the bits where they used different bases. The remaining values constitute

the sifted key. Due to the deviation of the PDC state from a perfectly correlated state (the EPR state) and the disturbance of the transmission (losses, noise, *etc.*), Alice and Bob may possess different sifted key.

3. *Estimate the transmission disturbance.* For QKD schemes with dichotomic variables, this step aims to estimate the transmission bit error rate with a subset of the sifted key. Since we consider a QKD protocol with continuous variables, there is no bit error rate defined. Rather Alice and Bob compare a subset of their sifted keys to construct the joint probability distribution of their measurement results, which reveals the properties of the transmission channel and the level of the transmission disturbance (loss, noise, *etc*). For quantum cryptography, Alice and Bob must consider the worst situation: all the discrepancies are introduced by an eavesdropper (Eve). With their joint probability distribution of the sifted keys, Alice and Bob can estimate their shared information and bound the information acquired by Eve.

4. *Interactive error correction.* The final goal of QKD is to allow Alice and Bob to possess the same secret key. Therefore they should remove the discrepancies in their sifted keys. This is done by exchange some reconciliation messages calculated from their bit strings over the public authenticated channel while minimizing the information revealed to Eve. There are various protocols for this step[167–169]. Depending from whom the reconciliation messages are sent, this protocol can be divided into two categories: forward reconciliation (Alice sends the messages)[167] and reverse reconciliation (Bob sends the messages)[170]. Re-

verse reconciliation plays an important role in the quadrature-based CV-QKD to overcome the channel loss[14]. It is also useful to discretize the continous variable at this step[169]. After this is done, Alice and Bob possess the same key, which is called the reconciled key. We will not discuss about the details of the reconciliation algorithms in this thesis, but rather focus on the conditions for the success of reconciliation.

5. *Privacy amplification*[71]. Taking into account the transmission disturbance, the information leakage during error correction, the characteristics of the source, Alice and Bob estimate the total information possessed by Eve. Then they shorten the reconciled key by a ratio calculated from a chosen function in order to annihilate Eve's information. The remaining data is the final key.

6. *Authentication.* At the beginning of the communication Alice and Bob use predefined messages, the authentication key, to establish authentication. After that, every time when they start a new session of key distribution, a small part of the previous private key will be used as the authentication key.

There are various options for steps 3 – 6. For example, there are more powerful ways to distill the secret keys known as the advantage distillation which tolerates higher transmission disturbance, but is less efficient[78]. Moreover, one can use a quantum mechanical way, known as entanglement purification[15], to distill the key. The protocol listed here is a classical option which is most plausible with current technologies. The technical details of each step and the comparison between different

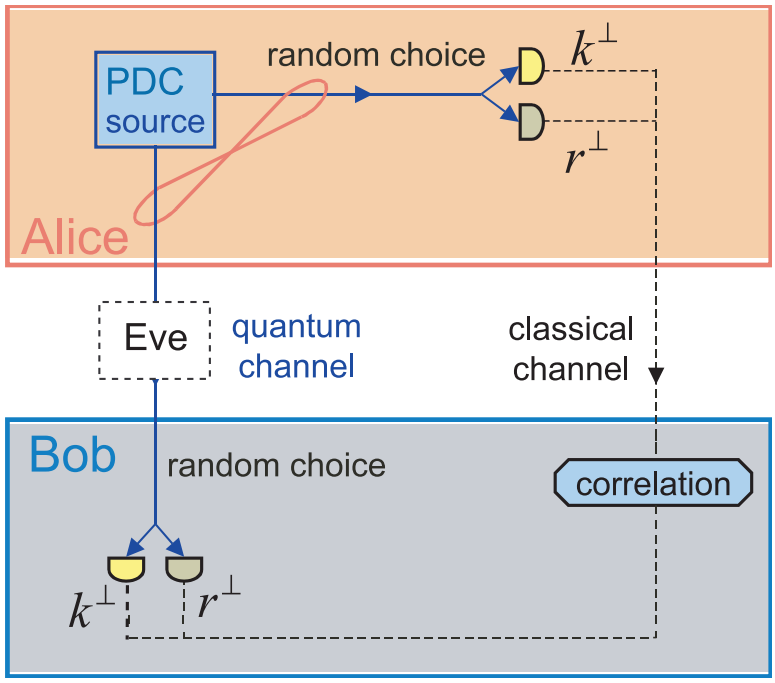


Figure 4.3 The scheme of single-photon CV-QKD. PDC photons are transmitted to Alice and Bob via a quantum channel. Then each party choose to measure either the position ($\mathbf{r}^{\perp}$) or momentum ($\mathbf{k}^{\perp}$) randomly and independently. The uncertainty principle $\Delta\mathbf{k}^{\perp}\cdot\Delta\mathbf{r}^{\perp} \geq 1$ prevents the simultaneous measurement of both variables. After the measurement they estimate the correlations of the results through an authenticated classical channel and draw the secret key.

protocols is a big topic and beyond the scope of this thesis. But rather we will discuss the preconditions for the success of the key distillation, which is the crucial part of a QKD protocol.

4.3 Security performance of single-photon CV-QKD

4.3.1 General security analysis: the EPR criterion

To accomplish a successful quantum key distribution, the QKD system must allow Alice and Bob to distill a secret key from the sifted raw key that is inaccessible to the adversary, Eve. This strongly depends on the success of the error correction and privacy amplification steps of the QKD protocol. As mentioned in Sec. 4.2, there are two ways to perform the error correction: forward reconciliation and reverse reconciliation. We consider forward reconciliation first. It has been shown that the achievable secret key rate is bounded below by [171]

$$\Delta I = I_{AB} - I_{AE}. \tag{4.8}$$

where I_{AB} is the mutual information between Alice and Bob, while I_{AE} is the mutual information between Alice and Eve. This equation indicates that the secure key distillation is possible when Alice and Bob has more inforamtion than Eve. Since the legitimate parties (Alice and Bob) only keep the values that they measure the same variable, I_{AB} is an average of mutual information when both measure in the momentum basis ($I(\mathbf{k}_A, \mathbf{k}_B)$) and in the position basis ($I(\mathbf{r}_A, \mathbf{r}_B)$). Here we

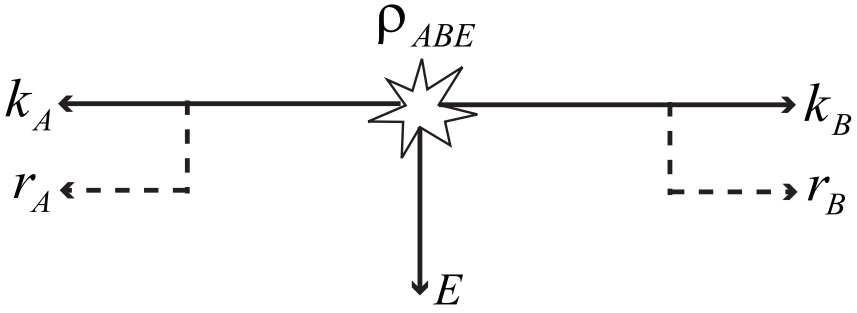


Figure 4.4 This figure depicts the eavesdropping attack discussed in the context. Alice, Bob and Eve share a tripartite entangled state ρ_{ABE}. Alice and Bob measure the momentum or postion of their received photons. E is Eve's ancilla.

remove the $\perp$ symbol for simplicity. We consider the case when both measure in the momentum basis first. To estimate I_{AE} we assume individual attacks: Alice, Bob and Eve share a tripartite entangled state and perform the measurement for each signal they received, as shown in Fig. 4.4. This can be achieved by entangling Eve's ancilla with the photon pairs transmitted to the legitimate parties. Eve can also block all photon pairs, preparing a tripartite state by herself and sending two of the photons to Alice and Bob separately. Quantum memories that can store quantum states coherently allow Eve to perform more powerful attacks known as coherent attacks. Here Eve keeps all her ancilla photons until Alice and Bob finish their classical communication through the authenticated channel, and performs positive operator valued measures (POVM) on the ancilla photons. It has been shown that the security against finite-size coherent attacks is similar to the individual attacks discussed below[98].

With these assumptions, we have

$$I_{AB} = H(\mathbf{k}_A) - H(\mathbf{k}_A|\mathbf{k}_B), \tag{4.9}$$

$$I_{AE} = H(\mathbf{k}_A) - H(\mathbf{k}_A|E), \tag{4.10}$$

where E is the measurement result Eve obtains from her ancilla. Since Eve's ancilla can be any quantum state, this measurement is not necessarily performed in the momentum or position representation. Substituting Eq. 4.9 and 4.10 into Eq. 4.8, we have

$$\Delta I = H(\mathbf{k}_A|E) - H(\mathbf{k}_A|\mathbf{k}_B). \tag{4.11}$$

Alice and Bob have the full knowledge about $H(\mathbf{k}_A|\mathbf{k}_B)$ since they can estimate the joint distribution $p(\mathbf{k}_A, \mathbf{k}_B)$ with their sifted keys. To estimate ΔI, it is necessary to bound $H(\mathbf{k}_A|E)$ with the information that Alice and Bob possess. Recall that Alice, Bob and Eve share a tripartite entangled state, if Bob measures position $\mathbf{r}_B$ of the signal he received, and Eve measures her ancilla E, Alice's received state will be projected onto $\rho_{A|\mathbf{r}_B,E}$ (pure or mixed). The measurement results for the momentum or position of $\rho_{A|\mathbf{r}_B,E}$ are restricted by the entropic uncertainty relation[172–174,174]

$$H_{\rho_{A|\mathbf{r}_B,E}}(\mathbf{k}_A) + H_{\rho_{A|\mathbf{r}_B,E}}(\mathbf{r}_A) \geq \log_2 \pi e. \tag{4.12}$$

Recall that entropy is a measure of uncertainty of a variable. Eq. 4.12 is an uncertainty relation between conjugate variables $\mathbf{k}_A$ and $\mathbf{r}_A$. There are some arguments

that this relation is a stronger condition than the Heisenberg uncertainty relation in the sense that it provides a tighter bound on the uncertainties of conjugate variables[172,175] .

Then we have the conditional entropy

$$H(\mathbf{k}_A|\mathbf{r}_B,E) = \int d\mathbf{r}_B \int dE\, p(\mathbf{r}_B,E) H_{\rho_{A|\mathbf{r}_B,E}}(\mathbf{k}_A), \tag{4.13}$$

$$H(\mathbf{r}_A|\mathbf{r}_B,E) = \int d\mathbf{r}_B \int dE\, p(\mathbf{r}_B,E) H_{\rho_{A|\mathbf{r}_B,E}}(\mathbf{r}_A). \tag{4.14}$$

Here $H(\mathbf{k}_A|\mathbf{r}_B,E)$ and $H(\mathbf{r}_A|\mathbf{r}_B,E)$ are conditional entropies of Alice's measurement results ($\mathbf{k}_A$ and $\mathbf{r}_A$) when Bob and Eve's measurement results are $\mathbf{r}_B$ and E respectively. From Eqns. 4.12 – 4.14, we have

$$H(\mathbf{k}_A|\mathbf{r}_B,E) + H(\mathbf{r}_A|\mathbf{r}_B,E) \geq \log_2 \pi e. \tag{4.15}$$

In the derivation of Eq. 4.15, we consider the state Alice has after Bob and Eve's measurements, which assumes that Bob and Eve perform the measurement before Alice. This is not a necessary condition. Since the joint probability distribution $p(\mathbf{k}_A,\mathbf{r}_B,E)$ and $p(\mathbf{k}_A,\mathbf{r}_B,E)$ are determined by the tripartite entangled state, not the sequence of the measurements.

From information theory, we have[176]

$$H(X|Y,Z) \leq H(X|Y), \tag{4.16}$$

$$H(X|Y,Z) \leq H(X|Z). \tag{4.17}$$

This can be understand as that any additional information (Z in Eq. 4.16 and Y in Eq. 4.17) will never increase the entropy. With Eqns. 4.15 – 4.17, we have

$$H(\mathbf{k}_A|E) + H(\mathbf{r}_A|\mathbf{r}_B) \geq \log_2 \pi e, \tag{4.18}$$

which bounds $H(\mathbf{k}_A|E)$ with Alice and Bob's measurement results $\mathbf{r}_A$ and $\mathbf{r}_B$.

Combining Eqns. 4.11 and 4.18, we have

$$\Delta I \geq \log_2 \pi e - H(\mathbf{r}_A|\mathbf{r}_B) - H(\mathbf{k}_A|\mathbf{k}_B), \tag{4.19}$$

which can be evaluated with Alice and Bob's sifted keys. Eq. 4.19 allows Alice and Bob to bound the secret key rate without knowing Eve's action. We need to mention that we obtain Eq. 4.19 by considering the secret information when both Alice and Bob measure the momentum of the photons they received (Eq. 4.11). Therefore, $\mathbf{r}_A$ and $\mathbf{r}_B$ are not the variables directly accessible, but rather the variables that could have been measured. It is reasonable to assume that the photons that both of Alice and Bob measure in the momentum basis has the same state as the photons that both of them measure in the position basis. Therefore $H(\mathbf{r}_A|\mathbf{r}_B)$ in Eq. 4.19 can be estimated by the statistical properties of the measurement results when Alice and Bob actually measure in the position basis.

We can further simply Eq. 4.19 by bounding the conditional entropies with the

inequality (see Appendix B for details)

$$H(X|Y) \leq \frac{1}{2}\log_2\left[2\pi e\Delta^2(x|y)\right] \tag{4.20}$$

where $\Delta^2(x|y)$ is the variance of X conditioned on Y defined in Eq. B.14. Thus Eq. 4.19 can be simplified as

$$\Delta I \geq \frac{1}{2}\log_2\left(\frac{1}{4}\frac{1}{\Delta^2(r_A|r_B)\Delta^2(k_A|k_B)}\right) \tag{4.21}$$

For simplicity, we consider the situation where both the position and momentum are 1D variables. So a sufficient condtion for $\Delta I \geq 0$, *i.e.* non-zero secure information is transfered from Alice to Bob, is

$$\Delta^2(r_A \mid r_B)\Delta^2(k_A \mid k_B) \leq \frac{1}{4}. \tag{4.22}$$

Similarly the security analysis for the situation when both Alice and Bob measure the position of the photons yields the same result. This result is expected due to the symmetry form of Eq. 4.22 in position and momentum. For high entanglement, this condition coincides with the EPR criterion[177,178]:

$$\Delta^2(r_A - r_B)\Delta^2(k_A + k_B) \leq \frac{1}{4}. \tag{4.23}$$

But according to Eqns. B.16 and B.17, Eq. 4.22 is usually a less strict condition than the EPR criterion. From the discussions in Sec. 2.5, the PDC state satisfies

Eq. 4.22. This has also been experimentally demonstrated recently [49,164].

For reverse reconciliation, the achievable secret key rate is bounded below by [171]:

$$\Delta I = I_{AB} - I_{BE}. \tag{4.24}$$

With a similar analysis we arrive at the following sufficiency condition for $\Delta I \geq 0$

$$\Delta^2(r_B \mid r_A)\Delta^2(k_B \mid k_A) \leq \frac{1}{4}. \tag{4.25}$$

4.3.2 Limitations of experimental imperfections on the legitimate parties

As mentioned previously, there have been several experiments that have measured the spatial correlations of the PDC state. However, almost all of these experiments employ a single detector to scan throughout the momentum or position values (with one exception in Ref[163], which employed three APD detectors on each party, and the spatial resolution is far from enough to explore the full characteristics of the spatial-correlated PDC state). In principle the outcome of each measurement is binary: either the photon hits the detector or not. Thus the information content in each of these experiments is reduced to one bit per photon. This setup is not suitable for single photon CV-QKD because not all of the possible position/momentum values are monitored at the same time. To realise the full potential of continuous variables, an array of detectors (avalanche photodiodes (APDs), pixels of a charge-coupled device (CCD) camera, etc.) is needed. To allow the information content

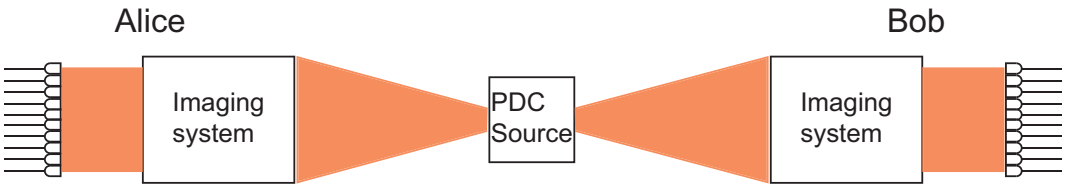


Figure 4.5 A schematic discription of the singl-photon CV-QKD system. The entangled photons pairs are generated by the PDC process and sent to Alice and Bob separately through free space transmission. Each receiver manipulates the photon they received with imaging systems (Sec. 2.6) and measures the momentum and position of the photon with a detector array. The choice of the imaging system can be implemented with a beam splitter.

I_{AB} detected, the detector number n should satisfy $n \geq 2^{I_{AB}}$. This implies that the dark count of the detectors will have a much higher impact on the error rate or key discrepancy than in standard BB84.

To see this, we consider a simplified setup shown in Fig. 4.5. The entangled photon pair is generated from the pump pulse with probability P_{PDC} and sent to Alice (signal) and Bob (idler) through two quantum channels with transmission coefficients t_A and t_B. Here we only consider the loss of the channel. For free space transmissions, the atmospheric turbulence effect introduces additional disturbance. This can be largely suppressed with the help of adaptive optics, and so we ignore it here. We should mention that it has been shown that the turbulence effect can cause the entanglement sudden death in an orbital-angular-momentum entangled two-photon state[179]. Although there is no proof that this effect will also cause entanglement sudden death in the continuous degree of freedom, it should be considered in the real implementation of a long distance link. Each party employs imaging systems to choose between the measurements of the position and momentum of the photons.

The choice of the imaging system can be implemented with a beam splitter. To measure the continuous variables, **r** and **k** each party maps the photon transverse field distribution to n identical detectors which are time-gated synchronously with the pump pulse. Since it is impossible to make the detector array infinitely large, there will be some truncation in the measurement. The magnification of the imaging system and the size of the detector array should be carefully selected to make the measurement region large enough so that the truncation effect is negligible. We denote the probability of recording a dark count (a false signal that cannot be distinguished from a single-photon event) within the detection time window for each detector as P_{dark} and the detection efficiency as η. The overall detection efficiency for Alice and Bob are ηt_A and ηt_B respectively. Alice and Bob keep only the results when one and only one detector clicks. For the analysis we ignore the backgournd light, which can be suppressed by carefully adjusting the transmission system. In principle this kind of noise can be treated similarly as the noise of detectors. So there are four cases to be considered: both parties have a dark count; Alice detects a photon and Bob has a dark count; Bob detects a photon and Alice has a dark count; both parties detect a photon. We analyse these four cases separately:

1. Both parties have a dark count. This can be further split into two situations:

(a) PDC pairs are not generated. The probability for this situation is

$$\begin{aligned} P(d,d|\text{no PDC}) &= (1-P_{PDC})\binom{n}{1}P_{dark}(1-P_{dark})^{n-1} \\ &\quad \times\binom{n}{1}P_{dark}(1-P_{dark})^{n-1} \\ &= (1-P_{PDC})n^2P_{dark}^2(1-P_{dark})^{2n-2}. \end{aligned} \quad (4.26)$$

(b) PDC pairs are generated, but not detected by Alice and Bob due to the loss. The probability for this event is

$$P(d,d|\text{PDC}) = P_{PDC}(1-\eta t_A)(1-\eta t_B)n^2P_{dark}^2(1-P_{dark})^{2n-2}. \quad (4.27)$$

Therefore the overall probability for the dark count - dark count event is

$$\begin{aligned} P(d,d) &= P(d,d|\text{no PDC}) + P(d,d|\text{PDC}) \\ &= [1-P_{PDC}+P_{PDC}(1-\eta t_A)(1-\eta t_B)] \\ &\quad \times n^2P_{dark}^2(1-P_{dark})^{2n-2}. \end{aligned} \quad (4.28)$$

Since the detectors are assumed to be identical, the measurement results of Alice and Bob should both be uniform over the measurement region, and uncorrelated with each other.

2. Alice detects a photon and Bob has a dark count. No doubt there is a PDC pair generated. Alice detects one of the photons and there is no dark count

in her detector array, while Bob fails to detect a photon and there is one dark count in his detector array. The probability for this situation is

$$\begin{aligned} P(p,d) &= P_{PDC}\eta t_A(1-P_{dark})^n(1-\eta t_B)\binom{n}{1}P_{dark}(1-P_{dark})^{n-1} \\ &= P_{PDC}\eta t_A(1-\eta t_B)nP_{dark}(1-P_{dark})^{2n-1}. \end{aligned} \tag{4.29}$$

In this situation, the measurement result of Alice should have the same distribution as the marginal distribution of the signal photon, while Bob's measurement results are uniform over the measurement region. Alice and Bob's measurement results are uncorrelated with each other.

3. Bob detects a photon and Alice has a dark count. This is identical to the previous situation with the positions of Alice and Bob switched. The probability for this event is

$$P(d,p) = P_{PDC}(1-\eta t_A)\eta t_B nP_{dark}(1-P_{dark})^{2n-1}. \tag{4.30}$$

In this situation, Alice's measurement results are uniformly distributed over the measurement region, while Bob's measurement results obey the marginal distribution of the idler photon. Their measurement results are uncorrelated.

4. Alice and Bob both detect a photon. This requires that a PDC pair is generated, both parties detect it and both parties do not have a dark count. The

probability for this situation is

$$P(p,p) = P_{PDC}\eta^2 t_A t_B (1 - P_{dark})^{2n}. \tag{4.31}$$

This is the only situation that reveals the quantum correlation of the photon pair. The joint probability distribution of the measurement results of the two parties is determined by the wave function of the PDC state.

There are also situations that the photon and a dark count arise at the same detector simultaneously. However the probability of this situation is negligible if $P_{dark} \ll 1$, which is a requirement for the detector array to distinguish the single-photon event. Similarly, the situation that two dark count arise at the same detector can also be ignored.

As mentioned in the previous discussion, among all the cases only $P(p,p)$ will reveal the quantum correlations. This probability decreases as the channel loss and the number of the detectors increase due to the increase of the background noise level. We consider a practical system with APDs as detectors and nanosecond time gating. The probability for generating a PDC pair within a pump pulse is around $P_{PDC} = 0.01$. The quantum efficiency of a typical APD (the probability that an input photon is converted to a photoelectron) is $\eta = 0.6$. The dark count level of a typical APD is around 250 dark counts per second. Therefore with a one-nanosecond time window, the probability P_{dark} to have a dark count is 10^{-6}. For the PDC source we fix the length of the BBO crystal to 2 mm and assume a 2

mm pump waist. The source can be anywhere between Alice and Bob. Here we consider the configuration where the source lies at Alice's station, *i.e.* $t_A \approx 1$ and $t_B = t$, where t is the transmission probability of the channel between Alice and Bob. Fig. 4.6 shows the changes of $P(d,d)$, $P(p,d)$, $P(d,p)$ and $P(p,p)$ (renormalized by $P(d,d)+P(p,d)+P(d,p)+P(p,p)$) with respect to channel loss $l = 1-t$ for $n = 128$ and $n = 256$ detectors. It is clear that $P(p,p)$ decreases with the increase of l, while both $P(p,d)$ and $P(d,d)$ increases with l. $P(d,p)$ also decreases with increasing l, since the probability that Bob detects the photon decreases when the channel loss increases, and the PDC source lies at Alice's station, so whether she detects the photon or a dark count is not affected by the channel loss. For a fixed l, $P(p,p)$ for $n = 256$ is smaller than that for $n = 128$, while all the other three probabilities are larger.

With this configuration, it can also be seen that for up to 40 dB of channel loss, $P(p,p)$ and $P(p,d)$ are much greater than $P(d,p)$ and $P(d,d)$, which means that the probability that Alice detects a photon is much higher than the probability that she detects a dark count. This is due to the zero loss for the photon transmission to Alice (though the detector efficiency still matters). Therefore it is a reasonable approximation to neglect the situation in which Alice has a dark count.

Fig. 4.7 shows the changes of the products $\Delta^2(r_A \mid r_B)\Delta^2(k_A \mid k_B)$ and $\Delta^2(r_B \mid r_A)\Delta^2(k_B \mid k_A)$ with repect to channel loss. In the security analysis of QKD protocols, Eve is assumed to have the full power allowed by quantum mechanics, *e.g.* she can replace a quantum channel with a lossless one, or change the

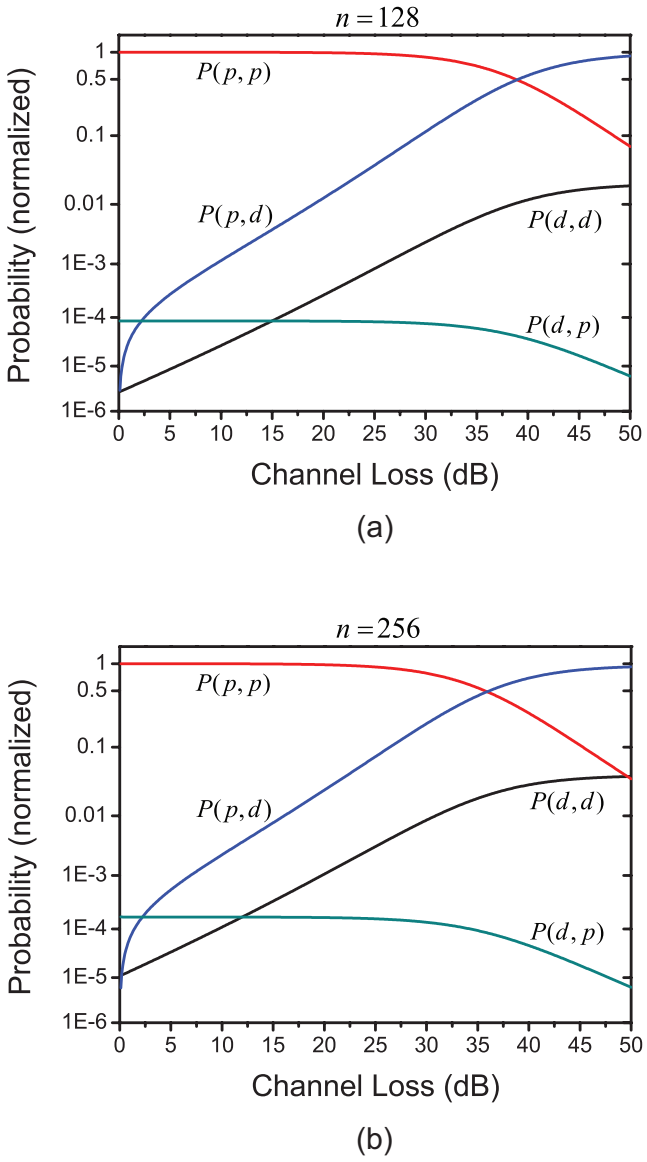


Figure 4.6 The change of $P(d,d)$, $P(p,d)$, $P(d,p)$ and $P(p,p)$ with respect to channel loss. Each probability is renormalized by $P(d,d)+P(p,d)+P(d,p)+P(p,p)$

detectors with noiseless ones. In principle, she can remove most of the disturbances of the transmission of quantum signals between Alice and Bob, and apply her eavesdropping attack. As long as the disturbance Eve introduced is no greater than that Alice and Bob expect from the original channel, they cannot tell that Eve exists. Therefore they must consider the worst-case scenario that all the disturbance is due to Eve and set an upper bound for the disturbance. Recall the condition for security is that either of the two products $\Delta^2(r_A \mid r_B)\Delta^2(k_A \mid k_B)$ for forward reconciliation and $\Delta^2(r_B \mid r_A)\Delta^2(k_B \mid k_A)$ reverse reconciliation is no bigger than 1/4 (Eqns. 4.22 and 4.25). From Fig. 4.7, this is satified for channel loss below 4.4dB(1.7dB) (channel throughput $t = 36\%(/68\%)$) assuming a detector array with $n = 128/256$ pixels for forward and reverse reconciliation. Both Eqns. 4.22 and 4.25 yield almost the same results, which means the forward reconciliation and reverse reconciliation have almost the same performance for this single-photon CV-QKD configuration. This is different from some quadrature-based CV-QKD[14], in which reverse reconciliation allows much higher channel loss than forward reconciliation. This difference is due to different experimental imperfections in single photon CV-QKD and quadrature-based CV-QKD.

For near-ground (terrestrial path) free space transmission the extinction coefficient varies within a large range (from 0.07 dB/km[180] to 28.9 dB/km[181]) due to the weather conditions. Here we assume it is 1dB/km, so the corresponding secure distance is 4.4km and 1.7km for $n = 128$ and $n = 256$ respectively. Beyond this range Eqns. 4.22 and 4.25 are no longer satisfied, and Eve stands a chance to gain

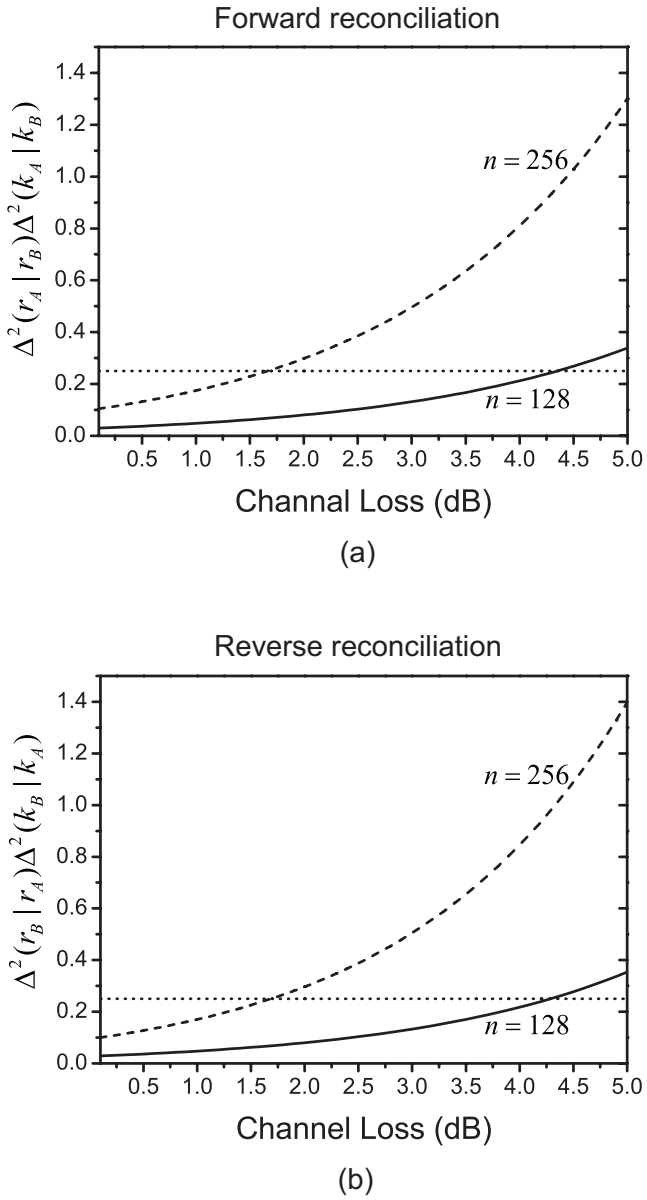


Figure 4.7 Variance products $\Delta^2(r_A \mid r_B)\Delta^2(k_A \mid k_B)$ and $\Delta^2(r_B \mid r_A)\Delta^2(k_B \mid k_A)$ with repect to channel loss l. When they are blow 1/4 (the dotted line), the security of the single-photon CV-QKD is insured.

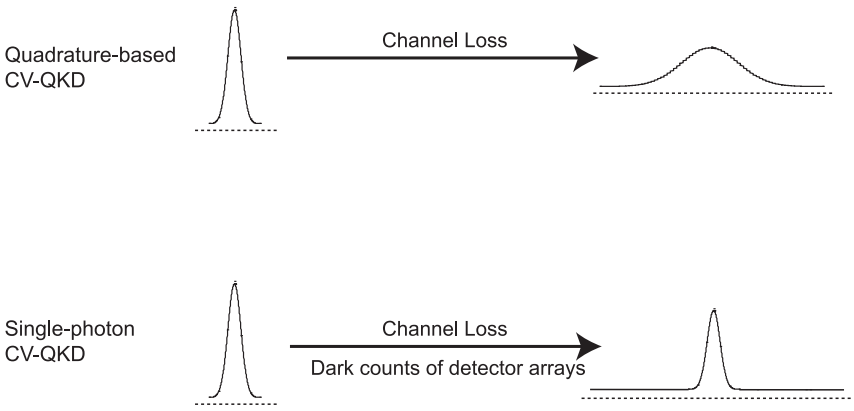


Figure 4.8 The effect of experimental imperfections for different CV-QKD schemes. For quadrature-based CV-QKD, the channel loss broadens the signal distribution, but still keeps the Gaussian characteristics, while for single-photon CV-QKD, the channel loss and detector noise yield a totally non-Gaussian distribution.

complete information about the key shared between Alice and Bob. But at these distances the probability of uncorrelated events $P(p,d) + P(d,p) + P(p,p)$ is less than 1%, which means that the noise level is still extremely low. This is because that $\Delta^2(X|Y)$ (the uncertainty in X when the value of Y is known) increases rapidly when the correlation between X and Y decreases.

4.3.3 Limitations of experimental imperfections on Eve: intercept-resend attack

Analysis of the variance product seems to suggest that this QKD scheme is not suitable for long-distance use. But we note that Eq. 4.22 is a tight bound for general CV-QKD schemes and it is possible to loosen the bound when considering special characteristics of the experimental imperfections in the single-photon CV-QKD protocol. Reconsidering the discussions in Sec. 4.3.1, we note that the equality in Eq.

4.21 can only be achieved when Eve's attacks satisfy certain strict conditions. The most important condition is that the distribution of Bob's measurement outcomes conditioned on Alice's results should be Gaussian (see Appendix B). A Gaussian attack is well known to be optimal for conventional CV-QKD using the quadratures of multi-photon states since in these systems experimental imperfections—mainly the loss of the channel—will preserve the Gaussian character of the transmitted state (recall the discussions in Sec. 1.1, this means the phase-space representation of the state is still a Gaussian function), broadening Bob's distribution (see Fig. 4.8). By replacing the channel with a lossless one and applying a Gaussian attack, Eve can hide behind the existing experimental imperfections. The normal way for Alice and Bob to detect Eve is to monitor the covariance matrix of their results. In contrast, for single-photon dichotomic-variable QKD (BB84 *etc*), the experimental imperfections (loss, noise, etc) yield uncorrelated detection events between Alice and Bob, which are typically interpreted as background noise. In single-photon CV-QKD the experimental imperfections play a similar role to those in standard dichotomic single-photon QKD. The events registered by each party are either from the PDC photons or from the detector noise, and the latter has a uniform distribution (due to the uniformity of the detectors). Hence Alice and Bob expect un-broadened Gaussian joint probability distributions from the quantum correlation measurements interspersed with uncorrelated flat background events, which in total represents a non-Gaussian distribution. In order to stay undetected Eve must mimic this distribution. Therefore she only has limited options and the optimal attack for multi-photon CV-QKD

is prohibited here. Moreover, for non-Gaussian distributions, the left side of Eq. 4.21 can be much bigger than the right side, which means even when the EPR criterion is violated ($\Delta^2(r_A \mid r_B)\Delta^2(k_A \mid k_B) > 1/4$), it is still possible for Alice and Bob to draw the secret key ($\Delta I > 0$).

It is unclear what will be Eve's optimal attack under the above conditions, but a possible eavesdropping strategy is an intercept-resend attack: Eve intercepts the photon sent to Bob, measures it in the randomly chosen variable (momentum or position), and resends a photon in the eigenstate based on her measurement result. If, by chance, she has chosen the same measurement basis as Alice and Bob, her operation will appear as an undisturbed channel between these two parties. Otherwise, measuring the conjugate variable Eve introduces a flat background noise, which cannot be distinguished from the dark noise of the detector array. Therefore by adjusting the loss of the channel, Eve can hide her disturbance behind the experimental imperfections. We define an intercept-resend ratio λ as

$$\lambda = \frac{\text{Number of photons intercepted by Eve}}{\text{Total number of photons Alice sends to Bob}}.$$

Now we estimate the mutual information $I(A, B)$ and $I(A, E)$. Here we ignore the channel loss and detector noise, and assume all disturbances are due to the presence of Eve, since this is the worst case that maximize Eve's information. We first consider the situation that both Alice and Bob measure the momentum of the photons. Since Eve does not know which variable the legitimate parties measured, she can do no

better than just picking randomly a measurement basis. There is 50% chance that she will pick the wrong basis for the photons she intercepted. If she measures the correct variable (the momentum), the joint probability of Alice and Bob is

$$\begin{aligned} p_{Ek}(k_A, k_B) &= \int dk_E \, p_{Ek}(k_A, k_E, k_B) \\ &= \int dk_E \, p_{PDC}(k_A, k_E) \, p_{Ek}(k_B|k_A, k_E), \end{aligned} \tag{4.32}$$

where $p_{PDC}(k_A, k_E)$ is given by the joint distribution of the momentum of the PDC state. Since the state that Eve resends to Bob only depends on her measurement result, $p_{Ek}(k_B|k_A, k_E)$ reduces to $p_{Ek}(k_B|k_E)$. If the state the Eve resends is the eigenstate of momentum, we have $p_{Ek}(k_B|k_E) = \delta(k_B - k_E)$ where $\delta(\cdot)$ is the Dirac-delta function. Therefore Eq. 4.32 can be written as

$$p_{Ek}(k_A, k_B) = p_{PDC}(k_A, k_B), \tag{4.33}$$

which is exactly what Alice and Bob expect from an undisturbed channel. If Eve measures the wrong variable (the position), the joint probability distribution of Alice and Bob is

$$\begin{aligned} p_{Er}(k_A, k_B) &= \int dr_E \, p_{Er}(k_A, r_E, k_B) \\ &= \int dr_E \, p_{PDC}(k_A, r_E) \, p_{Er}(k_B|k_A, r_E). \end{aligned} \tag{4.34}$$

Similarly, for an intercept-resend attack, $p_{Er}(k_B|k_A, r_E) = p_{Er}(k_B|r_E)$. Moveover,

if the state that Eve resends is an eigenstate of position, k_B and r_E are correlated (neglecting a phase factor), and $p_{Er}(k_B|r_E) = p_{Er}(k_B)$ is a uniform distribution over the measurement region. Thus Eq. 4.34 can be simplified as

$$p_{Er}(k_A, k_B) = p_{PDC}(k_A)\, p_{Er}(k_B), \tag{4.35}$$

where $p_{PDC}(k_A) = \int dr_E\, p_{PDC}(k_A, r_E)$ is the marginal distribution of k_A from the PDC state. Eq. 4.35 is exactly the same joint probability distribution when Alice receives a photon and Bob has a dark count. This attack cannot mimic the situations when Alice has a dark count, but this is not a problem, since Alice's detector array will automatically generate these events, and as shown in Fig. 4.6, this situation can usually be ignored. To summarize all three situations (Eve does not intercept the photon, Eve measures the momentum of the photon, Eve measures the position of the photon), the joint probability distribution of Alice and Bob is

$$\begin{aligned} p(k_A, k_B) &= (1-\lambda) p_{PDC}(k_A, k_B) + \frac{\lambda}{2} p_{Ek}(k_A, k_B) + \frac{\lambda}{2} p_{Er}(k_A, k_B) \\ &= \left(1 - \frac{\lambda}{2}\right) p_{PDC}(k_A, k_B) + \frac{\lambda}{2} p_{PDC}(k_A)\, p_{Er}(k_B). \end{aligned} \tag{4.36}$$

The mutual information $I(k_A, k_B)$ can be estimated from $p(k_A, k_B)$ with numerical methods. Since Eve can learn from the public channel the measurement basis that Alice chose, the mutual information between Alice and Eve is

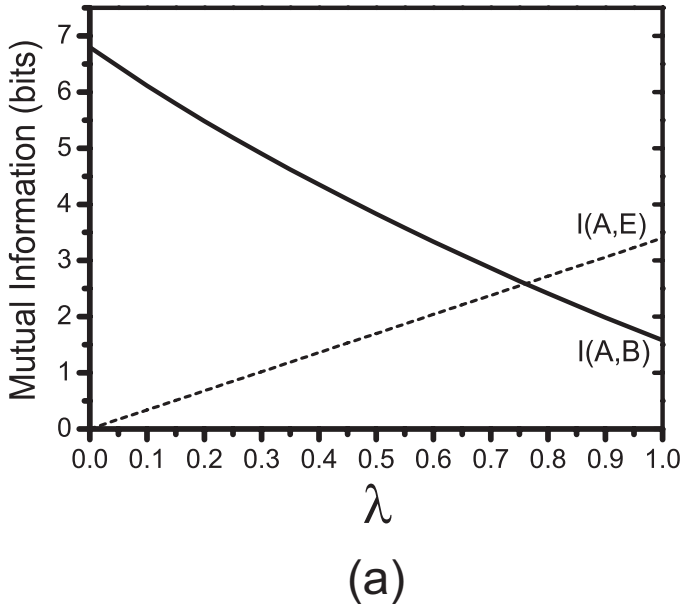
$$I(A, E) = \frac{\lambda}{2} I_{PDC}(k_A, k_E) + \frac{\lambda}{2} I_{PDC}(k_A, r_E) \approx \frac{\lambda}{2} I_{PDC}(k_A, k_E). \tag{4.37}$$

If Eve cannot learn Alice's measurement basis, $I(A,E)$ should be estimated from $p_{PDC}(k_A,k_E)+p_{PDC}(k_A,r_E)$ and is smaller than what is given in Eq. 4.37. This is due to the fact that by revealing their measurment basis, the legitimate parties leak additional information to Eve.

The mutual information when Alice and Bob both measure the position of the photons can be calculated in the similar way. Fig. 4.9(a) shows the calculated $I(A,B)$ and $I(A,E)$ with a type-I PDC source generated from a 2 mm-thick BBO crystal with a 2 mm pump beam waist. It can be seen that $\Delta I = I(A,B)-I(A,E) \geq 0$ for $\lambda < 76\%$, which is the limit that allows Alice and Bob to draw a secure key with forward reconciliation. However, Fig. 4.9(b) shows the EPR criterion (Eq. 4.22), which proves that Eq. 4.22 is only a sufficient condition for security, since for a non-Gaussian attack, it is possible to draw the secure key when this condition is violated.

For reverse reconciliation, the secret key rate is determined by $\Delta I = I(A,B) - I(B,E)$. We expect $I(B,E)$ should be sightly higher than $I(A,E)$, since for each photon that Eve intercepts and resends to Bob, their measurement results should be perfectly correlated when they measure the same variable. Therefore the secret key rate should be slightly lower for the reverse reconciliation than forward reconciliation.

As mentioned previously, although Eve's best strategy is to remove the experimental imperfections, the disturbance introduced by Eve should not exceed what is expected by Alice and Bob from the experimental imperfections, otherwise she will reveal her presence. If she intercepts and resends λ of the photons, there is a $1-\lambda/2$



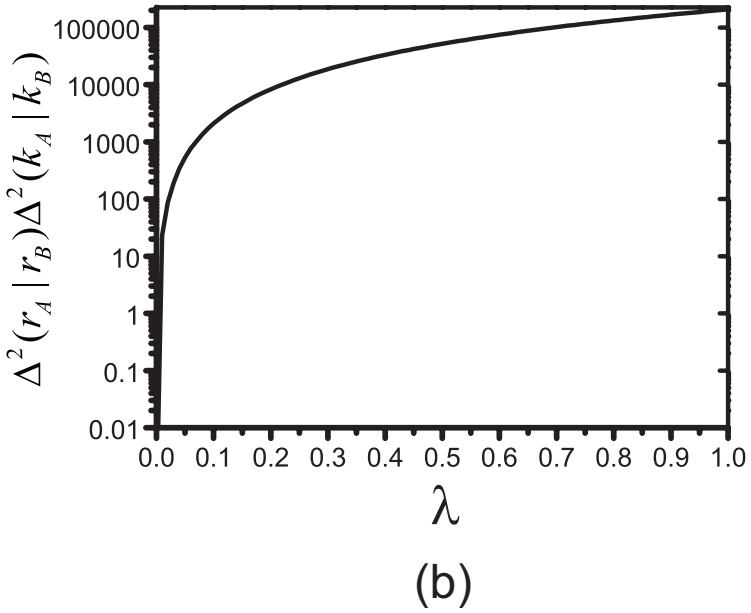


Figure 4.9 (a) Mutual information between Alice and Bob (I_{AB}), and that between Alice and Eve (I_{AE}) in terms of λ. (b) The product of position-momentum variance in Eq. 4.22 in terms of λ. The entangled photons are generated by a 2mm thick BBO crystal and the spot size of the pump is 2mm.

chance she appears as an undisturbed channel, and Alice and Bob's measurement results have the same distribution as if they both detect a photon from a PDC pair (the situation with probability $P(p,p)$ in Sec. 4.3.2); while there is a $\lambda/2$ chance Eve introduces uncorrelated results between Alice and Bob, which is exactly same situation as when Alice detects a photon and Bob has a dark count (the situation with probability $P(p,d)$ in Sec. 4.3.2). By balancing the disturbance introduced by Eve with the background noise, which originates from experimental imperfections, we find the maximum allowed intercept-resend ratio for Eve satisfies the condition

$$\frac{1-\lambda_{max}/2}{\lambda_{max}/2} = \frac{P(p,p)}{P(p,d)}. \tag{4.38}$$

Substituting Eqns. 4.29 and 4.31 into Eq. 4.38, we have

$$\lambda_{max} = \min\left\{\frac{2n}{\left(\frac{1}{l}-1\right)\left(\frac{1}{P_{dark}}-1\right)+n}, \quad 1\right\} \tag{4.39}$$

where $l = 1 - t\eta$ is the channel loss and n is the number of detectors. For a lossless channel ($l = 0$) or noiseless detectors ($P_{dark} = 0$), $\lambda_{max} = 0$, *i.e.* no eavesdropping is possible; while for fixed l and P_{dark}, λ_{max} increases with n. Eq. 4.39 clearly shows how the experimental imperfections open loopholes for Eve to attack.

The analysis for the intercept-resend attack shows that the minimum secret information that Alice and Bob are able to distill ($\Delta I^{min} = I_{AB}^{min} - I_{AE}^{max}$) can be directly estimated from λ_{max}. Combining this analysis and Eq. 4.39, we are able to estimate ΔI^{min} for a given channel transmission loss, which is shown in

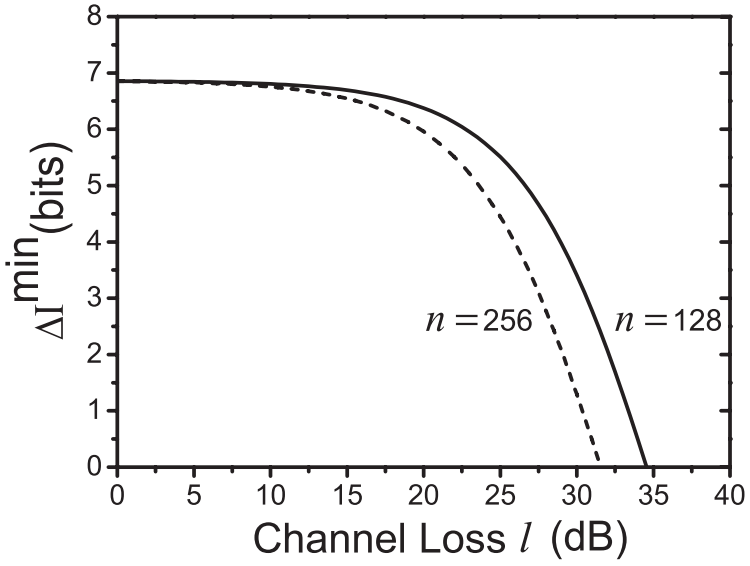


Figure 4.10 The minimum secret information per recorded photon pair (ΔI^{min}) is estimated numerically from λ_{max}. The corresponding channel loss l is calculated from Eq. 4.39. The initial entangled photons are generated by a 2mm-long BBO crystal and a pump at 400nm with 2mm beam waist.

Fig. 4.10. Comparing this result with those of the variance product analysis in Sec. 4.3.2 (4.4dB(1.7dB) for $n = 128(256)$), it is evident that the secure loss level (35dB(31.5dB) for $n = 128(256)$) is significantly improved for this eavesdropping strategy.

4.3.4 Entanglement and security

An important question in quantum cryptography is the relationship between entanglement and security. It has been proven that distributed entanglement between Alice and Bob is a necessary precondition for successful secret key distribution [25]. Also connections between quantum and secret correlations have been established [24]. Nevertheless it is still not clear how to draw a secure key from distributed entanglement, though there are several suggested protocols for particular situations [23,182]. For classical privacy amplification (forward or reverse reconciliation), the security limit is usually a stronger condition than the entanglement threshold [183]. As an example, we recall that the condition for security under a Gaussian attack is that the variance product should be no larger than 1/4 (the EPR criterion in Eq. 4.23), while the entanglement threshold is 1 (the entanglement witness in Eq. 2.45). We show that this is also the case for intercept-resend attack.

We start by considering the bipartite state shared between Alice and Bob. Denote the PDC state as

$$|\Psi_{PDC}\rangle = \int dk_s dk_i \, f(k_s, k_i)|k_s, k_i\rangle \tag{4.40}$$

where $f(k_s, k_i)$ is given by Eq. 2.27. Here we ignore the higher photon number components, since we assume this the PDC process is weak ($P_{PDC} = 0.01$).

When Eve does not apply measurement on the photon sent to Bob, *i.e.* she does not intercept and resend the photon, the state between Alice and Bob is

$$\rho_{AB|nE} = |\Psi_{PDC}\rangle\langle\Psi_{PDC}|. \tag{4.41}$$

If Eve measures the momentum k_i of the photon meant for Bob, and resends a photon in the state $|k_i\rangle$ to Bob, then the photon sent to Alice is projected into the state

$$|\Psi_{A|k_i}\rangle = \frac{1}{\sqrt{\int dk_s |f(k_s, k_i)|^2}} \int dk_s \, f(k_s, k_i)|k_s\rangle, \tag{4.42}$$

where the factor in front of the integration is required for normalization. Thus the joint state of Alice and Bob is

$$\rho_{AB|Ek} = \int dk_i \, p(k_i)|\Psi_{A|k_i}\rangle\langle\Psi_{A|k_i}| \otimes |k_i\rangle\langle k_i|, \tag{4.43}$$

where

$$p(k_i) = \int dk_s |f(k_s, k_i)|^2, \tag{4.44}$$

is the probability distribution of Eve's measurement result. State $\rho_{AB|Ek}$ is a separable state which contains no quantum correlations (entanglement) between Alice

and Bob. Substituting Eqns. 4.42 and 4.44 into Eq. 4.43, we have

$$\rho_{AB|Ek} = \int dk_i \int dk_s \int dk'_s \, f(k_s, k_i) f^*(k'_s, k_i) |k_s\rangle\langle k'_s| \otimes |k_i\rangle\langle k_i|. \tag{4.45}$$

Similarly, if Eve measures the position r_i of the photon sent to Bob, and resends a photon in state r_i to Bob, the joint state of Alice and Bob is

$$\rho_{AB|Er} = \int dr_i \int dk_s \int dk'_s \, \tilde{f}(k_s, r_i) \tilde{f}^*(k'_s, r_i) |k_s\rangle\langle k'_s| \otimes |r_i\rangle\langle r_i|, \tag{4.46}$$

where

$$\tilde{f}(k_s, r_i) = \mathcal{F}_{k_i}\left[f(k_s, k_i)\right] = \int dk_i \, f(k_s, k_i) e^{ik_i y_i}, \tag{4.47}$$

is the Fourier transform of $f(k_s, k_i)$ over k_i. Substituting Eq. 4.47 into Eq. 4.46, we have

$$\begin{aligned} \rho_{AB|Er} \quad = \quad & \int dk_s \int dk'_s \int dk_i \int dk'_i \int dk''_i \, f(k_s, k_i) f^*(k'_s, k'_i) |k_s\rangle\langle k'_s| \\ & \otimes |k''_i\rangle\langle k''_i + k'_i - k_i|. \end{aligned} \tag{4.48}$$

The state $\rho_{AB|Er}$ is also a separable state.

Combining these three situations, the overall state shared by Alice and Bob is

$$\rho_{AB} = (1-\lambda)\rho_{AB|nE} + \frac{\lambda}{2}\rho_{AB|Ek} + \frac{\lambda}{2}\rho_{AB|Er}. \tag{4.49}$$

Note that although ρ_{AB} is expressed in terms of k_s and k_i, it is independent of the

variables that Alice and Bob choose to measure.

To analyse the entanglement of ρ_{AB}, we resort to the logarithmic negativity discussed in Sec. 1.2.2 (Eq. 1.15). To estimate the negativity of a continuous variable state, we need to calculation of the Wigner function of the state. This is difficult for ρ_{AB} in practice. Therefore, instead of calculating the exact value of negativity, we try to bound it from below by decomposing the state into a $N \times N$ basis

$$|mn\rangle = \int_{k_s^m}^{k_s^{m+1}} dk_s \int_{k_i^n}^{k_i^{n+1}} dk_i \, g_{mn}(k_s, k_i), |k_s, k_i\rangle, \tag{4.50}$$

where

$$k_s^m = -k_0 + (m-1)\Delta k \qquad m = 1, 2, \cdots N, \tag{4.51}$$

$$k_i^n = -k_0 + (n-1)\Delta k \qquad n = 1, 2, \cdots N, \tag{4.52}$$

$$\Delta k = \frac{2k_0}{N}. \tag{4.53}$$

Here k_0 is selected so that $[-k_0, k_0] \otimes [-k_0, k_0]$ covers the majority of the momentum distribution of the signal and idler photons, *i.e.* $|f(k_s, k_i)|$ is negligible if (k_s, k_i) is outside this area.

The decomposition should not increase the amount entanglement in the original state. To guarantee this, $g_{mn}(k_s, k_i)$ is factorable in the sense that $g_{mn}(k_s, k_i) = u_m(k_s)v_n(k_i)$. Again, we should emphasize that with this decomposition we calculate a lower bound instead of the exact value of negativity. The decomposition can be

considered as Alice and Bob projecting their local states into

$$|\psi_m\rangle = \int_{k_s^m}^{k_s^{m+1}} dk_s \, u_m(k_s)|k_s\rangle, \tag{4.54}$$

and

$$|\phi_n\rangle = \int_{k_i^n}^{k_i^{n+1}} dk_i \, v_n(k_i)|k_i\rangle, \tag{4.55}$$

i.e., they apply the operator

$$\Lambda = \sum_{m=1}^{N} \sum_{n=1}^{N} |\psi_m\rangle\langle\psi_m| \otimes |\phi_n\rangle\langle\phi_n| \tag{4.56}$$

on state ρ_{AB}. Since Λ belongs to the class of local operations and classical communications (LOCC), the decomposition does not increase the amount of entanglement [184].

For simplicity, we choose $u_m(k_s) = v_n(k_i) = 1/\Delta k$. The elements of the discretized density matrix ρ_d is given by

$$\rho_{mn,op} = \langle mn|\rho_{AB}|op\rangle. \tag{4.57}$$

The partial transpose $\rho_d^{T_B}$ required to calculate the logarithmic negativity can be acquired by

$$\rho_{mn,op}^{T_B} = \rho_{mp,on} \tag{4.58}$$

and the Logarithmic Negativity can be calculated with Eq. 1.15.

We numerically calculate ρ_d and $E_{\mathcal{N}}(\rho_d)$ for $N = 2$ and $N = 4$, which is shown in Fig. 4.11. The PDC source considered here has the same configuration as that in Sec. 4.3.3. With $N = 4$, we already see that the state shared between Alice and Bob remains entangled until $\lambda = 1$. Recall that classical privacy amplification requires $\lambda < 76\%$ to draw a secret key. This shows that the detection of entanglement is not a sufficient condition for security with privacy amplification under intercept-resend attacks.

Entanglement purification[15] and advantage distillation[78] exceed privacy amplification in the sense that they may be able to employ the full potential of entanglement. But they are either very difficult to implement with current technology or have very low efficiency. Hence for a practical QKD scheme, the detection of entanglement may not be enough for secret key distillation.

4.4 Summary

To conclude, we have shown the potential to transfer more than one bit of information per photon through the spatial properties of entangled photon pairs. This result enables single-photon continuous-variable quantum cryptography. Due to the special non-Gaussian distributions of Alice and Bob's measurement results, the options for eavesdropping are quite limited. A detailed security analysis of a plausible attack, intercept-resend, shows that this protocol increases the secret key rate for mid-range transmission distances. Whether Eve gains advantages by means of more powerful attacks requires further study. However, it is clear that Gaussian attacks, optimal

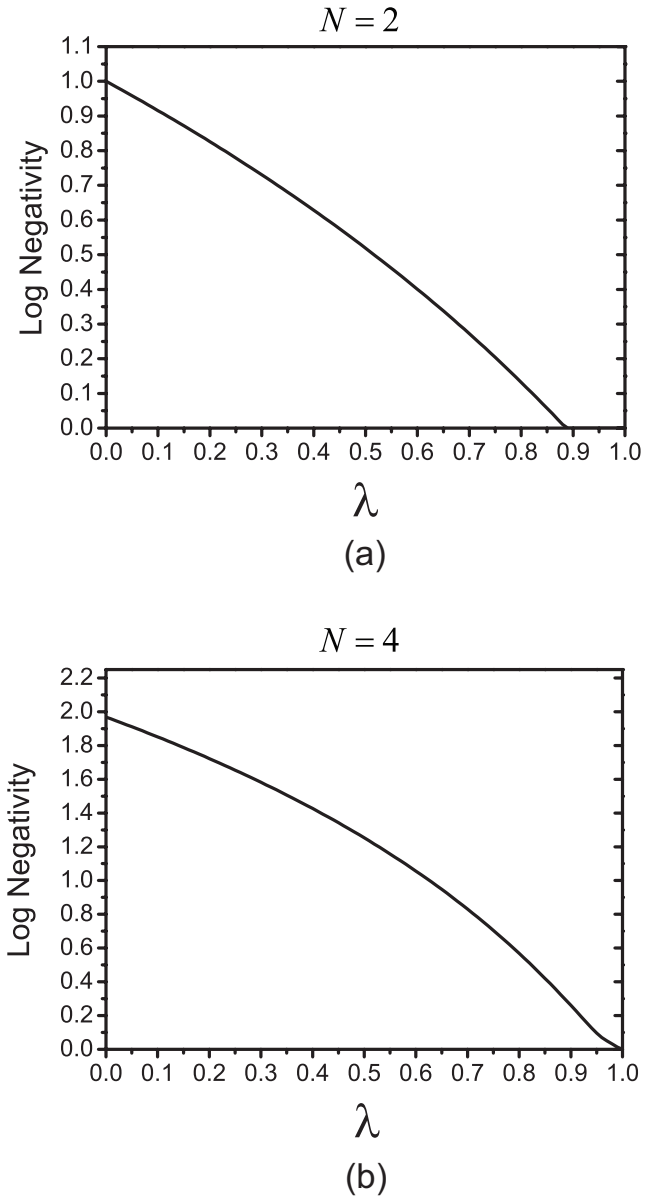


Figure 4.11 The calculated Logarithmic Negativity for the state shared between Alice and Bob after a intercept-resend attack. The initial entangled photons are generated by a 2mm-long BBO crystal and a pump at 400nm with 2mm beam waist.

for quadrature-based CV-QKD, are not optimal here. Refinement of the security analysis should take into account of turbulence effects for free space transmission, which will give Eve more options to attack.

Chapter 5

Characterization of Spatially-Multiplexed Photodetectors at the Single-Photon Level

Photons have a rich structure associated with their continuous variable (CV) degrees of freedoms: spectral (time-frequency) and spatial (position-momentum), as discussed in the previous chapters. This structure plays an important role in photonic quantum technologies, such as quantum information processing or quantum enhanced precision measurement. The manipulation and measurement of the spatial or spectral properties of photons requires experimental setups and detection

devices that differ from those commonly used in the optics laboratory. For the spectral degree of freedom, one requires nonstationary optical elements, such as shutters, phase modulators and especially detectors whose response time is in the femtosecond-picosecond range, which is much faster than those generally available. Such devices are difficult or impossible to build with current technology. On the other hand, optical elements with the analogous high spatial and angular resolutions are readily available, which makes spatial properties easier to manipulate. As dicussed in Sec. 4.3.2, to access the full potential of the continuous spatial variable a large array of detectors should be used to ensure high spatial resolution. Each detector in the array should have single-photon sensitivity enabling detection of individual light quanta, sufficiently high quantum efficiency and spatial resolution, and low noise (a more quantitive analysis is given in Sec. 5.1. Such a detector array has emerging applications in quantum imaging[122] and spatially multiplexed photon-number-resolving detection[185]. Some candidate detector arrays include the multi-pixel photon counter (MPCC), the avalanche photodiode (APD) array[185] and the charge coupled device (CCD). Among these options the CCD provides the largest potential number of pixels due to the relatively developed fabrication technology. There have been some experimental demonstrations[186,187] using an intensified CCD (ICCD) to detect the spatial location of single photons, which show the pairwise correlations between the signal and idler photons from PDC states. ICCD amplifies the input signal with an image intensifier, which converts the input photons into photoelectrons, amplifies them through a micro-channel plate (MCP),

converts the amplifed electrons back to photons and guide them to the CCD chip through a fiber optic coupler or a lens. This process limits the detection efficiency and spatial resolution of ICCDs. Recently another CCD for low light level detection has been developed. This CCD, the electron multiplying CCD (EMCCD), is expected to possess higher quantum efficiency and spatial resolution than the ICCD, though it also has its own defects.

Although the EMCCD has already been employed in astronomy [188] for low light level sensing, there is still no complete description of its performance in quantum optics applications, especially experiments that use non-classical light sources (*e.g.* single photons). In this chapter we develop methods to test the crucial parameters of a detector array in this exacting region and implement these tests experimentally. The light source employed in our experiments generates spatially entangled photon pairs by means of parametric downcoversion (PDC). We describe an experiment to use a detector array to characterize the spatial correlations of this source. The measurement results reveal the feasibility and limits of such a detector array when the input light level is single or a few photons. In particular we apply these tests to a typical EMCCD camera.

This chapter is organizes as follows: in Sec. 5.1 we discuss several crucial parameters of a detector array for single-photon detection, in Sec. 5.2 we introduce the principle of EMCCD operation. The details of the experiment setup is provided in Sec. 5.3. The tests of the major characteristics of a EMCCD camera with this setup are described in Sec. 5.4. In Sec. 5.5 we develop a model to measure the spatial

correlations of the PDC state with a detector array, and compare experiment results acquired with the EMCCD camera with numerical simulations.

5.1 General requirements for a single-photon detector array

To employ a detector array for low-light level, *e.g.* few photons detection, the detector array should possess several properties. Here we discuss several important requirements that such a detector array should possess for low-light level (one to few photons) detection.

5.1.1 Single-photon sensitivity

For a standard photodetector, each input photon has a chance to generate a photoelectron, with a probability determined by the quantum efficiency of the detector. However, due to the peripheral electronics, the detector unavoidably has some noise, which has a root mean square (RMS) error on the order of several to tens of electrons with current technology. This error is difficult to reduce below sub-electron levels even with cooling (superconducting photon detectors have much lower noise, but they are not widely available). Therefore with standard detectors, in order to recognise a single-photon event requires one to distinguish a photoelectron from a noise fluctuation with a RMS noise of several electrons, which is not feasible. To overcome this difficulty, some detectors amplify the photoelectron with an internal gain before it passes through the readout circuits. This can be achieved by impact

ionization (also known as the avalanche effect) in avalanche photodiodes (APDs) or secondary emission in photomultiplifier tubes (PMTs)[189]. If the internal gain is sufficiently large (10^2 – 10^6 for APDs, and up to 10^8 for PMT), the amplitude of the single-photon event will exceed the readout noise, and thus enable one to be distinguish single-photons.

5.1.2 Noise performance of a detector array: spurious charges

As mentioned in Sec. 5.1.1, a photodetector with internal gain is able to overcome most of the noise of normal detectors, but it also introduces a new source of noise: spurious charges may be generated ahead of the internal gain. For example, dark counts of APDs, which are due to the thermal generation of electron-hole pairs inside the semiconductors. These spurious charges will also experience internal gain, and thus can hardly be distinguished from the photoelectron generated by the input photon. The false detection events caused by these spuriou charges increase the error rate in the measurement of the properties of quantum light. As discussed in Sec. 4.3.2, for detector arrays, this problem can be more severe, for these dark counts scales rapidly with the number of detector pixels. Assume the probability to generate a spurious charge on one pixel of the array within a specified time period is P_{dark}. If the pixels are identical and independent with each other, then the probability to generate one spurious charge within n pixels is $nP_{dark}(1-P_{dark})^{n-1} \approx nP_{dark}$ when $P_{dark} \ll 1$. For the cases that no more than one photon is incident onto the detector array within the specified time period, increasing the number of pixels n

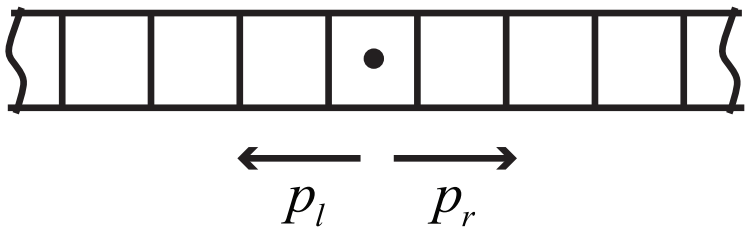


Figure 5.1 A schematic showing the 1D random walk of the electrons in a detector array.

will decrease the signal to noise ratio. A rough requirement is $nP_{dark} < \eta_{pixel}$, or $n < \eta_{pixel}/P_{dark}$, where η_{pixel} is the quantum efficiency of a pixel. This sets a limit for the size of the useful area of the detector array.

5.1.3 Crosstalk

For an ideal detector array, each pixel should act as an independent detector. However, for an integrated detector array, there is a possibility for signal leakage between different pixels due to scattering in the optical window, peripheral circuit noise, *etc.* This will cause crosstalk between different pixels and introduce additional error in the detection process. In particular, for a single-photon input, this will increase the uncertainty in the position measurement of input photon, and reduce the spatial resolution of the detector array.

The actual crosstalk behavior of a specific detector array depends on its design and contruction. Here we consider a simple model to show how it affects detection performance. Suppose that after one photo-electron is generated in a pixel of the detector array, it will experience several steps of random walks between adjacent

pixels before it is read out. The number of steps N is decided by the readout time and pixel transition time. For simplicity, the random walk is assumed to be one dimenstional, *i.e.*, during each step, the electron can move either to the left pixel, to the right, or stay at the same pixel, with probability p_l, p_r and $1-p_l-p_r$ respectively (Fig. 5.1). Define the original pixel to be the 0th pixel and the right to be positive direction, after N steps, the probability that the electron appears in the dth pixel is

$$P_{rm}(d) = \begin{cases} \sum_{n_r=\max\{d,0\}}^{\min\{N,\frac{N+d}{2}\}} \binom{N}{2n_r-d}\binom{2n_r-d}{n_r} p_r^{n_r}\, p_l^{n_r-d}\,(1-p_r-p_l)^{N+d-2n_r} & \text{for } |d| \le N \\ 0 & \text{for } |d| > N \end{cases} . \tag{5.1}$$

The mean value of d is $\mu(d) = N(p_r - p_l)$, and the variance is $\delta(d) = N(p_r + p_l) - N(p_r - p_l)^2$. So the position of each photo-electron will be displaced by $\mu(d)$ with an uncertainty $\sqrt{\delta(d)}$. When $p_r = 0$, equation 5.1 becomes a binominal distribution, which describes the charge transfer efficiency (CTE) issue of CCD arrays [190] (the noise when the charge in one pixel are moved to an other, see Sec. 5.5.3 for details). Fig. 5.2 shows two examples of the distribution $P_{rm}(d)$. Practical detector arrays usually have very low crosstalk for strong light input, *e.g.* for a typical CCD camera with a large charge packet (> 1000 electrons), p_l is below 0.00001 [190]. However, for low illumination levels, crosstalk may not be negligible due to the nonlinear relation between the CTE and the intensity of the charge packet [190].

In this section we discussed several parameters that are crucial for the performance of a detector array with low-light level input. In the following sections we will calibrate these parameters of a particular detector array, a EMCCD camera,

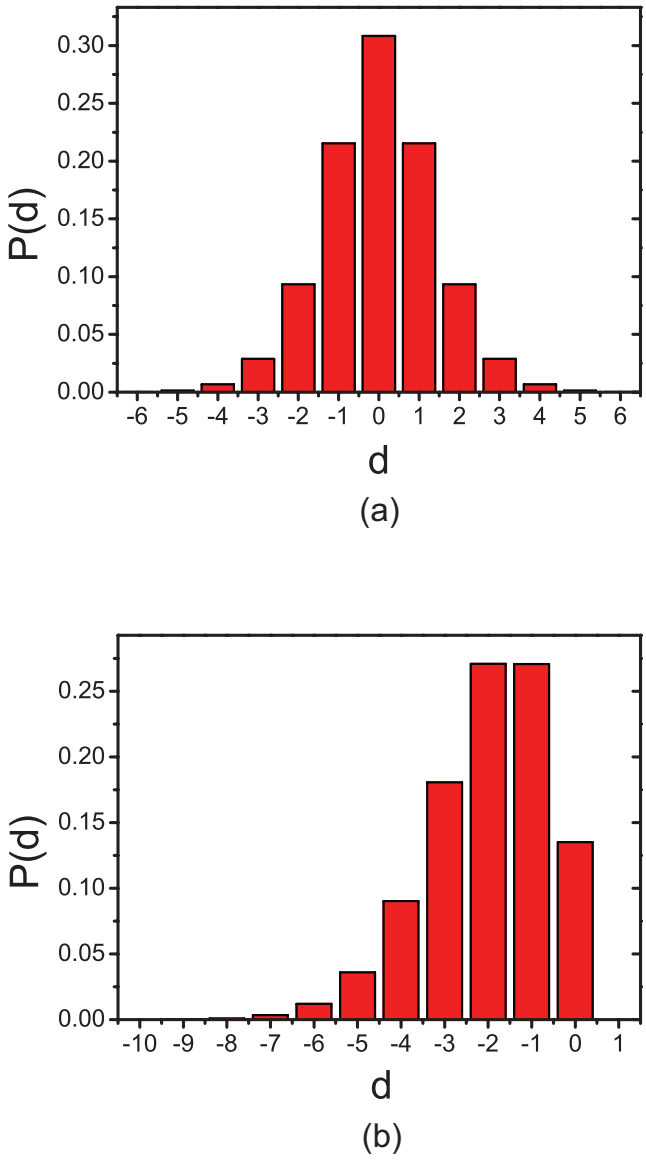


Figure 5.2 Probability of the crosstalk $P(d)$ after $N = 1000$ steps of random walk. (a) Symmetric random walk with $p_r = p_l = 0.001$. (b) Unsymmetric random walk with $p_r = 0$ and $p_l = 0.002$.

and show their impact experimentally.

5.2 Principle of EMCCD operation

A CCD image sensor can be considered as an array of photoactive capacitors (pixels). When an image is projected on a CCD array, an electric charge packet is created in each pixel with total charge proportional to the light intensity incident on that pixel. Once the exposure is done and the charge is accumulated, a control circuit causes the charges to be transferred from one pixel to the next. To accomplish the charge transfer a CCD is usually designed as three-phase device. Fig. 5.3 schematically shows how such a device works. Each pixel of the CCD consists of three gates (electrodes), each of which connects to phase (voltage)-1, -2 and -3 clocks ($\phi 1$, $\phi 2$ and $\phi 3$ in Fig. 5.3). During the charge collection, *i.e.* exposure period, one phase ($\phi 1$) is biased low and the other two phases ($\phi 2$ and $\phi 3$) are biased high, forming potential wells. Charges generated during exposure are collected in these wells. To transfer the charges from one pixel to another, the phases are controlled with different clock signals. For the situation described in Fig. 5.3, the charges are collected during time t_1. At time t_2 charge transfer commences. The $\phi 2$ clock is biased low, forming the same well as $\phi 1$. Thus the charges diffuse into two wells. During t_3, the $\phi 1$ clock goes high, which forces charges to transfer to the $\phi 2$ phase. From t_1 to t_3, $\phi 3$ is kept high as a barrier between different pixels. During t_4 and t_5, the charges are transferred from $\phi 2$ to $\phi 3$. This process is repeated. At t_7 the charges have been transferred through 3 phases, *i.e.* from one pixel to its neighbour,

completing a period of charge transfer.

There are three architectures for scientific CCDs: interline, full frame transfer and frame transfer. The EMCCD we employ has a frame transfer structure, which will be discussed briefly. The details of the other two architectures are beyond the scope of this thesis. The structure of a standard frame transfer (FT) CCD consists of an image area, a storage area, a shift register and an output amplifier (a structure similar to that shown in Fig. 5.4 but without the gain register). Usually the image area and the storage area are two halves of the same CCD chip which have exactly the same number of pixels and are independently clocked. The storage area is optically opaque and masked. During the exposure time a number of incoming photons hit the image area. A fraction of these, given by the quantum efficiency of the sensor chip, each generate a photo-electron. Once the exposure time has elapsed, the accumulated charges are rapidly transferred to the storage area, and then transferred vertically, line by line, to the horizontal shift register. From here the charges are transferred horizontally to the output amplifier. An EMCCD has the same structure, but with the shift register extended to include a section called the gain register (see Fig. 5.4). The gain register is similar to the shift register; it contains a three-phase structure (see Fig. 5.4(a)) that is driven with a sequence of clocks to move the charges from one register element to the next. The difference is that in a gain register element one of the three phases ($\phi 2$ in Fig. 5.4) is a high-voltage pulse (typically 40 - 60 volts)[191,192]. Due to this high electric field the electrons transferred from $\phi 1$ to $\phi 2$ can experience impact ionization (or avalanche

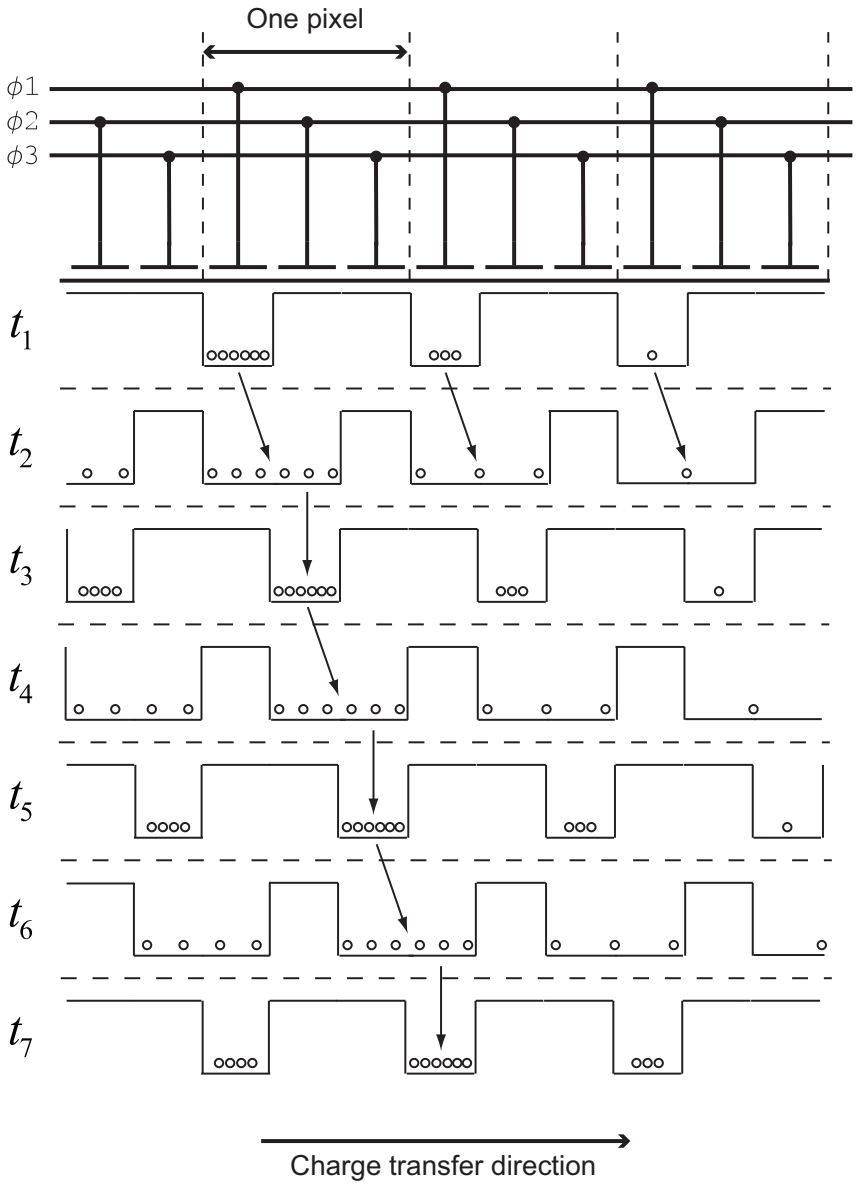


Figure 5.3 A schematic showing how the three-phase structure works to transfer charges. By adjusting the clock signal on each phase ($\phi 1$, $\phi 2$ and $\phi 3$), the charges can be transferred from one pixel to another.

multiplication). This impact ionization increases the number of electrons in the charge packet and adds noise. The gain per stage g is actually quite small, only around 1.01 to 1.015. However, with a large number of stages N, a substantial total mean electron multiplication (EM) gain $G = g^N$ can be achieved. For example, with $N = 520$ and $g = 1.015$, a total gain of over 2300 can be reached. To ensure good dynamic range (the maximum signal that can be detected or the full well capacity) and gain stability (the higher the gain, the greater the noise added to the amplified signal due to the voltage fluctuations), the actual gain is normally chosen to be no greater than 1000.

For a conventional CCD without a gain register, the detection limit of the input signal intensity is largely determined by the readout noise introduced by the output amplifier, whose variance σ_{read} varies between a few to tens of electrons depending on the readout rate. The multiplication process in an EMCCD applies internal gain via the gain register to the signal prior to the output amplifier, which acts to reduce the effective readout noise to levels smaller than one electron RMS. This makes single photo-electron detection possible. Ideally the same gain would be applied to every electron that passes through the gain register. Unfortunately due to the stochastic nature of the multiplication process this is not a one-to-one mapping between the number of the input and output electrons. Rather, there is a large range in the number of output electrons that can be produced from a given number of input electrons. In general, the probability distribution of the number of electrons, x,

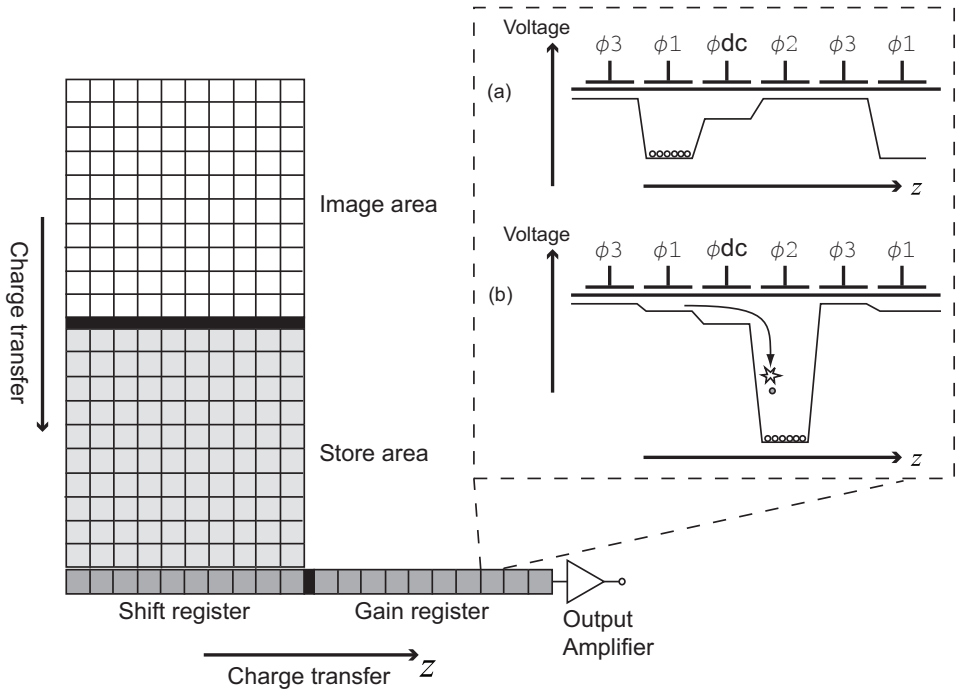


Figure 5.4 Schematic of EMCCD. Charges are driven across the shift and gain register by a sequence of voltage phases. The EMCCD achieves gain by applying a large voltage at phase $\phi 2$ causing an avalanche multiplication of the number of electrons through impact ionization, which is shown in (a) and (b).

after the gain register, given n input electrons, can be approximated by[193]

$$p_{EM}(x|n) = \frac{x^{n-1}\exp(-x/G)}{G^n(n-1)!}. \tag{5.2}$$

Here G is the total mean EM gain associated with the gain register.

Figure 5.5(a) shows $p_{EM}(x|n)$ for up to $n = 4$ with $G = 1000$. The spread in the number of output electrons increases the noise in camera signal and, through this, introduces uncertainty as to how many photo-electrons were at the input. In turn, this introduces uncertainty in the number of photons impinging on the camera. This camera noise is quantified by the excess noise factor (ENF) defined as

$$ENF = \frac{\sigma_{out}}{G\,\sigma_{in}}, \tag{5.3}$$

where σ_{in} and σ_{out} are the standard deviations of the input and output signals. For coherent light input, where the photon number distribution is Poissonian, the ENF tends to $\sqrt{2}$ when the gain is high[191,193]. This can be understood as doubling of the input noise. This noise performance is equivalent to that of a noiseless conventional CCD with half the quantum efficiency. When the input signal level is low, *i.e.*, no more than one photon per pixel on average, the EMCCD can be operated in a photon counting mode. Here any output signal with the number of electrons above some threshold that is much higher than the readout noise, is treated as arising from single-photon detection. Fig. 5.5(b) qualitively shows the probability distributions of the number of electrons after the output amplifier of the EMCCD

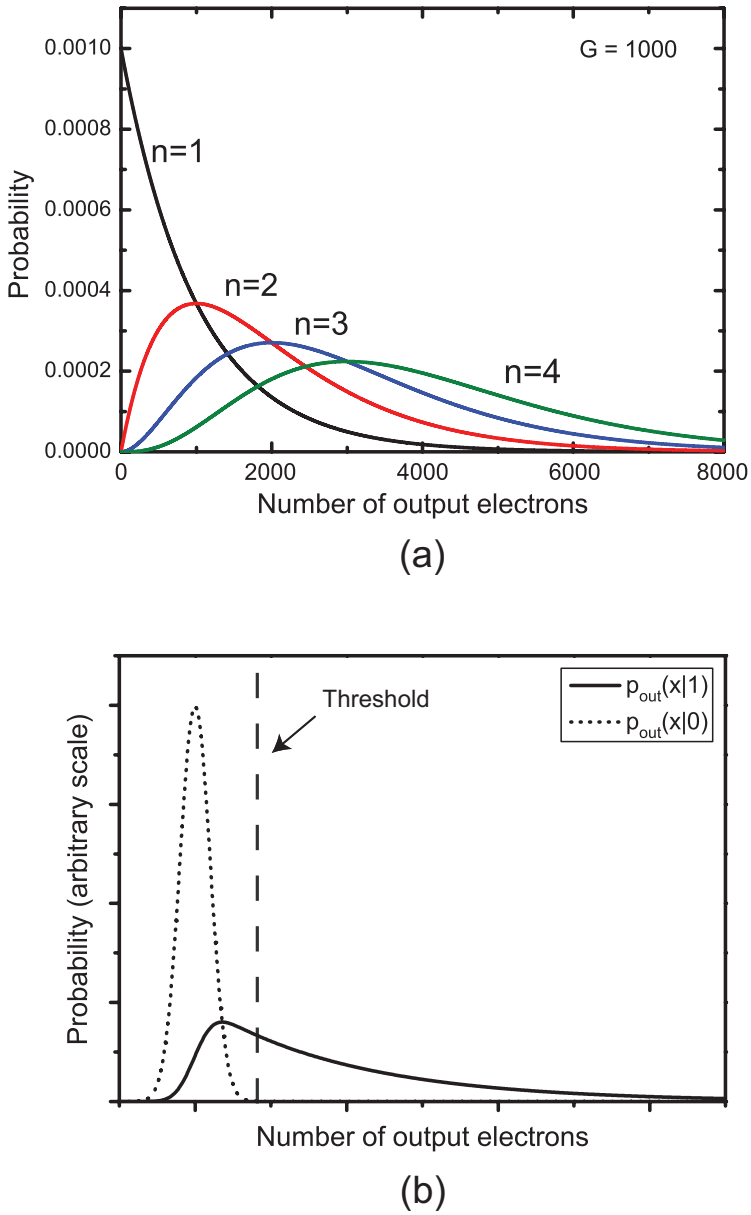


Figure 5.5 Theoretical calculations for (a) the output probability distributions of the EM gain for 1-4 input photo-electrons with $G = 1000$. (b) the probability distributions after the output amplifier for no photo-electron and single photo-electron input. A threshold is used to distinguish between these two events. Figure (b) is schematic and both the axes have arbitrary units.

for two different input events. When there is no photo-electron input (the dotted line), the output consists of the readout noise, which has a Gaussian distribution $p_{out}(x|0)$ with variance σ_{read}. For single photo-electron input (the solid line), the output $p_{out}(x|1)$ is given by the Gaussian readout noise $p_{out}(x|0)$ convolved with the exponentially decaying amplified signal $p_{EM}(x|1)$ for one photo-electron. To distinguish between zero and one input photo-electrons, one sets a signal threshold of $6\sigma_{read}$. Any signal registered above this level is treated as a photo-electron. Therefore the probability that a photo-electron will be detected is

$$P_t = \sum_{x=6\sigma_{read}}^{\infty} p_{out}(x|1) \approx \exp(-\frac{6\sigma_{read}}{G}). \tag{5.4}$$

P_t quantifies the capability of the camera to distinguish between zero and one input photon-electrons. This is the single-photon sensitivity of the camera. The effective quantum efficiency of an EMCCD when operated in this photon-counting mode is

$$\eta_{eff} = \eta P_t, \tag{5.5}$$

where η is the quantum efficiency of photo-electron generation. If the gain is sufficiently high $G \gg \sigma_{read}$, we have $\eta_{eff} \approx \eta$, which shows that the photon-counting operating mode of the detector removes the uncertainty introduced by the electron multiplication process and enables the detector to utilize the full quantum efficiency of the photo-electric conversion. However thresholding does have a drawback. As the input light intensity is increased, there is a growing chance that two photons will be

absorbed by a single pixel. Thresholding will attribute the output signal to at most one photon incorrectly. Basten *et al.* have shown that the photon-counting mode can be applied accurately up to 0.5 photon per pixel[193] for light with Poissonian input photon-number distribution. For the experiments described in this chapter, we maintain the input signal below this level.

5.3 The experimental setup

To examine the feasibility of current array detectors for spatially-resolved single-photon level detection, we performed a series of experiments on an EMCCD camera. The EMCCD camera we employ in our experiments is the Andor iXon DV887DCS-BV X-1223, containing a CCD87 sensor from E2V Technologies. This CCD is commonly used for low-light level applications in astronomy, but as far as we know there is little work describing its performance in quantum optical experiments, especially at the single-photon level. We tested the main characteristics (detection efficiency, noise performance, *etc.*, see Sec. 5.4 for details) of the EMCCD relevant for single-photon detection. The light source we employ is the photon pairs generated from the PDC process.

Fig. 5.6 sketches the experimental setup. The output of a Coherent Compass 405 laser diode module (with a wavelength of 405nm) is spatially filtered and then used to pump a 1mm-long β-barium borate (BBO) crystal to generate the Type-I PDC. The pump power can be adjusted to control the production rate of the PDC light. An interference filter (IF – 810 nm central wavelengh and 6 nm bandwidth) is

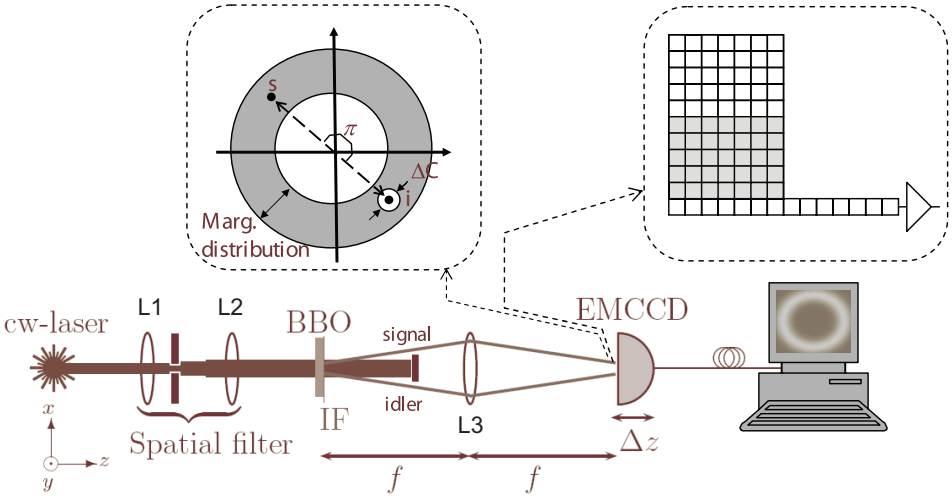


Figure 5.6 The experimental setup to study the spatial correlations of PDC with EMCCD. The downconverted photons propagate through a 2-f imaging system and are detected by the EMCCD camera. The inset shows the distribution of the photons at the detection plane.

used to select degenerate photon pairs which propagate through an imaging system and are detected by the EMCCD camera. Both the distance between the crystal and the imaging lens ($L3$ in Fig. 5.6), and the distance between the imaging lens ($L3$) and camera are set to equal the focal length of the imaging lens f. This 2-f imaging system performs a transverse spatial Fourier transform and maps the transverse momentum $\mathbf{k}^{\perp}$ distribution of the light originating at the crystal into the transverse position $\mathbf{r}$ distribution of the light in the detector plane with $\mathbf{r} = \frac{f}{k}\mathbf{k}^{\perp}$. Here $k = \omega/c$ is the wavenumber of the photon in free space. Hence, the joint distribution $P(\mathbf{r}_s, \mathbf{r}_i)$ of observing a photon at position $\mathbf{r}_s$ with its partner at $\mathbf{r}_i$ is

$$P(\mathbf{r}_s, \mathbf{r}_i) \propto P_{PDC}(\frac{K}{n_o f}\mathbf{r}_s, \frac{K}{n_o f}\mathbf{r}_i), \tag{5.6}$$

where $K = k_s = k_i$ is the wavenumber of the degenerate downconverted photons inside the crystal, n_o is the refractive index of crystal for the ordinary light, and P_{PDC} is the joint probability distribution of the momenta of the signal and idler photons created by the PDC, *i.e.* $P_{PDC}(\mathbf{k}_s, \mathbf{k}_i) = |f(\mathbf{k}_s, \mathbf{k}_i)|^2$, where $f(\mathbf{k}_s, \mathbf{k}_i)$ is the joint probability amplitude of PDC state given in Eq. 2.20. Recall the discussion about the position of photons in Sec. 1.4, $P(\mathbf{r}_s, \mathbf{r}_i)$ can be understood as the probability that a pixel at position $\mathbf{r}_s$ detects one photon and simultaneously a pixel at position $\mathbf{r}_i$ detects the other photon. Similarly, the marginal distribution for the signal photon is given by substituting $\mathbf{k}^{\perp} = \frac{K}{n_o f}\mathbf{r}$ into Eq. 2.36

$$P(\mathbf{r}_s) \propto \exp\left[-\frac{2\gamma L^2 K \Delta k}{n_o^2 f^2}(r_s - n_o f\sqrt{\frac{\Delta k}{K}})^2\right], \tag{5.7}$$

and the same expression is applied to the idler marginal distribution. The marginal distribution in Eq. 5.7 represents a ring with a diameter $D_r = 2n_o f\sqrt{\Delta k/K}$ and width $W_r = n_o f/(L\sqrt{\gamma K \Delta k})$, as shown in the left inset of Fig. 5.6. The conditional distribution can be deduced from Eq. 2.38 and gives

$$P(\mathbf{r}_s|\mathbf{r}_i) \propto \exp\left(-\frac{w_0^2 K^2}{2n_o^2 f^2}|\mathbf{r}_s + \mathbf{r}_i|^2\right). \tag{5.8}$$

The signal and idler photons are diametrically anti-correlated in position. The diameter (the full width at $1/e^2$ maximum) of the conditional distribution is

$$\Delta C \approx \frac{4n_o f}{K w_0}. \tag{5.9}$$

In summary, the position distribution of the photons at the EMCCD surface has the same properties of the momentum distribution of the PDC state discussed in Sec. 2.3, with the mapping condition $\mathbf{r} = \frac{n_o f}{K}\mathbf{k}^{\perp}$. This is shown in the left inset of Fig. 5.6.

It is useful to have the distribution of the PDC photons fit onto the whole area of the EMCCD camera, *i.e.* $D_r + W_r \approx S_{CCD}$, where S_{CCD} is the scale of the EMCCD array. From the parameters given in Sec. 5.4.1, $S_{CCD} = 16\mu\text{m} \times 512 = 8.2\text{mm}$. We choose the phase-matching angle of the PDC process to be approximately 3° (the angle between the downconverted modes and z-axis in free space), and the focal length of the lens to be 5 cm. This gives $D_r \approx 5.2$ mm and $W_r \approx 0.5$ mm.

5.4 Major characteristics of EMCCD

With the setup described in Sec. 5.3, we tested the key characteristics necessary to utilize the Andor iXon DV887DCS-BV X-1223 EMCCD camera in quantum applications. Here we discuss the results of these tests.

5.4.1 General features

Table 5.1 shows some of the main parameters given by the manufacturer, Andor Technology. The vertical clock speed here is actually the vertical shift time for one pixel (recall the three-phase structure). The pixel size and number of pixels define the spatial resolution of the camera, which determine the configuration of PDC setup and the imaging system used in our experiment, as shown in Sec. 5.3. This

will be further discussed in Sec. 5.5 as well. The readout mode, readout rate and clock speed define the temporal resolution of the camera, which will be discussed in Section 5.4.2.

Table 5.1 Values of the major parameters of Andor iXon DV887.

Description	Values
Pixel Size (μm)	16×16
No. of Pixels	512×512
Readout Mode	normal imaging mode, frame transfer mode
Readout Rate	1, 3, 5, 10 MHz
Vertical Clock Speed (μs)	0.4, 0.6, 1, 1.8, 3.4, 6.6, 13
Pre-Amplifier Gain	1×, 2.4×, 4.7×
Cooling Method / Temperature	-75°C/-95°C with air/water cooling
Quantum Efficiency (η)	75% at 810 nm

5.4.2 Time response features

The timing of detectors is an important issue for quantum communications, including quantum cryptography, where it sets the maximum transmitted key rate. It is also important for many quantum optical applications involving conicident detection of multiple photons, *e.g.*, in heralded single-photon sources, bipartite entanglement measurements, violation of a Bell inequality with entangled photon pairs, *etc.* Here, the detector time resolution sets the minimum time window with which the output signal can be gated to eliminate excess noise. For APDs, the time resolution is limited by the avalanche jitter, which is around half a nanosecond, while for a CCD camera, it is limited by either the shutter time or the minimum exposure time. If short enough, the exposure time itself could be used as a coincidence gating circuit

between different pixels, ensuring that two detected photons were likely to have originated from the same emitted pair. Due to the nature of its image intensifier, *i.e.* the adjustable control voltage between the photocathode and the micro-channel plate, the intensified CCD camera can have shutter times as short as a few hundred of picoseconds, which is shorter than the 3ns typically used in standard coincidence counting experiments with APDs. In contrast the EMCCD camera uses an electronic shutter similar to a normal CCD cameras which limits exposure times to no less than a few microseconds.

The Andor iXon DV887 camera can be operated in a non-frame-transfer mode as well as the frame transfer mode, and these have different minimum exposure times. In non-frame-transfer mode, the image area is kept clean from collecting charges until the exposure phase starts (stimulated by an internal or external trigger). When the exposure is done, the charges built up in the image area are quickly transferred to the storage area and read out through the shift register. At the completion of the readout phase, the camera is kept clean from collecting charges again until the next exposure phase starts. The minimum exposure time in this mode is 20 μs and is not related to the other time settings of the camera. A major difference between the frame transfer mode and the non-frame-transfer mode is that in frame transfer mode, apart from the transfer of charges from the image area to the the storage area, the image area is not cleaned between two exposure phases. Unless the previous read out phase is completed, the charges in the image area cannot be transferred to the storage area and the image area is kept exposed. Therefore the

exposure time has a minimum setting limited by the readout time, which is decided by the readout speed, the exposed area of the sensor and the number of pixels binned together. In our experiment the camera is operated in the frame transfer mode. To minimize the noise (see Sec. 5.4.3), the readout speed is set to 1 MHz and the vertical shift speed is chosen to be 0.4 μs. For this configuration the minimal exposure time is 0.02 s, which is much longer than the few nanoseconds typical in coincidence counting. Consequently, if we want to measure spatial correlations of the PDC state, the photon-pair generation rate of the PDC light source should be reduced to minimize the chance that two unpaired photons are detected in the same pixel or diametrically opposed pixels within the 0.02 s exposure time. The Andor camera is also equipped with a mechanical shutter, the operation time of which is tested to be 0.2 s by comparing the exposure level with and without this shutter. For the camera we used we found some synchronization problems between the CCD and the mechanical shutter, and so the shutter is not recommended for use.

5.4.3 Noise performance

Similar to normal CCDs, the noise source of an EMCCD can be divided into off-chip noise (readout noise from the amplifiers, analog-to-digital quantization noise, *etc.*) and on-chip noise. As discussed in Sec. 5.2, when the multiplication gain is sufficiently high, the contribution from off-chip noise is negligible. Excluding the multiplication gain noise as a separate type of noise, the on-chip noise is due to the spurious charge discussed in Sec. 5.1.2, which consists of thermal dark current,

clock-induced charge (CIC) *etc.* (for details, see Ref.[190]). These processes create electrons even when no light is incident on the detector. These electrons are subsequently multiplied as described in Sec. 5.2 and can result in false photon detections. Dark current in an EMCCD has a similar origin to that of the dark counts in APDs mentioned in Sec. 5.2. Its contribution to the signal can be greatly reduced by cooling the camera and keeping the exposure time as short as possible. CIC is generated when the camera is clocked during readout, and so it is mostly determined by the amplitude and frequency of the clock. In principle, CIC will increase slightly with the decrease of the operating temperature[190], but it has been shown that this increase is negligible for an EMCCD[194]. There are several points that a manufacturer needs to consider to minimize CIC when designing the camera, but for a user, there are very limited options and CIC sets the ultimate limit for the performance of EMCCD at low light levels.

To measure the noise performance at the single-photon level of the iXon DV887 camera, we take a number of frames with the camera blocked, *i.e.*, with no input signal. The histogram of the digitized output signal (in A/D counts or digitization numbers (DNs)) of the camera is shown in Fig. 5.7(a). Here the multiplication gain is set to its maximum, the vertical shift speed set to 3.4 μs, readout speed set to 1MHz and a temperature of -75° C. As expected from Sec. 5.2, the noise distribution is a weighted average of the two distributions (readout noise and single-electron events) shown in Fig. 5.5(b). The Gaussian-like peak is solely due to the readout noise (in these events, no on-chip noise source created an electron), while

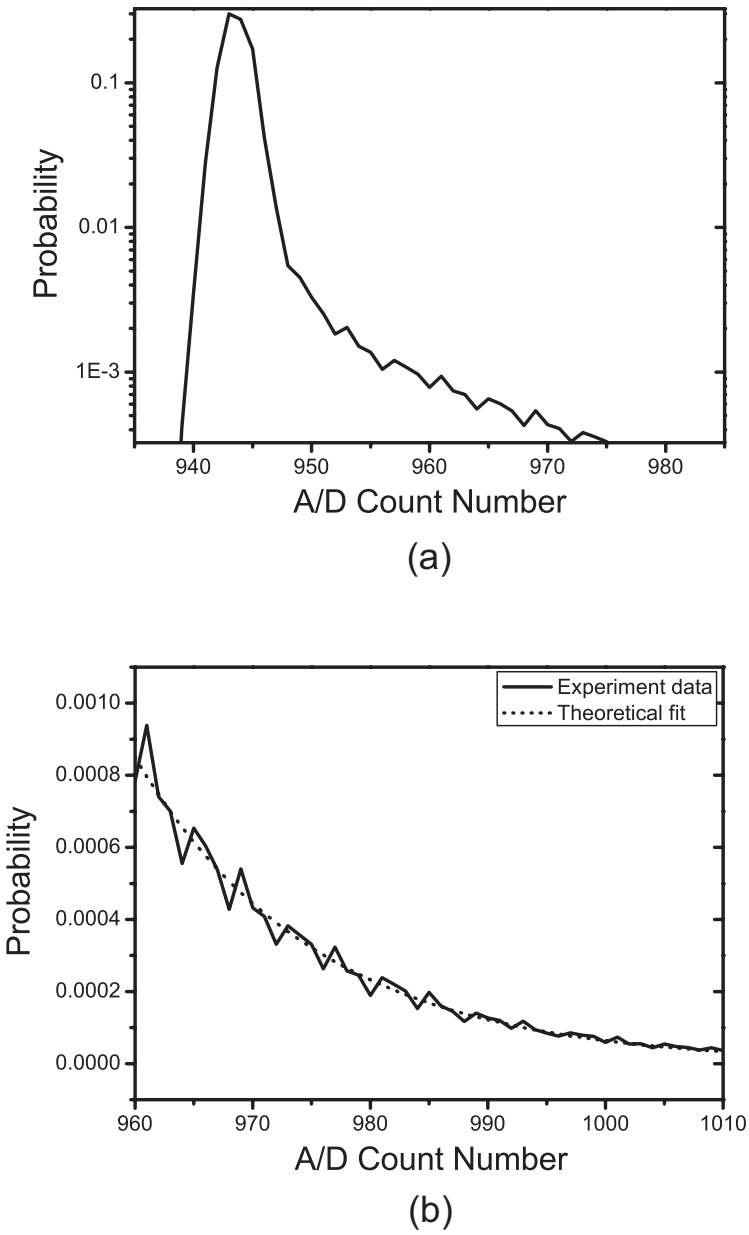


Figure 5.7 The noise performance of the iXon DV887 camera. (a) A histogram of the output digital signal per pixel for 2000 frames with a maximum multiplication gain and no input light. (b) A fit of the tail in (a) to an exponential decay in order to determine the noise contribution from clock induced charge.

the tail in the high DN region is the contribution due to multiplication of single electrons created through on-chip noise. In a careful examination this tail is found to be largely independent of the exposure time indicating it is mostly from the CIC. By examining the width of the peak when the multiplication gain is turned off, the RMS error of the readout noise (σ_{read}) is estimated to be less than 2 DNs. According to the manufacturer, for this readout speed there are 12 electrons per DN. This implies the readout noise is less than 20 electrons/pixel/frame. To estimate the CIC noise, we assume a distribution similar to that of single photo-electrons given by Eq. 5.2

$$p_{cic}(x) = \frac{n_{cic}}{G_{cic}} \exp(-x/G_{cic}), \tag{5.10}$$

where G_{cic} is the mean gain, and n_{cic} is the equivalent number of input electrons per pixel per frame due to CIC. Fig. 5.7(b) shows the fit of Eq. 5.10 to the experimental data in the high DN region (more than $6\sigma_{read}$ away from the Gaussian peak). This gives the evaluation of $n_{cic} = 0.04$ electrons/pixel/frame and $G_{cic} = 180$. The minimum CIC we found for this camera is $n_{cic} = 0.005$ electrons/pixel/frame with vertical shift speed of 0.4 μs and readout speed of 1 MHz, which means there is one false photon detection every 200 pixels per frame. Although every quantum optical application will have different requirements we can use this pixel number as an effective limit on the single-photon-detector array size and, thus as benchmark to compare competing detector arrays.

5.4.4 Multiplication gain

The multiplication gain G can be estimated in a similar way as G_{cic}. Photon pairs generated from a PDC source are used as the input light to the EMCCD camera. The photon-pair generation rate is first set to be high enough to allow the EMCCD camera to image the ring structure of the PDC (Fig. 5.8(a)) during one exposure. An area A_{PDC} of 10×10 pixels is selected around an arbitrary point on the peak intensity circle in the ring. Then the generation rate is lowered to ensure the maximum signal collected in A_{PDC} is much less than one photon per pixel per frame. A histogram of the EMCCD output signal from the pixels in A_{PDC} contains contributions from multiplied photo-electrons, multiplied CIC and the readout noise. We attempt to remove the latter two contributions by first recording histograms of the output signal within A_{PDC}, with and without input light. Each measurement is performed with 2000 exposures. The difference between the two histograms is due to single photon events. We fit an exponential decay function to the tail of the difference between the two histograms (shown in Fig. 5.8(b)) and find that the detected number of photons is 0.152 photon/pixel/frame and the gain is $G = 247$. Comparison between G and G_{cic} shows that CIC noise experiences less gain than input signal. This agrees with our expectation that the CIC will be created at random points in the gain register and, thus pass through fewer multiplication steps on average. This has also been confirmed by S. Tulloch[195].

From the measurement results in Sec. 5.4.3 and 5.4.4 and Eq. 5.4, if the camera is operated in photon-counting mode, the effective efficiency will be reduced by a

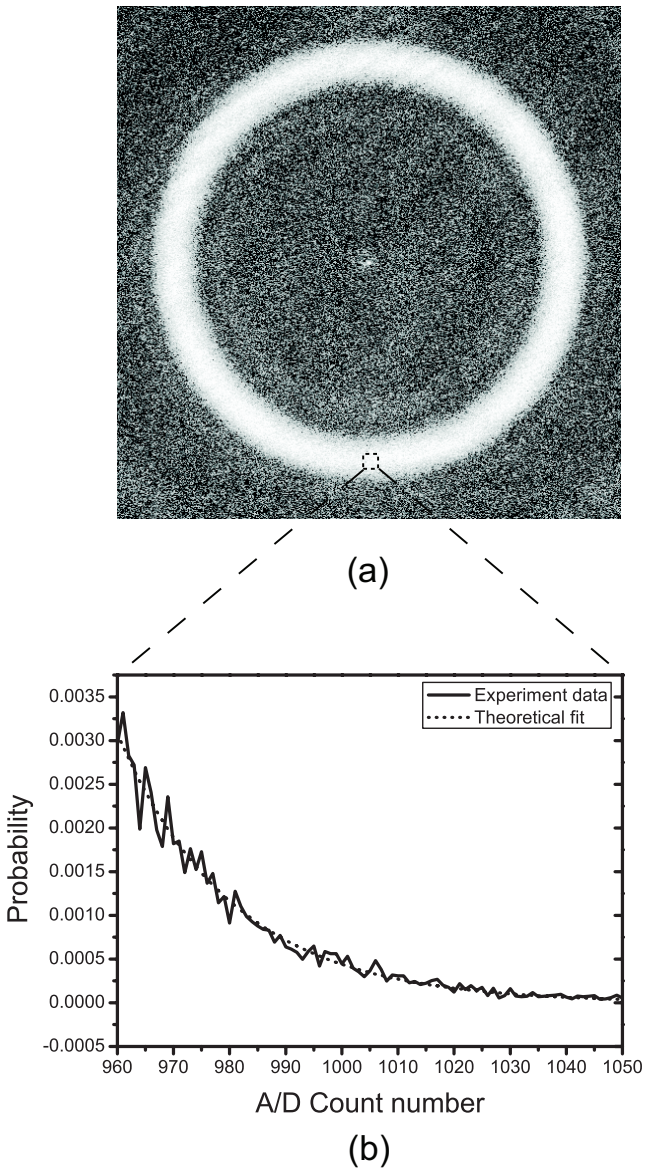


Figure 5.8 Measurement of the EM gain for a single photon input. (a) The ring structure of PDC detected by the EMCCD. An area of 10×10 pixels around the peak intensity is selected to construct an output signal histogram. The histogram is used to determine the EM gain for single input photo-electron. (b) The solid line is the histogram of the output distribution of single photon events. This is fitted with an exponential decay function (the dotted line) to estimate the EM gain and the average number of detected photons per pixel.

factor of $P_t = 0.67$. This rather large reduction is due to the low gain of our particular camera, which might be caused by gain-aging of the EMCCD [196]. For another EMCCD camera that we tested from Hamamatsu, we measured an EM gain of over 1000 and $P_t > 0.9$, which is an evidence of the potentially superior quantum efficiency of a brand new EMCCD operating at its peak.

5.4.5 Comparison between EMCCD and APD

To conclude this section, the detection efficiency of our EMCCD is compared with a standard silicon APD (Perkin Elmer, model no. SPCM-AQR-13-FC 5387.Rev.F). This APD module is the most widely used single-photon detector in quantum optics experiments. The attenuated laser diode pump, Coherent Compass 405 is coupled into a single-mode fiber and used as the input light for both of the detectors. The intensity of the laser is adjusted to give around 18000 clicks per second with the APD. The number of photons detected by the EMCCD is estimated with the method mentioned in Sec. 5.4.4 to be 13662 photons per second, which is close to that from the APD. Considering the additional loss introduced by the coupling into the camera, the intrinsic detection efficiencies η of the back illuminated EMCCD and APD are at the same level, at least for the wavelength we tested (405 nm).

5.5 Characterizing spatial correlations of PDC with an EMCCD array detector

As mentioned in previous chapters, photon pairs generated from PDC exhibit a high degree of correlation in their spatial degree of freedom. In order to experimentally access this degree of freedom requires a large detector array. From the various tests mentioned in Sec. 5.4, the EMCCD has single-photon sensitivity, good quantum efficiency comparable to APDs and relatively low noise. However, it is still unclear whether an EMCCD can be used as a detector array in which each pixel in the camera acts as an independent detector, and thus has the ability to reveal the non-classical spatial correlations of PDC light. In this section we discuss an experiment that employs an EMCCD to characterize the spatial correlations of PDC. The experimental results are compared with a numerical simulation of the EMCCD output signal, including all the factors discussed in Section 5.4. The difference between the experiment and theoretical model reveals the capabilities and limits of the EMCCD camera.

5.5.1 The measurement method

Typical experiments with two-photon states from PDC employ a pair of detectors counting coincidences with nanosecond time gating. This requires the generation of no more than one photon pair within the time-gating window, and a noise level low enough to achieve a reasonable signal to noise ratio. When a detector array, as mentioned in Sec. 5.1.2, is employed, the noise level increases linearly with

increasing number of pixels, which makes it difficult to distinguish the photon pair from background noise. One option to overcome this problem is to employ only a small area of the detector array to keep the noise low. For example, as shown in Sec. 5.4.3, the tested EMCCD has a CIC level no less than 0.005 electrons/pixel/frame. When this camera is used to measure the spatial correlations of the PDC state by using only a select group of pixels, the effective area should be much smaller than 200 pixels to obtain a sufficient SNR. However, there is always some advantage to employ the full area of the detector array. For example, with an increased number of detectors it is possible to close the detection efficiency loophole for the violation of Bell inequalities[197]. Moreover, larger detector arrays will benefit the signal collection, *i.e.*, enable the characterization of the spatial properties of SPDC without moving detectors.

To overcome the limit on the effective area imposed by noise, we resort to a different method. In this method the pump intensity is adjusted to allow several photon pairs to reach the camera within one time window (the exposure time for CCD). The detected photon level is much less than 1 photon/pixel/frame to avoid two photons registering as one, while still greater than the average CIC contribution in order to maintain a good SNR. To characterize the spatial correlations of the photons each frame $F(x, y)$ (here $F(x, y)$ is the image pattern recorded by the CCD, x and y are the horizontal and vertical coordinates in number of pixels) is convoluted with itself in order to measure the amount of overlap between this frame and its copy inverted and shifted version $F(2x_0 - x, 2y_0 - y)$. The result of each individual

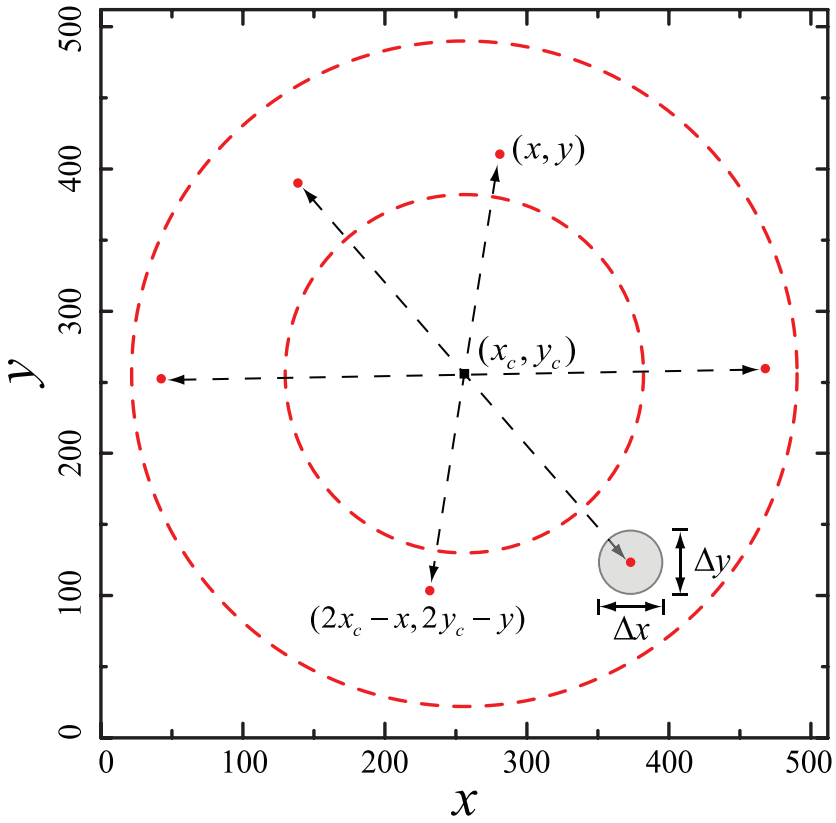


Figure 5.9 A frame with 3 photon pairs recorded. For each photon at point (x, y), there is another photon at $(2x_c - x, 2y_c - y)$, where (x_c, y_c) is the correlation center. In our setups, the photons are not perfectly correlated, but with uncertainties Δx and Δy.

convolution is then added together to give the total correlation

$$C_{tot}(x_0, y_0) = \sum_{l=1}^{N} F^l * F^l, \tag{5.11}$$

where $*$ denotes convolution and N is the number of frames. Fig. 5.9 shows a frame $F(x, y)$ with 3 photon pairs recorded. Since the photon pairs are anti-correlated in momentum, for each photon at (x, y), there is another photon at the diametrically opposite point $(2x_c - x, 2y_c - y)$ (where (x_c, y_c) is the center of the anti-correlation). Therefore C_{tot} will exhibit a peak where the shift $(x_0, y_0) = (x_c, y_c)$ such that each point in the original frame overlaps with the diametrically opposite point in the mirrored frame. In our setup, due to the PDC source configuration, the imaging system and other experimental imperfections, the coordinates of the two photons in each photon pair are not perfectly correlated, but with uncertainties $\Delta x \approx \Delta y \approx \Delta C$ (Eq. 5.9). We will show that as long as ΔC is not too big (no more than 5 pixels), the peak of C_{tot} is still able to be detected. In practical situations, photons are not always recorded due to the detection efficiency, and various noise should also be taken into account. Nevertheless, the noise is completely uncorrelated, therefore after accumulation of several frames, the contribution from noise is reduced, and one expects a peak with width ΔC to appear.

To see the correlation between photon pairs, our setup also allows one to apply an alternative method which is similar to the experiments done with APDs. In this method one can fix a given pixel and measure the coincidences between this

pixel and all other pixels. However, this requires a large number of frames, while the measurement of $C_{tot}(x_0, y_0)$ is more efficient since it uses all the pixels on each frame.

Here we give a more complete analysis of C_{tot} to show its physical meaning and how it is determined by the characteristics of the input state and the detector array. We assume the input state to the detector array is an entangled two-photon state with joint probability distribution $P_{\text{twin}}(\mathbf{r}_\text{s}, \mathbf{r}_\text{i})$ at the detection plane, with no further assumptions of the particular form of $P_{\text{twin}}(\mathbf{r}_\text{s}, \mathbf{r}_\text{i})$. Here we still use the labels signal and idler to distinguish each photon in the photon pair. The marginal distributions of each photon are $P_\text{s}(\mathbf{r}_\text{s})$ and $P_\text{i}(\mathbf{r}_\text{i})$ respectively. The number of photon pairs generated during the detection time window (*i.e.* frame for EMCCD) is m with probability $P(m)$. The overall detection efficiency of one pixel is η. Then the total correlation defined in Eq. 5.11 is (see Appendix C for the calculations):

$$\begin{aligned} C_{tot}(\mathbf{r}) &= N\langle m\rangle\eta\left[P_s(\frac{\mathbf{r}}{2}) + P_i(\frac{\mathbf{r}}{2})\right] + N\langle m^2\rangle\eta^2\Big[P_s(\mathbf{r}) * P_s(\mathbf{r}) + P_i(\mathbf{r}) * P_i(\mathbf{r}) \\ &\quad +2P_s(\mathbf{r}) * P_i(\mathbf{r})\Big] + 2N\langle m\rangle\eta^2\sum_{\mathbf{r}_s} P_{twin}(\mathbf{r}_s, \mathbf{r}-\mathbf{r}_s) + C_{noise}. \end{aligned} \tag{5.12}$$

Here $\langle\cdot\rangle$ denotes the ensemble average, and C_{noise} is a constant proportional to the spurious charge level, and N is the total number of frames again. Only the term with $P_{twin}(\mathbf{r}_\text{s}, \mathbf{r}-\mathbf{r}_\text{s})$ records the spatial correlation of the two-photon state, and contributes to the correlation peak discussed previously. The width of the peak can

be estimated as

$$\begin{aligned}\Sigma_{peak} &= \sum_{\mathbf{r}} \mathbf{r}^2 \sum_{\mathbf{r}_s} P_{twin}(\mathbf{r}_s, \mathbf{r} - \mathbf{r}s) \\ &= \sum_{\mathbf{r}_s} \sum_{\mathbf{r}_i} (\mathbf{r}_s + \mathbf{r}_i)^2 P_{twin}(\mathbf{r}_s, \mathbf{r}_i) \\ &= \Delta^2(\mathbf{r}_s + \mathbf{r}_i). \end{aligned} \tag{5.13}$$

Here we select the origin of the coordinates to make sure $\langle \mathbf{r}_s + \mathbf{r}_i \rangle = 0$. Recall the 2–f imaging system maps the momentum distribution on the detection plane, so that $\Sigma_{peak} \propto \Delta^2(\mathbf{k}_s + \mathbf{k}_i)$. We define another correlation function

$$C'_{tot}(\mathbf{r}) = \sum_{l}^{N} F^l \star F^l, \tag{5.14}$$

where $\star$ denotes the autocorrelation. With similar analysis, we will see that $C'_{tot}(\mathbf{r})$ has a peak with width $\Delta^2(\mathbf{r}_s - \mathbf{r}_i)$. If the photon pairs are transmitted through a 4–f imaging system, which images the position distribution of the photons onto the detection plane, $C'_{tot}(\mathbf{r})$ measures the position correlations of the input state. As mentioned in previous chapters, $\Delta^2(\mathbf{k}_s + \mathbf{k}_i)\Delta^2(\mathbf{r}_s - \mathbf{r}_i)$ reveals the entanglement of the input state. Other properties of $C_{tot}(\mathbf{r})$ for the PDC state will be discussed in Sec. 5.5.2

5.5.2 The simulation model

Eq. 5.12 gives a rough description of the total spatial correlation $C_{tot}(\mathbf{r})$ measured by a CCD array. For convenient comparison with the experimental results, we also

developed a simulation using Matlab®. In the simulations, the detected photon level (at the peak of the PDC distribution) is varied from 0.05 photon/pixel to 0.2 photon/pixel. The overall detection efficiency is difficult to determine experimentally. In the model we assumed $\eta = 0.05$, which should be lower than the actual value. We used Eqns. 5.7 and 5.8 to simulate the distribution of the downconverted photons over the camera sensor taking into account the input photon level, the overall quantum efficiency, the random and Poissonian distribution of the photon numbers and the uncertainty in the transverse momentum conservation of the photon pairs. The continuous distribution is discretized to the size of the pixels, and noise added to the resultant matrix in order to simulate the clock induced charge (CIC), where a spurious photo-electron can be generated in each pixel with a probability P_{cic}. Generally P_{cic} varies with the EMCCD configurations, and is measured experimentally. However, as a demonstration, in the simulation discussed in this section we use $P_{cic} = 0.04$, which is one of the values we obtained by experiment in Sec. 5.4.3.

The simulation of a single frame registered by the camera considering the overall set of parameters described above is shown in Fig. 5.10(a). Fig. 5.10(b) shows one frame after applying the thresholding, *i.e.* the camera is operated in photon-counting mode. After accumulation of several frames, the circular pattern produced by the distribution of transverse momenta in degenerate PDC becomes clear. Figures 5.10(c) and (d) show the accumulation of one hundred and one thousand thresholded frames, respectively, from which the ring may be clearly distinguished.

As a sample of the simulation output, Fig. 5.11 shows the 1D versions of the

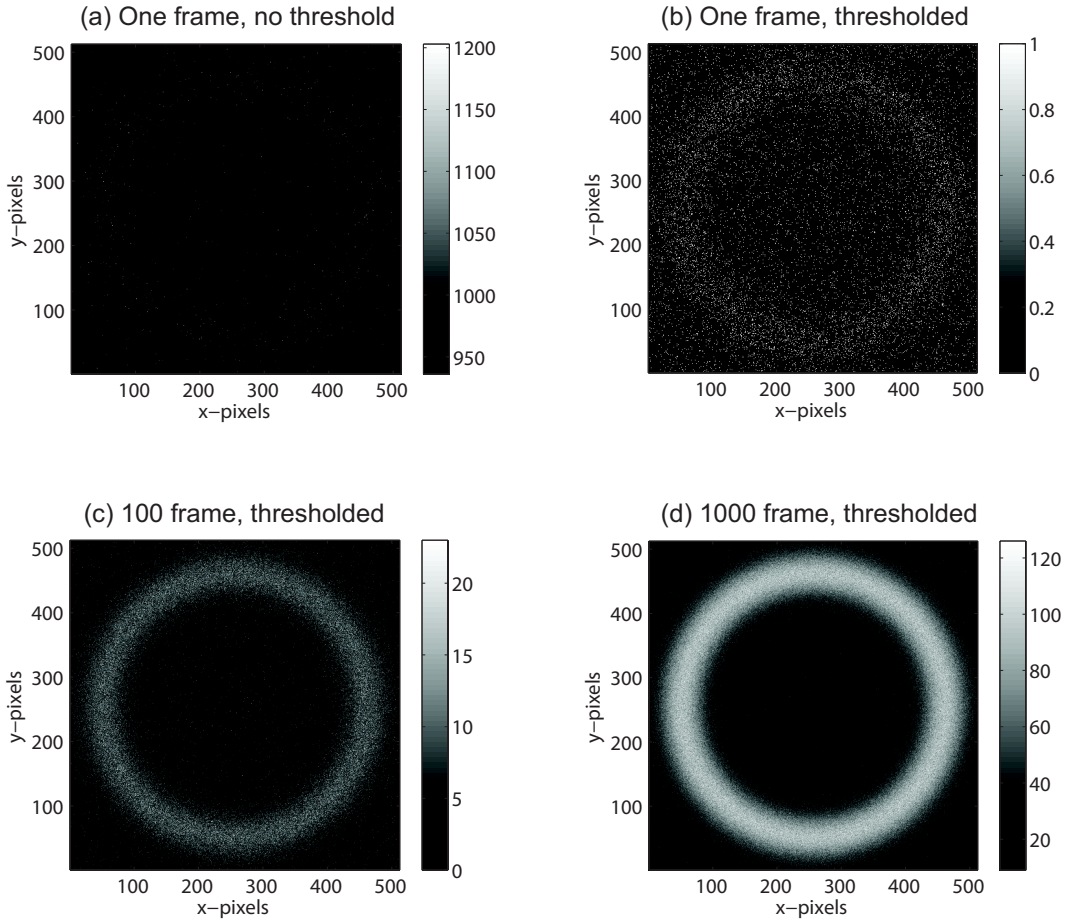


Figure 5.10 Frames generated by the simulation model. (a) One frame without threshold and (b) the same frame after threshold. (c) and (d) show the accumulation of 100 and 1000 frames, respectively, after each one is thresholded. The pump beam waist in this example was $w_0 = 2$ mm and the crystal length is $L = 0.5$ mm.

total correlation C_{tot} for the case where the pump beam waist is 2 mm. This gives a correlation area ($\Delta C = 12.5$ μm in Eq. 5.9) of around one pixel. Figure 5.11(a) is the correlation of just one frame. This graph is very noisy and does not allow one to extract any information about the correlations. For $n = 1000$ frames the total correlation is shown in Fig. 5.11(b). In this particular example we see a pronounced peak at the centre of the distribution, which is the signature of spatial correlations as discussed in Sec. 5.5.1. Although the EMCCD has 512 pixels in each dimensions, to show the complete characteristics of C_{tot} we would need an array of double the size due to the convolution calculation. The small peaks close to the edges are due to the contribution of $P_s(\frac{\mathbf{r}}{2}) + P_i(\frac{\mathbf{r}}{2})$ in Eq. 5.12. For degenerate type-I PDC, this is just the PDC ring with double radius. The large, broad peak close to the center (the 'bell' shape) is due to the term $P_s(\mathbf{r}) * P_s(\mathbf{r}) + P_i(\mathbf{r}) * P_i(\mathbf{r}) + 2P_s(\mathbf{r}) * P_i(\mathbf{r})$ in Eq. 5.12.

The same procedure was repeated for varying the pump beam waists from 100 μm to 3 mm, with detected light levels of 0.1 photon/pixel/frame, and over 1000 frames. Some results are shown in Fig. 5.12(a)-(e). As a comparison, in Fig. 5.12(f) we show the result for uncorrelated photons. These photons have the same marginal distribution of the PDC state, but there is no correlation between each photon and all the others, therefore there is no correlation peak at all. Here we only show the measurements for the center 512 pixels. Since the background is determined by the marginal distribution of the photons and the noise level, which does not vary with the pump beam waist, it remains at the same level from figure to figure. The height

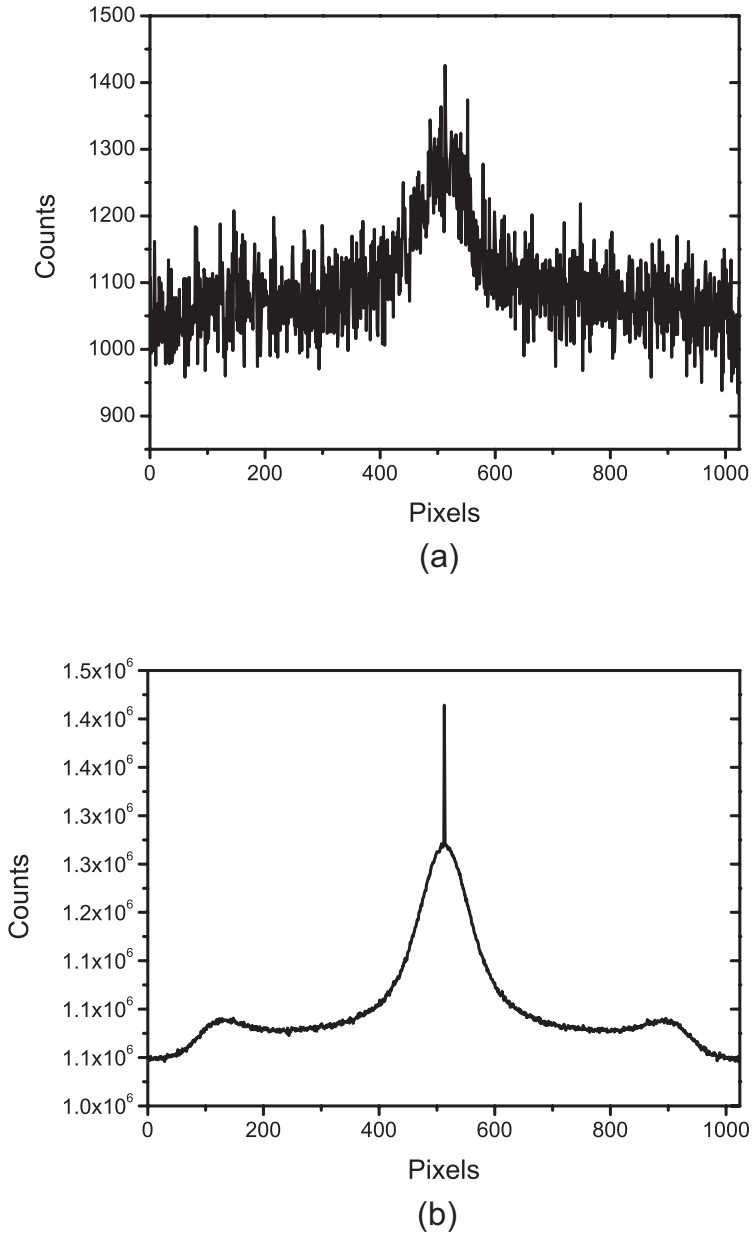


Figure 5.11 The 1D version of simulated results of total correlation C_{tot}. The number of frames analyzed is: (a) $n = 1$, (b) $n = 1000$. The pump beam waist in this example was $w_0 = 2$ mm, and the length of the crystal is $L = 0.5$ mm.

and width of the central peak that characterizes the spatial correlations is seen to change with the pump width as shown in the insets of Fig. 5.12. This is expected since the pump width defines the correlation area. As the pump waist gets smaller, the correlation area in the camera becomes larger (ΔC is inversely proportional to w_0). This reduces the overlap at the centre of the distribution and of its rotated version. After accumulation of 1000 frames, the reduced pump beam waist causes an increase in the width of the correlation peak and a reduction in its height. When the pump is strongly focused ($w_0 = 0.1$ mm for example), the correlation peak is so wide and low that it cannot be distinguished from the wide peak. In this case the camera is not able to distinguish PDC light from uncorrelated light as can be seen in the Fig. 5.12(e) and (f).

Let us define the height of the correlation peak as

$$H = 1 - \frac{1}{4} \sum_{m=\pm 1} \left[\frac{C_{tot}(x_{max}, y_{max} + m) + C_{tot}(x_{max} + m, y_{max})}{C_{max}} \right], \tag{5.15}$$

where $C_{max} = \max[C_{tot}(x_0, y_0)]$, x_{max} and y_{max} are the coordinates of C_{max}, *i.e.* they define the position of the correlation peak. The second term in Eq. 5.15 is an average value of the total correlation when we move one pixel outward from the centre in the $\pm x$ and $\pm y$ directions, normalized by C_{max}. Therefore H shows the 'sharpness' of the correlation peak. Fig. 5.13(a) shows the variation of the simulated results of H with the pump beam width w_0 for three different input photon levels of the PDC light ($N = 0.5$, 0.1 and 0.2 photons/pixel) and for an uncorrelated light

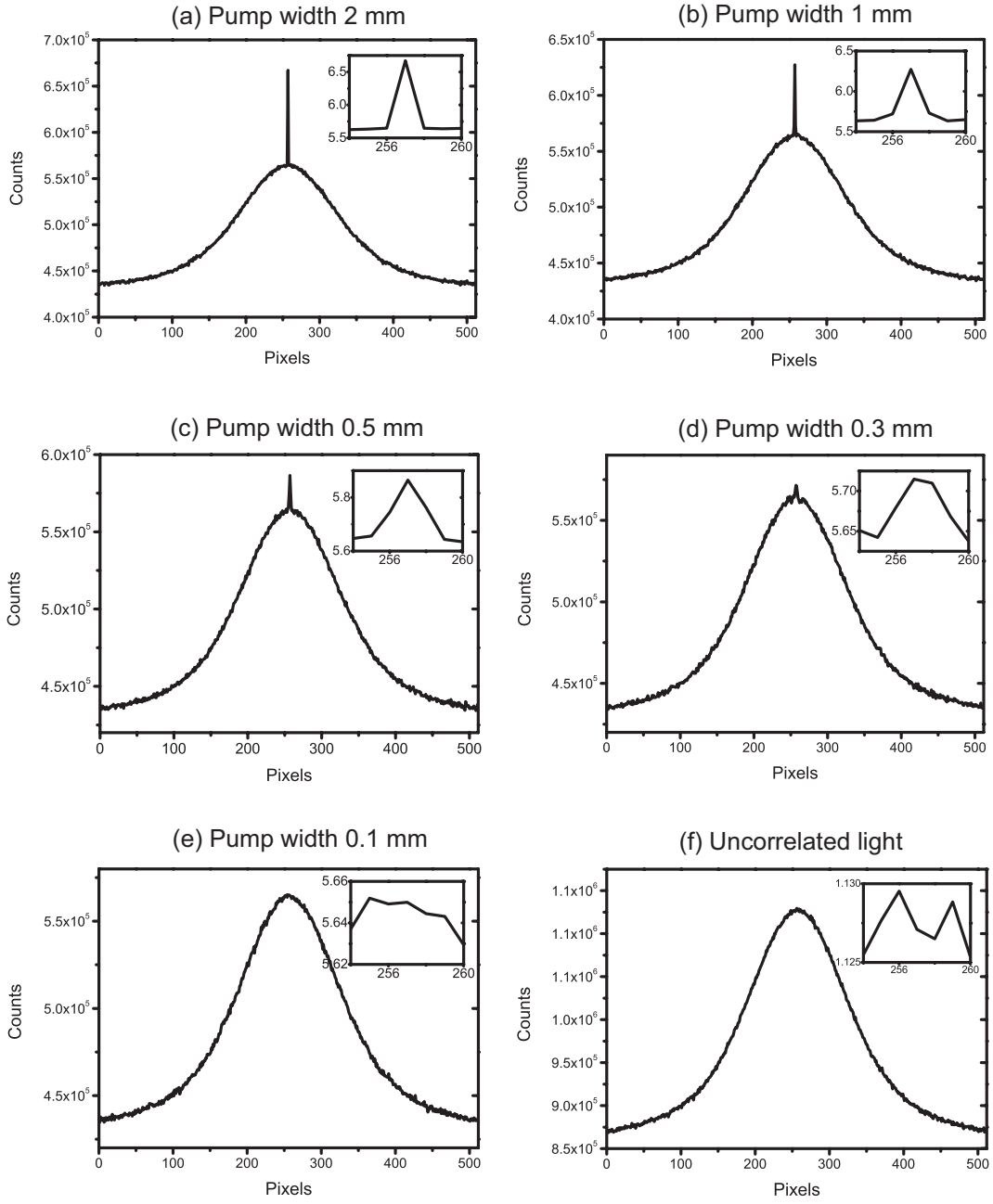


Figure 5.12 Simulated 1D correlation curves for: (a)-(e) the signal and idler beams generated by PDC with different pump beam waist and (f) photons with the same circular distribution of the PDC state, but totally uncorrelated. The inset in each figure shows a zoom in the correlation peak.

with the same marginal distribution as the PDC state. As expected the uncorrelated light shows no peak. Saturation is observed in H for the entangled beam from PDC light when w_0 is large enough for ΔC to be below one pixel size.

The results presented in Fig. 5.13(a) were obtained by considering a "perfect" 2-f imaging system, a monochromatic pump beam and neglecting the crosstalk between different pixels. In a realistic experiment, misalignments, finite pump bandwidth and non-negligible crosstalk would increase the effective correlation area of the downconverted photons. Fig. 5.13(b) shows the variation of H in terms of the correlation width ΔC in pixel numbers. It can be seen that for a correlation width of more than 5 pixels the correlation peak can hardly be distinguished from the background. Thus the increased correlation width should be no more than five pixels to allow the measurement of correlations. One possible way of avoiding these effects could be to increase the pixel size of the detector. In the camera this is possible through binning several pixels to act like one "super-pixel". However this must be traded against the additional noise in this super-pixel.

Another conclusion to be drawn from Fig. 5.13(a) is that, for a fixed pump beam waist, there is an optimal input intensity to maximize H. This cannot be attributed to a change in the degree of correlation, which is defined by the pump beam width, but solely due to the variation in the background level (SNR). If we increase the input level (from 0.1 photons/pixel to 0.2 photons/pixel in Fig. 5.13(a)) there will be a reduction in H caused by an increase in the height of the bell-shaped part of the correlation curve. If we decrease the input photon level (from 0.1 photons/pixel

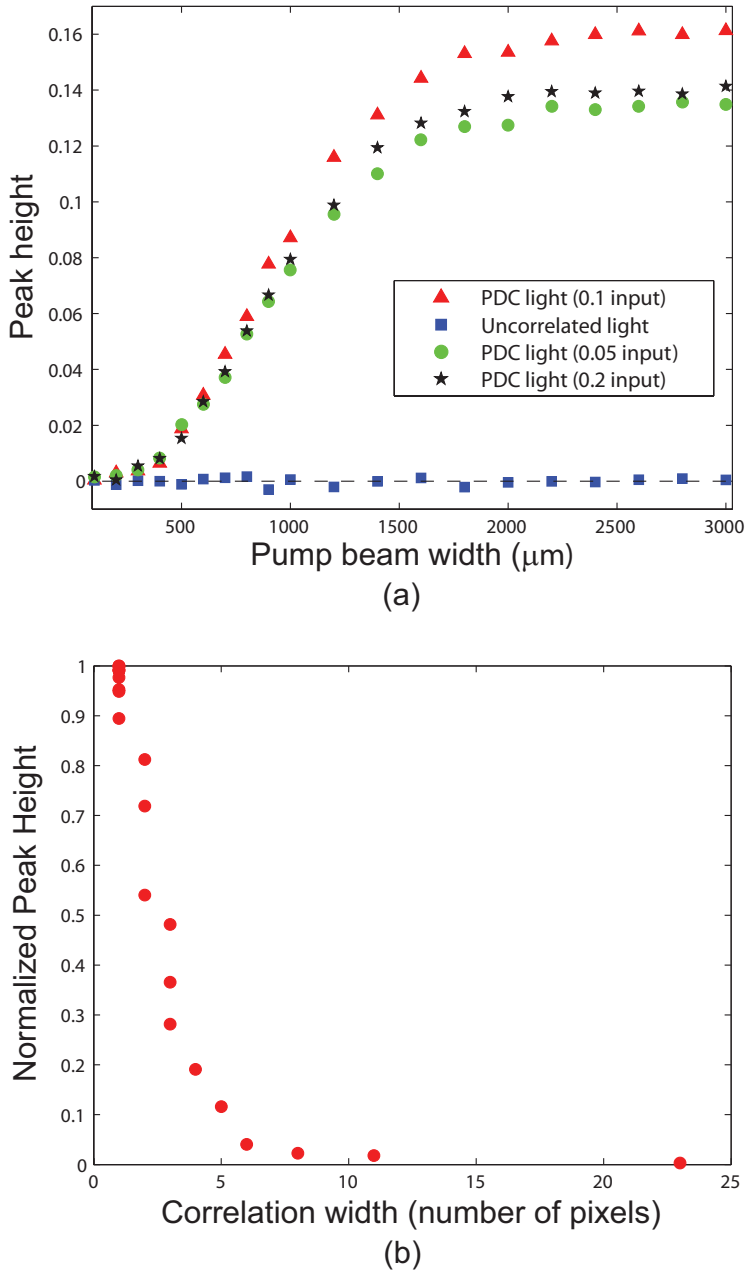


Figure 5.13 (a) Variation of the correlation peak height defined in Eq. 5.15 with the pump beam waist for three different SPDC input photon levels and uncorrelated light. (b) Variation of the normalized peak height (for 0.1 photon/pixel in (a)) with the correlation width.

to 0.05 photons/pixel in Fig. 5.13(a)), the noise will dominate the measurement and the background will reduce the relative height of the peak. This point is made clear by examing Eq. 5.12. By substituting the joint distribution (Eq. 5.6) and marginal distribution (Eq. 5.7) of the PDC state into Eq. 5.12, we find the maximum value of C_{tot} is

$$\begin{aligned} C_{max} &= C_{tot}(\mathbf{r}=0) \\ &= 4\sqrt{2}\langle m^2\rangle\eta^2\gamma LK + 2\sqrt{\pi}\langle m\rangle\eta^2 w_0^2 K^2 + 4\pi^{\frac{3}{2}} n_o^2 f_0^2 C_{noise}, \end{aligned} \tag{5.16}$$

while the maximum for the background in C_{tot} (contributions from uncorrelated events) is

$$C_{max}^{uncorr} = 4\sqrt{2}\langle m^2\rangle\eta^2\gamma LK + 4\pi^{\frac{3}{2}} n_o^2 f_0^2 C_{noise}. \tag{5.17}$$

Thus H can be approximated as

$$\begin{aligned} H &\approx \frac{C_{max} - C_{max}^{uncorr}}{C_{max}} \\ &= \frac{2\sqrt{\pi}\langle m\rangle\eta^2 w_0^2 K^2}{4\sqrt{2}\langle m^2\rangle\eta^2\gamma LK + 2\sqrt{\pi}\langle m\rangle\eta^2 w_0^2 K^2 + 4\pi^{\frac{3}{2}} n_o f_0^2 C_{noise}}. \end{aligned} \tag{5.18}$$

Note H in Eq. 5.18 is not exactly that defined in Eq. 5.15, since C_{max}^{uncorr} does not equal the second term in Eq. 5.15. However, this is a good approximation.

From Eq. 5.18, it is clear that for a fixed noise level C_{noise} there is an optimal signal level $\langle m\rangle$ that maximizes H. Apart from this, it can also be seen that H increases not only with increasing pump beam waist w_0, but also with decreasing

crystal length L, which yields the same asymptotic behavior as the mutual information analysis in Chapter 4 and the concurrence analysis in Ref. [35] between the signal and idler mode. This implies that H quantifies the non-classical spatial correlations for certain two-photon states.

The results shown in this section are examples using particular values for the parameters intended to illustrate the salient effects. To compare with the results of a particular experimental setup, the parameters for the actual experiment should be used. Still the general characteristics and behavior should be the same.

5.5.3 Experimental results and analysis

According to numerical simulations, for a fixed input light level $\langle m \rangle$, the height of the correlation peak decreases rapidly with increasing correlation width. With the parameters used in Sec. 5.5.2, it can be seen from Fig. 5.13 that when ΔC is greater than six pixels the peak is almost negligible. Since ΔC is inversely proportional to the pump beam width w_0, it is advantageous to make the pump width as large as possible, while ensuring it still completely passes through the crystal aperture. This is achieved by adjusting the magnification of the spatial filter in Fig. 5.6. We estimate ΔC by measuring the width of the pump image on the detection plane. This is done by monitoring it with EMCCD, or alternatively by gradually blocking it with a razor blade and measuring the transmitted power using a power meter. For unknown reasons, we were unable to obtain ΔC below one pixel, even though this is still much larger than the Rayleigh limit. The best we achieved for ΔC is

around 2 pixels, with a pump beam waist larger than 0.5 mm.

Another issue that should be mentioned is the large unexpected noise level. The EMCCD is configured for its optimal noise performance at the single-photon level with a vertical shift speed of 0.4 μs, readout speed of 1 MHz and a temperature of -75°C. The EM gain is set to the maximum level ($\sim$ 250). As mentioned in Sec. 5.4.3, under these conditions the CIC is approximately 0.005 electrons/pixel/frame. This is confirmed by measuring frames in a dark environment, and estimating the detected signal plus noise level. We look for background light from the source by turning on the pump, and rotating the BBO crystal by 90° degrees in the xy-plane to ensure no PDC photons are generated but all other conditions remain the same. Then we estimate the background level in the area that is far from the pump image. The result is 0.008 electrons/pixel/frame. The increase in background is due to fluorescence of the crystal and other optics, as well as the random scattered light. When the crystal is rotated back to its original position, which allows for the generation of downconverted photons, the pump intensity is adjusted so that the detected signal level at the peak of the PDC ring is 0.11 electrons/pixel/frame. Immediately we notice a strong increase in the background. This is confirmed by measuring the detected signal level in an area far from the PDC ring, which is found to be 0.07 electrons/pixel/frame. Futher tests show that this background increases with the pump power. However, from an analysis of the marginal distribution of the downconverted photons, we expect the probability to detect a photon in this area to be negligible. Therefore the sharp increase in background is unexpected,

and as we show with the rotated crystal tests, this should not be due to the crystal fluorescence. We performed the same test with several different BBO crystals, and obtained similar results. The reason for this issue is not clear to us. We took into account this effect in our simulations, and treat the increased background as uncorrelated events for the following analysis.

The crystal length selection is also a key issue. As shown in Eq. 5.18, a thinner crystal will give a more distinct correlation peak. Nevertheless, a thinner crystal also makes the distribution of the downconverted photons broader, therefore the intensity of the signal also decreases. Due to the background problem discussed above, thinner crystals give a lower signal-to-noise ratio. We performed tests with three different crystal length: 0.5 mm, 0.7 mm and 1 mm. The 1-mm thick crystal gave best results as quantified by the distinguishability of the correlations.

Figures 5.14 and 5.15 shows the experimental results for different input light levels and simulation results for comparable parameters. The results shown here are for C_{tot} averaged over the number of frames. The simulations are run with the parameters of the experimental setup (noise level, gain, *etc*). The largest difference between the simulation and experiment are in the background levels. We believe this is due to small noise level differences between the simulations and experiments. Although these differences are minute, after summing over 512×512 pixels, the cumulative differences become significant. Due to the increased background and crystal length, the correlation peaks in the simulation results are not as distinct as those shown in Sec. 5.5.1, but still strong enough to be distinguished from the

background. However, the experimental results are not as convincing. They do not show a clear signature of the correlation peak that can be distinguished from noise fluctuations.

This could be due to a problem with EMCCDs that has recently been reported in connection with astronomical imaging, which is the charge-transfer efficiency (CTE) problem. The CTE problem is another example of the crosstalk problem discussed in Sec. 5.1.3. For the previous simulations we assumed that each pixel of EMCCD is an independent detector. This is not a completely accurate description of the situation. As shown in Fig. 5.4, the signal detected by each pixel will be transfered through the same shift register and gain register. A measure of the ability of the CCD to transfer the charge from one potential well to another is given by the CTE, which has a typical efficiency of is less than unity. If the charges do not move to the adjacent stages at the required time, they will be left behind in one or other of the transfer steps and registered as if they come from a different originating pixel. Although the CTE of each transfer could be high for large charge packets (over 0.9999), after more than 1000 transfers, this will induce a noticeable spread of the charge from one pixel into adjacent pixels (for 0.9999 CTE, the spread will be over 2 pixels). This introduces crosstalk between different pixels and thus blur the final image. Moreover, the CTE is usually worse for low light levels. It has been reported that below the 0.5 photon/pixel/frame input level, the CTE of a typical EMCCD could cause a spread of several pixels[188]. There is no doubt that this effect will increase the effective correlation width ΔC (if the spread caused by the

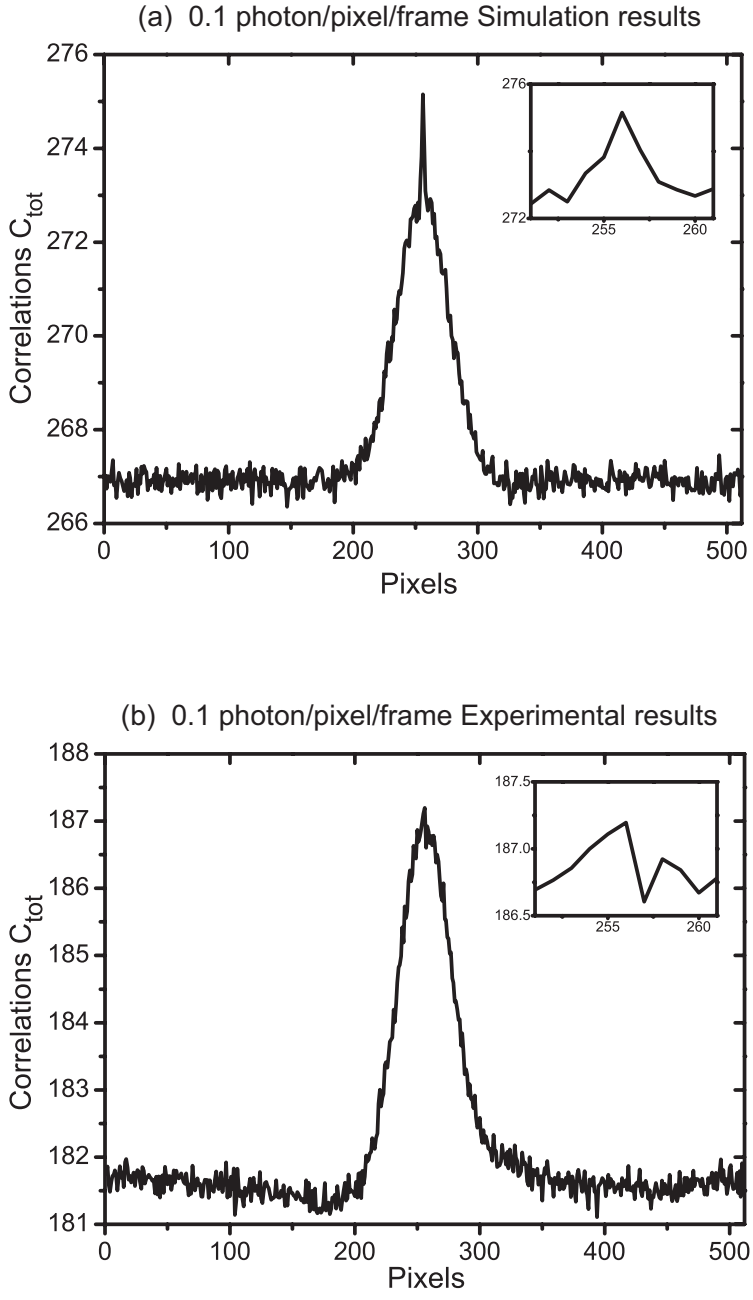


Figure 5.14 1D correlations curves C_{tot} averaged with the number of frames with the detected signal level 0.1 photon/pixel/frame. (a) is the simulation result, while (b) is the experiment result. The insets in the figures are zoomed plots of the correlation peak

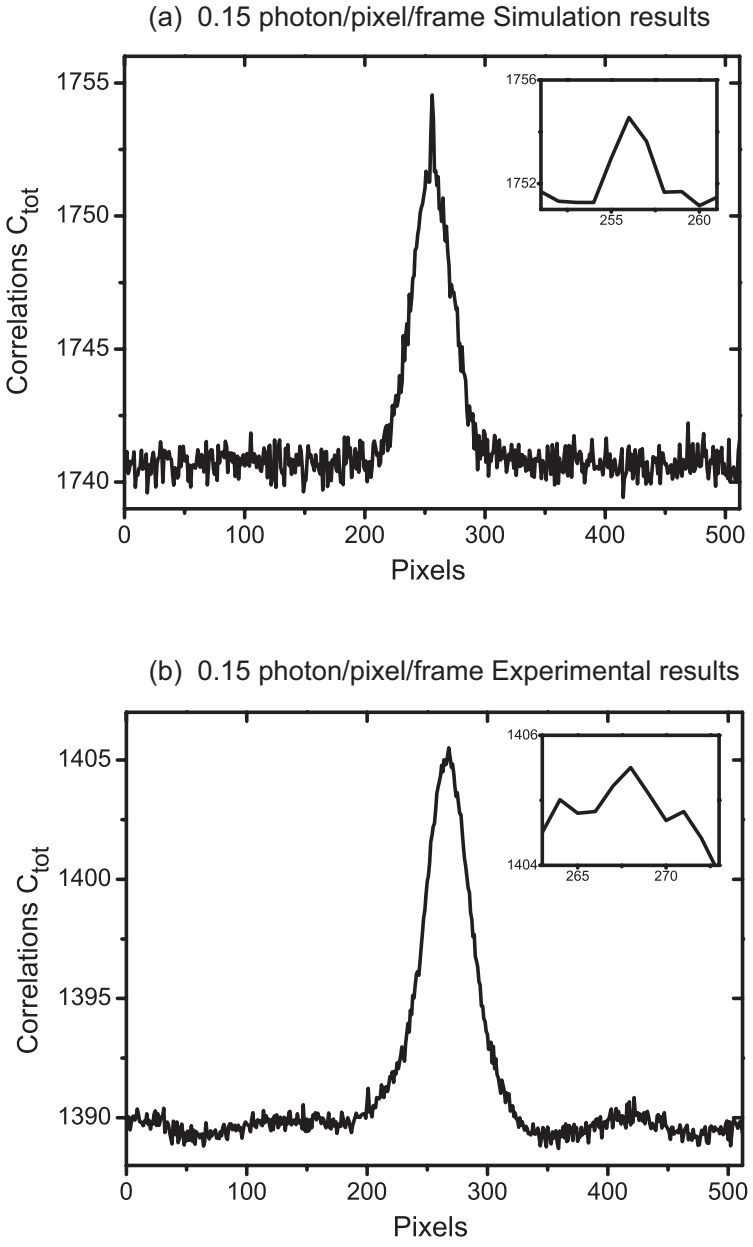


Figure 5.15 1D correlations curves C_{tot} averaged with the number of frames with the detected signal level 0.15 photon/pixel/frame. (a) is the simulation result, while (b) is the experiment result. The insets in the figures are zoomed plots of the correlation peak

crosstalk is $\sqrt{\delta(d)}$ (see Sec. 5.1.3), then the effective correlation width will become $\sqrt{(\Delta C)^2 + \delta(d)})$ and thus decrease the height of the correlation peak. Comparing the simulation results with the experimental results, we estimate the CTE induced spread to be 2 to 3 pixels. This then defines the effective spatial resolution of EMCCD for single-photon detection.

5.6 Summary of EMCCD configurations

As can be seen from the previous sections, an EMCCD allows users to change several acquisition parameters, which enables significant flexibility to configure the detector for different purposes. However, this also causes additional complexities for its usage. Since the most important issue in our experiments, and most applications with single photons, is the signal to noise ratio (SNR), we summarize the relations between different parameters and their effects on the SNR in Fig. 5.16. In principle, to reduce the noise, the readout speed should be decreased. On the other hand the clock speed also affects the CTE and thus the SNR in a more complex way. The effect of gain is a bit complicated: it amplifies the signal, while the CIC level also increases slightly with the increased gain. Fig. 5.16 explains how the parameters will affect the SNR. For practical setups to achieve the best performance the EMCCD array should be calibrated experimentally.

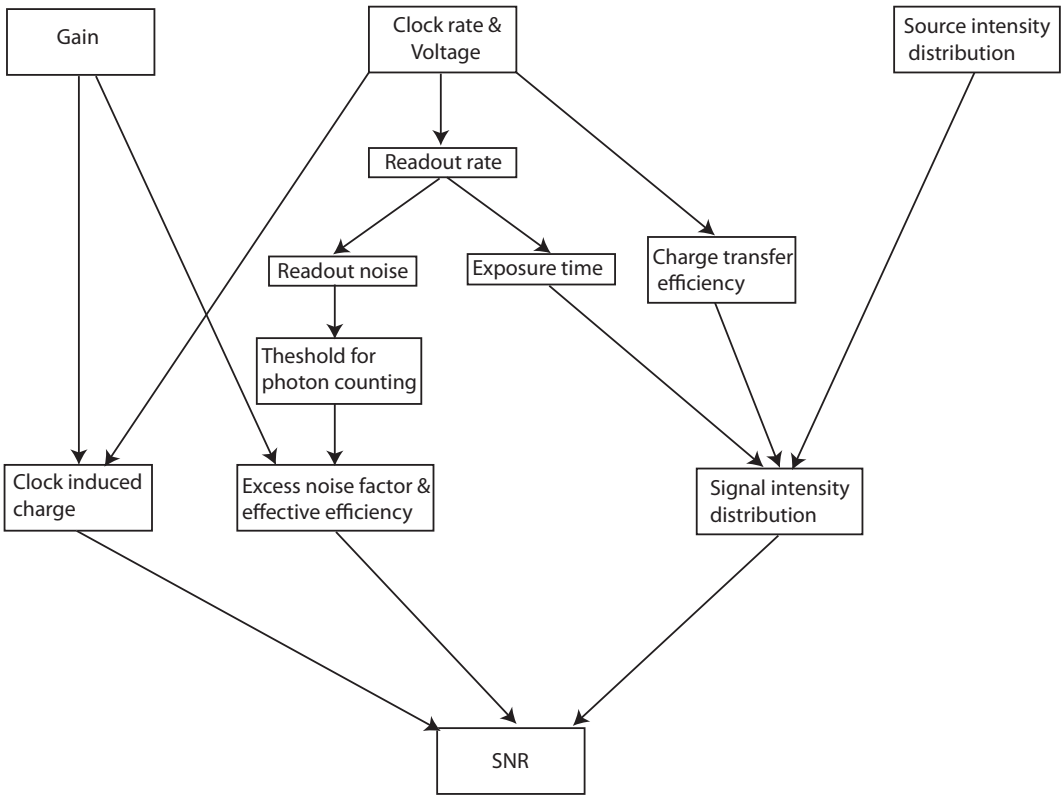


Figure 5.16 The relations between different parameters of EMCCD and their effects on signal to noise ratio (SNR). The clock configuration affects noise in several ways. In most situations a slow clock will be beneficial, though this will reduce the operating speed of the camera. The gain will amplify both the signal and spurious charges (CICs), as well as introduce additional noise quantified by excess noise factor (ENF). However one needs to keep the gain large enough to overcome the readout noise.

Chapter 6

Conclusion

Continuous variables (CVs) of single photons (momentum-position, time-frequency) offer another degree of freedom for quantum information processing (QIP) applications in addition to the dichotomic variables, *e.g.* the polarization. In particular, information can be encoded into the CV degree of freedom, enabling a photon to carry the d dimensional generalization of the qubit, the 'qudit'. This can dramatically increase the information content per transmitted photon, which enables higher data rates for various applications of quantum communication including quantum key distribution (QKD)[109,110]. Moreover, QKD with high dimensional states has the advantage of increased sensitivity to eavesdropping[198]. Considering the CV degrees of freedom, parametric downconversion (PDC) sources also produce high dimensional entanglement between the photons in each generated photon pair. This entanglement can be used to violate Bell inequalities in high dimensionality[123,153,199], and thus demonstrate that nature cannot be described by a local realistic theory.

Manipulation and measurment of single photon CVs require different schemes and devices than those for polarization. The work presented in this thesis studies a CV-QKD scheme based on the spatial degree of freedom the PDC state. An EMCCD camera is tested as a potential candidate for the detection device.

6.1 Summary

The thesis starts with the introduction of several crucial concepts, including the continuous variable quantum information processing (CV-QIP) based on the quadratures of the electromagnetic field, quantum entanglement, quantum key distribution (QKD) and CVs of single photons (position-momentum, time-frequency). The similarity between the CVs of single photons and those of the electromagnetic field enables one to consider CV-QIP applications using single photons or entangled photon pairs.

To analyse a single-photon CV-QIP application, one need to know the characteristics of the CV degrees of freedom of the single-photon state, which is largely determined by the generation process of the state. In this thesis we consider entangled photon pairs generated from the parametric downconversion (PDC) process, described in chapter 2. A theoretical framework is presented, and the spatio-temporal modal structure of the resulted two-photon state is derived. We emphasize the spatial degree of freedom of the PDC state by removing the spectral degree of freedom with interference filters.

The ability of a bipartite state to violation of a Bell inequality has many con-

nections with secure information transmisstion. In Chapter 3 we study this issue for the spatially correlated PDC state. A CHSH inequality based on the joint Wigner function of a two-photon state is contructed. This inequality allows one to employ the full continuum of the joint spatial amplitude of the PDC state. With a numerical calculation, it is shown that a realistic PDC state can strongly violate this inequality with a maximum value of 2.2, which demonstrates the ability of this state for secure information transmission. The extension of this method, together with the improved single-photon detector, may close an important experimental loophole of Bell inequality violations: the detection loophole.

The performance of the single-photon CV-QKD scheme based on the spatial degree of freedom of entangled photon pairs is analysed in chapter 4. We derive the information capacity in the spatial correlation of a realistic PDC state. The results confirm the potential to transfer several ($I > 7$) bits of information per photon through the spatial degree of freedom. A QKD protocol utilizing this form of information coding is proposed. Similar to the quadrature-based CV-QKD, the EPR criterion is a sufficient condition for the security of this QKD scheme. However, the non-Gaussian characteristics of the experimental imperfections (channel loss and detector noise) distinguish single-photon CV-QKD from quadrature-based CV-QKD, and severely limits the options of eavesdropping attack. A plausible attack, intercept-resend, is analysed to illuminate how secure information may be distilled well beyond the bound of the EPR criterion. As an example, it is shown that the secure information can be distilled with channel loss up to 35 (31.5) dB and a

detector array of 128 (256) pixels. A logarithmic negativity calculation confirms the entanglement between the legitimate parties.

Although the spatial correlation of the PDC state exhibits a large information content, to access this information content is not trivial. It requires one to employ a single-photon detector array, which has not been widely studied. In chapter 5 we develop methods to test the crucial parameters of a detector array for single photon detection, and implement these tests experimentally to a electron-multiplying charge coupled device (EMCCD) camera. With the photon pairs generated from a PDC source, we test the time response, noise performance, single-photon amplification and detection efficiency of this camera. The results show that the EMCCD has single-photon sensitivity, good quantum efficiency (comparable to a standard avalanche photodiode) and relatively low noise (spurious charge of 0.005 electrons/pixel/frame). An experiment that employs the EMCCD camera to measure the spatial correlations of the PDC state reveals the impact of the imperfect charge transfer efficiency of the camera, which reduces the spatial resolution by a factor of two or three.

6.2 Outlook

The work in this thesis can be roughly divided into three topics: i) engineering of the CV degrees of freedom of single photons or entangled photon pairs; ii) detection device for the CV degrees of freedom of photons and iii) their employments in QIP applications, specifically, in QKD. Therefore the future work will also follow these

three directions.

Engineering of the CV degrees of freedom of the PDC state

As can be seen from the discussions in previous sections, the internal correlations (the correlations between the spectral and spatial degrees of freedom) and the external correlations (the correlations between the signal and idler photons) of the PDC state strongly affect its performance in QIP applications. When PDC is used as a heralded single-photon source, it requires one to eliminate the correlations between the signal and the idler photons. On the other hand, many applications, for example, information transmission, Bell inequality violation *etc.*, will benefit from increasing the correlations in one CV degree of freedom while suppressing the correlation between different degrees of freedoms. Appendix A shows that the generation of a signal-idler factorable state is possible with non-collinear type-I PDC. This analysis considers a relatively simple situation, where the transverse walkoff of the pump in the crystal is ignored. For a short crystal, we expect this effect should be negligible. However, the existence of this effect will introduce additional spatio-temporal correlations between the two photons, decreasing the factorability of the PDC state. Therefore a more complete analysis that include the pump transverse walkoff is required to reinforce the results shown in this thesis. Moreover, due to the unsymmetric nature between the signal and idler photons in type-II PDC, we expect the generalization of this analysis to type-II PDC will be beneficial. For example, it allows one to use the state generated with degenerate collinear phase

matching conditions. However, the calculation should consider the variation of the extraordinary refractive index in different directions as well as the transverse walkoff of the extraordinary photon. We expect this can be done with numerical modelling.

Coupling photons into single-mode fibers is also a widely studied issue[200–202], since it is one possible solution to the long distance transmission of photons as well as integrated optical QIP circuits. It has been shown that the coupling efficiency strongly dependends on the modal structure of the PDC state[200]. Moreover, fiber coupling not only acts as a spatial filter, but also affects the joint spectral amplitude of the two-photon state due to the spatio-temporal correlations. Therefore to achieve a bright, factorable, fiber-coupled two-photon state requires further study.

As for the issue to increase the correlations in the CV degrees of freedom of photon pairs, we have shown that spatial correlation of the PDC state generated from a bulk crystal can be increased by adjusting the pump beam waist and the crystal length. However, this is not very efficient. It has been shown that by controlling the group velocity dispersion of the pump photon and the downconverted photon with a superlattice of nonlinear crystal and linear segments, the spectral correlations of the PDC state can be dramatically boosted (Schmidt number up to 10^7)[165]. As far as we know, few work has been done for the spatial correlations of the PDC state. We expecting similar analysis could be applied for the spatial degree of freedom of PDC states. This might be achieved with 2D photonic crystal structures.

Other candidates of single-photon detector arrays

Apart from EMCCD and ICCD, there are other candidates of single-photon detector arrays, for example, the multi-pixel photon counter (MPPC) [203] and the spatial resolving photon multiplier (PMT). Both of these detector arrays have been developed very recently, and their performance has not been completely tested. At the time when this thesis is finished, an experiment to test the photon number resolving performance of a MPPC is reported [204]. The major characteristics concerned in that work are quite similar to those we discussed in chapter 5. Since the method discussed in chapter 5 is designed to test any single-photon detector array, we believe our method will be a good complement to those discussed in Ref [204], and can also be used to test the performance of any other detector arrays for quantum optical applications.

Improving security analysis of single-photon CVQKD

In this thesis we have shown that the experimental imperfections of single-photon CV-QKD force Eve to apply non-Gaussian attacks, which, to our knowledge, have been scarcely studied in the previous works on CV-QKD. In chapter 4 we discuss the impact of one possible attack, intercept-resend attack. However, this is quite a simple attack. Whether more complex attacks, such as coherent attacks, will allow Eve to acquire more information is still unclear. This is a difficult question to answer since the analysis of non-Gaussian operations is not trivial. Instead we expect to set a bound on the maximum information that Eve can acquire with some inequalities

such as entropic uncertainty relations. How to get a bound tight enough also requires further study.

When consider the QKD protocol based on photons transmitted through free space, the turbulence effect should also be taken into account. Although the distortion introduced by this effect on information transmission can possibly be reduced by adaptive optics, it opens a potential loophole for eavesdropping attacks. Therefore it is worth to extend the security analysis to include the turbulence effect. There are also suggestions on QKD protocols based on the spectral correlations of entangled photons transmitted throught optical fiber [205]. Our analysis could be generalized for this scheme taking into account of the characteristics of fiber channel and detection device.

Appendix A

Parametric Downconversion Engineering

A.1 Introduction

In this appendix we give a more detailed study of the spatio-temporal correlations of the PDC state. We mainly consider two types of correlations within the continuous variable degrees of freedom of the two-photon PDC state. One is the correlation between the spectral and spatial degrees of freedom due to the dispersion relations of the nonlinear medium, as mentioned in Sec. 2.2. Mathematically, this means that the two photon joint amplitude $f(\omega_s, \omega_i, \vec{k}_s^{\perp}, \vec{k}_i^{\perp})$ cannot in general be written in the product form $g(\omega_s, \omega_i)\mathrm{h}(\vec{k}_s^{\perp}, \vec{k}_i^{\perp})$. This correlation makes it difficult to achieve full knowledge of either degree of freedom, since it requires to trace over the other degree of freedom. Practical systems usually resort to filtering (either spatial or

spectral) to remove one degree of freedom making the analysis easier. However the filtering process significantly decreases the photon flux. An alternative option is to use waveguided PDC to decouple the spatial degree of freedom from the spectral degree of freedom [206]. Still this approach also restricts the ability to modify spatial correlations of the downconverted photons.

The other correlation is the correlation that binds the signal and idler photons within each pair due to the phase matching conditions. This correlation makes the PDC state a bipartite entangled state and offers several benefits for quantum information processing applications, *e.g.*, quantum dense coding [20], quantum teleportation [207], and as will be shown in Chapter 4, quantum cryptography. However this type of entanglement degrades the performance of the PDC state when used as a heralded single-photon source. Since a detector used to record the trigger photon cannot resolve the frequency, nor the position precisely, the remaining heralded photon will be projected into a mixed spatio-temporal state. To be more precise, since we need to consider all the possible outcomes of the detection of the trigger photon, the reduced density matrix of one photon (say, the signal photon) when the other photon (idler) is detected can be calculated by tracing over the idler degrees of freedom in the biphoton density matrix

$$\hat{\rho}_s \equiv \mathrm{Tr}_i(\hat{\rho}), \tag{A.1}$$

where the biphoton density matrix is

$$\begin{aligned}\hat{\rho} &= \int d\omega_s d\omega_i d\omega_s' d\omega_i' d\mathbf{k}_s^{\perp} d\mathbf{k}_i^{\perp} d\mathbf{k}_s^{\perp'} d\mathbf{k}_i^{\perp'} f(\omega_s, \omega_i, \mathbf{k}_s^{\perp}, \mathbf{k}_i^{\perp}) \\ &\quad \times f^*(\omega_s', \omega_i', \mathbf{k}_s^{\perp'}, \mathbf{k}_i^{\perp'}) \left|\omega_s, \omega_i, \mathbf{k}_s^{\perp}, \mathbf{k}_i^{\perp}\right\rangle \left\langle \omega_s', \omega_i', \mathbf{k}_s^{\perp'}, \mathbf{k}_i^{\perp'}\right|. \end{aligned} \tag{A.2}$$

Here $f(\omega_s, \omega_i, \mathbf{k}_s^{\perp}, \mathbf{k}_i^{\perp})$ is the joint two-photon amplitude, and $\left|\omega_s, \omega_i, \mathbf{k}_s^{\perp}, \mathbf{k}_i^{\perp}\right\rangle$ is the two-photon state vector.

Substituting Eq. A.2 into Eq. A.1, we have

$$\hat{\rho}_s = \int d\omega_s d\omega_s' d\mathbf{k}_s^{\perp} d\mathbf{k}_s^{\perp'} \rho_s(\omega_s, \omega_s', \mathbf{k}_s^{\perp}, \mathbf{k}_s^{\perp'}) \left|\omega_s, \mathbf{k}_s^{\perp}\right\rangle \left\langle \omega_s', \mathbf{k}_s^{\perp'}\right|, \tag{A.3}$$

where

$$\rho_s(\omega_s, \omega_s', \mathbf{k}_s^{\perp}, \mathbf{k}_s^{\perp'}) = \int d\omega_i d\mathbf{k}_i^{\perp} f(\omega_s, \omega_i, \mathbf{k}_s^{\perp}, \mathbf{k}_i^{\perp}) f^*(\omega_s', \omega_i, \mathbf{k}_s^{\perp'}, \mathbf{k}_i^{\perp}). \tag{A.4}$$

is the heralded single photon matrix element.

Unless $\rho_s(\omega_s, \omega_s', \mathbf{k}_s^{\perp}, \mathbf{k}_s^{\perp'})$ is factorable so that it can be written as

$$\rho_s(\omega_s, \omega_s', \mathbf{k}_s^{\perp}, \mathbf{k}_s^{\perp'}) = m_s(\omega_s, \mathbf{k}_s^{\perp}) m_s^*(\omega_s', \mathbf{k}_s^{\perp'}), \tag{A.5}$$

the state described in Eq. A.3 is a mixed state. This severely limits the source performance in quantum information processing applications. For example, linear optical quantum computation [26] relies on the two-photon Hong-Ou-Mandel (HOM)

interference between photons from multiple sources. The visibility of the two-photon HOM interference is proportional to the purity of the input single-photon states when they are independent and identical. So to achieve a scalable quantum computation scheme, highly pure single-photon sources are required. As mentioned earlier, to ensure heralded pure-state single photons from PDC requires the heralded single photon matrix element $\rho_s(\omega_s, \omega_s', \mathbf{k}_s^{\perp}, \mathbf{k}_s^{\perp\prime})$ to be factorable.

One possible way to satisfy this condition is to tailor the biphoton amplitude $f(\omega_s, \omega_i, \mathbf{k}_s^{\perp}, \mathbf{k}_i^{\perp})$ so that the resulting biphoton amplitude is factorable

$$f_t(\omega_s, \omega_i, \mathbf{k}_s^{\perp}, \mathbf{k}_i^{\perp}) = u_s(\omega_s, \mathbf{k}_s^{\perp}) u_i(\omega_i, \mathbf{k}_i^{\perp}). \tag{A.6}$$

This can be done by applying filtering in both the spatial and spectral degree of freedoms of the photons[208,209]. When the filtering is strong enough, with the transmission function approaches a Dirac-delta function, the photon passed through it can be approximated as possessing a single spatio-temporal mode determined by the filtering function. Therefore the joint probability amplitude is factorable. However this method has obvious drawbacks: it reduces the photon flux dramatically and the factorization is asymptotic. Moreover, filtering PDC deteriorates the successful heralding rate of the single-photon generation: even without noise, the detection of the idler photon will not always herald a photon in the signal mode, since there is a large contribution from the vacuum state in the signal mode due to severe losses incurred by the filtration. To avoid this problem, an alternative method is proposed:

instead of using spectral and spatial filters to passively select the factorable spatio-temporal mode pair from a given PDC source, it is possible to engineer the original PDC state to be factorble with proper configurations[210]. It has been shown that by matching the group velocity of the pump with that of one of the downconverted photons, the joint spectral amplitude of the collinear, *i.e.* spatially filtered with single-mode fibers or pinholes, type-II PDC state can be factorable[211]. Using this technique of "group velocity matching" an experimental demonstration generating heralded single photons with purity over 94.4% has been reported[212,213].

This chapter generalizes the methods used in Refs[211–213] to both the spatial and spectral degrees of freedom. Using this approach we study the conditions that eliminate spatial and spectral corelations in PDC. The analysis is restricted to non-collinear type-I PDC here. This work has been done in collaboration with Dr. Alfred U'ren at Instituto de Ciencias Nucleares, Universidad Nacional Autónoma de México.

A.2 Preliminaries

We begin with the PDC state give in Eq. 2.17. Assuming a Gaussian pump is used, *i.e.*, both the spatial and spectral profiles of the pump are described by a Gaussian function

$$v(\mathbf{k}_p^{\perp}, \omega_p) = N \exp\left[-\frac{(\omega_p - \omega_{p0})^2}{\sigma^2}\right] \exp\left[\frac{w_0^2 (k_p^{\perp})^2}{4}\right], \tag{A.7}$$

where N is an overall amplitude, ω_{p0} is the pump central frequency, σ is the pump bandwidth, w_0 is the pump beam waist, and $k_p^\perp = |\mathbf{k}_p^\perp|$. The joint amplitude of the biphoton component is then given by:

$$f(\mathbf{k}_s^\perp, \omega_s; \mathbf{k}_i^\perp, \omega_i) = N \exp\left[-\frac{(\omega_s + \omega_i - \omega_{p0})^2}{\sigma^2}\right] \exp\left[\frac{w_0^2 \left|\mathbf{k}_s^\perp + \mathbf{k}_i^\perp\right|^2}{4}\right] \operatorname{sinc}\left[\frac{\Delta k_z L}{2}\right]. \tag{A.8}$$

Depending on the relative position between the pump beam waist and the center of the crystal along the z axis (where z axis is the propagation direction of the pump, and normal to the crystal, see Fig. 2.1(a)), there will be a phase term $\exp[i\Delta k_z z_0]$, where z_0 is the position of the beam waist with the crystal center at $z = 0$. When $z_0 = 0$, this term equals unity, which will be the situation considered in this chapter.

With the Gaussian approximation of the sinc function as in Eq. 2.33, the joint amplitude can be written as:

$$f(\mathbf{k}_s^\perp, \omega_s; \mathbf{k}_i^\perp, \omega_i) = N \exp\left[-\frac{(\omega_s + \omega_i - \omega_{p0})^2}{\sigma^2}\right] \exp\left[-\frac{w_0^2 \left|\mathbf{k}_s^\perp + \mathbf{k}_i^\perp\right|^2}{4} - \gamma\frac{\Delta k_z^2 L^2}{4}\right]. \tag{A.9}$$

and with the paraxial approximation the wavevector mismatch can be written as

$$\begin{aligned} \Delta k_z &= k_p^z - k_s^z - k_i^z \\ &= \sqrt{k_p^2 - |\mathbf{k}_s^\perp + \mathbf{k}_i^\perp|^2} - k_s^z - k_i^z \\ &\approx k_p - k_s^z - k_i^z - \frac{|\mathbf{k}_s^\perp + \mathbf{k}_i^\perp|^2}{2k_p}. \end{aligned} \tag{A.10}$$

For the following analysis, we apply the transformation from Cartesian coordi-

nates to spherical coordinates (Fig. A.1):

$$k_\mu^x = k_\mu(\omega_\mu)\,\sin\theta_\mu\cos\phi_\mu, \tag{A.11}$$

$$k_\mu^y = k_\mu(\omega_\mu)\,\sin\theta_\mu\sin\phi_\mu, \tag{A.12}$$

$$k_\mu^y = k_\mu(\omega_\mu)\,\cos\theta_\mu, \tag{A.13}$$

$$d\vec{k}_\mu^{\perp} = k_\mu(\omega_\mu)\sin\theta_\mu d\theta_\mu d\phi_\mu \tag{A.14}$$

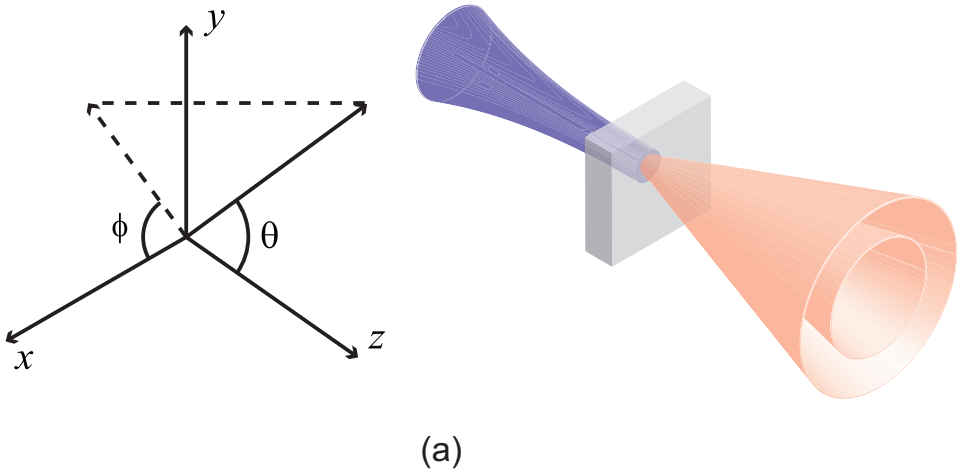
where $\mu = s, i$. For a general PDC process, k_μ should also depend on θ_μ and ϕ_μ, but here we consider the simple situation in which this dependence vanishes. This is applicable for (i) type-I PDC when both the signal and idler photons are ordinary waves or (ii) when the downconverted modes are restricted to the paraxial region, where θ_μ have a small range.

Substituting Eqn. A.14 into $|\mathbf{k}_s^\perp + \mathbf{k}_i^\perp|^2$, we have

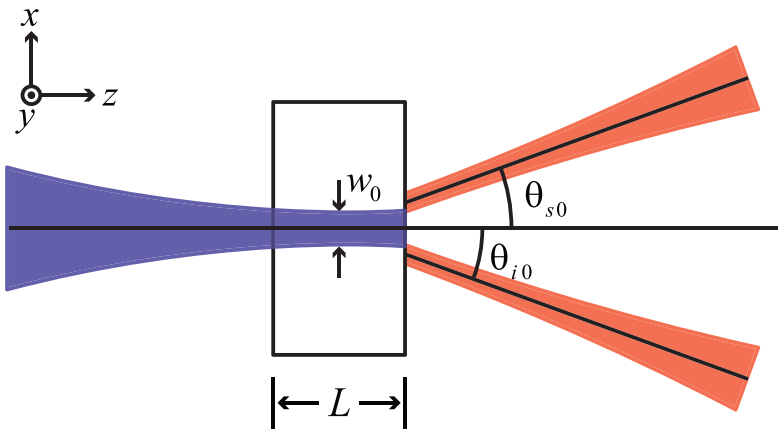
$$\left|\mathbf{k}_s^\perp + \mathbf{k}_i^\perp\right|^2 = k_s^2\sin^2\theta_s + k_i^2\sin^2\theta_i + 2k_sk_i\sin\theta_s\sin\theta_i\cos(\phi_s - \phi_i). \tag{A.15}$$

Since k_μ^z does not depend on ϕ_μ, the joint amplitude only depends on the difference between ϕ_s and ϕ_i, not the specific value of either ϕ_s or ϕ_i. This shows the downconverted modes in this situation are azimuthally symmetric, which confirms the arguments in Sec. 2.3.

For the following discussion we focus on type-I degenerate PDC, in which the center frequencies of the downconverted photons are $\omega_{s0} = \omega_{i0} = \omega_{p0}/2 = \omega_0$, and



(a)



(b)

Figure A.1 (a) Schematic showing the relation between the cartesian coordinates and the spherical coordinates. (b) A 2D figure shows the configuration of the PDC setup and major parameters.

center directions satisfy $\theta_{s0} = -\theta_{i0} = \theta_0$ and $\phi_{s0} = \phi_{i0} = \phi_0$. This satisfies the phase matching conditions in both the x and y directions $k_s^x(\omega_{s0}) + k_i^x(\omega_{i0}) = 0$ and $k_s^y(\omega_{s0}) + k_i^y(\omega_{i0}) = 0$. For the phase matching conditions in the z directions, we need

$$k_p(\omega_{p0}) - k_s^z(\omega_{s0}) - k_i^z(\omega_{i0}) = k_{p0} - 2k\cos\theta_0 = 0, \tag{A.16}$$

where $k = k_s(\omega_0) = k_i(\omega_0)$.

We define the spectral and angular detunings

$$\nu_\mu = \omega_\mu - \omega_{\mu 0}, \tag{A.17}$$

$$\Theta_\mu = \theta_\mu - \theta_{\mu 0}, \tag{A.18}$$

$$\Phi_\mu = \phi_\mu - \phi_{\mu 0}. \tag{A.19}$$

With these definitions we can apply a Taylor expansion on the components for the phase mismatch in Eq. A.9 up to first order (the zeroth order vanishes due to the phase matching conditions) giving

$$\begin{aligned} k_s^x + k_i^x &= k\cos\theta_0\cos\phi_0(\Theta_s + \Theta_i) + k\sin\theta_0\sin\phi_0(\Phi_i - \Phi_s) \\ &\quad + k'\sin\theta_0\cos\phi_0(\nu_s - \nu_i), \end{aligned} \tag{A.20}$$

$$\begin{aligned} k_s^y + k_i^y &= k\cos\theta_0\sin\phi_0(\Theta_s + \Theta_i) - k\sin\theta_0\cos\phi_0(\Phi_i - \Phi_s) \\ &\quad + k'\sin\theta_0\sin\phi_0(\nu_s - \nu_i), \end{aligned} \tag{A.21}$$

$$k_p - k_s^z - k_i^z = (k_p' - k'\cos\theta_0)(\nu_s + \nu_i) + k\sin\theta_0(\Theta_s - \Theta_i), \tag{A.22}$$

where $k' = \partial k_s/\partial\omega(\omega_0) = \partial k_i/\partial\omega(\omega_0)$ and $k'_p = \partial k_p/\partial\omega(2\omega_0)$. Since k' is the reciprocal of the group velocity v_g, it is convenient to define two variables in the time dimension

$$\tau_l = L(k'_p - k'\cos\theta_0), \tag{A.23}$$

$$\tau_t = w_0 k' \sin\theta_0, \tag{A.24}$$

which are called the longitudinal and transverse group delay.

Substituting Eqns. A.10, A.20 - A.21 into Eq. A.9, and keeping the terms up to quadratic in ν_s, ν_i, Θ_s, Θ_i, Φ_s and Φ_i, the joint amplitude can be approximated as

$$\begin{aligned} f(\nu_s,\nu_i,\Theta_s,\Theta_i,\Phi_s,\Phi_i) &= M\exp(-\frac{t_-^2}{2}\nu_s\nu_i - \frac{\alpha_-}{2}\Theta_s\Theta_i + 2\beta\Phi_s\Phi_i - \frac{\tau_-}{2}\nu_s\Theta_i \\ &+ \frac{\tau_-}{2}\nu_i\Theta_s - \frac{\tau_+}{2}\nu_s\Theta_s + \frac{\tau_+}{2}\nu_i\Theta_i - \frac{\alpha_+}{4}(\Theta_s^2+\Theta_i^2) \\ &- \frac{t_+^2}{4}(\nu_s^2+\nu_i^2) - \beta(\Phi_s^2+\Phi_i^2) + \vartheta(3)) \end{aligned} \tag{A.25}$$

where

$$\alpha_\pm = w_0^2k^2\cos^2\theta_0 \pm \gamma L^2k^2\sin^2\theta_0, \tag{A.26}$$

$$\beta = \frac{1}{4}w_0^2k^2\sin^2\theta_0, \tag{A.27}$$

$$\tau_\pm = w_0\tau_t k\cos\theta_0 \pm \gamma L\tau_l k\sin\theta_0, \tag{A.28}$$

$$t_\pm^2 = \frac{4}{\sigma^2} + \gamma\tau_l^2 \pm \tau_t^2, \tag{A.29}$$

where definitions in Eqns. A.23 and A.24 are used. $\alpha_\pm$ and β are dimensionless

parameters, while $\tau_\pm$ and $t_\pm$ have dimensions of time. Note that M is not a constant, since it contains $\sin\theta_s$ and $\sin\theta_i$, but it does not contain any cross term between ν_s, ν_i, Θ_s, Θ_i, Φ_s and Φ_i, so it will not affect the following discussions.

Eq. A.25 exhibits various types of correlations among ω_s, ω_i, θ_s, θ_i, ϕ_s and ϕ_i. These can be correlations between the variables of different photons (external correlations), *e.g.* the components contain $\nu_s\nu_i$, $\Theta_s\Theta_i$, $\Phi_s\Phi_i$, $\nu_s\Theta_i$ and $\nu_i\Theta_s$; or correlations between the variables of the same photon (internal correlations), *e.g.* the components $\nu_s\Theta_s$ and $\nu_i\Theta_i$. The external correlations compose the pairwise correlation between the signal and idler photons, and are the reasons that the detection of one photon (idler) projects the other (signal) into a mixed state unless the detector can resolve ω_i, θ_i and ϕ_i, or strong filtering is used. The internal correlations reveal hyperentanglement between spatial and spectral degrees of freedom arising from the dispersion relations. Interestingly there are no correlation terms involving the azimuthal angles (Φ_s and Φ_i) and any other variables (Θ_s, Θ_i, ν_s and ν_i). Therefore the azimuthal correlation is decoupled from the correlations of the other degrees of freedom. All of these correlations are summarized in Fig. A.2

A.3 PDC state engineering

Adjustments of the coefficients $\alpha_\pm$, β, $t_\pm$ and $\tau_\pm$ offer many ways to manipulate the PDC state for various purposes. As an example, we consider a special situation for collinear PDC where $\theta_{s0} = \theta_{i0} = 0$. Under this condition $\tau = 0$ in Eq. A.24,

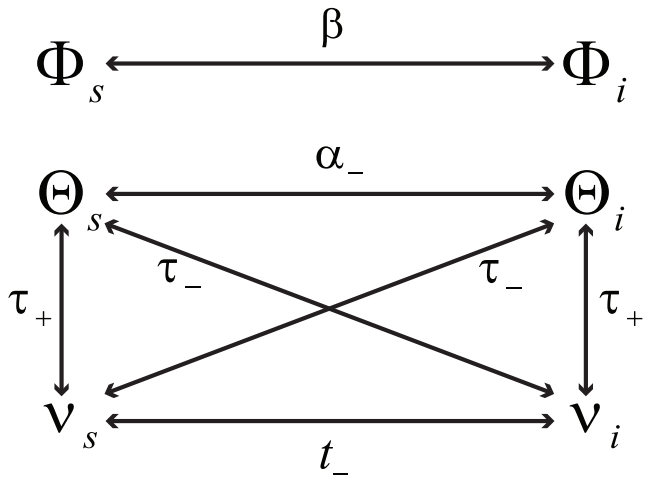


Figure A.2 Various correlations within the PDC state. Φ and Θ are spatial parameters. ν is the spectral parameter. The lines with arrowhead show the possible correlations between different variables. The parameter next to each line quantifies the strength of the correlation.

therefore

$$\beta = \tau_+ = \tau_- = 0, \tag{A.30}$$

$$\alpha_+ = \alpha_- = \alpha = w_0^2 k^2 \cos^2\theta_0, \tag{A.31}$$

$$t_+^2 = t_-^2 = t^2 = \frac{4}{\sigma^2} + \gamma\tau_l^2. \tag{A.32}$$

Thus the joint amplitude in Eq. A.25 is reduced to

$$f(\nu_s, \nu_i, \Theta_s, \Theta_i, \Phi_s, \Phi_i) = \exp\left[-\frac{t^2}{4}(\nu_s + \nu_i)^2 - \frac{\alpha}{4}(\Theta_s + \Theta_i)^2\right]. \tag{A.33}$$

There are several special features of this state. First, the azimuthal correlation vanishes, which is expected, since the downconverted photons are phase-matched at

collinear directions, where the azimuthal angles have no effect on the PDC state. Second, the frequency correlation is decoupled from the polar angle correlation. In some sense, this means the spatial degree of freedom is decorrelated from the spectral degree of freedom. But this is different from the situation discussed in Sec. A.1, where the spatial degree of freedom is expressed in terms of $k_s^\perp$ and $k_i^\perp$. Since

$$\sin\theta = \frac{k^\perp}{k(\omega)}, \tag{A.34}$$

we have

$$\Theta\cos\theta_0 = \frac{1}{k(\omega_0)}\Delta k^\perp + \frac{\sin\theta_0}{k(\omega_0)}\frac{\partial k}{\partial\omega}\bigg|_{\omega_0}\nu. \tag{A.35}$$

Unless the second term on the right side of Eq. A.35 is negligible, or $\sin\theta_0\,\frac{\partial k}{\partial\omega}\big|_{\omega_0} \ll 1$, there is no one-to-one mapping between Θ and $\Delta k^\perp$. Depending on the applications and the detection system configurations, we may choose either Θ, Φ or $k^\perp$ to represent the spatial degree of freedom.

A drawback of collinear degenerate type-I PDC is that it is hard to distinguish the signal photon from idler, since both of the photons have the same properties in their spatio-temporal degrees of freedoms (transverse wave vectors, pointing directions, frequencies *etc.*) and polarizations. This enables the generation of a single mode squeezed state, but strongly limits the possible usage of this kind of state as a heralded single-photon source. In the following discussions we focus on the non-collinear type-I PDC state.

As mentioned in Sec. A.1 a two-photon state that is factorable between signal

and idler degrees of freedom plays an important role in pure single-photon state generation. It can be seem from Eq. A.25 and Fig. A.2 that to achieve this requires $\tau_- = t_- = \alpha_- = \beta = 0$, *i.e.*

$$w_0\tau_t k\cos\theta_0 - \gamma L\tau_l k\sin\theta_0 = 0, \tag{A.36}$$

$$\frac{4}{\sigma^2} + \gamma\tau_l^2 - \tau_t^2 = 0, \tag{A.37}$$

$$w_0^2k^2\cos^2\theta_0 - \gamma L^2k^2\sin^2\theta_0 = 0, \tag{A.38}$$

$$\frac{1}{4}w_0^2k^2\sin^2\theta_0 = 0. \tag{A.39}$$

Note that Eq. A.37 implies the same condition proposed in Ref[210] for the generation of PDC state factorable in the spectral degree of freedom (spatially filtered), since t_- determines the correlations between ν_s and ν_i. Because the azimuthal correlations are decoupled from the polar angle and frequency correlations, we can consider Eqns. A.36 - A.38 first. Moreover, we assume a pump bandwidth σ that is sufficiently large so that the first term in Eq. A.37 is negligible. Thus solving these equations gives the relatively simple results

$$\tan\theta_0 = \frac{w_0}{\sqrt{\gamma}L}, \tag{A.40}$$

$$k' = k'_p\cos\theta_0. \tag{A.41}$$

Recall that θ_0 should satisfy the phase matching condition in Eq. A.16. Thus Eq. A.40 implies the focusing strength (the beam waist w_0) for a given crystal length.

Eq. A.41 is of particular interest. It can be rewritten as $v_{gp} = v_g \cos\theta_0 = v_g^z$, where v_{gp} is the group velocity of the pump, and v_g is the group velocity of signal and idler. Therefore this condition can be interpreted as the longitudinal group velocity matching condition, the longitudinal component of the group velocity of signal/idler equals the pump group velocity. Thus, similar to the technique proposed in the generation of a spectrally decorrelated state[211], group velocity matching plays an important role here. An explanation of this condition is illustrated in Fig. A.3. The pump photon may split into signal and idler photon pairs at any point as it propagates through the crystal. When the group velocity matching condition is satisfied, the photon pairs generated at different points will arrive at any plane that is normal to the z-axis at the same time. As a result, the time that the idler photon is detected will give no information about where the signal photon is generated. This indistinguishability is essential for the conditional generation of pure-state single photons.

Now we consider the azimuthal correlation, which is quantified by β. As shown in Eq. A.27, $\beta = 0$ when $\theta_0 = 0$ or $w_0 = 0$. Since we are considering non-collinear PDC, it is required to have $w_0 = 0$, so that the pump is a perfect point source. Due to diffraction, this is not achievable. So one option is to make β small enough so that the azimuthal correlation is negligible. For many applications involving conditional single photon generation, the detection device usually has a limited aperture due to the limited detector size or spatial filtering, thus will not cover the whole spatial distribution region of the PDC state. Since it is the detection of the idler photon

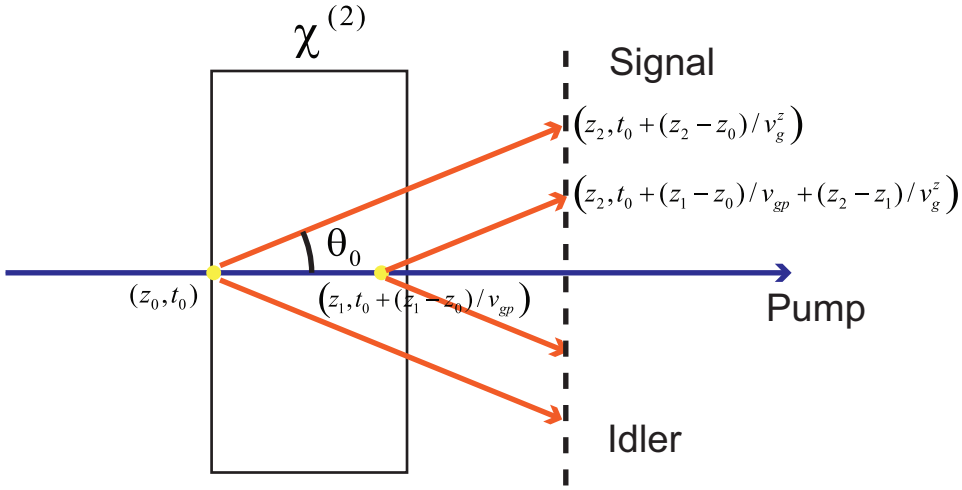


Figure A.3 The longitudinal group velocity matching condition. When $v_{gp} = v_g^z$, the downconverted photon generated at z_0 and z_1 will arrive the z_2 plane at the same time.

that projects the signal photon into a mixed state, we only need to consider the factorability of the PDC state within the detection aperture.

As shown in Fig. A.4, the detection device with a angular aperture ($\Delta\theta_d$) is placed at r, while the crystal is centered at the origin. The dimensions of the aperture along the x-axis and y-axis are then given by

$$\Delta X = r\Delta\theta_d, \tag{A.42}$$

$$\Delta Y = r\sin\theta_0\,\Delta\phi. \tag{A.43}$$

We assume $\Delta X = \Delta Y$, say, the detector is symmetric in x and y direction or a

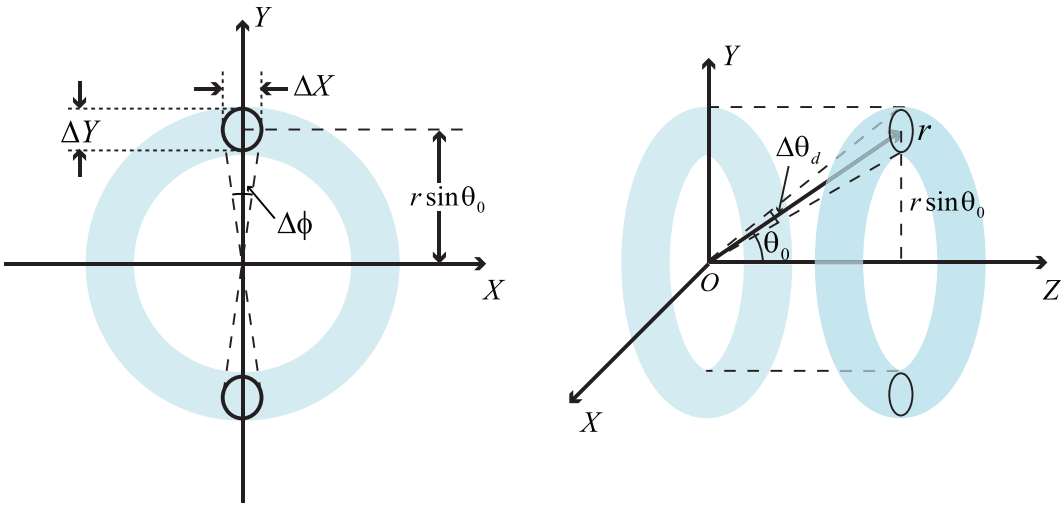


Figure A.4 The effect of limited detection aperture on the azimuthal correlations. The agular aperture is $\Delta\theta_d$.

circular iris filter is used. Then from Eqns. A.42 and A.43, we have

$$\Delta\phi = \frac{\Delta\theta_d}{\sin\theta_0}. \tag{A.44}$$

According to Eq. A.25, β defines the azimuthal correlation width of the PDC state, or more precisely $\Delta\Phi_- = 1/\sqrt{\beta}$ for $\Phi_- = \Phi_s - \Phi_i$. If $\Delta\phi \ll \Delta\Phi_-$, the component for azimuthal angle correlation in Eq. A.25 can be considered constant within the detection aperture, and the azimuthal angle dependence is removed. This requires

$$w_0 k \Delta\theta_d \ll 1, \tag{A.45}$$

where the definition of β in Eq. A.27 is used. From Eq. A.45 we can see that when the strong focusing $w_0 \to 0$ or spatial filtering $\theta_d \to 0$ is applied, the azimuthal

angle correlation vanishes, which, together with the previous discussions, allows us to achieve a factorable state.

In summary, the conditions for generating a completely factorable state are

1. Phase matching condition

$$k_{p0} - 2k\cos\theta_0 = 0.$$

2. Group velocity condition

$$k' = k'_p \cos\theta_0.$$

3. Pump, crystal and detection configuration condition

$$\tan\theta_0 = \frac{w_0}{\sqrt{\gamma}L},$$
$$w_0 k \Delta\theta_d \ll 1.$$

The PDC state we consider are non-collinear type-I, with the downconverted modes in the paraxial regime, and the spatial walkoff of the pump negligible.

To rigorously verify these conditions, we need to substitute them into Eq. A.8 and calculate the purity of the reduced density matrix in Eq. A.1. These results will be presented in the future work.

A.4 Further discussions

For the previous discussions, to achieve analytic results, we considered relatively simple configurations with several constraints (paraxial approximations, *etc.*). However, this also limits the options for tailoring the PDC state. In this section, we will discuss several issues for applying these ideas to more general situations.

A.4.1 Spatial walkoff

One effect that is ignored in our previous discussion is the spatial walkoff of the pump, signal and idler inside the crystal. This is due to the birefringence of the crystal, which makes the Poynting vector not parallel to the wavevector for the extraordinary polarized light. For type-I PDC considered in the previous sections, only the pump will experience transverse walkoff. Fig. A.5 shows the situation in the plane that contains the pump wavevector (assuming a plane wave for the purpose of illustration). It can be seen that although the o-rays (signal and idler) do not experience transverse walkoff, due to the skewness of the pump field, the signal and idler will result in different spatial patterns. Moreover, since the emission of PDC in the plane (yz) orthogonal to the pump plane (xz plane shown in Fig. A.5) is not affected by the pump walkoff, the emission pattern is not symmetric in both planes[214,215]. Therefore the azimuthal correlations depend not only on the azimuthal angle difference $\phi_s - \phi_i$ any more, but the particular values of ϕ_s and ϕ_i. This also introduces correlations between the azimuthal angle and the polar angle, and even correlations between the azimuthal angle and frequency. When the crytal

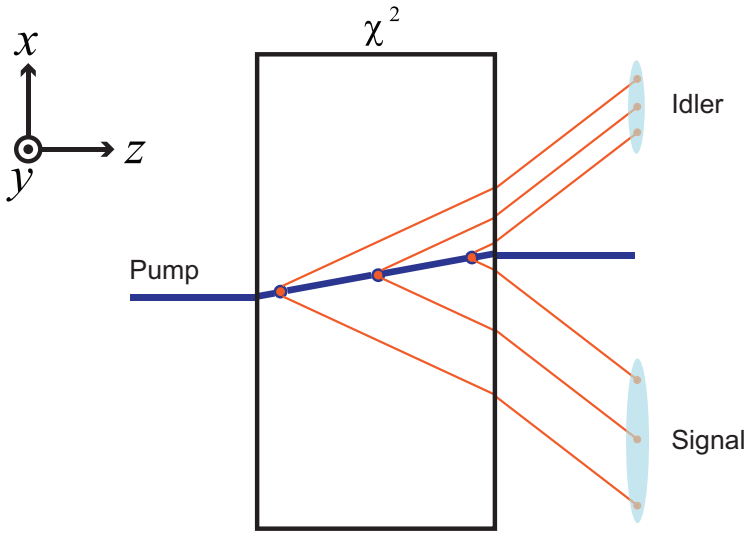


Figure A.5 Transverse walkoff in type-I PDC. This smears out the signal and idler emission pattern in different ways, and introduces additional correlations in the PDC state.

is short or the pump beam waist is broad so that the pump transverse walkoff is small compared to the beam waist, this effect can be ignored. However if a strongly focused pump is used, the transverse walkoff effect must be taken into the analysis. For type-II PDC, not only the pump, but one of the downconverted modes will experience transverse walkoff effect as well. This introduces even more complex correlations, *e.g.* time-position correlations [216].

A.4.2 Non-degenerate PDC

The above situations dicuss degenerate PDC, for which the signal and idler have exactly the same spectral characteristics. In some situations it will be convenient to consider non-degenerate situations to allow some difference between the downconverted modes. For example, the spectrally factorable state considered in Refs [211–213]

is achieved by asymmetric group velocity matching, *i.e.* matching the pump group velocity with the group velocity of one but not both of the downconverted modes. A non-degenerate situation allows us to vary the frequency of the signal mode (due to the energy conservation condition, the idler frequency is not completely independent of the signal frequency), therefore offers one more control parameter for tailoring the PDC state. Moreover, in this situation, the signal and idler modes can be distinguished using the spectral degree of freedom even for the collinear phase matching condition.

A.4.3 Fiber coupling efficiency

Coupling the downconverted photons into single-mode fibers is of particular interest, since it allows the photons to be transfered through a long distance, or benefits building integrated optical quantum information processing circuits. The coupling efficiency is crucial since it affects the scalability of the quantum information processing implementations based on photons. The state we discuss here is a signal-idler factorable state. Still there remain internal correlations, *i.e.*, between the polar angle and frequency. This frequency-angle correlation will diminish the coupling efficency. Another difficulty for calculating the coupling efficiency in spherical coordinate is that the fiber mode contains internal correlations between the polar and azimuthal angles. Therefore the calculation of the overlap between the PDC state and the fiber mode is not trivial. It is more convenient to do the calculation in Cartesian coordinates, but the PDC state engineering becomes a bit more obscure.

Appendix B

Conditional Entropy and Conditional Variance

The joint distribution $p(x, y)$ of variables X and Y can have numerous forms, which makes the conditional entropy $H(X|Y)$ difficult to estimate. However, it is possible to bound $H(X|Y)$ with some statistical properties that are more accessible, *e.g.* the variance of the variables. Recall the definition of $H(X|Y)$,

$$\begin{aligned} H(X|Y) &= -\iint dxdy\, p(x,y) \log_2 p(x|y) \\ &= -\int d\vartheta\, p(\vartheta) \int dx\, p(x|y=\vartheta) \log_2 p(x|y=\vartheta) \\ &= -\int d\vartheta\, p(\vartheta) H(X|Y=\vartheta). \end{aligned} \tag{B.1}$$

Assume the mean value and variance of the probability distribution $p(x|y=\vartheta)$ are μ_ϑ and σ_ϑ^2 respectively. Considering a normal distribution

$$g_\vartheta(x) = \frac{1}{\sigma_\vartheta\sqrt{2\pi}} \exp\left[-\frac{(x-\mu_\vartheta)^2}{2\sigma_\vartheta^2}\right], \tag{B.2}$$

we have

$$\begin{aligned}
& -\int dx\, p(x|y=\vartheta) \log_2 g_\vartheta(x) + \int dx\, g_\vartheta(x) \log_2 g_\vartheta(x) \\
= & \int dx\ [p(x|y=\vartheta) - g_\vartheta(x)] \left[\log_2(\sigma_\vartheta\sqrt{2\pi}) + \frac{(x-\mu_\vartheta)^2}{2\sigma_\vartheta^2}\right] \\
= & \int dx\ [p(x|y=\vartheta) - g_\vartheta(x)] \log_2(\sigma_\vartheta\sqrt{2\pi}) + \int dx\ [p(x|y=\vartheta) - g_\vartheta(x)] \\
& \times \frac{(x-\mu_\vartheta)^2}{2\sigma_\vartheta^2} \log_2 e \\
= & \ 0
\end{aligned} \tag{B.3}$$

where

$$\int dx\, p(x|y=\vartheta) = 1 \tag{B.4}$$

$$\int dx\, g_\vartheta(x) = 1 \tag{B.5}$$

$$\int dx\, p(x|y=\vartheta)(x-\mu_\vartheta)^2 = \sigma_\vartheta^2 \tag{B.6}$$

$$\int dx\, g_\vartheta(x)(x-\mu_\vartheta)^2 = \sigma_\vartheta^2 \tag{B.7}$$

are used.

We also have

$$\begin{aligned} H(X|Y=\vartheta) + \int dx\, p(x|y=\vartheta) \log_2 g_\vartheta(x) &= \int dx\, p(x|y=\vartheta) \log_2 \frac{g_\vartheta(x)}{p(x|y=\vartheta)} \\ &\leq \int dx\, p(x|y=\vartheta) \left[\frac{g_\vartheta(x)}{p(x|y=\vartheta)} - 1 \right] \\ &\quad \times \log_2 e \\ &= 0, \end{aligned} \tag{B.8}$$

where the inequality

$$\log x \leq x - 1, \tag{B.9}$$

Eq. B.4 and Eq. B.5 are used. Combining Eq. B.3 and Eq. B.8, we have

$$\begin{aligned} H(X|Y=\vartheta) &\leq \int dx\, g_\vartheta(x) \log_2 g_\vartheta(x) \\ &= \frac{1}{2} \log_2 \left[2\pi e \sigma_\vartheta^2 \right]. \end{aligned} \tag{B.10}$$

Substituting Eq. B.10 into Eq. B.1, we have

$$H(X|Y) \leq \frac{1}{2} \int d\vartheta\, p(\vartheta) \log_2 \left[2\pi e \sigma_\vartheta^2 \right] \tag{B.11}$$

$$\leq \frac{1}{2} \log_2 \left[2\pi e \int d\vartheta\, p(\vartheta) \sigma_\vartheta^2 \right] \tag{B.12}$$

$$= \frac{1}{2} \log_2 \left[2\pi e \Delta^2(x|y) \right], \tag{B.13}$$

where

$$\begin{aligned}\Delta^2(x|y) &= \int d\vartheta\, p(\vartheta)\sigma_\vartheta^2 \\ &= \int d\vartheta\, p(\vartheta) \int dx\, p(x|y=\vartheta)(x-\mu_\vartheta)^2 \end{aligned} \tag{B.14}$$

To derive Eq. B.12 from Eq. B.11, we use the condition that the logarithm is a concave function.

Eq. B.13 is the result we used in Chapter 4. Before concluding, we compare $\Delta^2(x|y)$ with other variances. Since

$$\int dx\, p(x|y=\vartheta)(x-\vartheta)^2 - \int dx\, p(x|y=\vartheta)(x-\mu_\vartheta)^2 = (\vartheta-\mu_\vartheta)^2 \geq 0, \tag{B.15}$$

we have

$$\begin{aligned}\Delta^2(x|y) &= \int d\vartheta\, p(\vartheta) \int dx\, p(x|y=\vartheta)(x-\mu_\vartheta)^2 \\ &\leq \int d\vartheta\, p(\vartheta) \int dx\, p(x|y=\vartheta)(x-\vartheta)^2 \\ &= \Delta^2(x-y) \end{aligned} \tag{B.16}$$

Similarly we have

$$\Delta^2(x|y) \leq \Delta^2(x+y). \tag{B.17}$$

Appendix C

The Calculation of C_{tot}

Assume m photon pairs (labeled as pair 1, pair 2 $\cdots$ pair m) are incident onto the detector array during one frame. Also, assume the detector array is operated in photon-counting mode, *i.e.* most detector noise can be ignored except the spurious charges. Then the two-dimensional pattern of the frame is

$$F^l(\mathbf{r}) = \sum_{j_s \in Q_s^l} \delta(\mathbf{r} - \mathbf{r}_{s,j_s}^l) + \sum_{j_i \in Q_i^l} \delta(\mathbf{r} - \mathbf{r}_{i,j_i}^l) + \sum_{j_n \in Q_n^l}, \delta(\mathbf{r} - \mathbf{r}_{n,j_n}^l) \tag{C.1}$$

where Q_s^l and Q_i^l are two different subsets of $\{1, 2, \cdots m\}$ due to the detection efficiency η, and $\mathbf{r}_{n,j_n}^l$ is the possible position of spurious charge. The first sum in Eq. C.1 is the contribution of signal photons, the second sum is the contribution of idler photons, and the third is due to the noise. Then the total correlation C_{tot}^n for all

the frames with the same m is

$$C^m_{tot}(\mathbf{r}) = \sum_l^{N_m} F^l * F^l = \sum_l \int d\mathbf{r}' F^l(\mathbf{r}') F^l(\mathbf{r}-\mathbf{r}'). \tag{C.2}$$

Substituting Eq. C.1 into Eq. C.2, we have

$$C^m_{tot}(\mathbf{r}) = C_{s,s}(\mathbf{r}) + C_{i,i}(\mathbf{r}) + C_{s,i}(\mathbf{r}) + C_{n,n}(\mathbf{r}) + C_{s,n}(\mathbf{r}) + C_{i,n}(\mathbf{r}), \tag{C.3}$$

where

$$C_{s,s}(\mathbf{r}) = \sum_l^{N_m} \sum_{j_s, j'_s \in Q^l_s} \delta(\mathbf{r} - \mathbf{r}^l_{s,j_s} - \mathbf{r}^l_{s,j'_s}), \tag{C.4}$$

$$C_{i,i}(\mathbf{r}) = \sum_l^{N_m} \sum_{j_i, j'_i \in Q^l_i} \delta(\mathbf{r} - \mathbf{r}^l_{i,j_i} - \mathbf{r}^l_{i,j'_i}), \tag{C.5}$$

$$C_{s,i}(\mathbf{r}) = 2\sum_l^{N_m} \sum_{j_s \in Q^l_s, j_i \in Q^l_i} \delta(\mathbf{r} - \mathbf{r}^l_{s,j_s} - \mathbf{r}^l_{i,j_i}), \tag{C.6}$$

$$C_{n,n}(\mathbf{r}) = \sum_l^{N_m} \sum_{j_n, j'_n \in Q^l_i} \delta(\mathbf{r} - \mathbf{r}^l_{n,j_n} - \mathbf{r}^l_{n,j'_n}), \tag{C.7}$$

$$C_{s,n}(\mathbf{r}) = \sum_l^{N_m} 2 \sum_{j_s \in Q^l_s, j_n \in Q^l_n} \delta(\mathbf{r} - \mathbf{r}^l_{s,j_s} - \mathbf{r}^l_{n,j_n}), \tag{C.8}$$

$$C_{i,n}(\mathbf{r}) = \sum_l^{N_m} 2 \sum_{j_i \in Q^l_i, j_n \in Q^l_n} \delta(\mathbf{r} - \mathbf{r}^l_{i,j_i} - \mathbf{r}^l_{n,j_n}), \tag{C.9}$$

Among all the terms, only $\delta(\mathbf{r} - \mathbf{r}^l_{s,j_s} - \mathbf{r}^l_{i,j_i})$ with $j_s = j_i$, *i.e.* the signal and idler photons from the same pair, contributes to the observation of the quantum correlations in the input state.

Now we consider each term in Eq. C.3.

$$\begin{aligned} C_{s,s}(\mathbf{r}) &= \sum_{l}^{N_m} \Big[\sum_{j_s=j'_s} \delta(\mathbf{r} - \mathbf{r}^l_{s,j_s} - \mathbf{r}^l_{s,j'_s}) + \sum_{j_s \neq j'_s} \delta(\mathbf{r} - \mathbf{r}^l_{s,j_s} - \mathbf{r}^l_{s,j'_s}) \Big] \\ &= \sum_{l}^{N_m} \sum_{j_s \in Q^l_s} \delta(\mathbf{r} - 2\mathbf{r}^l_{s,j_s}) + \sum_{l}^{N_m} \sum_{j_s \neq j'_s \in Q^l_s} \delta(\mathbf{r} - \mathbf{r}^l_{s,j_s} - \mathbf{r}^l_{s,j'_s}). \quad \text{(C.10)} \end{aligned}$$

Assume the marginal distribution of the position of the signal photon is $P_s(\mathbf{r})$, when N_m is large enough to ensure the number of $\mathbf{r}^l_{s,j_s}$ is approximately proportional to $P_s(\mathbf{r}^l_{s,j_s})$, then the first term in Eq. C.10 can be written as

$$\sum_{l}^{N_m} \sum_{j_s \in Q^l_s} \delta(\mathbf{r} - 2\mathbf{r}^l_{s,j_s}) = N_m m\eta \int d\mathbf{r}_s P_s(\mathbf{r}_s)\delta(\mathbf{r} - 2\mathbf{r}_s) = N_m m\eta P_s(\frac{\mathbf{r}}{2}), \quad \text{(C.11)}$$

where η is the detection efficiency, and the second term is

$$\begin{aligned} \sum_{l}^{N_m} \sum_{j_s \neq j'_s \in Q^l_s} \delta(\mathbf{r} - \mathbf{r}^l_{s,j_s} - \mathbf{r}^l_{s,j'_s}) &= N_m m\eta(m\eta - 1) \int d\mathbf{r}_s \int d\mathbf{r}'_s P_s(\mathbf{r}_s) P_s(\mathbf{r}'_s) \\ &\quad \times \delta(\mathbf{r} - \mathbf{r}_s - \mathbf{r}'_s) \\ &= N_m m\eta(m\eta - 1) \int d\mathbf{r}_s P_s(\mathbf{r}_s) P_s(\mathbf{r} - \mathbf{r}_s) \\ &= N_m m\eta(m\eta - 1) P_s(\mathbf{r}) * P_s(\mathbf{r}) \quad \text{(C.12)} \end{aligned}$$

where $*$ denotes convolution. Substituting Eqns. C.11 and C.12 into Eq. C.10, we have

$$C_{s,s}(\mathbf{r}) = N_m m\eta P_s(\frac{\mathbf{r}}{2}) + N_m m\eta(m\eta - 1) P_s(\mathbf{r}) * P_s(\mathbf{r}). \quad \text{(C.13)}$$

Similarly, we have

$$C_{i,i}(\mathbf{r}) = N_m m\eta P_i(\frac{\mathbf{r}}{2}) + N_m m\eta(m\eta - 1)P_i(\mathbf{r}) * P_i(\mathbf{r}). \tag{C.14}$$

$C_{s,i}(\mathbf{r})$ can also be split into two part

$$C_{s,i}(\mathbf{r}) = 2\sum_{l}^{N_m}\sum_{j_s=j_i}\delta(\mathbf{r} - \mathbf{r}^l_{s,j_s} - \mathbf{r}^l_{i,j_i}) + 2\sum_{l}^{N_m}\sum_{j_s\neq j_i}\delta(\mathbf{r} - \mathbf{r}^l_{s,j_s} - \mathbf{r}^l_{i,j_i}). \tag{C.15}$$

When N is large, the two terms can be written as

$$\begin{aligned}\sum_{l}^{N_m}\sum_{j_s=j_i}\delta(\mathbf{r} - \mathbf{r}^l_{s,j_s} - \mathbf{r}^l_{i,j_i}) &= N_m m\eta^2 \int d\mathbf{r}_s \int d\mathbf{r}_i P_{twin}(\mathbf{r}_s, \mathbf{r}_i)\delta(\mathbf{r} - \mathbf{r}_s - \mathbf{r}_i) \\ &= N_m m\eta^2 \int d\mathbf{r}_s P_{twin}(\mathbf{r}_s, \mathbf{r} - \mathbf{r}_s),\end{aligned} \tag{C.16}$$

and

$$\begin{aligned}\sum_{l}^{N_m}\sum_{j_s\neq j_i}\delta(\mathbf{r} - \mathbf{r}^l_{s,j_s} - \mathbf{r}^l_{i,j_i}) &= N_m m(m-1)\eta^2 \int d\mathbf{r}_s \int d\mathbf{r}_i P_s(\mathbf{r}_s)P_i(\mathbf{r}_i) \\ &\quad \times\delta(\mathbf{r} - \mathbf{r}_s - \mathbf{r}_i) \\ &= N_m m(m-1)\eta^2 \int d\mathbf{r}_s P_s(\mathbf{r}_s)P_i(\mathbf{r} - \mathbf{r}_s) \\ &= N_m m(m-1)\eta^2 P_s(\mathbf{r}) * P_i(\mathbf{r}),\end{aligned} \tag{C.17}$$

where $P_{twin}(\mathbf{r}_s, \mathbf{r}_i)$ is the joint probability distribution of the input state. Substitut-

ing Eqns. C.16 and C.16 into Eq. C.15, we have

$$C_{s,i}(\mathbf{r}) = 2N_m m\eta^2 \int d\mathbf{r}_s P_{twin}(\mathbf{r}_s, \mathbf{r}-\mathbf{r}_s) + 2N_m m(m-1)\eta^2 P_s(\mathbf{r}) * P_i(\mathbf{r}). \quad \text{(C.18)}$$

With similar analysis, we have

$$\begin{aligned} C_{n,n}(\mathbf{r}) &= N_m m_n P_n(\frac{\mathbf{r}}{2}) + N_m m_n(m_n-1) P_n(\mathbf{r}) * P_n(\mathbf{r}), & \text{(C.19)} \\ C_{s,n}(\mathbf{r}) &= N_m m\eta m_n P_s(\mathbf{r}) * P_n(\mathbf{r}), & \text{(C.20)} \\ C_{i,n}(\mathbf{r}) &= N_m m\eta m_n P_i(\mathbf{r}) * P_n(\mathbf{r}). & \text{(C.21)} \end{aligned}$$

where m_n is the averaged number of spurious charges per frame, and $P_n(\mathbf{r})$ is the distribution of spurious charges. If we consider the situation that each pixel in the detector array is identical, $P_n(\mathbf{r})$ is a uniform distribution, *i.e.*, $P_n(\mathbf{r}) = 1/\mathcal{S}$ where $\mathcal{S}$ is the size of the detector array. Eqns. C.19 – C.21 could be simplified as

$$\begin{aligned} C_{n,n}(\mathbf{r}) &= \frac{N_m m_n^2}{\mathcal{S}}, & \text{(C.22)} \\ C_{s,n}(\mathbf{r}) &= \frac{N_m m\eta m_n}{\mathcal{S}}, & \text{(C.23)} \\ C_{i,n}(\mathbf{r}) &= \frac{N_m m\eta m_n}{\mathcal{S}}. & \text{(C.24)} \end{aligned}$$

All three components do not change with $\mathbf{r}$. Note that in the derivation we assume the area $\mathcal{S}$ is much larger than the region of the distributions $P_s(\mathbf{r})$ and $P_i(\mathbf{r})$, otherwise $C_{n,n}(\mathbf{r})$, $C_{s,n}(\mathbf{r})$ and $C_{i,n}(\mathbf{r})$ fall off rapidly when $\mathbf{r}$ approachs the edge of the detector array. In our experiment, the PDC ring onto fits almost the entire

area of the EMCCD. In analysing the correlations, we artificially extend the size the detector array by extrapolating the random noise outside the original area. Substituting Eqns. C.13, C.14, C.18 and C.22 – C.24 into Eq. C.3, and denote C_{noise} as $C_{n,n} + C_{s,n} + C_{i,n}$, we have

$$\begin{aligned} C^m_{tot}(\mathbf{r}) &= N_m m\eta \left[P_s(\frac{\mathbf{r}}{2}) + P_i(\frac{\mathbf{r}}{2})\right] + N_m m\eta(m\eta - 1)\Big[P_s(\mathbf{r}) * P_s(\mathbf{r}) + P_i(\mathbf{r}) \\ &\quad * P_i(\mathbf{r})\Big] + 2N_m m\eta^2 \int d\mathbf{r}_s P_{twin}(\mathbf{r}_s, \mathbf{r} - \mathbf{r}_s) \\ &\quad + 2N_m m(m-1)\eta^2 P_s(\mathbf{r}) * P_i(\mathbf{r}) + C_{noise}. \end{aligned} \tag{C.25}$$

If the photon pair generation rate has a distribution $P(m)$, then for a total of N frames, $N_m = NP(m)$, the overall correlation is

$$C_{tot}(\mathbf{r}) = \sum_m P(m) C^m_{tot}(\mathbf{r}). \tag{C.26}$$

Substituting Eq. C.25 into Eq. C.26, and assume $\langle m \rangle \eta \gg 1$ (the average number of photon pairs detected per frame is much greater than 1, which is the situation in our experiment), we have

$$\begin{aligned} C_{tot}(\mathbf{r}) &= N\langle m \rangle \eta \left[P_s(\frac{\mathbf{r}}{2}) + P_i(\frac{\mathbf{r}}{2})\right] + N\langle m^2 \rangle \eta^2 \Big[P_s(\mathbf{r}) * P_s(\mathbf{r}) + P_i(\mathbf{r}) * P_i(\mathbf{r}) \\ &\quad + 2P_s(\mathbf{r}) * P_i(\mathbf{r})\Big] + 2N\langle m \rangle \eta^2 \int d\mathbf{r}_s P_{twin}(\mathbf{r}_s, \mathbf{r} - \mathbf{r}_s) + C_{noise}, \end{aligned} \tag{C.27}$$

where

$$\langle m \rangle = \sum_m m P(m), \tag{C.28}$$

is the mean value of m.

When the discretization effect of the detector array cannot be ignored, the intergration in Eq. 5.12 should be substituted with sum.

Bibliography

[1] O. Cohen, *Nonlocality of the original Einstein-Podolsky-Rosen state*, Phys. Rev. A, **56**, pp. 3484–3492 (1997).

[2] M. P. Almeida, S. P. Walborn, and P. H. S. Ribeiro, *Experimental investigation of quantum key distribution with position and momentum of photon pairs*, Arxiv preprint quant-ph//0411183 (2004).

[3] S. L. Braunstein and P. van Loock, *Quantum information with continuous variables*, Reviews of Modern Physics, **77**, 513 (2005).

[4] P. van Loock and S. L. Braunstein, *Multipartite Entanglement for Continuous Variables: A Quantum Teleportation Network*, Phys. Rev. Lett., **84**, pp. 3482–3485 (2000).

[5] H. Yonezawa, T. Aoki, and A. Furusawa, *Demonstration of a quantum teleportation network for continuous variables*, Nature, **431**, pp. 430–433 (2004).

[6] G. Adesso and G. Chiribella, *Quantum Benchmark for Teleportation and Storage of Squeezed States*, Physical Review Letters, **100**, 170503 (2008).

[7] H. Yonezawa, S. L. Braunstein, and A. Furusawa, *Experimental Demonstration of Quantum Teleportation of Broadband Squeezing*, Physical Review Letters, **99**, 110503 (2007).

[8] M. Ban, *Quantum dense coding via a two-mode squeezed-vacuum state*, Journal of Optics B: Quantum and Semiclassical Optics, **1**, pp. L9–L11 (1999).

[9] S. L. Braunstein and H. J. Kimble, *Dense coding for continuous variables*, Phys. Rev. A, **61**, p. 042302 (2000).

[10] T. C. Ralph, *Continuous variable quantum cryptography*, Phys. Rev. A, **61**, p. 010303 (1999).

[11] M. Hillery, *Quantum cryptography with squeezed states*, Phys. Rev. A, **61**, p. 022309 (2000).

[12] N. J. Cerf, M. Lévy, and G. V. Assche, *Quantum distribution of Gaussian keys using squeezed states*, Phys. Rev. A, **63**, p. 052311 (2001).

[13] C. Silberhorn, N. Korolkova, and G. Leuchs, *Quantum Key Distribution with Bright Entangled Beams*, Phys. Rev. Lett., **88**, p. 167902 (2002).

[14] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, *Quantum key distribution using gaussian-modulated coherent states*, Nature, **421**, pp. 238–241 (2003).

[15] L.-M. Duan, G. Giedke, J. I. Cirac, and P. Zoller, *Entanglement Purification of Gaussian Continuous Variable Quantum States*, Phys. Rev. Lett., **84**, pp. 4002–4005 (2000).

[16] E. Schrodinger, *Die gegenwrtige Situation in der Quantenmechanik*, Naturwissenschaften, **23**, pp. 807–812 (1935).

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

[18] D. Bruß, G. M. D'Ariano, M. Lewenstein, C. Macchiavello, A. Sen(De), and U. Sen, *Distributed Quantum Dense Coding*, Physical Review Letters, **93**, 210501 (2004).

[19] J. I. Latorre, *Image compression and entanglement*, Arxiv preprint quant-ph/0510031 (2005).

[20] J. T. Barreiro, T.-C. Wei, and P. G. Kwiat, *Beating the channel capacity limit for linear photonic superdense coding*, Nat Phys, **4**, pp. 282–286 (2008).

[21] H. Buhrman, R. Cleve, and W. van Dam, *Quantum Entanglement and Communication Complexity*, Arxiv preprint quant-ph/9705033 (1997).

[22] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, *Quantum repeaters based on entanglement purification*, Phys. Rev. A, **59**, pp. 169–181 (1999).

[23] A. Acín, L. Masanes, and N. Gisin, *Equivalence between Two-Qubit Entanglement and Secure Key Distribution*, Phys. Rev. Lett., **91**, p. 167901 (2003).

[24] A. Acín and N. Gisin, *Quantum Correlations and Secret Bits*, Physical Review Letters, **94**, 020501 (2005).

[25] M. Curty, M. Lewenstein, and N. Lütkenhaus, *Entanglement as a Precondition for Secure Quantum Key Distribution*, Physical Review Letters, **92**, 217903 (2004).

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

[27] D. E. Browne and T. Rudolph, *Resource-Efficient Linear Optical Quantum Computation*, Physical Review Letters, **95**, 010501 (2005).

[28] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, *Quantum entanglement*, Arxiv preprint quant-ph/0702225 (2007).

[29] R. F. Werner, *Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model*, Phys. Rev. A, **40**, pp. 4277–4281 (1989).

[30] L. Masanes, Y.-C. Liang, and A. C. Doherty, *All Bipartite Entangled States Display Some Hidden Nonlocality*, Physical Review Letters, **100**, 090403 (2008).

[31] R. Horodecki and P. Horodecki, *Quantum redundancies and local realism*, Physics Letters A, **194** (1994).

[32] M. Horodecki, J. Oppenheim, and A. Winter, *Partial quantum information*, Nature, **436**, pp. 673–676 (2005).

[33] M. Nielsen and I. Chuang, *Quantum Information and Quantum Computation*, Cambridge University Press, Cambridge, United Kingdom (2001).

[34] R. Grobe, K. Rzazewski, and J. H. Eberly, *Measure of electron-electron correlation in atomic physics*, Journal of Physics B: Atomic, Molecular and Optical Physics, **27**, pp. L503–L508 (1994).

[35] C. K. Law and J. H. Eberly, *Analysis and Interpretation of High Transverse Entanglement in Optical Parametric Down Conversion*, Physical Review Letters, **92**, 127903 (2004).

[36] S. Parker, S. Bose, and M. B. Plenio, *Entanglement quantification and purification in continuous-variable systems*, Phys. Rev. A, **61**, p. 032305 (2000).

[37] C. K. Law, I. A. Walmsley, and J. H. Eberly, *Continuous Frequency Entanglement: Effective Finite Hilbert Space and Entropy Control*, Phys. Rev. Lett., **84**, pp. 5304–5307 (2000).

[38] A. Peres, *Separability Criterion for Density Matrices*, Phys. Rev. Lett., **77**, pp. 1413–1415 (1996).

[39] K. Życzkowski, P. Horodecki, A. Sanpera, and M. Lewenstein, *Volume of the set of separable states*, Phys. Rev. A, **58**, pp. 883–892 (1998).

[40] M. B. Plenio and S. Virmani, *An introduction to entanglement measures*, QUANT.INF.COMP., **7**, p. 1 (2007).

[41] M. Horodecki, P. Horodecki, and R. Horodecki, *Mixed-State Entanglement and Distillation: Is there a Bound Entanglement in Nature?*, Phys. Rev. Lett., **80**, pp. 5239–5242 (1998).

[42] G. Vidal and R. F. Werner, *Computable measure of entanglement*, Phys. Rev. A, **65**, p. 032314 (2002).

[43] B. Terhal, *A Family of Indecomposable Positive Linear Maps based on Entangled Quantum States*, Arxiv preprint quant-ph/9810091 (1998).

[44] B. M. Terhal, *Bell inequalities and the separability criterion*, Physics Letters A, **271**, pp. 319–326 (2000).

[45] F. G. S. L. Brandao, *Quantifying entanglement with witness operators*, Physical Review A (Atomic, Molecular, and Optical Physics), **72**, 022310 (2005).

[46] O. Gühne and N. Lütkenhaus, *Nonlinear Entanglement Witnesses*, Physical Review Letters, **96**, 170502 (2006).

[47] J. Eisert, F. G. S. L. Brandao, and K. M. R. Audenaert, *Quantitative entanglement witnesses*, New Journal of Physics, **9**, pp. 46–46 (2007).

[48] M. Hillery and M. S. Zubairy, *Entanglement conditions for two-mode states*, Physical Review Letters, **96**, p. 050503 (2006).

[49] J. C. Howell, R. S. Bennink, S. J. Bentley, and R. W. Boyd, *Realization of the Einstein-Podolsky-Rosen Paradox Using Momentum- and Position-Entangled Photons from Spontaneous Parametric Down Conversion*, Physical Review Letters, **92**, 210403 (2004).

[50] M. Stobińska and K. Wódkiewicz, *Witnessing entanglement with second-order interference*, Physical Review A (Atomic, Molecular, and Optical Physics), **71**, 032304 (2005).

[51] O. Gühne, P. Hyllus, D. Bruß, A. Ekert, M. Lewenstein, C. Macchiavello, and A. Sanpera, *Detection of entanglement with few local measurements*, Phys. Rev. A, **66**, p. 062305 (2002).

[52] O. Gühne, P. Hyllus, D. Bruss, A. Ekert, M. Lewenstein, C. Macchiavello, and A. Sanpera, *Experimental detection of entanglement via witness operators and local measurements*, Journal of Modern Optics, **50**, pp. 1079–1102 (2003).

[53] A. Einstein, B. Podolsky, and N. Rosen, *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?*, Phys. Rev., **47**, pp. 777–780 (1935).

[54] J. S. Bell, *On the Einstein-Podolsky-Rosen paradox*, Speakable and Unspeakable in Quantum Mechanics, Cambridge University Press, Cambridge, England (1987).

[55] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, *Proposed Experiment to Test Local Hidden-Variable Theories*, Phys. Rev. Lett., **23**, pp. 880–884 (1969).

[56] A. Aspect, P. Grangier, and G. Roger, *Experimental Tests of Realistic Local Theories via Bell's Theorem*, Phys. Rev. Lett., **47**, pp. 460–463 (1981).

[57] A. Aspect, J. Dalibard, and G. Roger, *Experimental Test of Bell's Inequalities Using Time- Varying Analyzers*, Phys. Rev. Lett., **49**, pp. 1804–1807 (1982).

[58] 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**, pp. 4337–4341 (1995).

[59] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, *Violation of Bell Inequalities by Photons More Than 10 km Apart*, Phys. Rev. Lett., **81**, pp. 3563–3566 (1998).

[60] 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**, pp. 5039–5043 (1998).

[61] N. Gisin, *Bell's inequality holds for all non-product states*, Physics Letters A, **154**, pp. 201–202 (1991).

[62] N. Gisin and A. Peres, *Maximal violation of Bell's inequality for arbitrarily large spin*, Physics Letters A, **162**, pp. 15–17 (1992).

[63] P. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, Appl. Math. J. Comp, **26**, pp. 1484–1509 (1997).

[64] S. Wiesner, *Conjugate coding*, ACM SIGACT News, **15**, pp. 78–88 (1983).

[65] C. Bennett, G. Brassard, et al., *Quantum cryptography: Public key distribution and coin tossing*, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, pp. 175–179 (1984).

[66] H. Bechmann-Pasquinucci, *Eavesdropping without quantum memory*, Physical Review A (Atomic, Molecular, and Optical Physics), **73**, 044305 (2006).

[67] T. Kim, I. S. genannt Wersborg, F. N. C. Wong, and J. H. Shapiro, *Complete physical simulation of the entangling-probe attack on the Bennett-Brassard 1984 protocol*, Physical Review A (Atomic, Molecular, and Optical Physics), **75**, 042327 (2007).

[68] E. Waks, A. Zeevi, and Y. Yamamoto, *Security of quantum key distribution with entangled photons against individual attacks*, Phys. Rev. A, **65**, p. 052310 (2002).

[69] D. Collins, N. Gisin, and H. de Riedmatten, *Quantum Relays for Long Distance Quantum Cryptography*, Arxiv preprint quant-ph/0311101 (2003).

[70] C. Bennett, G. Brassard, and J. Robert, *Privacy Amplification by Public Discussion*, SIAM Journal on Computing, **17**, p. 210 (1988).

[71] C. Bennett, G. Brassard, C. Crepeau, U. Maurer, I. Center, and Y. Heights, *Generalized privacy amplification*, IEEE Transactions on Information Theory, **41**, pp. 1915–1923 (1995).

[72] C. H. Bennett, *Quantum cryptography using any two nonorthogonal states*, Phys. Rev. Lett., **68**, pp. 3121–3124 (1992).

[73] D. Bruß, *Optimal Eavesdropping in Quantum Cryptography with Six States*, Phys. Rev. Lett., **81**, pp. 3018–3021 (1998).

[74] W.-H. Kye, C.-M. Kim, M. S. Kim, and Y.-J. Park, *Quantum Key Distribution with Blind Polarization Bases*, Physical Review Letters, **95**, p. 040501 (2005).

[75] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, *Quantum Cryptography Using Entangled Photons in Energy-Time Bell States*, Phys. Rev. Lett., **84**, pp. 4737–4740 (2000).

[76] K. Inoue, E. Waks, and Y. Yamamoto, *Differential Phase Shift Quantum Key Distribution*, Phys. Rev. Lett., **89**, p. 037902 (2002).

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

[78] N. Gisin and S. Wolf, *Quantum Cryptography on Noisy Channels: Quantum versus Classical Key-Agreement Protocols*, Phys. Rev. Lett., **83**, pp. 4200–4203 (1999).

[79] A. Acín, N. Gisin, and L. Masanes, *From Bell's Theorem to Secure Quantum Key Distribution*, Physical Review Letters, **97**, 120405 (2006).

[80] B. Huttner, N. Imoto, N. Gisin, and T. Mor, *Quantum cryptography with coherent states*, Phys. Rev. A, **51**, pp. 1863–1869 (1995).

[81] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, *Limitations on Practical Quantum Cryptography*, Phys. Rev. Lett., **85**, pp. 1330–1333 (2000).

[82] N. Lütkenhaus and M. Jahma, *Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack*, New Journal of Physics, **4**, pp. 44–44 (2002).

[83] H.-K. Lo, X. Ma, and K. Chen, *Decoy State Quantum Key Distribution*, Physical Review Letters, **94**, 230504 (2005).

[84] W.-Y. Hwang, *Quantum Key Distribution with High Loss: Toward Global Secure Communication*, Phys. Rev. Lett., **91**, p. 057901 (2003).

[85] X. Ma, B. Qi, Y. Zhao, and H. K. Lo, *Practical Decoy State for Quantum Key Distribution*, Physical Review A, **72**, p. 012326 (2005).

[86] X.-B. Wang, *Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography*, Physical Review Letters, **94**, 230503 (2005).

[87] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, *Experimental Quantum Key Distribution with Decoy States*, Physical Review Letters, **96**, 070502 (2006).

[88] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, *Long-Distance Decoy-State Quantum Key Distribution in Optical Fiber*, Physical Review Letters, **98**, 010503 (2007).

[89] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, *Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km*, Physical Review Letters, **98**, 010504 (2007).

[90] Q. Wang, W. Chen, G. Xavier, M. Swillo, T. Zhang, S. Sauge, M. Tengner, Z.-F. Han, G.-C. Guo, and A. Karlsson, *Experimental Decoy-State Quantum Key Distribution with a Sub-Poissionian Heralded Single-Photon Source*, Physical Review Letters, **100**, 090501 (2008).

[91] C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, *Experimental Long-Distance Decoy-State Quantum Key Distribution Based on Polarization Encoding*, Physical Review Letters, **98**, 010505 (2007).

[92] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, *Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations*, Physical Review Letters, **92**, 057901 (2004).

[93] T. C. Ralph, *Security of continuous-variable quantum cryptography*, Phys. Rev. A, **62**, p. 062306 (2000).

[94] M. Reid, *Quantum cryptography with a predetermined key, using continuous-variable Einstein-Podolsky-Rosen correlations*, Phys. Rev. A, **62**, p. 062308 (2000).

[95] F. Grosshans and P. Grangier, *Continuous variable quantum cryptography using coherent states*, Physical Review Letters, **88**, p. 057902 (2002).

[96] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, *Continuous Variable Quantum Cryptography: Beating the 3 dB Loss Limit*, Phys. Rev. Lett., **89**, p. 167901 (2002).

[97] R. Namiki and T. Hirano, *Practical Limitation for Continuous-Variable Quantum Cryptography using Coherent States*, Physical Review Letters, **92**, 117901 (2004).

[98] F. Grosshans and N. J. Cerf, *Continuous-Variable Quantum Cryptography is Secure against Non-Gaussian Attacks*, Phys. Rev. Lett., **92**, p. 047905 (2004).

[99] F. Grosshans, *Collective Attacks and Unconditional Security in Continuous Variable Quantum Key Distribution*, Physical Review Letters, **94**, 020504 (2005).

[100] S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, *Continuous-variable quantum cryptography using two-way quantum communication*, Nature Phys., **4**, pp. 726–730 (2008).

[101] T. D. Newton and E. P. Wigner, *Localized States for Elementary Systems*, Rev. Mod. Phys., **21**, pp. 400–406 (1949).

[102] J. Jauch and C. Piron, *Generalized localizability*, Helv. Phys. Acta, **40**, pp. 559–570 (1967).

[103] L. Mandel, *Configuration-Space Photon Number Operators in Quantum Optics*, Phys. Rev., **144**, pp. 1071–1077 (1966).

[104] I. Bialynicki-Birula, *Exponential Localization of Photons*, Phys. Rev. Lett., **80**, pp. 5247–5250 (1998).

[105] I. Bialynicki-Birula, *Photon wave function*, Arxiv preprint quant-ph/0508202 (2005).

[106] J. E. Sipe, *Photon wave functions*, Phys. Rev. A, **52**, pp. 1875–1883 (1995).

[107] B. J. Smith and M. G. Raymer, *Photon wave functions, wave-packet quantization of light, and coherence theory*, New Journal of Physics, **9**, p. 414 (2007).

[108] M. V. Fedorov, M. A. Efremov, A. E. Kazakov, K. W. Chan, C. K. Law, and J. H. Eberly, *Spontaneous emission of a photon: Wave-packet structures and atom-photon entanglement*, Physical Review A (Atomic, Molecular, and Optical Physics), **72**, 032110 (2005).

[109] S. P. Walborn, D. S. Lemelle, M. P. Almeida, and P. H. S. Ribeiro, *Quantum Key Distribution with Higher-Order Alphabets Using Spatially Encoded Qudits*, Physical Review Letters, **96**, 090501 (2006).

[110] I. Ali-Khan, C. J. Broadbent, and J. C. Howell, *Large-Alphabet Quantum Key Distribution Using Energy-Time Entangled Bipartite States*, Physical Review Letters, **98**, 060503 (2007).

[111] P. G. Kwiat, *Hyper-entangled states*, Journal of Modern Optics, **44**, pp. 2173–2184 (1997).

[112] J. T. Barreiro, N. K. Langford, N. A. Peters, and P. G. Kwiat, *Generation of Hyperentangled Photon Pairs*, Physical Review Letters, **95**, 260501 (2005).

[113] L. Aolita and S. P. Walborn, *Quantum Communication without Alignment using Multiple-Qubit Single-Photon States*, Physical Review Letters, **98**, 100501 (2007).

[114] D. C. Burnham and D. L. Weinberg, *Observation of Simultaneity in Parametric Production of Optical Photon Pairs*, Phys. Rev. Lett., **25**, pp. 84–87 (1970).

[115] S. Friberg, C. K. Hong, and L. Mandel, *Measurement of Time Delays in the Parametric Production of Photon Pairs*, Phys. Rev. Lett., **54**, pp. 2011–2013 (1985).

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

[117] P. A. Franken and J. F. Ward, *Optical Harmonics and Nonlinear Phenomena*, Rev. Mod. Phys., **35**, pp. 23–39 (1963).

[118] A. G. White, D. F. V. James, P. H. Eberhard, and P. G. Kwiat, *Nonmaximally Entangled States: Production, Characterization, and Utilization*, Phys. Rev. Lett., **83**, pp. 3103–3107 (1999).

[119] C. H. Monken, P. H. S. Ribeiro, and S. Pádua, *Transfer of angular spectrum and image formation in spontaneous parametric down-conversion*, Phys. Rev. A, **57**, pp. 3123–3126 (1998).

[120] M. P. Almeida and P. H. S. Ribeiro, *Transmission of Quantum Images Through Long Distances*, Arxiv preprint quant-ph/0312134 (2003).

[121] D. P. Caetano, P. H. Souto Ribeiro, J. T. C. Pardal, and A. Z. Khoury, *Quantum image control through polarization entanglement in parametric down-conversion*, Phys. Rev. A, **68**, p. 023805 (2003).

[122] A. Gatti, E. Brambilla, and L. A. Lugiato, *Entangled Imaging and Wave-Particle Duality: From the Microscopic to the Macroscopic Realm*, Phys. Rev. Lett., **90**, p. 133603 (2003).

[123] A. Vaziri, G. Weihs, and A. Zeilinger, *Experimental Two-Photon, Three-Dimensional Entanglement for Quantum Communication*, Phys. Rev. Lett., **89**, p. 240401 (2002).

[124] N. K. Langford, R. B. Dalton, M. D. Harvey, J. L. O'Brien, G. J. Pryde, A. Gilchrist, S. D. Bartlett, and A. G. White, *Measuring Entangled Qutrits and Their Use for Quantum Bit Commitment*, Physical Review Letters, **93**, 053601 (2004).

[125] 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*, Physical Review Letters, **95**, p. 200502 (2005).

[126] P. R. Tapster, J. G. Rarity, and P. C. M. Owens, *Violation of Bell's Inequality over 4 km of Optical Fiber*, Phys. Rev. Lett., **73**, pp. 1923–1926 (1994).

[127] 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**, pp. R2267–R2269 (1998).

[128] M. M. Fejer, G. A. Magel, D. H. Jundt, and R. L. Byer, *Quasi-phase-matched second harmonic generation: tuning andtolerances*, IEEE Journal of Quantum Electronics, **28**, pp. 2631–2654 (1992).

[129] M. H. Rubin, D. N. Klyshko, Y. H. Shih, and A. V. Sergienko, *Theory of two-photon entanglement in type-II optical parametric down-conversion*, Phys. Rev. A, **50**, pp. 5122–5133 (1994).

[130] M. H. Rubin, *Transverse correlation in optical spontaneous parametric down-conversion*, Phys. Rev. A, **54**, pp. 5349–5360 (1996).

[131] P. M. Leung, W. J. Munro, K. Nemoto, and T. C. Ralph, *Spectral effects of strong chi[sup (2)] nonlinearity for quantum processing*, Physical Review A (Atomic, Molecular, and Optical Physics), **79**, 042307 (2009).

[132] J. E. Midwinter and J. Warner, *The effects of phase matching method and of uniaxial crystal symmetry on the polar distribution of second-order non-linear optical polarization*, British Journal of Applied Physics, **16**, pp. 1135–1142 (1965).

[133] A. Yariv, *Quantum Electronics*, Wiley&Sons, New York (1989).

[134] C. I. Osorio, A. Valencia, and J. P. Torres, *Spatiotemporal correlations in entangled photons generated by spontaneous parametric down conversion*, New Journal of Physics, **10**, pp. 113012– (2008).

[135] S. P. Walborn, A. N. de Oliveira, S. Pádua, and C. H. Monken, *Multimode Hong-Ou-Mandel Interference*, Phys. Rev. Lett., **90**, p. 143601 (2003).

[136] M. P. van Exter, A. Aiello, S. S. R. Oemrawsingh, G. Nienhuis, and J. P. Woerdman, *Effect of spatial filtering on the Schmidt decomposition of entangled photons*, Physical Review A (Atomic, Molecular, and Optical Physics), **74**, 012309 (2006).

[137] W. Wasilewski and M. G. Raymer, *Pairwise entanglement and readout of atomic-ensemble and optical wave-packet modes in traveling-wave Raman interactions*, Physical Review A (Atomic, Molecular, and Optical Physics), **73**, 063816 (2006).

[138] L.-M. Duan, G. Giedke, J. I. Cirac, and P. Zoller, *Inseparability criterion for continuous variable systems*, Physical Review Letters, **84**, p. 2722 (2000).

[139] R. Simon, *Peres-Horodecki Separability Criterion for Continuous Variable Systems*, Phys. Rev. Lett., **84**, pp. 2726–2729 (2000).

[140] S. Mancini, V. Giovannetti, D. Vitali, and P. Tombesi, *Entangling Macroscopic Oscillators Exploiting Radiation Pressure*, Phys. Rev. Lett., **88**, p. 120401 (2002).

[141] V. Giovannetti, S. Mancini, D. Vitali, and P. Tombesi, *Characterizing the entanglement of bipartite quantum systems*, Phys. Rev. A, **67**, p. 022320 (2003).

[142] V. Scarani and N. Gisin, *Quantum Communication between N Partners and Bell's Inequalities*, Phys. Rev. Lett., **87**, p. 117901 (2001).

[143] J. Barrett, L. Hardy, and A. Kent, *No Signaling and Quantum Key Distribution*, Physical Review Letters, **95**, p. 10503 (2005).

[144] B. S. Cirel'son, *Quantum generalizations of Bell's inequality*, Letters in Mathematical Physics, **4**, pp. 93–100 (1980).

[145] P. Grangier, *Quantum physics: Count them all*, Nature, **409**, pp. 774–775 (2001).

[146] A. Aspect, *Bell's inequality test: more ideal than ever*, Nature, **398**, pp. 189–190 (1999).

[147] A. Garg and N. D. Mermin, *Detector inefficiencies in the Einstein-Podolsky-Rosen experiment*, Phys. Rev. D, **35**, pp. 3831–3835 (1987).

[148] P. M. Pearle, *Hidden-Variable Example Based upon Data Rejection*, Phys. Rev. D, **2**, pp. 1418–1425 (1970).

[149] J. F. Clauser and M. A. Horne, *Experimental consequences of objective local theories*, Phys. Rev. D, **10**, pp. 526–535 (1974).

[150] P. G. Kwiat, P. H. Eberhard, A. M. Steinberg, and R. Y. Chiao, *Proposal for a loophole-free Bell inequality experiment*, Phys. Rev. A, **49**, pp. 3209–3220 (1994).

[151] S. F. Huelga, M. Ferrero, and E. Santos, *Loophole-free test of the Bell inequality*, Phys. Rev. A, **51**, pp. 5008–5011 (1995).

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

[153] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu, *Bell Inequalities for Arbitrarily High-Dimensional Systems*, Phys. Rev. Lett., **88**, p. 040404 (2002).

[154] J. S. Bell, *EPR correlations and EPW distributions*, Speakable and Unspeakable in Quantum Mechanics, Cambridge University Press, Cambridge, England, (1987).

[155] K. Banaszek and K. Wódkiewicz, *Nonlocality of the Einstein-Podolsky-Rosen state in the Wigner representation*, Phys. Rev. A, **58**, pp. 4345–4347 (1998).

[156] E. Wigner, *On the Quantum Correction For Thermodynamic Equilibrium*, Phys. Rev., **40**, pp. 749–759 (1932).

[157] A. Royer, *Wigner function as the expectation value of a parity operator*, Phys. Rev. A, **15**, pp. 449–450 (1977).

[158] E. Mukamel, K. Banaszek, I. A. Walmsley, and C. Dorrer, *Direct measurement of the spatial Wigner function with area-integrated detection*, Opt. Lett., **28**, pp. 1317–1319 (2003).

[159] B. J. Smith, B. Killett, M. G. Raymer, I. A. Walmsley, and K. Banaszek, *Measurement of the transverse spatial quantum state of light at the single-photon level*, Opt. Lett., **30**, pp. 3365–3367 (2005).

[160] K. Banaszek and K. Wódkiewicz, *Testing Quantum Nonlocality in Phase Space*, Phys. Rev. Lett., **82**, pp. 2009–2013 (1999).

[161] T. Yarnall, A. F. Abouraddy, B. E. A. Saleh, and M. C. Teich, *Experimental Violation of Bell's Inequality in Spatial-Parity Space*, Physical Review Letters, **99**, 170408 (2007).

[162] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Quantum Cryptography*, Arxiv preprint quant-ph/0101098 (2001).

[163] M. N. O'Sullivan-Hale, I. A. Khan, R. W. Boyd, and J. C. Howell, *Pixel Entanglement: Experimental Realization of Optically Entangled d = 3 and d = 6 Qudits*, Physical Review Letters, **94**, 220501 (2005).

[164] L. Neves, G. Lima, J. G. A. Gómez, C. H. Monken, C. Saavedra, and S. Pádua, *Generation of Entangled States of Qudits using Twin Photons*, Physical Review Letters, **94**, 100501 (2005).

[165] L. Zhang, A. U'ren, R. Erdmann, K. O'Donnell, C. Silberhorn, K. Banaszek, and I. Walmsley, *Generation of highly entangled photon pairs for continuous variable Bell inequality violation*, Journal of Modern Optics, **54**, pp. 707–719 (2007).

[166] C. E. Shannon, *A Mathematical Theory of Communication*, Bell System Technical Journal, **27**, pp. 379–423, 623–656 (1948).

[167] G. Brassard and L. Salvail, *Secret-Key Reconciliation by Public Discussion*, Lecture Notes in Computer Science, **765**, pp. 410–423 (1994).

[168] W. T. Buttler, S. K. Lamoreaux, J. R. Torgerson, G. H. Nickel, C. H. Donahue, and C. G. Peterson, *Fast, efficient error reconciliation for quantum cryptography*, Phys. Rev. A, **67**, p. 052303 (2003).

[169] G. Van Assche, J. Cardinal, and N. Cerf, *Reconciliation of a quantum-distributed Gaussian key*, IEEE Transactions on Information Theory, **50**, pp. 394–400 (2004).

[170] F. Grosshans and P. Grangier, *Reverse reconciliation protocols for quantum cryptography with continuous variables*, Arxiv preprint quant-ph/0204127 (2002).

[171] I. Csiszar and J. Korner, *Broadcast channels with confidential messages*, IEEE Transactions on Information Theory, **24**, pp. 339–348 (1978).

[172] I. Bialynicki-Birula and J. Mycielski, *Uncertainty relations for information entropy in wave mechanics*, Communications in mathematical physics, **4**, pp. 129–132 (1975).

[173] W. Beckner, *Inequalities in Fourier Analysis*, The Annals of Mathematics, **102**, pp. 159–182 (1975).

[174] H. Maassen and J. B. M. Uffink, *Generalized entropic uncertainty relations*, Phys. Rev. Lett., **60**, pp. 1103–1106 (1988).

[175] M. J. W. Hall, *Information Exclusion Principle for Complementary Observables*, Phys. Rev. Lett., **74**, pp. 3307–3311 (1995).

[176] T. Cover, J. Thomas, J. Wiley, and W. InterScience, *Elements of Information Theory*, Wiley-Interscience New York (2006).

[177] M. D. Reid and P. D. Drummond, *Quantum Correlations of Phase in Nondegenerate Parametric Oscillation*, Phys. Rev. Lett., **60**, pp. 2731–2733 (1988).

[178] M. D. Reid, *Demonstration of the Einstein-Podolsky-Rosen paradox using nondegenerate parametric amplification*, Phys. Rev. A, **40**, pp. 913–923 (1989).

[179] B. J. Smith and M. G. Raymer, *Two-photon wave mechanics*, Physical Review A (Atomic, Molecular, and Optical Physics), **74**, 062104 (2006).

[180] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Oemer, M. Fuerst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, *Free-Space distribution of entanglement and single photons over 144 km*, NATURE PHYSICS, **3**, p. 481 (2007).

[181] I. I. Kim, B. McArthur, and E. Korevaar, *Comparison of laser beam propagation at 785 nm and 1550 nm in fog and haze for optical wireless communications*, Proc. SPIE, **4214**, pp. 26–37 (2001).

[182] I. Devetak and A. Winter, *Relating Quantum Privacy and Quantum Coherence: An Operational Approach*, Phys. Rev. Lett., **93**, p. 080501 (2004).

[183] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, *Virtual Entanglement and Reconciliation Protocols for Quantum Cryptography with Continuous Variables*, Arxiv preprint quant-ph/0306141 (2003).

[184] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, *Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels*, Phys. Rev. Lett., **76**, p. 722 (1996).

[185] L. Jiang, E. Dauler, and J. Chang, *Photon-number-resolving detector with 10bits of resolution*, Physical Review A, **75**, p. 62325 (2007).

[186] B. Jost, A. Sergienko, A. Abouraddy, B. Saleh, and M. Teich, *Spatial correlations of spontaneously down-converted photon pairs detected with asingle-photon-sensitive CCD camera*, Opt. Express, **3**, pp. 81–88 (1998).

[187] S. S. R. Oemrawsingh, W. J. van Drunen, E. R. Eliel, and J. P. Woerdman, *Two-dimensional wave-vector correlations in spontaneous parametric down-conversion explored with an intensified CCD camera*, J. Opt. Soc. Am. B, **19**, pp. 2391–2395 (2002).

[188] R. Tubbs, *Lucky Exposures: Diffraction limited astronomical imaging through the atmosphere*, Arxiv preprint astro-ph/0311481 (2003).

[189] S. Flyckt and C. Marmonier, *Photomultiplier tubes: Principles and applications*, Photonis, Brive, France (2002).

[190] J. Janesick, *Scientific Charge-Coupled Devices*, SPIE Press (2001).

[191] B. Robbins, M.S.; Hadwen, *The noise performance of electron multiplying charge-coupled devices*, IEEE Transactions on Electron Devices, **50**, pp. 1227–1232 (2003).

[192] G. de Vree, A. Westra, I. Moody, F. van der Have, K. Ligtvoet, and F. Beekman, *Photon-counting gamma camera based on an electron-multiplying CCD*, IEEE Transactions on Nuclear Science, **52**, pp. 580–588 (2005).

[193] A. G. Basden, C. A. Haniff, and C. D. Mackay, *Photon counting strategies with low light level CCDs*, Mon. Not. R. Astron. Soc., **345**, p. 985 (2003).

[194] *Low-Light Technical Note 4: Dark Signal and Clock-Induced Charg in L3Vision CCD Sensors*, Technical report, E2V Technologies Ltd. (2004).

[195] S. Tulloch, *Photon counting and fast photometry with L3 CCDs*, Proceedings of SPIE, **5492**, pp. 604–614 (2004).

[196] *Low-Light Technical Note 5: An Overview of the Ageing Characteristics of L3Vision Sensors*, Technical report, E2V Technologies Ltd. (2006).

[197] A. Cabello, *Bipartite Bell inequalities for hyperentangled states*, Physical Review Letters, **97**, p. 140406 (2006).

[198] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, *Security of Quantum Key Distribution Using d-Level Systems*, Phys. Rev. Lett., **88**, p. 127902 (2002).

[199] D. Kaszlikowski, P. Gnaciński, M. Żukowski, W. Miklaszewski, and A. Zeilinger, *Violations of Local Realism by Two Entangled N-Dimensional Systems Are Stronger than for Two Qubits*, Phys. Rev. Lett., **85**, pp. 4418–4421 (2000).

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

[201] D. Ljunggren and M. Tengner, *Optimal focusing for maximal collection of entangled narrow-band photon pairs into single-mode fibers*, Physical Review A (Atomic, Molecular, and Optical Physics), **72**, 062301 (2005).

[202] A. Ling, A. Lamas-Linares, and C. Kurtsiefer, *Absolute emission rates of spontaneous parametric down-conversion into single transverse Gaussian modes*, Physical Review A (Atomic, Molecular, and Optical Physics), **77**, 043834 (2008).

[203] K. Yamamoto, K. Yamamura, K. Sato, T. Ota, H. Suzuki, and S. Ohsuka, *Development of multi-pixel photon counter (MPPC)*, IEEE Nuclear Science Symposium Conference Record, **2**, pp. 1094–1097 (2006).

[204] I. Afek, A. Natan, O. Ambar, and Y. Silberberg, *Quantum state measurements using multi-pixel photon detectors*, Arxiv preprint 0903.1415 (2009).

[205] I. A. Khan and J. C. Howell, *Experimental demonstration of high two-photon time-energy entanglement*, Physical Review A (Atomic, Molecular, and Optical Physics), **73**, 031801 (2006).

[206] 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**, p. 093601 (2004).

[207] Z. Zhao, Y.-A. Chen, A.-N. Zhang, T. Yang, H. J. Briegel, and J.-W. Pan, *Experimental demonstration of five-photon entanglement and open-destination teleportation*, Nature, **430**, pp. 54–58 (2004).

[208] R. Kaltenbaek, B. Blauensteiner, M. Żukowski, M. Aspelmeyer, and A. Zeilinger, *Experimental Interference of Independent Photons*, Physical Review Letters, **96**, 240502 (2006).

[209] J. Fulconis, O. Alibart, J. L. O'Brien, W. J. Wadsworth, and J. G. Rarity, *Nonclassical Interference and Entanglement Generation Using a Photonic Crystal Fiber Pair Photon Source*, Physical Review Letters, **99**, 120501 (2007).

[210] A. B. U'Ren, E. Mukamel, K. Banaszek, and I. A. Walmsley, *Managing Photons for Quantum Information Processing*, Philosophical Transactions: Mathematical, Physical and Engineering Sciences, **361**, pp. 1493–1506 (2003).

[211] A. B. U'ren, C. Silberhorn, K. Banaszek, I. A. Walmsley, R. Erdmann, W. Grice, and M. Raymer, *Generation of Pure-State Single-Photon Wavepacketes by Conditional Preparation Based on Spontaneous Parametric Downconversion*, Laser Physics, **15**, p. 146 (2005).

[212] P. J. Mosley, J. S. Lundeen, B. J. Smith, P. Wasylczyk, A. B. U'Ren, C. Silberhorn, and I. A. Walmsley, *Heralded Generation of Ultrafast Single Photons in Pure Quantum States*, Physical Review Letters, **100**, 133601 (2008).

[213] P. J. Mosley, J. S. Lundeen, B. J. Smith, and I. A. Walmsley, *Conditional preparation of single photons using parametric downconversion: a recipe for purity*, New Journal of Physics, **10**, pp. 093011– (2008).

[214] C. I. Osorio, G. Molina-Terriza, B. G. Font, and J. P. Torres, *Azimuthal distinguishability of entangled photons generated in spontaneous parametric downconversion*, Opt. Express, **15**, pp. 14636–14643 (2007).

[215] J. P. Torres, G. Molina-Terriza, and L. Torner, *The spatial shape of entangled photon states generated in non-collinear, walking parametric downconversion*, Journal of Optics B: Quantum and Semiclassical Optics, **7**, pp. 235–239 (2005).

[216] P. J. Mosley, *Generation of Heralded Single Photons in Pure Quantum States*, Ph.D. thesis, University of Oxford (2007).