Experimental quantum optics

A theoretical framework for quantum-optical communication - towards CV-QKD

Master thesis by

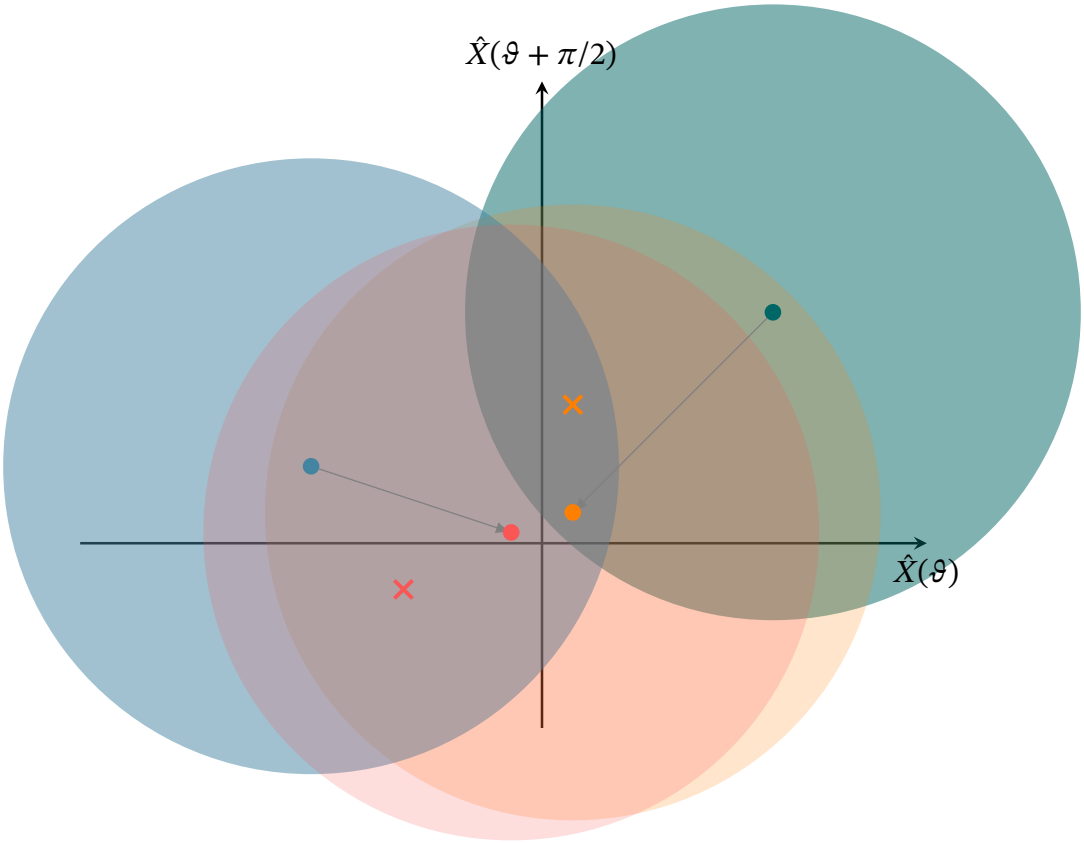
Bodo Kaiser
bodo.kaiser@physik.uni-muenchen.de

December 5, 2021

Internal supervisor: Prof. Dr. Monika Aidelsburger
External supervisor: Dr. Hans H. Brunner

Experimentelle Quantenoptik

Ein theoretisches Rahmenwerk für quantenoptische Kommunikation am Beispiel von CV-QKD



Masterarbeit von

Bodo Kaiser
bodo.kaiser@physik.uni-muenchen.de

5. Dezember 2021

Interner Betreuer:	Prof. Dr. Monika Aidelsburger
Externer Betreuer:	Dr. Hans H. Brunner

Abstract

Quantum-optical communication combines quantum aspects of light and communication engineering to bring forth novel approaches to communication. One of these approaches is quantum-key distribution, enabling practical and secure-key generation. As a fledgling discipline, quantum-optical communication lacks a unified theoretical framework on which both communication engineers and quantum physicists agree. Single-mode quantum optics, the standard framework used to describe the quantum properties of light, lacks the notion of a continuous spectrum, essential for communication theory.

The present thesis aims to deliver the missing theoretical framework for quantum-optical communication by reviewing the quantum description of a coherent-state transmission system implementing quantum-key distribution (QKD) in three steps: First, we present and compare QKD protocols and argue why continuous-variable quantum-key distribution (CV-QKD) resembles a coherent-state transmission system. Second, we derive a continuous-mode quantum theory of light rooted in quantum field-theory and apply it to describe the building blocks of a coherent-state transmission system. Third, we assemble the previously derived building blocks into a coherent-state transmission system and compare them to a software-defined implementation of a coherent-transmission system, emphasizing signal-processing aspects.

Our continuous-mode quantum theory of light is compatible with the few references on continuous-mode quantum optics but is more transparent in the underlying assumptions. Applied to quantum-optical communication, we motivate a generalized quadrature operator, which accounts for measurements of particular frequency bands. Furthermore, we show that the electro-optical in-phase/quadrature (I/Q) modulator and balanced detector implement up- and downconversion of classical signal processing. Applied to CV-QKD, we find a self-contained description that the respective domain experts can agree on, allowing for a future transfer of methods between quantum optics and communication engineering.

Notation

We mostly adopt the mathematical notation from popular quantum field-theory books, e.g. Refs. [1, 2].

Throughout the thesis, we exclusively use the natural unit system, where the natural constants, i.e., speed of light c, reduced Planck constant $\hbar$, electric charge e, electron mass m_e, dielectric constant ε_0, are set to one, significantly reducing notational clutter. If required, one can restore the SI units by dimensional analysis.

If not explicitly stated, the integration domain covers the n-dimensional real numbers, $\mathbb{R}^n$.

For the temporal Fourier transform, we choose the convention

$$f(t) = \int \frac{\mathrm{d}\omega}{2\pi} f(\omega) e^{+i\omega t} \qquad\qquad f(\omega) = \int \mathrm{d}t\, f(t) e^{-i\omega t}.$$

For the spatial Fourier transform, we choose the convention

$$f(\mathbf{x}) = \int \frac{\mathrm{d}^3 p}{(2\pi)^3} f(\mathbf{p}) e^{-i\mathbf{p}\cdot\mathbf{x}} \qquad\qquad f(\mathbf{p}) = \int \mathrm{d}^3 x\, f(\mathbf{x}) e^{+i\mathbf{p}\cdot\mathbf{x}}.$$

The four-dimensional (spacetime), Fourier transform follows from the combined temporal and spatial Fourier transform

$$f(t,\mathbf{x}) = \int \frac{\mathrm{d}^4 p}{(2\pi)^4} f(p_0,\mathbf{p}) e^{+ip_0 t - i\mathbf{p}\cdot\mathbf{x}} \qquad f(p_0,\mathbf{p}) = \int \mathrm{d}^4 x\, f(t,\mathbf{x}) e^{-ip_0 t + i\mathbf{p}\cdot\mathbf{x}}$$

where we identify p_0 with the energy ω. We denote the convolution operator with $*$, i.e,

$$(f * g)(t) = \int \mathrm{d}t'\, f(t') g(t - t') = \int \frac{\mathrm{d}\omega}{2\pi} f(\omega) g(\omega) e^{+i\omega t}$$

in the frequency and

$$(f * g)(\omega) = \int \frac{\mathrm{d}\omega'}{2\pi} f(\omega') g(\omega - \omega') = \int \mathrm{d}t\, f(t) g(t) e^{-i\omega t}$$

in the time domain.

To become proficient with the Minkowski metric and tensors, we recommend the study of Ref. [3]. Three-dimensional vectors are denoted by boldface, i.e.,

$$\mathbf{a} = \begin{pmatrix} a^1 \\ a^2 \\ a^3 \end{pmatrix}.$$

Sometimes, we express vectors as linear combinations of unit vectors, e.g.,

$$\mathbf{a} = a^i \hat{\mathbf{e}}_i = \sum_{i=1}^{3} a^i \hat{\mathbf{e}}_i$$

wherein we used the Einstein summation convention, summing over a pair of lower and upper indices, named "contraction". Three-dimensional vector components carry a latin index, e.g., i, j, k, l. Four-dimensional vector components carry a greek index, e.g., μ, ν, ρ. Four-dimensional vectors are denoted without boldface, i.e.,

$$a = a^\mu \hat{\mathbf{e}}_\mu = \begin{pmatrix} a^0 \\ \mathbf{a} \end{pmatrix} = \begin{pmatrix} a^0 \\ a^1 \\ a^2 \\ a^3 \end{pmatrix}$$

and we refer to the zeroth component a^0 as the time component and the other components a^i as the spatial components. It is common practice to refer to a vector by its component, i.e., a^μ refers to the four-dimensional vector a.

For the Minkowski metric $g^{\mu\nu}$ we adopt the "mostly minus" convention, i.e.,

$$g^{\mu\nu} = \begin{pmatrix} g^{00} & g^{01} & g^{02} & g^{03} \\ g^{10} & g^{11} & g^{12} & g^{13} \\ g^{20} & g^{21} & g^{22} & g^{23} \\ g^{30} & g^{31} & g^{32} & g^{33} \end{pmatrix} = \begin{pmatrix} +1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

The Minkowski product given two four-dimensional vectors, a^μ and b^μ, is given by the contraction

$$a^\mu g_{\mu\nu} b^\nu = a^0 b^0 - \mathbf{a} \cdot \mathbf{b} = a^0 b^0 - a_i b^i$$

wherein $\mathbf{a} \cdot \mathbf{b}$ is the scalar product on Euclidean space. The Minkowski metric can be used to raise and lower indices,

$$a_\mu = g_{\mu\nu} a^\nu = \begin{pmatrix} a^0 \\ -a^1 \\ -a^2 \\ -a^3 \end{pmatrix},$$

and a spatial component with a lower index is not in general equal to a spatial component with a raised index, $a_i \neq a^i$!

With regard to quantum mechanics, we use the standard bra-ket notation where we denote scalar-valued operators by a hat, e.g., $\hat{X}$, and vector-valued operators by boldface hat, e.g., $\hat{\mathbf{X}}$.

Analog to the continuous-time signal $x(t)$, we define the discrete-time signal

$$x[n] = \int \mathrm{d}t \, x(t) \delta^{(1)}(t - nT),$$

wherein T is the sampling period. Sometimes we refer to $x[n]$ as samples or a sample similar as $x(t)$ denotes a function or the function evaluated at t. To distinguish samples from symbols, which do not require a sampling period T, we use the index notation, i.e., x_m denotes a symbol while $x[m]$ denotes a sample.

Regarding operator ordering, we note the normal-ordering symbol, moving the creation operators, e.g., $\hat{a}^\dagger$, to the left and the annihilation operators, e.g., $\hat{a}$, to the right, by

$$:\hat{a}\hat{a}^\dagger\hat{b}: = \hat{a}^\dagger\hat{a}\hat{b}.$$

As time-ordering symbol we adopt $\mathcal{T}_+$, which evaluates an operator in forward time-order [2, p. 84],

$$\frac{1}{2}\hat{T}_+\int_{t_0}^{t}\mathrm{d}t_1\int_{t_0}^{t}\mathrm{d}t_2\,\hat{A}(t_1)\hat{B}(t_2) = \int_{t_0}^{t}\mathrm{d}t_1\int_{t_0}^{t_1}\mathrm{d}t_2\,\hat{A}(t_1)\hat{B}(t_2).$$

Acronyms

ADC analog-to-digital converter.

AES advanced encryption standard.

AM amplitude modulation.

AR anti-reflective.

BCH Baker-Campbell-Hausdorff.

BD balanced detector.

BS beam splitter.

CCR canonical commutation relation.

COM center of mass.

CV-QKD continuous-variable quantum-key distribution.

DAC digital-to-analog converter.

DOF degrees of freedom.

DPS-QKD differential phase-shift quantum-key distribution.

DSP digital signal processing.

DV-QKD discrete-variable quantum-key distribution.

EB entanglement-based.

ECDH elliptic-curve Diffie-Hellman.

EOM equation(s) of motion.

ETCR equal-time commutation relation.

FC fiber coupler.

GNFS generalized number field sieve.

I/Q in-phase/quadrature.

IQM in-phase and quadrature modulator.

LDPC low-density parity-check.

LO local oscillator.

LP low-pass.

LTI linear time-invariant.

MAC message authentication code.

MZI Mach-Zehnder interferometer.

MZM Mach-Zehnder modulator.

OFDM orthogonal frequency-division multiplexing.

OTP one-time pad.

P&M prepare-and-measure.

PBS polarized beam splitter.

PC polarization controller.

PD photodiode.

PKD public-key distribution.

POVM positive operator-valued measure.

PS phase-shifter.

PWM power meter.

QBER quantum-bit error-rate.

QED quantum electrodynamics.

QKD quantum-key distribution.

QPSK quadrature phase-shift keying.

RF radio frequency.

RRC root-raised-cosine.

RX receiver.

SNR signal-to-noise ratio.

SPD Single-photon detector.

SPS Single-photon source.

TIA transimpedance amplifier.

TX transmitter.

VOA variable optical attenuator.

Contents

Introduction **1**

1. Quantum-key distribution **6**
1.1. Secret-key distribution problem . . . 7
1.1.1. Public-key distribution . . . 8
1.1.2. Quantum-key distribution . . . 10
1.2. Qubit-based protocols . . . 12
1.2.1. Polarization-encoding BB84 . . . 15
1.2.2. Time-phase-encoding BB84 . . . 18
1.3. Boson-based protocols . . . 22
1.3.1. Squeezed-coherent-encoding BB84 . . . 25
1.3.2. Coherent-encoding GG02 . . . 28
1.4. Post-processing . . . 30
1.4.1. Symbol mapping . . . 33
1.4.2. Information reconciliation . . . 36
1.4.3. Privacy amplification . . . 39
1.5. Security analysis . . . 41
Summary . . . 44

2. Quantum theory of light **47**
2.1. Maxwell theory . . . 47
2.1.1. Maxwell Lagrangian . . . 48
2.1.2. Electromagnetism . . . 49
2.1.3. Gauge conditions . . . 51
2.1.4. Plane-wave expansion . . . 52
2.1.5. Canonical quantization . . . 54
2.2. Quantum states . . . 56
2.2.1. Vacuum state . . . 57
2.2.2. Particle states . . . 58
2.2.3. Fock space . . . 60
2.2.4. Number states . . . 61
2.2.5. Coherent states . . . 62
Summary . . . 66

3. Quantum theory of (electro-)optical components **69**
3.1. Coupler . . . 69
3.1.1. Beam splitter . . . 70
3.1.2. Waveguide coupler . . . 72
3.1.3. Unitary operator transform . . . 74
3.1.4. Coherent state transform . . . 75
3.1.5. Splitter and spectral filter . . . 77
3.2. Modulators . . . 79
3.2.1. Phase modulator . . . 79
3.2.2. Amplitude modulator . . . 84
3.3. Photodetectors . . . 87
3.3.1. Photoelectric effect . . . 87
3.3.2. Photocurrent operator . . . 90
3.3.3. Direct detector . . . 91
3.3.4. Balanced detector . . . 92
Summary . . . 95

4. Coherent state transmission system **99**
4.1. Transmitter . . . 100
4.1.1. Symbol encoding . . . 101
4.1.2. Upconversion . . . 106
4.2. Receiver . . . 109
4.2.1. Downconversion . . . 109
4.2.2. Homo- and heterodyning . . . 112
4.2.3. Symbol decoding . . . 114
Summary . . . 118

Conclusion and outlook **120**

A. Supplemental theorems to Maxwell field theory **122**

B. Nonlinear interaction theory **129**

C. Photodetection theory **133**

D. Receiver synchronization **136**

Bibliography **139**

Acknowledgements **146**

Introduction

Optical communication enables humanity worldwide to share information in a split second, with companies like Huawei undergoing tremendous efforts to advance the frontiers. In addition to incremental innovation increasing the performance and decreasing the cost of optical communication technology, we observe intensified activities towards disruptive innovations that challenge our present understanding of communication. One such branch of activity is quantum-optical communication, incorporating quantum aspects of light into classical communication and leading to novel communication technology like quantum-key distribution (QKD), which enables practical and secure-key generation. As a still young discipline, which emerged from two highly advanced fields, communication engineering and quantum physics, quantum communication lacks a unified description on which both communication engineers and quantum physicists agree. The present thesis aims to resolve the seeming discrepancies between communication engineering and quantum physics by reviewing a practical implementation of a quantum-communication system employing a continuous-variable quantum-key distribution (CV-QKD) protocol. In the process, we intend to develop a theoretical framework for quantum-optical communication, incorporating quantum effects into classical communication, which has applicability beyond CV-QKD.

Problem statement

To raise awareness of the challenges ahead, we review the best-known quantum theory of light, single-mode quantum optics, along with central ideas from classical communication and outline where these pictures conflict.

In single-mode quantum optics, we model monochromatic light with frequency ω_0 as a quantum harmonic oscillator with unit mass, $m = 1$, and Hamiltonian [4, 5]

$$\hat{H} = \omega_0 \hat{a}^\dagger \hat{a}, \tag{0.0.1}$$

wherein $\hat{a}$ and $\hat{a}^\dagger$ are the quantum annihilation and creation operators, destroying or creating an excitation or "mode" of frequency ω_0. The electric field operator,

$$\hat{E}(t, x) = \mathcal{E}_0 \left(\hat{a} + \hat{a}^\dagger\right) \sin(\omega_0 x), \tag{0.0.2}$$

wherein $\mathcal{E}_0$ has the interpretation of an electric field density, establishes the connection between the quantum harmonic oscillator and electromagnetic radiation, including light [4,

p. 12]. Two of the most important quantum states are the number and the coherent state,

$$|n\rangle = \frac{1}{\sqrt{n!}}\left(\hat{a}^\dagger\right)^n|0\rangle \qquad \text{and} \qquad |\alpha\rangle = \exp\left(-\frac{1}{2}|\alpha|^2\right)\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle. \tag{0.0.3}$$

The number state is parametrized by a natural number $n \in \mathbb{N}_0$ counting the number of excitations. The coherent state is parametrized by a complex number $\alpha \in \mathbb{C}$ encoding amplitude and phase. The expectation value of the electric field operator with respect to a coherent state,

$$\langle\alpha|\hat{E}(t)|\alpha\rangle = \sqrt{2}|\alpha|\mathcal{E}_0\sin\left(\omega_0 t - \theta\right), \tag{0.0.4}$$

equals a classical monochromatic wave with amplitude proportional to $|\alpha|$ and phase θ [4, p. 45].

The central concept in communication engineering is that of a signal, not specific to a particular physical realization, e.g., mechanical or electromagnetic waves. In that sense, light is primarily an implementation detail for carrying information-bearing signals. In the following, we assume the information-bearing signals to be narrowband, i.e., have a well-defined narrow bandwidth B_d in the power spectrum.[1] Complementary, the carrying signal, ideally, only comprises a single well-defined frequency component, tailored to the physical transmission channel, which typically is many magnitudes higher than the frequency components of the information-bearing signal. Superimposing carrier signals with frequencies sufficiently spaced apart allows multiplexing of information-bearing signals on a common transmission medium. Affiliating an information-bearing signal with a carrier is imple-

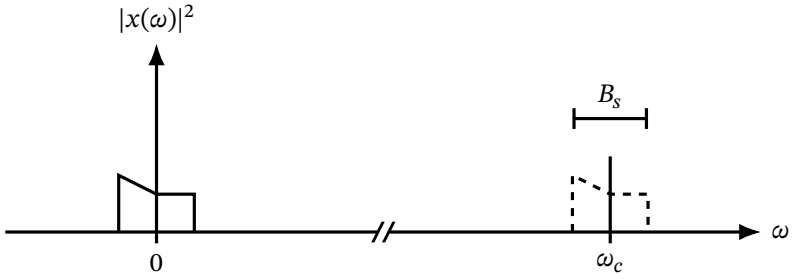


Figure 0.1.: Power spectrum comprising an information-bearing signal with bandwidth B_s at zero frequency, $\omega = 0$, a carrier signal at a carrier frequency much greater than the bandwidth, $\omega_c \gg B_s$. The upconverted information-bearing spectrum is indicated by dashed lines.

mented by modulating the information-bearing signal onto the carrier signal. On a more abstract level, the power spectrum of the information-bearing signal is shifted by the carrier frequency, as illustrated in Figure 0.1. The asymmetry of the information-bearing spectrum around zero frequency, $\omega = 0$, in Figure 0.1 implies that the information-bearing signal is

[1] In general, there is no requirement for the information-bearing signal to be narrowband, see, for instance, orthogonal frequency-division multiplexing (OFDM) and spread-spectrum techniques.

complex-valued. At the same time, the spectrum of the information-bearing signal modulated onto the carrier, denoted by the dashed spectrum around ω_c, has complex conjugate symmetry, i.e., is thus real-valued, as we would expect from a physical signal. As it is techni-

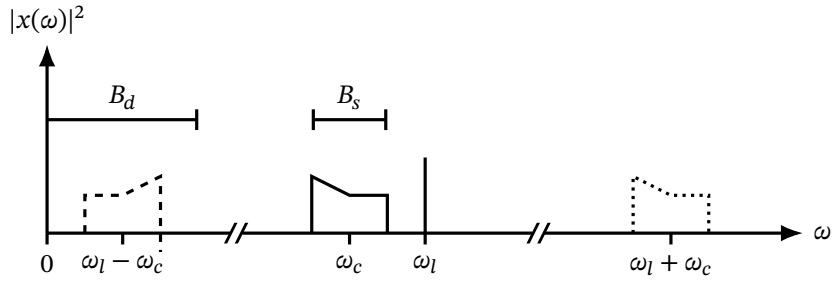


Figure 0.2.: Power spectrum comprising a modulated carrier signal at carrier frequency ω_c with bandwidth B_s, a local oscillator (LO) signal with frequency slightly above the carrier frequency, $\omega_l > \omega_c$. The downconverted modulated-carrier spectra are indicated by dashed lines, lower band at $\omega_l - \omega_c > 0$, and dotted lines, upper band at $\omega_l + \omega_c$. The detector bandwidth is indicated by $B_d > \omega_l - \omega_c$.

cal unfeasible to measure the modulated carrier directly at the carrier frequency, we demodulate or downconvert the information-bearing signal from the carrier by mixing the received signal with a LO at frequency ω_l, producing a low- and high-frequency signal at $\omega_l - \omega_c$ respectively $\omega_l + \omega_c$, as depicted in Figure 0.2. For a useful measurement, the LO frequency ω_l should be chosen such that the detector bandwidth B_d covers the complete low-frequency signal, i.e., $\omega_l - \omega_c + B_s/2 < B_d$. The relative dependence of the measured spectrum from the LO frequency ω_l and the fact that the modulated carrier signal and the information-bearing signal contain the same information suggests introducing the concept of base- and passband representation [6]. The passband representation corresponds to the physical reality where the information-bearing signal is modulated onto the carrier. The passband signal is real-valued, and the spectrum has complex conjugate symmetry. However, when we measure the spectrum, we do so with a relative frequency and obtain an asymmetric spectrum centered at zero frequency, the baseband representation. Figure 0.3 shows the power spectrum of a received signal in baseband representation comprising two signal bands and a pilot tone.

To sum up, single-mode quantum optics provides precise physical meaning to light, including quantum effects, although limited to monochromatic light. On the other side, communication engineering provides a framework for efficiently encoding, transmitting, receiving, and decoding information but attempts no statements about the underlying physics. For quantum-optical communication, it is inevitable to welcome and incorporate both views. For instance, people with a background in quantum optics but foreign to communication engineering often advocate the concept of "one state, one universe", where each quantum transmission is completely independent. However, if we include practical considerations, like assuming a single transmission line, the picture of "one state, one universe" is plagued by several ambiguities. For example, a single-mode quantum state with well-defined fre-

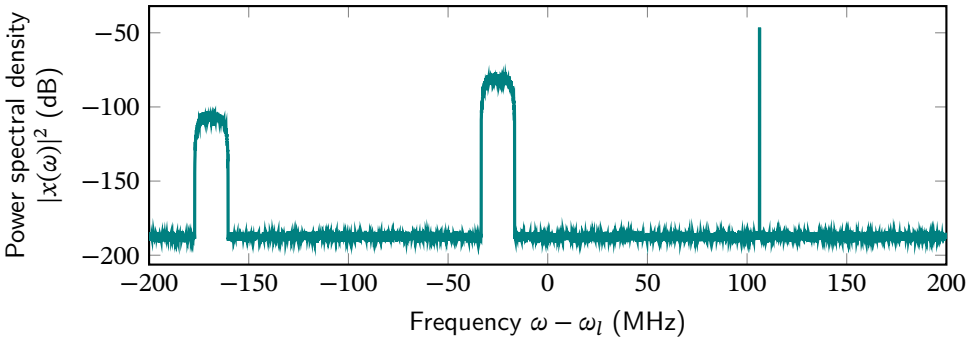


Figure 0.3.: Power spectrum comprising showing the received signal as baseband. At 100 MHz, the spectrum has a pilot tone. Centered at −25 MHz, the spectrum shows a first passband signal with 12.5 MHz bandwidth. Centered at −168.75 MHz, the spectrum has a second passband signal with 12.5 MHz bandwidth.

quency ω_0 represents a perfect sinusoidal wave with infinite duration, making information transmission absurd. The typical counter-argument is that single-mode quantum optics implicitly assumes pulses with ω_0 being the center frequency of the pulse. While the counter-argument is technically valid, we must admit that it only raises new questions, such as bandwidth-limitations on the pulse parameters, all properly addressed in communication engineering.

The multi-mode quantum-optics mentioned in popular quantum-optics books [4, 5] are insufficient to represent continuous-time signals, and performing a continuum limit might not be correct if we consider the huge differences between linear algebra and functional analysis. The advanced quantum-optics literature [7, 8] does sometimes use a continuous-mode formalism but does not explicitly investigate its properties. We are only aware of two quantum-optics books [9, 10] that explicitly discuss a continuous-mode theory of light but again open up new questions regarding the fundamental assumptions and justification thereof. If we are willing to go one step deeper, we find answers in the quantum field-theory literature [2, 11, 12, 13], but it is up to us to transfer these insights from particle physics to quantum-optics applications. We even have to go a bit deeper and look into mathematical quantum field-theory [14, 15, 16] to answer some questions. Finally, we want to understand and upgrade quantum models of (electro-)optical components in the literature [7, 17, 18, 8] to a mode continuum for comparison with the results from the optical-communication community [19, 20]. Regarding communication engineering, we retain the well-established signal-processing fundamentals, as presented, for example, in Refs. [21, 22, 23, 6, 24, 25].

Thesis outline

Our work is divided into four chapters. In Chapter 1, we present an introduction to QKD, emphasizing the similarities between the plethora of seemingly different protocols and attempting to argue why CV-QKD resembles a coherent-state communication system. In the following three chapters, we construct our theoretical framework for quantum-optical communication towards CV-QKD. Starting from a general quantum theory of light in Chapter 2, applying the quantum theory to describe the building blocks of coherent communication systems in Chapter 3, to an abstract description of a coherent-state transmission system's signal processing in Chapter 4. While the thesis chapter structure supports a bottom-up approach, it is equally possible to read the thesis from the back to the front, revealing more and more details.

Chapter 1.

Quantum-key distribution

Before diving deep into the technical details of our quantum theory of light, we would like to introduce the reader to quantum-key distribution (QKD) as an example of quantum optical communication. In particular, we want to emphasize the many different layers, quantum and classical, involved in practical quantum optical communication. Our introduction favors breadth over depth and ignores protocol-specific details to highlight the similarities, specifically between discrete-variable quantum-key distribution (DV-QKD) and continuous-variable quantum-key distribution (CV-QKD).

The literature divides QKD protocols among DV-QKD and CV-QKD and differential phase-shift quantum-key distribution (DPS-QKD), though this thesis will not address DPS-QKD further. One of the few resources painting a comprehensive and decisive picture of QKD, and providing much inspiration for the present chapter, is Ref. [26]. Other notable references are Ref. [27], reviewing the practical aspects of QKD, and Refs. [28, 29] for CV-QKD. DV-QKD is often approached in the context of Gaussian quantum information theory, see Refs. [30, 31]. More advanced resources highlighting the practical implementation of QKD are found in Refs. [32, 33, 34]. Compared to the existing literature, our introduction to QKD attempts to weaken the distinction between DV-QKD and CV-QKD by framing it as an encoding detail.

The chapter organizes as follows. First, we motivate the challenge of secure and practical key distribution in the context of secure communication. Second, we present the key concepts of protocols based on qubit and bosonic quantum information. Third, we discuss the classical post-processing procedure required to distill a shared secret key. Fourth, we provide rough ideas on how to perform a security analysis of QKD. Finally, we argue for the concept of a logical and encoding quantum layer for practical QKD. One of the most relevant conclusions to draw from this chapter is that a coherent-state transmission system resembles the encoding quantum layer for CV-QKD protocols.

1.1. Secret-key distribution problem

Two spatially distanced parties, Alice and Bob, share a communication channel that allows Alice to send messages to Bob. How can Alice and Bob secure their communication against an opposing third party, Eve? Alice needs to ensure that the message she transmits is confidential, i.e., only Bob can read it. Bob needs to ensure that the message he receives is integer, i.e., only Alice can have sent it. Figure 1.1 depicts a secure communication system

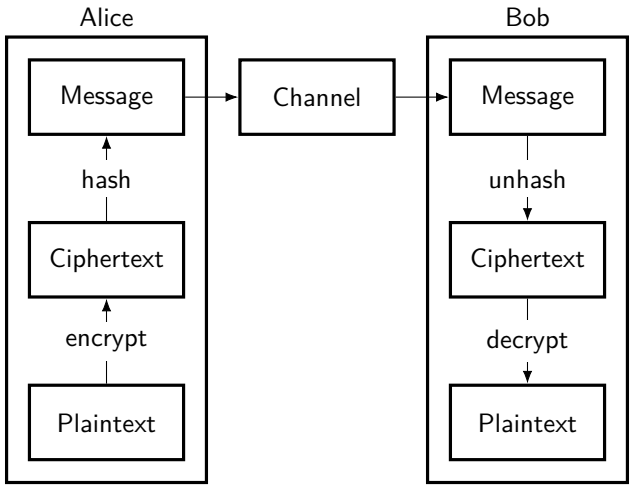


Figure 1.1.: Secure communication system comprising a transmitter (Alice), a receiver (Bob) and a public communication channel. Alice encrypts a plaintext message yielding a ciphertext. By adding the hash to the ciphertext, Alice constructs a message she transmits through the channel to Bob. Bob removes the hash from his received message to resolve the ciphertext. Decrypting the ciphertext unveils the plaintext for Bob.

implementing integrity and confidentiality between Alice and Bob.[1] First, Alice encrypts a plaintext message, using symmetric encryption like the one-time pad (OTP) [38] or the more practical advanced encryption standard (AES) [39], to ensure confidentiality. Second, she adds a message authentication code (MAC) using, e.g., universal hash functions [40], to ensure integrity. Bob receives the encrypted message with MAC from Alice. He confirms the integrity of the message by checking the MAC, then he decrypts the message to access the plaintext.

Message authentication and cipher require Alice and Bob to possess a shared secret key. If Alice and Bob use the OTP cipher and their secret key is truly random, the communication system is eternally secure [38] — provided that Alice and Bob do not re-use their secret key. Unless Alice and Bob do not want to meet in person every time they initiate communication, Alice and Bob need a practical method to distribute a secret key.

[1] For a discussion on the order of hashing and encryption, see Ref. [35, 36, 37].

1.1.1. Public-key distribution

The standard attempt to solve the key-distribution problem is to use an asymmetric cipher comprising a public key for encryption and a private key for decryption. One of the parties, for example, Bob, first generates an asymmetric key pair of which he discloses the public key to Alice. Alice generates a secret key from a true random generator, encrypts it with the public key, and sends it to Bob, see the left-hand side of Figure 1.2. Bob decrypts the message he received from Alice with his private key to obtain Alice's secret key, see the right-hand side of Figure 1.2. Assuming the asymmetric cipher to be secure, Alice and Bob now share a secret key. Public-key distribution algorithms, for instance, Diffie-Hellman [41] and

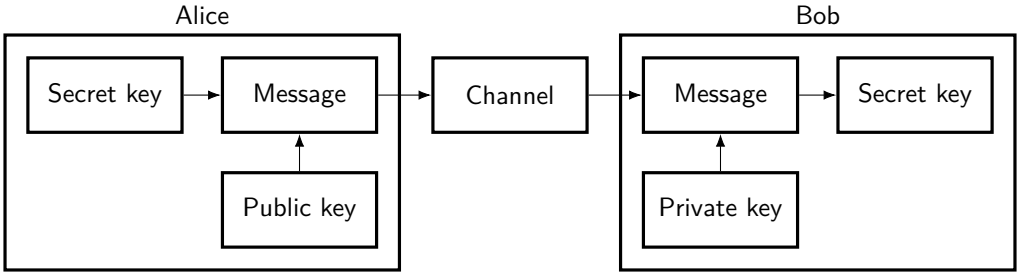


Figure 1.2.: Alices and Bob use an asymmetric cipher to distribute a secret key. Alice possesses the secret key and a public key, and Bob owns a private key corresponding to Alice's public key. Alice encrypts the secret key with the public key and transmits the message over a (public) channel to Bob. Bob decrypts the message with the private key to obtain the secret key.

variants thereof, e.g., elliptic-curve Diffie-Hellman (ECDH), are heavily employed on the internet because they are effortless to deploy.

The core principle behind asymmetric ciphers is the concept of one-way functions, functions easy to compute but difficult to invert. Here, easy and difficult refer to the computational complexity, denoting the upper bound of the best (known) algorithm to solve the problem. The time to break an asymmetric cipher depends on the computational resources and complexity. In practice, one chooses a key length, such that attacks, possible with present computational resources, become impractical. However, computational resources advance with time.[2] A key length that was considered secure in the past might be rendered useless in the future. It is imaginable to store communication from the present in the hope of breaking it in the future. In addition to technological progress in computing, discovering new algorithms may decrease the computational complexity and make certain attacks practicable. For example, Shor's quantum algorithm [43] provides an exponential speed-up in prime number factorization compared to the fastest (known) classical algorithm, GNFS, see Figure 1.3. As prime number factorization is used by, for instance, Diffie-Hellman key exchange, as a one-way function, a sufficiently-powerful quantum computer can break previously, assumed to

[2]According to Moore's observation, the number of transistors in integrated circuits doubles every two years.

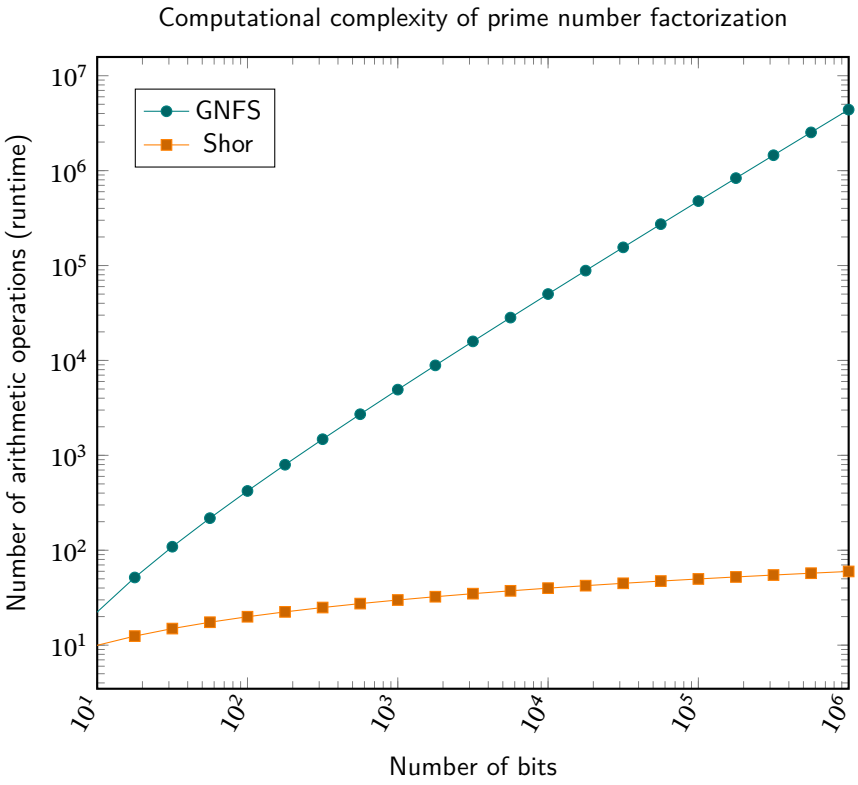


Figure 1.3.: Computational runtimes for prime number factorization algorithms: The most efficient known classical algorithm is the generalized number field sieve (GNFS) [42] (green) and Shor's algorithm [43] (orange). The runtime of the classical algorithm increases exponentially with the number of bits, while the quantum algorithm rises almost linearly.

be, secure communication.

As long as there exists no mathematical proof for a theoretical lower bound of the computational complexity of a particular class of one-way functions, PKD is not forward secure, i.e., might be broken in the future.[3]

[3]Post-quantum cryptography [44, 45] attempts to mitigate the vulnerability of present asymmetric ciphers against quantum algorithms by choosing a different class of one-way functions suspected to be secure. But again, as long as there is no absolute lower bound for the computational complexity of a particular class of one-way functions, forward security of PKD, including post-quantum ciphers, remains contestable.

1.1.2. Quantum-key distribution

The potential of public-key distribution (PKD) becoming a vulnerability inflames the demand for a practical and forward secure key distribution scheme. Ideally, the key-distribution scheme should dynamically react to any third-party interaction by compensating for the information leak or aborting the protocol. QKD claims to be such a key-distribution scheme. Based on the laws of quantum physics, QKD exploits the inherent uncertainty of measuring non-orthogonal quantum states to generate random correlations between Alice and Bob. Alice's and Bob's correlations provide insights about potential information loss to a third party. Using classical techniques, Alice and Bob can then compensate for the potential information loss or abort the protocol if necessary. Figure 1.4 presents a communication system profi-

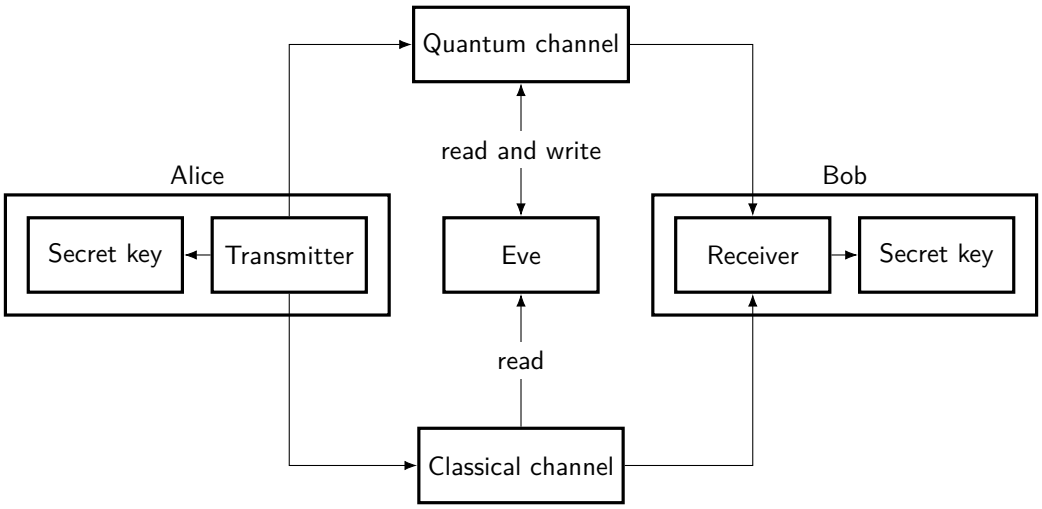


Figure 1.4.: Alice and Bob use a quantum and classical channel to generate a shared secret-key. Alice possesses a transmitter, and Bob owns a receiver. Transmitter and receiver both output a secret key and connect to a quantum and classical channel. A potential adversary, Eve, has read and write access to the quantum but only read access to the classical channel.

cient for QKD. The classical and quantum channel connecting Bob's receiver with Alice's transmitter is usually the same physical medium. For example, an optical fiber where the quantum and classical channels occupy different wavelengths or polarization. If the QKD protocol succeeds, Alice's transmitter and Bob's receiver output the same secret key to Alice, respectively Bob. The adversary, Eve, has full access (read and write) to the quantum channel but has only read access to the classical channel. The restriction that Eve has only read access over the classical channel is important to exclude man-in-the-middle attacks. However, the restriction is not a practical limitation as we can ensure integrity by promoting the classical channel to an authenticated channel using MACs.

The details on QKD strongly depend on the particular implementation at hand, the QKD

protocol. A huge zoo of QKD protocols exists, and it is useful to overview common features for a systematic presentation. The QKD literature typically distinguishes between DV-QKD, CV-QKD, and DPS-QKD. Leaving out DPS-QKD, it is unclear which features unambiguously differentiate between CV-QKD and DV-QKD. For instance, most practical DV-QKD protocols use weak coherent states [28], which are anything but discrete. The accepted opinion considers a protocol discrete when using a single photon and continuous when using a coherent detector. However, this view is challenged by discrete QKD protocols, like BB84 [46], using coherent detection [47]. What other feature can we use if the detection method does not clearly distinguish between CV-QKD and DV-QKD? Figure 1.5 summarizes common

Figure 1.5.: Common characteristics of QKD protocols in a tree diagram. The protocol schema is either prepare-and-measure (P&M) or entanglement-based (EB). The Measurement basis selection is either passive or active. The detection is usually coherent or based on single-photon clicks. The logical Hilbert space is either finite or countable. Among many, the physical encoding uses the field quadratures, polarization, or squeezing degrees of freedoms (DOFs) of light.

features among QKD protocols. Features like the protocol schema, the measurement basis selection, and the detector are uniquely determined. More opaque is the distinction between the physical encoding and the logical Hilbert space, a concept which we introduce here. The physical encoding refers to the light DOFs used to encode the data, for example, the polarization of light or the particular quantum state. More often, the technical facilities determine the physical encoding. For example, coherent light sources and detectors are mature technologies. At the same time, many QKD protocols assume a more simple quantum system than that of light, which we refer to as the logical Hilbert space. The logical Hilbert space is either finite or countable. If it is finite, it is often a qubit or generalization thereof. If it is countable, it is often bosonic. Therefore, we propose not to partition QKD protocols among CV-QKD or DV-QKD but by their logical Hilbert space being bosonic- or qubit-based[4], which we both present in the next two sections.

1.2. Qubit-based protocols

Many DV-QKD protocols, e.g., the BB84 [46], BB92, or the six-state protocol [48], are qubit-based in that the logical quantum system underlying the key generation is a two-state quantum system, a qubit.

A qubit state $|\psi\rangle$ is an element of a two-dimensional complex Hilbert space with norm one, i.e., $|\langle\psi|\psi\rangle|^2 = 1$. In the qubit basis $\{|0\rangle, |1\rangle\}$, a generic qubit state takes the form

$$|\psi\rangle = c_1|0\rangle + c_2|1\rangle \qquad \text{with } |c_1|^2 + |c_2|^2 = 1. \tag{1.2.1}$$

Table 1.1 lists different quantum systems which allow encoding of a qubit. To encode a

Encoding variable	Standard basis	
	$\|0\rangle$	$\|1\rangle$
Polarization	Horizontal	Vertical
Photon number	Vacuum	Single-photon
Time-bin	Early	Late
Phase-bin	0 deg	180 deg

Table 1.1.: Possible physical systems to encode a qubit with possible choices for the standard basis elements.

qubit the actual quantum systems does not have to be two-dimensional. For example, the photon Fock space is countable. Still, by restricting the basis elements to the vacuum and single-photon state, we have a qubit. Similar, we can partition the continuous time and phase parameters of a quantum system to separate bins.

[4]Such a distinction is also indicated in quantum information theory, see, for instance, Ref. [30, p. 2].

A useful visualization of qubit states is the Bloch sphere, see Figure 1.6. The Bloch sphere is

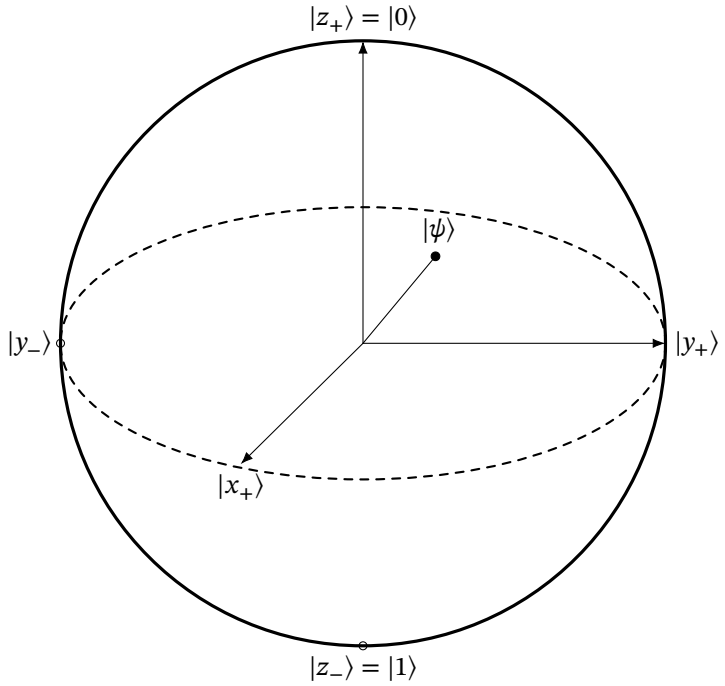


Figure 1.6.: Two-state quantum system in the Bloch sphere representation. The Bloch sphere is a three-dimensional sphere with unit radius. A pure quantum state $|\psi\rangle$ resides on its surface of a sphere.

a unit sphere embedded in three-dimensional space. Pure quantum states are elements on the surface of the Bloch sphere. Two antiparallel vectors correspond to orthogonal states. Typically, the standard axis in $\mathbb{R}^3$ are assigned to the three orthogonal Pauli eigenbases. A generic quantum state $|\psi\rangle$ in a certain basis can be found by projection. Figure 1.7 shows the projection among the X and Z Pauli eigenbases. In quantum mechanics, the projection coefficients, i.e., the inner product of two states, correspond to the probability amplitude of measuring the given state in particular basis. We can formalize this concept by introducing the generalized spin operator

$$\hat{S}(\hat{\mathbf{n}}) = \hat{\mathbf{S}} \cdot \hat{\mathbf{n}} = \frac{1}{2}\hat{\sigma}_j n^j = \begin{pmatrix} n_3 & n_1 - in_2 \\ n_1 + in_2 & -n + 3 \end{pmatrix} \tag{1.2.2}$$

wherein $\hat{\mathbf{n}} \in \mathbb{R}^3$ is a unit norm vector and $\hat{\sigma}_j$ is the jth Pauli matrix. Let $|\pm, \hat{\mathbf{n}}\rangle$ be the eigenstate of the generalized spin operator $\hat{S}(\hat{\mathbf{n}})$ to eigenvalues $\pm 1/2$, i.e.,

$$\hat{S}(\hat{\mathbf{n}})|\pm, \hat{\mathbf{n}}\rangle = \pm\frac{1}{2}|\pm, \hat{\mathbf{n}}\rangle, \tag{1.2.3}$$

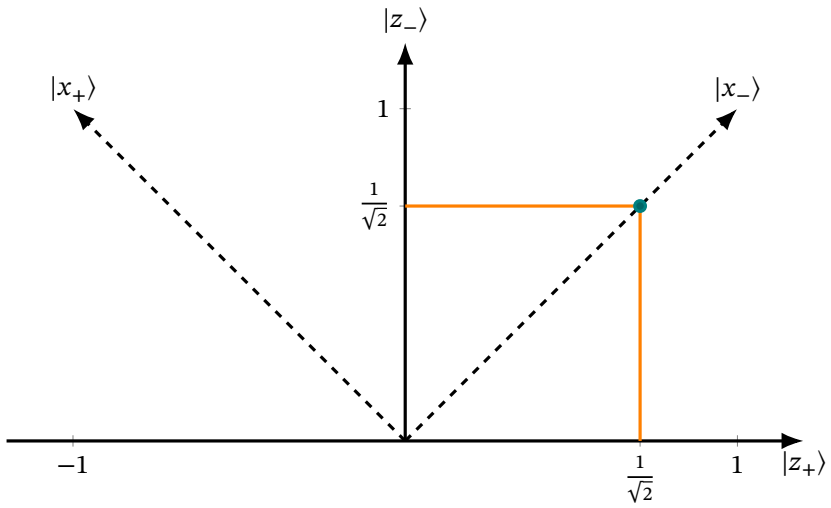


Figure 1.7.: Two-dimensional state space spanned by the X, Z Pauli eigenbases: Projecting the $|x_-\rangle$ state onto the Z eigenbasis yields a constant probability amplitude of $1/\sqrt{2}$.

then for $\hat{\mathbf{n}} = \hat{\mathbf{e}}_j$ we obtain the $\hat{\sigma}_j$ Pauli eigenstates, i.e.,

$$\hat{S}_x|x_\pm\rangle = \hat{\mathbf{S}}(\hat{\mathbf{e}}_x)|\pm, \hat{\mathbf{e}}_x\rangle = \pm\frac{1}{2}|\pm, \hat{\mathbf{e}}_x\rangle = \pm\frac{1}{2}|x_\pm\rangle \tag{1.2.4}$$

$$\hat{S}_y|y_\pm\rangle = \hat{\mathbf{S}}(\hat{\mathbf{e}}_y)|\pm, \hat{\mathbf{e}}_y\rangle = \pm\frac{1}{2}|\pm, \hat{\mathbf{e}}_y\rangle = \pm\frac{1}{2}|y_\pm\rangle \tag{1.2.5}$$

$$\hat{S}_z|z_\pm\rangle = \hat{\mathbf{S}}(\hat{\mathbf{e}}_z)|\pm, \hat{\mathbf{e}}_z\rangle = \pm\frac{1}{2}|\pm, \hat{\mathbf{e}}_z\rangle = \pm\frac{1}{2}|z_\pm\rangle. \tag{1.2.6}$$

By convention one identifies the Z Pauli eigenbasis with the qubit basis $\{|0\rangle, |1\rangle\}$.

Having introduced the concept of basis projections and the spin operator, we can discuss the BB84 (six state) protocol for which Alice and Bob must agree on two (or three) orthogonal bases[5] and a mapping between the basis states and some bit sequence, then

1. Alice encodes her bits into the state $|\psi\rangle$ and sends it to Bob.

2. Bob receives the state $|\psi\rangle$ from Alice and performs a measurement decoding some bits.

If Alice and Bob select the same basis, Bob can accurately decode Alice's key bit from the measurement. Alice and Bob's probability of choosing the same basis for one transmission is one divided by the number of orthogonal bases Alice and Bob have agreed on, e.g., 50 % if Alice and Bob agreed to use the X and Z Pauli eigenbasis, also called the quantum-bit error-rate (QBER). In the asymptotic limit of many transmissions, the QBER should approach the

[5] BB92 using non-orthogonal bases can be implemented by using the generalized spin operator with non-orthogonal vectors.

theoretical limit. Otherwise, an opposing third party, Eve, might have tempered with the transmission. Table 1.2 displays a possible transmission sequence between Alice and Bob. Alice randomly selects an initial key bit 0 or 1 and a state basis X or Z where X respective Z denote the eigenbasis of the Pauli σ_x respective σ_z matrix. Alice's initial key bit and selected basis determine the quantum state she prepares and sends to Bob. Bob randomly chooses a measurement basis. Only if Alice's and Bob's basis agree, the key bit is not discarded. After

		Transmission				
Party	Step	1	2	3	4	5
Alice	Initial key bit	0	1	1	0	0
	State basis	Z	X	X	Z	X
	Prepared state	$\|z_+\rangle$	$\|x_-\rangle$	$\|x_-\rangle$	$\|z_+\rangle$	$\|x_+\rangle$
Bob	Measurement basis	X	Z	X	Z	Z
	Possible outcomes	0,1	0,1	1	0	0,1
	Sifted outcomes	-	-	1	0	-

Table 1.2.: Possible transmission sequence for qubit-based QKD illustrating how Alice encodes a key bit into a qubit state and Bob attempt to decode.

the transmission sequence, Alice and Bob hold a partially correlated and partially secret bit string from which they can distill a shared secret bit string using classical post-processing.

1.2.1. Polarization-encoding BB84

In polarization-encoding BB84, the polarization of light is used as physical quantum system to encode the logical qubit system. Let $|\leftrightarrow\rangle$ and $|\updownarrow\rangle$ denote the horizontal respective vertical polarization states forming the rectilinear basis. Let $|\nwarrow\rangle$ and $|\nearrow\rangle$ denote the left- and right-diagonal polarization states forming the diagonal basis. Let $|\circlearrowleft\rangle$ and $|\circlearrowright\rangle$ denote the left- and right-circular polarization states forming the circular basis. We can express the diagonal and circular basis elements in terms of the rectilinear basis elements:

$$|\nwarrow\rangle = \frac{1}{\sqrt{2}}(|\leftrightarrow\rangle + |\updownarrow\rangle) \qquad |\nearrow\rangle = \frac{1}{\sqrt{2}}(|\leftrightarrow\rangle - |\updownarrow\rangle) \tag{1.2.7}$$

$$|\circlearrowleft\rangle = \frac{1}{\sqrt{2}}(|\leftrightarrow\rangle + i|\updownarrow\rangle) \qquad |\circlearrowright\rangle = \frac{1}{\sqrt{2}}(|\leftrightarrow\rangle - i|\updownarrow\rangle) \tag{1.2.8}$$

For clarity, we restrict the following discussion to qubit-based QKD protocols where two orthogonal bases are used, e.g., rectilinear and diagonal. Other protocols exist that use three orthogonal bases (six-state protocol) or even non-orthogonal bases.

A possible optical setup to implement such polarization-encoding is depicted in Figure 1.8. Alice configures her linear polarizer to select a basis element of the rectilinear or diagonal

polarization basis. Bob receives Alice's polarization state through the polarization controlled quantum channel. He rotates a rectilinear polarized beam splitter by either 0° or 45° to detect either rectilinear or diagonal polarized photons with his two single-photon detectors placed at the beam splitter output. Alice selects one of four polarization states $|\leftrightarrow\rangle, |\updownarrow\rangle, |\nwarrow\!\!\searrow\rangle, |\nearrow\!\!\swarrow\rangle$ by

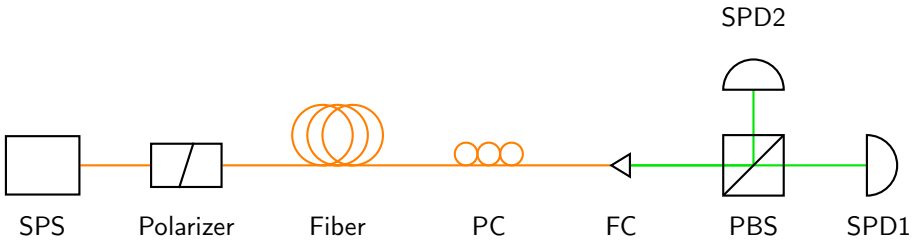


Figure 1.8.: Optical setup to implement polarization-encoding BB84 with active basis selection. The transmitter comprises an Single-photon source (SPS) and a polarizer connected to a fiber. The receiver comprises a polarization controller (PC), a fiber coupler (FC), a rotatable polarized beam splitter (PBS) with two Single-photon detectors (SPDs) at its outputs.

adjusting her linear polarizer to one of four angles $\theta \in \{0, \pi, \pi/2, 3\pi/2\}$. We can write Alice's state as

$$|\theta\rangle = \frac{1}{\sqrt{2}}\left(|\circlearrowleft\rangle + e^{i\theta}|\circlearrowright\rangle\right). \tag{1.2.9}$$

Unrotated, Bob's rectilinear polarized beam splitter monitored by two single-photon detectors is equivalent to the positive operator-valued measure (POVM) for detecting rectilinear-polarized light

$$\left\{\hat{P}_{\leftrightarrow} = |\leftrightarrow\rangle\langle\leftrightarrow|,\ \hat{P}_{\updownarrow} = |\updownarrow\rangle\langle\updownarrow|\right\}. \tag{1.2.10}$$

Rotated by 45°, Bob's rectilinear polarized beam splitter monitored by two single-photon detectors is equivalent to the POVM for detecting diagonal-polarized light

$$\left\{\hat{P}_{\nwarrow\!\!\searrow} = |\nwarrow\!\!\searrow\rangle\langle\nwarrow\!\!\searrow|,\ \hat{P}_{\nearrow\!\!\swarrow} = |\nearrow\!\!\swarrow\rangle\langle\nearrow\!\!\swarrow|\right\}. \tag{1.2.11}$$

Instead of Bob actively selecting the measurement basis, he can passively let the quantum randomness decide by splitting the photon with an unpolarized beam splitter towards a rectilinear and diagonal polarization detector. Figure 1.9 shows an optical setup implementing polarization-encoding BB84 with passive measurement basis selection. While Alice's transmitter setup is unchanged to the previous setup, Bob now has two polarization detectors. One polarization detector comprises a rectilinear-polarized beam splitter and two single-photon detectors. Another polarization detector comprises a diagonal-polarized beam splitter. The POVM describing Bob's measurement with passive basis selection is

$$\left\{\frac{1}{2}\hat{P}_{\leftrightarrow},\ \frac{1}{2}\hat{P}_{\updownarrow},\ \frac{1}{2}\hat{P}_{\nwarrow\!\!\searrow},\ \frac{1}{2}\hat{P}_{\nearrow\!\!\swarrow}\right\}. \tag{1.2.12}$$

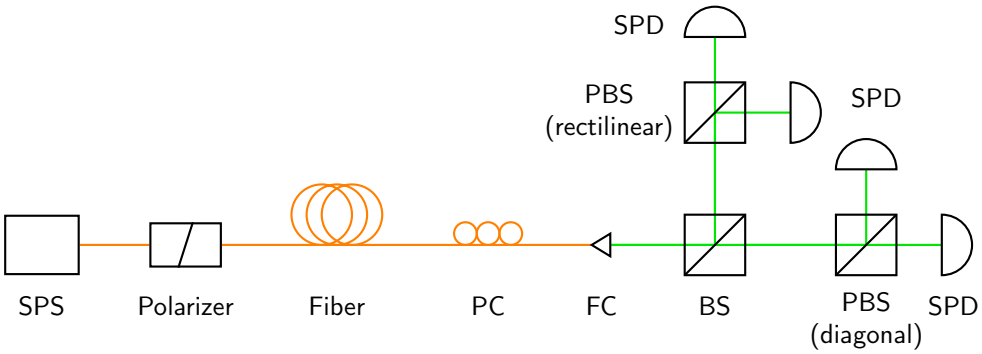


Figure 1.9.: Optical setup to implement polarization-encoding BB84 with passive basis selection. The transmitter comprises a SPS and a polarizer connected to a fiber. The receiver comprises a PC, a FC, an unpolarized beam splitter (BS), a rectilinear PBS with two SPDs at the outputs, and a diagonal PBS with two SPDs at the outputs. The receiver connects with the fiber through the PC. The FC couples the output of the PC with the BS which splits the beam among the two PBSs.

Bob may still have inconclusive measurements. For instance, if he receives a horizontal polarization state $|\leftrightarrow\rangle$ and the photon chooses the path towards the diagonal polarization detector, the clicks among the two single-photon detectors are equally distributed. The polarization of light is a qubit and we can simply relabel the polarization states with the Pauli eigenstates, i.e.,

$$|\nwarrow\rangle = |x_+\rangle \qquad |\circlearrowleft\rangle = |y_+\rangle, \qquad |\leftrightarrow\rangle = |z_+\rangle, \tag{1.2.13}$$

$$|\swarrow\rangle = |x_-\rangle \qquad |\circlearrowright\rangle = |y_-\rangle \qquad |\updownarrow\rangle = |z_-\rangle \tag{1.2.14}$$

to show equivalence to the general qubit description.

Prepared state	Measurement basis	Click probability p_1	Click probability p_2
$\|\updownarrow\rangle$	Rectilinear	100 %	0 %
	Diagonal	50 %	50 %
$\|\leftrightarrow\rangle$	Rectilinear	0 %	100 %
	Diagonal	50 %	50 %
$\|\nwarrow\searrow\rangle$	Rectilinear	50 %	50 %
	Diagonal	100 %	0 %
$\|\nearrow\swarrow\rangle$	Rectilinear	50 %	50 %
	Diagonal	0 %	100 %

Table 1.3.: Click probabilities for the polarization-encoding BB84 with active measurement basis selection depending on the states Alice prepared and the measurement bases Bob selected.

1.2.2. Time-phase-encoding BB84

In the following, we discuss the practical time-phase-encoding BB84 protocol and show its equivalence to the polarization-encoding BB84. The idea of using phase-encoding was first proposed as part of the BB92 protocol [49]. The basic setup is illustrated in Figure 1.10: Alice creates an entangled photon state using a first Mach-Zehnder interferometer (MZI) with phase $\theta \in \{0, \pi/2, \pi, 3\pi/2\}$ and sends it to Bob. Bob detects the photon state using a second MZI with phase $\phi \in \{0, \pi/2\}$ and two single-photon detectors monitoring the outputs.

To understand the time-phase encoding, we analyze the action of the asymmetric MZI with variable phase φ on a photon pulse $|t_0\rangle$ arriving at time t_0, see Figure 1.11. An ideal (lossless) and symmetric beam splitter transforms the single-photon input states into a superposition according to[6]

$$\hat{U}_{\mathrm{BS}}|1,0\rangle = \frac{1}{\sqrt{2}}\left(|1,0\rangle + i|0,1\rangle\right) \tag{1.2.15}$$

$$\hat{U}_{\mathrm{BS}}|0,1\rangle = \frac{1}{\sqrt{2}}\left(i|1,0\rangle + |0,1\rangle\right). \tag{1.2.16}$$

Then, the first beam splitter BS1 in Figure 1.11 (instantly) splits a photon pulse $|t_0\rangle$ arriving at t_0 into the superposition

$$\hat{U}_{\mathrm{BS}}|t_0,0\rangle = \frac{1}{\sqrt{2}}\left(|t_0,0\rangle + i|0,t_0\rangle\right) \tag{1.2.17}$$

[6] See Ref. [18, p. 137] and Ref. [4, p. 143]

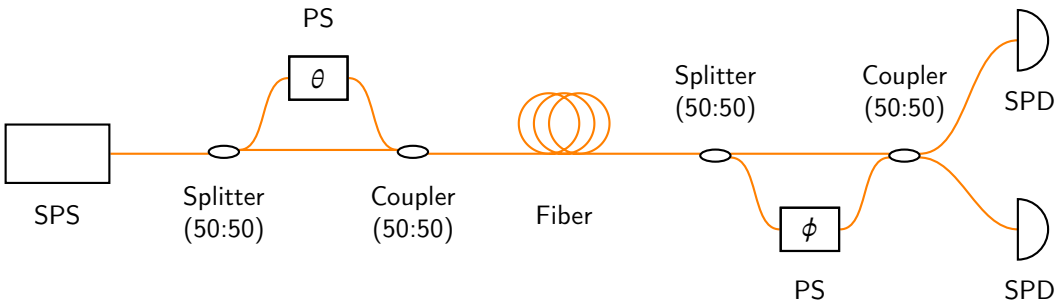


Figure 1.10.: Fiber-optical setup of the phase-encoding BB84 using active basis selection. The transmitter comprises a SPS and a first asymmetric MZI with variable phase-shift θ. The transmitter is connected to the receiver through a fiber. The receiver comprises a second asymmetric MZI with variable phase-shift ϕ. The first and second MZI are both made of two fiber couplers with a variable phase-shifter in the longer optical path. The outputs of the second asymmetric MZI is monitored by two SPDs.

where the first mode corresponds to the upper and the second mode to the lower optical path in Figure 1.11. The phase shifter adds a relative phase of φ between the upper and lower path and the input state to the second beam splitter BS2 is

$$\hat{U}_{\mathrm{PS}}\hat{U}_{\mathrm{BS}}|t_0,0\rangle = \frac{1}{\sqrt{2}}\left(|t_0+\tau,0\rangle + ie^{i\varphi}|0,t_0+\tau+\Delta\tau\rangle\right) \tag{1.2.18}$$

wherein τ is the time delay the pulse accumulates over the short upper path and $\Delta\tau$ is the difference in time delay between the shorter, lower and longer, upper path. The output state of BS2 is equal to the action of the MZI

$$\begin{aligned}\hat{U}_{\mathrm{MZM}}|t_0,0\rangle &= \hat{U}_{\mathrm{BS}}\hat{U}_{\mathrm{PS}}\hat{U}_{\mathrm{BS}}|t_0,0\rangle \\ &= \frac{1}{2}\Big[(|t_0+\tau,0\rangle + i|0,t_0+\tau\rangle) + ie^{i\varphi}\left(i|t_0+\tau+\Delta\tau,0\rangle + |0,t_0+\tau+\Delta\tau\rangle\right)\Big] \\ &= \frac{1}{2}\Big[|t_0+\tau,0\rangle - e^{i\varphi}|t_0+\tau+\Delta\tau,0\rangle + i\left(|0,t_0+\tau\rangle + e^{i\varphi}|0,t_0+\tau+\Delta\tau\rangle\right)\Big].\end{aligned} \tag{1.2.19}$$

Ignoring the vacuum state, we project the product state in eq. (1.2.19) onto each of the output modes and obtain

$$|t_1,\phi\rangle_1 = \frac{1}{\sqrt{2}}\left(|t_1\rangle - e^{i\varphi}|t_1+\Delta\tau\rangle\right) \tag{1.2.20}$$

$$|t_1,\phi\rangle_2 = \frac{i}{\sqrt{2}}\left(|t_1\rangle + e^{i\varphi}|t_1+\Delta\tau\rangle\right), \tag{1.2.21}$$

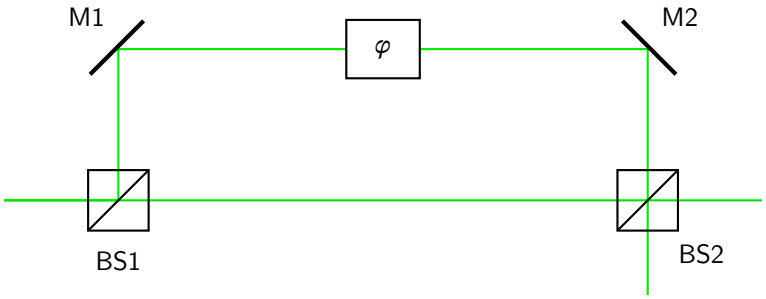


Figure 1.11.: Asymmetric MZI adding a constant time delay and variable phase difference between the upper and lower path. A pulsed state enters the first BS, BS1, to the left and is split among a longer upper path and a shorter lower path. A first mirror M1 directs the pulse from the upper path to a phase shifter which adds a relative phase of φ between the upper and lower path. A second mirror M2 directs the pulse from the phase shifter to a second BS, BS2, while the lower path is between BS1 and BS2.

wherein $t_1 = t_0 + \tau$.

Back to the time-phase-encoding BB84 setup depicted in Figure 1.10, we note that Alice's transmitter consists of a single-photon source and an asymmetric MZI where one output is dumped. Therefore, Alice's states are parametrized by the relative phase θ,

$$|t_0, \theta\rangle = \frac{1}{\sqrt{2}}\left(|t_0\rangle - e^{i\theta}|t_0 + \Delta\tau\rangle\right), \tag{1.2.22}$$

which equals the first output mode of the MZI, eq. (1.2.20), adapting the new time reference $t_1 \to t_0$. If Bob receives a pulse with time delay $\Delta\tau$ at some time t_1, i.e., $|t_1 + \Delta\tau\rangle$, then his MZI provides the two detectors with the states

$$|t_1 + \Delta\tau, \phi\rangle_1 = \frac{1}{\sqrt{2}}\left(|t_1 + \Delta\tau\rangle - e^{i\phi}|t_1 + 2\Delta\tau\rangle\right) \tag{1.2.23}$$

$$|t_1 + \Delta\tau, \phi\rangle_2 = \frac{i}{\sqrt{2}}\left(|t_1 + \Delta\tau\rangle + e^{i\phi}|t_1 + 2\Delta\tau\rangle\right). \tag{1.2.24}$$

We note that these are superpositions of states at three different time instances $0, \Delta\tau, 2\Delta\tau$. We drop the pulse time and introduce the state

$$|\Delta\tau = m\rangle = |t_1 + m\Delta\tau\rangle \tag{1.2.25}$$

corresponding to the mth detection time slot. In the new notation, Bob's detectors receive a superposition of Alice's states, eq. (1.2.24) and eq. (1.2.26),

$$|\theta, \phi\rangle_\pm = \frac{c_\pm(\theta - \phi)}{\sqrt{2}}\Big[|\Delta\tau = 0\rangle \mp \left(e^{i\phi} \pm e^{i\theta}\right)|\Delta\tau = 1\rangle \pm e^{i(\phi+\theta)}|\Delta\tau = 2\rangle\Big] \tag{1.2.26}$$

with phase-dependent normalization constant

$$c_{\pm}(\theta-\phi)=\frac{1}{\sqrt{2\pm\cos(\theta-\phi)}}. \tag{1.2.27}$$

Using the POVM for detecting a click at time slot m,

$$\left\{\hat{P}_m=|\Delta\tau=m\rangle\langle\Delta\tau=m|\right\}_{m=0,1,2}, \tag{1.2.28}$$

we find the click probabilities for the Bob's detectors to equal

$$\begin{aligned} p_{\pm,m} &= \operatorname{Tr}\hat{\rho}_{\pm}\hat{P}_m=\langle\hat{P}_m\rangle\theta,\phi_{\pm} \\ &= \begin{cases} |c_{\pm}(\theta-\phi)|^2\left(1\pm\cos(\theta-\phi)\right) & m=1 \\ |c_{\pm}(\theta-\phi)|^2\frac{1}{2} & m=0,2 \end{cases}. \end{aligned} \tag{1.2.29}$$

If we configure the detectors to trigger only on the $m=1$ time slot, we find the probability for a click of the plus and minus detectors to be

$$p_{\pm}(\theta-\phi)=\frac{1}{2}\left[1\pm\cos(\theta-\phi)\right]. \tag{1.2.30}$$

Table 1.4 summarizes the click probability of the plus and minus detectors triggered on the $m=1$ time slot for a restricted choice of phases: Alice choosing $\theta\in\{0,\pi\}$ corresponds to choosing the Z eigenbasis while $\theta\in\{\pi/2,3\pi/2\}$ corresponds to her choosing the X eigenbasis. Bob using no phase shift $\phi=0$ corresponds to a selection of the X basis while Bob adding a phase shift of $\phi=\pi/2$ corresponds to selection of X as measurement basis. Only if Alice and Bob choose the same basis, Bob's click is perfectly correlated with Alice's choice for a basis element. Otherwise, it is completely random. Comparing the click probabilities

Phase		Detector click probability	
θ	ϕ	$p_1(\theta-\phi)$	$p_2(\theta-\phi)$
0	0	100 %	0 %
	$\pi/2$	50 %	50 %
π	0	0 %	100 %
	$\pi/2$	50 %	50 %
$\pi/2$	0	50 %	50 %
	$\pi/2$	100 %	0 %
$3\pi/2$	0	50 %	50 %
	$\pi/2$	0 %	100 %

Table 1.4.: Click probabilities for the time-phase-encoding BB84 protocol depending on the MZI phase angles set by Alice and Bob.

of Table 1.4 with the probabilities of the qubit-based BB84, suggests equivalence of the time-phase-encoding BB84 with the more general qubit-based description of BB84. While we can identify Alice's state in the time basis in terms of the Y qubit basis,

$$|t_0, \theta\rangle = \frac{1}{\sqrt{2}}\left(|t_0\rangle - e^{i\theta}|t_0 + \Delta\tau\rangle\right) = \frac{1}{\sqrt{2}}\left(|y_+\rangle - e^{i\theta}|y_-\rangle\right) = |\theta\rangle, \tag{1.2.31}$$

the receiver side cannot simply be relabeled into the qubit-based description: Bob's Hilbert space, spanned by the three time slot states, $|\Delta\tau = m\rangle_{m=0,1,2}$, has one additional dimension compared to the qubit Hilbert space. Such complication can be addressed using "squashing" [50, 51]: We first find a unitary transformation for the input mode of Bob's receiver. Second, we show that the POVM yields the same probability distribution as the qubit-based description for all possible quantum states. The number state basis $\{|n\rangle\}_{n\in\mathbb{N}_0}$ is complete and countable allowing a proof by induction. It is important to show equivalence for all number states as Eve's not limited to the single-photon state.

1.3. Boson-based protocols

The quantum system of interest in boson-based protocols is a single bosonic mode, i.e., a quantum harmonic oscillator. For more information on boson information theory, see Ref. [30, 31] and Ref. [52, 53] for a particular application towards CV-QKD.

The central observable is the generalized quadrature operator [10, p. 36]

$$\hat{X}(\vartheta) = \frac{1}{\sqrt{2}}\left(\hat{a}e^{-i\vartheta} + \hat{a}^\dagger e^{+i\vartheta}\right) \tag{1.3.1}$$

wherein $\hat{a}^\dagger, \hat{a}$ are the bosonic creation and annihilation operators satisfying the canonical commutation relation (CCR)

$$[\hat{a}, \hat{a}^\dagger] = 1 \qquad\qquad [\hat{a}, \hat{a}] = 0 = [\hat{a}^\dagger, \hat{a}^\dagger]. \tag{1.3.2}$$

It follows that the generalized quadrature operator satisfies the commutator

$$[\hat{X}(\vartheta), \hat{X}(\vartheta + \Delta\vartheta)] = i\sin\Delta\vartheta. \tag{1.3.3}$$

The Robertson uncertainty relation provides a lower bound for the product of the standard deviation of two operators in terms of their commutator. The Robertson uncertainty relation for the generalized quadrature operator,

$$\langle\Delta\hat{X}(\vartheta)\rangle\langle\Delta\hat{X}(\vartheta + \Delta\vartheta)\rangle \geq \frac{1}{2}|\langle[\hat{X}(\vartheta), \hat{X}(\vartheta + \Delta\vartheta)]\rangle| = \frac{1}{2}\sin\Delta\vartheta, \tag{1.3.4}$$

generalizes Heisenberg's uncertainty relation and implies maximal uncertainty for orthogonal quadratures $\Delta\vartheta = \pi/2$. Let us assume the existence of an eigenstate $|x, \vartheta\rangle$ of the generalized quadrature operator $\Delta\hat{X}(\vartheta)$ with eigenvalue $x \in \mathbb{R}$, i.e.,[7]

$$\hat{X}(\vartheta)|x, \vartheta\rangle = x|x, \vartheta\rangle, \tag{1.3.5}$$

then the uncertainty relation implies that $|x, \vartheta\rangle$ and $|p, \vartheta + \Delta\vartheta\rangle$ for $\Delta\vartheta > 0$ are conjugate variables, i.e., increasing the precision of one variable decreases the precision of the other. Unsurprisingly, we can show that these eigenstates are non-orthogonal [54, p. 29]

$$\langle x, \vartheta|p, \vartheta + \pi/2\rangle = \frac{e^{ipx}}{\sqrt{2\pi}}. \tag{1.3.6}$$

Furthermore, by using the completeness of eigenstates, we can show that the eigenstates of orthogonal quadratures are related by an unitary transform,

$$|x, \vartheta\rangle = \int \frac{\mathrm{d}p}{\sqrt{2\pi}} e^{-ipx}|p, \vartheta + \pi/2\rangle = \hat{U}|p, \vartheta + \pi/2\rangle, \tag{1.3.7}$$

the Fourier transform. The non-orthogonality of the quadrature eigenstates, makes the bosonic system a candidate for QKD. For instance, we can envision a bosonic BB84 protocol:

1. Alice prepares the state $|\pm x, \vartheta + \Delta\vartheta\rangle$ where she randomly picks the sign of the eigenvalue $\pm x$ and $\Delta\vartheta = 0, \pi/2$.

2. Bob performs a homodyne measurement of one (active) or both (passive) quadratures.

Figure 1.12 visualizes Alice's four quantum states in the optical phase space. If she chooses the quadrature corresponding to $\Delta\vartheta = 0$, a measurement in the orthogonal quadrature eigenbasis yields a completely uncorrelated outcome. Only if Bob measures in the same quadrature, can he decode the sign of the eigenvalue. Table 1.5 summarizes a possible quantum-transmission sequence of bosonic BB84. Alice randomly selects the eigenvalue sign $x/|x|$ and a quadrature $\vartheta \in \{0, \pi/2\}$ which she encodes into a quantum state $|\pm x, \vartheta\rangle$ and sends it to Bob. Bob selects a quadrature for measurement. Only if Alice's and Bob's basis match, is Bob's outcome correlated with Alice's value. To convert the sifted outcome to bits, we can simply assign the bit value according to the sign. More advanced symbol mapping techniques are discussed in the post-processing section.

The suggested bosonic BB84 highlights the differences and similarities of boson- and qubit-based QKD. However, it cannot be implemented as no quadrature eigenstates exist - not even theoretically on the Hilbert space! That said, we can use squeezed coherent states as an approximation for quadrature eigenstates as discussed in the next section.

[7] Actually, the quadrature eigenstates only exist on the extended Hilbert space as they itself are not square-integrable.

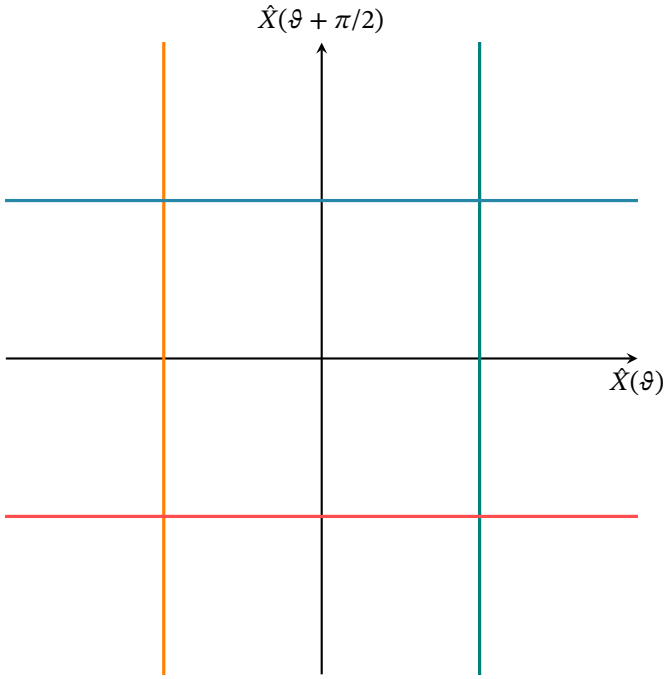


Figure 1.12.: Phase space representation of Alice's quantum states in bosonic BB84. The analog of Alice's basis selection is to choose between the two orthogonal quadratures with $\Delta\vartheta = \pi/2$. The analog of Alice's basis element selection is to choose the sign of the eigenvalue $\pm x$.

		Transmission				
Party	Step	1	2	3	4	5
Alice	Quadrature value	$+x$	$-x$	$-x$	$+x$	$-x$
	Quadrature angle	0	$\pi/2$	0	$\pi/2$	0
	Prepared state	$\lvert+x, 0\rangle$	$\lvert-x, \pi/2\rangle$	$\lvert-x, 0\rangle$	$\lvert+x, \pi/2\rangle$	$\lvert-x, 0\rangle$
Bob	Quadrature angle	$\pi/2$	$\pi/2$	0	$\pi/2$	0
	Sifted outcome	-	$-x$	$-x$	$+x$	$-x$

Table 1.5.: Possible quantum-transmission sequence for bosonic BB84 with active basis selection.

1.3.1. Squeezed-coherent-encoding BB84

A squeezed coherent state, denoted $|\alpha, \xi\rangle$, has the special property that the quadrature standard-deviation is parametrized [7, p. 95]

$$\langle \alpha, \xi | \Delta \hat{X}(\vartheta) | \alpha, \xi \rangle = |\mu e^{+i\vartheta} - \nu^* e^{-i\vartheta}| \tag{1.3.8}$$

wherein parameters ν, μ relate to the complex squeezing parameter $\xi = |\xi| e^{i\varphi}$ via [7, p. 90]

$$\mu = \cosh|\xi| = 1 + |\nu|^2 \qquad \nu = e^{i\varphi} \sinh|\xi| = |\nu| e^{i\varphi}. \tag{1.3.9}$$

If the squeezing angle φ satisfies a particular phase relation with the quadrature angle ϑ, the quadrature standard deviation takes the form [7, p. 96]

$$\langle \alpha, \xi_{\max/\min} | \Delta \hat{X}(\vartheta) | \alpha, \xi_{\max/\min} \rangle = \exp(\pm |\xi_{\max/\min}|). \tag{1.3.10}$$

In the limit of infinite squeezing magnitude $|\xi_{\max/\min}| \to \infty$, we obtain the previously discussed quadrature eigenstates $|x, \vartheta\rangle$. Therefore, we can implement bosonic BB84 using strongly squeezed coherent states. Figure 1.13 depicts the optical phase space for Alice's strongly squeezed coherent states for bosonic BB84. Contrary to quadrature eigenstates, the uncertainty in the unsqueezed quadrature is not infinite. Measurements of the unsqueezed quadrature are not completely uncorrelated. However, the squeezing magnitude $|\xi|$ can (in theory) be chosen arbitrarily large such that the correlation can be arbitrarily reduced. To implement the quadrature measurement, Bob can employ a homodyne detection. A fiber-optical setup for homodyne detection is depicted in Figure 1.14. At its heart, the homodyne detector consists of a local oscillator (LO), a balanced coupler (or beam splitter) and two photodiodes in balanced configuration. The LO is superimposed with the signal through the coupler and the two coupler outputs are monitored by one photodiode. In balanced configuration, the photocurrent of the photodiodes is subtracted removing the constant power of the signal and LO. Assuming a perfect detector and strong LO with coherent state $|\alpha_l\rangle$ and $|\alpha_l| \gg 1$, the mean balanced photodiode current is proportional to [7, p. 217]

$$\langle \Delta \hat{N}' \rangle = \langle \hat{N}_1' \rangle - \langle \hat{N}_2' \rangle = |\alpha_l| \langle \hat{X}(\vartheta) \rangle \tag{1.3.11}$$

wherein ϑ is the phase difference between the signal and the LO. Moreover, it can be shown that the POVM of an ideal homodyne detector is [7, p. 220]

$$\left\{ \hat{P}_{\Delta n} = \frac{1}{|\alpha_l|} |x, \vartheta\rangle\langle x, \vartheta| \right\}_{\Delta n \in \mathbb{Z}} \tag{1.3.12}$$

wherein $|x, \vartheta\rangle$ has quadrature eigenvalue $x = \Delta n / |\alpha_l|$. The single homodyne detector corresponds to an active measurement basis selection of Bob. As in the case of the polarization-encoding qubit-based QKD, Bob can also use a second homodyne detector to implement passive measurement basis selection. Such a setup is illustrated in Figure 1.15. Contrary to the quadrature eigenstates, squeezed coherent states are physical and have been prepared

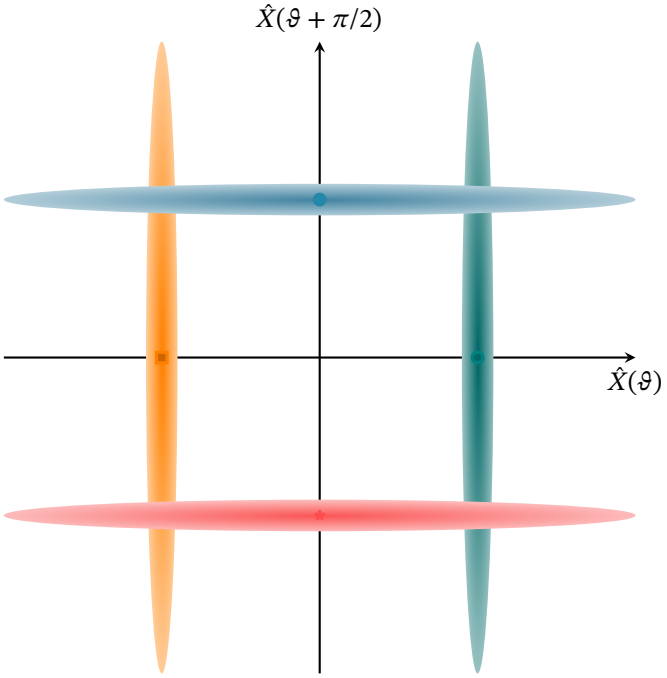


Figure 1.13.: Phase space representation of Alice's squeezed coherent states in bosonic BB84. The uncertainty is sufficiently squeezed to approximate the quadrature eigenstates.

and measured with up to 15 dB squeezing [55]. However, the production of squeezed coherent states requires nonlinear interactions, which are challenging to control and require with the current state of art a complex optical setup. Additionally, squeezed states quickly loose their squeezing by attenuation. We conclude that although squeezed coherent states present a possible quantum state for boson-based QKD, we prefer a more practical and reliable quantum state.

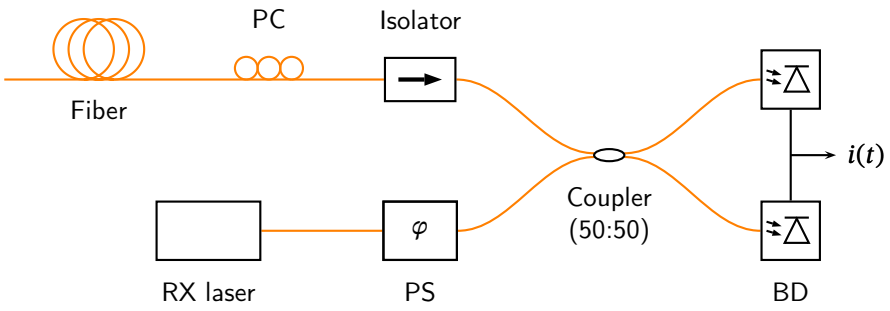


Figure 1.14.: Fiber-optical setup of a coherent receiver with active basis selection. The receiver comprises a receiver (RX) laser connected to a phase-shifter (PS) with phase φ in the lower left branch, and the signal fiber connected with a PC and protected by an optical isolator in the upper left branch. The phase-shifted RX laser is superimposed with the isolated and polarization-controlled signal in a balanced coupler where the two coupler outputs are monitored by two photodiodes (PDs) in balanced configuration, a balanced detector (BD).

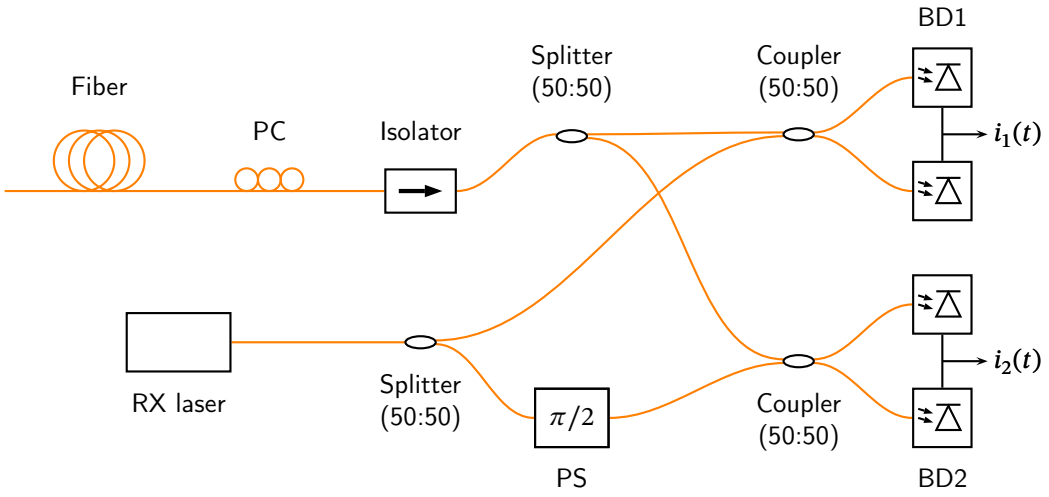


Figure 1.15.: Fiber-optical setup of a coherent receiver with passive basis selection. The upper left branch connects to the signal fiber with a PC and an optical isolator. The lower left branch splits a RX laser with equal power into two branches, where the lower one of them is phase-shifted by $\pi/2$. The isolated and polarization-controlled upper branch is coupled with the phase-shifted and non-phase shifted RX laser branches and then monitored by two BDs.

1.3.2. Coherent-encoding GG02

Coherent states are the ”most classical” quantum states and can be prepared using standard telecommunication components, see, for instance, Figure 1.16. Moreover, coherent states

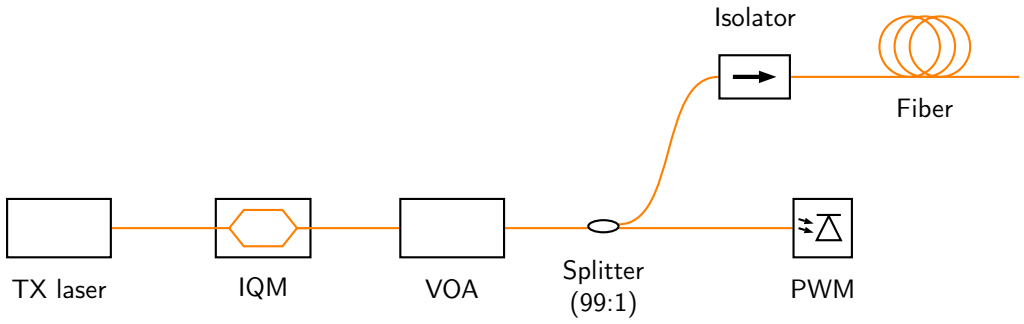


Figure 1.16.: Fiber-optical setup of a coherent transmitter. A transmitter (TX) laser is connected with an in-phase and quadrature modulator (IQM), followed by a variable optical attenuator (VOA). The output of the VOA is split into an upper low-power and a lower high-power branch. The high-power branch is monitored by a power meter (PWM), while the low-power branch passes an optical isolator connected with a fiber.

do not deteriorate to a different quantum state when interacting with the environment, e.g., inside a fiber channel. In sum, coherent states seem to be the most practical quantum states. One apparent disadvantage of coherent states is that the quadrature standard deviation is independent of the quadrature angle and the state parameters [10, p. 59]

$$\langle\alpha|\Delta\hat{X}(\vartheta)|\alpha\rangle = \frac{1}{\sqrt{2}}. \tag{1.3.13}$$

We cannot emulate a basis selection by changing the statistics of the quadratures and we need to rethink our approach to QKD: Instead of slowly producing highly correlated variables, we quickly produce hardly correlated variables. By employing sophisticated error correction techniques, Alice and Bob can still distill a shared bit string, see the post-processing section for details.

Figure 1.17 highlights the quantum transmission of two coherent states in coherent-encoding boson-based QKD. The mean (quadrature) of the coherent state is indicated by the colored marker. The variance of the coherent state is indicated by the shaded circles around the markers. The channel attenuates the coherent state by reducing the mean but the variance remains constant. An intercept-resend attempt by Eve is illustrated in Figure 1.18. When Eve intercepts and measures Alice's coherent state $|\alpha\rangle$, her outcome β (red star) is distributed around the mean α due to the quadrature uncertainty. Eve's best guess is to prepare a new

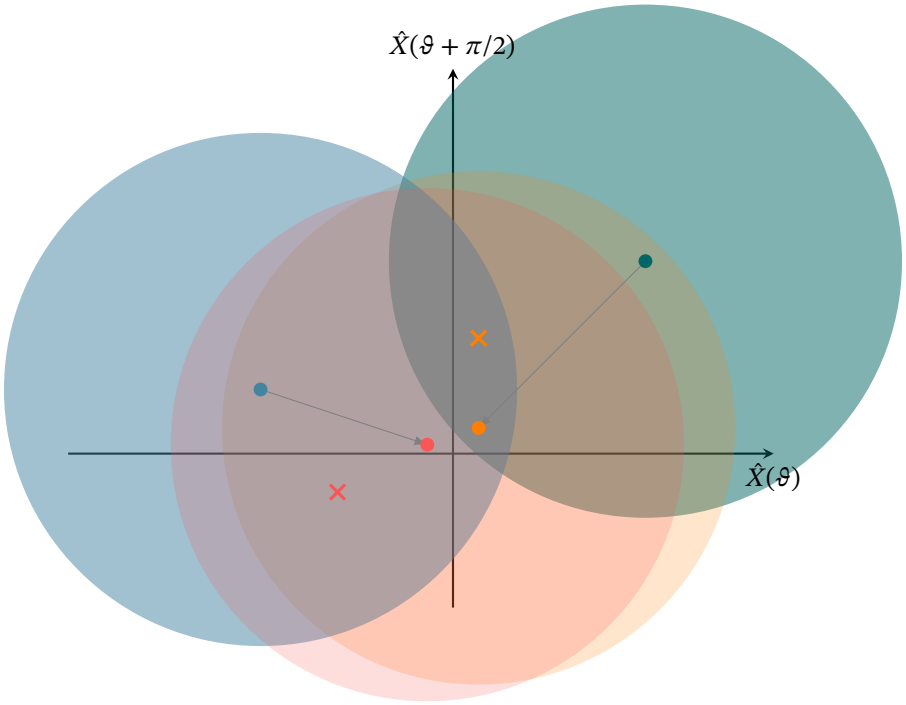


Figure 1.17.: Phase space representation of two coherent-state transmissions. Alice prepares the coherent states $|\alpha_1\rangle$ (green), $|\alpha_2\rangle$ (blue) with mean quadratures α_1 (green dot) respectively α_2 (blue dot) and sends them to Bob through a channel (gray arrow). Bob receives the attenuated coherent states $|\beta_1\rangle$ (orange) and $|\beta_2\rangle$ (red). He performs a dual homodyne measurement with outcomes β_1' respectively β_2'.

coherent state $|\beta\rangle$ where she prepares the mean β to be equal to her measurement outcome β. Although, the channel attenuation strongly deteriorates the signal-to-noise ratio (SNR), Bob's measurement distribution will be ragged due to Eve's imperfect state copy. Alice and Bob notice a higher than usual error when performing error correction. Alternatively, Eve can only measure a single quadrature and prepare a squeezed coherent state $|\beta, \xi\rangle$ to hide her measurement. If Bob uses a dual-quadrature homodyne receiver, he will directly notice the increase of noise in one of the quadratures. If Bob uses a single homodyne receiver, he will only notice every second measurement on average, which is still sufficient to detect Eve's tempering.

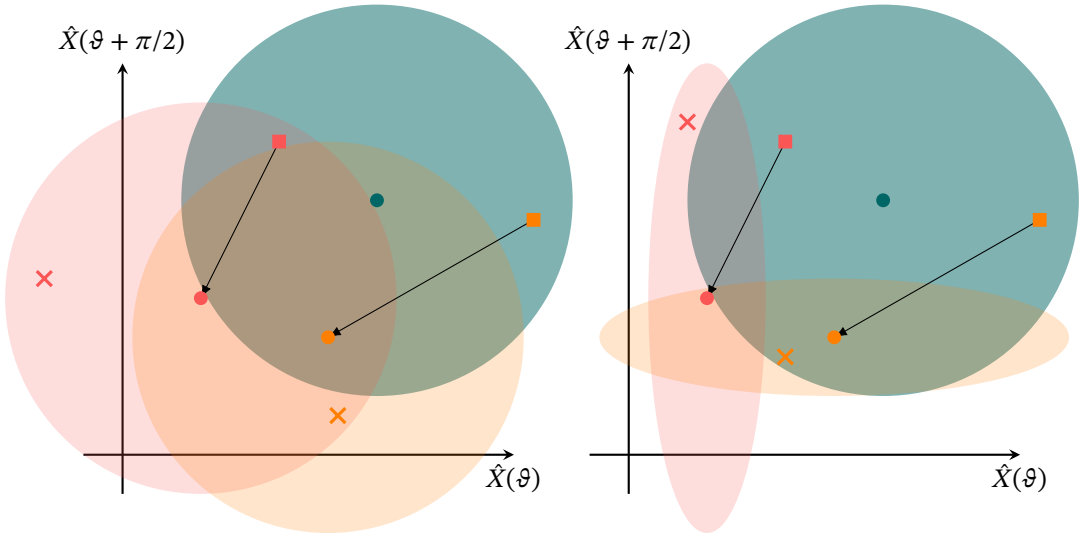


Figure 1.18.: Phase space representation of coherent-state transmission with an intercept-resend attack from Eve using a coherent state (left) and a squeezed coherent state (right). Alice always prepares the same coherent state (green circle). In a first realization, Eve intercepts Alice's state (green circle) and measures (red square) for the quadrature. She then prepares a coherent state with that quadrature and sends it to Bob. Through the attenuated channel (black arrow), Bob receives the coherent state (red circle) and measures (red cross) for the quadrature. In a second realization, Eve measures (orange square) for the quadrature of the intercepted state. She then prepares a new coherent state (orange circle) and sends it to Bob. Bob receives the attenuated state (orange circle) and finds (orange cross) in a quadrature measurement. Instead of preparing a coherent state, Eve can prepare squeezed coherent states (right) for which Bob receives squeezed coherent states of which he measures the quadrature.

1.4. Post-processing

In the previous sections, we focused on the quantum transmission producing raw data for Alice and Bob. Post-processing summarizes methods Alice and Bob employ over the classical channel to distill a shared secret key from the raw data. It is an important part of the protocol and may be very different depending on the particular implementation. In an attempt to identify common steps in post-processing, we found the data flow diagram depicted in Figure 1.19. The starting point of the post-processing is the raw data from the quantum transmission. For the transmitter, the raw data includes the bits determining the state preparation for transmission. On the contrary, the receiver's raw data consists of the measurement data. Alice and Bob agree over the classical channel on partitioning their raw data into raw key data ($\approx 80\,\%$) and raw calibration data ($\approx 20\,\%$). They disclose their raw calibration data to perform parameter estimation mainly used for error estimation, correlating

to Eve's information on the raw (key) data. Optionally, a comparison of the raw calibration data reveals information about the channel characteristics, improving error correction. The symbol mapping extracts correlated key data from the raw key data and might include base sifting. Information reconciliation transforms the correlated key data, which is different for Alice and Bob, into a partially secret key, which Alice and Bob agree. Unlike error correction, which might fail, information reconciliation ensures that Alice and Bob hold the same partially secret key, even at the cost of having a partially secret key of length zero. Privacy amplification removes Eve's information from the partially secret key by reducing the partially secret key length by Eve's information. Finally, by comparing a checksum, Alice and Bob verify that they indeed share the same secret key. If Eve's information is beyond a certain threshold or Alice and Bob do not share the same key, in the end, the post-processing is assumed to have failed, and the protocol is either aborted or the transmission block discarded. In the following, we introduce some of the most important steps in post-processing: symbol mapping, information reconciliation, and privacy amplification.

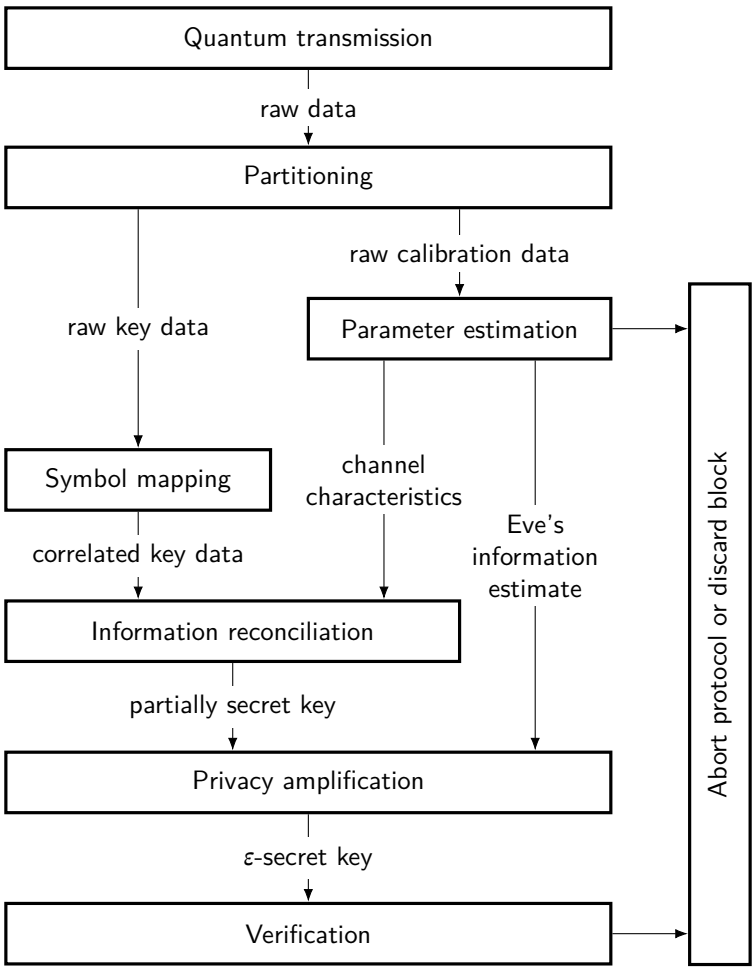


Figure 1.19.: Flow diagram of a generalized QKD post-processing procedure. The quantum transmission produces raw data, and partitioning splits the raw data into raw calibration and key data. Parameter estimation on the raw calibration data assesses the channel characteristics and Eve's information's upper bound, which decides whether to abort the protocol or discard the transmission block. Symbol mapping transforms the raw key data to correlated key data. Information reconciliation includes the channel characteristics to correct errors in the correlated key data or discard data blocks where error correction failed, yielding a partially secret key. Privacy amplification produces a secret key by removing the estimate for Eve's information from the partially secret key. Verification confirms if the post-processing produced a correct secret key, otherwise, abort the protocol or discards the transmission block.

1.4.1. Symbol mapping

The symbol mapping takes a sequence of symbols and maps it to a sequence of bits. The two basis elements of qubit-based QKD protocols have a natural interpretation as bits, i.e.,

$$\begin{aligned} \mathbf{s} &: \Omega \to \{0,1\} \\ \omega &\mapsto \mathbf{s}(\omega) = \begin{cases} 1 & \text{"click"} \\ 0 & \text{"no click"} \end{cases}. \end{aligned} \tag{1.4.1}$$

Not so the quadrature value in boson-based QKD protocol. While we can assign bits according to the sign of the quadrature

$$\begin{aligned} \mathbf{s} &: X \subseteq \mathbb{R} \to \{0,1\} \\ x &\mapsto \mathbf{s}(x) = \begin{cases} 1 & x \geq 0\,, \\ 0 & x < 0 \end{cases} \end{aligned} \tag{1.4.2}$$

such a symbol mapping turns out to be highly inefficient and more powerful techniques have been developed [56, 57].

Many CV-QKD protocols implement slice reconciliation [58] which includes a first error correction. The idea of slice reconciliation is to partition the value range into 2^m bins of equal width and assign them a bit string according to the binary representation of their index number. Figure 1.20 illustrates slice reconciliation for $m = 3$ yielding $2^m = 8$ different bins for a standard normal distributed random variable. Alice's x_i and Bob's variables x_i' are not equal but correlated. Alice and Bob assign bits to their variable according to the binning scheme. If Alice and Bob are lucky, the assignment yields the same bit sequence. For example, Alice and Bob both assign x_1 and x_1' to the third bin and now share bit string 011. However, it happens that Alice and Bob assign different bins, see, for instance, x_2 and x_2' which are assigned to the fourth bin (Alice) and the fifth bin (Bob). In this particular case, if Bob knows the least significant bit from Alice, he is able to correct his bit string assignment to 100.

In an alternative scheme, known as multidimensional reconciliation [57], Alice and Bob combine multiple variables into a d-dimensional vector, e.g., $\mathbf{x} = (x_1, \dots, x_d)$ respectively $\mathbf{x}' = (x_1', \dots, x_d')$ and agree on a set of equally-spaced apart symbol vectors $\hat{\mathbf{v}}_1, \dots, \hat{\mathbf{v}}_m \in \mathbb{R}^d$. Now, Bob finds a rotation matrix $R' \in \mathbb{R}^{d\times d}$ which maps his variable vector onto a symbol vector $\mathbf{v}_j = R'\mathbf{x}'$. Bob then discloses the parameters of his rotation matrix R' to Alice. Alice rotates her variable vector $R\mathbf{x}$ and finds the symbol vector $\mathbf{v}_k$ with least distance to $R\mathbf{x}$. Multidimensional reconciliation works best in high-dimensional spaces as the norm of a random vector approaches one (unit sphere) for $n \to \infty$.

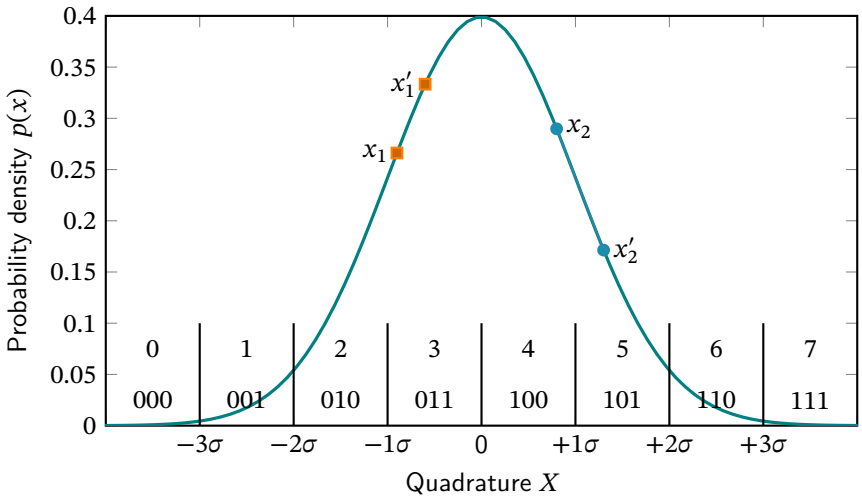


Figure 1.20.: Slice reconciliation for $m = 3$ with $2^m = 8$ bins for samples from a standard normal distribution. Alice prepared the values x_1, x_2 and Bob measured the values x_1', x_2'. x_1 and x_1' are located in the same bin 3 but x_2 and x_2' are located in bin 4 respectively bin 5. Slice reconciliation is able to detect and correct such errors with high probability.

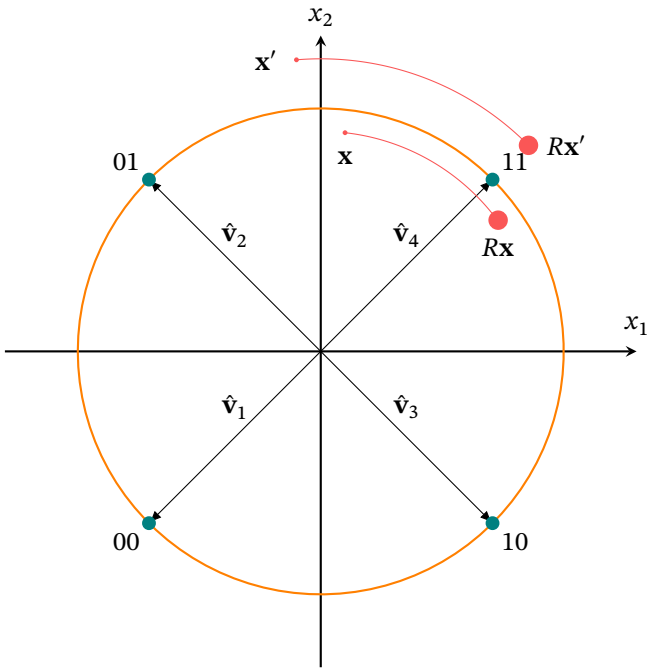


Figure 1.21.: Multidimensional reconciliation in $\mathbb{R}^2$: Alice and Bob encoded their prepared and measured values into two-dimensional vectors $\mathbf{x}$ and $\mathbf{x}'$. Bob calculates the rotation matrix R that rotates $\mathbf{x}'$ close to the symbol vector $\hat{\mathbf{v}}_4$ and shares the rotational parameters with Alice. Alice applies the rotation to her vector $R\mathbf{x}$. Both rotated vectors of Alice and Bob $R\mathbf{x}$ and $R\mathbf{x}'$ are assigned the 11 bit string with high confidence.

1.4.2. Information reconciliation

Information reconciliation summarizes methods required for Alice and Bob to agree on shared data. It includes error correction, and discarding of data failed to correct.

Let us first consider procedures for error correction. Error correction is a subdiscipline of coding theory, or more precisely, channel coding, which studies the arrangement of data for efficient and reliable transmission. The following discussion is a very brief introduction to binary linear codes based of Ref. [59, 60]. A (n, k) binary linear code encodes k-bit messagewords into n-bit codewords. The additional $n-k$ check bits are used to detect and correct errors, e.g., bit flips. In general, it is impossible to correct for all errors although practical linear block codes closely approach the theoretical (Shannon) limit set by the noisy-channel coding theorem.

Let $\mathbf{m} \in \{0,1\}^{1\times k}$ be a messageword, then the generator matrix

$$G = (\mathbb{1}_k|P) = \left(\begin{array}{cccc|ccc} 1 & 0 & \cdots & 0 & p_{1,1} & p_{1,2} & \cdots & p_{1,m} \\ 0 & 1 & \cdots & 0 & p_{2,1} & p_{2,2} & \cdots & p_{2,m} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & p_{n-m,1} & p_{n-m,2} & \cdots & p_{n-m,m} \end{array}\right) \in \{0,1\}^{k\times n}, \tag{1.4.3}$$

wherein $\mathbb{1}_k \in \{0,1\}^{k\times k}$ denotes an identity matrix and $P \in \{0,1\}^{k\times(n-k)}$ denotes the (parity) check matrix, encodes the messageword $\mathbf{m}$ into the codeword

$$\mathbf{x} = \mathbf{m}G \in \{0,1\}^{1\times n} \tag{1.4.4}$$

with the matrix multiplication being defined on the binary field $\mathbb{F}_2$[8]. The explicit form of the generator matrix depends on the linear block code. For instance, the $(n, 1)$ repetition code has the generator matrix

$$G = \begin{pmatrix} 1 & 1 & \cdots & 1 \end{pmatrix} \in \{0,1\}^{1\times n} \tag{1.4.5}$$

and the $(7, 4)$ Hamming code has the generator matrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \in \{0,1\}^{4\times 7}. \tag{1.4.6}$$

For the post-processing, we use low-density parity-check (LDPC) [61] where the generator matrix is a sparse random matrix. Table 1.6 and Table 1.7 show the possible codewords for the $(3, 1)$ repetition and $(7, 4)$ Hamming code. From Table 1.6, we note that the repetition code repeats the message word $n-k$ times. The $(n, 1)$ repetition code is able to detect all bit errors except the error when all bits are flipped and correct up to $\lfloor (n-1)/2 \rfloor$ bit errors [59, p. 5]. The $(7, 4)$ Hamming code is a more efficient block code which uses parity checks to detect and correct single-bit errors [59, p. 10]. The received codeword $\mathbf{y}$ of a linear channel

[8] Alternatively, we can define the addition and multiplication on the real field with modulo two.

Nr.	Information	Check
1	0	0 0
2	1	1 1

Table 1.6.: Possible codewords for $(3, 1)$ repetition code.

Nr.	Information				Check		
1	0	0	0	0	0	0	0
2	0	0	0	1	1	1	1
3	0	0	1	0	1	1	0
4	0	0	1	1	0	0	1
5	0	1	0	0	1	0	1
6	0	1	0	1	0	1	0
7	0	1	1	0	0	1	1
8	0	1	1	1	1	0	0
9	1	0	0	0	0	1	1
10	1	0	0	1	1	0	0
11	1	0	1	0	1	0	1
12	1	0	1	1	0	1	0
13	1	1	0	0	1	1	0
14	1	1	0	1	0	0	1
15	1	1	1	0	0	0	0
16	1	1	1	1	1	1	1

Table 1.7.: Possible codewords for $(7, 4)$ Hamming code [60, p. 109].

equals the sent codeword $\mathbf{x}$ plus a noise (row) vector $\mathbf{n}$, i.e.,

$$\mathbf{y} = \mathbf{x} + \mathbf{n} \in \{0, 1\}^n. \tag{1.4.7}$$

The noise vector introduces bit flips according to an assumed channel model, for example, the binary symmetric channel where a single bit flip occurs with probability p, see, e.g., Ref. [59, p. 148]. To detect errors of a received codeword $\mathbf{y}$, one uses the parity-check matrix

$$H = (-P^\intercal | \mathbb{1}_{n-k}) = \left(\begin{array}{cccc|cccc} p_{1,1} & p_{2,1} & \cdots & p_{n-m,1} & 1 & 0 & \cdots & 0 \\ p_{1,2} & p_{2,2} & \cdots & p_{n-m,2} & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ p_{1,m} & p_{2,m} & \cdots & p_{n-m,m} & 0 & 0 & \cdots & 1 \end{array}\right) \in \{0, 1\}^{(n-k)\times n} \tag{1.4.8}$$

where we used $-p_{i,j} = p_{i,j}$ for elements of the binary field $p_{i,j} \in \mathbb{F}_2$. The parity-check matrix is orthogonal to the generator matrix [60, p. 95], i.e.,

$$GH^\intercal = \mathbf{0} = HG^\intercal. \tag{1.4.9}$$

The orthogonality between generator and parity-check matrix implies that for the received codeword $\mathbf{y}$, the parity-check matrix yields, a binary vector called the syndrome (column) vector

$$\mathbf{s} = H\mathbf{y}^\top = HG^\top\mathbf{m}^\top + H\mathbf{n}^\top = H\mathbf{n}^\top \tag{1.4.10}$$

which only depends on the noise (row) vector $\mathbf{n}$. If the block code does not detect any error, we have $\mathbf{s} = 0$. Table 1.8 lists the possible syndromes for the $(3, 1)$ repetition code. To correct

Nr.	Received codeword				Syndrome		
1	0	0	0	0	0	0	0
2	0	0	0	1	0	0	1
3	0	0	1	0	0	1	0
4	0	0	1	1	0	1	1
5	0	1	0	0	1	0	0
6	0	1	0	1	1	0	1
7	0	1	1	0	1	1	0
8	0	1	1	1	1	1	1
9	1	0	0	0	1	1	1
10	1	0	0	1	1	1	0
11	1	0	1	0	1	0	1
12	1	0	1	1	1	0	0
13	1	1	0	0	0	1	1
14	1	1	0	1	0	1	0
15	1	1	1	0	0	0	1
16	1	1	1	1	0	0	0

Table 1.8.: Possible syndromes for the $(3, 1)$ repetition code. The first and last row are correct codewords (without noise) and yield a zero syndrome indicating no error. All other received codewords contain bit flips and thereby non-zero syndromes.

the error, one looks up the calculated syndrome in an error correction table. For example, Table 1.9 lists the bit-error corrections assigned to each syndrome of the $(7, 4)$ Hamming code.

Syndrome $\mathbf{s}$	001	010	011	100	101	110	111
Unflip bit	y_7	y_6	y_4	y_5	y_1	y_2	y_3

Table 1.9.: Bit-error correction lookup table for the $(7, 4)$ Hamming code [59, p. 11].

So far, we have implicitly assumed the (parity) check bits to be transmitted together with the data bits such that errors can be directly detected and corrected (forward error correction). Forward error correction does not make sense for QKD as the data bits are a result of the

post-processing and not directly transmitted. Instead of exchanging the check bits together with a data index as part of the error correction in QKD, one instead directly calculates the syndromes and transmits these depending on the implementation details.

There cannot exist a perfect error correction protocol as it is always possible that bits are flipped such that a different valid codeword is received. However, we have no use of data blocks where error correction have failed and we can simply discard them. To identify these data blocks, Alice and Bob exchange hashes of their data blocks to verify success of the error correction.

1.4.3. Privacy amplification

The final step of most QKD protocols is privacy amplification which removes Eve's information from the key. More formally, let us assume a key of length n, $s \in \{0,1\}^n$, and that Eve has partial information over the key equivalent to k bits. For privacy amplification, Alice and Bob need to agree on a map $f : \{0,1\}^n \to \{0,1\}^r$ with $r \leq n - k$ which extracts Eve's information from the key.

Bennett and Brassard proposed privacy amplification four years after BB84 in 1988. An information-secure proof that privacy amplification is possible was published one year later, now known as the leftover-hash-lemma [62] and later extended to the quantum leftover-hash-lemma [63]. In 1995, Bennett and Brassard generalized the privacy amplification outside of QKD [64].

In practice, privacy amplification is performed by randomly XORing the bits of a key. Let us illustrate this using a partially secret key $(s_1, s_2, s_3) \in \{0,1\}^3$ where Eve knows the value of s_3. After privacy amplification the initial key could be for example $(s_1 \oplus s_3, s_2 \oplus s_3)$ or $(s_1 \oplus s_2, s_2 \oplus s_3)$ and Eve's knowledge of the key bit s_3 does not help her infering a single bit of the new secret key.

Although not directly related to privacy amplification, it is helpful to consider the following Gedankenexperiment to gain intuition about XORing: Let us assume Alice and Bob generate a key by flipping a coin n times and assigning heads to zero and tails to one. Eve having no information about the key corresponds to Alice and Bob using an unbiased coin yielding heads and tails with equal probability. Eve having full information about the key corresponds to Alice and Bob using a biased coin always yielding, e.g., heads. Therefore, we can use the probability of the coin yielding heads, $p \in [0,1]$, to indicate Eve's information. If we now start to XOR all outcomes, we see the probability for obtaining either a one or zero to approach $1/2$. More precisely, let $X_1, X_2, \ldots, X_N$ be independent- and identical-distributed Bernoulli random-variables with probability $p, X_i \sim \text{Bern}(p)$, then the probability that XOR-

ing of all outcomes equals one is

$$\mathbb{P}\left[\text{"XOR of outcomes equals one"}\right] = \mathbb{P}\left[\sum_{n=1}^{N} X_n \bmod 2 = 1\right]. \tag{1.4.11}$$

The sum of Bernoulli random variables $X_1, \ldots, X_n$ equals a Binomial random variable $Y = \sum_{n=1}^{N} X_n \sim \text{Binom}(N, p)$, yielding

$$\mathbb{P}\left[Y \bmod 2 = 1\right] = \sum_{k\,\text{odd}}^{N} \mathbb{P}\left[Y = k\right] = \sum_{k\,\text{odd}}^{N} \binom{N}{k} p^k (1-p)^{N-k}. \tag{1.4.12}$$

Using the identity from Ref. [65], we can simplify eq. (1.4.12) to

$$\mathbb{P}\left[Y \bmod 2 = 1\right] = \frac{1}{2}\left(1 - (2p-1)^N\right) \xrightarrow{N\to\infty} \frac{1}{2} \tag{1.4.13}$$

where limit is true for $p \in]0,1[$ so even for $p = 0.9999$. Moreover, for any $\varepsilon > 0$ we can choose N such that $\mathbb{P}\left[Y \bmod 2 = 1\right] - 1/2 < \varepsilon$, meaning that we can arbitrarily reduce Eve's information by XORing more coin flips.

For practical applications, privacy amplification operates on the class of linear maps,

$$\begin{aligned} f:\ \{0,1\}^n &\to \{0,1\}^{n-k} \\ \mathbf{s} &\mapsto M\mathbf{s} \bmod 2 \end{aligned} \tag{1.4.14}$$

where $M \in \{0,1\}^{r\times n}$ is a random boolean matrix with at least $k+1$ ones [66]. For construction of M it is convenient to use Toeplitz matrices [33, p. 11]. A $n \times m$ Toeplitz matrix A has the form

$$A = \left(a_{i,j}\right) = \left(a_{i-j}\right) = \begin{pmatrix} a_0 & a_{-1} & \cdots & a_{1-m} \\ a_1 & a_0 & \cdots & a_{2-m} \\ \vdots & \ddots & \cdots & \vdots \\ a_{n-1} & a_{n-2} & \cdots & a_{n-m} \end{pmatrix}. \tag{1.4.15}$$

For example, if Alice and Bob estimate Eve to know three bits, they could agree on the Toeplitz coefficients $(a_{-4}, a_{-3}, \ldots, a_1, a_2) = (0,1,1,1,0,1,0)$ yielding the mapping

$$f(\mathbf{s}) = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} \bmod 2 \tag{1.4.16}$$

which for the key $\mathbf{s} = (0,1,1,0,1)$ would yield the secret key $\mathbf{s}' = (0,0,0)$.

1.5. Security analysis

For completeness, we provide a brief introduction to the security analysis of QKD in which we show under which assumptions a QKD protocol is secure. An overview of security proofs, including background information, can be found in Ref. [32]. For a security analysis of CV-QKD, see Ref. [53] and Ref. [34]. A mathematical treatment using recent information-theoretical tools, see Ref. [26].

Every QKD security proof assumes fundamentally [32, p. 10]:

1. Quantum theory to be complete and correct.

2. Authenticated communication to be possible.

The first assumption provides us with the framework of quantum (information) theory to formulate our proof. Furthermore, it states that an adversary is only limited by physical - not technological - means. The second assumption is vital to exclude man-in-the-middle attacks from an adversary. It can be practical implemented using MACs, for a security proof of Wegman-Carter-Shoup-type authenticators, see Ref. [67]. Most security proofs further assume ideal implementation [26, p. 124]:

1. Isolation of the transmitter and receiver from the adversary.

2. Perfect quantum state preparation and measurement.

3. True randomness in the state and bases selection.

4. Perfect timing and synchronization of the transmitter and receiver.

5. Post-processing protocols are secure and work as intended.

After establishing the security proof of the ideal protocol implementation, we can discuss side-channel attacks originating from imperfect implementations separately. For example, Ref. [68, p. 8] discusses attacks due to hardware imperfections, Ref. [33] analysis the security of a practical post-processing pipeline for BB84, and Ref. [63] gives a security proof of privacy amplification in the context of QKD.

So far, we have been rather vague about the notion of security. In particular, we need to parametrize the security of a key as there is no strict security. For example, consider the security of a binary key of length n. The probability for an adversary to guess the correct key is $\varepsilon = 2^{-n}$. Such a brute-force attack marks the absolute floor of a key's security which we refer to as ε-secure.

More formally, we define an ϵ-secure key obtained by a QKD protocol to satisfy [32, p. 10]

$$\frac{1}{2}\|\rho_{AE} - \rho_U \otimes \rho_E\|_{\mathrm{Tr}} \leq \varepsilon \tag{1.5.1}$$

where ρ_{AE} is the quantum state encoding the correlations between Alice's final key[9] and Eve, ρ_U is the mixed state of possible key configurations, ρ_E is a generic state of Eve, and $\|\cdot\|_{\mathrm{Tr}}$ is the trace norm which measures the distance between quantum states, see Ref. [26, p. 49]. Intuitively Equation (1.5.1) encodes the distance between an ideal key state $\rho_U \otimes \rho_E$ and a real key state ρ_{AE}. The real key state ρ_{AE} may be entangled with Eve's system while for the ideal key state, Eve's state ρ_E factorizes as a tensor product with the key state ρ_U, i.e., ρ_E and ρ_U describe independent systems. Further definitions with respect to security, for instance, ϵ-correctness, -robustness, and composability, are formalized in Ref. [26, p. 119]. Additionally, one classifies Eve's eavesdropping strategies according to how her ancillas interact with the states Alice sends and whether she performs a local or global measurement of her ancillas, see Table 1.10. Sometimes it is possible to reduce coherent attacks, the most

Attack	Alice's State	Eve's Unitary	Eve's Measurement
Individual	ρ_A^j	Local	Local
Collective	ρ_A^j	Local	Global
Coherent	$\bigotimes_{j=1}^n \rho_A^j$	Global	Global

Table 1.10.: Summary of Eve's attacks according to Ref. [26, p. 128]. Alice sends n quantum states $\rho_A^1, \ldots, \rho_A^n$ to Bob. For the individual attack, Eve attaches a single ancilla system to each of Alice's states ρ_A^j, applies a local unitary transformation and performs a separate measurement. The collective attack generalizes the individual attack by Eve performing a global measurement of all ancillas. For the coherent attack, Eve interacts with all of Alice's states $\bigotimes_{j=1}^n \rho_A^j$ at once and performs a single global measurement.

powerful attacks, to collective attacks, see the de Finetti theorem [26, p. 148].

One approach for a security proof is to derive an inequality of the form [32, p. 11]

$$\mathbb{P}\left[\frac{1}{2}\|\rho_{AE} - \rho_U \otimes \rho_E\|_{\mathrm{Tr}} \leq \varepsilon\right] \lesssim e^{l - F(\rho_{AE}, \varepsilon)} \tag{1.5.2}$$

where l is the secret-key length and F is the reference scale of the secret-key length. The reference scale F of the secret-key length depends on the protocol and channel parameters, for instance, Figure 1.22 shows the estimated secret-key rate for our CV-QKD protocol given different shot-noise levels. For secure key generation, the secret key length must be chosen smaller than the secret key length reference scale, i.e., $l \ll F$. In another approach, the

[9] It is sufficient to only consider Alice's state as Bob's shares the exact same state after post-processing.

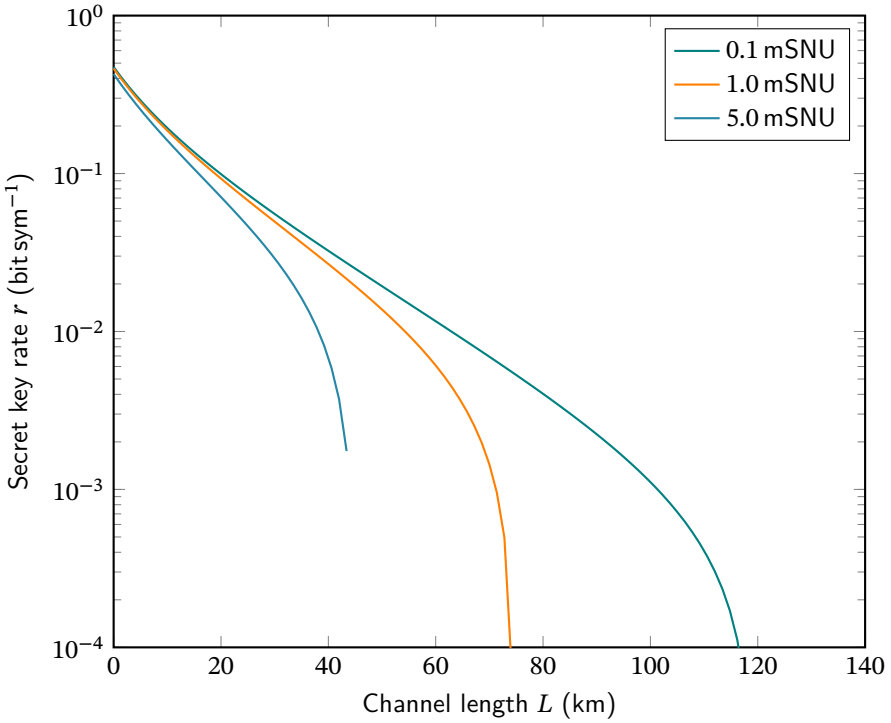


Figure 1.22.: Estimated minimum secret key rate for our CV-QKD protocol as a function of the channel length for different values of excess noise.

Devetak-Winter rate [26, p. 144] is derived. The Devetak-Winter rate provides a lower bound on the asymptotic secret key rate

$$r_{\text{sec}} \lesssim r_{\text{raw}}(I_{AB} - \chi_{BE}) \tag{1.5.3}$$

wherein r_{raw} is the raw transmission rate, I_{AB} is the mutual information between Alice and Bob, and χ_{BE} is the Holevo information encoding Eve's information on Bob's measurements.

A systematic approach to security proofs, first pioneered by Lo and Chau [69] and later extended by Shor [70], includes the following steps:

1. Convert the prepare-and-measure to an entanglement-based description.[10]

2. Employ quantum error correction codes to correct Alice's and Bob's qubits which then equals the secret key state.

3. Show equivalence of classical with quantum post-processing.

[10] If the protocol is entanglement-based, we can skip this step. For an equivalence proof of the BB84, see Ref. [26, p. 106].

Summary

We introduced QKD as an example of quantum-optical communication and a mechanism for practical and secure key-distribution, which, together with classical symmetric ciphers, enables secure communication, including means to estimate information leakage. To keep track of the diversity of QKD protocols, we restricted our treatment to CV-QKD and CV-QKD protocols. In an attempt to formalize the notion of CV-QKD and CV-QKD, we proposed the concept of logical and encoding quantum system, which suggests itself, when comparing theoretical with practical QKD transmission systems as illustrated in Figure 1.23. The idea

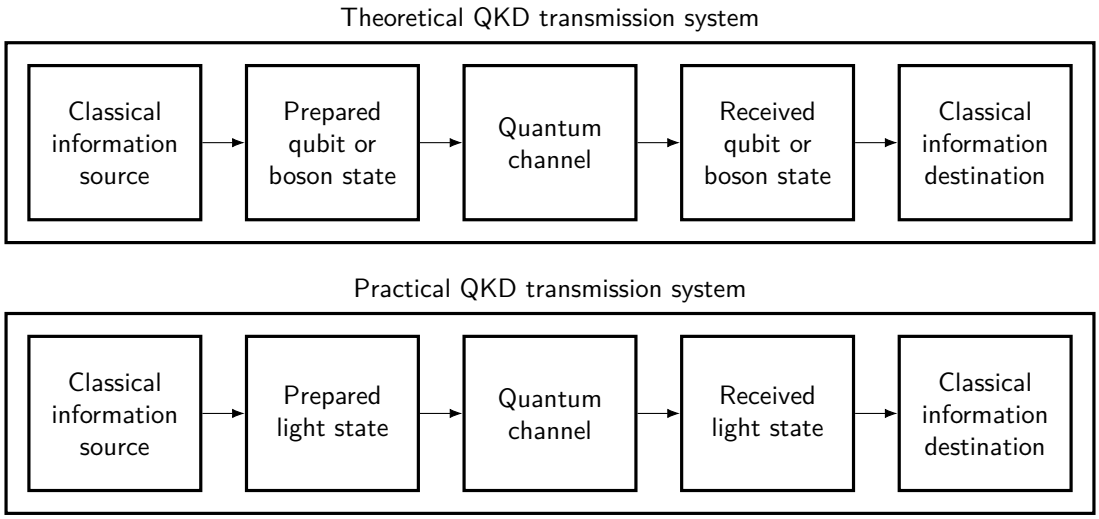


Figure 1.23.: Block diagram comparing a theoretical with a practical QKD transmission system. The theoretical QKD transmission system comprises a classical information source, a prepared qubit or boson state, a quantum channel, a received qubit or boson state, and a classical information source. Compared to the theoretical QKD transmission system, the practical QKD transmission system prepares and receives a light instead of a qubit or boson state.

here is that from an idealistic viewpoint, we encode classical information into a qubit or boson state, while for any practical implementation, we use light states for encoding. Table 1.11 summarizes the differences between qubit- and boson-based QKD for which discussed particular encoding schemes like the time-phase-encoding BB84 for qubit-based QKD or the coherent-encoding GG02 for boson-based QKD. Although security has been proven individually for theoretical and practical QKD protocols, the larger Hilbert space of light makes a unitary mapping between qubit or boson states and light states problematic [71], requiring further investigations. The technological maturity of coherent communication makes it highly practical to implement qubit- and boson-based using weak coherent states. However, the concept of a coherent-state transmission system opens up a new gap between theory and practice. While quantum information theory assumes the coherent states to be independent,

	Qubit-based	Boson-based
Visualization	Bloch sphere	Phase space
Hilbert space (dim)	Finite (two)	Countable (infinite)
Measurement operator	$\hat{\mathbf{S}}(\mathbf{n}) = \hat{S}_i n^i$	$\hat{X}(\vartheta) = \frac{1}{\sqrt{2}}\left(\hat{a}e^{-i\vartheta} + \hat{a}^\dagger e^{+i\vartheta}\right)$
Standard basis	$\{\|0\rangle, \|1\rangle\}$	$\{\|x\rangle, \|p\rangle : \ x, p \in \mathbb{R}\}$

Table 1.11.: Comparison of qubit- and boson-based QKD protocols.

i.e., the transmission sequence involves a tensor-product of (bosonic) coherent states, do we know from communication engineering that we need to consider continuously-modulated coherent states. In any case, we have shown that practical QKD implementations are very different from their original theoretical protocol, demanding an abstraction for these encoding details.

Back to our general treatment of QKD, we compiled classical methods to distill a shared secret-key between the transmitter and receiver, known as classical post-processing, from the quantum-transmission data. The classical post-processing maps the discrete or continuous data from the transmission sequence to binary symbols, corrects errors, discards failed data blocks, and removes information from the partially secret-key using privacy amplification. Finally, we roughly outlined some ideas for the security analysis of QKD.

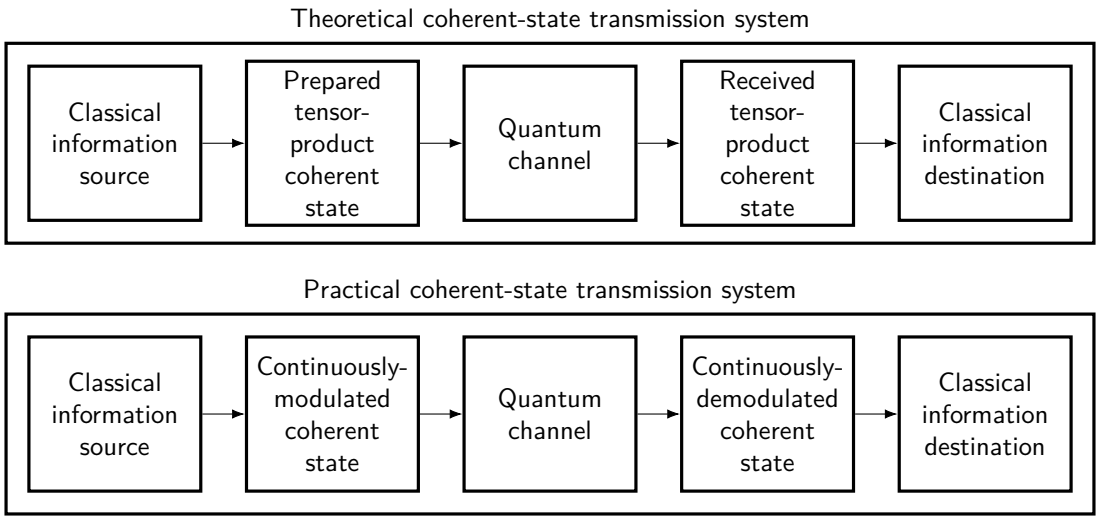


Figure 1.24.: Block diagram comparing a theoretical with a practical coherent-state transmission system. The theoretical coherent-state transmission system comprises a classical information source, a prepared tensor-product coherent state, a quantum channel, a received tensor-product coherent state, and a classical information source. Compared to the theoretical coherent-state transmission system, the practical coherent-state transmission system continuously-modulates and -demodulates a (continuous-time) coherent state.

Chapter 2.

Quantum theory of light

As stated in the introduction, a continuous-mode quantum theory of light is essential to describe time-continuous information-bearing signals. However, single-mode quantum optics [5, 4, 18, 72], the most established physical theory for describing quantum aspects of light, strictly assumes monochromatic, i.e., time-independent, light. The few references [10, 9] presenting a continuous-mode quantum theory of light are sparse on the justification or origin of their results, making the results overall difficult to assess. On the other hand, in quantum field theory, we find a description of light with a continuous momentum distribution but towards scattering experiments [13, 12, 11, 2].

In the following chapter, we derive a continuous-mode quantum theory of light rooted in quantum-field theory, which acts as the foundation of our theoretical framework. In the first part, we recap the classical description of the Maxwell field, which we quantize canonically in the last step to derive the relevant quantum field operators. In the second part, we axiomatically motivate the more general quantum states of the Maxwell field and discuss some of their properties.

2.1. Maxwell theory

The Maxwell field is the quantm field whose excitations correspond to photons, the mediators of the electromagnetic force. Our presentation of the Maxwell field heavily exploits the modern field-theoretic arguments that have shown great success in developing the standard model. First, we motivate the Maxwell Lagrangian from which we derive the equation(s) of motions (EOMs) encoding the field dynamics. Second, we relate the Maxwell field to the electromagnetic field components and discuss Maxwell theory in the context of classical electromagnetism. Third, we discuss and interpret the physical implications of the gauge symmetry of the Maxwell field. In the last two sections, we perform a plane-wave expansion of the Maxwell field and observables, followed by the canonical quantization in the

Coulomb gauge.

2.1.1. Maxwell Lagrangian

From a theoretical-physics viewpoint, Maxwell theory is a relativistic vector field theory with gauge symmetry. That alone is sufficient to "guess" the Maxwell Lagrangian from first principles [12, p. 149]. Having established the Maxwell Lagrangian, we can fully infer the physics of electromagnetism inside the field-theoretical framework.

As a relativistic vector field, we expect the Maxwell field A^μ to have four components, one time and three spatial components, and to transform as a Lorentz vector [2, p. 37]

$$A^\mu(x) \to A'^\mu(x') = \Lambda^\mu_\nu A^\nu(\Lambda^{-1}x). \tag{2.1.1}$$

Contracting Lorentz vectors, or in general Lorentz tensors, to a scalar yields a Lorentz-invariant quantity. Exclusively using Lorentz invariant quantities when constructing our theory ensures the compatibility of our theory with special relativity.

As a starting point for our theory's the Lagrangian (density), we propose

$$\mathcal{L} = c_1 \left(\partial_\mu A^\nu\right)\left(\partial^\mu A_\nu\right) + c_2 \left(\partial_\mu A^\mu\right)\left(\partial_\nu A^\nu\right) + c_3 \left(\partial_\mu A^\nu\right)\left(\partial_\nu A^\mu\right) + c_4 m^2 A_\mu A^\mu, \tag{2.1.2}$$

wherein we restricted ourselves to terms which allow for dimensionless coefficients $c1, c2, c3, c4 \in \mathbb{R}$, a mass term, and no (self-)interactions.[1] For the action integral

$$S = \int \mathrm{d}t\, L = \int \mathrm{d}^4x\, \mathcal{L} \tag{2.1.3}$$

to exist, we need A^μ to be square-integrable, i.e., vanish at the integration boundaries. The second and third term in eq. (2.1.2) are redundant [73], e.g.,

$$\begin{aligned}\int \mathrm{d}^4x \left(\partial_\mu A^\nu\right)\left(\partial_\nu A^\mu\right) &= -\int \mathrm{d}^4x\, A^\nu \left(\partial_\mu \partial_\nu A^\mu\right) \\ &= -\int \mathrm{d}^4x\, A^\nu \left(\partial_\nu \partial_\mu A^\mu\right) \\ &= \int \mathrm{d}^4x \left(\partial_\nu A^\nu\right)\left(\partial_\mu A^\mu\right),\end{aligned} \tag{2.1.4}$$

where we used partial integration with vanishing boundaries twice and commutation of the partial derivatives. To remove the redundancy, we set the third coefficient to zero, $c_3 = 0$. Demanding invariance under gauge transformations, i.e.,

$$A_\mu \to A'_\mu = A_\mu + \partial_\mu \chi, \tag{2.1.5}$$

[1] The restriction to dimensionless coefficients can be further motivated by renormalization arguments.

wherein χ is the scalar gauge field, requires removing the mass term and determining the Lagrangian up to an overall constant. The overall constant does not affect the dynamics, and its absolute value is equal to 1/2 by convention. We finally arrive at the well-known Lagrangian density of the Maxwell field,

$$\mathcal{L} = -\frac{1}{2}\left(\partial_\mu A^\nu\right)\left(\partial^\mu A_\nu\right) + \frac{1}{2}\left(\partial_\mu A^\mu\right)\left(\partial_\nu A^\nu\right). \tag{2.1.6}$$

While we can experimentally verify the vector nature of the Maxwell field by polarization experiments, the requirement of the Maxwell field having gauge symmetry appears artificial. If we accept the Dirac Lagrangian, describing charged fermions, then Noether's theorem links gauge symmetry to charge conservation. However, the Dirac Lagrangian itself cannot be made gauge-invariant without coupling to a gauge-invariant vector field, which turns out to be the Maxwell field. The complete gauge-invariant Lagrangian describing charged fermions coupled to the Maxwell field lays down the foundation of quantum electrodynamics (QED).

2.1.2. Electromagnetism

We have introduced the Maxwell field as the fundamental mediator of the electromagnetic force. However, so far, it is unclear how the electromagnetic field components relate to the Maxwell field. The manifest-covariant formulation makes it particularly difficult to identify the non-covariant electromagnetic vector fields. To shed some light, we first derive the covariant Lorentz force law and then compare it to the non-covariant vector formulation to identify the electromagnetic field components.

To derive the covariant Lorentz force law, let us consider the action of a point particle with mass m and charge q coupled to the Maxwell field A^μ [74, p. 244]

$$S = -m\int \mathrm{d}\tau \sqrt{-g_{\mu\nu}\frac{\mathrm{d}x^\mu}{\mathrm{d}\tau}\frac{\mathrm{d}x^\nu}{\mathrm{d}\tau}} + q\int \mathrm{d}\tau\, A_\mu\left(x(\tau)\right)\frac{\mathrm{d}x^\mu}{\mathrm{d}\tau} \tag{2.1.7}$$

wherein $g_{\mu\nu}$ is the Minkowski metric. The first term is the generalization of a line integral, parametrized by τ, to Minkowski spacetime. The second term describes the coordinate-dependent coupling of the Maxwell field with the charge of the particle. Invoking the variational calculus on the action, we recover the covariant formulation of Lorentz force law

$$m\frac{\mathrm{d}^2 x^\mu}{\mathrm{d}\tau^2} = qF^\mu_\nu(x)\frac{\mathrm{d}x^\nu}{\mathrm{d}\tau} \tag{2.1.8}$$

where we introduced the asymmetric field-strength tensor

$$F_{\mu\nu} = \partial_\mu A_\nu - \partial_\nu A_\mu. \tag{2.1.9}$$

The field-strength tensor covariantly encodes the electromagnetic field components.

Using the field-strength tensor $F_{\mu\nu}$ and including the interaction of the Maxwell field with an external classical current j^μ, we can rewrite the Maxwell Lagrangian of eq. (2.1.6) as

$$\mathcal{L} = -\frac{1}{4}F_{\mu\nu}F^{\mu\nu} + A_\mu j^\mu. \tag{2.1.10}$$

We note that the action of the interaction term in eq. (2.1.10) reduces to the second action term in eq. (2.1.7) when using the current of a point particle with charge q [2, p. 177]

$$j^\mu(x) = q\int \mathrm{d}\tau\, \frac{\mathrm{d}y^\mu(\tau)}{\mathrm{d}\tau}\delta^{(4)}\left(x - y(\tau)\right). \tag{2.1.11}$$

Comparison of the covariant Lorentz force law, eq. (2.1.8), with the non-covariant version

$$m\frac{\mathrm{d}^2\mathbf{x}}{\mathrm{d}t^2} = q\left(\mathbf{E} + \frac{\mathrm{d}\mathbf{x}}{\mathrm{d}t} \times \mathbf{B}\right), \tag{2.1.12}$$

we can relate the components of the field-strength tensor and the electromagnetic field [74, p. 245]

$$E^1 = F^{01} = -F_{01} \qquad E^2 = F^{02} = -F_{02} \qquad E^3 = F^{03} = -F_{03} \tag{2.1.13}$$

$$B^1 = F^{23} = -F_{23} \qquad B^2 = F^{31} = -F_{31} \qquad B^3 = F^{12} = -F_{12}, \tag{2.1.14}$$

which we can compactly summarize. [11, p. 336]

$$F^{0i} = E^i \qquad\qquad F^{ij} = \varepsilon^{ijk}B_k. \tag{2.1.15}$$

We have successfully related the rather abstract Maxwell field with the observable electromagnetic field components using the covariant field-strength tensor.

In a final step, we would like to express the Maxwell Lagrangian in terms of the electromagnetic fields to complete the bridge to classical electrodynamics. Using eq. (2.1.15), we can derive the identity [12, p. 142]

$$F_{\mu\nu}F^{\mu\nu} = -2\left(\mathbf{E}^2 - \mathbf{B}^2\right). \tag{2.1.16}$$

Inserting eq. (2.1.16) into eq. (2.1.10) we find the Maxwell Lagrangian as reported in many books on classical electrodynamics

$$\mathcal{L} = \frac{1}{2}\left(\mathbf{E}^2 - \mathbf{B}^2\right) + A_0 j^0 - \mathbf{A}\cdot\mathbf{j} \tag{2.1.17}$$

where we expanded the Minkowski inner product $A_\mu j^\mu$ in terms of the time and spatial components. We identify j^0 as the charge and $\mathbf{j}$ as the current density as well as A_0 as the scalar and $\mathbf{A}$ as the vector potential of electromagnetism.

The manifest Lorentz-covariant Maxwell equations are [11, p. 336]

$$\partial_\mu \tilde{F}^{\mu\nu} = 0 \tag{2.1.18}$$

$$\partial_\mu F^{\mu\nu} = j^\mu \tag{2.1.19}$$

where we defined the dual field-strength tensor [12, p. 142]

$$\tilde{F}^{\mu\nu} = \frac{1}{2}\varepsilon^{\mu\nu\rho\sigma}F_{\rho\sigma} \tag{2.1.20}$$

with $\varepsilon^{\mu\nu\rho\sigma}$ being the completely antisymmetric tensor. Equation (2.1.18) summarizes the homogeneous Maxwell equations and can be derived from the Bianchi identity. Equation (2.1.19) summarizes the inhomogeneous Maxwell equations and follows from the variational calculus of the Maxwell Lagrangian, i.e., represents the Maxwell field's EOMs. Evaluating the non-zero components of the Lorentz tensor equations and inserting the relation of the field-strength to the electromagnetic field, eq. (2.1.15), we arrive at the microscopic Maxwell equations

$$\boldsymbol{\nabla}\cdot\mathbf{E} = j_0 \qquad \boldsymbol{\nabla}\cdot\mathbf{B} = 0 \tag{2.1.21}$$

$$\boldsymbol{\nabla}\times\mathbf{E} = -\partial_t\mathbf{B} \qquad \boldsymbol{\nabla}\times\mathbf{B} = \mathbf{j} + \partial_t\mathbf{E}. \tag{2.1.22}$$

We derived Maxwell equations by guessing the Maxwell Lagrangian from fundamental principles and symmetries, whereas historically, Maxwell equations summarized decades of experiments studying the electromagnetic field.

2.1.3. Gauge conditions

As a four-dimensional vector field, we would expect the Maxwell field A^μ to have four degrees of freedoms (DOFs), one temporal A^0, one longitudinal $A_\parallel$, and two transverse $\mathbf{A}_\perp$. At the same time, freely propagating electromagnetic waves have only two DOFs, the polarization.[2] The zero mass of the photon requires the photon to travel at light speed, restricting the photon's temporal and longitudinal DOF. Gauge symmetry reflects the non-physicality, more precisely, the mathematical redundancy of two of the four DOFs. To remove the unphysical DOFs, we impose a gauge condition, i.e., we choose a specific gauge field χ and perform a gauge transformation

$$A_\mu \to A'_\mu = A_\mu + \partial_\mu\chi \tag{2.1.23}$$

to remove some components of the Maxwell field. Different gauge conditions exist, see Ref. [12, p. 144] and Ref. [11, p. 339], and some gauges may be more convenient than others depending on the problem under consideration. For instance, the Lorenz gauge

$$\partial_\mu A^\mu = 0 \tag{2.1.24}$$

has the advantage of being manifestly Lorentz covariant at the cost of having the different DOFs intertwined to be independent of a particular reference frame. The Coulomb gauge

$$\partial_i A^i = \boldsymbol{\nabla}\cdot\mathbf{A} = 0 \tag{2.1.25}$$

[2] Alternatively, we can take the particle picture and say that the photon has two helicities, ± 1.

corresponds to selecting a stationary reference frame in which the electromagnetic radiation is purely transverse [15, p. 40]. Imposing the Coulomb gauge only removes one DOF from the Maxwell field. We use the remaining residual gauge freedom to impose the temporal gauge

$$A_0 = 0. \tag{2.1.26}$$

The temporal gauge is valid when there is no charge distribution, $j_0 = 0$. Static charge distributions add a Coulomb interaction that does not involve the exchange of physical photons and is not subject to quantization. However, static charges add constant energy to the system and a longitudinal component to the electric field. In most cases, it is sufficient to discuss the effects of the Coulomb interaction separately from the radiation, justifying the temporal gauge. See Ref. [12, p. 145, 187, 200] for more detail on the Coulomb interaction and the Maxwell field's longitudinal DOF.

2.1.4. Plane-wave expansion

The next step is to find a general solution to the free EOM, eq. (2.1.19), which in the Coulomb and temporal gauge reduces to the relativistic wave equation

$$\partial_t^2 \mathbf{A}_\perp = \boldsymbol{\nabla}^2 \mathbf{A}_\perp \tag{2.1.27}$$

wherein $\mathbf{A}_\perp$ denotes the transverse Maxwell field. From now on, we drop the subscript and assume the Maxwell field to be transverse, i.e., to satisfy the Coulomb gauge condition, eq. (2.1.25). The existence of the Maxwell action requires the Maxwell field to be square-integrable which implies the existence of the Fourier expansion

$$\mathbf{A}(t, \mathbf{x}) = \int \frac{\mathrm{d}^3 p}{(2\pi)^3} \mathbf{A}(t, \mathbf{p}) e^{+i\mathbf{p}\cdot\mathbf{x}} = \int \frac{\mathrm{d}^4 p}{(2\pi)^4} \mathbf{A}(p_0, \mathbf{p}) e^{-ip_0 t + i\mathbf{p}\cdot\mathbf{x}} \tag{2.1.28}$$

with $\mathbf{A}(p_0, \mathbf{p})$ being the complex-valued Fourier vector amplitudes. Inserting the Maxwell field's Fourier expansion, eq. (2.1.28), into the relativistic wave equation, eq. (2.1.27), reduces the EOM in momentum space to

$$0 = p_0^2 - \mathbf{p}^2 = (p_0 - \|\mathbf{p}\|)(p_0 + \|\mathbf{p}\|). \tag{2.1.29}$$

Requiring the energy to be positive, $p_0 > 0$, we arrive at the relativistic energy-momentum relation

$$p_0 = \omega(\mathbf{p}) = \|\mathbf{p}\| \tag{2.1.30}$$

for massless particles. Fourier amplitudes satisfying the relativistic-energy momentum relation are plane-wave solutions to the Maxwell field's free EOM. We define the plane-wave expansion as the Fourier expansion, eq. (2.1.28), where we constrain the integration domain to

$$\Sigma = \left\{(p_0, \mathbf{p}) \in \mathbb{R}^4 : \; p_0^2 = \omega(\mathbf{p})^2\right\}.$$

Each plane-wave is a solution to the free EOM and the plane-wave expansion denotes a general solution. We can extend the integration domain of the plane-wave expansion back to the $\mathbb{R}^4$ by having the delta distribution ensure the relativistic energy-momentum relation

$$\begin{aligned}\mathbf{A}(t,\mathbf{x}) &= \int_{\Sigma} \frac{\mathrm{d}^4 p}{(2\pi)^4} \mathbf{A}(p_0,\mathbf{p}) e^{-ip_\mu x^\mu} \\ &= \int_{\mathbb{R}^4} \frac{\mathrm{d}^4 p}{(2\pi)^3} \delta^{(1)}\left(p_0^2 - \omega(\mathbf{p})^2\right) \mathbf{A}(p_0,\mathbf{p}) e^{-ip_\mu x^\mu}.\end{aligned} \tag{2.1.31}$$

Exploiting the composition property of the delta distribution,

$$\delta^{(1)}\left(p_0^2 - \omega(\mathbf{p})^2\right) = \frac{\delta^{(1)}\left(p_0 - \omega(\mathbf{p})\right) + \delta^{(1)}\left(p_0 + \omega(\mathbf{p})\right)}{\sqrt{2\omega(\mathbf{p})}}, \tag{2.1.32}$$

we further decompose the plane-wave expansion into a positive and negative frequency part

$$\begin{aligned}\mathbf{A}(t,\mathbf{x}) &= \int \frac{\mathrm{d}^4 p}{(2\pi)^3\sqrt{2\omega(\mathbf{p})}} \delta^{(1)}\left(p_0 - \omega(\mathbf{p})\right) \mathbf{A}(p_0,\mathbf{p}) e^{-ip_0 t + i\mathbf{p}\cdot\mathbf{x}} \\ &\quad + \int \frac{\mathrm{d}^4 p}{(2\pi)^3\sqrt{2\omega(\mathbf{p})}} \delta^{(1)}\left(p_0 + \omega(\mathbf{p})\right) \mathbf{A}(p_0,\mathbf{p}) e^{-ip_0 t + i\mathbf{p}\cdot\mathbf{x}} \\ &= \int \frac{\mathrm{d}^3 p}{(2\pi)^3\sqrt{2\omega(\mathbf{p})}} \mathbf{A}\left(\omega(\mathbf{p}),\mathbf{p}\right) e^{-i\omega(\mathbf{p})t + i\mathbf{p}\cdot\mathbf{x}} \\ &\quad + \int \frac{\mathrm{d}^3 p}{(2\pi)^3\sqrt{2\omega(\mathbf{p})}} \mathbf{A}\left(-\omega(\mathbf{p}),\mathbf{p}\right) e^{+i\omega(\mathbf{p})t + i\mathbf{p}\cdot\mathbf{x}} \\ &= \int \frac{\mathrm{d}^3 p}{(2\pi)^3\sqrt{2\omega(\mathbf{p})}} \mathbf{A}\left(\omega(\mathbf{p}),\mathbf{p}\right) e^{-i\omega(\mathbf{p})t + i\mathbf{p}\cdot\mathbf{x}} \\ &\quad + \int \frac{\mathrm{d}^3 p}{(2\pi)^3\sqrt{2\omega(\mathbf{p})}} \mathbf{A}\left(\omega(\mathbf{p}),\mathbf{p}\right)^* e^{+i\omega(\mathbf{p})t - i\mathbf{p}\cdot\mathbf{x}}.\end{aligned} \tag{2.1.33}$$

To arrive at eq. (2.1.33), we evaluated the delta distributions, performed the variable substitution $\mathbf{p} \to -\mathbf{p}$ in the second term and used the conjugate symmetry of the Maxwell field in momentum space, $A(-p_0,-\mathbf{p}) = A(p_0,\mathbf{p})^*$. The Maxwell field being transverse implies the momentum vector $\mathbf{p}$ being orthogonal to the Fourier amplitude,

$$\mathbf{p}\cdot\mathbf{A}\left(\omega(\mathbf{p}),\mathbf{p}\right) = 0. \tag{2.1.34}$$

We construct a orthonormal basis $\{\hat{\mathbf{e}}_\lambda\}_{\lambda=1,2}$ for each momentum vector $\mathbf{p}$, the polarization basis to momentum $\mathbf{p}$, which is orthogonal to the momentum $\mathbf{p}$ and complete [11, p. 341], i.e.,

$$\mathbf{p}\cdot\hat{\mathbf{e}}_\lambda(\mathbf{p}) = 0 \tag{2.1.35}$$

$$\hat{\mathbf{e}}_\lambda(\mathbf{p})\cdot\hat{\mathbf{e}}_{\lambda'}(\mathbf{p}) = \delta_{\lambda,\lambda'} \tag{2.1.36}$$

$$\sum_{\lambda=1,2} \hat{\mathbf{e}}_\lambda(\mathbf{p})^i \hat{\mathbf{e}}_\lambda(\mathbf{p})^j = \delta^{ij} - \frac{p^i p^j}{\mathbf{p}^2}. \tag{2.1.37}$$

Writing the Fourier vector amplitude in terms of the polarization basis

$$\mathbf{A}\left(\omega(\mathbf{p}), \mathbf{p}\right) = \sum_{\lambda=1,2} a_\lambda(\mathbf{p})\hat{\mathbf{e}}_\lambda(\mathbf{p}) \tag{2.1.38}$$

and inserting it back into the plane-wave expansion, eq. (2.1.33), we arrive at our final result

$$\mathbf{A}(t, \mathbf{x}) = \sum_{\lambda=1,2} \int \frac{\mathrm{d}^3 p}{(2\pi)^3\sqrt{2\omega(\mathbf{p})}} \left\{a_\lambda(\mathbf{p})\hat{\mathbf{e}}_\lambda(\mathbf{p})e^{-i\omega(\mathbf{p})t + i\mathbf{p}\cdot\mathbf{x}} + \text{c.c.}\right\} \tag{2.1.39}$$

The plane-wave expansion looks already similar to the quantum mode expansion of the Maxwell field but relies only on classical arguments.[3] In principle, we could stop here, replace the Fourier modes with the annihilation operator satisfying the canonical commutation relation (CCR), and we have quantized our field.[4] However, for completeness, we review the standard canonical quantization of the Maxwell field in the next section.

2.1.5. Canonical quantization

In canonical quantization, we work in the Hamiltonian picture, promoting the conjugate variables with operators that satisfy the equal-time commutation relation (ETCR). In the canonical quantization of gauge theories, like the Maxwell field, we have the additional technical complication of handling the unphysical DOFs. In the Coulomb gauge, we can take care of the transverse gauge condition by amending the equal-time commutation relations to be transverse, more to that later. In the Lorenz gauge, the Gupta-Bleuler method includes the unphysical DOF in the quantization process but removes them later by constraining the state space, see Ref. [12, p. 180].

Before performing the canonical quantization, we need to find the conjugate field variables and Hamiltonian (density). The conjugate momentum to the Maxwell field A_i is [11, p. 342]

$$\Pi_i = \frac{\partial \mathcal{L}}{\partial(\partial_t A_i)} = -\partial_t A^i = \partial_t A_i \tag{2.1.40}$$

where the sign change occurs due to the spatial components of the Minkowski metric when lowering a spatial index, $A^i = g^{ij}A_j = -\delta^{ij}A_j = -A_j$. In the Coulomb gauge, the electric field components are equal to the negative conjugate momentum components, i.e.,

$$E^i = F^{0i} = \partial_t A^i = -\Pi^i \tag{2.1.41}$$

where we used eq. (2.1.15) and the temporal gauge, $A^0 = 0$.[5] In the following, we replace the conjugate momentum with the electric field components, $\Pi^i = -E^i$. The Hamiltonian

[3] The similarity is not surprising if we consider $A(t, \mathbf{x})$ as the expectation value of the Maxwell field operator given a coherent state, $\langle\alpha|\hat{\mathbf{A}}(t, \mathbf{x})|\alpha\rangle$.

[4] The equivalence of Fourier and quantum modes has been experimentally established, see Ref. [75].

[5] We may not always explicitly write that we use the temporal gauge, $A^0 = 0$.

density of the Maxwell field is equal to

$$\mathcal{H} = \frac{1}{2}E_i E^i + \frac{1}{2}\partial_i A_j \partial^j A^i \tag{2.1.42}$$

and can be found by Legendre transform of the Lagrangian density [11, p. 342] or using the energy density component from the energy-momentum tensor [12, p. 148].

We now perform the canonical quantization by replacing the dynamical field variables $A_i, -E_i$ with the field operators $\hat{A}_i, -\hat{E}_i$ satisfying the ETCR [12, p. 197]

$$[\hat{A}_i(t,\mathbf{x}), \hat{E}_j(t,\mathbf{y})] = -i\delta^{(3)}_{\perp ij}(\mathbf{x}-\mathbf{y}) \tag{2.1.43}$$

$$[\hat{A}_i(t,\mathbf{x}), \hat{A}_j(t,\mathbf{y})] = [\hat{E}_i(t,\mathbf{x}), \hat{E}_j(t,\mathbf{y})] = 0 \tag{2.1.44}$$

where we adapted the transverse delta distribution [12, p. 198]

$$\delta^{(3)}_{\perp ij}(\mathbf{x}) = \left(\delta_{ij} - \frac{\partial_i\partial_j}{\partial^2}\right)\delta^{(3)}(\mathbf{x}) = \int \frac{\mathrm{d}^3 p}{(2\pi)^3}\left(\delta_{ij} - \frac{p_i p_j}{\mathbf{p}^2}\right)e^{i\mathbf{p}\cdot\mathbf{x}} \tag{2.1.45}$$

which implements the Coulomb gauge on the operator level.

Replacing the Fourier amplitudes, $a_\lambda(\mathbf{p})$ and $a_\lambda(\mathbf{p})^*$ in the plane-wave expansion of the Maxwell field with the annihilation operators $\hat{a}_\lambda(\mathbf{p})$ and the creation operator $\hat{a}^\dagger_\lambda(\mathbf{p})$, we find the Maxwell field operator to be

$$\hat{\mathbf{A}}(t,\mathbf{x}) = \hat{\mathbf{A}}^{(-)}(t,\mathbf{x}) + \hat{\mathbf{A}}^{(+)}(t,\mathbf{x}) \tag{2.1.46}$$

where we defined the positive and negative frequency parts to be

$$\hat{\mathbf{A}}^{(-)}(t,\mathbf{x}) = \sum_{\lambda=1,2}\int \frac{\mathrm{d}^3 p}{(2\pi)^3\sqrt{2\omega(\mathbf{p})}}\hat{a}_\lambda(\mathbf{p})\hat{\mathbf{e}}_\lambda(\mathbf{p})e^{-i\omega(\mathbf{p})t+i\mathbf{p}\cdot\mathbf{x}} \tag{2.1.47}$$

$$\hat{\mathbf{A}}^{(+)}(t,\mathbf{x}) = \sum_{\lambda=1,2}\int \frac{\mathrm{d}^3 p}{(2\pi)^3\sqrt{2\omega(\mathbf{p})}}\hat{a}^\dagger_\lambda(\mathbf{p})\hat{\mathbf{e}}_\lambda(\mathbf{p})^* e^{+i\omega(\mathbf{p})t-i\mathbf{p}\cdot\mathbf{x}}. \tag{2.1.48}$$

In the literature, we find different conventions concerning the integration measure, the sign of the complex exponentials, and the complex conjugation of the of polarization basis vectors in eqs. (2.1.47) and (2.1.48) originating from different conventions for the Fourier transform. For example, Refs. [2, 12] use $\hat{a}_\lambda(\mathbf{p})e^{-i\omega(\mathbf{p})t}$ while Refs. [11, 1] use $\hat{a}_\lambda(\mathbf{p})e^{+i\omega(\mathbf{p})t}$. Analog to the Maxwell field operator, we decompose the electric field operator into a positive and negative frequency part

$$\hat{\mathbf{E}}(t,\mathbf{x}) = \hat{\mathbf{E}}^{(-)}(t,\mathbf{x}) + \hat{\mathbf{E}}^{(+)}(t,\mathbf{x}) \tag{2.1.49}$$

where we find the electric field operator components via $\hat{E}^i = \partial_t \hat{A}^i$ leading to

$$\hat{\mathbf{E}}^{(-)}(t,\mathbf{x}) = -i\sum_{\lambda=1,2}\int \frac{\mathrm{d}^3 p}{(2\pi)^3\sqrt{2\omega(\mathbf{p})}}\omega(\mathbf{p})\hat{a}_\lambda(\mathbf{p})\hat{\mathbf{e}}_\lambda(\mathbf{p})e^{-i\omega(\mathbf{p})t+i\mathbf{p}\cdot\mathbf{x}} \tag{2.1.50}$$

$$\hat{\mathbf{E}}^{(+)}(t,\mathbf{x}) = +i\sum_{\lambda=1,2}\int \frac{\mathrm{d}^3 p}{(2\pi)^3\sqrt{2\omega(\mathbf{p})}}\omega(\mathbf{p})\hat{a}^\dagger_\lambda(\mathbf{p})\hat{\mathbf{e}}_\lambda(\mathbf{p})^* e^{+i\omega(\mathbf{p})t-i\mathbf{p}\cdot\mathbf{x}}. \tag{2.1.51}$$

Inserting the Maxwell and electric field operators into the equal-time commutation relation, we derive the CCR

$$[\hat{a}_\lambda(\mathbf{p}), \hat{a}^\dagger_{\lambda'}(\mathbf{q})] = (2\pi)^3 \delta_{\lambda\lambda'} \delta^{(3)}(\mathbf{p}-\mathbf{q}) \tag{2.1.52}$$

$$[\hat{a}_\lambda(\mathbf{p}), \hat{a}_{\lambda'}(\mathbf{q})] = [\hat{a}^\dagger_\lambda(\mathbf{p}), \hat{a}^\dagger_{\lambda'}(\mathbf{q})] = 0. \tag{2.1.53}$$

The Maxwell field's Hamilton and momentum operator are [12, p. 199]

$$\hat{H} = \sum_{\lambda=1,2} \int \frac{\mathrm{d}^3 p}{(2\pi)^3} \omega(\mathbf{p}) \hat{a}^\dagger_\lambda(\mathbf{p}) \hat{a}_\lambda(\mathbf{p}) \tag{2.1.54}$$

$$\hat{\mathbf{P}} = \sum_{\lambda=1,2} \int \frac{\mathrm{d}^3 p}{(2\pi)^3} \mathbf{p} \hat{a}^\dagger_\lambda(\mathbf{p}) \hat{a}_\lambda(\mathbf{p}) \tag{2.1.55}$$

and can be found by inserting the Maxwell field operator into the classical definitions of energy and momentum and performing normal ordering.[6] Reading the combination of annihilation and creation operator as particle number density

$$\hat{n}_\lambda(\mathbf{p}) = \hat{a}^\dagger_\lambda(\mathbf{p}) \hat{a}_\lambda(\mathbf{p}), \tag{2.1.56}$$

the energy and momentum operators then read as the total energy $\omega(\mathbf{p})$ and momentum $\mathbf{p}$ weighted by the number density. Equation (2.1.56) suggests the total particle number operator to be

$$\hat{N} = \int \frac{\mathrm{d}^3 p}{(2\pi)^3} \hat{a}^\dagger_\lambda(\mathbf{p}) \hat{a}_\lambda(\mathbf{p}). \tag{2.1.57}$$

Unsurprisingly, total particle number and total momentum are conserved quantities

$$[\hat{H}, \hat{\mathbf{P}}] = \mathbf{0} \qquad\qquad [\hat{H}, \hat{\mathbf{N}}] = 0. \tag{2.1.58}$$

In the next section, we provide a more rigorous discussion of the particle aspects by constructing the quantum states.

2.2. Quantum states

In the previous section, we derived the relevant field operators for the Maxwell field encoding electromagnetism. In the present section, we construct quantum states from these operators in a rather axiomatic approach as done in Ref. [76, p. 506] for the quantum harmonic oscillator, or in axiomatic field theory [14, 77, 16].

To keep the arguments and notation concise, we restrict the quantum state construction to one polarization mode of the Maxwell field. The Maxwell field then effectively becomes a

[6] Normal ordering removes infinite terms like the "vacuum energy".

Klein-Gordon field with field operator

$$\hat{A}(t,\mathbf{x}) = \int \frac{\mathrm{d}^3 p}{(2\pi)^3\sqrt{2\omega(\mathbf{p})}} \left\{\hat{a}(\mathbf{p})e^{-i\omega(\mathbf{p})t+i\mathbf{p}\cdot\mathbf{x}} + \hat{a}^\dagger(\mathbf{p})e^{+i\omega(\mathbf{p})t-i\mathbf{p}\cdot\mathbf{x}}\right\} \tag{2.2.1}$$

wherein the annihilation and creation operator, $\hat{a}(\mathbf{p})$, $\hat{a}^\dagger(\mathbf{p})$, satisfy the CCR

$$[\hat{a}(\mathbf{p}), \hat{a}^\dagger(\mathbf{q})] = (2\pi)^3\delta^{(3)}(\mathbf{p}-\mathbf{q}) \tag{2.2.2}$$

$$[\hat{a}(\mathbf{p}), \hat{a}(\mathbf{q})] = [\hat{a}^\dagger(\mathbf{p}), \hat{a}^\dagger(\mathbf{q})] = 0. \tag{2.2.3}$$

To extend the results back to two polarization modes, we can construct a two-dimensional tensor product space from the single polarization mode.

2.2.1. Vacuum state

The fundamental assumption our state construction relies upon is the existence of a unique, up to a constant phase factor, vacuum state $|0\rangle$ invariant under the unitary Poincaré transformation [14, p. 97]

$$\hat{U}(a,\Lambda)|0\rangle = |0\rangle \tag{2.2.4}$$

where Λ denotes a Lorentz transformation and a a spacetime translation. The vacuum state is an element of a one-dimensional complex Hilbert space, $\mathcal{H}^{(0)} = \mathcal{H}(\mathbb{C})$, the zero-particle state space. The generator of the unitary spacetime translation is the four-momentum operator $\hat{P}^\mu = \left(\hat{H}, \hat{\mathbf{P}}\right)$ [77, p. 28]

$$\hat{U}(a) = \hat{U}(a,\mathbb{1}) = e^{i\hat{P}_\mu a^\mu}. \tag{2.2.5}$$

The invariance of the vacuum under spacetime translations, eq. (2.2.5), implies that the vacuum is a zero eigenstate to the Hamilton and momentum operator

$$\hat{H}|0\rangle = 0 \qquad\qquad \hat{\mathbf{P}}|0\rangle = |0\rangle. \tag{2.2.6}$$

From the mode expansion of the Hamilton operator, eq. (2.1.54), and the vacuum state being a zero eigenstate to the Hamilton operator, we conclude that the vacuum state is also a zero eigenstate to the annihilation operator

$$\hat{a}(\mathbf{p})|0\rangle = 0. \tag{2.2.7}$$

In the next paragraph, we motivate why we understand the annihilation and creation operators as adding or removing a particle excitation to and from the field. Under these circumstances, we can read eq. (2.2.7) as destroying the vacuum state, ensuring no negative energy or negative particle number states.

2.2.2. Particle states

The motivation of why the annihilation and creation operators add or remove a particle with energy and momentum to and from the field follows from applying the commutators of the number and momentum operator with the creation operator

$$[\hat{N}, \hat{a}^\dagger(\mathbf{p})] = \hat{a}^\dagger(\mathbf{p}) \qquad [\hat{\mathbf{P}}, \hat{a}^\dagger(\mathbf{p})] = \mathbf{p}\hat{a}^\dagger(\mathbf{p}). \tag{2.2.8}$$

Applying the vacuum state $|0\rangle$ to the right of the commutator equations, yields eigenvalue equations for the number and momentum operator

$$\hat{N}\hat{a}^\dagger(\mathbf{p})|0\rangle = 1\hat{a}^\dagger(\mathbf{p})|0\rangle \qquad \hat{\mathbf{P}}\hat{a}^\dagger(\mathbf{p})|0\rangle = \mathbf{p}\hat{a}^\dagger(\mathbf{p})|0\rangle. \tag{2.2.9}$$

The eigenvalue equations suggest

$$|\mathbf{p}\rangle = \hat{a}^\dagger(\mathbf{p})|0\rangle \tag{2.2.10}$$

to be a single-particle state with momentum $\mathbf{p}$ and energy $\omega(\mathbf{p})$, a momentum state. [2, p. 23]. Unfortunately, the inner product between two momentum states does not yield a complex number $\mathbb{C}$ but, a distribution,

$$\langle \mathbf{p}|\mathbf{q}\rangle = \langle 0|[\hat{a}(\mathbf{p}), \hat{a}^\dagger(\mathbf{q})]|0\rangle = (2\pi)^3\delta^{(3)}(\mathbf{p}-\mathbf{q}) \tag{2.2.11}$$

suggesting that something essential is missing in our description.

It makes sense to take a step back and recap some mathematical context regarding distributions.[7] One approach considers distributions as functionals, i.e., maps from a function space, e.g., the space of real-valued square-integrable functions $L^2(\mathbb{R})$, to real numbers $\mathbb{R}$. Implicitly, we already used functionals when we considered the action integral

$$\hat{S}\left[x(t)\right] = \int_{t_0}^{t_1} \mathrm{d}t\, L\left(x(t), \dot{x}(t)\right), \tag{2.2.12}$$

wherein L is some classical Lagrangian, evaluated for some finite time interval $[t_0, t_1]$ maps the trajectory $x(t)$ of a point particle to a real number $\mathbb{R}$. Often a functional A acting on a function f is written

$$A[f] = \int \mathrm{d}x\, f(x)A(x) \tag{2.2.13}$$

wherein $A(x)$ is denoted the integration kernel representing the functional, which may be an ordinary function or a distribution. For example, the delta distribution $\delta(x-y)$ is the integration kernel of the functional δ_y

$$\delta_y[f] = \int \mathrm{d}x\, f(x)\delta(x-y) = f(y). \tag{2.2.14}$$

[7] See Ref. [78, p. 590] and Ref. [54, p. 193] for a mathematical discussion of distributions in a physical context.

Fourier transforms are another class of functionals we already used frequently. Linear functionals share many convenient properties with ordinary functions and physicists often skip the distinction. In axiomatic quantum field theory, the quantum field operators are precisely defined as operator-valued tempered distributions mapping from the space of smearing or test functions $\mathcal{S}(\mathbb{R}^4)$ to the the set of operators defined on the corresponding Hilbert space $\mathcal{O}(\mathcal{H})$ [77, p. 56].[8] A typical functional space for smearing functions is the Schwartz space, a subset of the space of square-integrable functions L^2, which rapidly fall off at infinity, a property which we exploit for partial integration with vanishing boundary terms of the action integral.[9]

Let us reinterpret the positive-frequency field operator with this mathematical background by considering its action on a smearing function, i.e.,

$$\hat{A}^{(+)}[f] = \int \mathrm{d}^4x\, f(t,\mathbf{x})\hat{A}^{(+)}(t,\mathbf{x}) = \int \frac{\mathrm{d}^3p}{(2\pi)^3\sqrt{2\omega(\mathbf{p})}} f(\omega(\mathbf{p}),\mathbf{p})\,\hat{a}^\dagger(\mathbf{p}) \tag{2.2.15}$$

where we inserted the plane-wave expansion for the field and the spacetime Fourier transform for the smearing function and used the orthogonality of the Fourier modes in the second equation. Applying the smeared positive frequency field operator to the vacuum state,

$$|1_f\rangle = \hat{A}^{(+)}[f]|0\rangle, \tag{2.2.16}$$

and comparing the result to the momentum state, eq. (2.2.10), we find the function f to smear the function in momentum and spacetime space [11, p. 35].[10] The inner product of two such smeared states yields a complex number $\mathbb{C}$

$$\langle 1_f|1_g\rangle = \int \frac{\mathrm{d}^3p}{(2\pi)^3 2\omega(\mathbf{q})} f(\mathbf{p})^* g(\mathbf{p}) \tag{2.2.17}$$

implying the smeared state $|1_f\rangle$ being normalizable if we require the smearing function to satisfy

$$\langle 1_f|1_f\rangle = \int \frac{\mathrm{d}^3p}{(2\pi)^3 2\omega(\mathbf{q})} |f(\mathbf{p})|^2 = 1. \tag{2.2.18}$$

With the normalization condition imposed, the smeared state $|1_f\rangle$ is an eigenstate of the number operator to eigenvalue one

$$\hat{N}|1_f\rangle = 1|1_f\rangle \tag{2.2.19}$$

suggesting the smeared state $|1_f\rangle$ to be the physical single-particle state we were looking for. The smeared state $|1_f\rangle$ is not an eigenstate of the energy and momentum operator anymore

[8] A criticism of this approach is that the space of test functions covers only a subset of the Hilbert space.

[9] Typical Schwartz functions are Gaussian functions multiplied with a monomial, e.g., $x^n e^{-a\|x\|^2}$ where $n \in \mathbb{N}_0$ and $a \in \mathbb{R}_+$.

[10] Interestingly though, only momentum components satisfying the energy-momentum relation, eq. (2.1.30), contribute to momentum space.

but has expectation values

$$\langle 1_f|\hat{H}|1_f\rangle = \int \frac{\mathrm{d}^3 p}{(2\pi)^3}\omega(\mathbf{p})|f(\omega(\mathbf{p}),\mathbf{p})|^2 \tag{2.2.20}$$

$$\langle 1_f|\hat{\mathbf{P}}|1_f\rangle = \int \frac{\mathrm{d}^3 p}{(2\pi)^3}\mathbf{p}|f(\omega(\mathbf{p}),\mathbf{p})|^2 \tag{2.2.21}$$

suggesting that the smearing function has the physical interpretation of a frequency spectrum.

Let $|1_f\rangle$ be a smeared particle state, then the single-particle wave function providing the probability amplitude density of finding the particle at $(t,\mathbf{x})$ [2, p. 24] equals

$$\Psi(t,\mathbf{x}) = \langle 0|\hat{A}(t,\mathbf{x})|1_f\rangle = \int \mathrm{d}t'\,\mathrm{d}^3x'\,D(t-t',\mathbf{x}-\mathbf{x}')f(t',\mathbf{x}'), \tag{2.2.22}$$

wherein $f(t,\mathbf{x})$ is the spacetime representation of the (initial) smearing function and

$$D(t,\mathbf{x}) = \int \frac{\mathrm{d}^3 p}{(2\pi)^3 2\omega(\mathbf{p})}e^{-i\omega(\mathbf{p})t+i\mathbf{p}\cdot\mathbf{x}} \tag{2.2.23}$$

is the propagator as defined in Ref. [2, p. 27]. Given the single-particle wave function, the relativistic probability current

$$j_\mu(t,\mathbf{x}) = 2\,\mathrm{Im}\left\{\Psi(t,\mathbf{x})^*\partial_\mu\Psi(t,\mathbf{x})\right\} \tag{2.2.24}$$

allows us to estimate the center-of-mass position and velocity of the particle, i.e.,

$$\langle\mathbf{x}(t)\rangle = \int \mathrm{d}^3x\,\mathbf{x}\rho(t,\mathbf{x}) \qquad\qquad \langle\mathbf{v}(t)\rangle = \int \mathrm{d}^3x\,\mathbf{j}(t,\mathbf{x}) \tag{2.2.25}$$

wherein $\rho(t,\mathbf{x}) = j_0(t,\mathbf{x})$ is the relativistic probability density. For more details on the properties of relativistic wave packets, e.g., dispersion, see Ref. [79] and Ref. [80].

To summarize our findings, we first motivated momentum eigenstates from the commutation algebra. However, the momentum eigenstates are prone to mathematical inconsistencies, following that the momentum states are strictly speaking distributions, not functions. Physically, the momentum states correspond to unphysical plane-waves. A mathematical consistent single-particle state requires a momentum spectrum. The momentum spectrum encodes many important physical properties like the localization and velocity of the particle.

2.2.3. Fock space

The single-particle state defined in eq. (2.2.16) is an element of the one-particle Hilbert space of square-integrable functions defined on three-dimensional space $\mathcal{H}^{(1)} = \mathcal{H}\left(L^2(\mathbb{R}^3)\right)$. The

generalization of the one-particle Hilbert space $\mathcal{H}^{(1)}$ to an n-particle Hilbert space $\mathcal{H}^{(n)}$ is the tensor product of one-particle Hilbert spaces

$$\mathcal{H}^{(n)} = \bigotimes_{i=1}^{n} \mathcal{H}^{(1)}. \tag{2.2.26}$$

Now, it is possible to have a superposition of, e.g., the vacuum state and a particle state

$$|\psi\rangle = c_1|0\rangle + c_2|1_f\rangle \tag{2.2.27}$$

with $c_1, c_2 \in \mathbb{C}$ which means that we need to combine orthonormal n-particle states. We first construct a tensor algebra over the Hilbert space $\mathcal{H}^{(1)}$ as the direct sum [16, p. 290]

$$\bigoplus_{n=0}^{\infty} S_+ \mathcal{H}^{(n)} \tag{2.2.28}$$

wherein S_+ symmetrizes the Hilbert space for bosons. Equipping the tensor algebra with an inner product and using the completeness of the n-particle Hilbert spaces, we obtain again a Hilbert space, named the symmetric Fock space $\mathcal{F}_+$ [77, p. 35].

2.2.4. Number states

Applying the creation operator $\hat{A}^{(+)}[f]$ wherein f is a smearing function or momentum spectrum satisfying the normalization condition, eq. (2.2.18), suggests defining

$$|n_f\rangle = \frac{1}{\sqrt{n!}} \hat{A}^{(+)}[f]^n |0\rangle \tag{2.2.29}$$

as number state with spectrum f.[11] The positive and negative frequency field operators $\hat{A}^{(\pm)}(t, \mathbf{x})$ generalize the quantum harmonic annihilation and creation operators by adding or removing a particle with spectrum f from the field

$$\hat{A}^{(+)}[f]|n_f\rangle = \sqrt{n+1}|n+1_f\rangle \tag{2.2.30}$$

$$\hat{A}^{(-)}[f]|n_f\rangle = \sqrt{n}|n-1_f\rangle. \tag{2.2.31}$$

While the generalized number state $|n_f\rangle$ is still an eigenstate of the number operator to eigenvalue n_f,

$$\hat{N}|n_f\rangle = n_f|n_f\rangle, \tag{2.2.32}$$

and has energy and momentum expectation values

$$\langle n_f|\hat{H}|n_f\rangle = n \int \frac{\mathrm{d}^3 p}{(2\pi)^3} \omega(\mathbf{p}) \left| \frac{f(\omega(\mathbf{q}), \mathbf{q})}{\sqrt{2\omega(\mathbf{p})}} \right|^2 \tag{2.2.33}$$

$$\langle n_f|\hat{\mathbf{P}}|n_f\rangle = n \int \frac{\mathrm{d}^3 p}{(2\pi)^3} \mathbf{p} \left| \frac{f(\omega(\mathbf{q}), \mathbf{q})}{\sqrt{2\omega(\mathbf{p})}} \right|^2. \tag{2.2.34}$$

[11] The factorial is required for normalization because bosons are indistinguishable.

The expectation value and variance of the electric field operator are

$$\langle n_f|\hat{E}(t,\mathbf{x})|n_f\rangle = 0 \tag{2.2.35}$$

$$\langle n_f|\left(\Delta\hat{E}(t,\mathbf{x})\right)^2|n_f\rangle = \frac{1}{2}\int \frac{\mathrm{d}^3p}{(2\pi)^3}\omega(\mathbf{p}) + n|\Psi(t,\mathbf{x})|^2. \tag{2.2.36}$$

The electric field vanishes for our number states as known in quantum optics, see, for instance, Ref. [4], but the variance contains an additional term to the "vacuum fluctuations" from the momentum spectrum. The vacuum fluctuations are in principle infinite, however, our detector is only able to detect a limited bandwidth which makes the vacuum fluctuations in practical applications finite again.

2.2.5. Coherent states

The interaction of a classical current $\mathbf{j}(t,\mathbf{x})$ with the Maxwell field operator in the Coulomb gauge $\hat{\mathbf{A}}(t,\mathbf{x})$ is given by the interaction Hamiltonian

$$\hat{H}_{\mathrm{int}}(t) = -\int \mathrm{d}^3x\, \mathbf{j}(t,\mathbf{x})\cdot\hat{\mathbf{A}}(t,\mathbf{x}). \tag{2.2.37}$$

Inserting the spatial Fourier transform of the current $\mathbf{j}(t,\mathbf{p})$ and the plane-wave expansion, eqs. (2.1.47) and (2.1.48), the interaction Hamiltonian becomes

$$\hat{H}_{\mathrm{int}}(t) = -\sum_{\lambda=1,2}\int \frac{\mathrm{d}^3p}{(2\pi)^3\sqrt{2\omega(\mathbf{p})}}\left\{(\mathbf{j}(t,\mathbf{p})^*\cdot\hat{\mathbf{e}}_\lambda(\mathbf{p}))\,\hat{a}_\lambda(\mathbf{p})e^{-i\omega(\mathbf{p})t} + \mathrm{H.c.}\right\}. \tag{2.2.38}$$

where we used the conjugate symmetry $\mathbf{j}(t,\mathbf{p})^* = \mathbf{j}(t,-\mathbf{p})$.

The effect of an interaction acting on a quantum state from time t_0 to t is encoded in the time-evolution operator[12]

$$\hat{U}(t_0,t) = \mathcal{T}_+\exp\left\{-i\int_{t_0}^{t}\mathrm{d}t'\,\hat{H}_{\mathrm{int}}(t')\right\} \tag{2.2.39}$$

wherein $\mathcal{T}_+$ denotes the time-ordering symbol. The Magnus expansion presents a systematic approach in finding an explicit form of the time-evolution operator[13], it is given by

$$\hat{U}(t_0,t) = \exp\left\{\sum_{n=1}\Omega^{(n)}(t_0,t)\right\} \tag{2.2.40}$$

[12] See Ref. [12, p. 215] for an introduction into the time-evolution operator and interactions.
[13] See Ref. [81, p. 42], for an introduction to the Magnus expansion with application to nonlinear processes.

wherein the first two terms are given by

$$\hat{\Omega}^{(1)}(t_0,t) = -i\int_{t_0}^{t} \mathrm{d}t'\, \hat{H}_{\mathrm{int}}(t') \tag{2.2.41}$$

$$\hat{\Omega}^{(2)}(t_0,t) = \frac{(-i)^2}{2!}\int_{t_0}^{t}\mathrm{d}t' \int_{t_0}^{t'} \mathrm{d}t''[\hat{H}_{\mathrm{int}}(t'),\hat{H}_{\mathrm{int}}(t'')]. \tag{2.2.42}$$

For some interactions there exists no exact solution and we can truncate the expansion up to some finite term. Compared to other expansions, e.g. the Neumann expansion, the truncated Magnus expansion is still unitary.

Let us apply the Magnus expansion to find the time-evolution operator corresponding to the interaction Hamiltonian of eq. (2.2.38). The first term of the Magnus expansion turns out to be

$$\hat{\Omega}^{(1)}(t_0,t) = i\sum_{\lambda=1,2}\int \frac{\mathrm{d}^3p}{(2\pi)^3\sqrt{2\omega(\mathbf{p})}}\{J_\lambda(t,t_0;\mathbf{p})\hat{a}_\lambda(\mathbf{p}) + \mathrm{H.c.}\} \tag{2.2.43}$$

where we defined the time-integrated current for polarization λ

$$J_\lambda(t_0,t;\mathbf{p}) = \int_{t_0}^{t}\mathrm{d}t'\,(\mathbf{j}(t,\mathbf{p})^*\cdot\hat{\mathbf{e}}_\lambda(\mathbf{p}))\,e^{-i\omega(\mathbf{p})t'}. \tag{2.2.44}$$

The second term in the Magnus expansion turns out to be complex

$$\hat{\Omega}^{(2)}(t_0,t) = i\sum_{\lambda=1,2}\int \frac{\mathrm{d}^3p}{(2\pi)^3\omega(\mathbf{p})}\,\mathrm{Im}\{J_\lambda(t_0,t';\mathbf{p})J_\lambda(t_0,t'';\mathbf{p})^*\} \tag{2.2.45}$$

which only contributes a phase to the time-evolution operator. As the second commutator is complex-valued, and therefore commutes, higher order commutators vanish and the Magnus expansion is exact with the first two terms. As long as we consider a single current source, no interference of phases can occur and we can ignore the complex phase originating from the second Magnus coefficient. The time-evolution operator of the Maxwell field interacting with a classical source current therefore is [13, p. 168]

$$\hat{U}(t_0,t) = \exp\left\{i\sum_{\lambda=1,2}\int \frac{\mathrm{d}^3p}{(2\pi)^3\sqrt{2\omega(\mathbf{p})}}\{J_\lambda(t,t_0;\mathbf{p})\hat{a}_\lambda(\mathbf{p}) + \mathrm{H.c.}\}\right\}. \tag{2.2.46}$$

Neglecting the polarization

$$\hat{U}(t_0,t) = \exp\left\{\int \frac{\mathrm{d}^3p}{(2\pi)^3\sqrt{2\omega(\mathbf{p})}}\{iJ(t,t_0;\mathbf{p})\hat{a}(\mathbf{p}) - \mathrm{H.c.}\}\right\} \tag{2.2.47}$$

we identify the time-evolution operator with the generalization of the displacement operator from quantum optics [10, p. 47]

$$\lim_{t\to\infty}\hat{U}(-t,+t) = \hat{D}\left[-iJ(\mathbf{p})\right] \tag{2.2.48}$$

where we take the generalized displacement operator to be

$$\begin{aligned}\hat{D}[\alpha] &= \exp\left\{\hat{A}^{(+)}[\alpha] - \hat{A}^{(-)}[\alpha^*]\right\} \\ &= \exp\left\{\int \frac{\mathrm{d}^3 p}{(2\pi)^3\sqrt{2\omega(\mathbf{p})}}\left\{\alpha(\mathbf{p})\hat{a}^\dagger(\mathbf{p}) - \alpha(\mathbf{p})^*\hat{a}(\mathbf{p})\right\}\right\}\end{aligned} \tag{2.2.49}$$

where we identified the generalized field creation and annihilation operators, $\hat{A}^{(+)}[\alpha]$ and $\hat{A}^{(-)}[\alpha^*]$. Noting that

$$[\hat{A}^{(+)}[\alpha], \hat{A}^{(-)}[\alpha^*]] = \int \frac{\mathrm{d}^3 p}{(2\pi)^3 2\omega(\mathbf{p})}|\alpha(\mathbf{p})|^2 \tag{2.2.50}$$

we can employ the Baker-Campbell-Hausdorff (BCH) formula as in Ref. [10, p. 48] to write the displacement operator in normal-order

$$\hat{D}[\alpha] = \exp\left\{-\frac{1}{2}[\hat{A}^{(+)}[\alpha], \hat{A}^{(-)}[\alpha^*]]\right\}\exp\left\{+\hat{A}^{(+)}[\alpha]\right\}\exp\left\{-\hat{A}^{(-)}[\alpha]\right\}. \tag{2.2.51}$$

Now, let us discuss some properties of the displacement operator. The product of two different displacements is equal to the sum of the displacement times a suppression factor depending on the overlap for the displacement, i.e.,

$$\begin{aligned}\hat{D}[\alpha]\hat{D}[\beta] &= \hat{D}[\alpha+\beta]\exp\left\{-\frac{1}{2}[\hat{A}^{(+)}[\alpha], \hat{A}^{(-)}[\beta^*]] + \frac{1}{2}[\hat{A}^{(+)}[\beta], \hat{A}^{(-)}[\alpha^*]]\right\} \\ &= \hat{D}[\alpha+\beta]\exp\left\{-\frac{1}{2}\int \frac{\mathrm{d}p}{(2\pi)^3 2\omega(\mathbf{p})}\left\{\alpha(\mathbf{p})\beta(\mathbf{p})^* - \alpha(\mathbf{p})^*\beta(\mathbf{p})\right\}\right\}.\end{aligned} \tag{2.2.52}$$

Using the product formula, we can quickly show that the displacement operator is unitary

$$\hat{D}[\alpha]\hat{D}[\alpha]^\dagger = \hat{D}[\alpha]\hat{D}[-\alpha] = \mathbb{1} \tag{2.2.53}$$

which is not too surprising given the time-evolution is unitary.

The radiation emitted by a classical current is coherent, suggesting to identify the quantum state produced by a classical current as the coherent state

$$|\alpha\rangle = \hat{D}[\alpha]|0\rangle = \exp\left\{-\frac{1}{2}[\hat{A}^{(+)}[\alpha], \hat{A}^{(-)}[\alpha^*]]\right\}\exp\left\{\hat{A}^{(+)}[\alpha]\right\}|0\rangle \tag{2.2.54}$$

where we used that the exponential of the generalized annihilation operator acting on the vacuum state produces the vacuum state. Coherent states are non-orthogonal, i.e.,

$$\begin{aligned}\langle\alpha|\beta\rangle &= \exp\left\{-\frac{1}{2}[\hat{A}^{(+)}[\alpha], \hat{A}^{(-)}[\alpha^*]] - \frac{1}{2}[\hat{A}^{(+)}[\beta], \hat{A}^{(-)}[\beta^*]] + [\hat{A}^{(+)}[\beta], \hat{A}^{(-)}[\alpha^*]]\right\} \\ &= \exp\left\{-\frac{1}{2}\int \frac{\mathrm{d}p}{(2\pi)^3 2\omega(\mathbf{p})}\left\{|\alpha(\mathbf{p})|^2 + |\beta(\mathbf{p})|^2 - 2\alpha(\mathbf{p})^*\beta(\mathbf{p})\right\}\right\}.\end{aligned} \tag{2.2.55}$$

The inner product of a coherent state with a number state yields

$$\langle n_f|\alpha\rangle = \frac{1}{\sqrt{n!}} e^{-\overline{n}/2} \left(\int \frac{\mathrm{d}p}{(2\pi)^3 2\omega(\mathbf{p})} f(\omega(\mathbf{p}),\mathbf{p})^* \, \alpha(\mathbf{p}) \right)^n . \tag{2.2.56}$$

The coherent state is an eigenstate to the annihilation operator

$$\hat{a}(\mathbf{p})|\alpha\rangle = \frac{\alpha(\mathbf{p})}{\sqrt{2\omega(\mathbf{p})}}|\alpha\rangle, \tag{2.2.57}$$

and therefore also an eigenstate of the negative-frequency Maxwell field operator

$$\hat{A}(t,\mathbf{x})|\alpha\rangle = \int \frac{\mathrm{d}^3 p}{(2\pi)^3 2\omega(\mathbf{p})} \alpha(\mathbf{p}) e^{-i\omega(\mathbf{p})t + i\mathbf{p}\cdot\mathbf{x}}|\alpha\rangle. \tag{2.2.58}$$

The coherent state being an eigenstate of the annihilation operator makes it easy to derive most expectation values, for instance, for the Hamiltonian operator

$$\langle\alpha|\hat{H}|\alpha\rangle = \int \frac{\mathrm{d}p}{(2\pi)^3} \omega(\mathbf{p}) \left| \frac{\alpha(\mathbf{p})}{\sqrt{2\omega(\mathbf{p})}} \right|^2 \tag{2.2.59}$$

and its variance

$$\langle\alpha|\left(\Delta\hat{H}\right)^2|\alpha\rangle = \int \frac{\mathrm{d}p}{(2\pi)^3} \omega(\mathbf{p})^2 \left| \frac{\alpha(\mathbf{p})}{\sqrt{2\omega(\mathbf{p})}} \right|^2 . \tag{2.2.60}$$

For the number operator we find the mean to equal the variance

$$\langle\alpha|\hat{N}|\alpha\rangle = \int \frac{\mathrm{d}p}{(2\pi)^3} \left| \frac{\alpha(\mathbf{p})}{\sqrt{2\omega(\mathbf{p})}} \right|^2 = \overline{n} \tag{2.2.61}$$

$$\langle\alpha|\left(\Delta\hat{N}\right)^2|\alpha\rangle = \overline{n}^2, \tag{2.2.62}$$

i.e., the photon number to be Poisson distributed, which follows simply by setting $\omega(\mathbf{p}) = 1$ in the results obtained for the Hamilton operator. The expectation value of the electric field operator reads

$$\begin{aligned} \langle\alpha|\hat{E}(t,\mathbf{x})|\alpha\rangle &= \int \frac{\mathrm{d}^3 p}{(2\pi)^3} \operatorname{Im}\left\{\alpha(\mathbf{p}) e^{-i\omega(\mathbf{p})t + i\mathbf{p}\cdot\mathbf{x}}\right\} \\ &= \int \frac{\mathrm{d}^3 p}{(2\pi)^3} |\alpha(\mathbf{p})| \sin(\mathbf{p}\cdot\mathbf{x} - \omega(\mathbf{p})t + \varphi) \end{aligned} \tag{2.2.63}$$

where we used the polar representation $\alpha(\mathbf{p}) = |\alpha(\mathbf{p})|e^{i\varphi}$. The variance of the electric field operator,

$$\langle\alpha|\left(\Delta\hat{E}(t,\mathbf{x})\right)^2|\alpha\rangle = \frac{1}{2}\int \frac{\mathrm{d}^3 p}{(2\pi)^3} \omega(\mathbf{p}), \tag{2.2.64}$$

is equal to the contribution from the vacuum fluctuations. The coherent state is also an eigenstate of the negative-frequency electric field operator

$$\hat{E}^{(-)}(t,\mathbf{x})|\alpha\rangle = \frac{1}{2i}\int \frac{\mathrm{d}^3 p}{(2\pi)^3}\alpha(\mathbf{p})e^{-i\omega(\mathbf{p})t+i\mathbf{p}\cdot\mathbf{x}}|\alpha\rangle, \tag{2.2.65}$$

which appears similar to a Fourier transform.

We have derived the generalized coherent state from the interaction of the Maxwell field with a classical current where we found the time-evolution operator to yield the displacement operator. The generalized coherent state and displacement operators share the same properties as their single-mode quantum optics counterparts which is not too surprising given that the modes are independent of another.

Summary

The present chapter consists of two stages. In the first stage, we derived the plane-mode expansions of the quantum Maxwell and electric field operators in the Coulomb gauge, eq. (2.1.46) and eq. (2.1.49), from field-theoretic arguments. In the second second, we axiomatically motivated a generalization of the number and coherent states to a momentum distribution. The momentum distribution is related to the wave function and generalizes the frequency spectrum, essential for communication, to three dimensions. While the properties of our generalized quantum states are qualitatively compatible with the simplified states from single-mode quantum optics, we presented them in a consistent framework justified by established results from quantum field theory.

Our field-theoretic description reduces to continuous-mode quantum optics [10, 9] if we ignore

1. the polarization DOFs of the Maxwell vector field,

2. the transverse momentum distribution, and

3. the Lorentz factor $1/\sqrt{2\omega}$.

The first approximation is straightforward and not a strong limitation as it is easy to restore the polarization DOFs through a tensor product of two scalar fields. For optical communication, and quantum optics, the transverse momentum profile transversal to the propagation axis carries no information and it is reasonable to ignore the transversal DOFs [76, p. 53]

$$\int_{\mathbb{R}^3} \frac{\mathrm{d}^3 p}{(2\pi)^3\sqrt{2\omega(\mathbf{p})}} \to \int_{-\infty}^{\infty} \frac{\mathrm{d}p}{(2\pi)\sqrt{2p}}. \tag{2.2.1}$$

The approximation can be made even stronger when neglecting back-scattering and reflection effects and restricting the momentum distribution to forward propagation, i.e.,

$$\int_{-\infty}^{\infty} \frac{\mathrm{d}p}{(2\pi)\sqrt{2p}} \approx \int_{0}^{\infty} \frac{\mathrm{d}p}{(2\pi)\sqrt{2p}} \tag{2.2.2}$$

where the identification of the forward momentum with the frequency, $p = \omega$ is often made. The third approximation requires some additional investigation. For one, every physical measurement is bandwidth-limited such that by the mean-value theorem for definite integrals

$$\int_{0}^{\infty} \frac{\mathrm{d}\omega}{(2\pi)\sqrt{2\omega}} \approx \frac{1}{\sqrt{2\omega_0}} \int_{0}^{\infty} \frac{\mathrm{d}\omega}{2\pi}, \tag{2.2.3}$$

the Lorentz factor is effectively constant. However, in principle, it should be possible to measure the Lorentz factor. That said, the Lorentz factor breaks our Fourier transform, making some results difficult for interpretation.[14] For instance, if we ignore the Lorentz factor and ignore the transverse momentum distribution, we find that the eigenvalue of the coherent state with regard to the Maxwell field operator, eq. (2.2.58), simplifies to

$$\hat{A}^{(-)}(t,x)|\alpha\rangle = \int \frac{\mathrm{d}p}{2\pi} \alpha(p) e^{-ip(t-x)} |\alpha\rangle = \alpha(t-x)^* |\alpha\rangle, \tag{2.2.4}$$

where $\alpha(t-x)$ is the time-domain signal.[15] Another assumption or restriction, which we have not mentioned explicitly yet, is the use of the Coulomb gauge. The Coulomb gauge restricts our predictions to a stationary reference frame. While a stationary reference frame appears reasonable for terrestrial communication, it must be questioned for space communication.

Another important operator, subject to controversies, which we have not mentioned so far, is the quadrature operator. Ref. [10, p. 79] defines the continuous-mode quadrature operator as[16]

$$\hat{X}(\vartheta) = \frac{1}{\sqrt{2}} \int \frac{\mathrm{d}p}{2\pi} \left\{ \hat{a}(p) e^{-i(pt+\vartheta)} + \hat{a}^\dagger(p) e^{+i(pt+\vartheta)} \right\}. \tag{2.2.5}$$

Comparing eq. (2.2.5) with the one-dimensional Maxwell operator,

$$\hat{A}(t,x) = \int \frac{\mathrm{d}p}{2\pi} \frac{1}{\sqrt{2p}} \left\{ \hat{a}_\lambda(p) e^{-ip(t-x)} + \hat{a}_\lambda^\dagger(p) e^{+ip(t-x)} \right\}, \tag{2.2.6}$$

we note that these are equal up to the Lorentz factor, a phase, and the spatial dependency x. For a measurement at a stationary location, the spatial dependency reduces to a phase,

[14] More precisely, we need to distinguish between the four-dimensional Fourier transform and the Fourier transform implementing the energy-momentum relation.

[15] We identify the negative-frequency Maxwell operator $\hat{A}^{(-)}$ with the Fourier transform of the annihilation operator used by Loudon [9].

[16] We adapted the quadrature operator to our convention of the Fourier transform, dividing the integration measure by 2π, and added time evolution.

which can be further modified using the phase-rotation operator [82, p. 38], i.e.,

$$e^{-i\vartheta\hat{N}}\hat{A}(t)e^{+i\vartheta\hat{N}} = \int \frac{\mathrm{d}p}{2\pi}\frac{1}{\sqrt{2p}}\left\{\hat{a}_\lambda(p)e^{-ip(t+\vartheta)} + \hat{a}^\dagger_\lambda(p)e^{+ip(t+\vartheta)}\right\}, \tag{2.2.7}$$

where $\hat{N}$ denotes the number operator defined in eq. (2.1.57). Using that practical measurements are bandwidth-limited, we can invoke the mean-value theorem for definite integrals and pull out the Lorentz factor $1/\sqrt{2p}$ from the integrand and thereby fully recovering the quadrature operator proposed by in Ref. [10], eq. (2.2.5). How can the Maxwell field be an observable when it is not gauge invariant? While it is true that the Maxwell field shows a gauge symmetry, the gauge symmetry is uniquely fixed through the Coulomb gauge, which is required to remove unphysical polarization DOFs.[17]

[17] See Ref. [83] for a discussion on the physicality of the Maxwell field and the gauge freedom.

Chapter 3.

Quantum theory of (electro-)optical components

In the last chapter, we derived a general quantum theory of light for optical communication. Now it is time to apply it to describe the electro-optical building blocks from which we later assemble a coherent-state transmission system. In particular, we present quantum models for the optical coupler, electro-optical modulators, and detectors, which we use to derive input-output relations for coherent states.

First, we introduce the optical coupler as a generalization of the beam splitter and the waveguide coupler. Second, we apply nonlinear quantum-optics to model electro-optical phase modulation [84] as nonlinear frequency-conversion [81] and employ it to perform amplitude modulation through electrically-driven interference. Third, we briefly review the photoelectric effect [8, 7] and derive direct and balanced detectors and their interpretation in terms of quantum measurements.

For the first two parts, we aim to motivate an evolution operator from some interaction Hamiltonian. At some point, we cannot give an explicit evolution operator but only argue why such an operator may, in principle, exist.

3.1. Coupler

An optical coupler is a passive component with two optical in- and outputs, generally assumed to be linear time-invariant (LTI), which appears in almost every optical setup or as a building block of ore complex components.[1]

[1] The optical splitter is a special case of the optical coupler where one of the two optical inputs is zero, or, more precisely, the vacuum state.

In the following, we would like to illuminate the versatile aspects of the optical coupler. We begin our investigation with the beam splitter, implementing an optical coupler and splitter, considering its reflection and transmission properties [4, 7]. Subsequently, we examine the waveguide coupler, which offers an alternative approach using an interaction Hamiltonian [18]. Finally, we provide a third entry point using a unitary transformation to transform the displacement operator yielding input-output relations for coherent states and discuss applications as a splitter and spectral filter [82, 7].

3.1.1. Beam splitter

The most commonly employed designs of the beam splitter are the cubic, plate, and pellicle beam splitters, see Figure 3.1. The cubic beam splitter is made of two triangular prisms. The

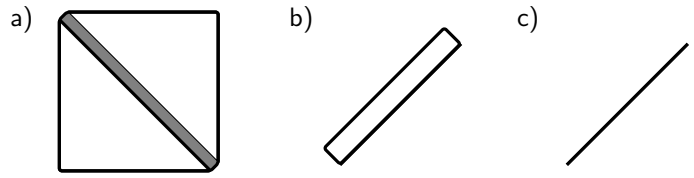


Figure 3.1.: Different types of free-ray beam splitters. (a) Cubic beam splitter made of two triangular prisms glued at their base (grey). (b) Plate beam splitter made of a dielectric plate. (c) Pellicle beam splitter made from a thin membrane.

interface between the two prisms is finished with a dielectric coating. The outward-facing surface of the prisms is grafted with an anti-reflective (AR) coating.[2] he pellicle beam splitter consists of a few micrometer thin membrane, optionally with a one-sided coating. The plate beam splitter is like a thick pellicle beam splitter made of glass.

To deduce the relation between the in- and output fields, we sequentially couple a laser pulse into each input while monitoring both outputs with a spectrum analyzer, see Figure 3.2. Assuming the beam splitter to be an LTI system, knowing the spectral shape of the laser pulse lets us infer the frequency responses of the beam splitter. Invoking the superposition principle for electromagnetic waves, we find the frequency responses of the beam splitter to relate the electric fields by

$$\begin{pmatrix} \langle \hat{E}_1'(\omega) \rangle \\ \langle \hat{E}_2'(\omega) \rangle \end{pmatrix} = \begin{pmatrix} t(\omega) & r'(\omega) \\ r(\omega) & t'(\omega) \end{pmatrix} \begin{pmatrix} \langle \hat{E}_1(\omega) \rangle \\ \langle \hat{E}_2(\omega) \rangle \end{pmatrix} \tag{3.1.1}$$

wherein $r(\omega), r'(\omega)$ and $t(\omega), t'(\omega)$ are the complex reflection respective transmission coefficients. The absolute values of the transmission, $|t(\omega)|$ and $|t'(\omega)|$, and reflection coefficients, $|r(\omega)|$ and $|r'(\omega)|$, determine the splitting ratio of the input power among the outputs. The

[2] The incident angle of the electric field is perpendicular to the surface of the cubic beam splitter. As the reflection angle is equal to the incidence angle, we have back-reflection of the input fields.

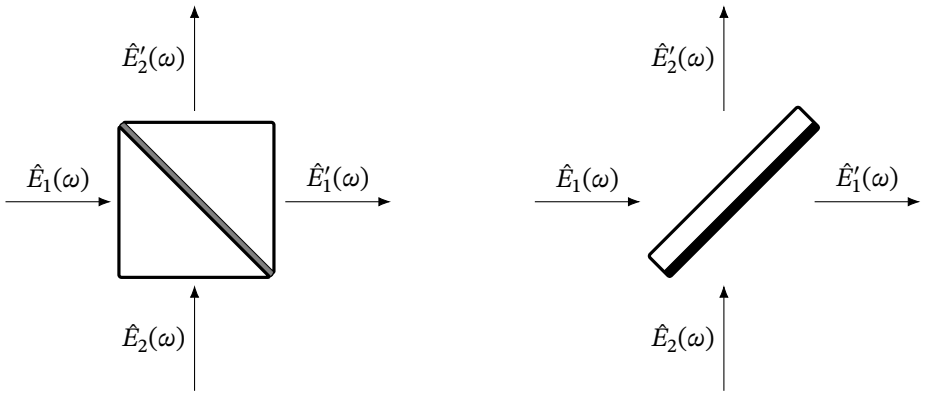


Figure 3.2.: Cubic (left) and plate beam splitter (right) with the two input fields, $\hat{E}_1(\omega)$ and $\hat{E}_2(\omega)$, and two output fields, $\hat{E}_1'(\omega)$ and $\hat{E}_2'(\omega)$, labelled by the momentum representation of the electric field operators.

complex phase factor of the reflection and transmission coefficients characterizes the phase shifts the output fields concerning the input fields. The beam splitter is a passive device implying the output energy to be bound by the input energy

$$|\langle\hat{E}_1'(\omega)\rangle|^2 + |\langle\hat{E}_2'(\omega)\rangle|^2 \leq |\langle\hat{E}_1(\omega)\rangle|^2 + |\langle\hat{E}_2(\omega)\rangle|^2, \tag{3.1.2}$$

or equivalently, constraining the reflection and transmission coefficients by

$$|r(\omega)|^2 + |t(\omega)|^2 \leq 1, \qquad |r'(\omega)|^2 + |t'(\omega)|^2 \leq 1. \tag{3.1.3}$$

The equality of these inequalities is only true for lossless devices for which there is no backscattering.[3] Sometimes, one finds the claim [18, p. 129] that the matrix transformation in eq. (3.1.1) is required to be symmetric (or reciprocal) due to Maxwell's equations. However, only optical systems with a single dielectric layer are reciprocal [85], but most physical beam splitters comprise multiple dielectric layers.[4] It is possible to derive exact expressions of the complex reflection, $r(\omega), r'(\omega)$, and transmission coefficients, $t(\omega), t'(\omega)$ using classical wave optics and perfect knowledge of the dimensions and material properties. For example, Hénault [86] derived an exact expression for the reflected and transmitted amplitudes of a plate beam splitter with one input and a single dielectric layer. Likewise, Hamilton [87] discusses the cubic beam splitter with two inputs and different coatings. In general, the complex reflection and transmission coefficients need to account for multiple reflections at different dielectric layers inside the beam splitter.

Inserting the mode expansion of the electric field operators, eqs. (2.1.49) to (2.1.51), and using the linearity of the device and the expectation value, we recover the transformation

[3] Using an optical circulator it is in principle possible to measure all 16 scattering parameters.

[4] For example, cubic beam splitters typically have a coating followed by optical cement between the prisms breaking reciprocal symmetry of the system.

for the annihilation operators, sometimes referred to as quantum modes,

$$\begin{pmatrix} \hat{a}_1'(\omega) \\ \hat{a}_2'(\omega) \end{pmatrix} = \begin{pmatrix} t(\omega) & r'(\omega) \\ r(\omega) & t'(\omega) \end{pmatrix} \begin{pmatrix} \hat{a}_1(\omega) \\ \hat{a}_2(\omega) \end{pmatrix} \tag{3.1.4}$$

in agreement with Refs. [82, 4].

3.1.2. Waveguide coupler

Contrary to the direct coupling in free-ray beam splitters, a fiber or waveguide coupler uses indirect coupling through the evanescent field. The evanescent field of an electromagnetic field does not propagate but decays exponentially. We often observe evanescent fields at the boundary of waveguiding structures. One must bring the waveguides in proximity for the evanescent fields of two waveguided modes to couple efficiently. The range where the waveguides are close is the interaction length l, see Figure 3.3. Over the interaction length, the two energy of the field modes oscillates back and forth between the two waveguides. The weak coupling through evanescent fields is conceptionally similar to weakly coupled

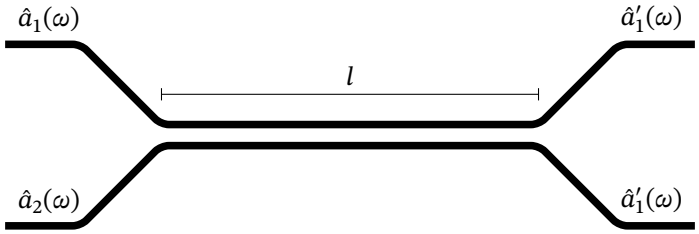


Figure 3.3.: Waveguide coupler with input quantum modes $\hat{a}_1(\omega)$ and $\hat{a}_2(\omega)$ coupled evanescent over an interaction length l yielding the output quantum modes $\hat{a}_1'(\omega)$ and $\hat{a}_2'(\omega)$.

harmonic oscillators. Haroche [18, p. 131] successfully exploits the analogy to derive the quantum beam splitter transform from interaction theory. We generalize his approach for the mode continuum derived in the previous chapter.

Let $\hat{a}_1(\omega)$ and $\hat{a}_2(\omega)$ be the annihilation operators of the first and second waveguide modes. The interaction Hamiltonian

$$\hat{H}_{\text{int}} = -\int \frac{\mathrm{d}\omega}{2\pi} \left\{ g(\omega)\hat{a}_1(\omega)\hat{a}_2^\dagger(\omega) + g^*(\omega)\hat{a}_1^\dagger(\omega)\hat{a}_2(\omega) \right\}, \tag{3.1.5}$$

wherein $g(\omega)$ is a complex-valued coupling parameter encoding the material and geometry of the coupler, describes the transitions of excitations between the first and the second mode. As the interaction Hamiltonian is time-independent, all but the first term in the Magnus expansion vanish, and the time evolution operator is

$$\hat{U}_{\text{int}} = \exp\left\{ i \int \mathrm{d}t' \int \frac{\mathrm{d}\omega}{2\pi} \left\{ g(\omega)\hat{a}_1(\omega)\hat{a}_2^\dagger(\omega) + g^*(\omega)\hat{a}_1^\dagger(\omega)\hat{a}_2(\omega) \right\} \right\} \tag{3.1.6}$$

wherein the time integration is over the duration of the interaction. Assuming the interaction to be limited to the interaction length l, the interaction duration T is approximately equal to the interaction length l divided by the group velocity $v_g(\omega)$. The group velocity depends on the materials of the coupler, suggesting redefining the coupling parameter to include the different interaction durations, i.e.,

$$\hat{U}_{\text{int}} = \exp\left\{ i \int \frac{\mathrm{d}\omega}{2\pi} \theta(\omega) \left\{ \hat{a}_1(\omega)\hat{a}_2^\dagger(\omega) e^{-i\varphi(\omega)} + \hat{a}_1^\dagger(\omega)\hat{a}_2(\omega) e^{+i\varphi(\omega)} \right\} \right\} \tag{3.1.7}$$

where the real-valued couplings $\theta(\omega)$ and $\varphi(\omega)$ implicitly depend on the materials and geometry of the waveguide coupler and the interaction length l. We define the generator

$$\hat{G} = -i \int \frac{\mathrm{d}\omega}{2\pi} \theta(\omega) \left\{ \hat{a}_1(\omega)\hat{a}_2^\dagger(\omega) e^{-i\varphi(\omega)} + \hat{a}_1^\dagger(\omega)\hat{a}_2(\omega) e^{+i\varphi(\omega)} \right\} \tag{3.1.8}$$

and calculate the commutator of the generator with the annihilation operators

$$[\hat{G}, \hat{a}_1(\omega)] = i\theta(\omega)\hat{a}_2(\omega) e^{+i\varphi(\omega)} \qquad [\hat{G}, \hat{a}_2(\omega)] = i\theta(\omega)\hat{a}_1(\omega) e^{-i\varphi(\omega)}. \tag{3.1.9}$$

The transformed annihilation operators turn out to be[5],

$$\begin{aligned}
\hat{a}_1'(\omega) &= \hat{U}_{\text{int}}^\dagger \hat{a}_1(\omega) \hat{U}_{\text{int}} = e^{+\hat{G}} \hat{a}_1(\omega) e^{-\hat{G}} \\
&= \hat{a}_1 + [\hat{G}, \hat{a}_1] + \frac{1}{2!}[\hat{G}, [\hat{G}, \hat{a}_1]] + \frac{1}{3!}[\hat{G}, [\hat{G}, [\hat{G}, \hat{a}_1]]] + \ldots \\
&= \hat{a}_1(\omega) + i\theta(\omega)\hat{a}_2(\omega) e^{+i\varphi(\omega)} + \frac{1}{2!}\left(i\theta(\omega)\right)^2 \hat{a}_1(\omega) + \frac{1}{3!}\left(i\theta(\omega)\right)^3 \hat{a}_2(\omega) e^{+i\varphi(\omega)} + \ldots \\
&= \cos\theta(\omega)\hat{a}_1(\omega) + i\sin\theta(\omega)\hat{a}_2(\omega) e^{+i\varphi(\omega)}
\end{aligned} \tag{3.1.10}$$

and

$$\begin{aligned}
\hat{a}_2'(\omega) &= \hat{U}_{\text{int}}^\dagger \hat{a}_2(\omega) \hat{U}_{\text{int}} = e^{+\hat{G}} \hat{a}_2(\omega) e^{-\hat{G}} \\
&= \hat{a}_2 + [\hat{G}, \hat{a}_2] + \frac{1}{2!}[\hat{G}, [\hat{G}, \hat{a}_2]] + \frac{1}{3!}[\hat{G}, [\hat{G}, [\hat{G}, \hat{a}_2]]] + \ldots \\
&= \hat{a}_2(\omega) + i\theta(\omega)\hat{a}_1(\omega) e^{-i\varphi(\omega)} + \frac{1}{2!}\left(i\theta(\omega)\right)^2 \hat{a}_2(\omega) + \frac{1}{3!}\left(i\theta(\omega)\right)^3 \hat{a}_1(\omega) e^{-i\varphi(\omega)} + \ldots \\
&= \cos\theta(\omega)\hat{a}_2(\omega) + i\sin\theta(\omega)\hat{a}_1(\omega) e^{-i\varphi(\omega)},
\end{aligned} \tag{3.1.11}$$

where we used a kind of Baker-Campbell-Hausdorff (BCH) formula, in agreement with Ref. [18, p. 131]. In matrix notation, the transformation of the annihilation operators reads

$$\begin{pmatrix} \hat{a}_1'(\omega) \\ \hat{a}_2'(\omega) \end{pmatrix} = U(\omega) \begin{pmatrix} \hat{a}_1(\omega) \\ \hat{a}_2(\omega) \end{pmatrix} = \begin{pmatrix} \cos\theta(\omega) & i\sin\theta(\omega) e^{+i\varphi} \\ i\sin\theta(\omega) e^{-i\varphi} & \cos\theta(\omega) \end{pmatrix} \begin{pmatrix} \hat{a}_1(\omega) \\ \hat{a}_2(\omega) \end{pmatrix}. \tag{3.1.12}$$

Comparison of the annihilation operator transformation for the waveguide coupler, eq. (3.1.12), and the beam splitter, eq. (3.1.4), our waveguide result implies lossless coupling. Lossless

[5] Strictly speaking, the annihilation operators in the interaction picture have an additional factor $e^{-i\omega t}$.

coupling is essential for the transformed annihilation operators to satisfy the canonical commutation relation (CCR) [4, p. 38]. Modeling an absorbing coupler requires four quantum modes, two annihilation operators for the field, and two for a bosonic reservoir, see Ref. [7, p. 210] for details.

3.1.3. Unitary operator transform

The derived transforms of the free-ray beam splitter and the fiber or waveguide coupler, eqs. (3.1.4) and (3.1.12), have in common that they are two-dimensional unitary matrices, which is not surprising since a unitary matrix transform conserves energy. The optical coupler transform being linear and unitary is not surprising since the coupler is a linear passive device, which we further assumed to be lossless. It presents itself to take the unitary matrix transform as the defining property of an ideal optical coupler.

A general decomposition of a two-dimensional unitary matrix is the product [82, p. 95]

$$U(\omega) = \begin{pmatrix} e^{+i\Phi/2} & 0 \\ 0 & e^{-i\Phi/2} \end{pmatrix} \begin{pmatrix} \cos(\Theta/2) & \sin(\Theta/2) \\ -\sin(\Theta/2) & \cos(\Theta/2) \end{pmatrix} \begin{pmatrix} e^{+i\Psi/2} & 0 \\ 0 & e^{-i\Psi/2} \end{pmatrix} e^{i\Lambda/2} \tag{3.1.13}$$

wherein we suppress the frequency-dependence of the real parameters, $\Lambda(\omega)$, $\Theta(\omega)$, $\Psi(\omega)$, $\Phi(\omega)$, for clarity. We can read the matrix decomposition, eq. (3.1.13), as first adding a global phase shift $\Lambda/2$, then adding a relative phase shift of Ψ between the incident fields, rotating (mixing) the field amplitudes by the angle $\Theta/2$, and adding another relative phase shift of Ψ between the outgoing fields.

While the unitary matrix transforms the annihilation operators and the field amplitudes, it cannot transform a generic quantum state. In the previous subsection, we found a time evolution operator $\hat{U}$ from linear mode coupling theory, which related to the unitary matrix transform U via

$$U(\omega) \begin{pmatrix} \hat{a}_1(\omega) \\ \hat{a}_2(\omega) \end{pmatrix} = \begin{pmatrix} \hat{a}'_1(\omega) \\ \hat{a}'_2(\omega) \end{pmatrix} = \begin{pmatrix} \hat{U}^\dagger \hat{a}_1(\omega) \hat{U} \\ \hat{U}^\dagger \hat{a}_2(\omega) \hat{U} \end{pmatrix} = \hat{U}^\dagger \begin{pmatrix} \hat{a}_1(\omega) \\ \hat{a}_2(\omega) \end{pmatrix} \hat{U}. \tag{3.1.14}$$

The unitary operators corresponding to the unitary matrix decomposition in eq. (3.1.13) are

the Jordan-Schwinger operators[6]

$$\hat{L}_t = \frac{1}{2}\int \frac{\mathrm{d}\omega}{2\pi} \begin{pmatrix} \hat{a}_1(\omega) \\ \hat{a}_2(\omega) \end{pmatrix}^\dagger \mathbb{1}_2 \begin{pmatrix} \hat{a}_1(\omega) \\ \hat{a}_2(\omega) \end{pmatrix} = \frac{1}{2}\int \frac{\mathrm{d}\omega}{2\pi} \left(\hat{a}_1^\dagger(\omega)\hat{a}_1(\omega) + \hat{a}_2^\dagger(\omega)\hat{a}_2(\omega)\right) \tag{3.1.15}$$

$$\hat{L}_x = \frac{1}{2}\int \frac{\mathrm{d}\omega}{2\pi} \begin{pmatrix} \hat{a}_1(\omega) \\ \hat{a}_2(\omega) \end{pmatrix}^\dagger \sigma_x \begin{pmatrix} \hat{a}_1(\omega) \\ \hat{a}_2(\omega) \end{pmatrix} = \frac{1}{2}\int \frac{\mathrm{d}\omega}{2\pi} \left(\hat{a}_1^\dagger(\omega)\hat{a}_2(\omega) + \hat{a}_2^\dagger(\omega)\hat{a}_1(\omega)\right) \tag{3.1.16}$$

$$\hat{L}_y = \frac{1}{2}\int \frac{\mathrm{d}\omega}{2\pi} \begin{pmatrix} \hat{a}_1(\omega) \\ \hat{a}_2(\omega) \end{pmatrix}^\dagger \sigma_y \begin{pmatrix} \hat{a}_1(\omega) \\ \hat{a}_2(\omega) \end{pmatrix} = \frac{i}{2}\int \frac{\mathrm{d}\omega}{2\pi} \left(\hat{a}_2^\dagger(\omega)\hat{a}_1(\omega) - \hat{a}_1^\dagger(\omega)\hat{a}_2(\omega)\right) \tag{3.1.17}$$

$$\hat{L}_z = \frac{1}{2}\int \frac{\mathrm{d}\omega}{2\pi} \begin{pmatrix} \hat{a}_1(\omega) \\ \hat{a}_2(\omega) \end{pmatrix}^\dagger \sigma_z \begin{pmatrix} \hat{a}_1(\omega) \\ \hat{a}_2(\omega) \end{pmatrix} = \frac{1}{2}\int \frac{\mathrm{d}\omega}{2\pi} \left(\hat{a}_1^\dagger(\omega)\hat{a}_1(\omega) - \hat{a}_2^\dagger(\omega)\hat{a}_2(\omega)\right) \tag{3.1.18}$$

where $\sigma_1, \sigma_2, \sigma_3$ denote the two-dimensional Pauli matrices. The Jordan-Schwinger operators satisfy the angular-momentum commutation algebra [82, p. 97]

$$[\hat{L}_i, \hat{L}_j] = i\varepsilon_{ijk}\hat{L}^k \qquad\qquad [\hat{L}_t, \hat{L}_i] = 0 \tag{3.1.19}$$

and act as generator for the individual components of the matrix decomposition in eq. (3.1.13). The generator of the unitary matrix, eq. (3.1.13), is

$$\hat{U} = e^{i\Lambda\hat{L}_t} e^{i\Phi\hat{L}_z} e^{i\Theta\hat{L}_y} e^{i\Psi\hat{L}_z}. \tag{3.1.20}$$

The inverse of the unitary operator, eq. (3.1.20), can be written

$$\begin{aligned} \hat{U}(\Lambda, \Phi, \Theta, \Psi)^\dagger &= e^{-i\Psi\hat{L}_z} e^{-i\Theta\hat{L}_y} e^{-i\Phi\hat{L}_z} e^{-i\Lambda\hat{L}_t} \\ &= e^{-i\Lambda\hat{L}_t} e^{-i\Psi\hat{L}_z} e^{-i\Theta\hat{L}_y} e^{-i\Phi\hat{L}_z} \\ &= \hat{U}(-\Lambda, -\Psi, -\Theta, -\Phi), \end{aligned} \tag{3.1.21}$$

where we used that $\hat{L}_t$ commutes with the other Jordan-Schwinger operators, and can be used to find the reversed transform,

$$\hat{U} \begin{pmatrix} \hat{a}_1(\omega) \\ \hat{a}_2(\omega) \end{pmatrix} \hat{U}^\dagger = U(\omega)^\dagger \begin{pmatrix} \hat{a}_1(\omega) \\ \hat{a}_2(\omega) \end{pmatrix}, \tag{3.1.22}$$

of the annihilation operators.

3.1.4. Coherent state transform

Let us now consider the action of the ideal coupler on the tensor product of input coherent-states[7]

$$|\boldsymbol{\alpha}(t)\rangle = |\alpha_1(t), \alpha_2(t)\rangle. \tag{3.1.23}$$

[6] Generalized to a frequency continuum from Ref. [82, p. 97].

[7] Other quantum states typically produce entangled output states, see, for instance, Ref. [88], which is not of interest here.

The output states are given by applying the unitary evolution operator $\hat{U}$, e.g., eq. (3.1.20), onto the input state

$$\hat{U}|\boldsymbol{\alpha}(t)\rangle = \hat{U}\hat{D}\left[\boldsymbol{\alpha}(t)\right]\hat{U}^\dagger\hat{U}|0,0\rangle = \hat{U}\hat{D}\left[\boldsymbol{\alpha}(t)\right]\hat{U}^\dagger|0\rangle, \tag{3.1.24}$$

wherein we inserted $\mathbb{1} = \hat{U}^\dagger\hat{U}$ in the second step and we used the invariance of the vacuum state in the third step. The transformed displacement operator reads[8]

$$\begin{aligned}\hat{U}\hat{D}\left[\boldsymbol{\alpha}(t)\right]\hat{U}^\dagger &= \hat{U}\exp\left\{\int\frac{\mathrm{d}\omega}{2\pi}\left\{\boldsymbol{\alpha}(\omega)^\mathsf{T}e^{-i\omega t}\begin{pmatrix}\hat{a}_1^\dagger(\omega)\\ \hat{a}_2^\dagger(\omega)\end{pmatrix} - \boldsymbol{\alpha}(\omega)^\dagger e^{+i\omega t}\begin{pmatrix}\hat{a}_1(\omega)\\ \hat{a}_2(\omega)\end{pmatrix}\right\}\right\}\hat{U}^\dagger \\ &= \exp\left\{\int\frac{\mathrm{d}\omega}{2\pi}\left\{\boldsymbol{\alpha}^\mathsf{T}e^{-i\omega t}\hat{U}\begin{pmatrix}\hat{a}_1^\dagger(\omega)\\ \hat{a}_2^\dagger(\omega)\end{pmatrix}\hat{U}^\dagger - \boldsymbol{\alpha}^\dagger e^{+i\omega t}\hat{U}\begin{pmatrix}\hat{a}_1(\omega)\\ \hat{a}_2(\omega)\end{pmatrix}\hat{U}^\dagger\right\}\right\},\end{aligned} \tag{3.1.25}$$

wherein we used the operator identity

$$\hat{U}e^{\hat{A}}\hat{U}^\dagger = \sum_{n=0}^{\infty}\frac{1}{n!}\hat{U}\hat{A}^n\hat{U}^\dagger = \sum_{n=0}^{\infty}\frac{1}{n!}\hat{U}\hat{A}\hat{U}^\dagger\cdots\hat{U}\hat{A}\hat{U}^\dagger = \sum_{n=0}^{\infty}\frac{1}{n!}\left(\hat{U}\hat{A}\hat{U}^\dagger\right)^n = e^{\hat{U}\hat{A}\hat{U}^\dagger} \tag{3.1.26}$$

in the second step to move the unitary operators into the argument of the exponential. We already expressed the transformed annihilation operators in the second term of the exponential using the unitary matrix in eq. (3.1.22). The transformed creation operators in the first term can be brought into a similar form, i.e.,

$$\begin{aligned}\hat{U}\begin{pmatrix}\hat{a}_1^\dagger(\omega)\\ \hat{a}_2^\dagger(\omega)\end{pmatrix}\hat{U}^\dagger &= \begin{pmatrix}\left[\hat{U}\hat{a}_1(\omega)\hat{U}^\dagger\right]^\dagger\\ \left[\hat{U}\hat{a}_2(\omega)\hat{U}^\dagger\right]^\dagger\end{pmatrix} = \left[\begin{pmatrix}\hat{U}\hat{a}_1(\omega)\hat{U}^\dagger\\ \hat{U}\hat{a}_2(\omega)\hat{U}^\dagger\end{pmatrix}^\dagger\right]^\mathsf{T} = \left[\left(U(\omega)\begin{pmatrix}\hat{a}_1(\omega)\\ \hat{a}_2(\omega)\end{pmatrix}\right)^\dagger\right]^\mathsf{T} \\ &= \left[\begin{pmatrix}\hat{a}_1(\omega)\\ \hat{a}_2(\omega)\end{pmatrix}^\dagger U(\omega)\right]^\mathsf{T} = U(\omega)^\mathsf{T}\begin{pmatrix}\hat{a}_1^\dagger(\omega)\\ \hat{a}_2^\dagger(\omega)\end{pmatrix}.\end{aligned} \tag{3.1.27}$$

Inserting the previous result back into the transformed displacement operator, eq. (3.1.25), we factor the unitary matrix to the Fourier amplitudes

$$\begin{aligned}\hat{D}'\left[\boldsymbol{\alpha}(t)\right] &= \exp\left\{\int\frac{\mathrm{d}\omega}{2\pi}\left\{\boldsymbol{\alpha}(\omega)^\mathsf{T}e^{-i\omega t}U(\omega)^\mathsf{T}\begin{pmatrix}\hat{a}_1^\dagger(\omega)\\ \hat{a}_2^\dagger(\omega)\end{pmatrix} - \boldsymbol{\alpha}(\omega)^\dagger e^{+i\omega t}U(\omega)^\dagger\begin{pmatrix}\hat{a}_1(\omega)\\ \hat{a}_2(\omega)\end{pmatrix}\right\}\right\} \\ &= \exp\left\{\int\frac{\mathrm{d}\omega}{2\pi}\left\{\left(U(\omega)\boldsymbol{\alpha}(\omega)\right)^\mathsf{T}e^{-i\omega t}\begin{pmatrix}\hat{a}_1^\dagger(\omega)\\ \hat{a}_2^\dagger(\omega)\end{pmatrix} - \left(U(\omega)\boldsymbol{\alpha}(\omega)\right)^\dagger e^{+i\omega t}\begin{pmatrix}\hat{a}_1(\omega)\\ \hat{a}_2(\omega)\end{pmatrix}\right\}\right\}\end{aligned} \tag{3.1.28}$$

in agreement with Ref. [7, p. 210]. The transformed Fourier amplitudes are given by the matrix product

$$\boldsymbol{\alpha}'(\omega) = U(\omega)\boldsymbol{\alpha}(\omega). \tag{3.1.29}$$

[8] We adopt matrix notation as in Ref. [7, p. 206] to have our result independent of a particular choice of the unitary matrix.

The product in frequency space implies a convolution in the time domain, i.e.,

$$\boldsymbol{\alpha}'(t) = (U * \boldsymbol{\alpha})(t) = \int \frac{\mathrm{d}\omega}{2\pi} U(\omega)\boldsymbol{\alpha}(\omega)e^{+i\omega t}, \tag{3.1.30}$$

and we conclude that a tensor product of coherent states transforms under an ideal optical coupler according to

$$\hat{U}|\alpha(t)\rangle = |(U * \boldsymbol{\alpha})(t)\rangle \qquad\qquad U(t) = \int \frac{\mathrm{d}\omega}{2\pi} U(\omega)e^{+i\omega t} \tag{3.1.31}$$

wherein $U(\omega)$ is a two-dimensional unitary matrix characterizing the coupler.

The fact that the ideal optical coupler only transforms the amplitudes of the input coherent-states is specific to coherent states. The coherent states owe this special property due to having a Poisson number distribution and the Poisson distribution being memoryless. As a consequence, the output coherent-states are independent and consider a subsystem by performing a partial trace, e.g.,

$$\mathrm{Tr}_2\{|\alpha,\beta\rangle\langle\alpha,\beta|\} = \mathrm{Tr}_2\{|\alpha\rangle\langle\alpha| \otimes |\beta\rangle\langle\beta|\} = |\alpha\rangle\langle\alpha| \otimes \mathrm{Tr}_2\{|\beta\rangle\langle\beta|\} = |\alpha\rangle\langle\alpha|, \tag{3.1.32}$$

where we used

$$\mathrm{Tr}_2\{|\beta\rangle\langle\beta|\} = \sum_{n=0}^{\infty} \langle n|\beta\rangle\langle\beta|n\rangle = \sum_{n=0}^{\infty} |\langle n|\beta\rangle|^2 = 1, \tag{3.1.33}$$

is equivalent to the projection of the subsystem

$$\mathrm{Tr}_2\{|\alpha,\beta\rangle\langle\alpha,\beta|\} = |\alpha\rangle\langle\alpha| = \hat{P}_1|\alpha,\beta\rangle\langle\alpha,\beta|\hat{P}_1. \tag{3.1.34}$$

For non-coherent quantum states, it is not correct to project out a subsystem as the partial trace does not generally yield a mixed but a pure state.

3.1.5. Splitter and spectral filter

Our considerations have so far been quite general except for restricting ourselves to input coherent-states. We will now discuss two applications of our results: First, we consider the special case of a coupler being used as a splitter. Second, we consider a coupler as an optical filter relevant to signal processing and quantum-information theory.

An ideal optical splitter redistributes the power of one input among two outputs and is a special case of the optical coupler with one input state being the vacuum state. Using eq. (3.1.29), we find the transformed Fourier amplitudes to be

$$\begin{aligned}\begin{pmatrix}\alpha_1'(\omega)\\ \alpha_2'(\omega)\end{pmatrix} &= e^{i\Lambda/2}\begin{pmatrix}\cos(\Theta/2)e^{i(+\Phi+\Psi)/2} & \sin(\Theta/2)e^{i(+\Phi-\Psi)/2}\\ -\sin(\Theta/2)e^{i(-\Phi+\Psi)/2} & \cos(\Theta/2)e^{i(-\Phi-\Psi)/2}\end{pmatrix}\begin{pmatrix}\alpha(\omega)\\ 0\end{pmatrix}\\ &= \alpha(\omega)\begin{pmatrix}+\cos(\Theta/2)e^{+i\Phi/2}\\ -\sin(\Theta/2)e^{-i\Phi/2}\end{pmatrix}e^{i(\Lambda+\Psi)/2}\end{aligned} \tag{3.1.35}$$

wherein we again suppressed the frequency dependency of the splitting parameters. Instead of choosing a parametrization for the splitting coefficients, which directly ensures energy conservation, we can more generally write

$$\begin{pmatrix}\alpha_1'(\omega)\\ \alpha_2'(\omega)\end{pmatrix} = \alpha(\omega)\begin{pmatrix}c_1(\omega)\\ c_2(\omega)\end{pmatrix} \qquad |c_1(\omega)|^2 + |c_2(\omega)|^2 = 1. \tag{3.1.36}$$

Assuming the Fourier transform of $c_1(\omega), c_2(\omega)$ to be well-defined, we find the output coherent-states to be

$$\hat{U}|\alpha(t), 0\rangle = |(c_1 * \alpha)(t), (c_2 * \alpha)(t)\rangle \tag{3.1.37}$$

according to eq. (3.1.31). If we further assume the signal $\alpha(t)$ to be bandwidth-limited to B and the splitting coefficients to be approximately constant over the bandwidth B, i.e.,

$$c_1(\omega) \approx c_1(\omega_0) \qquad c_2(\omega) \approx c_2(\omega_0) \qquad \forall\omega \in B, \tag{3.1.38}$$

the output state takes the simple form

$$\hat{U}|\alpha(t), 0\rangle = |c_1\alpha(t), c_2\alpha(t)\rangle \tag{3.1.39}$$

and the splitter only redistributes the signal power among the outputs while leaving the signal itself unaltered.

Equation (3.1.37) already suggests the similarity of the ideal optical splitter with an optical filter, the difference being that only one output matters for the optical filter. To remove the second output, we perform a partial trace over the second subsystem, equivalent to applying the projection operator to eq. (3.1.37), i.e.,

$$\hat{P}_1\hat{U}|\alpha(t), 0\rangle = |(h * \alpha)(t)\rangle \tag{3.1.40}$$

where we introduced the optical filter function $h = c_1$. Ref. [7, p. 199] discusses a spectral filter made of a dielectric slab of thickness l and refractive index n, see Figure 3.4, with incoming and outgoing quantum modes to each side. Let $\hat{a}_1(\omega)$ be the signal mode approaching the dielectric slab from the left. Let us assume that the mode $\hat{a}_2(\omega)$ is in vacuum and that we are only interested in the mode $\hat{a}_2'(\omega)$, outgoing to the right. Then the optical filter function in eq. (3.1.40) is equal to the transmission coefficient of the dielectric slab which is equal to [7, p. 199]

$$h(\omega) = \frac{1-r^2}{1-r^2\exp(2i\omega nl)}\exp\left[-i(n-1)l\omega\right] \qquad r^2 = \left(\frac{n-1}{n+1}\right)^2. \tag{3.1.41}$$

By carefully selecting the geometry and dielectric (layers), it should be possible to tailor the transmission coefficient in a specific bandwidth to implement a custom optical filter function h.

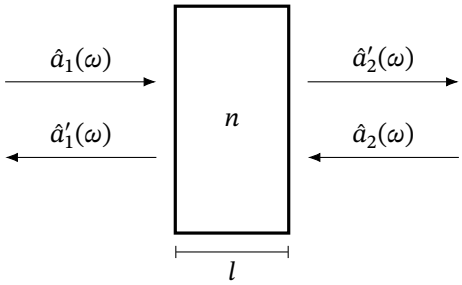


Figure 3.4.: Dielectric slab of thickness l and refractive index n used as a spectral filter with incident quantum modes, denoted by the annihilation operators, $\hat{a}_1(\omega)$ from the left, and $\hat{a}_2(\omega)$ from the right, and outgoing quantum modes, $\hat{a}_1'(\omega)$ to the left, and $\hat{a}_2(\omega)$ to the right.

3.2. Modulators

The (electro-optical) modulators allow encoding an electrical signal onto an optical carrier, and in that sense, are the interface between the electrical and optical domains. The domain crossover occurs at the electro-optical phase modulator, which we attempt to describe as a nonlinear-mixing process mediated by the dielectric. Following, we construct, in the optical domain, a complex amplitude modulator, or in-phase and quadrature modulator (IQM), using Mach-Zehnder interferometers (MZIs) driven by electro-optical phase modulators.

3.2.1. Phase modulator

In an electro-optical phase modulator, an electrical signal changes the refractive index of an optical transmission medium, causing a phase shift. The linear electro-optic effect, also known as the Pockels effect, characterizes a linear refractive index change proportional to the amplitude of an external electric field [89, Ch. 18]. It is present in noncentrosymmetric crystals [90, p. 2], e.g., lithium niobate [91, p. 237], commonly used in photonic integration. Figure 3.5 depicts a traveling-wave electro-optical phase modulator. The phase modulation signal is applied to the electrodes creating a traveling-wave RF field between the two electrodes. The linear-electro optical effect couples the different RF and optical frequency components. The output field contains sidebands, $\omega \pm \Omega_0$, at the modulation frequency, Ω_0.

The modulation frequency, Ω, is typically many magnitudes smaller than the optical frequency, ω, and the phase-shift due to the refractive index change appears static from the optical domain. In this case, we expect the complex amplitude of the optical signal leaving the phase modulator to be

$$\alpha'(t) = \alpha(t)e^{-i\varphi(t)}, \tag{3.2.1}$$

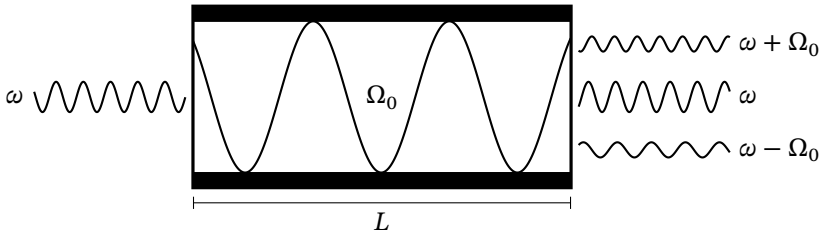


Figure 3.5.: Traveling-wave electro-optical phase modulator comprising two electrodes of length L (black). The electrodes are driven by a sinusoidal voltage signal creating an radio frequency (RF) field with frequency Ω_0 between the electrodes. An optical field with frequency ω reaches the phase modulator from the left, and an optical field with multiple frequency components, $\omega, \omega \pm \Omega_0$, exits the phase modulator to the right.

wherein $\alpha(t)$ is the initial amplitude and $\varphi(t)$ is some time-dependent phase. To a good approximation, the phase modulator is an LTI system for which the time-dependent phase signal is a convolution

$$\varphi(t) = (h * x)(t) = \int \mathrm{d}t'\, h(t')x(t - t') \tag{3.2.2}$$

with $h(t)$ being the linear time-response of the phase modulator system and $x(t)$ being the voltage signal driving the modulator. As a rough estimate of when the phase is effectively static concerning the optical field, we can compare the transmission time of the optical signal through the modulator with the period of the optical signal.[9]

While the former classical approach is perfectly sufficient, it does not fit well into our quantum-mechanical framework using interactions and unitary operators. In the following, we present the essence of Ref. [81] and Ref. [84] to get an insight into quantum-optical frequency-conversion. To simplify the discussion, we approximate the electric field (averages) inside the dielectric with free electric field operators at the cost of correctness relating to, e.g., phase-matching. One particular challenge regarding time-dependent phase modulation is that there exists no simple representation in the frequency domain for arbitrary modulation signals. The best we can do is assume a sinusoidal modulation, e.g.,

$$\varphi(t) = \beta_0 \sin(\Omega_0 t + \phi), \tag{3.2.3}$$

for which we can use the Jacobi-Anger expansion [84, eq. 23]

$$e^{-i\beta_0 \sin(\Omega_0 t + \phi)} = \sum_{m \in \mathbb{Z}} J_m(\beta_0) e^{-im(\Omega_0 t + \phi)} \tag{3.2.4}$$

wherein $J_m(\beta_0)$ is the mth Bessel function of the first kind. Inserting eq. (3.2.3) into eq. (3.2.1)

[9] The transmission time T is equal to the group velocity, $v_g(\omega)$, divided by the length of the modulator, L.

and performing the Jacobi-Anger expansion, we identify the Fourier transform with

$$\begin{aligned}\alpha'(\omega) &= \sum_{m\in\mathbb{Z}} J_m(\beta_0)e^{-im\phi}\int \mathrm{d}t\,\alpha(t)e^{-i(\omega+m\Omega_0)t} \\ &= \sum_{m\in\mathbb{Z}} J_m(\beta_0)e^{-im\phi}\alpha(\omega+m\Omega_0).\end{aligned} \tag{3.2.5}$$

Sinusoidal phase modulation with frequency Ω_0 creates infinitely many sidebands around the carrier frequency ω. As we can write an arbitrary time-dependent signal as a sum of sinusoidals of different frequencies, we have to deal with an integral of infinite sums, making arbitrary phase-modulation untractable.

Creating new frequency components requires a nonlinear interaction, not unlike the classical case, where a diode is used as a nonlinear element for frequency conversion. In Appendix B, we discuss nonlinear processes mediated by the electric susceptibility of a nonabsorptive dielectric and find the interaction Hamiltonian corresponding to frequency conversion to be

$$\hat{H}_{\mathrm{int}} = \int \frac{\mathrm{d}\omega}{2\pi}\int \frac{\mathrm{d}\Omega}{2\pi} g(\omega,\Omega)\hat{a}^\dagger(\omega)\hat{a}(\Omega)\hat{a}(\omega-\Omega) + \mathrm{H.c.}, \tag{3.2.6}$$

wherein $g(\omega,\Omega)$ encodes the geometry and properties of the dielectric material. The coupling parameter $g(\omega,\Omega)$ is only non-zero for ω being an optical and Ω being an electrical frequency. The operators in eq. (3.2.6) describe the simultaneous absorption of an "electric" photon with RF Ω, $\hat{a}(\Omega)$, and an "optical" photon with frequency $\omega-\Omega$, $\hat{a}(\omega-\Omega)$, to create an "optical" photon at a higher frequency ω, $\hat{a}^\dagger(\omega)$. We are not interested in the quantum properties of the RF field and assume it to be in a coherent state with complex amplitude $\beta(t)$

$$\hat{H}_{\mathrm{int}} = \int \frac{\mathrm{d}\omega}{2\pi}\int \frac{\mathrm{d}\Omega}{2\pi} g(\omega,\Omega)\beta(\Omega)\hat{a}^\dagger(\omega)\hat{a}(\omega-\Omega) + \mathrm{H.c.}, \tag{3.2.7}$$

wherein $\beta(\Omega)$ is the Fourier amplitude corresponding to $\beta(t)$. A sinusoidal modulation signal has a single frequency component,

$$\beta(t) = \beta_0 e^{i\Omega_0 t} \qquad\qquad \beta(\Omega) = \beta_0(2\pi)\delta^{(1)}(\Omega-\Omega_0), \tag{3.2.8}$$

Inserting the frequency representation of the sinusoidal modulation into the interaction Hamiltonian, eq. (3.2.7), we find

$$\hat{H}_{\mathrm{int}} = \beta_0\int \frac{\mathrm{d}\omega}{2\pi} g(\omega,\Omega_0)\hat{a}^\dagger(\omega)\hat{a}(\omega+\Omega_0) + \mathrm{H.c.}. \tag{3.2.9}$$

Let the optical signal be limited to the bandwidth B, then according to the mean-value theorem for integrals, there exists an $\omega_0 \in B$ such that we can write

$$\begin{aligned}\hat{H}_{\mathrm{int}} &= \beta_0 g(\omega_0,\Omega_0)\int \frac{\mathrm{d}\omega}{2\pi}\hat{a}^\dagger(\omega)\hat{a}(\omega+\Omega_0) + \beta_0^* g(\omega_0,\Omega_0)^*\int \frac{\mathrm{d}\omega}{2\pi}\hat{a}^\dagger(\omega)\hat{a}(\omega-\Omega_0) \\ &= \beta_0 g(\omega_0,\Omega_0)\int \frac{\mathrm{d}\omega}{2\pi}\hat{a}^\dagger(\omega-\Omega_0)\hat{a}(\omega) + \beta_0^* g(\omega_0,\Omega_0)^*\int \frac{\mathrm{d}\omega}{2\pi}\hat{a}^\dagger(\omega+\Omega_0)\hat{a}(\omega)\end{aligned} \tag{3.2.10}$$

where we performed an integration variable substitution in the second step.

We define the up- and downconversion operators for the frequency Ω_0 as

$$\hat{T}_{\pm}(\Omega_0) = \int \frac{\mathrm{d}\omega}{2\pi} \hat{a}^{\dagger}(\omega \pm \Omega_0)\hat{a}(\omega) \tag{3.2.11}$$

which are related via the Hermitian conjugate, $\hat{T}_{+}(\Omega_0) = \hat{T}_{-}(\Omega_0)^{\dagger}$, and satisfy the commutation relations

$$[\hat{T}_{\pm}(\Omega_0), \hat{a}(\omega)] = -\hat{a}(\omega \mp \Omega_0) \qquad [\hat{T}_{\pm}(\Omega_0), \hat{a}^{\dagger}(\omega)] = +\hat{a}^{\dagger}(\omega \pm \Omega_0), \tag{3.2.12}$$

which can be used to up- or donwconvert the frequency of a photon by Ω_0.

The time-evolution operator corresponding to the interaction Hamiltonian in eq. (3.2.10) turns out to be

$$\hat{U}(\theta, \Omega_0, \varphi) = \exp\{-iT\hat{H}_{\mathrm{int}}\} = \exp\left\{-i\frac{1}{2}\theta\left[\hat{T}_{+}(\Omega_0)e^{-i\varphi} + \hat{T}_{-}(\Omega_0)e^{+i\varphi}\right]\right\} \tag{3.2.13}$$

where we new parameters Θ, φ relate to the old coupling parameters via

$$\beta_0^* g(\omega_0, \Omega_0)^* T = \frac{1}{2}\theta e^{+i\varphi} \tag{3.2.14}$$

with T being the interaction time approximately equal to the transmit time of the light through the phase modulator.[10] Before, we transform the annihilation operator, we define the generator

$$\hat{G}(\varphi, \Omega_0) = \hat{T}_{+}(\Omega_0)e^{-i\varphi} + \hat{T}_{-}(\Omega_0)e^{+i\varphi} \tag{3.2.15}$$

which relates to the evolution operator via

$$\hat{U}(\theta, \Omega_0, \varphi) = \exp\left\{-i\frac{1}{2}\theta\hat{G}(\varphi, \Omega_0)\right\}. \tag{3.2.16}$$

The iterated commutators of the generator with the annihilation operator are

$$[\hat{G}, \hat{a}(\omega)] = (-1)\left[\hat{a}(\omega - \Omega_0)e^{-i\varphi} + \hat{a}(\omega + \Omega_0)e^{+i\varphi}\right] \tag{3.2.17}$$

$$[\hat{G}, [\hat{G}, \hat{a}(\omega)]] = (-1)^2\left[\hat{a}(\omega - 2\Omega_0)e^{-2i\varphi} + 2\hat{a}(\omega) + \hat{a}(\omega + 2\Omega_0)e^{+2i\varphi}\right] \tag{3.2.18}$$

$$[\hat{G}, [\hat{G}, [\hat{G}, \hat{a}(\omega)]]] = (-1)^3\big[\hat{a}(\omega - 3\Omega_0)e^{-3i\varphi} + 2^2\hat{a}(\omega - \Omega_0)e^{-i\varphi} \tag{3.2.19}$$

$$+ \hat{a}(\omega + 3\Omega_0)e^{+3i\varphi} + 2^2\hat{a}(\omega + \Omega_0)e^{+i\varphi}\big] \tag{3.2.20}$$

and we can invoke the BCH formula, to transform the annihilation operator

$$\begin{aligned}\hat{a}'(\omega) &= \hat{U}(\theta, \Omega_0, \varphi)^{\dagger}\hat{a}(\omega)\hat{U}(\theta, \Omega_0, \varphi) \\ &= \hat{a}(\omega) + \frac{i\theta}{2}[\hat{G}, \hat{a}(\omega)] + \frac{i^2\theta^2}{2^2 2!}[\hat{G}, [\hat{G}, \hat{a}(\omega)]] + \frac{i^3\theta^3}{2^3 3!}[\hat{G}, [\hat{G}, ...]] + ... \\ &= \sum_{m\in\mathbb{Z}} J_m(\theta)e^{im(\varphi - \pi/2)}\hat{a}(\omega + m\Omega_0)\end{aligned} \tag{3.2.21}$$

[10] Strictly speaking, the transmit time is frequency-dependent requiring a frequency response filter instead of coupling constant.

in agreement with Ref. [84, eq. 40].

To transform the displacement operator, we need to evaluate

$$\begin{aligned}\hat{U}(\theta,\Omega_0,\varphi)\hat{a}^\dagger(\omega)\hat{U}(\theta,\Omega_0,\varphi)^\dagger &= \left[\hat{U}(\theta,\Omega_0,\varphi)\hat{a}(\omega)\hat{U}(\theta,\Omega_0,\varphi)^\dagger\right]^\dagger \\ &= \left[\hat{U}(-\theta,\Omega_0,\varphi)^\dagger\hat{a}(\omega)\hat{U}(-\theta,\Omega_0,\varphi)\right]^\dagger \\ &= \left[\sum_{m\in\mathbb{Z}} J_m(-\theta)e^{+im(\varphi-\pi/2)}\hat{a}(\omega+m\Omega_0)\right]^\dagger \\ &= \sum_{m\in\mathbb{Z}} J_m(-\theta)e^{-im(\varphi-\pi/2)}\hat{a}^\dagger(\omega+m\Omega_0) \\ &= \sum_{m\in\mathbb{Z}} J_m(\theta)e^{+im(\varphi+\pi/2)}\hat{a}^\dagger(\omega+m\Omega_0)\end{aligned} \tag{3.2.22}$$

where we used

$$J_m(-\theta)e^{-im(\varphi-\pi/2)} = (-1)^m J_m(\theta)e^{+im(\varphi-\pi/2)} = J_m(\theta)e^{+im(\varphi+\pi/2)} \tag{3.2.23}$$

in the last step. The transformed displacement operator then reads

$$\begin{aligned}\hat{D}'\left[\alpha(t)\right] &= \hat{U}(\theta,\Omega_0,\varphi)\hat{D}\left[\alpha(t)\right]\hat{U}(\theta,\Omega_0,\varphi)^\dagger \\ &= \exp\left\{\int\frac{\mathrm{d}\omega}{2\pi}\left[\alpha(\omega)\hat{U}(\theta,\Omega_0,\varphi)\hat{a}^\dagger(\omega)\hat{U}(\theta,\Omega_0,\varphi)^\dagger - \text{H.c.}\right]\right\} \\ &= \exp\left\{\int\frac{\mathrm{d}\omega}{2\pi}\left[\sum_{m\in\mathbb{Z}}\alpha(\omega)J_m(\theta)e^{+im(\varphi+\pi/2)}\hat{a}^\dagger(\omega+m\Omega_0) - \text{H.c.}\right]\right\} \\ &= \exp\left\{\int\frac{\mathrm{d}\omega}{2\pi}\left[\sum_{m\in\mathbb{Z}}J_m(\theta)\alpha(\omega-m\Omega_0)e^{im(\varphi+\pi/2)}\hat{a}^\dagger(\omega) - \text{H.c.}\right]\right\} \\ &= \exp\left\{\int\frac{\mathrm{d}\omega}{2\pi}\left[\alpha'(\omega)\hat{a}^\dagger(\omega) - \text{H.c.}\right]\right\}\end{aligned} \tag{3.2.24}$$

where we identified the transformed Fourier amplitude with

$$\alpha'(\omega) = \sum_{m\in\mathbb{Z}} J_m(\theta)e^{im(\varphi+\pi/2)}\alpha(\omega-m\Omega_0). \tag{3.2.25}$$

Written as a convolution, the transformed Fourier amplitude reads

$$\alpha'(\omega) = \int\frac{\mathrm{d}\omega'}{2\pi}h(\omega')\alpha(\omega-\omega'), \tag{3.2.26}$$

where the convolution kernel is the Dirac train

$$\sum_{m\in\mathbb{Z}} J_m(\theta)e^{im(\varphi+\pi/2)}(2\pi)\delta^{(1)}(\omega'-m\Omega_0). \tag{3.2.27}$$

As the transformed Fourier amplitude is a convolution in frequency space, we expect a product in time space, i.e.,

$$\begin{aligned}\alpha'(t) = \int \frac{\mathrm{d}\omega}{2\pi}\alpha'(\omega)e^{-i\omega t} &= \int \frac{\mathrm{d}\omega}{2\pi}\alpha(\omega - m\Omega_0)e^{-i\omega t}\sum_{m\in\mathbb{Z}} J_m(\theta)e^{im(\varphi+\pi/2)} \\ &= \int \frac{\mathrm{d}\omega}{2\pi}\alpha(\omega)e^{-i\omega t}\sum_{m\in\mathbb{Z}} J_m(\theta)e^{-im(\Omega_0 t-\varphi-\pi/2)} \\ &= \alpha(t)e^{-i\theta\sin(\Omega_0 t-\varphi-\pi/2)} = \alpha(t)e^{+i\theta\cos(\Omega_0 t-\varphi)}\end{aligned} \tag{3.2.28}$$

where we again used the Jacobi-Anger expansion, eq. (3.2.4). We conclude that a coherent state transform under sinusoidal phase-modulation as

$$\hat{U}(\theta,\Omega_0,\varphi)|\alpha(t)\rangle = \left|\alpha(t)e^{+i\theta\cos(\Omega_0 t-\varphi)}\right\rangle. \tag{3.2.29}$$

To extend our result to signals of finite duration, we first note that we can write such a signal as a sum of harmonics, i.e.,

$$\varphi(t) = \sum_{k=0}^{N}\theta_k\cos(\Omega_k t-\varphi_k), \tag{3.2.30}$$

and apply a product of sinusoidal phase modulation operators, eq. (3.2.13),

$$\left(\prod_{k=0}^{N}\hat{U}(\theta_k,\Omega_k,\varphi_k)\right)|\alpha(t)\rangle = \left|\alpha(t)e^{+i\varphi(t)}\right\rangle, \tag{3.2.31}$$

which corresponds to having a different sinusoidal phase modulators in sequence. For different frequencies in the same phase modulator, we have the problem that they all interact. That said, it should be possible to generalize the frequency up- and downconversion operators to a spectrum and argue that the commutator between the generator, eq. (3.2.15), and the annihilation operator vanishes except for the dominant frequency components.

3.2.2. Amplitude modulator

The Mach-Zehnder modulator (MZM) uses two phase modulators to perform amplitude modulation through interference. Figure 3.6 shows a symmetric MZI[11] using free-space optics with one signal input; the other input being in the vacuum state. The most crucial components of the MZI are a splitter, a coupler, and two independent phase modulators. The splitter divides the input light into two branches, which are phase modulated with $\phi_1(t)$ and $\phi_2(t)$ by PM1 respectively PM2. The coupler recombines both branches into two outputs. Two cubic beam splitters implement the splitter (BS1) and the coupler (BS2) for our free-space setup. For additional beam alignment, our free-space setup utilizes two mirrors (M1 and M2).

[11] We distinguish between MZI and MZM, whether it is an optical MZI or integrated MZM embodiment. However, there is no difference in the theoretical treatment.

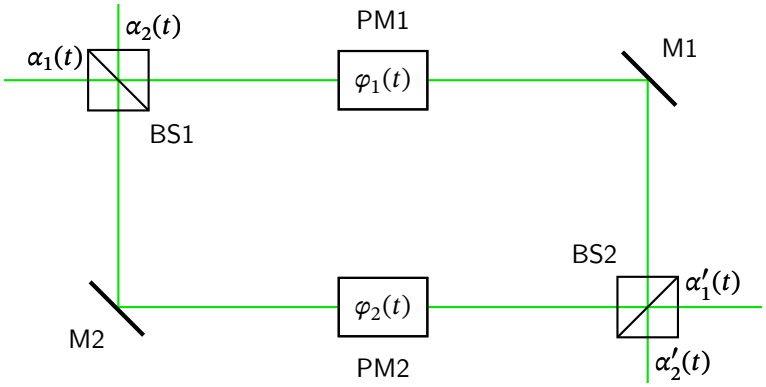


Figure 3.6.: Symmetric MZI using free-space optics comprising two balanced beam splitter (BS), BS1 and BS2, two mirrors, M1 and M2, and two phase modulators, PM1 and PM2. The input amplitudes, $\alpha_1(t)$ and $\alpha_2(t)$, enter BS1 and are split into an upper and lower path. The upper path receives a phase shift of $\phi_1(t) + \pi$ from PM1 and M1 before entering BS2 from the top. The lower path receives a phase shift of $\phi_2(t) + \pi$ from M2 and PM2 before entering BS2 from the left. BS2 recombines the phase-shifted upper and lower path into the output Fourier amplitudes $\alpha_1'(t)$ and $\alpha_2'(t)$.

To find the effect of the MZM on an input coherent-state, we study the cumulative effect of the individual optical components. One particular challenge is that the transformation of passive components is a convolution in the time domain. In contrast, the transformation of active components is a convolution in the frequency domain. A possible way forward is to invoke the narrow-bandwidth approximation and assume that the passive components are free of dispersion over the relevant optical bandwidth. Under this simplifying assumption, the passive components are described by the ideal transformations

$$U_{\mathrm{BS1}} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \qquad U_{\mathrm{BS2}} = \frac{1}{\sqrt{2}}\begin{pmatrix} i & 1 \\ 1 & i \end{pmatrix}, \tag{3.2.32}$$

which are valid in both time and frequency space.[12] The transformation of the active phase modulation is

$$U_{\mathrm{PM}}(t) = \begin{pmatrix} e^{i\phi_1(t)} & 0 \\ 0 & e^{i\phi_2(t)} \end{pmatrix}, \tag{3.2.33}$$

where we ignored static phase shifts.[13] The composition of these transformations yields the transformation of the MZM

$$U_{\mathrm{MZM}}(t) = U_{\mathrm{BS2}} U_{\mathrm{PM}}(t) U_{\mathrm{BS1}} = \begin{pmatrix} \cos\phi_-(t) & +\sin\phi_-(t) \\ -\sin\phi_-(t) & \cos\phi_-(t) \end{pmatrix} i e^{i\varphi_+(t)}, \tag{3.2.34}$$

[12] The particular choice corresponds to a perfect cubic beam splitter with a single dielectric layer [4, p. 139], where we exchanged the rows of the second BS for consistency with the input labels.

[13] For practical applications, one calibrates the phase modulators with a static bias voltage to compensate for undesired static phase shifts.

where we introduced the common-mode and differential-mode phase signals

$$\phi_+(t) = \frac{\phi_2(t) + \phi_1(t)}{2} \qquad \phi_-(t) = \frac{\phi_2(t) - \phi_1(t)}{2}. \tag{3.2.35}$$

For the input state being a tensor product of a coherent and a vacuum state

$$|\boldsymbol{\alpha}(t)\rangle = |\alpha(t), 0\rangle, \tag{3.2.36}$$

the matrix transformation of the MZM, eq. (3.2.34), predicts the output amplitudes to be

$$\alpha'(t) = U_{\mathrm{MZM}}(t)\alpha(t) = \alpha(t)\begin{pmatrix} \cos\phi_-(t) \\ -\sin\phi_-(t) \end{pmatrix} ie^{i\varphi_+(t)} \tag{3.2.37}$$

where the common-mode phase signal $\varphi_+(t)$ changes the global phase of the output signal and the differential-mode signal $\varphi_-(t)$ changes the power splitting ratio of the outputs. In the previous sections, we derived the unitary evolution operator corresponding to the unitary matrix transforms. We therefore claim the existence of an unitary operator, $\hat{U}_{\mathrm{MZM}}$, corresponding to the unitary matrix transform of eq. (3.2.34), where the action of such operator on a coherent and vacuum input state is

$$\hat{U}_{\mathrm{MZM}}(t)|\alpha(t), 0\rangle = \left|\alpha(t)\cos\phi_-(t)ie^{i\varphi_+(t)}, \alpha(t)\sin\phi_-(t)ie^{i\varphi_+(t)}\right\rangle. \tag{3.2.38}$$

Usually, one output is monitored for bias control of the phase modulators, and the other output is used for further processing. In this case, we can remove the other other output using a projection operator, $\hat{P}$, and we find

$$\hat{P}\hat{U}_{\mathrm{MZM}}(t)|\alpha(t), 0\rangle = |\alpha(t)\beta_{\mathrm{MZM}}(t)\rangle, \tag{3.2.39}$$

where we defined the complex-valued amplitude modulation signal $\beta(t)$ with $|\beta(t)| \leq 1$.

Equation (3.2.39) suggests that a MZM with two independent phase modulators allows for complex amplitude modulation, i.e., modulation of in-phase and quadrature components of the input signal $\alpha(t)$. In practice, however, we implement the IQM using three MZMs as depicted in Figure 3.7. The phases of the MZM in an integrated IQM are only driven differentially. The upper branch modulates the in-phase component, $I(t)$, while the lower branch modulates the quadrature component, $Q(t)$. A third MZM adds a static relative phase Λ between the in-phase and quadrature branch such that these branches are recombined at $\pi/2$. For the output coherent-state, we find

$$|\alpha'(t)\rangle = \hat{U}_{\mathrm{IQM}}(t)|\alpha(t)\rangle = \left|\alpha(t)\beta_{\mathrm{IQM}}(t)\right\rangle \tag{3.2.40}$$

wherein the complex amplitude-modulation signal is now

$$\beta_{\mathrm{IQM}}(t) = I(t) + iQ(t). \tag{3.2.41}$$

While the IQM is equivalent to a MZM with two independent phase modulators for time-independent modulation, the MZM cannot, in general, perform continuously phase modulation. The reason being that the complex phase of the MZM, eq. (3.2.37), cannot be increased arbitrary for practical electro-optical phase modulators but must be brought back to some working point, which would require instantaneous jumps.

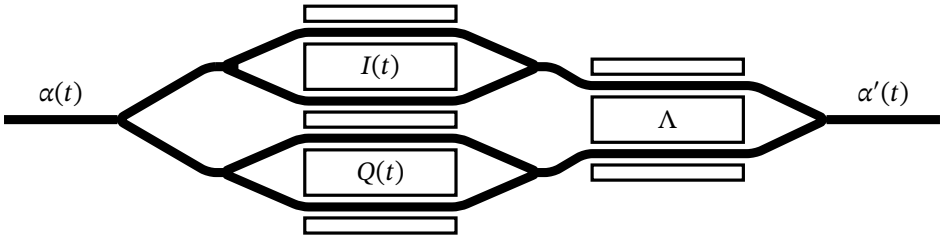


Figure 3.7.: Integrated IQM using three MZM arms. An input signal with amplitude $\alpha(t)$ is split into an upper and lower branch. The upper and lower branches comprise an integrated MZM that performs amplitude modulation with the in-phase and quadrature signal, $I(t)$ respectively $Q(t)$. The integrated MZM consists of a hexagonal-shaped waveguide with an inside signal electrode and two outer grounds. The outputs of the in-phase- and quadrature-modulated form a third MZM used to set a relative phase of Λ between the in-phase and quadrature signals, yielding an output signal with amplitude $\alpha'(t)$.

3.3. Photodetectors

The photodetectors let us probe the quantum-optical states via an electrical signal. In the following, we will briefly review the results of the photodetection theory according to Refs. [8, 26] and then take a closer look at the direct and balanced detector.

3.3.1. Photoelectric effect

The photoelectric effect describes the emission of electrons from an illuminated material. Historically, it provided strong evidence for the existence of a light quantum, the photon, as the kinetic energy of the emitted electrons,

$$E_k = E_\gamma - E_w, \tag{3.3.1}$$

does not depend on the intensity but on the frequency, $E_\gamma = \omega$, of the incident light minus some work energy, E_w. The photoelectric effect relates the momentum spectrum of electrons with the frequency spectrum of photons and provides a mechanism for photodetection. We present two kinds of photodetectors exploiting the photoelectric effect: the phototube and the photodiode.

A phototube (Figure 3.8) comprises a metallic cathode and a biased anode parallel to the cathode. Whenever photons with energy $\omega > E_w$, wherein E_w is the work energy of the cathode, hit eject an electrode, the anode accelerates the emitted electrons away from the cathode. The cathode is then in excess of positive charge carriers, creating a positive current, I.

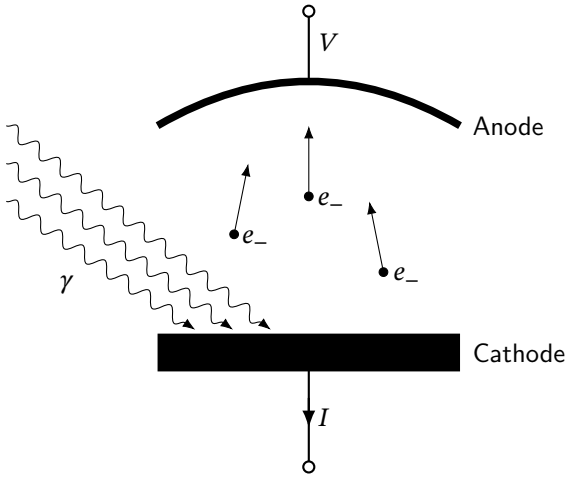


Figure 3.8.: Schematic of a phototube, a vacuum tube utilizing the photoelectric effect for photodetection. Photons, γ, hit a metallic cathode and eject electrons, $e\_$, through the photoelectric effect. The anode is biased with a positive voltage, $V > 0$, to attract the emitted electrons. The cathode is in excess of positive charge carriers, creating a positive electric current, $I > 0$.

Contrary, a photodiode is typically made of a PN-junction (Figure 3.9), a junction of a positively- (P) with a negatively-doped (N) semiconductor, supplemented by a contact on the P- and a contact on the N-doped semiconductor. The contact at the P-doped semiconductor is negatively charged, creating a depletion layer between the PN-junction with no free charge carriers. The P layer absorbs incident photons, γ, exciting electrons, which accelerate through the depletion layer towards the cathode, creating the photocurrent, I. Contrary to the phototube, the excited electrons are not truly free but rather excited to an energy band, where they move with higher mobility through the semiconductor. That said, the central idea of exciting photoelectrons through photon absorption to some higher energy, applies to both kinds of photodetectors [92, p. 128].

We will oversee the subtile differences and assume a single photoelectron bound to a single atom in a unique ground state, $|g\rangle$, which is excited through photon absorption to some excited state continuum, $|e\rangle$.[14] The Hamiltonian of an electron is

$$\hat{H}_e = \frac{\hat{\mathbf{p}}^2}{2m_e} + V(\hat{\mathbf{x}}), \tag{3.3.2}$$

wherein $V(\hat{\mathbf{x}})$ denotes the binding potential. We expect the ground state, $|g\rangle$, to be an energy eigenstate with eigenvalue, E_g. In the ground state, $|g\rangle$, the electron is bound and dominated by the potential term in the Hamiltonian. In an excited state, $|e\rangle$, the electron is approximately free and dominated by the kinetic term in the Hamiltonian. Figure 3.10 shows the

[14] Quantum models for photon absorption specific to semiconductors are found in Ref. [93] and Ref. [94].

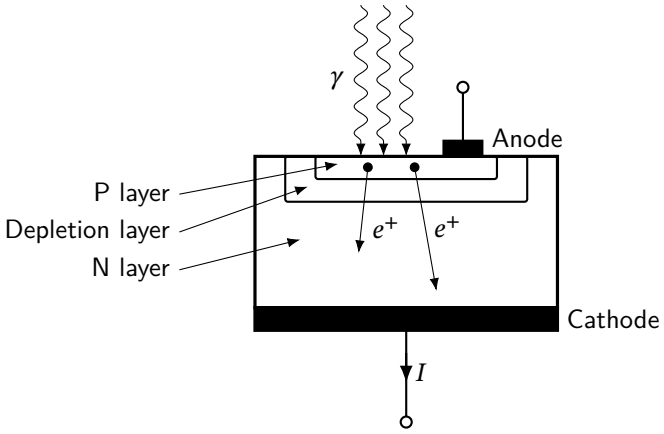


Figure 3.9.: Schematic of a photodiode, a PN-junction. The P layer absorbs incident photons, γ, exciting electrons, e_-, and holes, e_+. The electrons are accelerated towards the anode (not shown), and the holes are accelerated towards the cathode, creating a photocurrent I.

corresponding energy level diagram. The ground state, $|g\rangle$, is unique and has the single energy E_g. For the excited state, $|e\rangle$, an energy continuum exists with energies ranging from $\min_e E_e$ to $\max_e E_e$. The difference of the lowest excited energy, $\min_e E_e$, and the ground state energy, E_g, is equivalent to the bandgap energy inside a semiconductor. The transition from the ground to an excited state, $|g\rangle \rightarrow |e\rangle$, through photon absorption requires the photon energy, ω, to be at least the bandgap energy, $\omega \geq \min_e E_e - E_g$. In Appendix C we extend the photoelectron model to derive the differential probability for photoelectron emission.

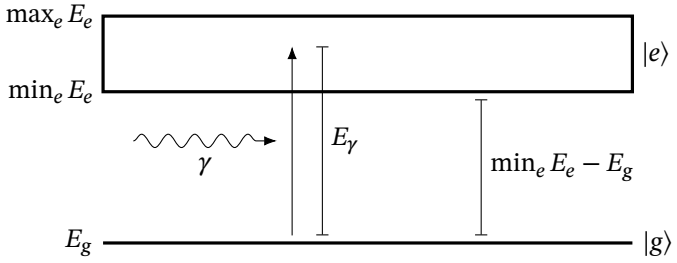


Figure 3.10.: Energy level diagram of a photoelectron excited from a bound ground state, $|g\rangle$, with energy E_g to a free excited state, $|e\rangle$, with energy E_e by absorbing a photon with energy E_γ. To excite the electron from the ground state the photon must have at least the energy of the bandgap, $\min_e E_e - E_g$, wherein $\min_e E_e$ is the minimum energy of the excitation energy band.

3.3.2. Photocurrent operator

Ref. [8, p. 725] generalizes the differential probability for a single photoelectron excitation to the positive operator-valued measure (POVM) of counting m photoelectrons from infinitely many independent detector atoms from time t to $t + T$ as[15]

$$\hat{P}_m(t,T) = \mathcal{T}_+ : \frac{1}{m!}\hat{I}(t,T)^m \exp\left\{-\hat{I}(t,T)\right\} :, \tag{3.3.3}$$

wherein the photocurrent operator is equal to the integrated equal-time correlation function of the electric field,[16]

$$\hat{I}(t,T) = \eta \int_t^{t+T} \mathrm{d}t' \langle \hat{E}^{(+)}(t')\hat{E}^{(-)}(t')\rangle \tag{3.3.4}$$

with detector efficiency constant η. From a signal-processing perspective, it is more natural to define a detector response function, $\eta(t)$, which generalizes the measurement period T and is experimentally accessible. The convolved photocurrent operator,

$$\hat{I}(t) = \eta \int \mathrm{d}t'\, \eta(t')\langle \hat{E}^{(+)}(t-t')\hat{E}^{(-)}(t-t')\rangle, \tag{3.3.5}$$

reduces to the integrated photocurrent operator, eq. (3.3.4), when using a constant step response for the detector. From here on, we use the eq. (3.3.3) with the convolved photocurrent operator, eq. (3.3.5).

[15] If we assume no sources present inside the detector, the fields are approximately free at the detector, and we can neglect the time-ordering in eq. (3.3.6) [7, p. 183].

[16] In Ref. [8] the photocurrent operator is equal to the equal-time correlation function of the Maxwell field. The electric and Maxwell field operator are connected by an unitary transformation.

Using the generating function of the photoelectron POVM, eq. (3.3.3), we find the average number of photoelectrons emitted at t to be [7, p. 183]

$$\overline{n(t)} = \sum_{m \in \mathbb{N}_0} m \langle \hat{P}_m(t) \rangle = \langle \hat{I}(t) \rangle. \tag{3.3.6}$$

For the variance, we find [8, p. 736]

$$\overline{(\Delta n(t))^2} = \overline{n(t)} + \langle \left(\Delta \hat{I}(t)\right)^2 \rangle, \tag{3.3.7}$$

wherein $\langle \left(\Delta \hat{I}(t)\right)^2 \rangle$ denotes the variance of the bandwidth-limited intensity operator, eq. (3.3.5), which can become negative indicating sub-Poissionian statistics for certain quantum states.

3.3.3. Direct detector

The direct detector resembles a power or intensity measurement of the optical state, so it is also sometimes called a square-law detector. Figure 3.11 presents the electronic schematic of a direct-detector circuit. A photodiode, PD, is reverse biased with voltage $-V_b < 0$ to reduce the response time of the photodiode. Under optical illumination, PD produces a photocurrent, $i(t)$, which in natural units is equal to the mean photoelectron number, eq. (3.3.6). For

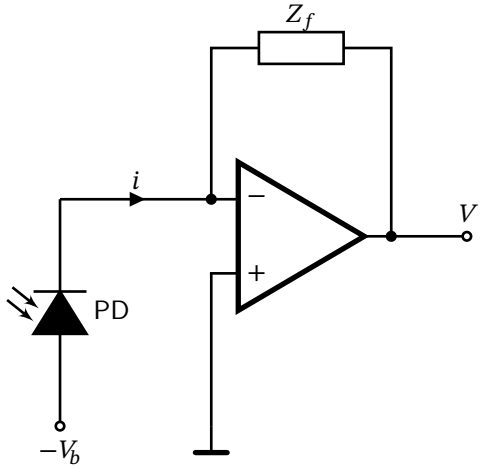


Figure 3.11.: Electronic schematic of a direct (intensity) detector comprising a photodiode and an operational amplifier with a transimpedance amplifier (TIA) frontend. The anode of the photodiode is reverse biased with voltage $-V_b < 0$. The cathode of the photodiode emits the photocurrent i and is connected to the inverting input of the operational amplifier. The non-inverting input of the operational amplifier is connected with ground, while the inverting input is coupled with feedback impedance Z_f to the operational amplifier output voltage, V.

a coherent state, $|\alpha(t)\rangle$, we find the mean photocurrent to be equal to the power of the signal, $|\alpha(t)|^2$, convolved with the detector response function,

$$i(t) = \int \mathrm{d}t'\, \eta(t')|\alpha(t-t')|^2 = \left(\eta * |\alpha|^2\right)(t). \tag{3.3.8}$$

Assuming an ideal operational amplifier, the TIA outputs the voltage signal proportional to the feedback impedance

$$V_p(t) = -Z_f i_p(t). \tag{3.3.9}$$

More realistically, we expect the response of the TIA to be characterized by a frequency-response function h, and the output voltage is given by

$$V_p(t) = (h * i)(t) = \left(h * \eta * |\alpha|^2\right)(t). \tag{3.3.10}$$

In eq. (3.3.10), we find the absolute square of the signal to be convolved with the detector response-function and the response function of the TIA, which can be summarized into one effective response-function.

3.3.4. Balanced detector

To obtain information about the quadratures of the signal, we can mix the optical signal with a local oscillator (LO) and measure the mixer outputs with two direct detectors in a balanced configuration. Figure 3.12 shows a possible arrangement of electro-optical components for balanced detection. Assuming a perfectly-balanced beam splitter over the optical bandwidths, we find the output amplitudes to be

$$\alpha_\pm(t) = \frac{1}{\sqrt{2}}\left[\alpha_s(t) \pm \alpha_l(t)\right], \tag{3.3.11}$$

where we choose the phase properties of the beam splitter for notational convenience.[17] Figure 3.13 shows the electrical setup of the two photodiodes, PD1 and PD2. PD1 and PD2 are both reverse biased to reduce the response time and connected to each other to directly produce a difference photocurrent signal,

$$\begin{aligned} i(t) = i_+(t) - i_-(t) &= \left(\eta * \left[|\alpha_+|^2 - |\alpha_-|^2\right]\right)(t) \\ &= \left(\eta * \left[\alpha_s\alpha_l^* + \alpha_s^*\alpha_l\right]\right)(t) \\ &= \left(\eta * 2\,\mathrm{Re}\left[\alpha_s\alpha_l^*\right]\right)(t), \end{aligned} \tag{3.3.12}$$

[17] In practice, the phase properties of the optical coupler, as well as the input fields, are not well-known, and must be corrected.

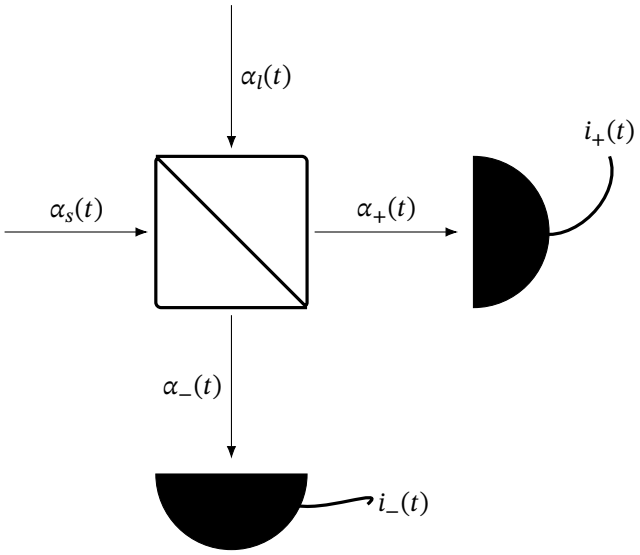


Figure 3.12.: Electro-optical setup of a balanced detector comprising a beam splitter and two photodetectors. The beam splitter superimposes the signal and LO fields, $\alpha_s(t)$ and $\alpha_l(t)$, to the output fields $\alpha_\pm(t)$, each monitored by a photodiode with output current $i_\pm(t)$.

wherein we used the linearity of the convolution and inserted eq. (3.3.11). We rewrite the product of the input and LO signal to equal

$$\begin{aligned}\alpha_s(t)\alpha_l(t)^* = \alpha(t)e^{-i(\omega_l t-\vartheta)} &= \int_{-\infty}^{+\infty}\frac{\mathrm{d}\omega}{2\pi}\alpha(\omega)e^{+i\omega t}e^{-i(\omega_l t-\vartheta)}\\ &= \int_{-\infty}^{+\infty}\frac{\mathrm{d}\omega}{2\pi}\alpha(\omega+\omega_l)e^{+i(\omega t+\vartheta)},\end{aligned} \tag{3.3.13}$$

wherein we redefined the signal amplitude

$$\alpha(t) = \alpha_s(t)g(t)^* \tag{3.3.14}$$

to include the linewidth profile $g(t)$ of the LO signal $\alpha_l(t) = g(t)e^{-i(\omega_l t-\vartheta)}$.[18]. Inserting eq. (3.3.13) into eq. (3.3.12), we find

$$i(t) = 2\,\mathrm{Re}\left[\eta * (\alpha_s\alpha_l^*)\right](t) = 2\,\mathrm{Re}\int_{-\infty}^{+\infty}\frac{\mathrm{d}\omega}{2\pi}\eta(\omega+\omega_l)\alpha(\omega+\omega_l)e^{+i(\omega t+\vartheta)}. \tag{3.3.15}$$

Assuming the detector response-function $\eta(\omega)$ to be constant over the detector bandwidth B_d, eq. (3.3.15) simplifies to

$$i(t) \propto 2\,\mathrm{Re}\int_{-B_d/2}^{+B_d/2}\frac{\mathrm{d}\omega}{2\pi}\alpha(\omega+\omega_l)e^{+i(\omega t+\vartheta)}. \tag{3.3.16}$$

[18]For instance, $g(t) \propto e^{-\gamma t/2}$ for a Lorentzian profile, see Ref. [95].

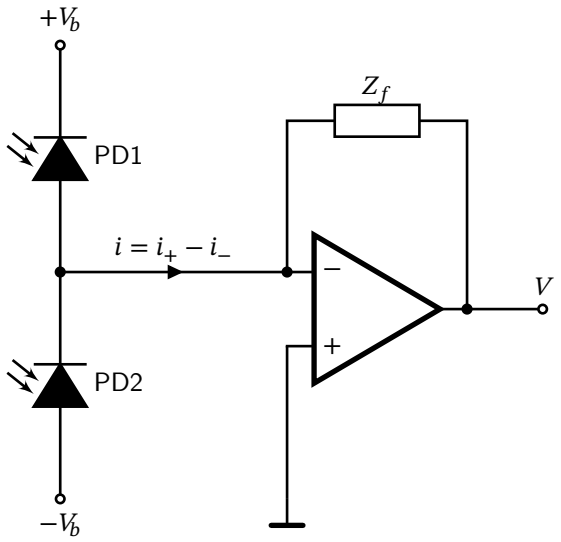


Figure 3.13.: Electronic schematic of a balanced (quadrature) detector comprising two photodiodes and an operational amplifier in TIA configuration. The cathode of the first photodiode, PD1, is reverse biased with voltage $+V_b > 0$. The cathode of the second photodiode, PD2, is reverse biased with voltage $-V_b < 0$. The cathode of PD1 and the anode of PD2 are connected to supply the difference photocurrent signal, $i(t) = i_+(t) - i_-(t)$, to the inverting input of the operational amplifier. The non-inverting input of the operational amplifier is connected to ground. The inverting input is coupled to the output through the feedback impedance Z_f. The TIA outputs a voltage signal $V(t)$ proportional to the difference photocurrent signal $i(t)$.

Comparing our final result for the photocurrent, eq. (3.3.15), with the expectation value of the quadrature operator for the coherent state $|\alpha(t)\rangle$,

$$\langle\alpha(t)|\hat{X}(t)|\alpha(t)\rangle = \int_{-\infty}^{+\infty} \frac{\mathrm{d}\omega}{2\pi} \left[\beta(\omega)e^{-i\omega t} + \text{c.c.}\right] = 2\,\mathrm{Re}\int_{-\infty}^{+\infty} \frac{\mathrm{d}\omega}{2\pi}\beta(\omega)e^{-i\omega t}, \tag{3.3.17}$$

we note that the quadrature operator lacks the notion of a downconversion frequency and phase as well as a bandwidth. Fortunately, we already derived a unitary frequency-conversion operator in our treatment of the phase modulator, eq. (3.2.13). Transforming the quadrature operator with the frequency-conversion operator $\hat{U}_{\mathrm{FC}}$,

$$\begin{aligned}\hat{U}_{\mathrm{FC}}^\dagger \hat{X}(t)\hat{U}_{\mathrm{FC}} &= \int_{-\infty}^{+\infty} \frac{\mathrm{d}\omega}{2\pi} \left[\hat{U}_{\mathrm{FC}}^\dagger \hat{a}(\omega)\hat{U}_{\mathrm{FC}}e^{-i\omega t} + \text{H.c.}\right] \\ &= \sum_{m\in\mathbb{Z}} J_m(\theta) \int_{-\infty}^{+\infty} \frac{\mathrm{d}\omega}{2\pi} \left[\hat{a}(\omega + m\omega_l)e^{-i(\omega t + m\vartheta)} + \text{H.c.}\right],\end{aligned} \tag{3.3.18}$$

creates not only the downconversion frequency ω_l but also all of its harmonics. To remove the harmonics, we add a reservoir to the detection system, which we assume to be in the vac-

uum state [19], and couple it such that it absorbs all the energy outside the frequency interval $[-B_d/2, +B_d/2]$. As a result, we discover the generalized quadrature operator,

$$\hat{X}(t;\omega_l,B_d) \propto \int_{-B_d/2}^{+B_d/2} \frac{\mathrm{d}\omega}{2\pi} \left[\hat{a}(\omega+\omega_l)e^{-i(\omega t+\vartheta)} + \text{H.c.}\right], \tag{3.3.19}$$

which for coherent states has expectation value equal to the photocurrent of our balanced detector, eq. (3.3.16).

Summary

In this chapter, we presented quantum models of the optical coupler, electro-optical modulator, and detector. We left out a quantum theory of a coherent-state source with narrow line width in the optical range, typically implemented by a laser. Proper quantum-treatment of the laser requires analysis of nonlinear quantum-stochastic equations and is beyond the scope of this thesis. We refer the interested reader to Ref. [8, p. 900] and Ref. [96, 97]. For an intuitive argument why lasers emit coherent states based on decoherence, see Ref. [98].

For the lossless and LTI optical coupler, we found the most intuitive a characterization in terms of a unitary scattering matrix comprising reflection and transmission coefficients [7]. That said, we also investigated theoretical methods including evolution operators [18] and the Jordan-Schwinger operator algebra [17]. Concerning coherent states, the scattering ma-

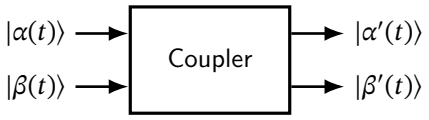


Figure 3.14.: Quantum-optical coupler with the input coherent-states, $|\alpha(t)\rangle$ and $|\beta'(t)\rangle$, on the left side, and the output coherent-states, $|\alpha'(t)\rangle$ and $|\beta'(t)\rangle$, on the right side.

trix connects the amplitudes of the coherent in- and output states in Figure 3.14 via

$$\begin{pmatrix}\alpha'(t)\\ \beta'(t)\end{pmatrix} = \begin{pmatrix}r(t) & t'(t)\\ t(t) & r'(t)\end{pmatrix} * \begin{pmatrix}\alpha(t)\\ \beta(t)\end{pmatrix} \tag{3.3.1}$$

in the time and

$$\begin{pmatrix}\alpha'(\omega)\\ \beta'(\omega)\end{pmatrix} = \begin{pmatrix}r(\omega) & t'(\omega)\\ t(\omega) & r'(\omega)\end{pmatrix}\begin{pmatrix}\alpha(\omega)\\ \beta(\omega)\end{pmatrix} \tag{3.3.2}$$

in the frequency domain. The complex reflection and transmission coefficients, the scattering-matrix parameters, are required to satisfy

$$|r(\omega)| + |t'(\omega)| = 1 = |t(\omega)| + |r'(\omega)| \tag{3.3.3}$$

[19] In a more realistic model, we would assume the reservoir to be in a thermal state, which directly includes thermal noise into our signals.

for conservation of energy flow and the CCR, making the scattering matrix unitary. If we assume the input coherent-states to be narrow-bandwidth and the optical coupler to have a constant frequency response over the optical bandwidth, the convolution in the time domain reduces to a multiplication. Certain embodiments of the optical coupler, such as the plate beam-splitter, arbitrarily superimpose two input coherent-states. That said, most implementations of optical couplers exhibit backscattering, which accounting for requires an optical four-port. As the scattering matrix of an optical four-port requires 16 complex parameters, most calculations become impractical. An optical coupler with a vacuum state as

Figure 3.15.: Quantum optical filter with input coherent-state, $|\alpha(t)\rangle$, and output coherent-state, $|\alpha'(t)\rangle$.

a second input and tracing out one output effectively implements a linear filter. The output coherent-state in Figure 3.15 relates to the input coherent-state via

$$\alpha'(t) = (h * \alpha)(t) \qquad\qquad \alpha'(\omega) = h(\omega)\alpha(\omega)$$

in the time and frequency domain, wherein the frequency-response function of the filter is required to satisfy $|h(\omega)| \leq 1$.

Using the linear electro-optical effect and nonlinear frequency-conversion with the help of Ref. [84, 81], we derived a unitary evolution operator corresponding to phase modulation with a sinusoidal signal. Neglecting second-order interactions between the modulation sidebands, we argued that phase modulation with an arbitrary signal is thinkable. The am-

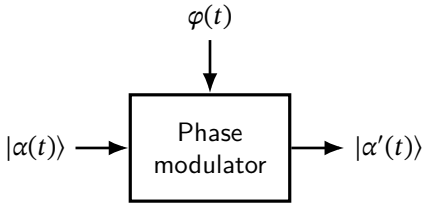


Figure 3.16.: Quantum-optical phase modulator with electric phase signal $\varphi(t)$, input coherent-state $|\alpha(t)\rangle$, and output coherent-state, $|\alpha'(t)\rangle$.

plitude of the output coherent-state in Figure 3.17 is

$$\alpha'(t) = \alpha(t)e^{i\varphi(t)} \qquad\qquad \alpha'(\omega) = (g * \alpha)(\omega) \tag{3.3.4}$$

in the time and frequency domain, where we can only give an explicit expression for the kernel $g(\omega)$ in the case of a sinusoidal modulation, eq. (3.2.27). Arranging two electro-optical phase modulators in an MZM and driving the modulators with a differential voltage enables

electro-optical amplitude modulation. Arranging two electrically-driven MZMs with a relative phase shift of $\pi/2$ generalizes amplitude modulation with a real- to a complex-valued signal. The amplitude of the output coherent-state in Figure 3.17 is

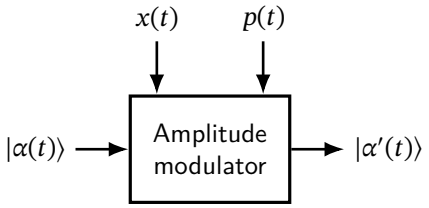


Figure 3.17.: Quantum-optical amplitude modulator with input voltage-signals, $x(t)$ and $p(t)$, input coherent-state $|\alpha(t)\rangle$, and output coherent-state $|\alpha'(t)\rangle$.

$$\alpha'(t) = [x(t) + ip(t)]\,\alpha(t) \qquad |x(t)|, |p(t)| \leq 1, \tag{3.3.5}$$

wherein $x(t)$ and $p(t)$ are proportional to the differential voltages driving the MZMs and the constraint follows from the constructive interference used for amplitude modulation (AM). As with the phase modulator, no closed form exists for the convolution kernel in the frequency domain.

Regarding the detectors, we studied photodetection theory from Ref. [8, 99, 7] in the appendix, Appendix C, and started employing the photocurrent operator to predict the mean photocurrent. Additionally, we presented an electric circuit of a TIA converting and amplifying the photocurrent to a voltage signal. The output voltage-signal $y(t)$ in Figure 3.18

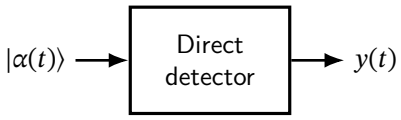


Figure 3.18.: Quantum-optical direct detector with input coherent-state $|\alpha(t)\rangle$, and output voltage-signal $y(t)$.

is equal to the photon flux $|\alpha(t)|^2$ convolved with the combined response-function of the detector and the TIA $\eta(\omega)$, i.e.,

$$y(t) = \left(\eta * |\alpha|^2\right)(t) = \int_{-\infty}^{+\infty} \frac{\mathrm{d}\omega}{2\pi} \eta(\omega) |\alpha(\omega)|^2, \tag{3.3.6}$$

wherein $|\alpha(\omega)|^2$ is the signal power. The direct detector is a square-law detector where the photocurrent is proportional to the signal power. To resolve the quadratures of the signal, we combine the input with a LO signal in an optical coupler and monitor the outputs with two direct detectors in a balanced configuration. The output voltage-signal $z(t)$ in Figure 3.19 is equal to the projection of the downconverted signal $\alpha(t)$ onto a real axis under the LO angle

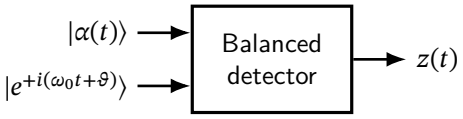


Figure 3.19.: Quantum-optical balanced detector with input coherent-state $|\alpha(t)\rangle$, LO coherent-state $|e^{i(\omega_0 t+\vartheta)}\rangle$, and output voltage-signal $z(t)$.

ϑ, i.e.,

$$z(t) = 2\,\mathrm{Re}\int_{-\infty}^{+\infty}\frac{\mathrm{d}\omega}{2\pi}\eta(\omega+\omega_l)\alpha(\omega+\omega_l)e^{+i(\omega t+\vartheta)}, \tag{3.3.7}$$

wherein ω_l and ϑ are the LO frequency and phase, and the LO lineshape is absorbed into the signal $\alpha(\omega)$. Comparison of the balanced detector's mean voltage signal with the expectation value of the quadrature operator leads us to motivate the generalized quadrature operator

$$\hat{X}(t;\omega_l,B_d) = \int_{-B_d/2}^{+B_d/2}\frac{\mathrm{d}\omega}{2\pi}\left[\hat{a}(\omega+\omega_l)e^{-i(\omega t+\vartheta)} + \mathrm{H.c.}\right], \tag{3.3.8}$$

accounting for an effective detector-bandwidth B_d and downconversion frequency and phase, by combining the frequency-conversion operator with a spectral filter. Our results are compatible with Ref. [97, 19, 9, 7, 20] on homo- and heterodyne detection but are more general in that we account for continuous-time signals, downconversion frequency and phase, and the detector bandwidth.

Chapter 4.

Coherent state transmission system

In the chapter on quantum-key distribution (QKD), Chapter 1, we argued why practical continuous-variable quantum-key distribution (CV-QKD) devices are effectively coherent-state transmission systems. In the present chapter, we use the theoretical framework of the preceding sections to provide a quantum description of a coherent-state transmission system and solve the mystery of CV-QKD.

A coherent-state transmission system attempts to correlate a classical information destination at a spacetime event y with a classical information source at a spacetime event x, wherein y is in the forward light cone of x, by sending coherent states. Figure 4.1 presents

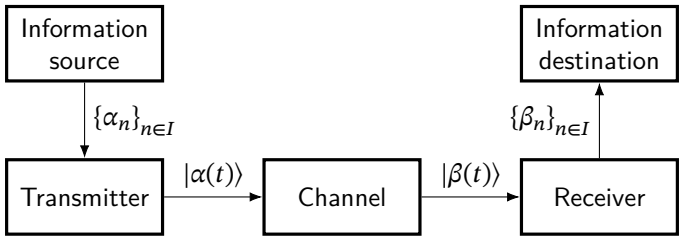


Figure 4.1.: Block diagram of a coherent-state transmission system used for practical QKD. An information source supplies a sequence of complex numbers, $\{\alpha_n \in \mathbb{C} : n \in I\}$, to a transmitter which encodes the information onto a coherent state $|\alpha(t)\rangle$ and transmits it through a (quantum) channel. The channel maps the transmitted coherent state $|\alpha(t)\rangle$ to a received coherent state $|\beta(t)\rangle$. The receiver decodes a sequence of complex numbers, $\{\beta_n \in \mathbb{C} : n \in I\}$, from the received coherent state $|\beta(t)\rangle$ and passes it to the information destination.

an attempt to extend the classical communication system introduced by Shannon [100] to coherent states.[1] We represent the classical information of the source and destination as a

[1] Contemporary to the literature, we distinguish between a transmission and a communication system. The former allows only unidirectional, the later bidirectional transport of information.

sequence of complex numbers, which we term symbols. On the one hand, a complex number is a natural parameterization for the amplitude and phase of a single-mode coherent state also representing a plane wave. On the other hand, there are many established techniques to map information to complex numbers, e.g., quadrature phase-shift keying (QPSK). For our description, it is irrelevant whether the complex numbers are value-continuous or -discrete, so we only restrict ourselves to time-discrete symbols. The transmitter encodes the symbol sequence $\{\alpha_n \in \mathbb{C} : n \in I\}$[2] onto a continuous-time coherent state $|\alpha(t)\rangle$ and passes this on to the (quantum) channel. The received coherent state $|\beta(t)\rangle$ contains information about the transmitted state. The receiver decodes a symbol sequence $\{\beta_n \in \mathbb{C} : n \in I\}$ from the received state $|\beta(t)\rangle$. The received symbols are realizations of a complex normal distribution due to the quantum uncertainty in the measurement. More precisely, the jth symbol at the receiver, β_j, is a realization of the complex normal distribution

$$\mathcal{CN}\left(\alpha_j, \Sigma\right),$$

wherein α_j is the corresponding jth symbol at the transmitter and Σ is a two-dimensional Hermitian and non-negative definite covariance matrix. For an ideal coherent-state transmission system, we expect the covariance matrix to be proportional to the noise of the system.

4.1. Transmitter

We introduced the transmitter as a component encoding a sequence of complex symbols,

$$\{\alpha_n \in \mathbb{C} : n \in I\}, \tag{4.1.1}$$

onto a coherent state $|\alpha(t)\rangle$. Efficient transmission through the channel and effective receiver detection impose additional constraints on the space of useful coherent states. Together with practical considerations, these constraints lead to the particular design embodiment of the transmitter we will discuss.

First and foremost, the channel and receiver limit the spectrum of useful coherent states. For instance, the receiver has limited bandwidth to detect the signal with signal power outside that bandwidth being lost. Apart from that, the physical channel only shows favorable transmission properties over a certain frequency range, outside the signal is strongly suppressed and distorted.[3] Additionally, different users may jointly use the same physical channel, and using the available bandwidth efficiently while reducing interference between users, requires the signal bandwidth to be well-defined.

[2] I denotes an index set, e.g., $I = \mathbb{N}$

[3] For instance, the C-band, spanning wavelengths from 1530 nm to 1565 nm, is widely deployed for optical telecommunication.

While the symbol rate effectively defines the bandwidth, insufficient usage of the bandwidth degrades the signal-to-noise ratio (SNR). In addition, we need to shift the baseband spectrum to an optical frequency ω_0 for which the channel shows desirable transmission characteristics. So from a signal-processing point of view, we want the transmitter to

1. first create a baseband signal with well-defined spectrum,[4]

2. then transfer it to a passband signal in the optical domain.

In the following, we term the first step symbol encoding and the second step upconversion.

In the present setup, the signal is almost exclusively constructed in the digital domain, and the analog part is limited to the digital-to-analog conversion. Constructing the signal digitally allows for greater flexibility in the development process is mostly software-defined. For upconversion of the analog signal to the optical domain, we modulate the electric signal onto an optical carrier. Figure 4.2 illustrates how such a software-defined transmitter

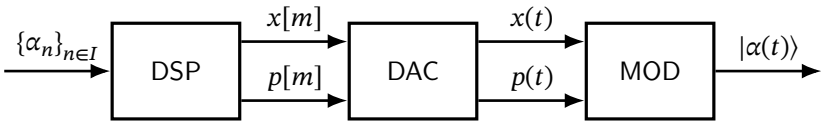


Figure 4.2.: Block diagram of the transmitter's signal-processing domains. The digital signal processing (DSP) transforms a complex symbol sequence $\{\alpha_n\}_{n\in I}$ into two digital signals, $x'[m]$ and $p'[m]$, corresponding to the real and imaginary part. The digital-to-analog converter (DAC) converts the digital signals to analog signals, $x(t)$ and $p(t)$ we modulate onto a coherent state $|\alpha(t)\rangle$.

architecture applies to our coherent-state transmission system. The software-defined DSP constructs the bandwidth-optimized digital signals $x[m]$ and $p[m]$, encoding the real and imaginary parts of the complex symbols. The DAC stage converts the digital signals, $x[m]$ and $p[m]$, to bandwidth-limited analog signals $x(t)$ and $p(t)$. Finally, the analog signals are modulated onto an optical carrier yielding a coherent state $|\alpha(t)\rangle$ with well-defined spectrum.

4.1.1. Symbol encoding

To construct a bandwidth-optimized baseband signal, encoding the complex symbol sequence $\{\alpha_n \in \mathbb{C} : n \in I\}$, we first remark that the symbol sequence itself has no notion of time. In contrast, a digital (time-discrete) signal, consisting of discrete samples, includes

[4]We consider a spectrum well-defined if bandwidth-limited and compatible with the Nyquist criterion, which requires the signal bandwidth B to equal at least half the symbol rate $2B > f_s$.

a time reference, the sample period T_s, denoting the temporal distance between two consecutive samples. By defining the digital signal with samples equal to the symbols, $\alpha[n] = \alpha_n$, and introducing the symbol period T_s as sample period, we find ourselves with the complete DSP toolbox at our disposal.[5] Figure 4.3 summarizes the essential DSP steps including

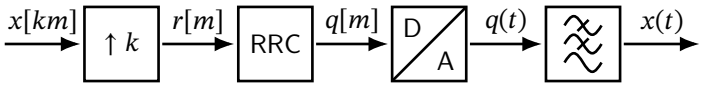


Figure 4.3.: Block diagram of the signal processing for the symbol encoding. The digital signal $x[km]$ is upsampled by a factor k to $r[m]$ and pulse-shaped by a root-raised-cosine (RRC) filter to yield $q[m]$. A DAC converts the pulse-shaped signal $q[m]$ to the analog signal $q(t)$. Finally, the analog signal $q(t)$ is low-pass (LP) filtered to yield the analog anti-aliased signal $x(t)$.

analog conversion of a real-valued digital signal $x[km]$ to construct a bandwidth-optimized analog baseband signal $x(t)$.[6] The digital signal $x[km]$, containing the symbols, is first upsampled by an upsampling factor of k, adding k zero-valued samples in between the original samples. The pulse-shaping of the RRC filter interpolates between the non-zero samples, the symbols, to precisely define the signal bandwidth. Finally, an ideal DAC converts the digital signal $q[m]$ to the analog signal $q(t)$, equivalent to infinite upsampling. The analog signal $q(t)$ contains infinite aliases through the upsampling, which we remove by filtering $q(t)$ with a LP, yielding the anti-aliased analog signal $x(t)$. Figure 4.4 illustrates the time domain signals for each signal-processing step for a symbol sequence which contains only a single non-zero symbol with unit value. We see very well how the upsampling increases the resolution of the digital signal in the time domain and how the pulse-shaping filter interpolates between the samples. We also see that the RRC pulse-shaping filter corresponds to a sinc-like impulse response. The similarity of the analog signal with a sinc pulse is not surprising since the RRC is the square-root of the raised-cosine filter. The raised-cosine filter has frequency response

$$|h_{\mathrm{rc}}(f/f_s)| = \begin{cases} 1 & |f/f_s| \leq (1-\alpha) \\ \cos\left[\frac{\pi}{4\alpha}\left(|f/f_s| - 1 + \alpha\right)\right] & 1-\alpha \leq |f/f_s| \leq 1+\alpha \\ 0 & \text{otherwise} \end{cases}, \tag{4.1.2}$$

wherein $f_s = 1/T_s$ is the symbol rate and α determines the roll-off and satisfies the Nyquist criterion for optimal bandwidth [6, p. 51]. Taking the square-root of the raised-cosine pulse-shaping filter and applying it once on the transmitter-side and once on the receiver-side, where it is named the matched filter, also satisfies the Nyquist criteria but suppresses out-of-band noise.[7] Figure 4.5 illustrates the time domain signals for each signal-processing

[5] Even if the DSP itself does not work explicitly with the time reference T_s, we need time to give a meaningful interpretation of the signal between the steps.

[6] The baseband construction generalizes to a complex digital signal by applying the real-valued baseband construction separately to the real and imaginary part.

[7] From a mathematical point of view, the matched filter is only asymptotically ideal for close-to-zero SNR. For sufficiently bad SNR the matched filter is almost as good as a Wiener filter.

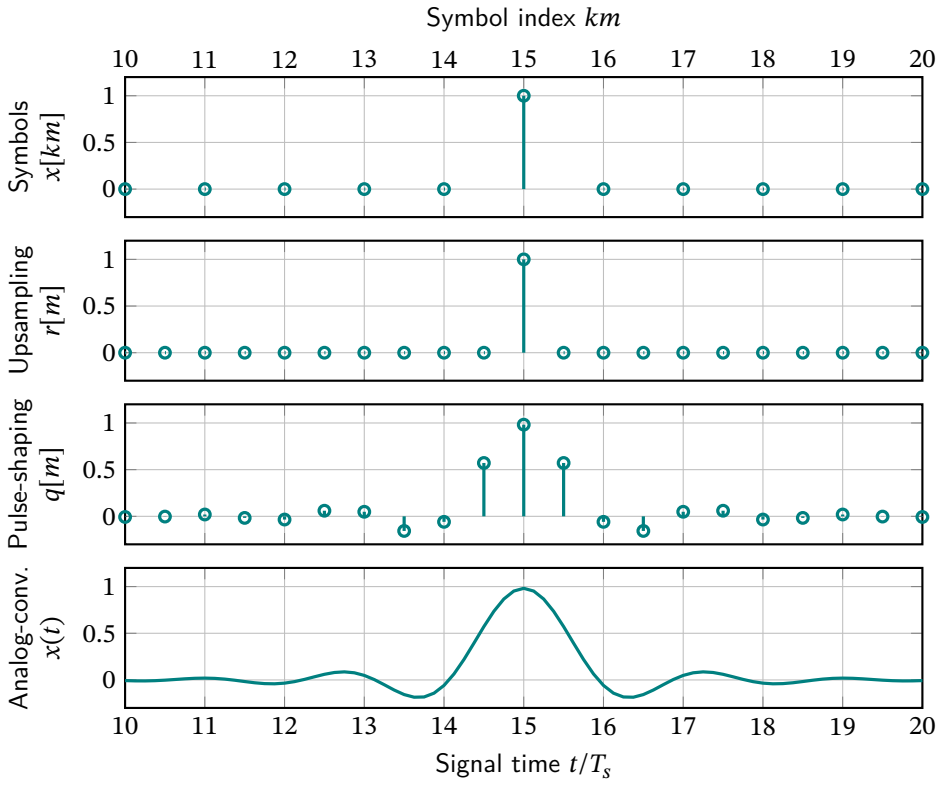


Figure 4.4.: Symbol encoding for a single unit symbol in the time domain. The symbol sequence $\{x_n \in \mathbb{R} : n \in I\}$ is represented by the digital signal $x[km]$ with sample period T_s (first row). The digital signal $x[km]$ is upsampled to $r[m]$ by an upsampling factor of $k = 2$ (second row). The upsampled signal $r[m]$ is pulse-shaped with a RRC filter to yield $q[m]$ (third row). The pulse-shaped digital signal $q[m]$ is converted to the anti-aliased analog signal $x(t)$.

step for a random QPSK symbol sequence. Figure 4.6 provides further inside into the signal-processing steps by presenting the power spectrum of the unit and QPSK symbol sequences. In the frequency domain, it is very clear to see how upsampling widens the spectrum without adding additional information. We also see how the pulse-shaping filter shapes the upsampled spectrum, and the LP filter suppresses aliases.

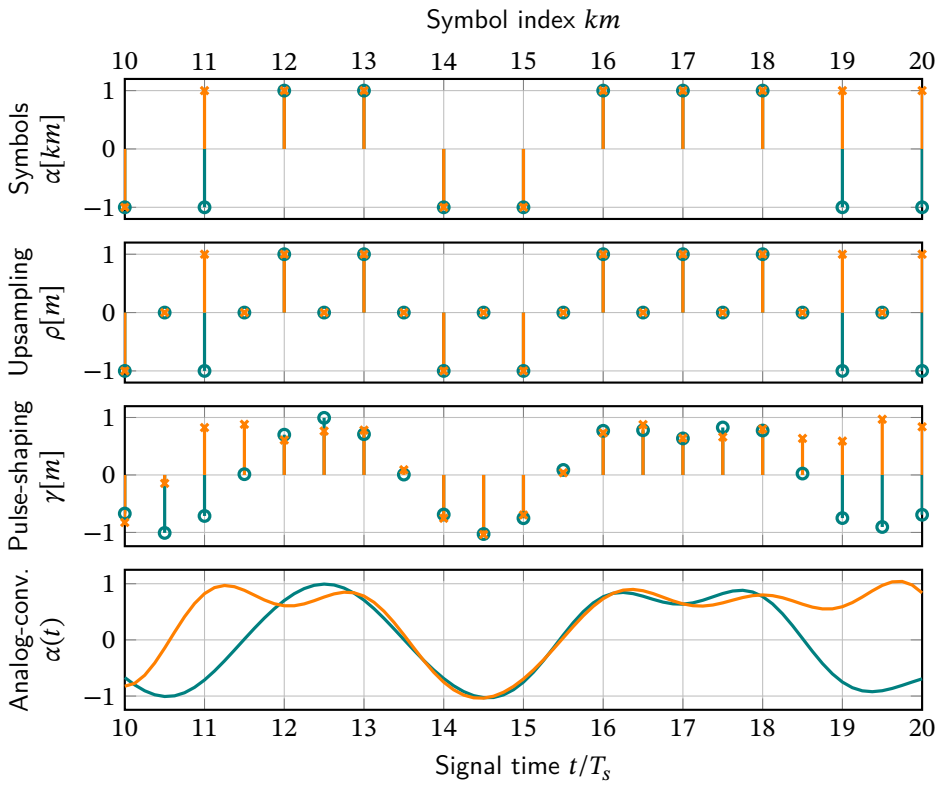


Figure 4.5.: Symbol encoding for a random QPSK symbol-sequence in the time domain with real (orange) and imaginary (green) part . The complex symbol sequence $\{\alpha_n \in \mathbb{C} : \ n \in I\}$ is represented by the digital signal $\alpha[km]$ with sample period T_s (first row). The digital signal $\alpha[km]$ is upsampled to $\rho[m]$ by an upsampling factor of $k = 2$ (second row). The upsampled signal $\rho[m]$ is pulse-shaped with a RRC filter to yield $\gamma[m]$ (third row). The pulse-shaped digital signal $\gamma[m]$ is converted to the anti-aliased analog signal $\alpha(t)$.

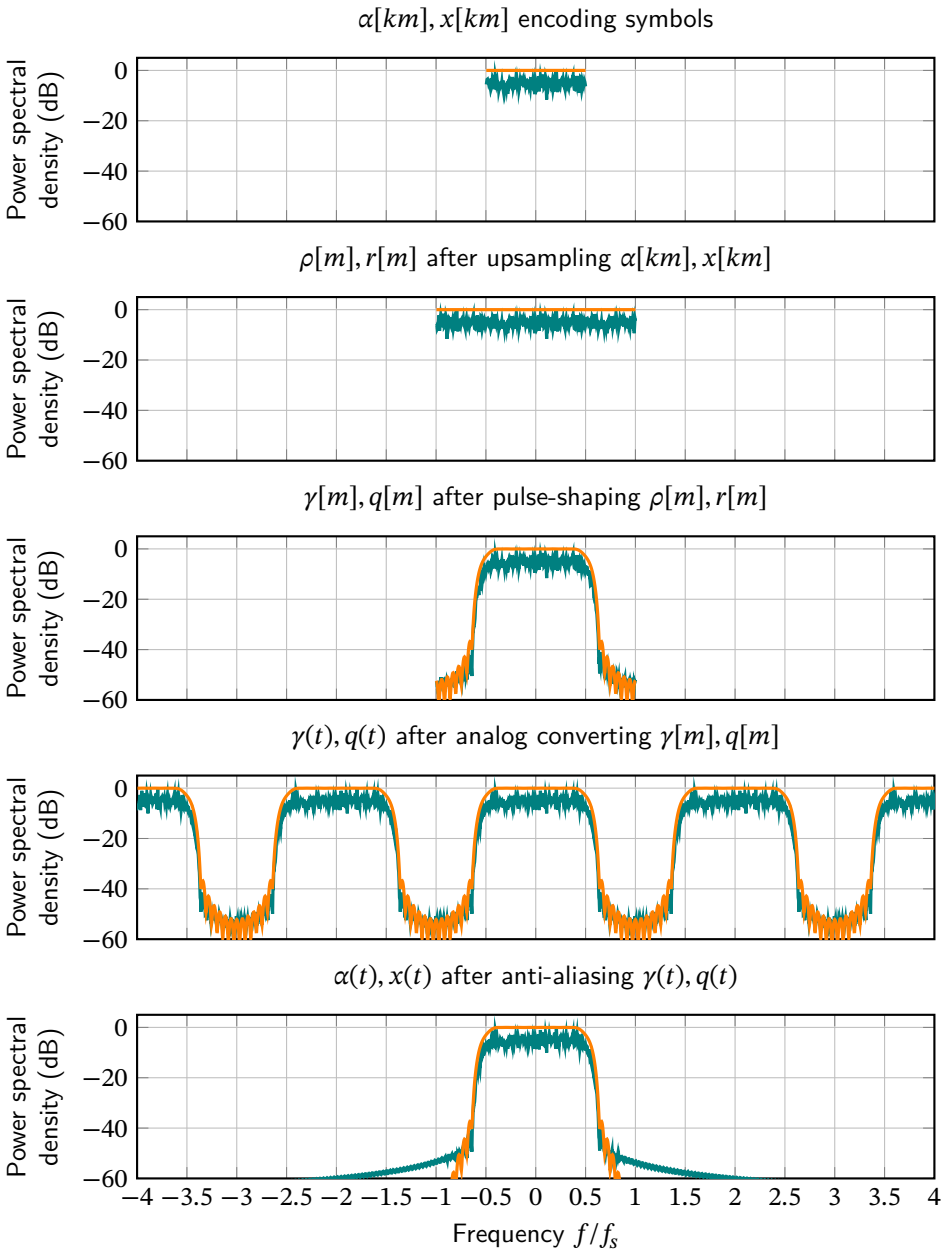


Figure 4.6.: Power spectrum of the symbol encoding steps for a random QPSK symbol sequence (green) and the unit symbol sequence (orange). The initial spectrum spans from $-1/2$ to $+1/2$ the normalized sampling frequency f/f_s (first row). Upsampling by $k = 2$ adds aliases left and right to the initial spectrum (second row). Pulse-shaping suppresses the left and ride flanks of the spectrum to precisely define the spectrum (third row). Analog conversion corresponds to infinite upsampling, adding infinite aliases left and right of the spectrum. (fourth row). Applying a LP filter strongly suppresses the aliases with relaxed requirements on the filter spectrum (last row).

4.1.2. Upconversion

We previously constructed the pulse-shaped baseband signals $x(t)$ and $p(t)$ encoding the real respective imaginary part of a complex symbol sequence $\{\alpha_n \in \mathbb{C} : n \in I\}$. Modulating the signals onto the optical carrier frequency ω_c resembles an upconversion by the frequency ω_c, corresponding to the multiplication with an local oscillator (LO) signal, as illustrated in Figure 4.7. In the frequency representation, we find that the multiplication of the signal

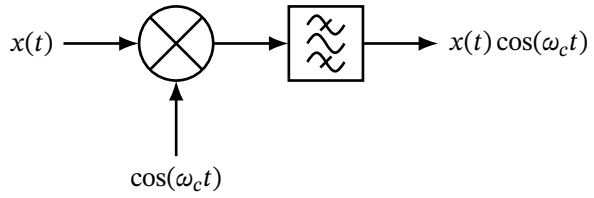


Figure 4.7.: Block diagram of single-quadrature upconversion. The signal $x(t)$ is mixed with the LO signal $\cos(\omega_c t)$ and the output is filtered by a bandpass to remove harmonics.

$x(t)$ with the LO signal $\cos(\omega_c t)$ creates two copies of the spectrum $x(\omega)$, at the positive and negative upconversion-frequency $\pm\omega_c$, as illustrated in Figure 4.8. Because Figure 4.8

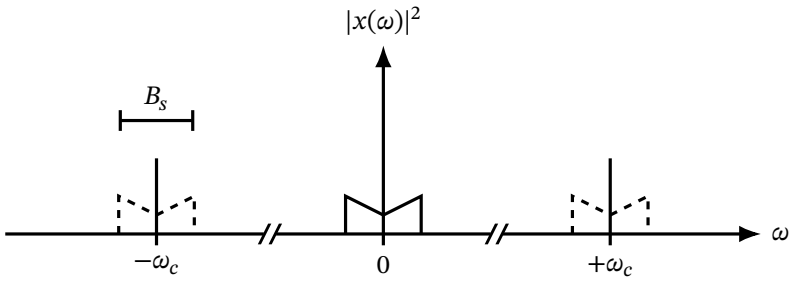


Figure 4.8.: Power spectrum illustrating upconversion of the real-valued signal $x(t)$ centered at zero frequency $\omega = 0$ (solid spectrum) to the carrier frequencies $\pm\omega_c$ (dashed spectra).

shows the power spectrum, it fails to convey that the spectrum at the negative frequencies is complex conjugate, $x(-\omega) = x(\omega)^*$, with respect to the positive frequencies, as required

for real-valued signals, i.e.,

$$\begin{aligned}
x(t)\cos(\omega_c t) &= \int_{-B_s/2}^{+B_s/2} \frac{\mathrm{d}\omega}{2\pi} x(\omega) e^{+i\omega t} \cos(\omega_c t) \\
&= \frac{1}{2} \int_{-B_s/2}^{+B_s/2} \frac{\mathrm{d}\omega}{2\pi} x(\omega) \left[e^{+i(\omega+\omega_c)t} + e^{+i(\omega-\omega_c)t} \right] \\
&= \frac{1}{2} \int_{+\omega_c-B_s/2}^{+\omega_c+B_s/2} \frac{\mathrm{d}\omega}{2\pi} x(\omega-\omega_c) e^{+i\omega t} + \frac{1}{2} \int_{-\omega_c-B_s/2}^{-\omega_c+B_s/2} \frac{\mathrm{d}\omega}{2\pi} x(\omega+\omega_c) e^{+i\omega t} \\
&= \frac{1}{2} \int_{+\omega_c-B_s/2}^{+\omega_c+B_s/2} \frac{\mathrm{d}\omega}{2\pi} x(\omega-\omega_c) e^{+i\omega t} - \frac{1}{2} \int_{+\omega_c+B_s/2}^{+\omega_c-B_s/2} \frac{\mathrm{d}\omega}{2\pi} x(-\omega+\omega_c) e^{-i\omega t} \\
&= \frac{1}{2} \int_{+\omega_c-B_s/2}^{+\omega_c+B_s/2} \frac{\mathrm{d}\omega}{2\pi} x(\omega-\omega_c) e^{+i\omega t} + \frac{1}{2} \int_{+\omega_c-B_s/2}^{+\omega_c+B_s/2} \frac{\mathrm{d}\omega}{2\pi} x(\omega-\omega_c)^* e^{-i\omega t} \\
&= \mathrm{Re} \int_{+\omega_c-B_s/2}^{+\omega_c+B_s/2} \frac{\mathrm{d}\omega}{2\pi} x(\omega-\omega_c) e^{+i\omega t},
\end{aligned} \tag{4.1.3}$$

wherein we used the conjugate symmetry of the spectrum in the last step.

Figure 4.9 shows how to extend the previously-discussed single-quadrature upconversion to dual-quadrature upconversion by splitting a single LO with relative phase shift of $\pi/2$. The filtered output of the lower branch mixer is obtained by adding a phase of $\pi/2$ to the

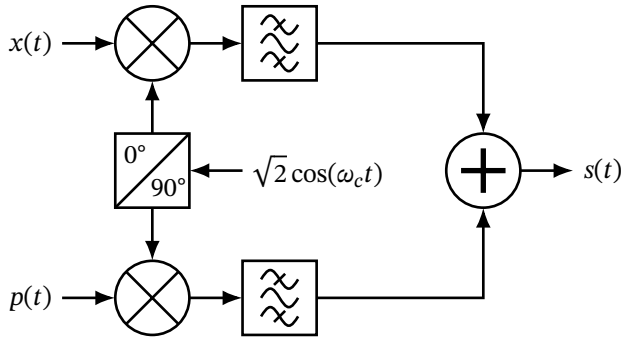


Figure 4.9.: Block diagram illustrating upconversion of two real-valued baseband signals, $x(t)$ and $p(t)$, to a real-valued passband signal $s(t)$. The LO signal $\sqrt{2}\cos(\omega_c t)$ is split into two branches with a relative phase shift between the branches of $\pi/2$. One branch is mixed with the baseband signal $x(t)$, the other is mixed with $p(t)$. The output of each mixer is filtered to remove harmonics and then added to yield the upconverted signal $s(t)$.

complex exponential and replacing $x(t)$ with $p(t)$ in eq. (4.1.4), i.e.,

$$p(t)\sin(\omega_c t) = \mathrm{Im}\int_{+\omega_c - B_s/2}^{+\omega_c + B_s/2} \frac{\mathrm{d}\omega}{2\pi} p(\omega - \omega_c) e^{+i\omega t}. \tag{4.1.4}$$

The sum of both branches in Figure 4.9 equals

$$\begin{aligned} s(t) &= x(t)\cos(\omega_c t) - p(t)\sin(\omega_c t) \\ &= \mathrm{Re}\int_{+\omega_c - B_s/2}^{+\omega_c + B_s/2} \frac{\mathrm{d}\omega}{2\pi} x(\omega - \omega_c) e^{+i\omega t} - \mathrm{Im}\int_{+\omega_c - B_s/2}^{+\omega_c + B_s/2} \frac{\mathrm{d}\omega}{2\pi} p(\omega - \omega_c) e^{+i\omega t} \\ &= \mathrm{Re}\int_{+\omega_c - B_s/2}^{+\omega_c + B_s/2} \frac{\mathrm{d}\omega}{2\pi} \left[x(\omega - \omega_c) + i p(\omega - \omega_c)\right] e^{+i\omega t}, \end{aligned} \tag{4.1.5}$$

where we used $\mathrm{Im}(z) = -\mathrm{Re}(iz)$ in the last step. Equation (4.1.5) suggests defining the complex-valued baseband signal

$$\alpha(t) = x(t) + i p(t) \tag{4.1.6}$$

for which we can show that the dual-quadrature upconversion equals the multiplication with a complex exponential, i.e.,

$$s(t) = \mathrm{Re}\left[\alpha(t) e^{+i\omega_c t}\right], \tag{4.1.7}$$

demonstrating equivalence between the baseband and passband representations. Compared

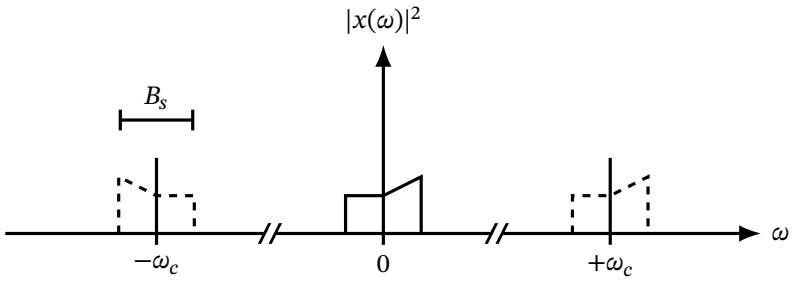


Figure 4.10.: Power spectrum illustrating dual-quadrature upconversion of the complex-valued signal $\alpha(t)$ centered at zero frequency $\omega = 0$ (solid spectrum) to the carrier frequencies $\pm\omega_c$ (dashed spectra).

to the power spectrum illustrating the single-quadrature upconversion in Figure 4.9, the power spectras concentrated are now asymmetric around their respective carrier frequencies, $\omega = 0, \pm\omega_c$. However, the upconverted spectrum including the positive and negative frequencies remains to have complex conjugate symmetry, as depicted in Figure 4.10.

Using the complex baseband representation, eq. (4.1.6), it is simple to link the dual-quadrature upconversion to our result of the electro-optical in-phase and quadrature modulator (IQM).

In particular, if we assume a narrow-linewidth LO at frequency ω_c, represented by the coherent state

$$|g(t)e^{+i\omega_c t}\rangle \tag{4.1.8}$$

with $g(t)$ encoding the laser profile, the unitary evolution operator associated with the IQM acting on the LO coherent state produces,

$$\hat{U}_{\mathrm{IQM}}[\alpha(t)]|g(t)e^{+i\omega_c t}\rangle = |(g\alpha)(t)e^{+i\omega_c t}\rangle, \tag{4.1.9}$$

the upconversion from the electrical to the quantum-optical domain.

4.2. Receiver

We introduced the receiver as a component decoding a sequence of complex symbols,

$$\{\beta_n \in \mathbb{C} : n \in I\}, \tag{4.2.1}$$

from a coherent state $|\beta(t)\rangle$. Just like the transmitter, we want to keep the receiver software-defined. Figure 4.11 shows the signal processing of a possible software-defined receiver. The

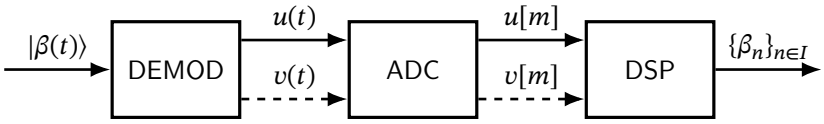


Figure 4.11.: Block diagram of the receiver's signal processing domains. The analog electrical signals $u(t)$, and optional $v(t)$, are demodulated from the quadratures of the optical coherent state $|\beta(t)\rangle$, and then converted to the digital signals $u[m]$, and optional $v[m]$, from which the DSP decodes the symbol sequence $\{\beta_n \in \mathbb{C} : n \in I\}$.

coherent state is transferred from the optical via the analog to the digital.

4.2.1. Downconversion

At the transmitter, we upconverted two real baseband signals to a real passband signal. For the receiver, we discuss options involving one and two real baseband signals. We first consider the simpler case of direct downconversion as depicted in Figure 4.12. In direct down-

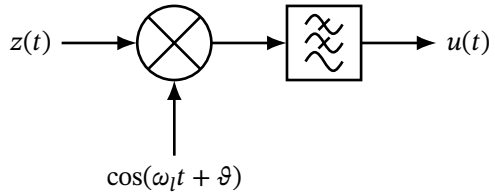


Figure 4.12.: Block diagram of single-quadrature downconversion. The signal $z(t)$ is mixed with the LO signal $\cos(\omega_l t + \vartheta)$. The downconverted signal $u(t)$ is obtained by LP filtering the output signal of the mixing.

conversion, we mix a real-valued signal,

$$\begin{aligned} z(t) = \int_{-\infty}^{+\infty} \frac{\mathrm{d}\omega}{2\pi} z(\omega) e^{+i\omega t} &= \int_{0}^{+\infty} \frac{\mathrm{d}\omega}{2\pi} z(\omega) e^{+i\omega t} + \int_{-\infty}^{0} \frac{\mathrm{d}\omega}{2\pi} z(\omega) e^{+i\omega t} \\ &= \int_{0}^{+\infty} \frac{\mathrm{d}\omega}{2\pi} z(\omega) e^{+i\omega t} - \int_{+\infty}^{0} \frac{\mathrm{d}\omega}{2\pi} z(-\omega) e^{-i\omega t} \\ &= \int_{0}^{+\infty} \frac{\mathrm{d}\omega}{2\pi} \left[z(\omega) e^{+i\omega t} + z(\omega)^* e^{-i\omega t} \right] \\ &= \int_{0}^{+\infty} \frac{\mathrm{d}\omega}{2\pi} 2\,\mathrm{Re}\left[z(\omega) e^{+i\omega t} \right], \end{aligned} \tag{4.2.2}$$

where we used the conjugate symmetry, $z(-\omega) = z(\omega)^*$, of the Fourier transform of a real-valued function $z(t)$. Multiplication with the LO signal $\cos(\omega_l t + \vartheta)$, the mixing produces a high- and low-frequency band

$$\begin{aligned} z(t)\cos(\omega_l t + \vartheta) &= 2\,\mathrm{Re} \int_{0}^{\infty} \frac{\mathrm{d}\omega}{2\pi} z(\omega) e^{+i\omega t} \cos(\omega_l t + \vartheta) \\ &= \mathrm{Re} \int_{0}^{\infty} \frac{\mathrm{d}\omega}{2\pi} z(\omega) e^{+i\omega t} \left[e^{+i(\omega_l t + \vartheta)} + e^{-i(\omega_l t + \vartheta)} \right] \\ &= \mathrm{Re} \int_{0}^{\infty} \frac{\mathrm{d}\omega}{2\pi} z(\omega) \left[e^{+i(\omega + \omega_l) t + i\vartheta} + e^{+i(\omega - \omega_l) t - i\vartheta} \right] \\ &= \mathrm{Re} \int_{+\omega_l}^{\infty} \frac{\mathrm{d}\omega}{2\pi} z(\omega - \omega_l) e^{+i\omega t + i\vartheta} \\ &\quad + \mathrm{Re} \int_{-\omega_l}^{\infty} \frac{\mathrm{d}\omega}{2\pi} z(\omega + \omega_l) e^{+i\omega t - i\vartheta}. \end{aligned} \tag{4.2.3}$$

However, we suppress the high-frequency band using an ideal LP filter with bandwidth B_d,

$$\begin{aligned} u(t) &= \mathrm{Re} \int_{-B_d/2}^{+B_d/2} \frac{\mathrm{d}\omega}{2\pi} z(\omega+\omega_l) e^{+i\omega t - i\vartheta} \\ &= \mathrm{Re} \int_{0}^{+B_d/2} \frac{\mathrm{d}\omega}{2\pi} z(\omega+\omega_l) e^{+i\omega t - i\vartheta} + \mathrm{Re} \int_{-B_d/2}^{0} \frac{\mathrm{d}\omega}{2\pi} z(\omega+\omega_l) e^{+i\omega t - i\vartheta} \\ &= \mathrm{Re} \int_{0}^{+B_d/2} \frac{\mathrm{d}\omega}{2\pi} z(\omega+\omega_l) e^{+i\omega t - i\vartheta} - \mathrm{Re} \int_{B_d/2}^{0} \frac{\mathrm{d}\omega}{2\pi} z(\omega-\omega_l)^* e^{-i\omega t - i\vartheta} \\ &= \mathrm{Re} \int_{0}^{+B_d/2} \frac{\mathrm{d}\omega}{2\pi} \left[z(\omega+\omega_l) e^{+i\omega t} + z(\omega-\omega_l)^* e^{-i\omega t} \right] e^{-i\vartheta}, \end{aligned} \tag{4.2.4}$$

where we assumed $\omega_l \gg B_d/2$. For $\vartheta = 0$, the downconverted signal $v(t)$ is equal to projecting the real part of the complex input spectrum $z(\omega)$, losing the imaginary part's information. Furthermore, when rewriting $u(t)$ as an integral over positive frequencies, i.e., frequencies we can measure, we find a second term mirroring the first term. Figure 4.13

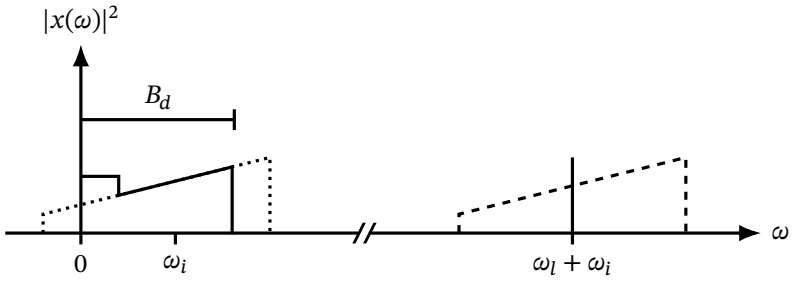


Figure 4.13.: Power spectrum illustrating downconversion of a passband signal (solid spectrum) mixed with a LO signal ω_l to the intermediate frequency ω_i (dashed spectrum) and measurement with bandwidth B_d (dotted spectrum).

shows the downconversion of the signal $z(t)$ around the LO at ω_l to the intermediate frequency ω_i. The actual measurement involved only positive frequencies up to the detector bandwidth $B_d/2$ causing the actual signal to be imposed with the mirrored spectrum.

Single-quadrature downconversion only reveals a real projection of the complex spectrum. To conserve both quadratures, we need to split the input signal into two branches and perform single-quadrature downconversion with two orthogonal phase references of the LO, see Figure 4.14. The signal of the upper branch $u(t)$ is equal to our result for the single-quadrature downconversion, eq. (4.2.4). The signal of the lower branch,

$$\begin{aligned} v(t) &= \mathrm{Im} \int_{-B_d/2}^{+B_d/2} \frac{\mathrm{d}\omega}{2\pi} z(\omega-\omega_l) e^{+i(\omega t+\vartheta)} \\ &= \mathrm{Im} \int_{0}^{+B_d/2} \frac{\mathrm{d}\omega}{2\pi} \left[z(\omega-\omega_l) e^{+i(\omega t+\vartheta)} + z(\omega+\omega_l)^* e^{-i(\omega t+\vartheta)} \right], \end{aligned} \tag{4.2.5}$$

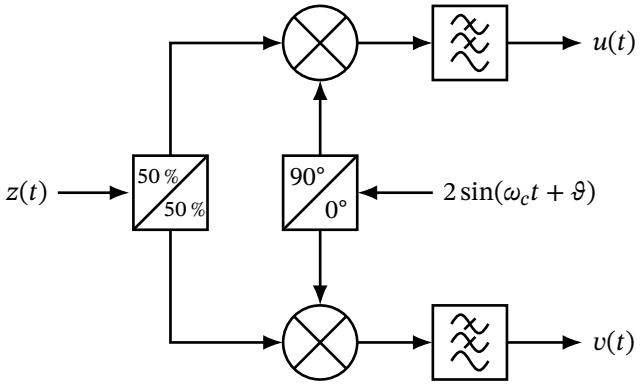


Figure 4.14.: Block diagram of dual-quadrature downconversion. The signal $z(t)$ is divided equally into an upper and a lower branch. The upper branch is mixed with the phase shifted LO signal $\cos(\omega_c t + \vartheta)$. The lower branch is mixed with LO signal $\sin(\omega_c t + \vartheta)$. The mixer outputs are filtered separately by a LP yielding the downconverted signals $u(t)$ and $v(t)$.

is simply obtained from eq. (4.2.4) by shifting the LO phase reference by 90°, i.e., $\vartheta \to \vartheta + \pi/2$. Regardless of the particular value of the LO phase reference ϑ, dual-quadrature downconversion recovers the complete information, the real and imaginary part, of the input signal spectrum $z(\omega)$.

We presented the electro-optical receiver setups implementing single- and dual-quadrature downconversion in Figure 1.14 and Figure 1.15 in Chapter 1. In Chapter 3, we investigated the balanced detector, effectively implementing the single-quadrature downconversion.

4.2.2. Homo- and heterodyning

So far, we have not assumed any particular signal for the downconversion but treated the receiver as a spectrum analyzer. If we now assume the input signal to be from the coherent-state transmitter $|\beta(t)\rangle$, eq. (4.1.5), the downconverted signals read

$$u(t) = \mathrm{Re} \int_{-B_d/2}^{+B_d/2} \frac{\mathrm{d}\omega}{2\pi} \beta(\omega - \omega_c + \omega_l) e^{+i(\omega t + \theta)} \tag{4.2.6}$$

$$v(t) = \mathrm{Im} \int_{-B_d/2}^{+B_d/2} \frac{\mathrm{d}\omega}{2\pi} \beta(\omega - \omega_c + \omega_l) e^{+i(\omega t + \theta)}, \tag{4.2.7}$$

wherein θ accounts for the phases of the up- and downconversion LOs. We define the the intermediate frequency as the difference between the transmitter and receiver LOs, i.e.,

$$\omega_i = |\omega_c - \omega_l| < B_d/2, \tag{4.2.8}$$

and distinguish between homodyning for zero intermediate frequency $\omega_i = 0$, and otherwise, heterodyning $\omega_i \neq 0$. In heterodyning, we shift the spectrum surrounding ω_c, dashed

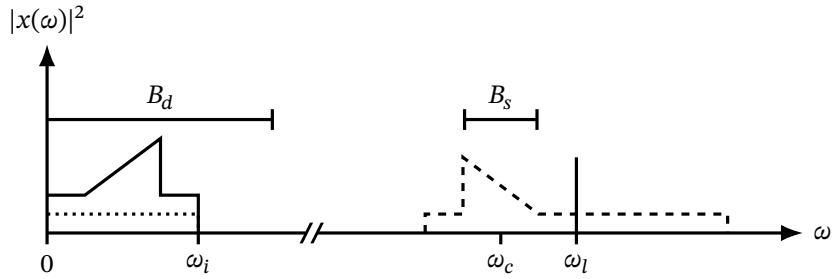


Figure 4.15.: Power spectrum illustrating heterodyne detection. The passband signal with carrier frequency ω_c and bandwidth B_s (dashed) is downconverted with the LO frequency $\omega_l > \omega_c$. The downconverted spectrum is measured with bandwidth B_d (solid), which contains the image band (dotted) from the right side of the LO.

lines in Figure 4.15, to the zero frequency $\omega = 0$, where we superimpose the negative frequencies with the positive frequencies, dotted lines in Figure 4.15. The noise spectrum opposite of LO frequency, which contributes to the measurement, is knowns as the image band. In homodyning, we calibrate the LO signal to match the carrier frequency, $\omega_l = \omega_c$, as illustrated in Figure 4.16, which separates the image from the signal band but folds the positive and negative frequencies of the baseband signal. As a result, homodyning recovers only one

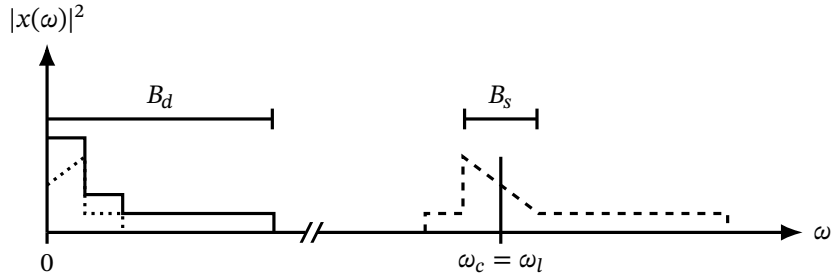


Figure 4.16.: Power spectrum illustrating homodyne detection. The passband signal with carrier frequency ω_c and bandwidth B_s (dashed) is downconverted with the LO frequency, equal to the carrier frequency, $\omega_l = \omega_c$. The downconverted spectrum is measured with bandwidth B_d (solid), which contains the mirror (dotted) from the right side of the LO.

quadrature To resolve both quadratures, we need to perform dual-quadrature downconversion requiring two homodyne detectors. Table 4.1 summarizes the characteristics between the single- and dual-quadrature homodyning and heterodyning. A strong advantage of the heterodyne receiver design is that both quadratures can be resolved with a single balanced detector, keeping the optical complexity low. Concerning the SNR, dual-quadrature homo-

Scheme	Homodyne (single)	Homodyne (dual)	Heterodyne
Balanced detectors	1	2	1
Quadratures	1	2	2
Intermediate frequency	$\omega_i = 0$		$\omega_i \neq 0$
Optical complexity	Low	High	Low
Signal bandwidth	High	High	Low
LO synchronization	Frequency and phase	Frequency	Bandwidth

Table 4.1.: Comparison of receiver schemes according to Ref. [101]. The single-quadrature homodyne detection offers low optical complexity and high bandwidth but only resolves one of two quadratures and required frequency and phase synchronization of the LO. The dual-quadrature homodyne detection resolves both quadratures with high bandwidth but requires two balanced detectors increasing the optical complexity and phase synchronization of the LO. The heterodyne detection schemes resolves both quadratures with low complexity and no requirements on LO synchronization at the cost of signal bandwidth.

dyne and heterodyne detection offer the same performance. For dual-quadrature homodyning, the signal power reduces among the two detectors, while the image band degrades the SNR for heterodyning.

4.2.3. Symbol decoding

We continue our receiver description, starting from the single-quadrature downconversion and assuming the more general heterodyning, which for $\omega_i = 0$ reduces to single-quadrature homodyning. Figure 4.17 summarizes the relevant signal processing for the symbol decod-

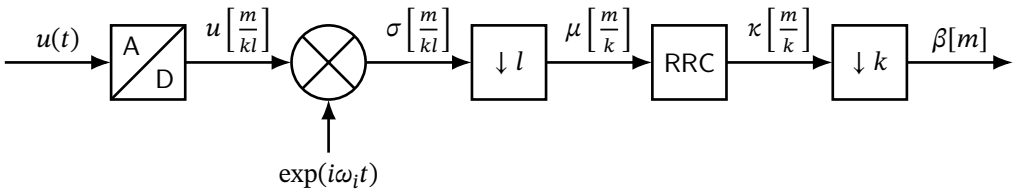


Figure 4.17.: Block diagram of the signal processing for the symbol decoding. The analog signal $u(t)$ is converted to the digital signal $u[m/(kl)]$. The real digital signal $u[m/(kl)]$ is multiplied with the complex exponential $\exp(i\omega_i t)$, yielding the complex digital signal $\sigma[m/(kl)]$. $\sigma[m/(kl)]$ is downsampled by l to yield the complex digital signal $\mu[m/k]$. $\mu[m/k]$ is pulse-shaped with the matched RRC filter to yield the complex digital signal $\kappa[m/k]$. $\kappa[m/k]$ is downsampled to the complex digital signal $\beta[m]$ corresponding to the decoded symbol sequence.

ing. The downconverted signal $u(t)$ corresponding to the real part of the received coherent-state spectrum $\beta(\omega)$, eq. (4.2.6), is sampled by an analog-to-digital converter (ADC), yielding the digital signal $u[m/(kl)]$. We remove the intermediate frequency in $u[m/(kl)]$ by multiplication with a complex exponential, i.e,

$$\sigma\left[\frac{m}{kl}\right] = u\left[\frac{m}{kl}\right] e^{+2\pi i(m/kl)T_s}, \tag{4.2.9}$$

making the signal complex-valued. It follows a downsampling by l of the signal such that we can apply the same RRC filter, the matched filter, which we used in the symbol encoding to maximize SNR. Finally, we downsample by k to restore a digital signal corresponding to the symbol sequence. Figure 4.18 illustrates how the symbol decoding is carried out in the frequency domain. The demodulated signal spectrum is a passband signal at the intermediate frequency and downconversion reduces the passband to a baseband signal. Completing the pulse-shaping with the matched filter increases the steepness of the flanks which are collapsed with aliasing by the final downsampling step. Figure 4.19) shows the symbol decoding in the time domain.

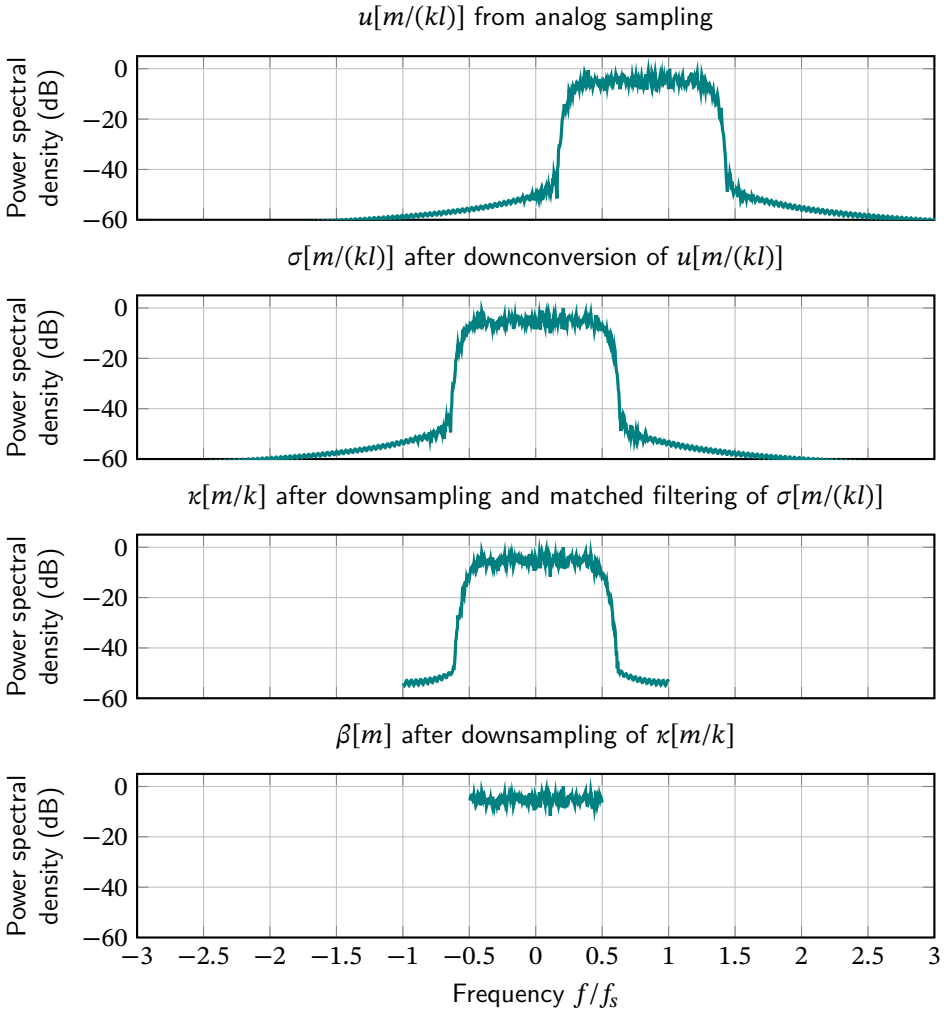


Figure 4.18.: Power spectrum of the symbol-decoding steps for a random QPSK symbol-sequence. The demodulated signal is a real-valued passband signal centered at the intermediate frequency (first row). After digital downconversion we have a complex-valued baseband signal, centered at zero frequency (second row). Applying the matched RRC filter completes the pulse-shaping (third row). Downsampling recovers the initial symbol band (last row).

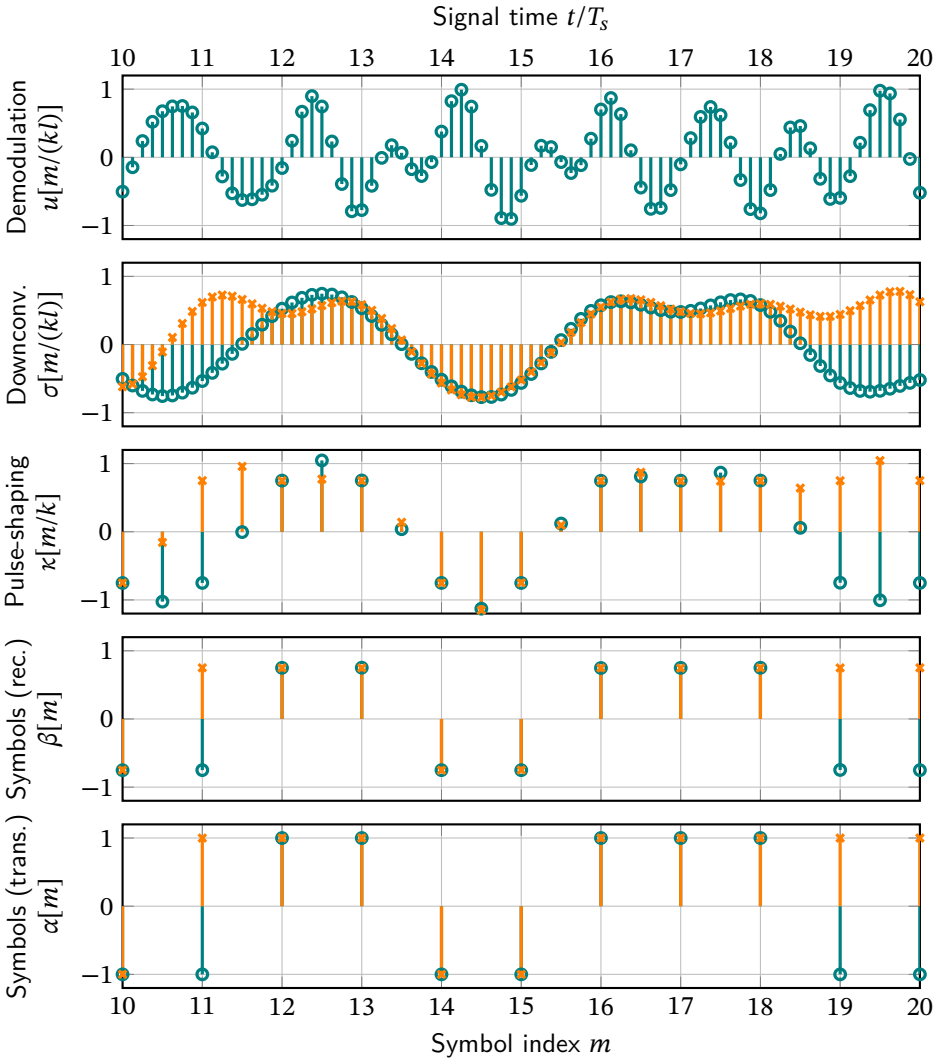


Figure 4.19.: Signal amplitude of the symbol decoding steps for a random QPSK symbol-sequence. The real-valued demodulated signal oscillates at the intermediate frequency (first row). Digital downconversion removed the intermediate frequency, yielding a complex signal (second row). Completing the pulse-shaping and downsampling by applying a matched RRC filter (third row). Downsampling recovers the complex symbol sequence equal to the transmitted sequence (fourth and last row).

Summary

We presented a software-defined coherent-state transmission system for en- and decoding of a complex symbol sequence onto and from an optical coherent state by following the signal processing across the quantum-optical, analog and digital domains. For simplicity, we assumed a perfect noiseless quantum channel without attenuation and perfect synchronization between the transmitter and receiver clocks.[8] Ref. [102] considers realistic quantum channels, like the quantum analog of the classical additive Gaussian white-noise channel. To extend the detection to nonclassical states, methods of quantum tomography, as discussed in, for example, Ref. [7], need to be considered.

Figure 4.20 summarizes the transmitter's signal processing in a block diagram. First, the complex digital signal corresponding to the symbol sequence $\alpha[n]$ are encoded in two real-valued bandwidth-optimized digital baseband signals. The digital baseband signals are transferred to the analog domain, where we upconvert them to a single passband signal. For

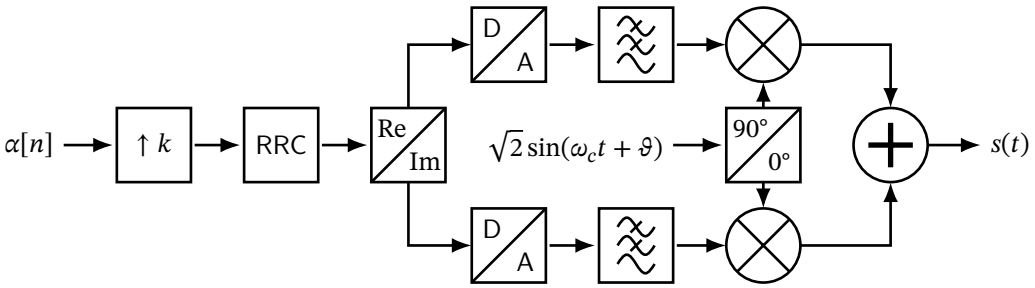


Figure 4.20.: Block diagram of the transmitter's signal processing. The real and imaginary part of a complex digital signal $\alpha[n]$ is upsampled, pulse-shaped and converted to anti-aliased analog signals, $x(t)$ and $p(t)$. The analog signals are individually mixed with a phase-shifted LO with carrier frequency ω_c and then added to yield a complex signal $\alpha(t)$.

the receiver we discussed the differences between a single, dual homo- and heterodyne receiver. With homodyning, the optical signal is directly downconverted without intermediate frequency, $\omega_i = 0$, while with heterodyning we have an intermediate frequency, which we remove in the digital domain. Although, homodyning directly reveals the quadrature information, it requires dual-quadrature downconversion in the electro-optical domain, increasing the hardware complexity. Using heterodyning both quadratures can be digitally restored given sufficient detector bandwidth. Figure 4.21 summarizes our heterodyning receiver's signal processing in a block diagram. First, the received passband signal $z(t)$ is downconverted to an intermediate (radio) frequency and converted to a digital signal. The digital signal is multiplied by a complex exponential removing the intermediate frequency

[8] Appendix D summarizes some important techniques to compensate for synchronization error of the optical LOs and the ADC clock.

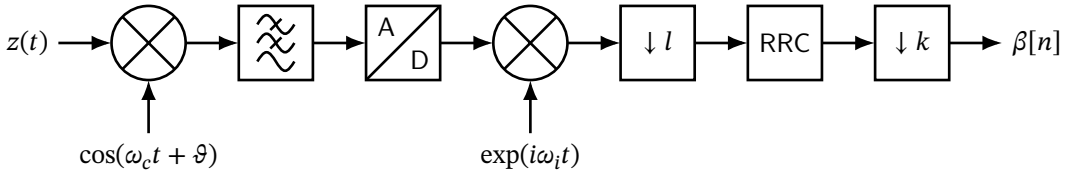


Figure 4.21.: Block diagram of the heterodying receiver's signal processing. The signal $z(t)$ is mixed with $\cos(\omega_c t+\vartheta)$. The mixed analog signal is bandwidth-limited through a LP filter and converted to the digital domain where it is digitally downconverted through multiplication with $\exp(i\omega_i t)$. The digitally downconverted signal is downsampled a first time for compatibility with the matched RRC filter and then downsampled a second time to recover the symbols.

and recovering dual-quadrature information. Finally, the pulse shaping is completed and the digital signal is downsampled to recover the digital signal $\beta[n]$ corresponding to the symbol sequence.

We found the coherent-state transformations for the IQM and balanced detector, derived in the previous chapter, to exactly implement the electro-optical up- and downconversion of the transmitter respectively receiver. Table 4.2 summarizes the relation between input

Signal-processing	Optical implementation	Input signal	Output signal
Upconversion	Modulation	$\alpha(t)$	$\lvert\alpha(t)e^{-i\omega_c t}\rangle$
Downconversion	Balanced detection	$\lvert\alpha(t)e^{-i\omega_c t}\rangle$	$\alpha(t)e^{-i\omega_i t}$

Table 4.2.: Electro-optical components implementing signal-processing operations with complex baseband signal $\alpha(t)$, optical carrier frequency ω_c and electrical intermediate frequency ω_i.

and output state and signals for the electro-optical components implementing the up- and downconversion. We have thus successfully bridged the gap between signal processing and quantum-optical communication.

Conclusion and outlook

This thesis aimed to outline the incorporation of quantum aspects into optical communication. By crafting a continuous-mode theory of light and applying it to describe electro-optical components essential for optical communication, we proposed a coherent-state transmission system as an extension of a classical optical transmission system to the quantum regime. The suggested coherent-state transmission system offers a platform to explore and formulate novel communication protocols inspired by classical communication and quantum mechanics, especially practical quantum-key distribution (QKD) protocols based on weak coherent states.

Next to the practical results of our work, we illuminate quantum aspects of light that have physical relevance but otherwise fall short, as our result on the generalized quadrature measurement shows. From an abstract point of view, we can draw two key lessons from our work. On the one hand, we need to be more careful in employing reductionism. Some concepts are notoriously difficult to grasp, and there exists no shortcut to understanding them truly. On the other hand, we need to be more encouraged to search for answers outside our traditional domain. In deriving a continuous-mode quantum theory of light from quantum field theory, we consciously opted against extending single-mode quantum optics, which turned out to be a key factor in our research's success, as there is more clarity in simplifying a complete theory as opposed to extending a simplified theory. Of course, this does not mean disavowing established methods. Rather it proves useful to switch perspectives from time to time. For example, towards the end of our research, it turned out to be favorable to move away from a constructive bottom-up approach and work our way backward from the classical results.

Our work is difficult to place into the existing literature, largely since our problem statement emerges from an applied industry-related setting. The closest to our research is Shapiro's work regarding a quantum theory of optical communication [19]. However, besides the photodetection, Shapiro approaches the topic from a quantum-information perspective and does neither consider a practical implementation nor a transmission setup. Concerning the quantum theory of light, we are the first to our knowledge to present a continuous-mode theory rooted in quantum field theory and emphasizing the communication aspects. The few existing references [10, 9] do not attempt to justify their results but apply their formalism towards quantum optics. For the quantum theory of electro-optical components, we have summarized and unified the existing literature, most notably the beam splitter [18, 17, 7], the photodetector [7, 8, 19], and the phase modulator [84, 81].

Some topics, e.g., quantum information and non-classical quantum states, require additional attention to complete a theoretical framework for quantum-optical communication not limited to practical QKD using weak coherent states. In addition, our description of the coherent-state transmission system misses a discussion of the quantum statistics and effects of a non-ideal quantum channel.

Even though our work leaves many open questions, it provides as many opportunities it provides, the most obvious being the transfer of classical communication protocols to QKD like, for example, orthogonal frequency-division multiplexing (OFDM) [103], which requires a continuous-mode theory of light. Another potential research direction concerns security proofs for practical QKD protocols based on weak coherent states. Specific to continuous-variable quantum-key distribution (CV-QKD), we can think of investigating mirror-band and frequency-entangled squeezed-states with our framework. More general, it would be interesting to follow up on the concept of a logical quantum channel investigating the equivalence of a tensor-product coherent-state transmission system with our continuous-time coherent-state transmission system. Such an equivalence, if confirmed, could be a useful tool to simplify existing and future security proofs. Last but not least, it would be interesting to extend our theoretical framework to the transmission of non-classical quantum states and discuss if and how one can make sense of a communication system conveying not classical but quantum information. One promising direction, which would benefit from our framework, is the transmission of frequency-entangled squeezed states, also known as broadband squeezed states [7, 8].

Appendix A.

Supplemental theorems to Maxwell field theory

In the present appendix, we provide supplementary theorems to support our claims of Chapter 2. As the following excerpts highlight, many proofs reduce to exercising operator algebra, which is rather verbose than interesting.

When working with the operator algebra of the Maxwell field, we frequently expand the Maxwell field into positive and negative frequency parts and sometimes into the annihilation and creation operators to invoke the canonical commutation relation (CCR). The following lemma is useful when working with both representations.

Lemma A.0.1. *Let $\hat{a}(\mathbf{k})$ and $\hat{a}^\dagger(\mathbf{k})$ be the annihilation and creation operator satisfying the CCR and $\hat{A}^{(\pm)}$ be the positive and negative frequency field operator, then the commutator of the annihilation and creation operator with the positive and negative smeared field operators yields*

$$[\hat{a}(\mathbf{p}), \hat{A}^{(+)}[f]] = +\frac{f\left(\omega(\mathbf{p}), \mathbf{p}\right)}{\sqrt{2\omega(\mathbf{p})}} \tag{A.0.1}$$

$$[\hat{a}^\dagger(\mathbf{p}), \hat{A}^{(-)}[f]] = -\frac{f\left(\omega(\mathbf{p}), \mathbf{p}\right)^*}{\sqrt{2\omega(\mathbf{p})}}. \tag{A.0.2}$$

Proof. Inserting the smeared field operator in momentum space and using the CCR to evaluate the integral yields the first identity

$$[\hat{a}(\mathbf{p}), \hat{A}^{(+)}[f]] = \int \frac{\mathrm{d}^3 q}{(2\pi)^3\sqrt{2\omega(\mathbf{q})}} f\left(\omega(\mathbf{q}), \mathbf{q}\right) [\hat{a}(\mathbf{p}), \hat{a}^\dagger(\mathbf{q})] = +\frac{f\left(\omega(\mathbf{p}), \mathbf{p}\right)}{\sqrt{2\omega(\mathbf{p})}}. \tag{A.0.3}$$

The second identity follows analog

$$[\hat{a}^\dagger(\mathbf{p}), \hat{A}^{(-)}[f]] = \int \frac{\mathrm{d}^3 q}{(2\pi)^3\sqrt{2\omega(\mathbf{q})}} f\left(\omega(\mathbf{q}), \mathbf{q}\right)^* [\hat{a}^\dagger(\mathbf{p}), \hat{a}(\mathbf{q})] = -\frac{f\left(\omega(\mathbf{p}), \mathbf{p}\right)^*}{\sqrt{2\omega(\mathbf{p})}}. \tag{A.0.4}$$

□

The number states form a countable and complete basis which heavily suggests employing mathematical induction as a proof technique. The following lemma turns out to be of great help in simplifying the induction steps.

Lemma A.0.2. *Let $\hat{a}(\mathbf{k})$ be the annihilation operator and $\hat{A}^{(-)}$ be the negative frequency field operator, then their commutator yields*

$$\hat{a}(\mathbf{p})|n_f\rangle = \sqrt{n}\frac{f(\omega(\mathbf{p}),\mathbf{p})}{\sqrt{2\omega(\mathbf{p})}}|n-1_f\rangle. \tag{A.0.5}$$

Proof. First, we note the recursive relation

$$\hat{a}(\mathbf{p})|n_f\rangle = \frac{1}{\sqrt{n}}\left[\frac{f(\omega(\mathbf{p}),\mathbf{p})}{\sqrt{2\omega(\mathbf{p})}}|n-1_f\rangle + \hat{A}^{(+)}[f]\hat{a}(\mathbf{p})|n-1_f\rangle\right], \tag{A.0.6}$$

where we used the commutator from lemma A.0.1. The induction start, $n = 0$, follows from the action of the annihilation operator on the vacuum state, eq. (2.2.7). The induction step, $n \to n+1$, goes

$$\begin{aligned}
\hat{a}(\mathbf{p})|n+1_f\rangle &= \frac{1}{\sqrt{n+1}}\hat{a}(\mathbf{p})\hat{A}^{(+)}[f]|n_f\rangle \\
&= \frac{1}{\sqrt{n+1}}\left[\frac{f(\omega(\mathbf{p}),\mathbf{p})}{\sqrt{2\omega(\mathbf{p})}} + \hat{A}^{(+)}[f]\hat{a}(\mathbf{p})\right]|n_f\rangle \\
&= \frac{1}{\sqrt{n+1}}\left[\frac{f(\omega(\mathbf{p}),\mathbf{p})}{\sqrt{2\omega(\mathbf{p})}}|n_f\rangle + \hat{A}^{(+)}[f]\sqrt{n}\frac{f(\omega(\mathbf{p}),\mathbf{p})}{\sqrt{2\omega(\mathbf{p})}}|n-1_f\rangle\right] \\
&= \frac{1}{\sqrt{n+1}}\frac{f(\omega(\mathbf{p}),\mathbf{p})}{\sqrt{2\omega(\mathbf{p})}}\left[|n_f\rangle + n|n_f\rangle\right] \\
&= \sqrt{n+1}\frac{f(\omega(\mathbf{p}),\mathbf{p})}{\sqrt{2\omega(\mathbf{p})}}|n_f\rangle,
\end{aligned} \tag{A.0.7}$$

where we used the recursive relation. □

With the help of lemma A.0.2, most of the expectation values of the number states follow easily, as we demonstrate with the expectation value of the momentum operator.

Theorem A.0.3. *Let $|n_f\rangle$ be a number state and $\hat{\mathbf{P}}$ be the momentum operator, eq.* (2.1.55)*, then*

$$\langle n_f|\hat{\mathbf{P}}|n_f\rangle = n\int \frac{\mathrm{d}^3p}{(2\pi)^3}\mathbf{p}\left|\frac{f(\omega(\mathbf{q}),\mathbf{q})}{\sqrt{2\omega(\mathbf{p})}}\right|^2. \tag{A.0.8}$$

Proof. We insert the definition of the momentum operator and use the action of the annihilation operator on the number state, lemma A.0.2, and the Hermitian conjugate thereof, i.e.,

$$\begin{aligned}\langle n_f|\hat{\mathbf{P}}|n_f\rangle &= \int \frac{\mathrm{d}^3p}{(2\pi)^3}\mathbf{p}\langle n_f|\hat{a}^\dagger(\mathbf{p})\hat{a}(\mathbf{p})|n_f\rangle \\ &= n\int \frac{\mathrm{d}^3p}{(2\pi)^3}\mathbf{p}\left|\frac{f(\omega(\mathbf{q}),\mathbf{q})}{\sqrt{2\omega(\mathbf{p})}}\right|^2\langle n-1_f|n-1_f\rangle,\end{aligned} \tag{A.0.9}$$

and are left to note that the number states are normalized to arrive at eq. (A.0.8). □

For the mean and variance of the electric field operator, we need the following lemma.

Lemma A.0.4. *Let $\hat{E}^{(+)}(t,\mathbf{x})$ and $\hat{E}^{(-)}(t,\mathbf{x})$ be the positive and negative frequency part of the electric field operator, then their commutator equals*

$$[\hat{E}^{(-)}(t,\mathbf{x}),\hat{E}^{(+)}(t,\mathbf{x})] = \frac{1}{2}\int\frac{\mathrm{d}^3p}{(2\pi)^3}\omega(\mathbf{p}), \tag{A.0.10}$$

known as the "vacuum energy".

Proof. Inserting the mode expansion of the positive and negative frequency operators and using the CCR of the annihilation and creation operator, we find

$$\begin{aligned}[\hat{E}^{(-)}(t,\mathbf{x}),\hat{E}^{(+)}(t,\mathbf{x})] &= \int\frac{\mathrm{d}^3p}{(2\pi)^3\sqrt{2\omega(\mathbf{p})}}\omega(\mathbf{p})e^{+i\omega(\mathbf{p})t-i\mathbf{p}\cdot\mathbf{x}} \\ &\quad+\int\frac{\mathrm{d}^3q}{(2\pi)^3\sqrt{2\omega(\mathbf{q})}}\omega(\mathbf{q})e^{-i\omega(\mathbf{q})t+i\mathbf{q}\cdot\mathbf{x}}[\hat{a}(\mathbf{p}),\hat{a}^\dagger(\mathbf{q})] \\ &= \int\frac{\mathrm{d}^3p}{(2\pi)^3\sqrt{2\omega(\mathbf{p})}}\omega(\mathbf{p})e^{+i\omega(\mathbf{p})t-i\mathbf{p}\cdot\mathbf{x}} \\ &\quad+\int\frac{\mathrm{d}^3q}{(2\pi)^3\sqrt{2\omega(\mathbf{q})}}\omega(\mathbf{q})e^{-i\omega(\mathbf{q})t+i\mathbf{q}\cdot\mathbf{x}}(2\pi)^3\delta^{(3)}(\mathbf{q}-\mathbf{p}) \\ &= \int\frac{\mathrm{d}^3p}{(2\pi)^32\omega(\mathbf{p})}\omega(\mathbf{p})^2.\end{aligned} \tag{A.0.11}$$

□

Although the "vacuum energy" appears to be infinite, our processes are always bandwidth-limited. We now employ lemma A.0.4 to find the mean and variance of the electric field operator with respect to a number state.

Theorem A.0.5. *Let $|n_f\rangle$ be a number state and $\hat{E}(t,\mathbf{x})$ be the electric field operator, then we have zero mean and variance equal to the vacuum energy plus the wave function probability, i.e.,*

$$\langle n_f|\hat{E}(t,\mathbf{x})|n_f\rangle = 0, \tag{A.0.12}$$

$$\langle n_f|\left(\Delta\hat{E}(t,\mathbf{x})\right)^2|n_f\rangle = \frac{1}{2}\int \frac{\mathrm{d}^3p}{(2\pi)^3}\omega(\mathbf{p}) + n|\Psi(t,\mathbf{x})|^2. \tag{A.0.13}$$

Proof. The expectation values of an unequal number of annihilation and creation operators is always zero. Expanding the electric field operator into positive and negative frequency parts

$$\langle n_f|\hat{E}(t,\mathbf{x})|n_f\rangle = \langle n_f|\hat{E}^{(-)}(t,\mathbf{x})|n_f\rangle + \langle n_f|\hat{E}^{(+)}(t,\mathbf{x})|n_f\rangle, \tag{A.0.14}$$

we note that the first term comprises $n+1$ annihilation and n creation operators, and the second term comprises n annihilation and $n+1$ creation operators, i.e., an unequal number of annihilation and creation operators, and conclude that the expectation value is zero. The variance is equal to the second moment as the first moment is zero

$$\langle n_f|\left(\Delta\hat{E}(t,\mathbf{x})\right)^2|n_f\rangle = \langle n_f|\hat{E}(t,\mathbf{x})^2|n_f\rangle = \langle n_f|\hat{E}^{(+)}(t,\mathbf{x})\hat{E}^{(-)}(t,\mathbf{x})|n_f\rangle + \text{H.c.} \tag{A.0.15}$$

where we expanded the square of the electric field operator in its positive and negative frequency parts and used that only mixed terms survive in the second equation. Using lemma A.0.4, we can rewrite

$$\langle n_f|\left(\Delta\hat{E}(t,\mathbf{x})\right)^2|n_f\rangle = \frac{1}{2}\int \frac{\mathrm{d}^3p}{(2\pi)^3}\omega(\mathbf{p}) + 2\langle n_f|\hat{E}^{(+)}(t,\mathbf{x})\hat{E}^{(-)}(t,\mathbf{x})|n_f\rangle \tag{A.0.16}$$

and are left to evaluate the remaining mixed frequency term. Using lemma A.0.2, we find

$$\begin{aligned}
\langle n_f|\hat{E}^{(+)}(t,\mathbf{x})\hat{E}^{(-)}(t,\mathbf{x})|n_f\rangle &= \int \frac{\mathrm{d}^3p}{(2\pi)^3\sqrt{2\omega(\mathbf{p})}}\omega(\mathbf{p})e^{+i\omega(\mathbf{p})t-i\mathbf{p}\cdot\mathbf{x}} \\
&\quad\times\int \frac{\mathrm{d}^3q}{(2\pi)^3\sqrt{2\omega(\mathbf{q})}}\omega(\mathbf{q})e^{-i\omega(\mathbf{q})t+i\mathbf{q}\cdot\mathbf{x}} \\
&\quad\times\langle n_f|\hat{a}^\dagger(\mathbf{p})\hat{a}(\mathbf{q})|n_f\rangle \\
&= \frac{n}{2}\left|\int \frac{\mathrm{d}^3p}{(2\pi)^3} f\left(\omega(\mathbf{p}),\mathbf{p}\right)e^{+i\omega(\mathbf{p})t-i\mathbf{p}\cdot\mathbf{x}}\right|^2 \\
&= \frac{n}{2}|\Psi(t,\mathbf{x})|^2,
\end{aligned} \tag{A.0.17}$$

where we identified the momentum space representation of the momentum distribution with the probability of the wave function. □

Unlike in single-mode quantum optics, the variance of the electric field of a number state contains a contribution from the wave function. Let us now find the mean and variance of the electric field operator with respect to a coherent state.

Theorem A.0.6. *Let $|\alpha\rangle$ be a coherent state and $\hat{E}(t,\mathbf{x})$ be the electric field operator, then the electric field's mean evaluates to*

$$\langle\alpha|\hat{E}(t,\mathbf{x})|\alpha\rangle = \frac{i}{2}\int \frac{\mathrm{d}^3p}{(2\pi)^3}\left\{\alpha(\mathbf{p})e^{+i\omega(\mathbf{p})t-i\mathbf{p}\cdot\mathbf{x}} - \alpha(\mathbf{p})^* e^{-i\omega(\mathbf{p})t+i\mathbf{p}\cdot\mathbf{x}}\right\} \tag{A.0.18}$$

Proof. Inserting the positive and negative parts of the electric field operator

$$\langle\alpha|\hat{E}(t,\mathbf{x})|\alpha\rangle = \langle\alpha|\hat{E}^{(-)}(t,\mathbf{x})|\alpha\rangle + \langle\alpha|\hat{E}^{(+)}(t,\mathbf{x})|\alpha\rangle, \tag{A.0.19}$$

we evaluate the first term using that the coherent state is eigenstate of the annihilation operator, eq. (2.2.57),

$$\begin{aligned}
\hat{E}^{(-)}(t,\mathbf{x})|\alpha\rangle &= -i\int \frac{\mathrm{d}^3p}{(2\pi)^3\sqrt{2\omega(\mathbf{p})}}\omega(\mathbf{p})e^{-i\omega(\mathbf{p})t+i\mathbf{p}\cdot\mathbf{x}}\hat{a}(\mathbf{p})|\alpha\rangle \\
&= -i\int \frac{\mathrm{d}^3p}{(2\pi)^3\sqrt{2\omega(\mathbf{p})}}\omega(\mathbf{p})e^{-i\omega(\mathbf{p})t+i\mathbf{p}\cdot\mathbf{x}}\frac{\alpha(\mathbf{p})}{\sqrt{2\omega(\mathbf{p})}}|\alpha\rangle \\
&= -\frac{i}{2}\int \frac{\mathrm{d}^3p}{(2\pi)^3}\alpha(\mathbf{p})e^{-i\omega(\mathbf{p})t+i\mathbf{p}\cdot\mathbf{x}}|\alpha\rangle.
\end{aligned}$$

Using the normalization of the coherent states the expectation value equals

$$\begin{aligned}
\langle\alpha|\hat{E}(t,\mathbf{x})|\alpha\rangle &= \frac{1}{2i}\int \frac{\mathrm{d}^3p}{(2\pi)^3}\alpha(\mathbf{p})e^{-i\omega(\mathbf{p})t+i\mathbf{p}\cdot\mathbf{x}} - \text{c.c.} \\
&= \mathrm{Im}\int \frac{\mathrm{d}^3p}{(2\pi)^3}\alpha(\mathbf{p})e^{-i\omega(\mathbf{p})t+i\mathbf{p}\cdot\mathbf{x}},
\end{aligned} \tag{A.0.20}$$

resembling a superposition of plane-waves in three dimensions. □

Theorem A.0.7. *Let $|\alpha\rangle$ be a coherent state and $\hat{E}(t,\mathbf{x})$ be the electric field operator, then the electric field's variance evaluates to*

$$\langle\alpha|\left(\Delta\hat{E}(t,\mathbf{x})\right)^2|\alpha\rangle = \frac{1}{2}\int \frac{\mathrm{d}^3p}{(2\pi)^3}\omega(\mathbf{p}) \tag{A.0.21}$$

Proof. We expand the square of the electric field operator and invoke lemma A.0.4 to replace one of the mixed-frequency terms, i.e.,

$$\begin{aligned}
\hat{E}(t,\mathbf{x})^2 &= \left[\hat{E}^{(+)}(t,\mathbf{x}) + \hat{E}^{(-)}(t,\mathbf{x})\right]^2 \\
&= \hat{E}^{(+)}(t,\mathbf{x})^2 + \hat{E}^{(-)}(t,\mathbf{x})^2 + \hat{E}^{(+)}(t,\mathbf{x})\hat{E}^{(-)}(t,\mathbf{x}) + \hat{E}^{(-)}(t,\mathbf{x})\hat{E}^{(+)}(t,\mathbf{x}) \\
&= \frac{1}{2}\int \frac{\mathrm{d}^3p}{(2\pi)^3}\omega(\mathbf{p}) + \hat{E}^{(+)}(t,\mathbf{x})^2 + \hat{E}^{(-)}(t,\mathbf{x})^2 + 2\hat{E}^{(+)}(t,\mathbf{x})\hat{E}^{(-)}(t,\mathbf{x}).
\end{aligned} \tag{A.0.22}$$

For the mixed-frequency term, we find

$$\begin{aligned}\langle\alpha|\hat{E}^{(+)}(t,\mathbf{x})\hat{E}^{(-)}(t,\mathbf{x})|\alpha\rangle &= \langle\alpha|\left(+i\int\frac{\mathrm{d}^3p}{(2\pi)^2\sqrt{2\omega(\mathbf{p})}}\omega(\mathbf{p})\hat{a}^\dagger(\mathbf{p})e^{+i\omega(\mathbf{p})t-i\mathbf{p}\cdot\mathbf{x}}\right)\\ &\quad\times\left(-i\int\frac{\mathrm{d}^3q}{(2\pi)^2\sqrt{2\omega(\mathbf{q})}}\omega(\mathbf{q})\hat{a}(\mathbf{q})e^{-i\omega(\mathbf{q})t+i\mathbf{q}\cdot\mathbf{x}}\right)|\alpha\rangle\\ &= \langle\alpha|\left(+\frac{i}{2}\int\frac{\mathrm{d}^3p}{(2\pi)^2}\alpha(\mathbf{p})^*e^{+i\omega(\mathbf{p})t-i\mathbf{p}\cdot\mathbf{x}}\right)\\ &\quad\times\left(-\frac{i}{2}\int\frac{\mathrm{d}^3p}{(2\pi)^2}\alpha(\mathbf{p})e^{-i\omega(\mathbf{p})t+i\mathbf{p}\cdot\mathbf{x}}\right)|\alpha\rangle\\ &= \frac{1}{4}\left|\int\frac{\mathrm{d}^3p}{(2\pi)^2}\alpha(\mathbf{p})e^{-i\omega(\mathbf{p})t+i\mathbf{p}\cdot\mathbf{x}}\right|^2.\end{aligned} \tag{A.0.23}$$

For the positive-frequency term, we find

$$\begin{aligned}\langle\alpha|\hat{E}^{(+)}(t,\mathbf{x})^2|\alpha\rangle &= \langle\alpha|\left(+\frac{i}{2}\int\frac{\mathrm{d}^3p}{(2\pi)^3}\alpha(\mathbf{p})^*e^{+i\omega(\mathbf{p})t-i\mathbf{p}\cdot\mathbf{x}}\right)^2|\alpha\rangle\\ &= -\frac{1}{4}\left(\int\frac{\mathrm{d}^3p}{(2\pi)^3}\alpha(\mathbf{p})^*e^{+i\omega(\mathbf{p})t-i\mathbf{p}\cdot\mathbf{x}}\right)^2,\end{aligned} \tag{A.0.24}$$

and for the negative-frequency term, we find

$$\langle\alpha|\hat{E}^{(+)}(t,\mathbf{x})^2|\alpha\rangle = -\frac{1}{4}\left(\int\frac{\mathrm{d}^3p}{(2\pi)^3}\alpha(\mathbf{p})e^{-i\omega(\mathbf{p})t+i\mathbf{p}\cdot\mathbf{x}}\right)^2. \tag{A.0.25}$$

We now define

$$z(t,\mathbf{x}) = \int\frac{\mathrm{d}^3p}{(2\pi)^3}\alpha(\mathbf{p})e^{-i\omega(\mathbf{p})t+i\mathbf{p}\cdot\mathbf{x}} \tag{A.0.26}$$

and find for the second moment

$$\begin{aligned}\langle\alpha|\hat{E}(t,\mathbf{x})^2|\alpha\rangle &= \frac{1}{2}\int\frac{\mathrm{d}^3p}{(2\pi)^3}\omega(\mathbf{p}) + \frac{1}{4}\left[2|z(t,\mathbf{x})|^2 - z(t,\mathbf{x})^2 - (z(t,\mathbf{x})^*)^2\right]\\ &= \frac{1}{2}\int\frac{\mathrm{d}^3p}{(2\pi)^3}\omega(\mathbf{p}) + \frac{1}{2}|z(t,\mathbf{x})|^2.\end{aligned} \tag{A.0.27}$$

For the square of the first moment, we find

$$\begin{aligned}\langle\alpha|\hat{E}(t,\mathbf{x})|\alpha\rangle^2 &= \left[\frac{i}{2}z(t,\mathbf{x}) - \frac{i}{2}z(t,\mathbf{x})^*\right]^2\\ &= -\frac{1}{4}\left[z(t,\mathbf{x})^2 + (z(t,\mathbf{x})^*)^2 - 2|z(t,\mathbf{x})|^2\right]\\ &= +\frac{1}{2}|z(t,\mathbf{x})|^2\end{aligned} \tag{A.0.28}$$

such that the total variance is equal to

$$\begin{aligned}\langle\alpha|\left(\Delta\hat{E}(t,\mathbf{x})\right)^2|\alpha\rangle &= \langle\alpha|\hat{E}(t,\mathbf{x})^2|\alpha\rangle - \langle\alpha|\hat{E}(t,\mathbf{x})|\alpha\rangle^2 \\ &= \frac{1}{2}\int\frac{\mathrm{d}^3p}{(2\pi)^3}\omega(\mathbf{p}).\end{aligned} \tag{A.0.29}$$

□

Appendix B.

Nonlinear interaction theory

In the following, we summarize some results on nonlinear (quantum-)optics from Refs. [104, 90, 81, 8], which are important for describing the linear electro-optic effect, essential for our investigation of the phase modulator.

We start by looking into the Pockels effect by investigating the interaction of the classical electric field with a dielectric exhibiting a nonlinear susceptibility. The electric displacement field, in the frequency domain given by [8, p. 1070]

$$D_i(\omega) = E_i(\omega) + P_i(\omega), \tag{B.0.1}$$

accounts for macroscopic effects through the macroscopic polarization density P_i. Although the Pockels effect causes a linear change of the refractive index by an external electric field, it is macroscopically described by the second-order macroscopic polarization density, in the time domain given by [90, p. 55]

$$P_i^{(2)}(t) = \int \mathrm{d}t_1 \int \mathrm{d}t_2 \, \chi_{ijk}^{(2)}(t_1, t_2) E^j(t - t_1) E^k(t - t_2) \tag{B.0.2}$$

wherein $\chi_{ijk}^{(2)}(t_1, t_2)$ is the second-order time-response tensor of the dielectric. Inserting the Fourier transform of the electric field components, we find

$$P_i^{(2)}(t) = \int \frac{\mathrm{d}\omega_1}{2\pi} \int \frac{\mathrm{d}\omega_2}{2\pi} \chi_{ijk}^{(2)}(\omega_1, \omega_2) E^j(\omega_1) E^k(\omega_2) e^{-i(\omega_1+\omega_2)t} \tag{B.0.3}$$

wherein the second-order frequency-response tensor is the Fourier transform of the time-response tensor, i.e.,

$$\chi_{ijk}^{(2)}(\omega_1, \omega_2) = \int \mathrm{d}t_1 \int \mathrm{d}t_2 \, \chi_{ijk}^{(2)}(t_1, t_2) e^{+i\omega_1 t} e^{+i\omega_2 t}. \tag{B.0.4}$$

The Fourier transform of the second-order polarization density turns out to be

$$\begin{aligned} P_i^{(2)}(\omega) &= \int \mathrm{d}t\, P_i^{(2)}(t) e^{+i\omega t} \\ &= \int \frac{\mathrm{d}\omega_1}{2\pi} \int \frac{\mathrm{d}\omega_2}{2\pi} \chi_{ijk}^{(2)}(\omega_1, \omega_2) E^j(\omega_1) E^k(\omega_2) \int \mathrm{d}t\, e^{-i(\omega_1+\omega_2-\omega)t} \\ &= \int \frac{\mathrm{d}\omega_1}{2\pi} \int \frac{\mathrm{d}\omega_2}{2\pi} \chi_{ijk}^{(2)}(\omega_1, \omega_2) E^j(\omega_1) E^k(\omega_2) (2\pi)\delta^{(1)}(\omega_2 - \omega + \omega_1) \\ &= \int \frac{\mathrm{d}\omega'}{2\pi} \chi_{ijk}^{(2)}(\omega', \omega - \omega') E^j(\omega') E^k(\omega - \omega'). \end{aligned} \tag{B.0.5}$$

The presence of the integral in eq. (B.0.5) breaks the linearity in the electric field E^k. To restore linearity, the external electric field is assumed to be effectively static, simplifying the second-order polarization density to [90, p. 495]

$$P_i^{(2)}(\omega) = \chi_{ijk}^{(2)}(0, \omega) E^j(0) E^k(\omega). \tag{B.0.6}$$

Inserting the so linearized second-order polarization density and inserting it into eq. (B.0.1),

$$\begin{aligned} D_i(\omega) &= E_i(\omega) + \chi_{ijk}^{(2)}(0, \omega) E^j(0) E^k(\omega) \\ &= \left[\delta_{ik} + \chi_{ijk}^{(2)}(0, \omega) E^j(0)\right] E^k(\omega), \end{aligned} \tag{B.0.7}$$

we can read off the electric susceptibility tensor

$$\varepsilon_{ik}(\omega) = \delta_{ik} + \chi_{ijk}^{(2)}(0, \omega) E^j(0). \tag{B.0.8}$$

The refractive-index tensor is defined as the square root of the electric susceptibility tensor [105, p. 3]

$$n_{ij}(\omega) = \sqrt{\varepsilon_{ij}} \approx n_{ik}^{(0)}(\omega) + n_{ijk}^{(1)}(\omega) E^j(0), \tag{B.0.9}$$

where we performed a series expansion of the square root and introduced the refractive-index coefficients [106]

$$n_{ik}^{(0)}(\omega) = \sqrt{1 + \chi_{ij}^{(1)}(\omega)} \qquad n_{ijk}^{(1)}(\omega) = \frac{\chi_{ijk}^{(2)}(\omega)}{2\sqrt{1 + \chi_{ij}^{(1)}(\omega)}}. \tag{B.0.10}$$

With eq. (B.0.9), we have shown the linear change of the refractive index with an external electric field. However, it was necessary to assume the external electric field to be effectively static in time to linearize the second-order macroscopic polarization density.

For a simple quantum treatment, we replace the classical fields with their respective free-field operator. For instance, the quantum Hamiltonian of the electromagnetic field in a dielectric is [107, p. 124]

$$\hat{H} = \frac{1}{2} \int \mathrm{d}^3x \left\{\hat{E}^i(t, \mathbf{x}) \hat{D}_i(t, \mathbf{x}) + \hat{B}^i(t, \mathbf{x}) \hat{B}_i(t, \mathbf{x})\right\}, \tag{B.0.11}$$

wherein $\hat{D}_i(t,\mathbf{x})$ is the electric displacement operator. Expanding the electric displacement operator in terms of the macroscopic polarization-density operators, we find the interaction Hamiltonian to involve three electric fields, i.e.,

$$\begin{aligned}\hat{H}^{(2)}_{\text{int}}(t) &= \frac{1}{2}\int \mathrm{d}^3x\, \hat{E}^i(t,\mathbf{x})\hat{P}^{(2)}_i(t,\mathbf{x}) \\ &= \frac{1}{2}\int \mathrm{d}^3x \int \mathrm{d}t_1 \int \mathrm{d}t_2\, \chi^{(2)}_{ijk}(t_1,t_2,\mathbf{x})\hat{E}^i(t,\mathbf{x})\hat{E}^j(t-t_1,\mathbf{x})\hat{E}^k(t-t_2,\mathbf{x}) \\ &\approx \frac{1}{2}\int \mathrm{d}z \int \mathrm{d}t_1 \int \mathrm{d}t_2\, \chi^{(2)}(t_1,t_2,z)\hat{E}(t,z)\hat{E}(t-t_1,z)\hat{E}(t-t_2,z),\end{aligned} \tag{B.0.12}$$

where we assumed the electric fields to be polarized along the same axis in the last step and ignored the transverse mode profile. Expanding the electric field operators into positive and negative frequency parts reveals the possible absorption and emission processes. For frequency conversion, we drop all but the following terms

$$\hat{H}^{\text{FC}}_{\text{int}}(t) \approx \frac{1}{2}\int \mathrm{d}z \int \mathrm{d}t_1 \int \mathrm{d}t_2\, \chi^{(2)}(t_1,t_2,z)\hat{E}^{(+)}(t,z)\hat{E}^{(-)}(t-t_1,z)\hat{E}^{(-)}(t-t_2,z) + \text{H.c.}. \tag{B.0.13}$$

Inserting the plane-wave expansion of the positive- and negative-frequency electric-field operators, eqs. (2.1.50) and (2.1.51),

$$\begin{aligned}\hat{H}^{\text{FC}}_{\text{int}}(t) &= \frac{1}{2}\int \mathrm{d}z \int \mathrm{d}t_1 \int \mathrm{d}t_2\, \chi^{(2)}(t_1,t_2,z) \int \frac{\mathrm{d}\omega_1}{2\pi}\int \frac{\mathrm{d}\omega_2}{2\pi}\int \frac{\mathrm{d}\omega_3}{2\pi}\omega_1\omega_2\omega_3 \\ &\qquad \times \hat{a}^\dagger(\omega_1)\hat{a}(\omega_2)\hat{a}(\omega_3)e^{+i\omega_1(t-z)}e^{-i\omega_2(t-t_1)+i\omega_2 z}e^{-i\omega_3(t-t_2)+i\omega_3 z} + \text{H.c.} \\ &= \frac{1}{2}\int \frac{\mathrm{d}\omega_1}{2\pi}\int \frac{\mathrm{d}\omega_2}{2\pi}\int \frac{\mathrm{d}\omega_3}{2\pi}\omega_1\omega_2\omega_3 \int \mathrm{d}z\, \chi^{(2)}(\omega_2,\omega_3,z) \\ &\qquad \times \hat{a}^\dagger(\omega_1)\hat{a}(\omega_2)\hat{a}(\omega_3)e^{+i(\omega_1-\omega_2-\omega_3)t}e^{-i(\omega_1-\omega_2-\omega_3)z} + \text{H.c.},\end{aligned} \tag{B.0.14}$$

where we identified the Fourier transform of the second-order electric susceptibility

$$\chi^{(2)}(\omega_2,\omega_3,z) = \int \mathrm{d}t_1 \int \mathrm{d}t_2\, \chi^{(2)}(t_1,t_2,z)e^{+i\omega_2 t_1}e^{+i\omega_3 t_2}. \tag{B.0.15}$$

We assume the second-order electric susceptibility to be constant over the interaction length L and zero otherwise, then we can further simplify the frequency-conversion Hamiltonian to

$$\hat{H}^{\text{FC}}_{\text{int}}(t) = \frac{1}{2}\int \frac{\mathrm{d}\omega_1}{2\pi}\int \frac{\mathrm{d}\omega_2}{2\pi}\int \frac{\mathrm{d}\omega_3}{2\pi} g(\omega_1,\omega_2,\omega_3)\hat{a}^\dagger(\omega_1)\hat{a}(\omega_2)\hat{a}(\omega_3)e^{+i(\omega_1-\omega_2-\omega_3)t} + \text{H.c.}, \tag{B.0.16}$$

where we introduced the phase-matching function

$$g(\omega_1,\omega_2,\omega_3) = \omega_1\omega_2\omega_3\chi^{(2)}(\omega_2,\omega_3)\,\mathrm{sinc}\left(\frac{\omega_1-\omega_2-\omega_3}{L/2}\right). \tag{B.0.17}$$

Approximating the phase-matching function with a Delta distribution,

$$g(\omega_1,\omega_2,\omega_3) \approx g(\omega_1,\omega_2)(2\pi))\delta^{(1)}(\omega_1-\omega_2-\omega_3), \tag{B.0.18}$$

the interaction Hamiltonian further simplifies to

$$\hat{H}_{\text{int}}^{\text{FC}} = \frac{1}{2}\int \frac{\mathrm{d}\omega_1}{2\pi}\int \frac{\mathrm{d}\omega_2}{2\pi} g(\omega_1,\omega_2)\hat{a}^\dagger(\omega_1)\hat{a}(\omega_2)\hat{a}(\omega_1-\omega_2) + \text{H.c.}, \tag{B.0.19}$$

which agrees in the most important characteristics with the result reported in Ref. [84, eq. 35].

Appendix C.

Photodetection theory

This section aims to derive the differential photoelectron-emission probability from which one can derive the photocurrent operator. Our derivation summarizes the steps in Refs. [8, 7] but adds additional details on the truncated steps.

The transition of a bound electron to a free photoelectron is a probabilistic process. Let $|i\rangle$ and $|f\rangle$ denote the initial and final light states, and let $|g\rangle$ and $|e\rangle$ be the electron ground and excited states. The probability for the transition, $|g,i\rangle \to |e,f\rangle$, from time t to $t+\Delta t$ is equal to

$$|\langle e,f|\hat{U}_{\text{int}}(t,t+\Delta t)|g,i\rangle|^2, \tag{C.0.1}$$

wherein $\hat{U}_{\text{int}}$ is the time-evolution operator of the photo-atom interaction in the dipole approximation [8, p. 689],

$$\hat{U}_{\text{int}}(t,t+\Delta t) = \mathcal{T}_+ \exp\left\{-i\int_t^{t+\Delta t} \mathrm{d}t'\, \hat{H}_{\text{int}}(t')\right\} \qquad \hat{H}_{\text{int}}(t) = -\hat{\mathbf{p}}(t)\cdot\hat{\mathbf{A}}(t) \tag{C.0.2}$$

with $\hat{\mathbf{p}}$ being the electron's momentum operator, $\hat{\mathbf{A}}(t) = \hat{\mathbf{A}}(t,\mathbf{x}_0)$ being the Maxwell field in the Coulomb gauge approximated at the atom center of mass (COM), and $\mathcal{T}_+$ denoting (forward) time-ordering. In the more general density operator formailism eq. (C.0.1) reads [8, p. 686]

$$\begin{aligned}
|\langle e,f|\hat{U}_{\text{int}}(t,t+\Delta t)|g,i\rangle|^2 &= \langle e,f|\hat{U}_{\text{int}}(t,t+\Delta t)|g,i\rangle\langle g,i|\hat{U}_{\text{int}}(t,t+\Delta t)^\dagger|e,f\rangle \\
&= \mathrm{Tr}\Big\{\langle e,f|\hat{U}_{\text{int}}(t,t+\Delta t)|g,i\rangle\langle g,i|\hat{U}_{\text{int}}(t,t+\Delta t)^\dagger|e,f\rangle\Big\} \\
&= \mathrm{Tr}\Big\{|e,f\rangle\langle e,f|\hat{U}_{\text{int}}(t,t+\Delta t)|g,i\rangle\langle g,i|\hat{U}_{\text{int}}(t,t+\Delta t)^\dagger\Big\} \\
&= \mathrm{Tr}\Big\{\hat{\varrho}_{e,f}\hat{U}_{\text{int}}(t,t+\Delta t)\hat{\rho}(t)\hat{U}_{\text{int}}(t,t+\Delta t)^\dagger\Big\} \\
&= \mathrm{Tr}\Big\{\hat{\varrho}_{e,f}\hat{\rho}(t+\Delta t)\Big\},
\end{aligned} \tag{C.0.3}$$

wherein we used that the trace of a scalar is the scalar in the second line and the cyclic property of the trace in the third line. Performing the Magnus expansion of the time-evolution operator, eq. (C.0.2), up to the first term,

$$\hat{U}_{\text{int}}(t, t+\Delta t) \approx \exp\left\{-i \int_t^{t+\Delta t} \mathrm{d}t' \, \hat{H}_{\text{int}}(t')\right\}, \tag{C.0.4}$$

we use it to evolve the state in eq. (C.0.3),

$$\begin{aligned}\hat{\rho}(t+\Delta t) &= \hat{U}_{\text{int}}(t, t+\Delta t)\hat{\rho}(t)\hat{U}_{\text{int}}(t, t+\Delta t)^\dagger \\ &= \hat{\rho}(t) + (-i)\int_t^{t+\Delta t} \mathrm{d}t_1 [\hat{H}_{\text{int}}(t_1), \hat{\rho}(t_0)] \\ &\quad \times + \frac{(-i)^2}{2!}\int_t^{t+\Delta t} \mathrm{d}t_1 \int_t^{t_1} \mathrm{d}t_2 [\hat{H}_{\text{int}}(t_1), [\hat{H}_{\text{int}}(t_2), \hat{\rho}(t)]] + \ldots\end{aligned} \tag{C.0.5}$$

where the second equation follows from the Baker-Campbell-Hausdorff (BCH) formula. Inserting the expansion into the photoemission probability, eq. (C.0.3), the first two term vanish due to orthogonality with $\hat{\varrho}_{e,f}$ [8, p. 686], leaving us with

$$\begin{aligned}\mathrm{Tr}\left\{\hat{\varrho}_{e,f}\hat{\rho}(t_0+\Delta t)\right\} &= \int_t^{t+\Delta t} \mathrm{d}t_1 \int_t^{t_1} \mathrm{d}t_2 \, \mathrm{Tr}\left\{\hat{\varrho}_{e,f}\hat{H}_{\text{int}}(t_1)\hat{\rho}(t)\hat{H}_{\text{int}}(t_2)\right\} + \text{c.c.} \\ &= \int_t^{t+\Delta t} \mathrm{d}t_1 \int_t^{t_1} \mathrm{d}t_2 \langle e, f|\hat{H}_{\text{int}}(t_1)\hat{\rho}(t)\hat{H}_{\text{int}}(t_2)|e, f\rangle + \text{c.c.}.\end{aligned} \tag{C.0.6}$$

Inserting the interaction Hamiltonian, eq. (C.0.2), into our previous result, we find [8, p. 693]

$$\begin{aligned}\mathrm{Tr}\left\{\hat{\varrho}_{e,f}\hat{\rho}(t_0+\Delta t)\right\} = \langle e|\hat{p}^i|g\rangle\langle g|\hat{p}^j|e\rangle \int_t^{t+\Delta t} \mathrm{d}t_1 \int_t^{t_1} \mathrm{d}t_2 \\ \times \langle f|\hat{A}_i(t_1)|i\rangle\langle i|\hat{A}_j(t_2)|f\rangle e^{i(E_e-E_g)(t_1-t_2)} + \text{c.c.},\end{aligned} \tag{C.0.7}$$

wherein we used the energy eigenvalues of the electron's ground and excited state, $|g\rangle, |e\rangle$. The final states of the light field are of no interest to use and can be marginalized [8, p. 694], i.e.,

$$\begin{aligned}\sum_f \mathrm{Tr}\left\{\hat{\varrho}_{e,f}\hat{\rho}(t_0+\Delta t)\right\} = \langle e|\hat{p}^i|g\rangle\langle g|\hat{p}^j|e\rangle \int_t^{t+\Delta t} \mathrm{d}t_1 \int_t^{t_1} \mathrm{d}t_2 \\ \times \langle i|\hat{A}_i(t_1)\hat{A}_j(t_2)|i\rangle e^{i(E_e-E_g)(t_1-t_2)} + \text{c.c.}\end{aligned} \tag{C.0.8}$$

and we conclude the probability for a single photoelectron to be emitted between time t and $t+\Delta t$ to be

$$p(t, \Delta t) = \int_t^{t+\Delta t} \mathrm{d}t_1 \int_t^{t_1} \mathrm{d}t_2 \, k^{ij}(t_1 - t_2)\langle \hat{A}_i(t_1)\hat{A}_j(t_2)\rangle + \text{c.c.}, \tag{C.0.9}$$

wherein $k_{ij}(t)$ is the effective response function of the detector atom[1], and the expectation value of the Maxwell field two-point correlation function is with respect to the initial light state. It is possible to show that only the normal-ordered Maxwell field expectation value contributes to the photoemission probability [8, p. 696]

$$p(t,\Delta t) = \int_t^{t+\Delta t} \mathrm{d}t_1 \int_t^{t_1} \mathrm{d}t_2\, k^{ij}(t_1 - t_2) \langle : \hat{A}_i(t_1)\hat{A}_j(t_2) : \rangle + \text{c.c.}. \tag{C.0.10}$$

We select a coordinate system in which the Maxwell field propagates along the z direction, then one can show [99] that

$$\begin{aligned} p(t,\Delta t) &= \int_t^{t+\Delta t} \mathrm{d}t_1 \int_t^{t_1} \mathrm{d}t_2\, k(t_1 - t_2) \sum_{\lambda=1,2} \langle : \hat{A}_\lambda(t_1)\hat{A}_\lambda(t_2) : \rangle \\ &= \int_t^{t+\Delta t} \mathrm{d}t_1 \int_t^{t_1} \mathrm{d}t_2\, k(t_1 - t_2) \langle : \hat{A}(t_1)\hat{A}(t_2) : \rangle + \text{c.c.}, \end{aligned} \tag{C.0.11}$$

wherein we defined the scalar polarization-averaged Maxwell field and have the effective response function

$$k(t) = \int_0^\infty \frac{\mathrm{d}E}{2\pi} K(E) e^{-i(E-E_g)t} \tag{C.0.12}$$

with $K(E)$ being a function of the electron wave function along the xy plane.

Expanding the normal-ordered two-point correlation function of the Maxwell field into positive and negative frequency parts

$$\begin{aligned} \langle : \hat{A}_i(t_1)\hat{A}_j(t_2) : \rangle &= \langle : \left[\hat{A}_i^{(-)}(t_1) + \hat{A}_i^{(+)}(t_1)\right]\left[\hat{A}_j^{(-)}(t_2) + \hat{A}_j^{(+)}(t_2)\right] : \rangle \\ &= \langle \hat{A}_i^{(+)}(t_1)\hat{A}_j^{(-)}(t_2)\rangle + \langle \hat{A}_i^{(+)}(t_2)\hat{A}_j^{(-)}(t_1)\rangle, \end{aligned} \tag{C.0.13}$$

where the non-mixed frequency terms vanish because they contain an unequal number of annihilation and creation operators [92, p. 134]. Inserting the mixed frequency terms into the photoemission probability and expanding the effective detector response function in the frequency domain, we drop the highly oscillatory terms and find[2]

$$p(t,\Delta t) = \int_t^{t+\Delta t} \mathrm{d}t_1 \int_t^{t_1} \mathrm{d}t_2\, k^{ij}(t_1 - t_2) \langle \hat{A}_i^{(+)}(t_1)\hat{A}_j^{(-)}(t_2)\rangle + \text{c.c.}. \tag{C.0.14}$$

The differential probability for photoelectron emission of a single detector atom is [99]

$$p(t,\Delta t) \approx K(\omega_0 + E_g) \langle \hat{A}^{(+)}(t)\hat{A}^{(-)}(t)\rangle \Delta t \tag{C.0.15}$$

wherein ω_0 is an optical center frequency.

[1] The effective response function depends on the electron's density of states and dipole transition moments, see Ref. [8, p. 694].

[2] See Ref. [8, p. 697] and Ref. [92, p. 136] for an exact argument.

Appendix D.

Receiver synchronization

Our presentation of the coherent-state transmission system assumes the receiver and transmitter use the same time reference, particularly regarding the analog-to-digital converter (ADC), digital-to-analog converter (DAC), and laser local oscillators (LOs). However, in practice, the receiver and transmitter run independent clocks requiring synchronization procedures.

As shown in Chapter 4, the transmitter LO defines the upconversion frequency ω_c, and the receiver LO determines the downconversion frequency ω_l. Together the up- and downconversion frequencies defines the intermediate frequency $\omega_i = \omega_c - \omega_l$. For drifting transmitter and receiver LOs, the intermediate frequency shifts and, in the worst case, exceeds the detector bandwidth. The transmitter adds a pilot tone, a strong narrow-linewidth signal to provide a frequency reference for the receiver.[1] Additionally to frequency offsets, the pilot tone allows to suppress phase noise by employing a Wiener filter [111] on the broadened lineprofile of the pilot tone, as illustrated in Figure D.1.

The second set of oscillators that need synchronization are the clocks of the DAC and ADC. Unlike the optical LOs, the electronic clocks oscillate much slower, and we only need to compensate for timing offsets. Figure D.2 illustrates the timing offset between the transmitted and received samples. To correct for symbol-timing errors on the receiver, one can employ, for instance, the Goddard algorithm [112], which exploits that a delay increases the phase of a signal.[2].

On a protocol level, the receiver needs to detect the beginning of a data frame, i.e., a related symbol sequence, and assign a frame number. One possibility for the transmitter to inform the receiver about the beginning of a new frame is to interleave the data sequences with a fixed training sequence, see Figure D.3, known to the receiver.

[1] Refs. [108, 109, 110] discuss the usage of a pilot tone for continuous-variable quantum-key distribution (CV-QKD).

[2] See Ref. [24, p. 359] for more details on symbol-timing estimation techniques.

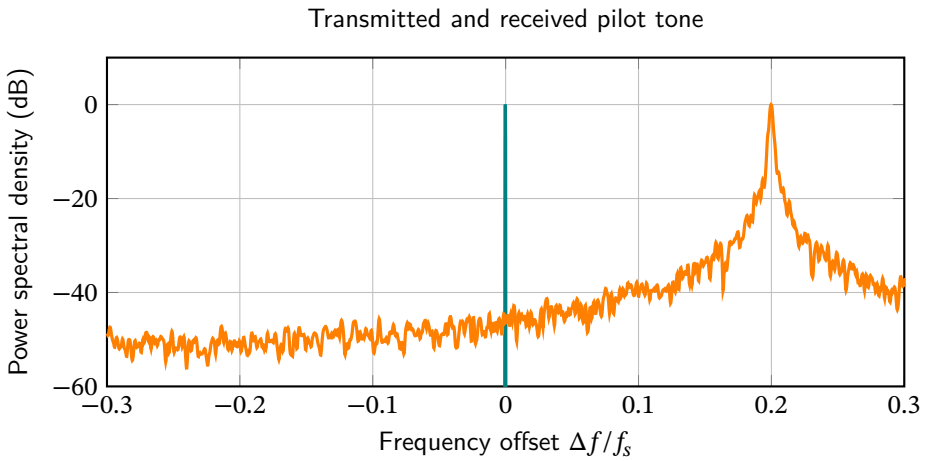


Figure D.1.: Power spectrum of the transmitted and received pilot tone. The transmitted pilot tone (green) represents a perfect sinusoidal. The received pilot tone (orange) is broadened by phase noise and shifted by the offset between the transmitter and receiver LO.

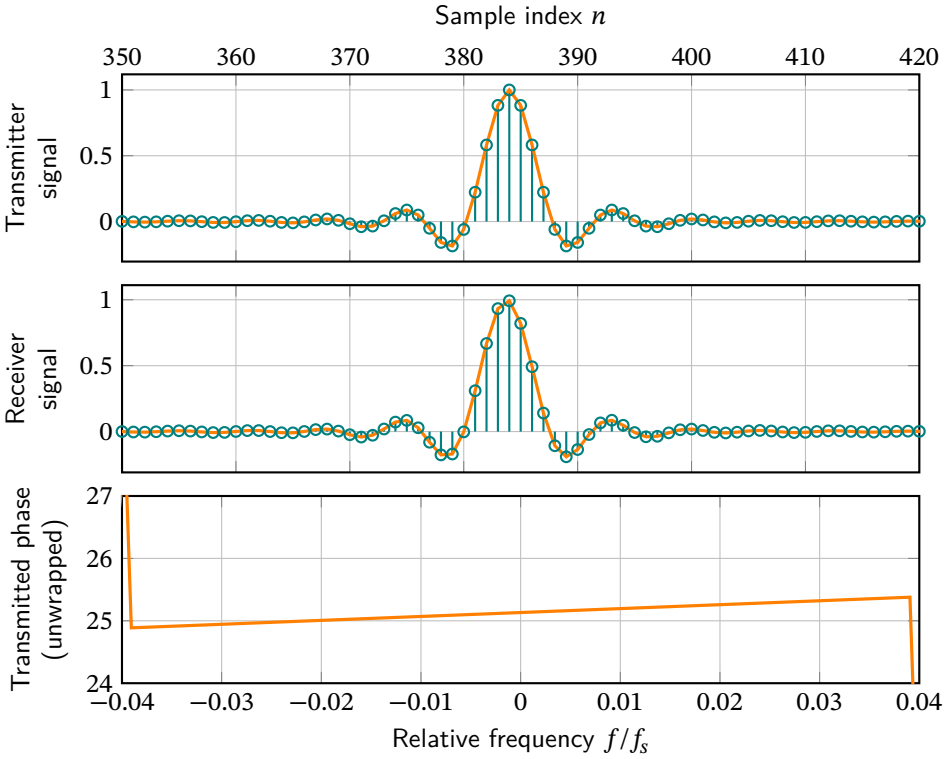


Figure D.2.: Timing offset between the DAC (first row) and ADC (second row) samples. The third row shows the linear increase in phase due to the accumulated delay.

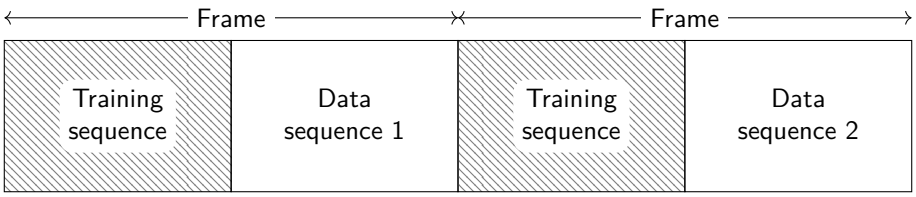


Figure D.3.: Data layout of the transmission frames. A frame comprises a training and data sequence. The training sequence is the same for all frames.

Bibliography

[1] Steven Weinberg. *The quantum theory of fields*. Vol. 2. Cambridge university press, 1995.

[2] M.E. Peskin and D.V. Schroeder. *An Introduction To Quantum Field Theory*. Frontiers in Physics. Avalon Publishing, 1995. ISBN: 9780813345437.

[3] Sean M. Carroll. "Lecture notes on general relativity". In: (Dec. 1997).

[4] C. Gerry, P. Knight, and P.L. Knight. *Introductory Quantum Optics*. Cambridge University Press, 2005. ISBN: 9780521527354.

[5] A.M. Fox et al. *Quantum Optics: An Introduction*. Oxford Master Series in Physics. OUP Oxford, 2006. ISBN: 9780198566724.

[6] U. Madhow. *Fundamentals of Digital Communication*. Cambridge University Press, 2008. ISBN: 9781139470261.

[7] W. Vogel and D.G. Welsch. *Quantum Optics*. Wiley, 2006. ISBN: 9783527608454.

[8] L. Mandel, E. Wolf, and Cambridge University Press. *Optical Coherence and Quantum Optics*. EBL-Schweitzer. Cambridge University Press, 1995. ISBN: 9780521417112.

[9] R. Loudon. *The Quantum Theory of Light*. OUP Oxford, 2000. ISBN: 9780191589782.

[10] S. Barnett and P.M. Radmore. *Methods in Theoretical Quantum Optics*. Oxford Series in Optical and Imaging Sciences. Clarendon Press, 2002. ISBN: 9780198563617.

[11] M. Srednicki. *Quantum Field Theory*. Cambridge University Press, 2007. ISBN: 9781139462761.

[12] W. Greiner, D.A. Bromley, and J. Reinhardt. *Field Quantization*. Springer Berlin Heidelberg, 2013. ISBN: 9783642614859.

[13] C. Itzykson and J.B. Zuber. *Quantum Field Theory*. Dover Books on Physics. Dover Publications, 2012. ISBN: 9780486134697.

[14] Raymond F Streater and Arthur S Wightman. *PCT, spin and statistics, and all that*. Princeton University Press, 2016.

[15] NN Bogolyubov and DV Shirkov. *Quantum Fields*. 1982.

[16] N.N. Bogolubov et al. *General Principles of Quantum Field Theory*. Mathematical Physics and Applied Mathematics. Springer Netherlands, 1989. ISBN: 9780792305408.

[17] Ulf Leonhardt. "Quantum physics of simple optical instruments". In: *Reports on Progress in Physics* 66.7 (July 2003), pp. 1207–1249. DOI: 10.1088/0034-4885/66/7/203.

[18] S. Haroche, J.M. Raimond, and Oxford University Press. *Exploring the Quantum: Atoms, Cavities, and Photons*. Oxford Graduate Texts. OUP Oxford, 2006. ISBN: 9780198509141.

[19] Jeffrey Shapiro. “The Quantum Theory of Optical Communications”. In: *IEEE journal of selected topics in Quantum Electronics* 15.6 (Jan. 2009), pp. 1547–1569.

[20] Kazuro Kikuchi. “Fundamentals of Coherent Optical Fiber Communications”. In: *J. Lightwave Technol.* 34.1 (Jan. 2016), pp. 157–179.

[21] Christoph Rauscher, Volker Janssen, and Roland Minihold. *Grundlagen der Spektrumanalyse*. Rohde & Schwarz, 2011.

[22] Josef A. Nossek. *Systeme der Signalverarbeitung - Skriptum zur Vorlesung*. 2015.

[23] Richard G Lyons. *Understanding digital signal processing, 3/E*. Pearson Education India, 2004.

[24] P. Massoud Salehi and J. Proakis. *Digital Communications*. McGraw-Hill Education, 2007. ISBN: 9780072957167.

[25] R.G. Gallager. *Principles of Digital Communication*. Cambridge University Press, 2008. ISBN: 9781139468602.

[26] R. Wolf. *Quantum Key Distribution: An Introduction with Exercises*. Lecture Notes in Physics. Springer International Publishing, 2021. ISBN: 9783030739904.

[27] Eleni Diamanti et al. “Practical challenges in quantum key distribution”. In: *npj Quantum Information* 2.1 (2016), pp. 1–12.

[28] Miloslav Dušek, Norbert Lütkenhaus, and Martin Hendrych. “Quantum cryptography”. In: *Progress in Optics* 49 (2006), pp. 381–454.

[29] Nicolas Gisin et al. “Quantum cryptography”. In: *Reviews of modern physics* 74.1 (2002), p. 145.

[30] Christian Weedbrook et al. “Gaussian quantum information”. In: *Reviews of Modern Physics* 84.2 (2012), p. 621.

[31] Alessandro Ferraro, Stefano Olivares, and Matteo GA Paris. “Gaussian states in continuous variable quantum information”. In: *arXiv preprint quant-ph/0503237* (2005).

[32] Valerio Scarani et al. “The security of practical quantum key distribution”. In: *Reviews of modern physics* 81.3 (2009), p. 1301.

[33] Chi-Hang Fred Fung, Xiongfeng Ma, and HF Chau. “Practical issues in quantum-key-distribution postprocessing”. In: *Physical Review A* 81.1 (2010), p. 012318.

[34] Fabian Laudenbach et al. “Continuous-variable quantum key distribution with gaussian modulation—the theory of practical implementations”. In: *Advanced Quantum Technologies* 1.1 (2018), p. 1800011.

[35] Tadayoshi Kohno, Adriana Palacio, and John Black. “Building Secure Cryptographic Transforms, or How to Encrypt and MAC.” In: *IACR Cryptol. ePrint Arch.* 2003 (2003), p. 177.

[36] Hugo Krawczyk. “The order of encryption and authentication for protecting communications (or: How secure is SSL?)” In: *Annual International Cryptology Conference*. Springer. 2001, pp. 310–331.

[37] Mihir Bellare and Chanathip Namprempre. “Authenticated encryption: Relations among notions and analysis of the generic composition paradigm”. In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2000, pp. 531–545.

[38] Claude E Shannon. “Communication theory of secrecy systems”. In: *The Bell system technical journal* 28.4 (1949), pp. 656–715.

[39] Joan Daemen and Vincent Rijmen. “AES proposal: Rijndael”. In: (1999).

[40] J Lawrence Carter and Mark N Wegman. “Universal classes of hash functions”. In: *Journal of computer and system sciences* 18.2 (1979), pp. 143–154.

[41] W. Diffie and M. Hellman. “New directions in cryptography”. In: *IEEE Transactions on Information Theory* 22.6 (1976), pp. 644–654. DOI: 10.1109/TIT.1976.1055638.

[42] Arjen K Lenstra et al. “The number field sieve”. In: *The development of the number field sieve*. Springer, 1993, pp. 11–42.

[43] Peter W. Shor. “Polynomial time algorithms for prime factorization and discrete logarithms on a quantum computer”. In: *SIAM J. Sci. Statist. Comput.* 26 (1997), p. 1484. DOI: 10.1137/S0097539795293172.

[44] Daniel J Bernstein and Tanja Lange. “Post-quantum cryptography”. In: *Nature* 549.7671 (2017), pp. 188–194.

[45] Lily Chen et al. *Report on post-quantum cryptography*. Vol. 12. US Department of Commerce, National Institute of Standards and Technology, 2016.

[46] Charles H Bennett and Gilles Brassard. “Quantum cryptography: Public key distribution and coin tossing”. In: *arXiv preprint arXiv:2003.06557* (2020).

[47] Bing Qi. “Bennett-Brassard 1984 quantum key distribution using conjugate homodyne detection”. In: *Physical Review A* 103.1 (2021), p. 012606.

[48] Helle Bechmann-Pasquinucci and Nicolas Gisin. “Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography”. In: *Physical Review A* 59.6 (1999), p. 4238.

[49] Charles H Bennett. “Quantum cryptography using any two nonorthogonal states”. In: *Physical review letters* 68.21 (1992), p. 3121.

[50] Normand J Beaudry, Tobias Moroder, and Norbert Lütkenhaus. “Squashing models for optical measurements in quantum communication”. In: *Physical review letters* 101.9 (2008), p. 093601.

[51] Oleg Gittsovich et al. “Squashing model for detectors and applications to quantum-key-distribution protocols”. In: *Physical Review A* 89.1 (2014), p. 012325.

[52] Jérôme Lodewyck et al. “Quantum key distribution over 25 km with an all-fiber continuous-variable system”. In: *Physical Review A* 76.4 (2007), p. 042305.

[53] Eleni Diamanti and Anthony Leverrier. “Distributing secret keys with quantum continuous variables: principle, security and implementations”. In: *Entropy* 17.9 (2015), pp. 6072–6092.

[54] V. Mukhanov, S. Winitzki, and Cambridge University Press. *Introduction to Quantum Effects in Gravity*. Cambridge University Press, 2007. ISBN: 9780521868341.

[55] Henning Vahlbruch et al. "Detection of 15 dB squeezed states of light and their application for the absolute calibration of photoelectric quantum efficiency". In: *Physical review letters* 117.11 (2016), p. 110801.

[56] Gilles Van Asche, Jean Cardinal, and Nicolas J Cerf. "Reconciliation of a quantum-distributed Gaussian key". In: *IEEE Transactions on Information Theory* 50.2 (2004), pp. 394–400.

[57] Anthony Leverrier et al. "Multidimensional reconciliation for a continuous-variable quantum key distribution". In: *Physical Review A* 77.4 (2008), p. 042325.

[58] Frédéric Grosshans and Philippe Grangier. "Continuous variable quantum cryptography using coherent states". In: *Physical review letters* 88.5 (2002), p. 057902.

[59] D.J.C. MacKay et al. *Information Theory, Inference and Learning Algorithms*. Cambridge University Press, 2003. ISBN: 9780521642989.

[60] O. Mildenberger and H. Schneider-Obermann. *Kanalcodierung: Theorie und Praxis fehlerkorrigierender Codes*. Studium Technik. Vieweg+Teubner Verlag, 2013. ISBN: 9783322909466.

[61] Robert Gallager. "Low-density parity-check codes". In: *IRE Transactions on information theory* 8.1 (1962), pp. 21–28.

[62] R. Impagliazzo, L. A. Levin, and M. Luby. "Pseudo-Random Generation from One-Way Functions". In: *Proceedings of the Twenty-First Annual ACM Symposium on Theory of Computing*. STOC '89. Seattle, Washington, USA: Association for Computing Machinery, 1989, pp. 12–24. ISBN: 0897913078. DOI: 10.1145/73007.73009.

[63] Renato Renner and Robert König. "Universally composable privacy amplification against quantum adversaries". In: *Theory of Cryptography Conference*. Springer. 2005, pp. 407–425.

[64] Charles H Bennett et al. "Generalized privacy amplification". In: *IEEE Transactions on Information theory* 41.6 (1995), pp. 1915–1923.

[65] Shreyas R (https://math.stackexchange.com/users/391323/shreyas-r). *Sum of odd terms of a binomial expansion:* $\sum_{k\ odd} \binom{n}{k} a^k b^{n-k}$. Mathematics Stack Exchange. URL:https://math.stackexchange.com/q/2528974 (version: 2017-11-20).

[66] C. H. Bennett, G. Brassard, and J. Robert. "How to Reduce Your Enemy's Information (Extended Abstract)". In: *CRYPTO*. 1985.

[67] Daniel J Bernstein. "Stronger security bounds for Wegman-Carter-Shoup authenticators". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2005, pp. 164–180.

[68] Hoi-Kwong Lo, Marcos Curty, and Kiyoshi Tamaki. "Secure quantum key distribution". In: *Nature Photonics* 8.8 (2014), pp. 595–604.

[69] Hoi-Kwong Lo and H. F. Chau. "Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances". In: *Science* 283.5410 (1999), pp. 2050–2056. DOI: 10.1126/science.283.5410.2050.

[70] Peter W Shor and John Preskill. "Simple proof of security of the BB84 quantum key distribution protocol". In: *Physical review letters* 85.2 (2000), p. 441.

[71] Anthony Chefles. "Deterministic quantum state transformations". In: *Physics Letters A* 270.1-2 (May 2000), pp. 14–19. ISSN: 0375-9601. DOI: 10.1016/s0375-9601(00)00291-7.

[72] P. Meystre and M. Sargent. *Elements of Quantum Optics*. Springer-Verlag Berlin Heidelberg, 2007. ISBN: 9783540742111.

[73] Claudia de Rham. "Massive gravity". In: *Living reviews in relativity* 17.1 (2014), pp. 1–189.

[74] A. Zee. *Einstein Gravity in a Nutshell*. In a Nutshell. Princeton University Press, 2013. ISBN: 9781400847457.

[75] Randall G Hulet, Eric S Hilfer, and Daniel Kleppner. "Inhibited spontaneous emission by a Rydberg atom". In: *Physical review letters* 55.20 (1985), p. 2137.

[76] Claude Cohen-Tannoudji, Bernard Diu, and Franck Laloë. *Quantum Mechanics, Volume 1: Basic Concepts, Tools, and Applications*. John Wiley & Sons, 2019.

[77] Rudolf Haag. *Local quantum physics: Fields, particles, algebras*. Springer Science & Business Media, 2012.

[78] E. Zeidler. *Quantum Field Theory I: Basics in Mathematics and Physics: A Bridge between Mathematicians and Physicists*. Springer Berlin Heidelberg, 2016. ISBN: 9783662500941.

[79] D. V. Naumov. "On the theory of wave packets". In: *Physics of Particles and Nuclei Letters* 10.7 (Dec. 2013), pp. 642–650. ISSN: 1531-8567. DOI: 10.1134/s1547477113070145.

[80] Dmitry V. Naumov and Vadim A. Naumov. "Relativistic wave packets in a field theoretical approach to neutrino oscillations". In: *Russ. Phys. J.* 53 (2010). Ed. by Dmitry Naumov and Alexander Vall, pp. 549–574. DOI: 10.1007/s11182-010-9458-2.

[81] Juan Nicolas Quesada Mejia. "Very Nonlinear Quantum Optics". PhD thesis. University of Toronto, Nov. 2015.

[82] U. Leonhardt. *Essential Quantum Optics: From Quantum Measurements to Black Holes*. Cambridge University Press, 2010. ISBN: 9780521869782.

[83] Andrew (https://physics.stackexchange.com/users/27732/andrew). *Equivalence of Maxwell and electric field operator in the Coulomb gauge (minimal and polar coupling)*. Physics Stack Exchange. URL:https://physics.stackexchange.com/q/676622 (version: 2021-11-14).

[84] DB Horoshko, MM Eskandary, and S Ya Kilin. "Quantum model for traveling-wave electro-optical phase modulator". In: *JOSA B* 35.11 (2018), pp. 2744–2753.

[85] R J Potton. "Reciprocity in optics". In: *Reports on Progress in Physics* 67.5 (Apr. 2004), pp. 717–754. DOI: 10.1088/0034-4885/67/5/r03.

[86] François Hénault. “Quantum physics and the beam splitter mystery”. In: *The Nature of Light: What are Photons? VI* (Sept. 2015). Ed. by Chandrasekhar Roychoudhuri, Al F. Kracklauer, and HansEditors De Raedt. DOI: 10.1117/12.2186291.

[87] M. W. Hamilton. “Phase shifts in multilayer dielectric beam splitters”. In: *American Journal of Physics* 68.2 (2000), pp. 186–191. DOI: 10.1119/1.19393.

[88] Armin Windhager et al. “Quantum interference between a single-photon Fock state and a coherent state”. In: *Optics Communications* 284.7 (2011), pp. 1907–1912.

[89] B.E.A. Saleh and M.C. Teich. *Fundamentals of Photonics*. Wiley Series in Pure and Applied Optics. Wiley, 2007. ISBN: 9780471358329.

[90] Robert W Boyd. *Nonlinear optics*. Academic press, 2020.

[91] A. Yariv et al. *Optical Waves in Crystals: Propagation and Control of Laser Radiation*. A Wiley interscience publication. Wiley, 1984. ISBN: 9780471091424.

[92] C. Cohen-Tannoudji et al. *Atom-Photon Interactions: Basic Processes and Applications*. A Wiley-Interscience publication. Wiley, 1992. ISBN: 9780471293361.

[93] W Hoyer, M Kira, and SW Koch. “Quantum Optical Effects in Semiconductors”. In: *Advances in Solid State Physics*. Springer, 2002, pp. 55–66.

[94] Fausto Rossi and Tilmann Kuhn. “Theory of ultrafast phenomena in photoexcited semiconductors”. In: *Reviews of Modern Physics* 74.3 (2002), p. 895.

[95] Wolfgang Demtröder. *Laser spectroscopy 1: basic principles*. Springer, 2014.

[96] H. Haken. *Laser Theory*. Springer Berlin Heidelberg, 2012. ISBN: 9783642455568.

[97] C.W. Gardiner, C.W. Gardiner, and P. Zoller. *Quantum Noise: A Handbook of Markovian and Non-Markovian Quantum Stochastic Methods with Applications to Quantum Optics*. Springer series in synergetics. Springer, 2000. ISBN: 9783540665717.

[98] Julio Gea-Banacloche. “Emergence of classical radiation fields through decoherence in the Scully-Lamb laser model”. In: *Foundations of physics* 28.4 (1998), pp. 531–548.

[99] HJ Kimble and L Mandel. “Photoelectric detection of polychromatic light”. In: *Physical Review A* 30.2 (1984), p. 844.

[100] Claude Elwood Shannon. “A mathematical theory of communication”. In: *The Bell system technical journal* 27.3 (1948), pp. 379–423.

[101] Hans H. Brunner et al. “A low-complexity heterodyne CV-QKD architecture”. In: *2017 19th International Conference on Transparent Optical Networks (ICTON)*. 2017, pp. 1–4. DOI: 10.1109/ICTON.2017.8025030.

[102] M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010. ISBN: 9781107002173.

[103] Sima Bahrani, Mohsen Razavi, and Jawad A Salehi. “Orthogonal frequency-division multiplexed quantum key distribution”. In: *Journal of Lightwave Technology* 33.23 (2015), pp. 4687–4698.

[104] Y.V.G.S. Murti and C. Vijayan. *Essentials of Nonlinear Optics*. ANE/Athena Books. Wiley, 2014. ISBN: 9781118902349.

[105] Geoffrey Brooker. *Modern classical optics*. Vol. 8. Oxford University Press, 2003.

[106] Michel Rérat et al. "From anisotropy of dielectric tensors to birefringence: a quantum mechanics approach". In: *Rendiconti Lincei. Scienze Fisiche e Naturali* (2020), pp. 1–17.

[107] J.D. Jackson. *Classical Electrodynamics, 3RD ED*. Wiley India Pvt. Limited, 2007. ISBN: 9788126510948.

[108] Duan Huang et al. "High-speed continuous-variable quantum key distribution without sending a local oscillator". In: *Optics letters* 40.16 (2015), pp. 3695–3698.

[109] Bing Qi et al. "Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection". In: *Physical Review X* 5.4 (2015), p. 041009.

[110] Daniel BS Soh et al. "Self-referenced continuous-variable quantum key distribution protocol". In: *Physical Review X* 5.4 (2015), p. 041010.

[111] Jingdong Chen et al. "New insights into the noise reduction Wiener filter". In: *IEEE Transactions on audio, speech, and language processing* 14.4 (2006), pp. 1218–1234.

[112] D Godard. "Passband timing recovery in an all-digital modem receiver". In: *IEEE Transactions on Communications* 26.5 (1978), pp. 517–523.

Acknowledgements

> So believe that voice that says
> that you can run a little faster
> and you can throw a little harder,
> that for you, the laws of physics
> are merely a suggestion.
>
> *(TCU Baseball)*

First and foremost, I want to thank Monika for making the present thesis possible and supporting me selflessly on my journey over the last few years. Second, I want to thank Hans for welcoming me to the group and looking out for me. Hans persistently challenged my physical understanding by never giving in to shortcuts in my explanations and sharing his unbiased and unorthodox perspectives as an engineer. Third, I want to thank Fred for the many funny moments and shared laughter. Fred's sharp mind quickly uncovered the logical fallacies in my many ideas, crucial for separating the good from the bad. Regardless of what day or time, Fred was always open to my inquiries without judging their quality. Fourth, I want to thank Stefano for the entertaining anecdotes from his rich life experience. I will especially keep in mind the whiteboard sessions, where he inspired me with his combination of precision and creativity. Fifth, I want to thank Momtchil for being available to the most unchristian times and keeping me clear of administrative burden. Momtchil's passion for advanced mathematical concepts and humorous stories about eastern Europe will remain in my memory.

I hope this work conserves a tiny fraction of the enormous knowledge aggregated by Hans, Fred, Stefano, and Momtchil and correctly reflects their unique contributions to quantum-key distribution (QKD). In particular, I tried to adhere to Fred's quantum information expertise in Chapter 1 and Stefano's insights on macroscopic electrodynamics and the modulators in Chapter 3. Hans's profound knowledge in signal processing guided me in drafting Chapter 4. His criticisms of the quadrature measurement, one of many initial motivations for this work, led to the generalized quadrature operator in Chapter 3. For the final proof-readings, I want to thank Dominik, Hans, Marianne, Markus.

Although not directly contributing to this thesis, I want to thank my family and friends for being here with me. Especially, I want to thank my grandmother and mother for taking care of me whenever I needed to recharge from work. Furthermore, I owe a deep debt to Julia, who helped me gain confidence in myself and motivated me to pursue this thesis. Finally, I want sincerely welcome my dear friends, including Abdullah, Anxiang, Chris,

Daniel, Daniele, Dominik, Fabian, Haci, Jonas, Markus, Marvin, Max, Michael, Nils, Roman and Myriam, Stefan, Valentin, and Wolfang, for accepting me for who I am and the shared memories.

Originality statement

I hereby declare that this submission is my own work and to the best of my knowledge it contains no materials previously published or written by another person, except where due acknowledgement is made in the thesis. Any contribution made to the research by others is explicitly acknowledged in the thesis. I also declare that the intellectual content of this thesis is the product of my own work, except to the extent that assistance from others in the project's design and conception or in style, presentation and linguistic expression is acknowledged.

Munich, December 5, 2021