Study of realistic devices for quantum key-distribution

by

Varun Narasimhachar

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Science
in
Physics – Quantum Information

Waterloo, Ontario, Canada, 2011

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

Quantum key-distribution (QKD) is a scheme for establishing shared secret key between remote parties. In such a scheme, quantum preparation and measurement devices (sources and detectors) are used. In existing theoretical treatments of QKD, the device models used do not capture all the imperfections which might occur in realistic devices. This creates a gap between the practical implementations and theoretical descriptions of QKD. In the present work, we contribute in bridging this gap by three methods: 1) Advancing the study of squashing models of measurement devices, 2) Devising an alternative to squashing models using statistical estimation in optical QKD, and 3) Modifying the security proof formalism of QKD to account for imperfect devices.

Acknowledgements

I would like to express my sincere gratitude to my supervisor, Prof. Norbert Lütkenhaus, for his help and support in my graduate studies. I thank Prof. Michele Mosca, Prof. Thomas Jennewein and Prof. Andrew Childs for their support as members of my graduate advisory committee and defence committee.

I acknowledge the academic, financial and infrastructural support of the University of Waterloo and the Institute for Quantum Computing.

I thank our research group, the Optical Quantum Communication Theory group headed by Prof. Lütkenhaus, for much help and encouragement. My thanks are also due to my project collaborators Agnes Ferenczi, Dr. Oleg Gittsovich and Normand Beaudry.

I am deeply grateful to my family and friends for their support.

All my work is dedicated to my parents.

Contents

List of Figures

Introduction

Quantum cryptography is a field which has been growing in importance over the last two decades. It is one of the two most important applications (the other being quantum computing) of the science of quantum information, which has seen unprecedented developments during this period. Within the realm of quantum cryptography, an important branch is the study of quantum key-distribution (QKD). The seed of QKD was planted by the landmark work of Bennett and Brassard in 1984 [1]. Since then, the field has made leaps and bounds. One aspect of growth has been the emergence of various new QKD schemes ([2, 3, 4] etc.). Secondly, there has been much improvement in the understanding of information-theoretic security, first in the context of specific QKD schemes and limiting assumptions ([5, 6, 7, 8] etc.) and later in more general settings ([9, 10, 11, 12] etc.). Finally, there have been many practical implementations ([13, 14, 15, 16, 17] etc.) and development of the theory from an abstract context to a form which applies to these practical implementations ([18, 19, 20, 21, 22] etc.).

Our concern in the present work is with this third important branch, namely bridging the gap between the abstract theoretical framework of security proofs and the realistic world of practical implementations. Before discussing the specific problems which we address, let us first give a brief background. For a detailed discussion of QKD and its practical implementations, we refer to [23].

Broadly, QKD is any technique designed for two remote honest parties, Alice and Bob, to establish a shared secret key in the possible presence of an adversarial eavesdropper, Eve. For use in this task, Alice and Bob are given access to an insecure quantum channel and an authenticated but public classical channel. The first step of most QKD schemes consists of Alice preparing some quantum systems in some state and sending them over the insecure quantum channel to Bob. In the theoretical formulation and security proof formalism of most QKD schemes, these quantum systems are simple abstractions such as qubits. On the other hand, in all existing practical implementations of QKD, the quantum systems are optical modes, which are much more complex in their structure than simple systems such as qubits. Another aspect in which implementations deviate from the theoretical description is that the devices used in QKD — Alice's source and Bob's measurement device — do not in practice behave in the manner in which they are modelled in theory. The real devices differ from their abstract theoretical models in three important aspects:

1. Fundamental structure: The model might be fundamentally simpler than the real

device. For example, while the real device emits or detects optical states, the model might work on qubits.

2. Efficiency: The real device might not always be in functioning condition. For example, detectors might sometimes not register received signals, either because of limited efficiency or other reasons, such as not having recovered sufficiently from previous activity. Another example is that signal strength might be lost by dissipation along the channel, by coupling loss, and by other means.

3. Precision: Even if a model be made complex enough to account for the added structure of the real device, and even if inefficiencies be addressed, there remains the possibility that the real device *even in its functional state* does not behave as modelled. For example, a source might not prepare the exact states which it is modelled to, and a detector might not execute exactly a measurement as it is mathematically described.

The endeavour of overcoming these limitations of the theory has been started by others much before the present work. The accomplishments thus far are mainly in addressing the first two of the above-mentioned points. In order to successfully tackle the problem on the source (Alice) side, the technique of decoy states [24, 25], supplemented by the concept of tagging, has been developed. On the detector (Bob) side, the mathematical tool of squashing models [26, 27] has been devised, which can bridge the gaps in the security proof without requiring any modification to the practical scheme. Squashing models are mathematical constructions which simplify high-dimensional descriptions of measurements by replacing them by equivalent low-dimensional models.

However, squashing models are not always straightforward to find, and in some cases, they don't exist. The first part (Chapter 1) of the present work is a study aimed at advancing the theory of squashing models. Specifically, the important role of classical post-processing of measurement statistics is addressed. Through this work, we have been able to find that the existence of a squashing model may be denied by certain post-processing schemes while admitted by certain others, whereas in some cases a meaningful post-processing scheme might not exist at all. The theory thus developed is applied to a specific example of practical significance: the detection setup used in the so-called phase-encoded BB84 (PEBB84) QKD scheme.

As we mentioned before, squashing models do not always exist. An alternative has been proposed by Fung *et al.* in [28], which is based on finding some bounds based on observed statistics. In Chapter 2, we present another alternative, based similarly on statistically-inferred bounds, through the examples of BB84 and PEBB84.

Finally, in Chapter 3, we address the third of the points raised above — the possibility of devices functioning differently from their models. Previous work [29, 30] on this aspect is limited to the special case of BB84. While Mayers and Yao [29] have presented a method to test sources for proper functioning for BB84, Gottesman *et al.* [30] address the

case of specific faults such as basis-dependent imperfections, again in the case of BB84. We consider the general formalism of QKD as presented in Renato Renner's PhD Thesis [12], which can be applied to any QKD protocol, and develop a heuristic formalism for incorporating imperfect devices under a limited model of imperfections.

We hope that these efforts provide a starting point and motivation for further advancement in the mission of realizing QKD for practical applications. At the end of the thesis, we discuss the state at which the present work leaves this mission, and what important problems remain open.

Chapter 1

Squashing models and classical post-processing

1.1 Introduction

Measurements are an essential part of quantum information-processing (QIP). Many tasks which employ QIP are performed in adversarial situations. One such example is quantum key-distribution (QKD), where two mutually-trustful parties intend to establish a shared secret key using the common resource of a public quantum channel and a public, but authenticated, classical channel. In a QKD scheme, quantum states are exchanged over the public quantum channel and later measured to extract classical information. Typical proofs for the security of QKD protocols work with simplifying assumptions about the dimensions of the Hilbert space on which the measured states are supported. However, an adversary has complete access and control over the channel, and in principle the legitimate parties have no handle over what quantum states are received by their measurement devices. In a practical implementation, for instance with optical signals, the canvas of Hilbert space available to an adversary is potentially unbounded — an infinite-dimensional Fock space of an optical mode, for example.

In the realm of quantum optics experiments, we are used to the idea of approximating these infinite-dimensional systems easily by lower-dimensional descriptions, e.g. describing parametric downconversion experiments only on the level of vacuum and single-photon pairs. We can do that, because we can handle the approximations well on a theoretical level such that theoretical predictions and experimental verifications coincide with high precision. But in cryptographic situations, such as QKD or quantum coin-tossing [1, 31], this is not good enough. Here we have to be able to bound exactly our error in any prediction, because, for example, experimental verification of third-party information about some measurement data is not possible.

One possible recourse is of course to carry out detailed calculations in the infinite-dimensional Hilbert spaces [19, 32]. Often this is technically challenging. The other pos-

sibility then is to truncate to finite-dimensional subspaces. This has to be done not only in the form of approximations, but as truncations that hold also under adversarial conditions. There are two approaches here. The traditional way would be to provide exact bounds on the effects of truncations and to extend the theoretical finite-dimensional analysis to accommodate the effects of the truncation. This approach has been followed, for example, in [33] in the context of a specific application, while a more general framework of this approach has recently been formulated by [28], and in another part of our work (Chapter 2). The tool of squashing models affords a second way, postulated already in [30] (where the term 'squashing' has been coined), which performs a truncation of the Hilbert space in such a way that provides a direct link between the optical implementation and the abstract low-dimensional protocol, without the necessity to amend the theoretical analysis. To take a concrete example from QKD, this approach means that for a generic QKD protocol with a BB84 [1] polarization encoding we can assume without loss of generality that single photons enter the detection device of the receiver.

In the present discussion, we concern ourselves with this latter approach, namely the use of squashing models. Squashing models effect a truncation of a high-dimensional Hilbert space to some low-dimensional target space which holds also under adversarial conditions that occur in cryptographic contexts. We build on earlier work by Beaudry *et al.* [27], that gave a well-defined notion of a squashing map. Note that Tsurumaru and Tamaki [26, 34] have independently investigated squashing models.

The matter presented in § 1.2 is already contained in previous work [27]. The SDP formulation of squashing problems, presented in § 1.4, has been carried out in the past by Moroder, Beaudry and others as part of the work going into [35, 27]. However, we find it useful to include it in the present work, because it has not been summarized in an accessible form anywhere in the Literature.

A rough idea of what a squashing model does is represented in Fig. 1.1. A physical measurement device B corresponds to some basic distinguishable events, which are associated with a POVM F_B. These basic events may be subjected to (classical) post-processing to a different definition of events. This post-processing might be, for instance, coarse-graining, where any of several basic outcomes is treated as the occurrence of one post-processed outcome. The post-processing might also be probabilistic, wherein each basic event triggers some probabilistic assignment of post-processed outcomes. In general, the post-processing is a stochastic map from the set of basic outcomes to some other set of defined outcomes. We refer to the combination of basic events and post-processing as the full measurement, and denote the effective POVM by F_M. This classical post-processing will be an essential tool in making squashing models work, as we shall see.

Consider another POVM, called F_Q, which distinguishes the same number of outcomes as F_M, but acts on a smaller Hilbert space. The role of a squashing model is to connect a measurement like F_M with one like F_Q: a squashing model consists of an abstract map (which describes a process which is, in principle, physically allowed within the framework of quantum mechanics), such that a device consisting of the map followed by F_Q is

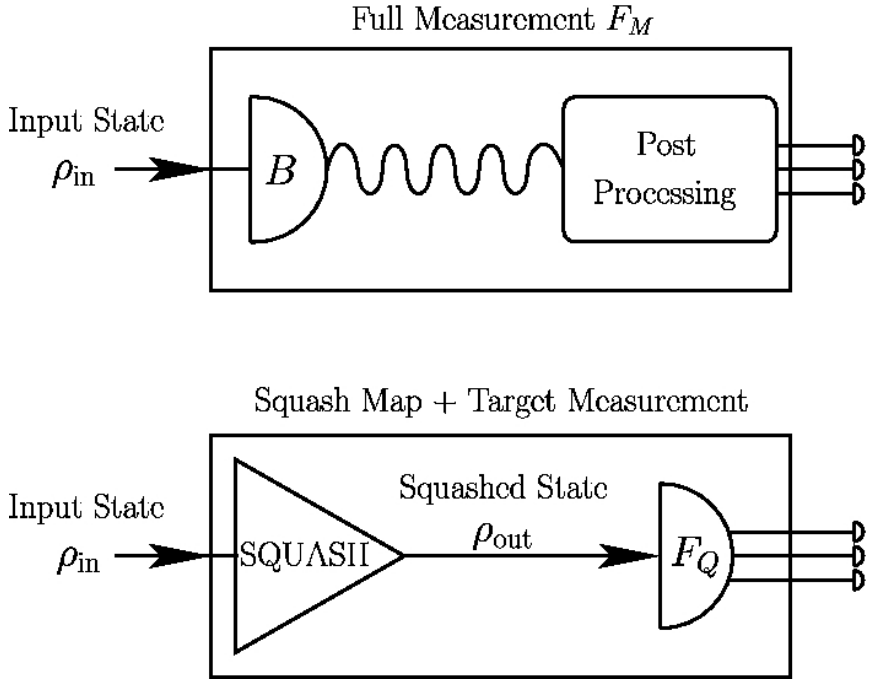


Figure 1.1: The full measurement F_M (above) has a general optical input ρ_{in}, which is first measured by a receiver's measurement device B, followed by classical post-processing. The squashed measurement (below) has the same general optical input ρ_{in}, which is then squashed by a map Λ to a smaller Hilbert space, followed by a fixed physical measurement F_Q. It is required that both of these measurements produce the same output statistics for all ρ_{in}.

equivalent to one effecting the POVM F_M, i.e. the two situations depicted in Fig. 1.1 are indistinguishable for every input.

Given the exact mathematical equivalence of the two situations depicted in Fig. 1.1, we can perform all calculations pertaining to the respective application[1] assuming the second model (Fig. 1.1, bottom), i.e. the one with the squashing map followed by F_Q. In fact, by basing all our calculations on a device model where the device consists only of the measurement F_Q and where *any input whatsoever in the input space of* F_Q can enter such a device, we naturally account for the particular case where those inputs are the result of applying the squashing map on some pre-inputs.

This is the case, for example, if the device is part of a cryptographic scheme and if we formulate a security proof for the scheme under the assumption of an F_Q device. The security proof would then cover for all kinds of input to F_Q, in particular ones produced by the squashing map. Since the real situation (Fig. 1.1, top) is equivalent to the one where the squashing map precedes F_Q (Fig. 1.1, bottom), we can assume this latter situation

[1]These calculations might constitute, for instance, the formulation of a security proof if the application is a cryptographic protocol.

and, further, concede the squashing part to the channel, retaining only F_Q in the device. Even if the channel is under adversarial control, we do not compromise on security, since our calculations are valid for any input whatsoever to F_Q.

1.2 Mathematical preliminaries

Here we give the necessary mathematical definitions of the relevant notions, including mainly that of a squashing map.

We denote as $\mathcal{H}_M$ the high-dimensional (often infinite-dimensional) Hilbert space on which the basic measurement POVM F_B and also the full measurement F_M are described. Recall from the previous section (see Fig. 1.1) that F_B denotes the unprocessed action of a physical measurement device, while F_M denotes the post-processed full measurement. Further, we denote by $\mathcal{H}_Q$ the low-dimensional Hilbert space of the target POVM F_Q. The elements of the POVM, one for each measurement outcome, are denoted respectively by $F_X^{(i)}$ for $X \in \{B, M, Q\}$, and the index i runs over the set of outcomes for the corresponding measurement (which are necessarily of the same number for Q and M). Quantum-mechanical states are described by density matrices ρ, which are non-negative Hermitian operators with unit trace. We denote by ρ_M a generic state on $\mathcal{H}_M$. The probability distribution of measurement results is then given by Born's rule, namely $\Pr_X^{(i)}[\rho] = \mathrm{Tr}\left[F_X^{(i)}\rho\right]$.

Before moving on to the formal definition of a squashing map, we need to state precisely what constitutes valid classical post-processing. Classical post-processing is applied to the measurement outcomes and allows, for example, the combination of different outcomes into one (coarse-graining). It plays an important role in developing squashing models. One thing it achieves is to create a full measurement F_M out of the basic measurement events F_B such that the POVM F_M contains the same number of elements as the target measurement F_Q. Otherwise, obviously, no squashing model can exist. Formally, post-processing can be described as a stochastic matrix $\mathcal{P}$ which acts on the vector of probabilities of the measurement outcomes. The entries $\mathcal{P}_{ij} = \Pr[i|j]$ of the matrix are given by the conditional probabilities which describe the redistribution of outcomes of the POVM F_B with index j into events of the full measurement POVM F_M with index i.

Definition 1.2.1. (Classical post-processing) Let $\vec{p}_{\mathrm{bas}}$ be the vector of the outcome probabilities of the basic measurement B (for some input state). Any classical post-processing scheme which can be applied to $\vec{p}_{\mathrm{bas}}$ is described by a stochastic matrix $\mathcal{P}$ and results in some new outcome probability distribution $\vec{p'}$ such that

$$\begin{aligned} \vec{p'} &= \mathcal{P}\vec{p}_{\mathrm{bas}}, \\ \forall j, \quad \sum_i \mathcal{P}_{ij} &= \sum_i \Pr[i|j] = 1. \end{aligned} \tag{1.1}$$

Since taking the trace of an operator is a linear operation, post-processing can be seen

as a linear transformation on the POVM elements, resulting in a new POVM:

$$F_M^{(i)} = \sum_j \mathcal{P}_{ij} F_B^{(j)}. \tag{1.2}$$

Similarly, the target POVM can also be a post-processed version of a more basic measurement. But in the typical problems encountered in squashing, it is sufficient to consider one fixed target POVM, so that even if it be post-processed, we don't have to consider variations in the post-processing.

Definition 1.2.2. (Squashing model) Let (F_Q, F_B) denote a measurement apparatus, associated with a complete target POVM with elements $F_Q^{(i)}$, $i = 1, \ldots, N_Q$, and a basic unprocessed full POVM with elements $F_B^{(j)}$, $j = 1, \ldots, N_B$, also complete. Denote by $F_M^{(i)}$, $i = 1, \ldots, N_M$ the full measurement POVM elements for some **fixed** classical post-processing $\mathcal{P}$ of the basic events that assures that $N_Q = N_M$.

We say that there exists a squashing model for $(F_Q, F_B, \mathcal{P})$ iff there exists a map Λ_S such that

1. For any state ρ_M
$$\mathrm{Tr}\left[F_M^{(i)} \rho_M\right] = \mathrm{Tr}\left[F_Q^{(i)} \Lambda_S\left[\rho_M\right]\right], \forall i, \tag{1.3}$$
where $F_M^{(i)} = \sum_j \mathcal{P}_{ij} F_B^{(j)}$;

2. Λ_S is a completely-positive (CP) trace-preserving (TP) map, denoted CPTP for short.

Remark 1.2.3. *We introduce the adjoint map $\Lambda_S^\dagger$ to find that Eq. (1.3) implies that*

$$Tr\left[F_M^{(i)} \rho_M\right] = Tr\left[\Lambda_S^\dagger\left[F_Q^{(i)}\right] \rho_M\right], \forall i \tag{1.4}$$

has to hold for any state ρ_M. Therefore

$$\Lambda_S^\dagger\left[F_Q^{(i)}\right] = F_M^{(i)} \quad \forall i = 1, \ldots, N_Q. \tag{1.5}$$

Since F_Q and F_M are both complete POVMs, the adjoint map has to satisfy

$$\Lambda_S^\dagger\left[\mathbb{1}_Q\right] \quad = \mathbb{1}_M, \tag{1.6}$$

which, together with the CP requirement, entails that $\Lambda_S^\dagger$ be CP and unital, or equivalently, that Λ_S be CP and trace-preserving (CPTP).

The reason we treat the target and full POVMs as two components of one device is that, in typical situations where squashing models are sought, the target POVM is the restriction of the action of a detection setup to some subspace of inputs (for example,

restriction to single-photon inputs to a linear-optic detection device), while the full POVM is the unrestricted version of the same.

The definition of the squashing model consists of two essential parts. In order to provide a squashing model for a given measurement apparatus (F_Q, F_B), one first has to agree on a meaningful post-processing, as defined in Eq. (1.2). The classical post-processing can be seen as a freedom in searching for a squashing model. That is, the post-processing fixes the full measurement and influences the linear constraints (1.3), which have to be fulfilled by the squashing map Λ_S. The squashing map Λ_S has to be a CPTP map. Its existence, given the constraints, can therefore be investigated by exploiting the Choi-Jamiołkowski isomorphism [36]. Note that variations of squashing models that require only positive, but not completely-positive, maps have been investigated and utilized in [35].

We conclude this section by summarizing that by the existence of a squashing map, we mean that *for a given measurement device with basic measurement events described by POVM F_B and a fixed post-processing $\mathcal{P}$ resulting in full measurements F_M, and a target measurement described by the POVM F_Q, there exists a CPTP map Λ_S such that the full measurement F_M can be thought of as the composition of the squashing map Λ_S followed by the target measurement F_Q.*

1.3 The role of classical post-processing

In this section, we shall zoom in on one important aspect of the squashing problem, namely the role that classical post-processing plays. We shall see that much of the structure of a typical squashing problem is decided by this aspect, and that it is useful to consider this aspect independently before considering the whole squashing problem.

As per the previous section, the central question addressed in the context of squashing models is whether a squashing map exists *when the target and post-processed full POVMs, F_Q and F_M, are completely specified.* This question itself comes *after* first fixing some post-processing scheme $\mathcal{P}$. In a typical situation where squashing models are invoked, there is no *a priori* clear definition or directive principle to fix a particular $\mathcal{P}$. So in fact, the complete question is not just the one we posed before, but also *whether there exists a valid $\mathcal{P}$, which is also meaningful (in a sense we will discuss later), such that that question can be answered in the affirmative.*

1.3.1 Constraints from linear relations

Given a certain measurement device (F_B, F_Q) which carries out basic full measurement F_B and a target POVM F_Q, we can already find some constraints on the allowed post-processing schemes, as follows. Recall that we seek a *linear* CP map $\Lambda_S^\dagger$ taking the target POVM elements to the corresponding post-processed full POVM elements. The linearity

property implies that any linear relations[2] between elements of the map's domain must be obeyed by their images under the map. That is,

$$\sum_{i=1}^{N_Q} \alpha_i F_Q^{(i)} = 0 \Rightarrow \sum_{i=1}^{N_Q} \alpha_i F_M^{(i)} = 0$$
$$\Leftrightarrow \sum_{i,j} \alpha_i \mathcal{P}_{ij} F_B^{(j)} = 0. \tag{1.7}$$

We can restate the foregoing in a more useful way. If we denote by $\mathbb{N}_Q$ the null-space of the F_Q over the reals, i.e. the subspace of $\mathbb{R}^{N_Q}$ such that

$$\alpha \in \mathbb{N}_Q \Leftrightarrow \sum_{i=1}^{N_Q} \alpha_i F_Q^{(i)} = 0, \tag{1.8}$$

and likewise by $\mathbb{N}_B$ the null-space of the F_B over the reals, i.e. the subspace of $\mathbb{R}^{N_B}$ such that

$$\beta \in \mathbb{N}_B \Leftrightarrow \sum_{i=1}^{N_B} \beta_i F_B^{(i)} = 0, \tag{1.9}$$

then a constraint (equivalent to (1.7)) on the choice of $\mathcal{P}$ is that

$$\forall \alpha \in \mathbb{N}_Q, \mathcal{P}^{\mathrm{T}} \alpha \in \mathbb{N}_B. \tag{1.10}$$

Another equivalent condition, which is the most useful form in practical situations (e.g. in numerical investigations), is as follows. If we denote by $\mathbf{N}_Q$ a matrix whose columns comprise an orthonormal basis spanning $\mathbb{N}_Q$, and by $\mathbf{R}_B$ a matrix whose rows comprise an orthonormal basis spanning the subspace of $\mathbb{R}^{N_B}$ orthogonal to $\mathbb{N}_B$, then we require that

$$\mathbf{R}_B \mathcal{P}^{\mathrm{T}} \mathbf{N}_Q = 0. \tag{1.11}$$

The constraint in the above form can be used, for instance, as one of the linear constraints when the squashing problem is formulated numerically using semidefinite programming (SDP) (see §1.4).

1.3.2 Meaningful post-processing: "No-mixing" constraint

In addition to the basic linear constraint on the post-processing which is necessitated by the very mathematics of the problem (discussed in the preceding subsection), another class of linear constraints arises from practical considerations. Usually, as mentioned before, the target measurement is a special case of the full measurement restricted to a certain subspace of inputs. The statistics gathered from this measurement carries information relevant to

[2]Throughout this work, when we use the term "linear relations", we mean *homogeneous* linear relations, i.e. those not involving nonzero additive constants.

the particular application, e.g. QKD. Since the post-processing applies also when the actual measurement occurring might happen to be the target measurement (since it is a special case of the full measurement), or even in other cases when the measurement outcome contains important information, the post-processing scheme must be such that it does not disturb the relevant information contained in the measurement outcomes. In order to motivate the constraints that arise from this, let us consider the following.

It is easy to see that there always exists a family of trivial post-processing schemes which each admit a squashing map, namely one which assigns target events with the same distribution for any full measurement event whatsoever; a valid squashing map for such a post-processing scheme is a constant map whose image is a state on the target space whose outcome statistics under the target measurement matches the one which the post-processing scheme produces. It is obvious that such a squashing map would obliterate the practicality of any application because it would require us to simulate some fixed statistics which carries none of the actual information relevant to the application.

For example, in the six-state QKD protocol with active basis-choice[3], the appropriate target measurement would be a polarization measurement on one photon, with active switching between three mutually-unbiased bases. For an input state with more than one photon, there are three possible outcomes for each basis choice: a click in either detector (0 or 1 in the respective basis), or clicks in both detectors. While some post-processing scheme is required so that the statistics of these outcomes can be reduced to statistics on a two-outcome event space, it must be chosen judiciously so that the useful information in the single clicks is retained as much as possible. One (unwise) way to find a squashing map from many photons to a single photon would be to ignore the input and always produce uniformly-random outcomes in each basis. Obviously this would kill all information essential for key-extraction, which is contained in single-click outcomes from single-photon as well as multiple-photon inputs. It is only double-click outcomes which don't provide meaningful information, and therefore it would be counterproductive to introduce randomness in single-click outcomes.

The above examples, though extreme cases, demonstrate nevertheless that some post-processing schemes can destroy useful information. Therefore, in general, in addition to the constraints discussed in the preceding subsection, we impose certain other linear constraints, specific to the particular application in consideration, which are motivated by the intention to prevent useful information from getting disturbed. We refer to this class of constraints by the term "no-mixing", since it is a requirement that meaningful information not get mixed up. Since the usual "meaningful" outcomes are single clicks in most applications, the no-mixing constraint usually amounts to requiring the post-processing scheme to map single-click events deterministically to the corresponding target single-click

[3]The term "passive basis-choice" refers to a situation where the basis-choice is executed using a passive linear-optic element, i.e. a beam-splitter whose output branches contain measurements in different bases. "Active basis-choice" is a situation where the choice is made using a mechanism which is external to the linear optics.

events. This notion will become clear in §1.5 where we shall discuss the example of the phase-encoded BB84 detection setup.

1.4 Semidefinite programming in squashing models

The theory of semidefinite problems and semidefinite programming (SDP) plays an important role in the field of quantum information. Many important problems in the field turn out to have alternative formulations in terms of SDPs. This affords an advantage in numerical computations, because many efficient computational applications are available for solving SDPs numerically. The problem of finding squashing models can also be formulated in terms of SDPs. This allows us to employ numerical computation using SDPs as an aid, supplementing or guiding analytical methods.

A semidefinite program (SDP) is an optimization problem over an inner-product space. There exist several equivalent standard descriptions of SDPs. We use the following, which fits well into our present purpose:

$$\begin{aligned} \min_{\mathbf{x}\in\mathbb{R}^n} \quad & c^{\mathsf{T}}\mathbf{x} \\ \text{subject to} \quad & H_0 + \sum_{i=1}^{n} x_i H_i \geq 0, \end{aligned} \tag{1.12}$$

where $c \in \mathbb{R}^n$ is a constant, and the H_i are constant Hermitian matrices of some dimension. Note that the "$\geq$" above refers to the notion of semidefinite order of Hermitian matrices.

In order to state the problem of finding a squashing model for a certain device[4] (F_Q, F_B) and post-processing scheme $\mathcal{P}$ in the form of an SDP, we first make the following convenient constructions. Let $\{|i\rangle\}$ be an orthonormal basis spanning the Hilbert space $\mathcal{H}_Q$ of the target. Consider the following linear map which executes a "vectorization" of operators[5]:

$$\begin{aligned} \mathcal{V}_Q : & \mathcal{L}[\mathcal{H}_Q] \to \mathcal{H}_Q \otimes \mathcal{H}_Q \\ \forall i,j \quad & \mathcal{V}_Q[|i\rangle\langle j|] = |i\rangle \otimes |j\rangle. \end{aligned} \tag{1.13}$$

Some inspection shows that this vectorization is a basis-independent operation. We can therefore use the abbreviated notation $\mathcal{V}_Q[A_Q] \equiv |A_Q\rangle\!\rangle$, where A_Q is any operator in $\mathcal{L}[\mathcal{H}_Q]$. We can define a similar map on the full measurement space $\mathcal{H}_M$, with the abbreviated notation $\mathcal{V}_M[A_M] \equiv |A_M\rangle\!\rangle$. We naturally extend this notation to the corresponding bras.

[4]The notions $(F_Q, F_B, \mathcal{P})$ and other mathematical notations are introduced in §1.2.

[5]For two Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$, we use the notation $\mathcal{L}[\mathcal{H}_1, \mathcal{H}_2]$ for the set of all linear operators mapping vectors in $\mathcal{H}_2$ to those in $\mathcal{H}_1$. Further, keeping with convention, we condense $\mathcal{L}[\mathcal{H}, \mathcal{H}]$ to $\mathcal{L}[\mathcal{H}]$.

Now consider the linear "rearrangement" map defined by

$$\begin{aligned} &\mathcal{R} : \mathcal{L}\left[\mathcal{H}_M \otimes \mathcal{H}_Q\right] \to \mathcal{L}\left[(\mathcal{H}_M)^{\otimes 2}, (\mathcal{H}_Q)^{\otimes 2}\right] \\ &\forall A_M \in \mathcal{L}\left[\mathcal{H}_M\right], B_Q \in \mathcal{L}\left[\mathcal{H}_Q\right] \quad \mathcal{R}\left[A_M \otimes B_Q\right] = |A_M\rangle\!\rangle\langle\!\langle B_Q|. \end{aligned} \tag{1.14}$$

For any linear map $\Lambda : \mathcal{L}\left[\mathcal{H}_Q\right] \to \mathcal{L}\left[\mathcal{H}_M\right]$, the Choi matrix

$$M_\Lambda := (\Lambda \otimes \mathsf{id}) \left[\sum_{i,j} |i\rangle\langle j| \otimes |i\rangle\langle j|\right] \tag{1.15}$$

of Λ has the property that

$$\forall A_Q \in \mathcal{L}\left[\mathcal{H}_Q\right], \quad \left(\mathcal{R}\left[M_\Lambda\right]\right)|A_Q\rangle\!\rangle = |\Lambda\left[A_Q\right]\rangle\!\rangle. \tag{1.16}$$

Therefore, for a given detection setup and post-processing $(F_Q, F_B, \mathcal{P})$, if we construct the vectorizations $|F_Q^{(i)}\rangle\!\rangle$ and $|F_M^{(i)}\rangle\!\rangle$ (recall that $\mathcal{P}$ defines F_M uniquely) of the target and full POVM elements, then we can write the linear constraints (1.5) on the squashing map Λ_{S} as

$$\forall i, \quad \left(\mathcal{R}\left[M_{\Lambda_{\mathrm{S}}^\dagger}\right]\right)|F_Q^{(i)}\rangle\!\rangle = |F_M^{(i)}\rangle\!\rangle. \tag{1.17}$$

Therefore, we can state the squashing problem as an SDP:

$$\begin{aligned} \min_{M \in \mathcal{L}[\mathcal{H}_M \otimes \mathcal{H}_Q], \lambda \in \mathbb{R}} \quad & \lambda \\ \text{subject to} \quad & \left(\mathcal{R}\left[M\right]\right)|F_Q^{(i)}\rangle\!\rangle = |F_M^{(i)}\rangle\!\rangle, \\ & M + \lambda \mathbb{1}_{M \otimes Q} \geq 0. \end{aligned} \tag{1.18}$$

The squashing problem thus stated has a solution (i.e. a squashing model exists) iff the minimum value of the objective function is nonpositive (which implies that the Choi matrix is positive-semidefinite).

This can be reduced to the standard form (1.12) as follows:

1. Parametrize the variable M in terms of an appropriate number of real parameters, and consider these along with λ as the variable $\mathbf{x}$.
2. Decompose each equality constraint into a pair of "sandwich" semidefiniteness constraints. For example, if there is an equality constraint $A = B$ between two matrices, replace it by $A \geq B$ and $B \geq A$.
3. Bunch all constraints into one matrix semidefiniteness constraint on a direct-sum space.

The resulting problem statement is seen to be in the form (1.12) because the constraint is a matrix semidefiniteness linear in the variable vector, and also the objective function

is linear in the variable vector. We can see that even the more general problem of finding first an appropriate post-processing scheme $\mathcal{P}$, and then a squashing model under that scheme, can be formulated as an SDP, since the constraints on $\mathcal{P}$ are all linear. However, including the post-processing scheme as a variable greatly increases the complexity of the computation, and therefore might not be feasible in practice. For example, in the case of the phase-encoded BB84 detection setup (§1.5), the number of outcomes in the basic measurement is 126, making the number of open parameters in $\mathcal{P}$ considerably large. Our attempts to run a numerical SDP for this case failed.

Notwithstanding their limitations, the SDP statements of squashing problems are frequently employed in numerical computations which serve to aid analytical methods, as for instance in the work leading to the results presented in §1.5.

1.5 Squashing model for the phase-encoded BB84 detection setup

In this section, we report our investigation, and results thereof, on a squashing model for a certain linear-optic detection device used in a particular QKD implementation. The pertinent QKD scheme is a variation of the Bennett–Brassard 1984 (BB84) protocol [1] which uses as the logical degree of freedom the relative optical phase[6] between two coherent light pulses, instead of the polarization of a single pulse as in the original form of BB84. We call this implementation phase-encoded BB84 (PEBB84). We introduce here the details of the detection setup we are concerned with, without discussing the other aspects of the PEBB84 scheme, which are irrelevant in the context of squashing.

1.5.1 Model of the measurement device in PEBB84 and its imperfections

The measurement device (Fig. 1.2) used in PEBB84 is a Mach-Zehnder interferometer which accepts two time-separated optical modes u_1 and u_2. These modes go through a 50-50 beam-splitter, resulting in several modes on the two arms of the interferometer. The modes in the longer arm are influenced by a phase-modulator, and then allowed to interfere with those from the shorter arm through a second 50-50 beam-splitter. The path difference between the longer and shorter arms is exactly equal to that between the two input modes.

Depending on the initial phase difference between u_1 and u_2, and on the receiver's *active* choice of the phase in the phase-modulator, the modes propagating through the interferometer interfere differently on the output-port beam-splitter, producing six output modes w, spread over three time windows. These output modes are then detected by two

[6]Hereafter, whenever we use the term "phase" in this thesis, we mean the optical phase and not the quantum-mechanical phase.

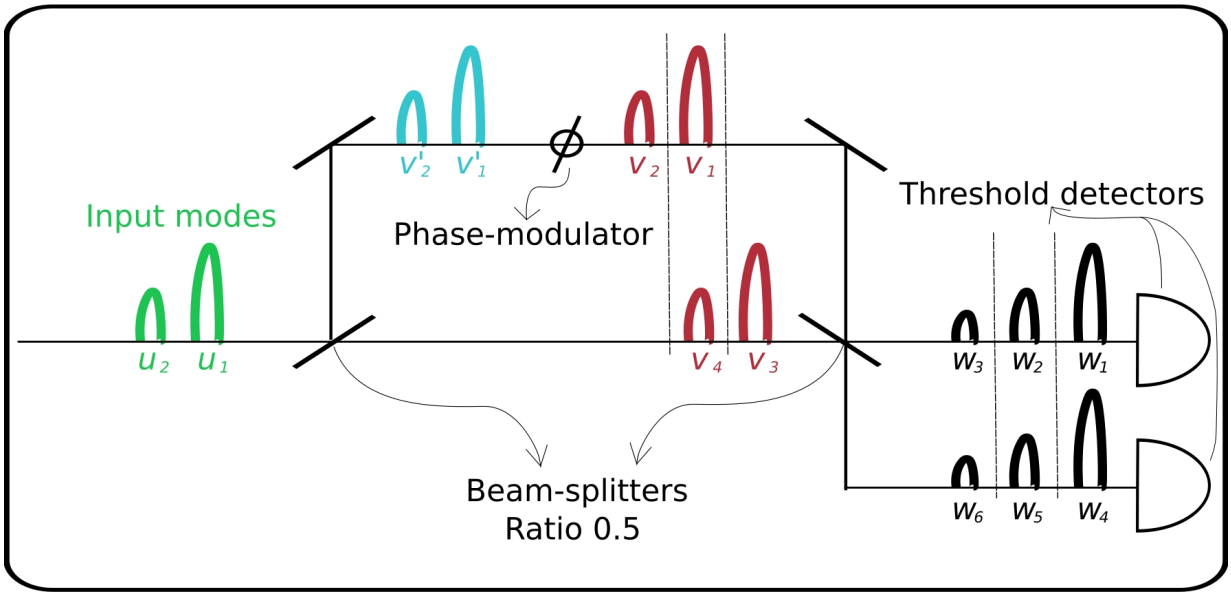


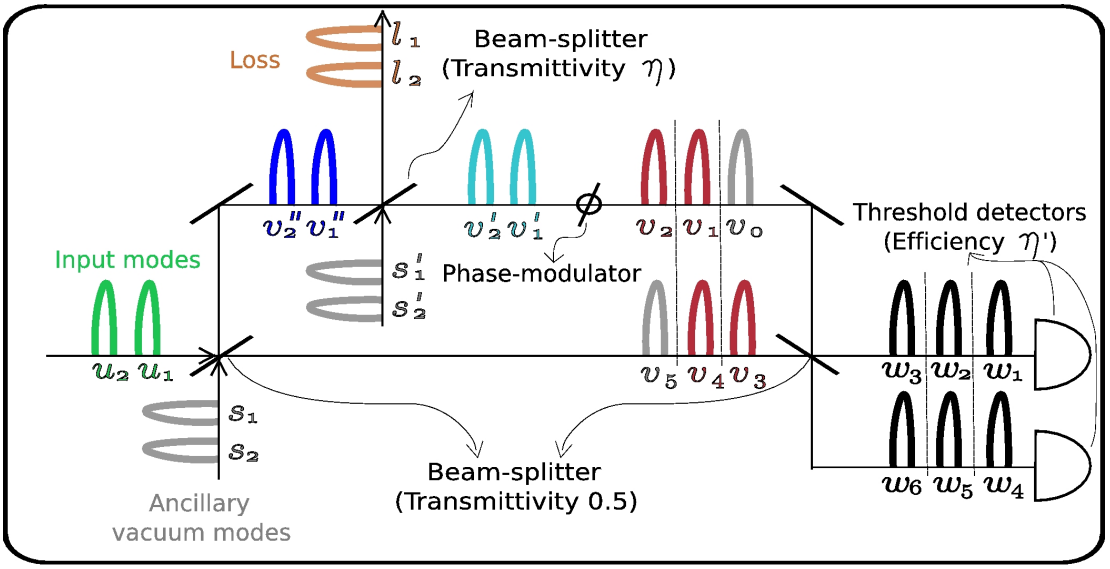
Figure 1.2: Linear-optic model of the PEBB84 detection device.

threshold detectors. As one can deduce from Fig. 1.2, the relevant phase information is carried by the modes in the second time window, because it is only the output modes occurring in this time window that result from interference between the two input modes.

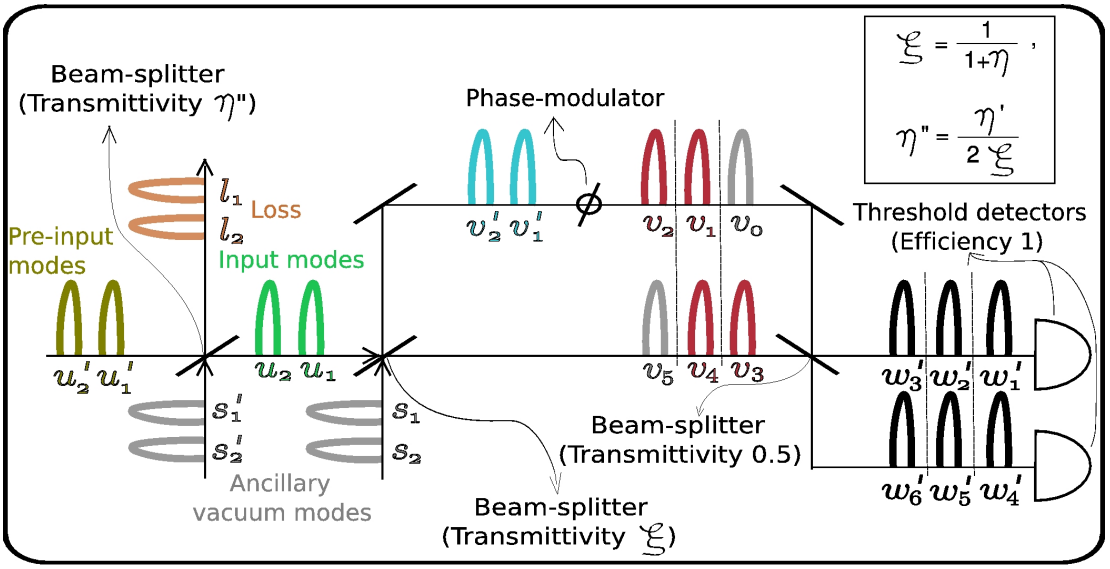
In the ideal model which does not account for any imperfections, the detection setup is lossless, the two detectors are perfectly efficient, and there are no dark counts. We simplify our model inasmuch as we disregard altogether the possibility of unequal efficiencies in the two detectors, as well as the occurrence of dark counts. We also assume that the downtime of the detectors is small enough that each of the three time windows described above can be resolved. However, we do consider the other imperfections which occur in practice, namely equal inefficiencies in the two detectors, and losses in the interferometer.

Fig. 1.3(a) shows the detection setup with all its imperfections (the loss in the phase-modulator modelled by a beam-splitter before it). Fig. 1.3(b) shows the same detection setup with the imperfections outsourced to the channel: equal inefficiencies η' in the two detectors, along with the overall loss in the interferometer's arms due to the transmittance η of the phase-modulator, are accounted-for by inserting a beam-splitter of transmittance $\eta'' = \eta'/2\xi$ in the channel, where $\xi = 1/(1+\eta)$. The relative loss between the longer and shorter arms is then accounted-for by changing the transmittance of the first beam-splitter from 0.5 to ξ.

Having thus modified the model, the global loss that is now before the measurement device can be ascribed to the channel (which is controlled completely by the adversary Eve), and the detection setup in consideration is then the rest of Fig. 1.3(b), with the u modes as input instead of u'. Detailed calculations demonstrating that this model is indeed equivalent to the one in Fig. 1.3(a) are presented in Appendix A. Note that the assumption



(a) Model of detection setup with imperfections: Two input modes u pass through a Mach-Zehnder interferometer with a $(1-\eta)$-lossy phase-modulator in the longer arm, and finally give rise to 6 output w modes, detected by two threshold detectors of equal efficiency η'.



(b) Model of detection setup with imperfections moved to channel: The loss is removed from the longer arm and the detectors replaced with perfectly-efficient ones; To compensate, a loss η'' is inserted in the channel and the first Mach-Zehnder beam-splitter transmittance is changed to ξ.

Figure 1.3: Model of the measurement device (a) with its imperfections and (b) after the imperfections have been outsourced to the channel.

of ascribing the detector losses to Eve is a simplification in the model. In the matter of security, this is a safe simplification to make, since it amounts to assuming that some part of Bob's device (namely the lossy elements) is controlled entirely by the adversary Eve, whereas in reality no part of the device is accessible by Eve. This means that in principle, we formulate a security proof for the scenario where Eve may not even "use" these lossy elements which have been "conceded" to her in the simplifying assumption, which is clearly a more compromised situation than the one where she has no access to any part of Bob's device. As a consequence, the security proof formulated for the simplified model is also valid in the actual situation where the device is not compromised. The principles used in this argument are essentially along the same lines as those on Page 6.

With the detection setup described, we next move on to the investigation of squashing models of the device. But before that, an important remark on the parameter ξ (i.e. the modified ratio of the first beam-splitter): in general ξ lies between 0.5 and 1. The value 0.5 corresponds to the case where the phase-modulator is lossless ($\eta = 1$). For this particular value of ξ the mathematics (linear relations, etc.) of the squashing problem have some peculiar properties which are not shared by the other cases ($\xi > 0.5$). However, the squashing problem for the $\xi = 0.5$ case reduces to that of the usual polarization-encoded BB84, where a squashing model has already been found [27]. On the other hand, $\xi = 1$ corresponds to a phase-modulator with zero transmittance ($\eta = 0$), so values of ξ close to 1 are not encountered in practice. Therefore, all our analysis in the present work is assumed to be for a general value of ξ which is neither 0.5 nor very close to 1.

1.5.2 Target POVM

The target POVM which fits the purpose of the security proof of the PEBB84 QKD scheme is a coarse-grained form of the action on single-photon inputs of the detection setup discussed in the preceding subsection. Note that the phase setting of the phase-modulator is actively chosen to be either 0 or $\frac{\pi}{2}$. On a given single-photon input (i.e. an input state which contains a single photon distributed over the two input modes), we distinguish between five different events:

- A click in the upper detector in the second time window for each of the two settings of the phase-modulator.
- A click in the lower detector in the second time window for each of the two settings of the phase-modulator.
- A click in either detector in any of the other time windows, for either phase setting. This event is a coarse-graining of 8 distinct basic events, which we call collectively as *outside clicks*.

Since the input is restricted to contain a single photon, it is obvious that no events occur with fewer or more clicks than one (in the two detectors over the three time intervals).

All imperfections having been moved to the quantum channel, we can use the input-output relations in Eq. (A.7) in order to write the target POVM elements on the single-photon-input space:

$$
\begin{aligned}
F_Q^{0,\phi_B} &:= \frac{1}{2} w_{2,\phi_B}'^{\dagger} |0\rangle\langle 0| w_{2,\phi_B}', \quad \phi_B \in \left\{0, \frac{\pi}{2}\right\}; \\
F_Q^{1,\phi_B} &:= \frac{1}{2} w_{5,\phi_B}'^{\dagger} |0\rangle\langle 0| w_{5,\phi_B}', \quad \phi_B \in \left\{0, \frac{\pi}{2}\right\}; \\
F_Q^{\mathrm{Out}} &:= \frac{1}{2} \sum_{\substack{i=1,3,4,6 \\ \phi_B=0,\frac{\pi}{2}}} w_{i,\phi_B}'^{\dagger} |0\rangle\langle 0| w_{i,\phi_B}',
\end{aligned}
\tag{1.19}
$$

where $|0\rangle$ is the vacuum, and the $\frac{1}{2}$ is inserted as the probability of each basis choice[7]. Note that the $w_{i,\phi_B}' \equiv w_{i,\phi_B}'[u_1, u_2]$ are not normalized annihilation operators, but unnormalized linear combinations of u_1 and u_2, which are themselves normalized field operators corresponding to the input modes.

1.5.3 Full measurement: basic POVM and post-processing

For a general input state with an undetermined number of photons on the input modes, the basic detection events are patterns of clicks on the two threshold detectors over the three time bins. Since each detector in each of the three time slots can either click or not click, the total number of distinct outcomes is $2^6 = 64$. Because of the two possible basis choices, the number doubles to 128. Further, because the POVM elements on the infinite-dimensional Fock space of the two input modes are block-diagonal with respect to the eigenspaces of the total photon number over the output modes (this can be easily verified), the action of this POVM commutes with a quantum non-demolition (QND) measurement of the total photon number over the output modes. Therefore such a photon-counting measurement over the output modes would preserve all the quantum information which we are interested in. But since our detector model is now lossless, and since we assume that no dark counts occur, it follows that a QND photon-counting measurement collectively on the output modes is equivalent to photon-counting collectively over the input modes. Therefore, we can assume without loss of generality that each input state contains a specific number n of photons. Since all losses and inefficiencies have been moved to the channel, the click pattern with no clicks at all does not occur for either basis choice when n is nonzero. This reduces the total number of basic outcomes for a general nonzero n to 126.

Therefore, each basic event can be characterized by a basis choice ϕ_B and a click pattern $C := (c_1, c_2, c_3, c_4, c_5, c_6)$, where each c_i is either 0 or 1 (no click or click) and the index i

[7]We can make a correspondence between measurement devices for phase- and polarization-encoded protocols. Without loss of generality, we can choose the phase $\phi_B = 0$ ($\phi_B = \pi/2$) to correspond to the measurement in the basis + (×). With this understanding, we use the term "basis choice" to refer to the choice of phase setting.

corresponds to the index of the output optical mode (see Fig. 1.3(b)). This combination of indices provides an exact description of which detector has clicked and when.

Since we intend to squash to a target POVM with five events, the 126 basic full measurement outcomes must be post-processed stochastically to 5 POVM elements. Recall that the linear constraints on the post-processing scheme stem from two sources: linear relations between the target POVM elements, and the no-mixing requirement. In the case of PEBB84, the relevant information is in single-click events in the second (middle) time interval. Therefore the no-mixing constraint is that among single-click events, single clicks in the middle time slot must always be mapped to the corresponding target event in the same basis, while no other single-click event must be mapped to any of these "meaningful" single clicks.

As for linear relations between the target POVMs, in the present case there exists only one, viz.

$$F_Q^{0,0} + F_Q^{1,0} = F_Q^{0,\frac{\pi}{2}} + F_Q^{1,\frac{\pi}{2}}. \tag{1.20}$$

Using these constraints and running a numerical search, we were able to find some candidates for valid post-processing schemes $\mathcal{P}$. For each of these, we had to first look for numerical evidence for a CP squashing map. To this end, our problem was greatly simplified by the following properties of the target POVM, which are straightforward to see from the definition (1.19) of the POVM elements:

$$\begin{aligned}
\frac{2}{\sqrt{\xi\,(1-\xi)}}\left(F_Q^{0,0} - F_Q^{1,0}\right) &= \sigma_X, \\
\frac{2}{\sqrt{\xi\,(1-\xi)}}\left(F_Q^{0,\frac{\pi}{2}} - F_Q^{1,\frac{\pi}{2}}\right) &= \sigma_Y, \\
\frac{1}{2\xi - 1}\left(\mathbb{1}_2 - 2F_Q^{\mathrm{Out}}\right) &= \sigma_Z,
\end{aligned} \tag{1.21}$$

where the σ's are the Pauli matrices. The Choi-Jamiołkowski isomorphism establishes that for a linear map Λ from one C^*-algebra $\mathcal{L}(\mathcal{H}_1)$ to another, $\mathcal{L}(\mathcal{H}_2)$, complete positivity is equivalent to positive-semidefiniteness of the so-called Choi operator constructed from the map:

$$\Lambda \text{ CP} \iff (\Lambda \otimes \mathsf{id})\left[|\psi^+\rangle\langle\psi^+|\right] \geq 0, \tag{1.22}$$

where $|\psi^+\rangle$ is a state on $\mathcal{H}_1^{\otimes 2}$ maximally-entangled between the two factor copies of $\mathcal{H}_1$.

In the case of PEBB84, the target measurement is on the Hilbert space of a qubit. And since the adjoint to the squashing map, $\Lambda_{\mathrm{S}}^\dagger$, must be CP, we require that

$$\left(\Lambda_{\mathrm{S}}^\dagger \otimes \mathsf{id}\right)\left[|\psi^+\rangle\langle\psi^+|\right] \geq 0, \tag{1.23}$$

where $|\psi^+\rangle$ is a maximally-entangled state on two qubits. The two-qubit Bell state usually

denoted by $|\psi^+\rangle$ can be decomposed in terms of the Pauli operators as

$$|\psi^+\rangle\langle\psi^+| = \frac{1}{4}\left(\mathbb{1}_2 \otimes \mathbb{1}_2 + \sigma_X \otimes \sigma_X - \sigma_Y \otimes \sigma_Y + \sigma_Z \otimes \sigma_Z\right). \tag{1.24}$$

Since a particular $\mathcal{P}$ completely determines the action of $\Lambda_S^\dagger$ on each target POVM element, and since the identity operator on the qubit and the three Pauli operators can be expressed in terms of the POVM elements (the former from the completeness of the POVM, and the latter from (1.21)), it follows that the Choi operator is uniquely determined, without any free parameters. This means that for any $\mathcal{P}$, we have only to construct this Choi matrix to verify the existence of a squashing map instead of having to run an SDP, which would normally be the case in the presence of free parameters.

However, such a verification cannot be done numerically for every photon-number subspace, because there are infinitely-many such subspaces. Numerical tests serve only as an aid or clue in this case.

Using these insights, we numerically (using SDP) looked for valid post-processing schemes showing some evidence of the existence of a squashing map, and found such evidence in the case of the following post-processing scheme.

Definition 1.5.1. Post-processing scheme for the PEBB84 detector, denoted $\mathcal{P}_{\text{PE}}$:

1. Single clicks in either of the detectors in the second time slot, for either basis choice, i.e. events with $C = (0,1,0,0,0,0)$ or $C = (0,0,0,0,1,0)$, are always mapped to the corresponding single-photon outcomes;

2. Simultaneous clicks in the two detectors in only the second time slot, for either basis choice, i.e. events with $C = (0,1,0,0,1,0)$, are mapped with equal probability to each of the single-photon outcomes in the same basis;

3. All events with clicks only in the first and the third time slots (outside clicks) are mapped onto the outside click event of the target measurement;

4. Any event with clicks in both the second and any of the outer time slots is mapped with probability 0.5 onto the outside click event of the target measurement and with probability 0.125 onto each of the four other events of the target measurement.

In order to write down the form of the post-processed full POVM elements under $\mathcal{P}_{\text{PE}}$, it would be convenient to first define the following operators in the space of n-photon states

on the two input modes:

$$
\begin{aligned}
P_M^{0|\phi_B} &:= \frac{1}{n!}\left(w_{2,\phi_B}'^{\dagger}\right)^n |0\rangle\langle 0|\left(w_{2,\phi_B}'\right)^n,\\
P_M^{1|\phi_B} &:= \frac{1}{n!}\left(w_{5,\phi_B}'^{\dagger}\right)^n |0\rangle\langle 0|\left(w_{5,\phi_B}'\right)^n,\\
P_M^{\mathrm{Out}} &:= \sum_{r=0}^{n} \xi^r (1-\xi)^{n-r} |r, n-r\rangle\langle r, n-r|,\\
P_M^{\mathrm{In}} &:= \sum_{r=0}^{n} \xi^{n-r} (1-\xi)^{r} |r, n-r\rangle\langle r, n-r|,
\end{aligned}
\tag{1.25}
$$

where $\phi_B \in \left\{0, \frac{\pi}{2}\right\}$ and $|r, n-r\rangle := \frac{1}{\sqrt{r!(n-r)!}}\left(u_1^\dagger\right)^r\left(u_2^\dagger\right)^{n-r}|0\rangle$.

We make the following observations:

1. $P_M^{0|\phi_B}$ (respectively, $P_M^{1|\phi_B}$) is the POVM element for a single click in detector 0 (respectively, 1) *conditioned on* the basis-choice ϕ_B.

2. P_M^{Out} is the POVM for all events with no click in the middle time interval ("outside-only events"), independent of the basis-choice ϕ_B. This can be understood intuitively by observing (see Fig. 1.3(b)) that outside-only events happen if and only if the ξ beam-splitter sends all photons on the leading input mode u_1 to the shorter arm and all those on u_2 to the longer arm, *regardless of the basis-choice*. Similar observations can be used in understanding the next point.

3. P_M^{In} is the collective POVM for all events with clicks only in the middle time interval ("inside-only events"), independent of the basis-choice ϕ_B. Consequently, $P_M^{0|\phi_B}$ and $P_M^{1|\phi_B}$ are some of the constituents in P_M^{In}.

4. The POVM element for *inside double-clicks* conditioned on the basis-choice ϕ_B is given by the part of P_M^{In} other than single-clicks:

$$P_M^{\mathrm{In,D}|\phi_B} = P_M^{\mathrm{In}} - P_M^{0|\phi_B} - P_M^{1|\phi_B}.$$

5. The POVM element for events with simultaneous inside and outside clicks is given by the complement of inside-only and outside-only events combined, for either basis-choice:
$$P_M^{\mathrm{In,Out}} = \mathbb{1}_M - P_M^{\mathrm{In}} - P_M^{\mathrm{Out}}.$$

6. Since the basis-choice is made uniformly, the POVM element for the *joint* (as opposed to *conditional*) occurrence of any type of event, say E, and the basis-choice ϕ_B, is
$$P_M^{\mathrm{E},\phi_B} = \Pr[\phi_B] P_M^{\mathrm{E}|\phi_B} = \frac{1}{2} P_M^{\mathrm{E}|\phi_B}.$$
The overall POVM element for a certain event type E is
$$P_M^{\mathrm{E}} = P_M^{\mathrm{E},0} + P_M^{\mathrm{E},\frac{\pi}{2}}.$$

We now build the post-processed full POVM elements corresponding to the post-processing scheme $\mathcal{P}_{\mathrm{PE}}$ described by Definition 1.5.1, first using only the basic definitions:

$$\begin{aligned}
F_M^{0,\phi_B} &:= P_M^{0,\phi_B} + \frac{1}{2} P_M^{\mathrm{In,D},\phi_B} + \frac{1}{8} P_M^{\mathrm{In,Out}}, \\
F_M^{1,\phi_B} &:= P_M^{1,\phi_B} + \frac{1}{2} P_M^{\mathrm{In,D},\phi_B} + \frac{1}{8} P_M^{\mathrm{In,Out}}, \\
F_M^{\mathrm{Out}} &:= P_M^{\mathrm{Out}} + \frac{1}{2} P_M^{\mathrm{In,Out}}, \\
\phi_B &\in \left\{0, \frac{\pi}{2}\right\}.
\end{aligned} \tag{1.26}$$

Using the observations enumerated above, we can reduce these to

$$\begin{aligned}
F_M^{0,\phi_B} &= \frac{1}{2} P_M^{0|\phi_B} + \frac{1}{4}\left(P_M^{\mathrm{In}} - P_M^{0|\phi_B} - P_M^{1|\phi_B}\right) + \frac{1}{8}\left(\mathbb{1}_M - P_M^{\mathrm{In}} - P_M^{\mathrm{Out}}\right), \\
F_M^{1,\phi_B} &= \frac{1}{2} P_M^{1|\phi_B} + \frac{1}{4}\left(P_M^{\mathrm{In}} - P_M^{0|\phi_B} - P_M^{1|\phi_B}\right) + \frac{1}{8}\left(\mathbb{1}_M - P_M^{\mathrm{In}} - P_M^{\mathrm{Out}}\right), \\
F_M^{\mathrm{Out}} &= P_M^{\mathrm{Out}} + \frac{1}{2}\left(\mathbb{1}_M - P_M^{\mathrm{In}} - P_M^{\mathrm{Out}}\right), \\
\phi_B &\in \left\{0, \frac{\pi}{2}\right\}.
\end{aligned} \tag{1.27}$$

Recall that in order for a linear map to provide a valid squashing model, it must satisfy two classes of constraints: the linear constraints (from linear relations among the target POVMs and from no-mixing), and complete positivity (equivalent to positive-semidefiniteness of the Choi matrix).

As for the linear constraints, we observe that the post-processing defined above satisfies no-mixing, since the "meaningful" events, i.e. single clicks in the middle time slot, are

mapped to the corresponding target events, and no noise is introduced at the single-photon level. Furthermore, recalling that the only linear relation between the target POVMs is (1.20), it is easy to see that this post-processing scheme preserves this linear relation. From these observations, it follows that all relevant linear constraints are satisfied (which is not surprising, since we found $\mathcal{P}_{\mathrm{PE}}$ by running a search subject to these very linear constraints).

In the following, we present a semi-analytical proof[8] that the Choi operator defined by the above post-processing (recall that in this case the post-processing completely determines the Choi matrix) is positive-semidefinite for a range of values of the characteristic parameter ξ, and that therefore a squashing model exists for this range of parameter values.

1.5.4 Proof of complete positivity

We begin the proof by constructing the Choi matrix explicitly for the map defined by the post-processing in consideration. Recalling that $\Lambda_{\mathrm{S}}^{\dagger}\left[F_Q^{(i)}\right] = F_M^{(i)}$ (where (i) stands for any descriptive superscript), the decomposition (1.24) of the Bell state, and the properties (1.21) of the target POVM, we compute

$$
\begin{aligned}
4\left(\Lambda_{\mathrm{S}}^{\dagger}\otimes\mathsf{id}\right)\left[|\psi^+\rangle\langle\psi^+|\right] &= \left(\Lambda_{\mathrm{S}}^{\dagger}\otimes\mathsf{id}\right)\left[\mathbb{1}_2\otimes\mathbb{1}_2+\sigma_X\otimes\sigma_X-\sigma_Y\otimes\sigma_Y+\sigma_Z\otimes\sigma_Z\right]\\
&= \left(\Lambda_{\mathrm{S}}^{\dagger}\otimes\mathsf{id}\right)\Bigg[\mathbb{1}_2\otimes\mathbb{1}_2+\frac{2}{\sqrt{\xi\,(1-\xi)}}\left(F_Q^{0,0}-F_Q^{1,0}\right)\otimes\sigma_X\\
&\quad-\frac{2}{\sqrt{\xi\,(1-\xi)}}\left(F_Q^{0,\frac{\pi}{2}}-F_Q^{1,\frac{\pi}{2}}\right)\otimes\sigma_Y+\frac{1}{2\xi-1}\left(\mathbb{1}_2-2F_Q^{\mathrm{Out}}\right)\otimes\sigma_Z\Bigg]\\
&= \mathbb{1}_M\otimes\mathbb{1}_2+\frac{2}{\sqrt{\xi\,(1-\xi)}}\left(F_M^{0,0}-F_M^{1,0}\right)\otimes\sigma_X\\
&\quad-\frac{2}{\sqrt{\xi\,(1-\xi)}}\left(F_M^{0,\frac{\pi}{2}}-F_M^{1,\frac{\pi}{2}}\right)\otimes\sigma_Y+\frac{1}{2\xi-1}\left(\mathbb{1}_M-2F_M^{\mathrm{Out}}\right)\otimes\sigma_Z\\
&= \mathbb{1}_M\otimes\mathbb{1}_2+\frac{1}{\sqrt{\xi\,(1-\xi)}}\left(P_M^{0|0}-P_M^{1|0}\right)\otimes\sigma_X\\
&\quad-\frac{1}{\sqrt{\xi\,(1-\xi)}}\left(P_M^{0|\frac{\pi}{2}}-P_M^{1|\frac{\pi}{2}}\right)\otimes\sigma_Y+\frac{1}{2\xi-1}\left(\mathbb{1}_M-2F_M^{\mathrm{Out}}\right)\otimes\sigma_Z. \qquad (1.28)
\end{aligned}
$$

From the definitions (1.25), it is evident that for either choice of ϕ_B, the operator $\left(P_M^{0|\phi_B}-P_M^{1|\phi_B}\right)$ is of the form $\frac{1}{2^n}\left(|u\rangle\langle u|-|v\rangle\langle v|\right)$ for some normalized vectors $|u\rangle$ and $|v\rangle$. For two such normalized vectors with inner product $\langle u|v\rangle=\alpha$, the traceless rank-2 operator $\left(|u\rangle\langle u|-|v\rangle\langle v|\right)$ has the eigenvalues $\pm\sqrt{1-|\alpha|^2}$. In the case of $\left(P_M^{0|\phi_B}-P_M^{1|\phi_B}\right)$, for either ϕ_B, $|\alpha|^2=(2\xi-1)^{2n}$.

[8] By semi-analytical, we mean that part of the proof is based on numerical computations.

Again from (1.25), along with the definition of F_M^{Out} in (1.27), we see that

$$\left(\mathbb{1}_M - 2F_M^{\mathrm{Out}}\right) = \sum_{r=0}^{n} \left((1-\xi)^r \xi^{n-r} - \xi^r (1-\xi)^{n-r}\right) |r, n-r\rangle\langle r, n-r|. \tag{1.29}$$

The eigenvalue spectrum of an operator $A \otimes B$ in the form of a Kronecker product of two operators is just the set of all products ab, where a is an eigenvalue of A and b one of B. While the first term in our expression (1.28) for the Choi matrix (modulo the factor 4, which does not affect the arguments regarding positive-semidefiniteness) is just the identity operator, each of the other terms is the Kronecker product of a traceless Hermitian operator on the M space and a Pauli operator on a qubit. Thus, it is straightforward to determine the smallest (i.e. most negative) eigenvalue of each of the last three terms. Adding together these smallest eigenvalues and augmenting their sum by 1 (the "smallest" eigenvalue of the first term, i.e. the identity operator), we arrive at the following lower bound on the smallest eigenvalue of the Choi matrix (for, the smallest eigenvalue of the sum of some operators cannot be smaller than the sum of the respective smallest eigenvalues of the operators):

$$\begin{aligned}
\lambda_{\min}[\xi, n] &\geq \frac{1}{4}\left(1 - \frac{1}{2^n}\sqrt{\frac{1-(2\xi-1)^{2n}}{\xi(1-\xi)}} - \frac{1}{2^n}\sqrt{\frac{1-(2\xi-1)^{2n}}{\xi(1-\xi)}} - \left(\frac{\xi^n - (1-\xi)^n}{2\xi - 1}\right)\right) \\
&= \frac{1}{4}\left(1 - 2^{1-n}\sqrt{\frac{2\sum_{r=1}^{2n}(2\xi-1)^{r-1}}{\xi}} - \sum_{k=1}^{n}\xi^{n-k}(1-\xi)^{k-1}\right) \\
&=: \frac{1}{4}\left(1 - g_1[\xi, n] - g_2[\xi, n]\right).
\end{aligned} \tag{1.30}$$

Now,

$$\begin{aligned}
g_1[\xi, n] &= 2^{1-n}\sqrt{\frac{2\sum_{r=1}^{2n}(2\xi-1)^{r-1}}{\xi}} \\
&\leq 2^{2-n}\sqrt{\frac{n}{\xi}} \\
&=: f_1[\xi, n],
\end{aligned} \tag{1.31}$$

where we used the fact that $0.5 \leq \xi \leq 1$, so that $0 \leq 2\xi - 1 \leq 1$. On the other hand,

$$\begin{aligned} g_2[\xi, n] &= \sum_{r=1}^{n} \xi^{n-r}(1-\xi)^{r-1} \\ &\leq n\xi^{n-1} \\ &=: f_2[\xi, n], \end{aligned} \tag{1.32}$$

again using the fact that $0.5 \leq \xi \leq 1$, whereby $\xi \geq 1 - \xi \geq 0$.

Therefore,

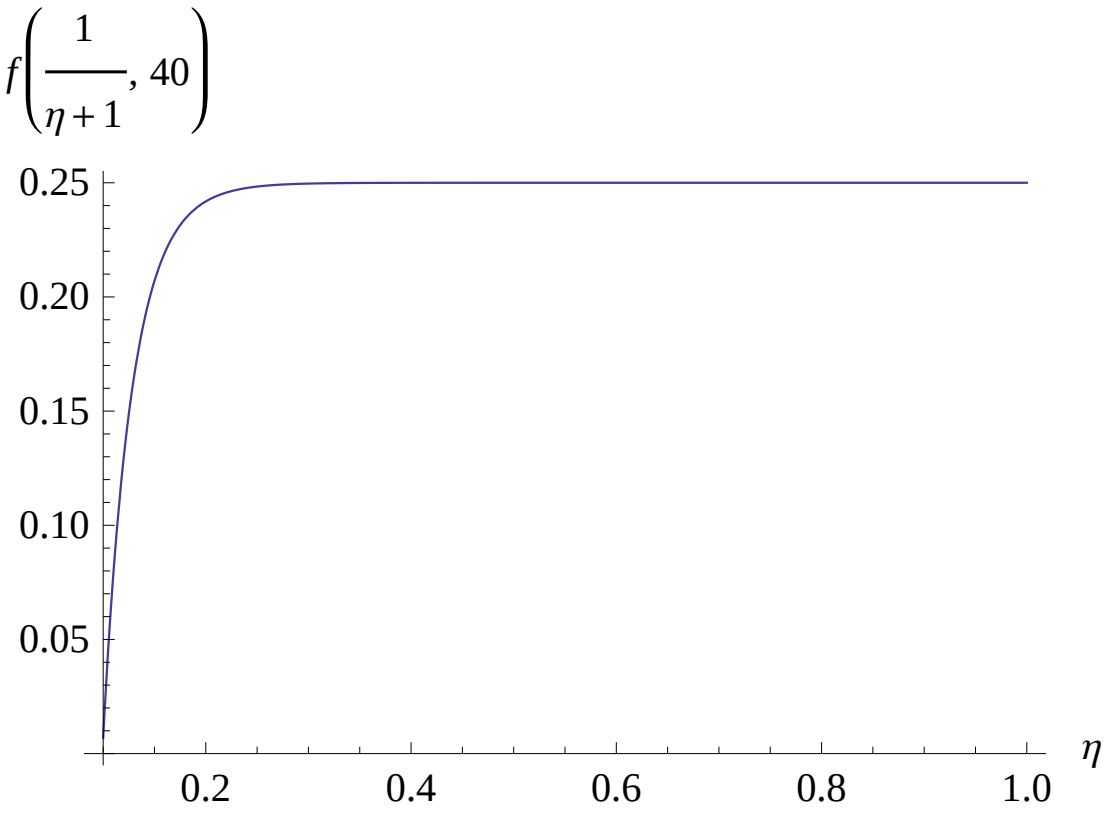
$$\begin{aligned} \lambda_{\min}[\xi, n] &\geq \frac{1}{4}\left(1 - g_1[\xi, n] - g_2[\xi, n]\right) \\ &\geq \frac{1}{4}\left(1 - f_1[\xi, n] - f_2[\xi, n]\right) \\ &=: f[\xi, n]. \end{aligned} \tag{1.33}$$

Further, $\forall n \geq 1$ and $\forall \xi \in [0.5, 1]$, $f_1[\xi, n+1] \leq f_1[\xi, n]$. On the other hand, f_2 has the property that $\forall n \geq 1$, $f_2[\xi, n+1] \leq f_2[\xi, n]$ $\forall \xi \leq \frac{n}{n+1}$, i.e. whenever $\eta \geq \frac{1}{n}$ (recall that $\xi = \frac{1}{1+\eta}$). Therefore, for some $n_0 > 1$, $f[\xi, n] \geq f[\xi, n_0]$ $\forall n \geq n_0$ and $\forall \eta \geq \frac{1}{n_0}$. Choosing $n_0 = 40$, we get

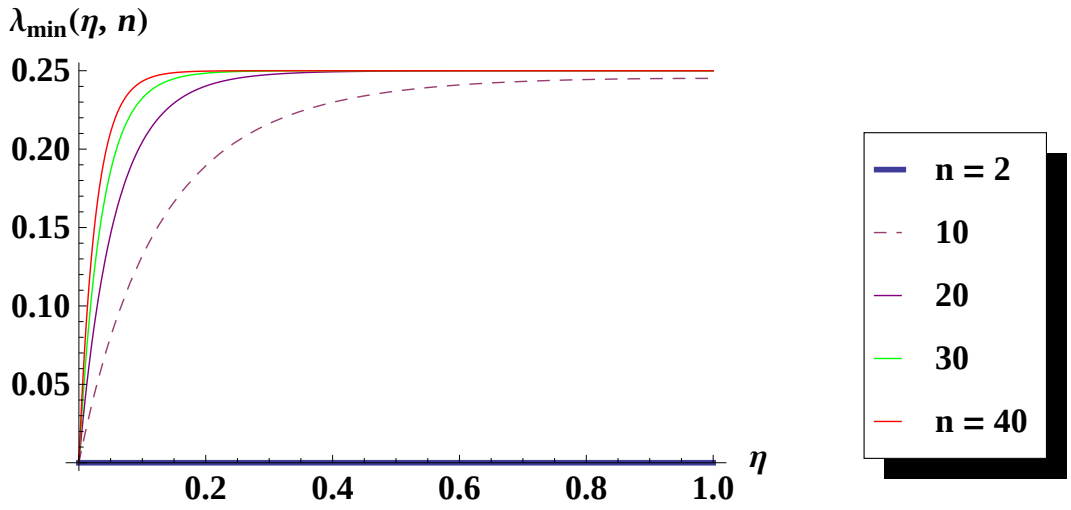
$$\lambda_{\min}[\xi, n] \geq f[\xi, 40] \quad \forall n \geq 40, \forall \xi \geq 0.025. \tag{1.34}$$

Fig. 1.4(a) shows a plot of this bound against the phase-modulator transmittance η for $0.1 \leq \eta \leq 1$, showing that the bound is nonnegative over this range of η. This proves the positive-semidefiniteness of the Choi matrix for $n \geq 40$ and $\eta \geq 0.1$. We have numerically verified the positive-semidefiniteness for all $n < 40$ throughout the whole range of η. The plots of the smallest eigenvalue for some selected values of n are presented in Fig. 1.4(b) as a sample.

Thus, we have established the existence of a squashing model for the PEBB84 detection setup under the present post-processing scheme for $\eta \geq 0.1$. Note that our choice of the cutoff n_0 was arbitrary. By choosing a higher cutoff, we could in principle get the limit of the range arbitrarily close to $\eta = 0$. However, the range $\eta \geq 0.1$ covers the characteristic values of phase-modulator transmissivity encountered in practical implementations, which are usually around $\eta \approx 0.5$ [37]. Therefore, for practical purposes, our squashing model suffices.



(a) Plot of the lower bound $f\left[\frac{1}{1+\eta}, 40\right]$ vs. η for $0.1 \leq \eta \leq 1$.



(b) Plot of the smallest eigenvalue $\lambda_{\min}[\eta, n]$ of the Choi matrix vs. η for $n \in \{2, 10, 20, 30, 40\}$. Note: the plot for $n = 2$, rendered in thick blue style, coincides with the horizontal axis.

Figure 1.4: Plots accompanying the proof for the complete positivity of the PEBB84 squashing map.

Chapter 2

Statistical estimation methods for linear optics

2.1 Introduction

Linear optics is among the most promising platforms for implementing quantum computing and quantum communication applications such as quantum key-distribution (QKD). In many of these applications, control and / or knowledge of the number of photons in optical signals is of critical importance [38]. In QKD, for example, mathematical proofs for the information-theoretic security of a protocol typically rely on assumptions about the number of photons emitted by a source as well as of those received by a detector. The state of the art in detector and source technology does not yet provide feasible realizations of devices with a handle on the number of photons emitted or detected. This necessitates some other methods to monitor or estimate the photon-number statistics, or, if possible, to render the mathematical proofs applicable to scenarios where the photon-number statistics is unrestricted, uncharacterized or partially-characterized. Several such methods have been successfully devised with varied applicability. On the source side, the method of the so-called decoy states [24, 25] enables us to use a statistical characterization of a source to track the flow of information through signals with specific numbers of photons. On the detector side, squashing models [26, 27] enable us to treat all detection statistics as though they were produced by the detection of only a restricted class of signals, for instance only single-photon signals.

While squashing models afford an excellent solution where they can be found, there are many important situations where finding such models is not straightforward. In such cases, alternative methods must be found, which may vary depending on the application. In the present discussion, we shall focus on the QKD application. In this context, as mentioned before, the need for squashing models arises because security proofs are formulated on restricted mathematical models of detection devices. Such a model does not cover the whole extent of physical behaviour of the respective device. Specifically, it assumes a certain size

of the Hilbert space on which the states entering the device are mathematically described. A squashing model allows us to hold on to that assumption, effectively only being too conservative in our defence against eavesdropping (by overestimating the eavesdropper's ability), which obviously does not threaten the security of a QKD scheme.

In the absence of a squashing model, alternate methods must be used to account for these gaps between theory and implementation. Recently, Fung *et al.* [28] have devised a method to use a universal squashing map to provide bounds on relevant security parameters. In the present work, we present another method, similar to [28] in its approach inasmuch as it is based on statistical inferences to derive bounds.

Our method is based on the fact that in the absence of a squashing model, security can still be salvaged at the cost of some performance, i.e. by extracting key at a smaller rate. The question of what fraction of the key-rate must be sacrificed is closely related to that of what fraction of detected signals satisfies the assumption in the model, regarding the size of the Hilbert space. In the following we shall first state this connection mathematically, subsequently describing the different methods we devised in particular contexts to estimate the latter fraction. In the remainder, we refer to such methods, which are loosely connected in their approach, collectively as "the estimation method". While there has been previous work on statistical inference in linear optics, e.g. Lütkenhaus [39] and Koashi *et al.* [40], our contribution consists of systematizing the approach to statistical estimation, with clear motivation from QKD. We also apply the method to the phase-encoded BB84 protocol, which has not been done previously.

The chapter is structured as follows. In §2.2 we present the mathematical motivation, followed in §2.3 by a demonstration of the statistical estimation method on a simple example, that of standard polarization-encoded optical BB84 (already presented in [39]). In §2.4, we present the application of the estimation method in the phase-encoded BB84 protocol.

Note that the use of the estimation method does not require any change in the hardware used in implementing a QKD scheme. It only requires some small calculations to be added to the parameter-estimation step to calculate some bounds, which are later used to decide the length of the final key. Operationally, these are simple modifications to the protocol.

2.2 Motivation for the estimation method

Consider a QKD scheme based on optical signals. It can be described as follows: two honest parties, Alice and Bob, want to establish a shared secret key oblivious to an adversarial eavesdropper, Eve. Alice prepares some optical signals and sends them to Eve. Eve performs an attack of her choice on the signals, and sends (possibly different) signals to Bob. We restrict to cases where the optical phase between signals in distinct rounds of the protocol is irrelevant, although each round might consist of several optical modes with mutual phase reference, for example in phase-encoded BB84 (§2.4). This allows us

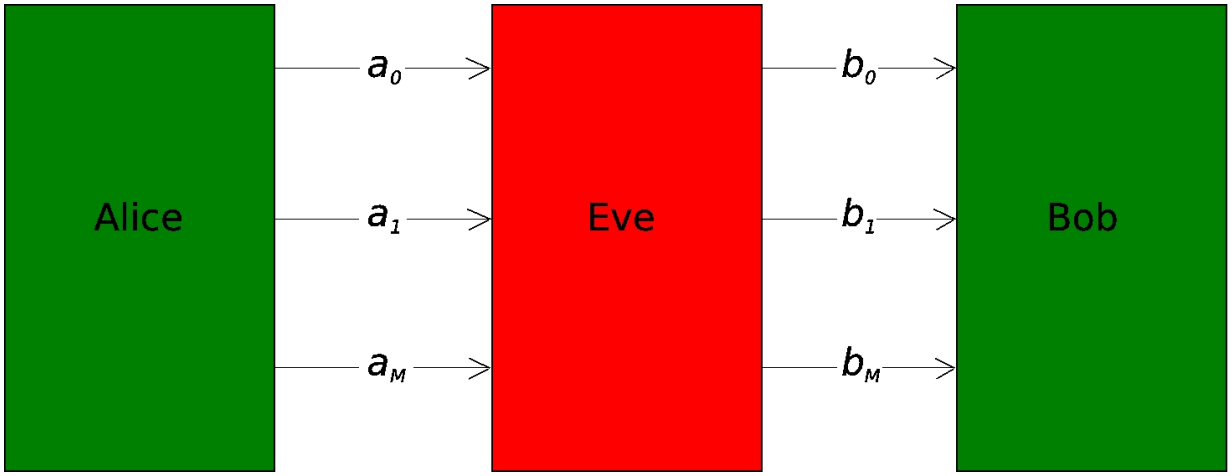


Figure 2.1: Schematic of an optical QKD protocol: a refers to signals sent by Alice, b to those received by Bob's device, and the subscripts denote photon numbers.

to assume without further loss of generality that different rounds are mutually phase-randomized, and consequently, a QND measurement of the total photon number, both at the source's output and at the detector's input for each round, would not disturb the quantum information relevant to the protocol. Therefore, following the line of reasoning employed in §1.5.3, we can assume that the signals in each round (those sent by Alice as well as those received by Bob) consist of specific numbers of photons.

Figure 2.1 shows a schematic diagram of such a QKD protocol. In every round of the protocol, Alice sends a signal to Eve, and Eve sends one to Bob (recall that each "signal" may consist of several individual optical modes). In each round, Alice might send a signal with either no photons (a_0), with one photon (a_1), or with multiple (more than one) photons (a_M) distributed over the modes constituting the signal. Similarly, in every round, Bob's device might receive no photons (b_0), one photon (b_1), or multiple photons (b_M).

Usually, security proofs are devised for the case that Alice's device emits a single photon and Bob's device receives a single photon. In order that the security analysis remain valid for the realistic scenario where signals can contain multiple photons or vacua, we use a conservative method called "tagging". Tagging is the assumption that in any round where either Alice's or Bob's signals contain multiple photons or vacua[1], Eve knows everything about the state of the signals, and therefore that no key must be extracted from these rounds. Operationally, this amounts to additional shortening of the key during privacy-amplification. In order to better understand tagging, let us briefly discuss the derivation of the formula for the secure key-rate. The details of the terms appearing in the formula vary

[1]While this is the most general description of tagging, we usually work under the assumption that Bob's device does not click when the input is a vacuum (which includes the assumption that there are no dark counts in Bob's detectors).

depending on the particular scheme in consideration, but the general philosophy remains the same. For a more detailed and precise description, we refer to [12].

Denote the initial size of the raw key by N. This raw key consists of all the data remaining after the initial quantum communication and measurement step of the QKD scheme, and possibly sifting. It is convenient to think of N not as the absolute size but the fraction of a total initial size, while assuming that the initial size is very large (statistically-significant). The next step is parameter-estimation (PE), where some of the raw key is publicly announced for the purpose of making some statistical inferences on the remaining part. Assume that a portion m of the key is used up for PE. The size of the remaining key is $N - m =: n$. The next step is error-correction (EC), where an amount denoted by leak_{EC} of information is leaked publicly. We shall have to subtract this amount from the final length of the key. For our present purpose, N, m, n and leak_{EC} are merely symbols without much significance, because no photon-number-based filtration has been done yet. The role of the estimation method is in the subsequent steps of the calculation (although operationally it is part of the PE step).

Denote by $f(a_1, b_1)$ the fraction of the remaining key n which comes from rounds with the properties a_1 and b_1, i.e. where Alice's device emitted one photon and Bob's device received one photon. Further, denote by e_{a_1,b_1} the error-rate in this part of the key. In the next (and final) step of the QKD scheme, which is privacy-amplification (PA), the remaining key must be further shortened by an amount dependent of these parameters. Let $s[e_{a_1,b_1}]$ denote the fraction of shortening required on the part of the key that comes from (a_1, b_1)-rounds[2]. This means that from every bit in this part, $1 - s[e_{a_1,b_1}]$ bits of key can be extracted. On the other hand, by our tagging assumption, no key can be extracted from the remaining part. Therefore, recalling that we must subtract the amount leaked during EC, the formula for the secure key-rate is

$$r = nf(a_1, b_1)\left(1 - s[e_{a_1,b_1}]\right) - \text{leak}_{\text{EC}}.$$

Since we assume that the size of the data is statistically-significant, and since none of the steps before PA consisted of photon-number-based filtration, it follows that the statistical quantities appearing in the above expression for the key-rate, $f(a_1, b_1)$ and e_{a_1,b_1}, would be identical in the test data used in PE and the rest of the data. Therefore, it would suffice to find a way to determine these quantities on the test data.

As for a_1, a technique using what are known as *decoy states* [24, 25] allows us to calculate, in principle, *any property of the statistics conditioned on specific numbers of photons emitted by Alice's device.* It remains to find a way to calculate or estimate the relevant quantities further conditioned on b_1. To this end, there are different ways. If a squashing model exists for Bob's device, then for all practical purposes, we can assume that all the data comes from b_1-rounds (squashing models are discussed in Chapter 1). But in the absence of such a model, the estimation method discussed here plays a role.

[2]Details of the calculation of $s[e_{a_1,b_1}]$ in terms of the Holevo quantity may be found in [12].

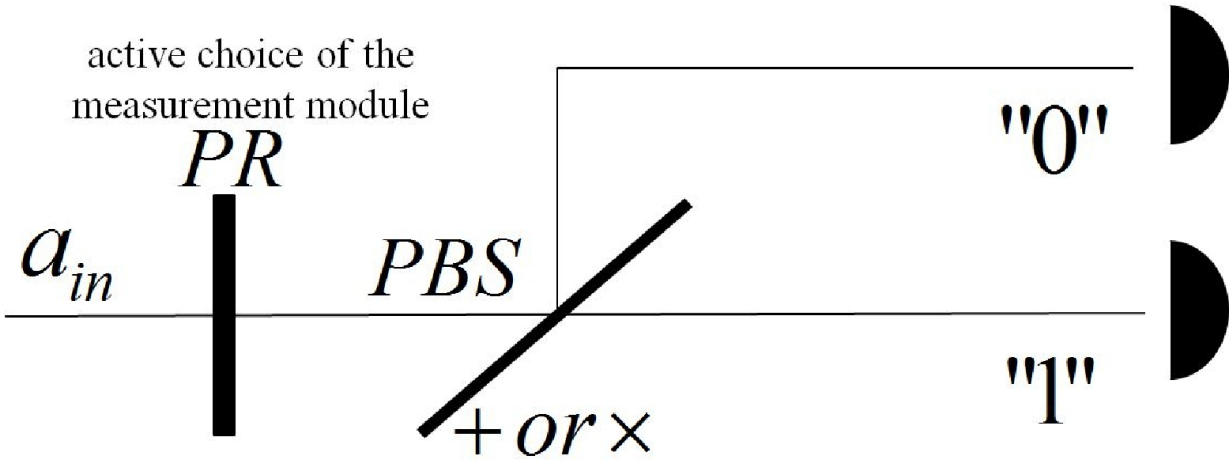


Figure 2.2: Schematic diagram of the detection setup for optical polarization-encoded BB84 with active basis-choice.

Specifically, we aim to find a nonzero lower bound on $f(a_1, b_1)$, so that the worst-case key-rate can be calculated by an optimization over a range of values of $f(a_1, b_1)$. In the absence of a nonzero lower bound, the worst-case key-rate would trivially become zero.

The details of the optimization mentioned above (for example, the intricacies of optimizing also over e_{a_1,b_1}) are beyond the scope of the present discussion. It suffices to note here that essentially, we seek a lower bound on the fraction of single-photon detection events occurring at Bob's device (or equivalently, an upper bound on the multi-photon components). The subject of this chapter is how to find such bounds using the statistical estimation method.

2.3 Example of the estimation method: BB84

(The results demonstrated in this section have originally been presented by Lütkenhaus in his doctoral thesis [39].)

One of the simplest detection devices in optics-based QKD is the one used in the standard Bennett–Brassard 1984 (BB84) QKD protocol with active basis-choice (Fig. 2.2). It consists of a polarizer whose plane of polarization can be switched actively between two mutually-unbiased settings, followed by a polarizing beam-splitter which separates two orthogonally-polarized components and feeds them to two threshold detectors. We make the following important simplifying assumptions:

1. The efficiencies of the two detectors are equal, so that the associated loss can be outsourced to the channel.

2. There are no dark counts in either of the detectors.

The security proof for the BB84 protocol is based on a mathematical description on qubits. But an actual optical implementation would involve signals with more than one photons (both on the source side and the detector side), whose quantum-mechanical states would not be qubits, and therefore there is a need for a theoretical bridge. In this case, such a fix has already been formulated: on the source side, decoy states and tagging can be used, while on the detector side a squashing model has been found. However, we still present here a statistical estimation method, which would be necessary only if there were no squashing model, just as a demonstration of the method on a simple example. This method can be used to estimate the relative weights of the single- and multiple-photon components in the detected signals, so that the tagging arguments in §2.2 may be used to compute a bound on the secure key-rate.

The basic philosophy of the method is as follows. For the detection setup in question, for either choice of the measurement basis, any non-vacuum input results in one of three outcomes: a click in one or the other of the two threshold detectors, or a simultaneous click in both. We refer to the latter as double-click events, or simply double-clicks. Likewise, we refer to the other detection events as single-clicks. It is intuitively evident that double-clicks should be more frequent for input states with higher numbers of photons. Also, we know that a single-photon input would never result in a double-click. This might enable us to use the fraction of double-clicks among all detection events to estimate the relative weights of single-photon and multi-photon components in the received signals. We shall now make this intuition more precise mathematically, and then in §2.3.1 derive the necessary parameters in order to apply it. We shall see, however, that our initial idea doesn't quite do the job we desire of it. In §2.3.2 we present a modification which fixes this problem.

In order to understand the estimation method more precisely, let us introduce some notation. We denote by the lowercase Latin s, d and e, respectively, single-clicks, double-clicks and error events. In order to understand what we mean by an error event, we must give some background about the BB84 protocol. In every round of communication in optical polarization-encoded BB84, the sender ("Alice") sends the receiver ("Bob") an optical signal polarized in a certain way. Alice chooses the direction of polarization based on two random choices: a basis $A \in \{+, \times\}$ and a bit $\alpha \in \{0, 1\}$. Say the direction of propagation of the signal is z in some reference frame. Then, for the choices $(+, 0)$ she uses the x polarization, while for $(+, 1)$, $(\times, 0)$ and $(\times, 1)$ the y, the diagonal $(x + y)$, and the antidiagonal $(x - y)$ polarizations, respectively. At his end, Bob randomly chooses a measurement basis $B \in \{+, \times\}$ and gets either no click, a double-click, or a single-click outcome $\beta \in \{0, 1\}$. An error event, or simply "an error", denoted by e, is one where Bob gets a single click such that $A = B$ but $\alpha \neq \beta$. Note that an e (error event) is always also an s (single-click), by definition.

For any description i of a type of events, we denote by M^i the POVM measure for that class of events. For some input state ρ, we denote the probability for an event of type i to

occur by $\Pr[i|\rho]$. That is to say, $\Pr[i|\rho] = \mathrm{Tr}[M^i\rho]$. We see that

$$\begin{aligned} M^s &= M^{+,0} + M^{+,1} + M^{\times,0} + M^{\times,1}, \\ M^d &= \mathbb{1} - M^s. \end{aligned} \tag{2.1}$$

Note that the latter only holds for non-vacuum input. As for the error events e, there is no context-independent definition. Rather, the POVM for an error event depends on (A, α):

$$M^{e|(A,\alpha)} = M^{A,\alpha\oplus 1}, \tag{2.2}$$

where $\oplus$ denotes addition modulo 2.

For a particular run of BB84, consisting of a statistically-significant number of rounds, we denote the relative frequency of events of type i by $\mathrm{Fr}[i]$. Since the detection POVM is block-diagonal in the number of photons at the input, we can assume without loss of generality that every detection event is a detection of a state with a specific number of photons. We denote the property of an event to have been triggered by an n-photon state by the symbol p_n. For example, $\mathrm{Fr}[p_3]$ would denote the relative frequency of events triggered by 3-photon states. With frequencies, as with probabilities, we use the established notation for conditionals. For instance, $\mathrm{Fr}[s|p_5]$ would denote the relative frequency of single-clicks among all events triggered by 5-photon states.

We denote a generic n-photon state for a general n by ρ_n. For an event type i, we define

$$\begin{aligned} \Pr^n_{\min}[i] &:= \min_{\rho_n} \Pr[i|\rho_n], \\ \Pr^{\geq n}_{\min}[i] &:= \min_{m\geq n} \Pr^m_{\min}[i]. \end{aligned} \tag{2.3}$$

Having defined the notation, let us look at the basic rationale of all the estimation methods we shall present subsequently. Let i be some event type, possibly with additional qualifiers. We judiciously choose properties i such that $\Pr^0_{\min}[i] = \Pr^1_{\min}[i] = 0$ (for instance,

i could be d). The rest of the argument goes as follows:

$$\begin{aligned}
\mathrm{Fr}\left[i\right] &= \sum_{n=0}^{\infty} \mathrm{Fr}\left[p_n\right] \mathrm{Fr}\left[i|p_n\right] \\
&\geq \sum_{n=0}^{\infty} \mathrm{Fr}\left[p_n\right] \mathrm{Pr}^n_{\min}[i] \\
&= \sum_{n=2}^{\infty} \mathrm{Fr}\left[p_n\right] \mathrm{Pr}^n_{\min}[i] \\
&\geq \mathrm{Pr}^{\geq 2}_{\min}[i] \sum_{n=2}^{\infty} \mathrm{Fr}\left[p_n\right]. \\
\Rightarrow \sum_{n=2}^{\infty} \mathrm{Fr}\left[p_n\right] &\leq \frac{\mathrm{Fr}\left[i\right]}{\mathrm{Pr}^{\geq 2}_{\min}[i]}. \qquad (2.4)
\end{aligned}$$

In the chain of arguments above, we have used the definitions of $\mathrm{Pr}^n_{\min}$ and $\mathrm{Pr}^{\geq n}_{\min}$, and the assumptions made earlier, that $\mathrm{Pr}^0_{\min}[i] = \mathrm{Pr}^1_{\min}[i] = 0$.

Thus, by finding suitable event types i, we can derive upper bounds on the multiple-photon components. Provided $\mathrm{Pr}^{\geq 2}_{\min}[i]$ can be calculated, we can directly compute the bound, since $\mathrm{Fr}\left[i\right]$ is an observable. The only thing we must hope in addition to the conditions already stated above is that $\mathrm{Pr}^{\geq 2}_{\min}[i]$ should be nonzero. For the above reasoning to work, it is important that the sample from which the frequency distribution is drawn be of a statistically-significant size.

2.3.1 Estimation from double-clicks

Our first guess at a suitable property i is $i = d$, i.e. double-clicks. From our assumption that there are no dark counts, $\mathrm{Fr}\left[d|p_0\right]$ and $\mathrm{Fr}\left[d|p_1\right]$ are obviously zero, and therefore, naturally, $\mathrm{Pr}^0_{\min}[d] = \mathrm{Pr}^1_{\min}[d] = 0$. In order to find $\mathrm{Pr}^{\geq 2}_{\min}[d]$, we can in principle compute $\mathrm{Pr}^n_{\min}[d]$ explicitly as a function of n. But we shall see shortly that this is unnecessary. We first observe the following: for any positive operator M, $\min_{\rho} \mathrm{Tr}\left[M\rho\right]$ over all normalized density matrices ρ on the pertinent Hilbert space is just the smallest eigenvalue of M.

Next, we consider the POVM operator associated with double-clicks on the 2-photon subspace. If $a_1^\dagger$ is the creation operator of a photon in the X-polarized optical mode, $a_2^\dagger$ that for the Y-polarized mode, and $|0\rangle$ denotes the vacuum state, then the POVM element for double-clicks in the 2-photon subspace can be constructed as

$$M_2^d = \frac{1}{2}\left(a_1^\dagger a_2^\dagger |0\rangle\langle 0| a_1 a_2\right) + \frac{1}{2}\left(\left(\frac{a_1^\dagger + a_2^\dagger}{\sqrt{2}}\right)\left(\frac{a_1^\dagger - a_2^\dagger}{\sqrt{2}}\right)|0\rangle\langle 0|\left(\frac{a_1 + a_2}{\sqrt{2}}\right)\left(\frac{a_1 - a_2}{\sqrt{2}}\right)\right), \qquad (2.5)$$

where the $\frac{1}{2}$ is the probability of each basis-choice. In the Fock basis $\{|2,0\rangle, |1,1\rangle, |0,2\rangle\}$, where the two quantum numbers denote the excitation numbers of the a_1 and a_2 modes

respectively, this operator looks like

$$M_2^d = \begin{bmatrix} \frac{1}{4} & 0 & -\frac{1}{4} \\ 0 & \frac{1}{2} & 0 \\ -\frac{1}{4} & 0 & \frac{1}{4} \end{bmatrix}. \tag{2.6}$$

It is clear that M_2^d is singular, and that therefore $\Pr_{\min}^{n=2}[d] = 0$. It follows that $\Pr_{\min}^{\geq 2}[d] = 0$, and so our first guess for the event type, $i = d$, turns out to be unsuitable for our purpose.

2.3.2 Estimation from double-clicks and errors

From the previous calculation, we see that double-clicks alone cannot be used to detect all photon-number components greater than 1, because in the two-photon subspace there exist states which would never produce double-clicks. Our next guess for a suitable event type is $i = (d \vee e)$, i.e. the property of being either a double-click or an error. Again, as before, it is easy to see that $\mathrm{Fr}\left[d \vee e | p_0\right] = 0$. As for the single-photon subspace, we know that for each (A, α) there exists a single-photon state ρ such that $\Pr\left[e|\rho\right] = 0$, and double-clicks never occur anyway. Therefore, $\Pr_{\min}^{1}[d \vee e] = 0$.

In order to calculate $\Pr_{\min}^{\geq 2}[d \vee e]$, we shall now directly compute $\Pr_{\min}^{n}[d \vee e]$ explicitly as a function of n. For this, we must construct the associated POVM operator for a general n. Recall that the definition of an error event is contextually dependent on (A, α). However, we need calculate only in one of the four cases of (A, α). By symmetry, the same would hold for each of the other three cases, and consequently also on an average overall.

Let us consider the choice $(A, \alpha) = (+, 0)$ and some $n \neq 0$. In this case, the only outcomes which are not double-clicks or errors are single-clicks $(+, 1)$, $(\times, 0)$ and $(\times, 1)$. Therefore the POVM element for $d \vee e$ is

$$M_n^{(d \vee e)|(+,0)} = \mathbb{1} - \frac{1}{2}\left(|n, 0\rangle_{++}\langle n, 0| + |n, 0\rangle_{\times\times}\langle n, 0| + |0, n\rangle_{\times\times}\langle 0, n|\right). \tag{2.7}$$

Further, because

$$\begin{gathered} {}_{+}\langle n, 0|n, 0\rangle_{+} = {}_{\times}\langle n, 0|n, 0\rangle_{\times} = {}_{\times}\langle 0, n|0, n\rangle_{\times} = 1, \\ {}_{\times}\langle n, 0|0, n\rangle_{\times} = 0, \text{ and} \\ {}_{\times}\langle n, 0|n, 0\rangle_{+} = {}_{\times}\langle 0, n|n, 0\rangle_{+} = \frac{1}{\sqrt{2^n}}, \end{gathered} \tag{2.8}$$

we can choose a basis on the span of these three vectors such that

$$
\begin{aligned}
{}_{\times}\langle n,0| &= \begin{bmatrix} 1 & 0 & 0 \end{bmatrix}, \\
{}_{\times}\langle 0,n| &= \begin{bmatrix} 0 & 1 & 0 \end{bmatrix}, \text{ and} \\
{}_{+}\langle n,0| &= \begin{bmatrix} \frac{1}{\sqrt{2^n}} & \frac{1}{\sqrt{2^n}} & \sqrt{1-\frac{1}{2^{n-1}}} \end{bmatrix}.
\end{aligned} \tag{2.9}
$$

In this basis, the POVM measure restricted to this subspace[3] looks like

$$
M_n^{(d\vee e)|(+,0)} = \begin{pmatrix} \frac{1}{2}\left(1-2^{-n}\right) & -2^{-1-n} & -\frac{\sqrt{1-2^{1-n}}}{2\sqrt{2}\sqrt{2^{-1+n}}} \\ -2^{-1-n} & \frac{1}{2}\left(1-2^{-n}\right) & -\frac{\sqrt{1-2^{1-n}}}{2\sqrt{2}\sqrt{2^{-1+n}}} \\ -\frac{\sqrt{1-2^{1-n}}}{2\sqrt{2}\sqrt{2^{-1+n}}} & -\frac{\sqrt{1-2^{1-n}}}{2\sqrt{2}\sqrt{2^{-1+n}}} & \frac{1}{2}\left(1+2^{1-n}\right) \end{pmatrix}. \tag{2.10}
$$

Using Mathematica, we find the smallest eigenvalue of this operator to be $\frac{1}{2} - 2^{-\frac{n+1}{2}}$. This argument would hold for all the other choices of (A, a), and therefore, this would also be the value of $\Pr^n_{\min}[d \vee e]$. Furthermore, we can see that $\Pr^2_{\min}[d \vee e] = \frac{1}{2} - \frac{1}{2\sqrt{2}}$, and that $\Pr^n_{\min}[d \vee e] \geq \Pr^2_{\min}[d \vee e]\ \forall n \geq 2$, and therefore

$$
\Pr^{\geq 2}_{\min}[d \vee e] = \frac{1}{2} - \frac{1}{2\sqrt{2}}. \tag{2.11}
$$

Thus, we see in this simple example that while the statistics of double-clicks alone is insufficient in providing an estimate on multiple-photon components, the combined statistics of double-clicks and errors does fit the purpose. As mentioned before, this estimation method is not really necessary for polarization-encoded BB84, as there exists a squashing model. But this example serves as a demonstration before we take up the more complex example of phase-encoded BB84 in the next section.

2.4 Estimation method for phase-encoded BB84

Phase-encoded BB84 (PEBB84) is a QKD protocol modelled after BB84 (discussed in the previous section), but using optical phase instead of polarization as the encoding degree of freedom. The detection setup used in PEBB84 has already been introduced in §1.5 and Appendix A, while studying squashing models on this setup. Recall that a squashing model was found for the practical range of values of the characteristic parameter η, but not throughout the range of values that can occur in principle. Here we present a method

[3]Since the POVM operator on the entire space is block-diagonal with respect to this rank-3 subspace and the orthogonal subspace, and since the restriction of the operator on the orthogonal subspace is just the identity on that subspace, it follows that the eigenspace of the smallest eigenvalue is contained in this rank-3 subspace.

to bound the multiple-photon component in the detection statistics, which may be used in cases where the existence of a squashing model is not proven.

Fig. 2.3 reproduces the model of the detection setup, presented already in §1.5. In this case, the type of events whose statistics we use in our estimation are those with clicks in both the second ("middle") time slot and one (or both) of the outer time slots, regardless of which detector clicks (possibly both). We refer to such events as "cross-clicks", abbreviated by c.

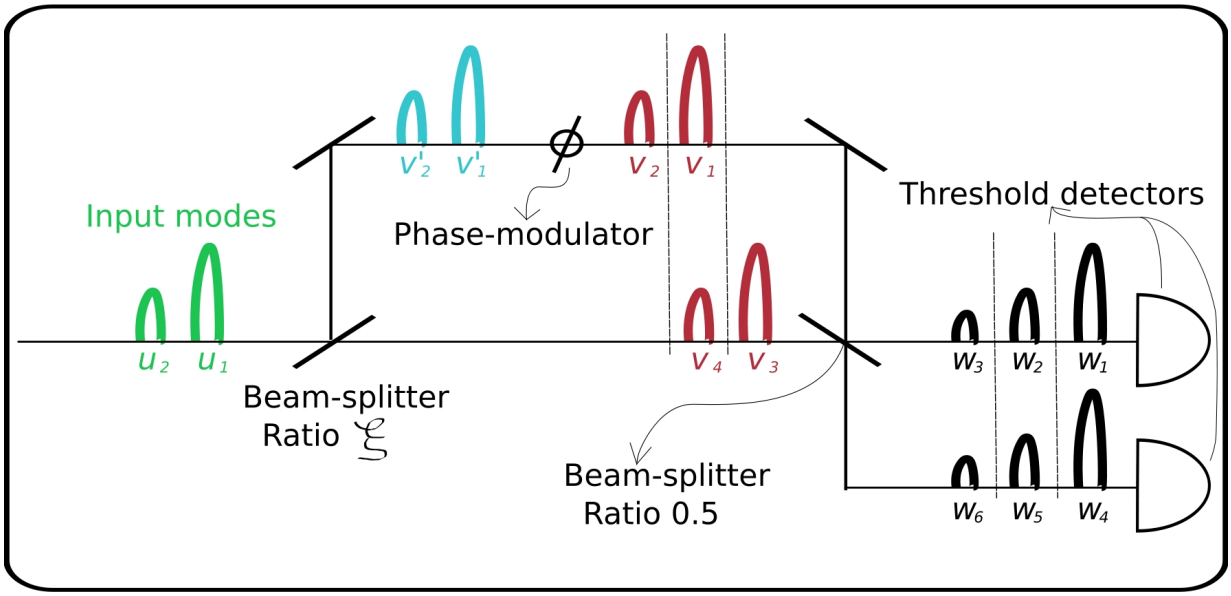


Figure 2.3: Linear-optic model of the PEBB84 detection device.

With regard to cross-click events, we make the following observations (Fig. 2.4 depicts each of these observations pictorially):

1. The statistics of click patterns would be unaffected by performing QND photon-counting measurements individually on the six w modes, because the POVM corresponding to resolving the click patterns commutes with the projectors onto photon-number subspaces on the modes, which are the Kraus operators realizing photon-number counting (we used similar reasoning in §1.5.3).

2. Following the same line of reasoning, if we could only resolve the time bins of clicks but not between the two threshold detectors, then the statistics of click patterns (which would now be just patterns on three bins instead of six) would be unaffected by photon-counting on the three time bins.

3. Counting photons on the three time bins at the w site is equivalent to performing individual photon-counting on v_3, the collective pair v_1 and v_4, and v_2. Therefore photon-counting on these three bins would not affect the statistics of time-bin click patterns.

4. Since each of the modes v_1 and v_4 affects only the middle time bin, individual photon-counting on these two would still leave the statistics unaffected. This means that individual photon-counting on each of the v modes would not affect the statistics of time-bin click patterns.

5. Since photon-counting on v_1 is equivalent to that on v_1', and photon-counting on v_2 is equivalent to that on v_2', the above reasoning can be carried over to v_1', v_2', v_3 and v_4.

6. Since the more resolved measurement of individual photon-counting on the four modes leaves the time-bin statistics unchanged, any less-resolved version of the measurement would also preserve the statistics. Specifically, collective photon-counting on v_1' and v_3, and another collectively on v_2' and v_4, would preserve the time-bin statistics.

7. But joint photon-counting on v_1' and v_3 has the same effect as photon-counting on u_1, and joint photon-counting on v_2' and v_4 has the same effect as photon-counting on u_2. Therefore, photon-counting on each of the u modes does not affect the time-bin click statistics.

8. This means that for any n-photon state[4] ρ_n for any n, $\Pr[c|\rho_n]$ would be unaffected after such a measurement.

9. The above reasoning shows that $\Pr[c|\rho_n]$ for any state ρ_n is just a convex combination of those for the occupancy eigenstates $|i, n-i\rangle\langle i, n-i|$ on the two input modes. This means that $\Pr^n_{\min}[c]$ for any given n would be simply the least of the $(n+1)$ quantities $\Pr[c||i, n-i\rangle\langle i, n-i|]$.

10. For a specific $|i, n-i\rangle$, an inside-only event can occur only if all i photons in the u_1 mode are reflected and all $(n-i)$ photons in u_2 are transmitted by the ξ beam-splitter. The probability of this is $\xi^{n-i}(1-\xi)^i$. Similarly, an outside-only event occurs with probability $\xi^i(1-\xi)^{n-i}$. Since all events other than inside-only and outside-only events are cross-clicks,

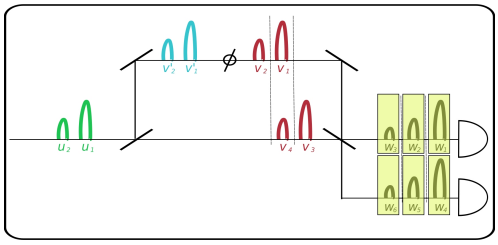
$$\Pr[c||i, n-i\rangle\langle i, n-i|] = 1 - \xi^{n-i}(1-\xi)^i - \xi^i(1-\xi)^{n-i}.$$

It is now straightforward to find the least of these quantities over the range of i, whereupon we get

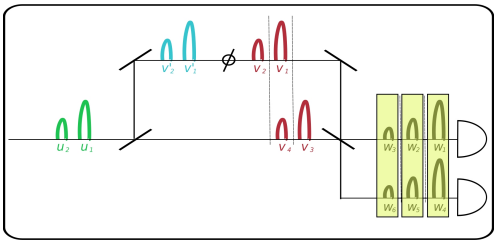
$$\Pr^n_{\min}[c] = 1 - \xi^n - (1-\xi)^n, \tag{2.12}$$

where $\xi = \frac{1}{1+\eta}$ is the ratio of the first beam-splitter in the Mach-Zehnder interferometer of our detector model.

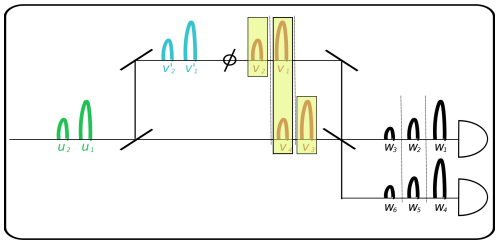
[4]Since collective counting on the two input modes is only a coarse-graining of individual counting, we can restrict consideration to input states with definite numbers of photons.



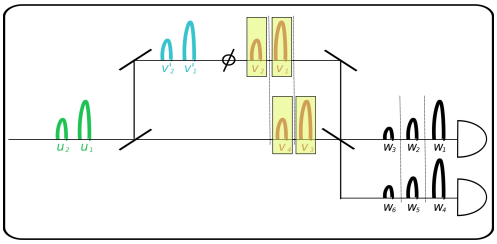
(a) Photon-counting on each of the w modes.



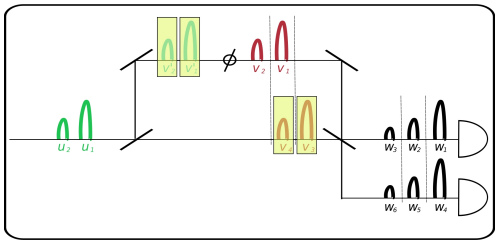
(b) Photon-counting on each of the w time bins.



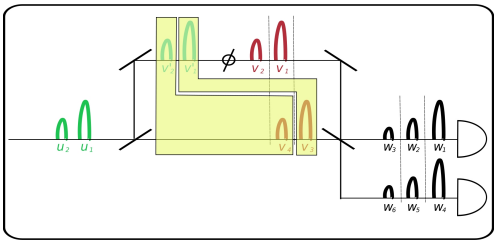
(c) Photon-counting on each of the v time bins.



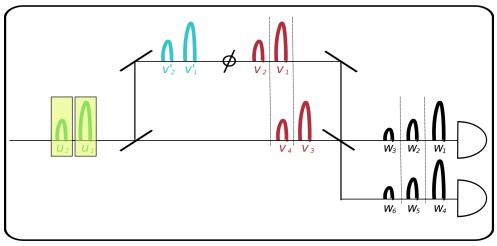
(d) Photon-counting on each of the v modes.



(e) Individual photon-counting on v_1', v_2', v_3 and v_4.



(f) Photon-counting on $v_1'+v_3$ collectively and $v_2'+v_4$ collectively.



(g) Photon-counting on each of the u modes.

Figure 2.4: Photon-counting argument for the calculation of $\Pr^n_{\min}[c]$.

Since $0.5 \leq \xi \leq 1$, the expression derived above has the property

$$\forall n \geq 2, \Pr^n_{\min}[c] \geq \Pr^2_{\min}[c], \tag{2.13}$$

and therefore, $\Pr^{\geq 2}_{\min}[c] = \Pr^2_{\min}[c] = 2\xi(1-\xi)$.

Thus, we have derived a method of estimating multiple-photon components entering the PEBB84 detection setup using the statistics of what we call cross-clicks.

2.5 Comparison of the estimation method with squashing

Having described the estimation method, we would now like to address the question of how this method performs in QKD compared to using a squashing model (where one exists). The figure of merit we use in judging performance is the rate of key that can be extracted in the QKD protocol. It might seem at first that it is always advantageous to use a squashing model if one is available. However, we shall see that this is not true: there are some cases where using the estimation method allows us to extract more key than using a squashing model.

We illustrate this by considering the simple example of the BB84 protocol. We further simplify the example by assuming that Alice uses a single-photon source, so that we do not have to get into the details of decoy states etc. (at any rate, the role of the squashing or estimation method is on Bob's side). The expression for the key-rate for BB84 can be derived in various ways, for example using the methods of [8] or [41]. Denote the total number of protocol rounds (after sifting) by N and the size of the raw key by kN. In the asymptotic limit ($N \to \infty$), we can ignore the loss of raw key in parameter-estimation. Now, say the error-rate in the entire data is e_k. Further, let $k_1 N$ be the size of the part of the data which comes from events where Bob's device received single photons, and e_1 the error-rate in this part of the data. Assuming that the error-correction (EC) is carried out at peak efficiency (i.e. the Shannon limit), the cost in key-size due to EC is $kNh[e_k]$, where $h[x] := -x \log_2 x - (1-x)\log_2(1-x)$ is the binary entropy function.

Moving on to the privacy-amplification (PA) step, the fractional shortening required to be done on the $k_1 N$-sized single-photon part is given by $h[e_1]$, whereas the rest of the raw key (the $(k-k_1)N$-sized part coming from events other than single-photon ones) must be completely discarded ("tagging"). Dividing the respective sizes by the number N of rounds, the final secure key-rate is

$$\begin{aligned} r[k_1, e_1] &= k\,(1 - h[e_k]) - k_1 h[e_1] - (k - k_1) \\ &= k_1\,(1 - h[e_1]) - k h[e_k]. \end{aligned} \tag{2.14}$$

We must now modify this formula for the situation where we don't know k_1 and e_1 exactly but can only give some constraints on them based on observed data[5], for example by limiting their ranges. If $\mathcal{K}$ is the set of all the pairs of values (k_1, e_1) compatible with

[5]Of course, we always know k and e_k exactly, since these are direct observables: k is the size of the entire data and e_k the rate of errors in it (which is exactly estimated by PE in the asymptotic limit).

observations, then the secure key-rate is given by the worst-case value

$$r_{\mathcal{K}} = \min_{(k_1,e_1)\in\mathcal{K}} r[k_1, e_1]. \tag{2.15}$$

The squashing model for BB84, found in [27], uses a post-processing scheme where a uniform random bit is assigned upon each double-click event. Consequently, this post-processing would add to the errors already present in the single-click events an amount which is half the number of double-clicks. Now, recalling the estimation method using double-clicks and errors (§2.3.2), we imagine two toy situations:

1. There are no double-clicks, and the error-rate in the data is e. The two methods, namely squashing and estimation, deal with this case as follows:

   (a) Squashing: The size of the data is N. Since there are no double-clicks, the post-processing would add no further errors. Since a squashing map exists, all the available data can be assumed to come from single-photon events. Therefore $k_1 = k = 1$, $e_1 = e$, and the key-rate is

   $$r_{\text{Sq}} = 1 - 2h[e].$$

   (b) Estimation: Since there are no double-clicks, the size of the data is N, and the bound from the estimation method is trivial: $k_1 = k = 1$. Consequently, $e_1 = e$, and the key-rate is the same as in the squashing case,

   $$r_{\text{Es}} = 1 - 2h[e].$$

2. As a fraction of N, the rate of double-clicks is f_D, while there are no errors in the single-click events. In this situation, the two methods perform as follows:

   (a) Squashing: The size of the data is N, since double-clicks are post-processed into key bits. The error-rate is $e_k = 0.5 f_D$, as discussed before. Since a squashing map exists, all the available data can be assumed to come from single-photon events. Therefore $k_1 = k = 1$, $e_1 = 0.5 f_D$, and the key-rate is

   $$r_{\text{Sq}} = 1 - 2h\left[\frac{f_D}{2}\right].$$

   (b) Estimation: Since double-clicks do not contribute to the raw key, the size of the data is $N(1 - f_D)$. There are no errors at all, and therefore $e_k = e_1 = 0$. The estimation method gives the bound

   $$k_1 \geq 1 - \frac{f_D}{\frac{1}{2} - \frac{1}{2\sqrt{2}}} =: k_0[f_D].$$

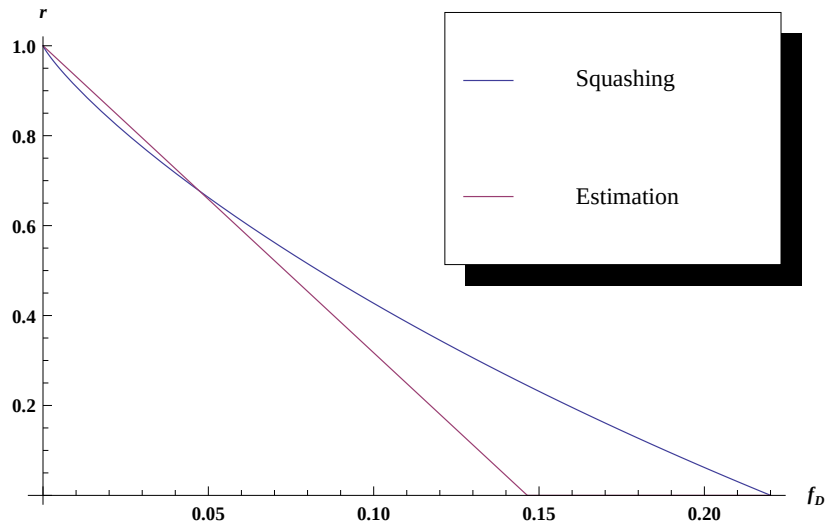


Figure 2.5: Comparison between the key-rates using squashing and estimation for BB84 with no single-click errors.

Therefore, the key-rate is

$$r_{\mathrm{Es}} = \min_{k_0[f_D] \le k_1 \le 1} k_1 = 1 - \frac{f_D}{\frac{1}{2} - \frac{1}{2\sqrt{2}}}.$$

Figure 2.5 shows a plot of the key-rate vs. the rate f_D of double-clicks for the two methods, in the second case, i.e. when there are no errors in the single-click events. We can see that there is a range of values of f_D for which the estimation method performs better. In the absence of double-clicks, both methods perform equally-well.

This simple example, though using contrived statistics, illustrates that the choice between the squashing and estimation methods must be made carefully, based on how they compare in the particular situation in consideration.

Chapter 3

Quantum key-distribution with imperfect devices

3.1 Introduction

The existing formalism of quantum key-distribution (QKD) works with the assumption of well-characterized preparation and measurement devices (sources and detectors). The actions of these devices used in QKD are assumed to be described precisely. But in practice, the devices do not behave as described by these precise models. Practical devices always deviate from the ideal descriptions. In the present work, we seek to build a mathematical formalism to treat imperfections in the functioning of sources and detectors and to incorporate the effects of such imperfections on the security and performance of QKD implementations. We have been able to build a limited formalism which can account for a restricted class of imperfections, which is modelled in terms of a distance measure between measurement operations. We hope that this is the first step towards more generally-applicable models. Previously, Gottesman *et al.* [30] have addressed the problem of QKD with imperfect devices, but in the limited case of the BB84 scheme [1] and certain specific types of imperfections. Mayers and Yao [29] have also addressed this issue, but again in the special case of BB84.

In developing our formalism, we use as the substrate the security-proof framework developed by Renato Renner in his doctoral thesis [12], and build on it. In §3.2 we review the formalism presented in Renner's thesis (we sometimes refer to the work using the phrase "the Thesis"). Then in §3.3 we present our refinements.

3.2 Renner security formalism

Let us here outline the Renner formalism. Here, we follow Renner's thesis, but avoiding the de Finetti argument for the generalization from collective to coherent attacks, we

employ Christandl, König and Renner's postselection technique [42]. First we describe the formalism in words, and thereafter present the essential mathematical steps.

3.2.1 Operational description

In this formalism, a QKD scheme (assumed to satisfy the criteria for invariance under permutations) consists of the following steps:

1. Quantum communication: In practice, usually Alice prepares quantum states and sends them to Bob, who makes measurements on whatever he receives. But in the mathematical treatment, we can consider a mathematically-equivalent picture which differs in its details from the actual implementation in two aspects, viz. 1) Eve prepares states for Alice and Bob and Alice's preparation is modelled by a measurement on her "state" (which is just fictional), and 2) Alice and Bob's measurements are made in later steps (parameter-estimation and blockwise information-processing). In the Renner formalism, the first step consists of states being shared by Alice, Bob and Eve, where in principle Eve can prepare any state she wants[1]. This state lives on a composite physical system consisting of many identical subsystems, each having sub-parts in Alice, Bob and Eve's possession.

2. Parameter-estimation: In this step, Alice and Bob perform some measurement on a fraction of the identical subsystems in order to estimate some statistical properties of the rest. Based on the statistics observed in this step, they deterministically either continue the QKD scheme or abort.

3. Blockwise information-processing: On the remaining subsystems, Alice and Bob perform blockwise local measurements, reducing them to classical strings on some alphabet.

4. Information-reconciliation: Some error-correcting code is used to reconcile Alice and Bob's classical strings.

5. Privacy-amplification: Based on the statistics observed in the parameter-estimation step, and on chosen performance parameters, Alice and Bob (mathematically) construct a set of density matrices compatible with their observations. They then calculate the minimum over that set of an entropic quantity related to security. Based on the value of this minimum, they choose a final key-length and use hashing to shorten their strings to that length.

[1]The fact that in reality Alice prepares the states can be used to impose a constraint on the set of states considered in the entropy calculations, viz. that Alice's marginal state is constrained to be a constant, independent of Eve's attack.

The postselection technique of [42] necessitates two modifications over and above the framework in Renner's thesis: 1) the performance parameters must be chosen polynomially tighter than the desired ones, and 2) the output of the hashing must be shortened polynomially more than the amount ordained by calculations along the lines of the Thesis. In other words, in order to incorporate the postselection technique, all we have to do is to follow the methods in Section 6.5.3 of Renner's thesis, except for choosing the $\bar{\epsilon}$ of inequality 6.7 to be zero, and choosing all the other epsilons tighter than our target by the polynomial factor computed in [42].

The exact form of these polynomial-sized parameters are not relevant in our present discussion. Also, while the Thesis works with a convex combination of "almost-iid" states, with the "almostness" parametrized by a certain r, the postselection technique allows us to work with $r = 0$, i.e. a convex combination of iid states. In the following, however, we stick to the older, de-Finetti method (Section 6.5.3 of the Thesis), which may be modified easily to fit into the postselection framework, as discussed above. The arguments pertaining to device imperfections, which are the subject of the present study, are not affected. We shall use a notation which can be modified quite easily to suit either case.

3.2.2 Mathematical details

As mentioned, we shall follow closely along the lines of Section 6.5.3 of Renner's thesis, sometimes changing the notation to suit our purpose. Before we start, we must state some definitions.

Definition 3.2.1. (Definition 4.1.1 of [12]) The symmetric subspace $\mathrm{Sym}[\mathcal{H}^{\otimes n}]$ of a Hilbert space $\mathcal{H}^{\otimes n}$ is defined as the subspace consisting of all those vectors which are invariant under arbitrary permutations of the n factor spaces $\mathcal{H}$:

$$\mathrm{Sym}\left[\mathcal{H}^{\otimes n}\right] := \{|\psi\rangle \in \mathcal{H}^{\otimes n} : \pi|\psi\rangle = |\psi\rangle \forall \pi \in \mathcal{S}_n\}, \tag{3.1}$$

where the permutations act as unitary transformations in a natural way.

Definition 3.2.2. (Definition 4.1.4 of [12]) Definition of the symmetric subspace along a product state: First, for any $|\theta\rangle \in \mathcal{H}$ we define the subset (which is not a vector space)

$$\mathcal{V}\left[\mathcal{H}^{\otimes n}, |\theta\rangle^{\otimes m}\right] := \{\pi(|\theta\rangle^{\otimes m} \otimes |\psi\rangle) : \pi \in \mathcal{S}_n, |\psi\rangle \in \mathcal{H}^{\otimes(n-m)}\}. \tag{3.2}$$

Then, for any $|\theta\rangle \in \mathcal{H}$, the symmetric subspace of $\mathcal{H}^{\otimes n}$ along $|\theta\rangle^{\otimes m}$ is defined as

$$\mathrm{Sym}\left[\mathcal{H}^{\otimes n}, |\theta\rangle^{\otimes m}\right] := \mathrm{Sym}\left[\mathcal{H}^{\otimes n}\right] \cap \mathrm{span}\mathcal{V}\left[\mathcal{H}^{\otimes n}, |\theta\rangle^{\otimes m}\right]. \tag{3.3}$$

Let us suppose that at the end of the quantum communication step (and possibly after performing random permutations on their subsystems and discarding some, depending on what method is used to generalize to security against coherent attacks), Alice, Bob and

Eve share a state $\rho_{(ABE)^{bn+m}}$ on $(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E)^{\otimes(bn+m)}$, where b, n and m are integers. Since the best Eve can do is to possess purifications of Alice and Bob's states, it suffices to consider $\mathcal{H}_E \cong \mathcal{H}_A \otimes \mathcal{H}_B$. First we write, in our modified notation, inequality 6.7 of the Thesis, which states that $\rho_{(ABE)^{bn+m}}$ is close to a convex combination of almost-iid states:

$$\left\| \rho_{(ABE)^{bn+m}} - \int_{\mathcal{S}_1} \rho^{|\theta\rangle}_{(ABE)^{bn+m}} \nu[|\theta\rangle] \right\|_1 \leq \epsilon_0. \tag{3.4}$$

Here we denote by ϵ_0 any trace distance remaining at this stage of the protocol, which might be the one stemming from the de Finetti theorem, or zero if the postselection method is used, or any other value that might appear as per the details of the protocol. Likewise, $\rho^{|\theta\rangle}_{(ABE)^{bn+m}}$ might be iid or almost-iid, depending on those details. "Almost-iid" means the following:

$$\rho^{|\theta\rangle}_{(ABE)^{bn+m}} \in \mathcal{S}\left[\mathrm{Sym}\left[(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E)^{\otimes(bn+m)}, |\theta\rangle^{\otimes(bn+m-r)}\right]\right] \tag{3.5}$$

for some small $r \leq bn + m$.

As in the Thesis, the integral runs over the set $\mathcal{S}_1$ of all normalized vectors $|\theta\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$. So far, both the terms appearing in the trace distance expression are normalized density matrices (ν is a normalized measure over $\mathcal{S}_1$). However, the next step, parameter-estimation (PE), involves post-selection. This step is described by a CP trace-nonincreasing linear map[2]

$$\mathcal{E}^{\mathcal{M}_0}_{\mathsf{PE}} : \mathcal{S}\left[(\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes m}\right] \to [0, 1] \tag{3.6}$$

acting on m of the $(bn + m)$ subsystems in Alice and Bob's possession, nothing done on the rest of their subsystems or on any of Eve's.

The action of $\mathcal{E}^{\mathcal{M}_0}_{\mathsf{PE}}$ is to map a density matrix to either 0 or 1 depending on whether the state described by the matrix gets rejected or accepted by the PE routine. In other words, it maps a density matrix to the probability of its state getting accepted. The operation of this step is as follows: a POVM $\mathcal{M}_0$ is performed on each of Alice and Bob's m test subsystems. If the distribution of the observed outcomes, Q, is contained in a certain set $\mathcal{Q}$ of distributions, the state is accepted and the protocol continues. If not, the state is

[2] We denote by $\mathcal{P}[\mathcal{H}]$ the set of all positive-semidefinite linear operators on a Hilbert space $\mathcal{H}$, and by $\mathcal{S}[\mathcal{H}]$ the set of all *normalized states*, i.e. positive-semidefinite linear operators of unit trace, on $\mathcal{H}$. Where we describe a linear map as taking elements in the $\mathcal{S}$ of one space to those in the $\mathcal{S}$ of another, we don't mean that the action of the map is not defined on other positive operators (or, indeed, other Hermitian operators; for of course, the action of the map is defined, by its linearity, on all Hermitian operators), but only that it is trace-preserving. Likewise, the action of a map taking elements in the $\mathcal{P}$ of one space to those in the $\mathcal{P}$ of another is defined by linearity on other Hermitian operators, but is so described to emphasize its being a positive map.

rejected and the protocol is aborted. Defining, as in the Thesis,

$$\rho^{\mathcal{M}_0}_{(ABE)^{bn}E^m} := \left(\mathsf{id}_{(ABE)^{bn}} \otimes \mathcal{E}^{\mathcal{M}_0}_{\mathsf{PE}} \otimes \mathsf{id}_{E^m}\right)\left[\rho_{(ABE)^{bn+m}}\right],$$
$$\rho^{\mathcal{M}_0}_{(ABE)^{bn}} := \mathsf{Tr}_{E^m}\left[\rho^{\mathcal{M}_0}_{(ABE)^{bn}E^m}\right]$$

and

$$\rho^{|\theta\rangle,\mathcal{M}_0}_{(ABE)^{bn}E^m} := \left(\mathsf{id}_{(ABE)^{bn}} \otimes \mathcal{E}^{\mathcal{M}_0}_{\mathsf{PE}} \otimes \mathsf{id}_{E^m}\right)\left[\rho^{|\theta\rangle}_{(ABE)^{bn+m}}\right],$$
$$\rho^{|\theta\rangle,\mathcal{M}_0}_{(ABE)^{bn}} := \mathsf{Tr}_{E^m}\left[\rho^{|\theta\rangle,\mathcal{M}_0}_{(ABE)^{bn}E^m}\right],$$

we have, by virtue of the trace-nonincreasing property of the map, the analog of inequality 6.10 of the Thesis,

$$\left\|\rho^{\mathcal{M}_0}_{(ABE)^{bn}} - \int_{\mathcal{S}_1} \rho^{|\theta\rangle,\mathcal{M}_0}_{(ABE)^{bn}} \nu[|\theta\rangle]\right\|_1 \leq \epsilon_0. \tag{3.7}$$

In view of the overall operational role of the PE sub-protocol, which is (apart from the primary role of aborting insecure runs) to simplify the key-rate calculation by narrowing down the set over which it is to be performed, it is useful to deviate slightly from the path taken in the Thesis. Specifically, in the formalism presented in the Thesis, all the analysis involves considering the whole set $\mathcal{Q}$ of distributions accepted by the PE. This would be necessary only if the PE were a blackbox which only informed Alice and Bob of the acceptance or rejection, without revealing to them which of the distributions in $\mathcal{Q}$ occurred during an accepted round. But this is an unnecessary assumption, since PE involves public announcements anyway, so that Alice and Bob might as well make use of their knowledge of the distribution.

In essence, provided that the particular distribution of outcomes that is observed, Q, is contained in $\mathcal{Q}$, we can proceed with the protocol, considering only Q for the subsequent analysis. Specifically, this means that instead of constructing the $\mathcal{V}$ set based on the probability of the finite statistics to only be contained in $\mathcal{Q}$, we can construct it based on the probability of the statistics to be, in addition to being contained in $\mathcal{Q}$, even coincident with the particular distribution observed, viz. Q.

This *a posteriori* knowledge means that instead of $\mathcal{E}^{\mathcal{M}_0}_{\mathsf{PE}}$, whose output is *the probability that the statistical distribution of the outcomes of* $\mathcal{M}_0^{\otimes m}$ *on the input state is contained in* $\mathcal{Q}$, we can describe the action of the PE operation by a Q-specific map $\mathcal{E}^{\mathcal{M}_0,Q}_{\mathsf{PE}}$, whose output is *the probability that the statistical distribution of the outcomes of* $\mathcal{M}_0^{\otimes m}$ *on the input state is coincident with* Q. Note that operationally, the PE is described correctly by the a-priori $\mathcal{E}^{\mathcal{M}_0}_{\mathsf{PE}}$. This narrowing down to $\mathcal{E}^{\mathcal{M}_0,Q}_{\mathsf{PE}}$ is possible only after the observations are made.

Before proceeding, it would be convenient to make some definitions, fix some notation and state an important lemma:

Definition 3.2.3. For a POVM $\mathcal{M} \coloneqq (M^i)_{i=1}^k$ with $M^i \in \mathcal{P}[\mathcal{H}] \quad \forall i$ and $\sum_{i=1}^{k} M^i = \mathbb{1}_{\mathcal{H}}$, a positive integer m, and a density matrix $\rho_m \in \mathcal{S}[\mathcal{H}^{\otimes m}]$, define

$$\lambda_m^{\mathcal{M}}[\rho_m]$$

to be the random (k-variate) variable corresponding to the (k-point) distribution of the (k-valued) outcomes obtained upon applying the measurement $\mathcal{M}^{\otimes m}$ to ρ_m. Also, for convenience, define for any density matrix $\rho \in \mathcal{S}[\mathcal{H}]$

$$\lambda_\infty^{\mathcal{M}}[\rho] \coloneqq \left(\mathsf{Tr}\left[M^i\rho\right]\right)_{i=1}^k. \tag{3.8}$$

Definition 3.2.4. For a POVM $\mathcal{M} \coloneqq (M^i)_{i=1}^k$, a k-point distribution Q and a real number $\mu > 0$, define

$$\mathcal{V}_{\mathcal{M}}^{Q,\leq\mu} \coloneqq \{|\theta\rangle \in \mathcal{S}_1[\mathcal{H} \otimes \mathcal{H}_E] : \left\|\lambda_\infty^{\mathcal{M}}[\mathsf{Tr}_E|\theta\rangle\langle\theta|] - Q\right\|_1 \leq \mu\}, \tag{3.9}$$

where $\mathcal{H}_E$ is an extension (isomorphic to $\mathcal{H}$) which contains purifications of states on $\mathcal{H}$, and $\mathcal{S}_1[\mathcal{H} \otimes \mathcal{H}_E]$ denotes the unit sphere on the product space.

We now restate Lemma 6.2.2 of the Thesis without proof:

Lemma 3.2.5. *For a POVM $\mathcal{M} \coloneqq (M^i)_{i=1}^k$, a k-point distribution Q, positive integers m and $r \leq \frac{m}{2}$, and a real number $\epsilon > 0$, if*

$$\mu \coloneqq 2\sqrt{\frac{\log[1/\epsilon]}{m} + h\left[\frac{r}{m}\right] + \frac{k}{m}\log\left[\frac{m}{2}+1\right]},$$

where h denotes the binary entropy function, then for any state

$$\rho_m \in \mathcal{S}\left[\mathrm{Sym}\left[(\mathcal{H}\otimes\mathcal{H}_E)^{\otimes m}, |\theta\rangle^{\otimes(m-r)}\right]\right]$$

with $|\theta\rangle \notin \mathcal{V}_{\mathcal{M}}^{Q,\leq\mu}$,

$$\mathsf{Pr}\left[\lambda_m^{\mathcal{M}}[\mathsf{Tr}_{E^m}\rho_m] = Q\right] \leq \epsilon. \tag{3.10}$$

Having stated these definitions and Lemma, let us come back to the QKD protocol. Picking up where we left at Inequality (3.7), we first write the *a posteriori*, Q-specific version of the inequality:

$$\left\|\rho_{(ABE)^{bn}}^{\mathcal{M}_0,Q} - \int_{\mathcal{S}_1} \rho_{(ABE)^{bn}}^{|\theta\rangle,\mathcal{M}_0,Q}\nu[|\theta\rangle]\right\|_1 \leq \epsilon_0, \tag{3.11}$$

where the Q-specific density matrices are defined in the natural way.

Next, we introduce a choosable security parameter ϵ_{PE} characterizing the PE operation. Further, if

$$\mu_{\mathsf{PE}} \coloneqq 2\sqrt{\frac{\log[1/\epsilon_{\mathsf{PE}}]}{m} + h\left[\frac{r}{m}\right] + \frac{k}{m}\log\left[\frac{m}{2}+1\right]}, \tag{3.12}$$

with the appropriate r (for example, zero if using the postselection technique), chosen such that Equation 3.5 holds.

Lemma 3.2.5 above assures us that $\forall |\theta\rangle \in \left(\mathcal{S}_1 \setminus \mathcal{V}_{\mathcal{M}_0}^{Q,\leq \mu_{\mathsf{PE}}}\right)$,

$$\begin{aligned}\left\| \rho^{|\theta\rangle,\mathcal{M}_0,Q}_{(ABE)^{bn}E^m} \right\|_1 \equiv \left\| \left(\mathsf{id}_{(ABE)^{bn}} \otimes \mathcal{E}_{\mathsf{PE}}^{\mathcal{M}_0,Q} \otimes \mathsf{id}_{E^m}\right)\left[\rho^{|\theta\rangle}_{(ABE)^{bn+m}}\right] \right\|_1 \leq \epsilon_{\mathsf{PE}} \\ \Rightarrow \left\| \rho^{|\theta\rangle,\mathcal{M}_0,Q}_{(ABE)^{bn}} \right\|_1 \leq \epsilon_{\mathsf{PE}},\end{aligned} \tag{3.13}$$

where we have used the fact that tracing over a subsystem cannot increase the trace norm. Furthermore,

$$\begin{aligned}&\left\| \rho^{\mathcal{M}_0,Q}_{(ABE)^{bn}} - \int_{\mathcal{V}_{\mathcal{M}_0}^{Q,\leq \mu_{\mathsf{PE}}}} \rho^{|\theta\rangle,\mathcal{M}_0,Q}_{(ABE)^{bn}} \nu[|\theta\rangle] \right\|_1 \\ &\qquad = \left\| \rho^{\mathcal{M}_0,Q}_{(ABE)^{bn}} - \int_{\mathcal{S}_1} \rho^{|\theta\rangle,\mathcal{M}_0,Q}_{(ABE)^{bn}} \nu[|\theta\rangle] + \int_{\mathcal{S}_1 \setminus \mathcal{V}_{\mathcal{M}_0}^{Q,\leq \mu_{\mathsf{PE}}}} \rho^{|\theta\rangle,\mathcal{M}_0,Q}_{(ABE)^{bn}} \nu[|\theta\rangle] \right\|_1 \\ &\qquad \leq \left\| \rho^{\mathcal{M}_0,Q}_{(ABE)^{bn}} - \int_{\mathcal{S}_1} \rho^{|\theta\rangle,\mathcal{M}_0,Q}_{(ABE)^{bn}} \nu[|\theta\rangle] \right\|_1 + \left\| \int_{\mathcal{S}_1 \setminus \mathcal{V}_{\mathcal{M}_0}^{Q,\leq \mu_{\mathsf{PE}}}} \rho^{|\theta\rangle,\mathcal{M}_0,Q}_{(ABE)^{bn}} \nu[|\theta\rangle] \right\|_1 \\ &\qquad \leq \epsilon_0 + \left\| \int_{\mathcal{S}_1 \setminus \mathcal{V}_{\mathcal{M}_0}^{Q,\leq \mu_{\mathsf{PE}}}} \rho^{|\theta\rangle,\mathcal{M}_0,Q}_{(ABE)^{bn}} \nu[|\theta\rangle] \right\|_1 \\ &\qquad \leq \epsilon_0 + \int_{\mathcal{S}_1 \setminus \mathcal{V}_{\mathcal{M}_0}^{Q,\leq \mu_{\mathsf{PE}}}} \left\| \rho^{|\theta\rangle,\mathcal{M}_0,Q}_{(ABE)^{bn}} \right\|_1 \nu[|\theta\rangle] \\ &\qquad \leq \epsilon_0 + \epsilon_{\mathsf{PE}} \int_{\mathcal{S}_1 \setminus \mathcal{V}_{\mathcal{M}_0}^{Q,\leq \mu_{\mathsf{PE}}}} \nu[|\theta\rangle] \\ &\qquad \leq \epsilon_0 + \epsilon_{\mathsf{PE}} \int_{\mathcal{S}_1} \nu[|\theta\rangle] \\ &\qquad = \epsilon_0 + \epsilon_{\mathsf{PE}}.\end{aligned} \tag{3.14}$$

The first and third inequalities above follow from the triangle inequality for the trace distance, while the second and fourth follow from (3.11) and (3.13), respectively. The last two lines are by definition of the measure $\nu[|\theta\rangle]$ normalized on $\mathcal{S}_1$.

The next step is blockwise measurements and information-processing (BI) by Alice and Bob to reduce the systems in their possession to classical strings. This is modelled by a CPTP map $\mathcal{E}_{\mathsf{BI}}^{\mathcal{J}_0,\mathcal{K}_0}$ acting on each of Alice and Bob's n blocks of size b and taking it to one classical symbol each with Alice and Bob. Mathematically, the action of this map can be described as

$$\begin{aligned}\mathcal{E}_{\mathsf{BI}}^{\mathcal{J}_0,\mathcal{K}_0} &: \mathcal{S}\left[(\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes b}\right] \to \mathcal{S}\left[\mathcal{H}_X \otimes \mathcal{H}_Y\right] \\ \mathcal{E}_{\mathsf{BI}}^{\mathcal{J}_0,\mathcal{K}_0}[\sigma] &:= \sum_{x \in \mathcal{X}, y \in \mathcal{Y}} \mathsf{Tr}\left[\left(J_0^x \otimes K_0^y\right)\sigma\right] |x\rangle\langle x| \otimes |y\rangle\langle y|,\end{aligned} \tag{3.15}$$

where $\mathcal{J}_0 \coloneqq (J_0^x)_{x\in\mathcal{X}}$ and $\mathcal{K}_0 \coloneqq (K_0^y)_{y\in\mathcal{Y}}$ are complete POVMs on $\mathcal{P}\left[\mathcal{H}_A^{\otimes b}\right]$ and $\mathcal{P}\left[\mathcal{H}_B^{\otimes b}\right]$, respectively, and $\{|x\rangle : x \in \mathcal{X}\}$ and $\{|y\rangle : y \in \mathcal{Y}\}$ are orthonormal bases spanning $\mathcal{H}_X$ and $\mathcal{H}_Y$, respectively. Here $\mathcal{X}$ and $\mathcal{Y}$ are Alice and Bob's alphabets, respectively, which are in most QKD schemes identical.

Now defining

$$\begin{aligned}\rho_{X^nY^nE^{bn+m}}^{\mathcal{M}_0,Q,\mathcal{J}_0,\mathcal{K}_0} &\coloneqq \left(\left(\mathcal{E}_{\mathsf{BI}}^{\mathcal{J}_0,\mathcal{K}_0}\right)^{\otimes n}\otimes \mathsf{id}_{E^{bn+m}}\right)\left[\rho_{A^{bn}B^{bn}E^{bn+m}}^{\mathcal{M}_0,Q}\right],\\ \rho_{X^nY^nE^{bn}}^{\mathcal{M}_0,Q,\mathcal{J}_0,\mathcal{K}_0} &\coloneqq \mathsf{Tr}_{E^m}\left[\rho_{X^nY^nE^{bn+m}}^{\mathcal{M}_0,Q,\mathcal{J}_0,\mathcal{K}_0}\right]\end{aligned}$$

and

$$\begin{aligned}\rho_{X^nY^nE^{bn+m}}^{|\theta\rangle,\mathcal{M}_0,Q,\mathcal{J}_0,\mathcal{K}_0} &\coloneqq \left(\left(\mathcal{E}_{\mathsf{BI}}^{\mathcal{J}_0,\mathcal{K}_0}\right)^{\otimes n}\otimes \mathsf{id}_{E^{bn+m}}\right)\left[\rho_{A^{bn}B^{bn}E^{bn+m}}^{|\theta\rangle,\mathcal{M}_0,Q}\right],\\ \rho_{X^nY^nE^{bn}}^{|\theta\rangle,\mathcal{M}_0,Q,\mathcal{J}_0,\mathcal{K}_0} &\coloneqq \mathsf{Tr}_{E^m}\left[\rho_{X^nY^nE^{bn+m}}^{|\theta\rangle,\mathcal{M}_0,Q,\mathcal{J}_0,\mathcal{K}_0}\right],\end{aligned}$$

we infer from Inequality (3.14) and the monotonicity of the trace distance under CPTP maps that

$$\left\|\rho_{X^nY^nE^{bn}}^{\mathcal{M}_0,Q,\mathcal{J}_0,\mathcal{K}_0} - \int_{\mathcal{V}_{\mathcal{M}_0}^{Q,\leq\mu_{\mathsf{PE}}}} \rho_{X^nY^nE^{bn}}^{|\theta\rangle,\mathcal{M}_0,Q,\mathcal{J}_0,\mathcal{K}_0}\nu\left[|\theta\rangle\right]\right\|_1 \leq \epsilon_0 + \epsilon_{\mathsf{PE}}. \tag{3.16}$$

After this, if an ϵ_{IR}-secure information-reconciliation scheme with a leakage of $\mathrm{leak}_{\mathsf{IR}}$ bits is used, and then 2-universal hashing is used to shorten the key to a length ℓ satisfying

$$\begin{aligned}\ell \leq H_{\min}^{\epsilon_{\mathsf{PA}}+\epsilon_0+\epsilon_{\mathsf{PE}}}\left[\rho_{X^nE^{bn}}^{\mathcal{M}_0,Q,\mathcal{J}_0,\mathcal{K}_0}|E^{bn}\right] - \mathrm{leak}_{\mathsf{IR}} - 2\log\left[\frac{1}{\epsilon_{\mathsf{PA}}+\epsilon_0+\epsilon_{\mathsf{PE}}}\right]\\ - (m+k_0)\log\left[\dim\mathcal{H}_A\otimes\mathcal{H}_B\right] - \ell_0,\end{aligned} \tag{3.17}$$

then the resulting key is $\eta\left(\epsilon_{\mathsf{IR}} + \frac{3}{2}(\epsilon_{\mathsf{PA}}+\epsilon_0+\epsilon_{\mathsf{PE}})\right)$-secure. Here ϵ_{PA} is a choosable "smoothness" parameter, ℓ_0 and η are polynomial-sized corrections necessary if using the postselection technique of [42], and k_0 is the number of subsystems discarded before retaining the $bn+m$ with which we started our calculations. These do not affect the reasoning pertaining to device imperfections; what is important is the following lower bound on the entropy term appearing in the key-length expression, which follows from Inequality (3.16), combined with the definition and convexity of the conditional smooth min-entropy:

$$H_{\min}^{\epsilon_{\mathsf{PA}}+\epsilon_0+\epsilon_{\mathsf{PE}}}\left[\rho_{X^nE^{bn}}^{\mathcal{M}_0,Q,\mathcal{J}_0,\mathcal{K}_0}|E^{bn}\right] \geq \min_{|\theta\rangle\in\mathcal{V}_{\mathcal{M}_0}^{Q,\leq\mu_{\mathsf{PE}}}} H_{\min}^{\epsilon_{\mathsf{PA}}}\left[\rho_{X^nY^nE^{bn}}^{|\theta\rangle,\mathcal{M}_0,Q,\mathcal{J}_0,\mathcal{K}_0}|E^{bn}\right]. \tag{3.18}$$

This bound, in turn, is usually convenient to calculate, for example by approximating it using the von Neumann entropy of states on smaller spaces, as in the Thesis. While it appears to depend on the nature of $\mathcal{M}_0$, this is not really so, since the state parametrized by θ is almost-iid and depends only on θ and the BI map. The only influence of $\mathcal{M}_0$ on the minimum is in determining the set over which it is evaluated. In the remainder,

when we attempt to incorporate the effects of device imperfections, we shall not concern ourselves with how this bound is calculated, but rather take for granted that a method for its computation is known for the ideal measurements $(\mathcal{J}_0, \mathcal{K}_0)$, and only aim to reduce the corresponding calculations in the imperfect case to quantities in terms of such "assumed known" quantities.

3.3 QKD with imperfect devices

In this section we describe our first heuristic method for incorporating device imperfections in the Renner QKD framework. In §3.3.1 we discuss some distance measures which form the basis of our model for imperfections, and then in §3.3.2 we discuss how device imperfections within such a model can be accounted for in the QKD formalism.

3.3.1 Distance measures and the imperfection model

Since both preparation and measurement devices are modelled in our formalism by measurements, device imperfections can be modelled by measurement imperfections. Therefore, in order to model these imperfections, we first study distance measures between measurements. Let $\mathcal{M}_1 := (M_1^i)_{i=1}^k$ and $\mathcal{M}_2 := (M_2^i)_{i=1}^k$ be two complete POVMs on a Hilbert space $\mathcal{H}$, such that for either $j \in \{1,2\}$, $M_j^i \in \mathcal{P}[\mathcal{H}] \quad \forall i$ and $\sum_{i=1}^k M_j^i = \mathbb{1}_{\mathcal{H}}$.

We denote by $\mathcal{E}^{\mathcal{M}_j}$ the action of the POVM $\mathcal{M}_j$ as a CPTP map:

$$\mathcal{E}^{\mathcal{M}_j}[\sigma] := \sum_{i=1}^{k} \mathsf{Tr}\left[M_j^i \sigma\right] |i\rangle\langle i|, \tag{3.19}$$

where $\sigma \in \mathcal{S}[\mathcal{H}]$, and $|i\rangle \in \mathcal{H}_{\mathcal{I}}$ is a state on a classical register storing the measurement outcome.

Towards the objective of a meaningful model for device imperfections, we make the following observations:

1. Let $\mathcal{H}_E$ be an extension Hilbert space (it is sufficient to consider one congruent to $\mathcal{H}$, but we need not assume anything here). Then for any $\rho \in \mathcal{B}[\mathcal{H} \otimes \mathcal{H}_E]$, i.e.

$\rho \in \mathcal{P}\left[\mathcal{H} \otimes \mathcal{H}_E\right]$ with $\mathsf{Tr}[\rho] \leq 1$,

$$\begin{aligned}
\left\|\left(\left(\mathcal{E}^{\mathcal{M}_1} - \mathcal{E}^{\mathcal{M}_2}\right) \otimes \mathsf{id}_E\right)[\rho]\right\|_1 &= \left\|\sum_{i=1}^{k} |i\rangle\langle i| \otimes \left(\left(\mathsf{Tr} \otimes \mathsf{id}_E\right)\left[\left(\left(M_1^i - M_2^i\right) \otimes \mathbb{1}_E\right)\rho\right]\right)\right\|_1 \\
&= \sum_{i=1}^{k} \left\|\left(\mathsf{Tr} \otimes \mathsf{id}_E\right)\left[\left(\left(M_1^i - M_2^i\right) \otimes \mathbb{1}_E\right)\rho\right]\right\|_1 \\
&\leq \sum_{i=1}^{k} \left\|\left(\left(M_1^i - M_2^i\right) \otimes \mathbb{1}_E\right)\rho\right\|_1 \\
&\leq \sum_{i=1}^{k} \left\|M_1^i - M_2^i\right\|_\infty . \qquad (3.20)
\end{aligned}$$

Here the first equality follows by definition, and the other from the block-diagonal structure. The first inequality is a consequence of the monotonicity of the trace norm under partial-trace operations, while the other owes to the sub-normalization of ρ.

2. Since the bound in (3.20) is independent of ρ (and indeed of $\mathcal{H}_E$), it follows from the definition of the diamond norm,

$$\left\|\mathcal{E}\right\|_\diamond := \sup_{\mathcal{H}_E} \max_{\rho \in \mathcal{B}[\mathcal{H} \otimes \mathcal{H}_E]} \left\|\left(\mathcal{E} \otimes \mathsf{id}_E\right)[\rho]\right\|_1 , \qquad (3.21)$$

that

$$\left\|\mathcal{E}^{\mathcal{M}_1} - \mathcal{E}^{\mathcal{M}_2}\right\|_\diamond \leq \sum_{i=1}^{k} \left\|M_1^i - M_2^i\right\|_\infty . \qquad (3.22)$$

This means that in place of the diamond norm we may use the above bound in terms of the POVM elements, which (plausibly) might lead eventually to an imperfection model that is practically suited to calibrate a device against. We may go so far as to define a new distance measure between measurements:

Definition 3.3.1. $\left\|\mathcal{M}_1 - \mathcal{M}_2\right\|_{\mathsf{M}} := \sum_{i=1}^{k} \left\|M_1^i - M_2^i\right\|_\infty$.

That this is a valid distance measure on the set of all POVMs on $\mathcal{H}$ with k outcomes or fewer (*provided we establish a correspondence between the outcomes of different POVMs*), follows from the fact that the uniform norm induces a valid distance measure on $\mathcal{P}[\mathcal{H}]$.

3. For any $\rho \in \mathcal{S}[\mathcal{H}]$,

$$\left\|\left(\mathcal{E}^{\mathcal{M}_1} - \mathcal{E}^{\mathcal{M}_2}\right)[\rho]\right\|_1 = \left\|\left(\lambda_\infty^{\mathcal{M}_1} - \lambda_\infty^{\mathcal{M}_2}\right)[\rho]\right\|_1 , \qquad (3.23)$$

holds, where the right-hand side is the trace distance between the probability distributions induced on ρ by the two measurements. From (3.22) and the definition of the diamond norm, it follows that

$$\left\|\left(\lambda_\infty^{\mathcal{M}_1} - \lambda_\infty^{\mathcal{M}_2}\right)[\rho]\right\|_1 \leq \left\|\mathcal{M}_1 - \mathcal{M}_2\right\|_{\mathsf{M}} . \qquad (3.24)$$

This concludes the discussion of distance measures, wherein we have defined a measure, of distance between POVMs, which might prove useful in designing a practically-applicable model for device imperfections. With this anticipation, we use this M-distance measure for our imperfection model, although the model would work just as well with the diamond distance. Next we discuss how to modify the QKD framework discussed in §3.2 to account for device imperfections under this M-distance model.

3.3.2 QKD formalism with imperfect devices

We begin by noting that in the QKD formalism reviewed in §3.2, there are exactly two steps on which device imperfections can have an influence[3]: the parameter-estimation (PE) step, and the blockwise information-processing (BI) step, for it is these steps that contain preparations (modelled by measurements) and measurements. Specifically, we assume that our knowledge of device imperfections consists of the following promises:

1. Say the device used to carry out the measurement in the PE step behaves imprecisely in such a way as to perform a POVM $\mathcal{M}^{\otimes m}$ instead of the desired $\mathcal{M}_0^{\otimes m}$ on the m test systems. Then we are promised that there is a small $\epsilon_{\mathsf{MP}} \geq 0$ such that[4]

$$\|\mathcal{M} - \mathcal{M}_0\|_{\mathsf{M}} \leq \epsilon_{\mathsf{MP}}. \tag{3.25}$$

   Note that we model the imperfect measurement as being identical on all m subsystems because Lemma 3.2.5 relies on such a structure of the measurement. However, this does not mean that in reality the device has to behave identically on every subsystem: it suffices if its departure from the ideal on each subsystem is bounded by ϵ_{MP}. As long as we are ignorant of the exact nature of the departure (except for the promise that it is bounded by ϵ_{MP}), the effective measurement *is* in fact identical on every subsystem.

2. If the devices used in Alice's preparations and Bob's key-forming measurements, i.e. in the BI step, behave such as to execute a map $\bigotimes_{i=1}^{n} \mathcal{E}_{\mathsf{BI}}^{\mathcal{J}_i,\mathcal{K}_i}$ instead of the desired $\left(\mathcal{E}_{\mathsf{BI}}^{\mathcal{J}_0,\mathcal{K}_0}\right)^{\otimes n}$, then we are promised that there is a small $\epsilon_{\mathsf{MI}} > 0$ such that

$$\forall i, \quad \|\mathcal{J}_i - \mathcal{J}_0\|_{\mathsf{M}} + \|\mathcal{K}_i - \mathcal{K}_0\|_{\mathsf{M}} \leq \epsilon_{\mathsf{MI}}. \tag{3.26}$$

   Here we can work without the assumption of the imperfections being identical over different uses of the same device, which we made in the case of PE[5].

[3]Imperfections in the communication channel are not to be worried about by cryptographers, as the channel is assumed to be controlled by the adversary anyway!

[4]Note that such an ϵ_{MP} always exists; the promise consists of the assurance that it is *small*.

[5]In practice, however, we are likely to be ignorant of the precise nature of the imperfections, whereupon the imperfections would effectively be identical.

Note that it is usual for the measurements used in PE to be the same as those used in BI, but we leave the formulation general.

With this model for device imperfections, let us once again walk through the QKD scheme. We start at the end of the quantum communication step by reproducing (3.4), which is unaffected:

$$\left\| \rho_{(ABE)^{bn+m}} - \int_{\mathcal{S}_1} \rho^{|\theta\rangle}_{(ABE)^{bn+m}} \nu[|\theta\rangle] \right\|_1 \leq \epsilon_0. \tag{3.27}$$

Next, the PE step, but now instead of $\mathcal{M}_0$ we would have some $\mathcal{M}$:

$$\left\| \rho^{\mathcal{M},Q}_{(ABE)^{bn}} - \int_{\mathcal{S}_1} \rho^{|\theta\rangle,\mathcal{M},Q}_{(ABE)^{bn}} \nu[|\theta\rangle] \right\|_1 \leq \epsilon_0. \tag{3.28}$$

Again, we use Lemma 3.2.5 to restrict the integral to a subset, but first we note that

$$\begin{aligned}
&\forall |\theta\rangle \in \mathcal{S}_1, \\
|\theta\rangle \notin \mathcal{V}^{Q,\leq \mu_{\mathsf{PE}}+\epsilon_{\mathsf{MP}}}_{\mathcal{M}_0} &\Rightarrow \left\| \lambda^{\mathcal{M}_0}_{\infty} \left[\mathsf{Tr}_E |\theta\rangle\langle\theta| \right] - Q \right\|_1 > \mu_{\mathsf{PE}} + \epsilon_{\mathsf{MP}} \\
&\Rightarrow \left\| \left(\lambda^{\mathcal{M}_0}_{\infty} - \lambda^{\mathcal{M}}_{\infty} \right) \left[\mathsf{Tr}_E |\theta\rangle\langle\theta| \right] \right\|_1 + \left\| \lambda^{\mathcal{M}}_{\infty} \left[\mathsf{Tr}_E |\theta\rangle\langle\theta| \right] - Q \right\|_1 > \mu_{\mathsf{PE}} + \epsilon_{\mathsf{MP}} \\
&\Rightarrow \left\| \lambda^{\mathcal{M}}_{\infty} \left[\mathsf{Tr}_E |\theta\rangle\langle\theta| \right] - Q \right\|_1 > \mu_{\mathsf{PE}} \\
&\Rightarrow |\theta\rangle \in \mathcal{S}_1 \setminus \mathcal{V}^{Q,\leq \mu_{\mathsf{PE}}}_{\mathcal{M}} \\
&\Rightarrow \left\| \left(\mathsf{id}_{(ABE)^{bn}} \otimes \mathcal{E}^{\mathcal{M},Q}_{\mathsf{PE}} \otimes \mathsf{id}_{E^m} \right) \left[\rho^{|\theta\rangle}_{(ABE)^{bn+m}} \right] \right\|_1 \leq \epsilon_{\mathsf{PE}}.
\end{aligned} \tag{3.29}$$

The first line follows by definition of the parametrized $\mathcal{V}$ set, the next one from the triangle inequality for the trace distance, and the third from Promise 1 above regarding the imperfections in the PE measurement (along with (3.24)). The fourth line follows again from Lemma 3.2.5 and the definition of the $\mathcal{V}$ set, along the same lines as (3.13).

Therefore, we can restrict the integral to the set $\mathcal{V}^{Q,\leq \mu_{\mathsf{PE}}+\epsilon_{\mathsf{MP}}}_{\mathcal{M}_0}$, incurring the same trace-distance as before, viz. ϵ_{PE}, by means of another triangle inequality. This gives us

$$\left\| \rho^{\mathcal{M},Q}_{(ABE)^{bn}} - \int_{\mathcal{V}^{Q,\leq \mu_{\mathsf{PE}}+\epsilon_{\mathsf{MP}}}_{\mathcal{M}_0}} \rho^{|\theta\rangle,\mathcal{M},Q}_{(ABE)^{bn}} \nu[|\theta\rangle] \right\|_1 \leq \epsilon_0 + \epsilon_{\mathsf{PE}}. \tag{3.30}$$

The next step is blockwise measurements and information-processing (BI). Although the consideration of our model of imperfections entails a change in the map characterizing BI, it is still useful to write the following inequality, which describes the situation *if* the ideal map were to be applied:

$$\left\| \rho^{\mathcal{M},Q,\mathcal{J}_0,\mathcal{K}_0}_{X^n Y^n E^{bn}} - \int_{\mathcal{V}^{Q,\leq \mu_{\mathsf{PE}}+\epsilon_{\mathsf{MP}}}_{\mathcal{M}_0}} \rho^{|\theta\rangle,\mathcal{M},Q,\mathcal{J}_0,\mathcal{K}_0}_{X^n Y^n E^{bn}} \nu[|\theta\rangle] \right\|_1 \leq \epsilon_0 + \epsilon_{\mathsf{PE}}. \tag{3.31}$$

Of course, the actual situation is described by the application of a map of the form $\bigotimes_{i=1}^{n} \mathcal{E}_{\mathsf{BI}}^{\mathcal{J}_i,\mathcal{K}_i}$ instead of the desired $\left(\mathcal{E}_{\mathsf{BI}}^{\mathcal{J}_0,\mathcal{K}_0}\right)^{\otimes n}$. We denote the actual state at this point by $\rho_{X^nY^nE^{bn}}^{\mathcal{M},Q,\mathcal{J},\mathcal{K}}$, where the $\mathcal{J},\mathcal{K}$ stand for the imperfect measurements. Owing to Promise 2 stated earlier about the measurements used in the raw-key-generation, and to the sub-normalization of $\rho_{(ABE)^{bn}}^{\mathcal{M},Q}$, it follows that

$$\begin{aligned}
\left\|\rho_{X^nY^nE^{bn}}^{\mathcal{M},Q,\mathcal{J},\mathcal{K}} - \rho_{X^nY^nE^{bn}}^{\mathcal{M},Q,\mathcal{J}_0,\mathcal{K}_0}\right\|_1 &= \left\|\left(\left(\bigotimes_{i=1}^{n} \mathcal{E}_{\mathsf{BI}}^{\mathcal{J}_i,\mathcal{K}_i} - \left(\mathcal{E}_{\mathsf{BI}}^{\mathcal{J}_0,\mathcal{K}_0}\right)^{\otimes n}\right) \otimes \mathsf{id}_{E^{bn}}\right)\left[\rho_{(ABE)^{bn}}^{\mathcal{M},Q}\right]\right\|_1 \\
&\leq \left\|\bigotimes_{i=1}^{n} \mathcal{E}_{\mathsf{BI}}^{\mathcal{J}_i,\mathcal{K}_i} - \left(\mathcal{E}_{\mathsf{BI}}^{\mathcal{J}_0,\mathcal{K}_0}\right)^{\otimes n}\right\|_\diamond \\
&\leq \sum_{i=1}^{n} \left\|\mathcal{E}_{\mathsf{BI}}^{\mathcal{J}_i,\mathcal{K}_i} - \mathcal{E}_{\mathsf{BI}}^{\mathcal{J}_0,\mathcal{K}_0}\right\|_\diamond \\
&\leq \sum_{i=1}^{n} \left(\left\|\mathcal{J}_i - \mathcal{J}_0\right\|_{\mathsf{M}} + \left\|\mathcal{K}_i - \mathcal{K}_0\right\|_{\mathsf{M}}\right) \\
&\leq n\epsilon_{\mathsf{MI}}. \qquad (3.32)
\end{aligned}$$

Using (3.31), (3.32) and the triangle inequality for the trace norm, we get

$$\left\|\rho_{X^nY^nE^{bn}}^{\mathcal{M},Q,\mathcal{J},\mathcal{K}} - \int_{\mathcal{V}_{\mathcal{M}_0}^{Q,\leq \mu_{\mathsf{PE}}+\epsilon_{\mathsf{MP}}}} \rho_{X^nY^nE^{bn}}^{|\theta\rangle,\mathcal{M},Q,\mathcal{J}_0,\mathcal{K}_0} \nu[|\theta\rangle]\right\|_1 \leq \epsilon_0 + \epsilon_{\mathsf{PE}} + n\epsilon_{\mathsf{MI}}. \qquad (3.33)$$

As before, if an ϵ_{IR}-secure information-reconciliation scheme with a leakage of $\mathrm{leak}_{\mathsf{IR}}$ bits is used, and then 2-universal hashing is used to shorten the key to a length ℓ satisfying

$$\begin{aligned}
\ell \leq H_{\min}^{\epsilon_{\mathsf{PA}}+\epsilon_0+\epsilon_{\mathsf{PE}}+n\epsilon_{\mathsf{MI}}}\left[\rho_{X^nE^{bn}}^{\mathcal{M},Q,\mathcal{J},\mathcal{K}}|E^{bn}\right] - \mathrm{leak}_{\mathsf{IR}} - 2\log\left[\frac{1}{\epsilon_{\mathsf{PA}}+\epsilon_0+\epsilon_{\mathsf{PE}}+n\epsilon_{\mathsf{MI}}}\right] \\
- (m+k_0)\log\left[\dim\mathcal{H}_A\otimes\mathcal{H}_B\right] - \ell_0, \qquad (3.34)
\end{aligned}$$

then the resulting key is $\eta\left(\epsilon_{\mathsf{IR}} + \frac{3}{2}(\epsilon_{\mathsf{PA}}+\epsilon_0+\epsilon_{\mathsf{PE}}+n\epsilon_{\mathsf{MI}})\right)$-secure, again with ϵ_{PA} a choosable "smoothness" parameter, ℓ_0 and η polynomial-sized corrections, and k_0 the number of subsystems discarded before retaining the $bn+m$ with which we started our calculations. The refined lower bound on the entropy term appearing in the key-length expression, which follows from Inequality (3.33), is:

$$H_{\min}^{\epsilon_{\mathsf{PA}}+\epsilon_0+\epsilon_{\mathsf{PE}}+n\epsilon_{\mathsf{MI}}}\left[\rho_{X^nE^{bn}}^{\mathcal{M},Q,\mathcal{J},\mathcal{K}}|E^{bn}\right] \geq \min_{|\theta\rangle\in\mathcal{V}_{\mathcal{M}_0}^{Q,\leq\mu_{\mathsf{PE}}+\epsilon_{\mathsf{MP}}}} H_{\min}^{\epsilon_{\mathsf{PA}}}\left[\rho_{X^nY^nE^{bn}}^{|\theta\rangle,\mathcal{M},Q,\mathcal{J}_0,\mathcal{K}_0}|E^{bn}\right]. \qquad (3.35)$$

An advantage of this bound is that the entropy calculation is required to be done only under the ideal measurements $\mathcal{J}_0,\mathcal{K}_0$, as before, albeit over a larger set of states. In many important examples, such as the BB84 and six-state protocols, the entropy calculation under the ideal measurements is highly simplified by the existence of symmetries, whereas

it would be in general a nontrivial problem to estimate the effect of imperfect measurements on the value of the entropy.

However, there are some important disadvantages:

1. The minimum in the upper bound for secure key-rate is calculated over a larger set $\mathcal{V}_{\mathcal{M}_0}^{Q,\leq\mu_{\mathsf{PE}}+\epsilon_{\mathsf{MP}}} \supset \mathcal{V}_{\mathcal{M}_0}^{Q,\leq\mu_{\mathsf{PE}}}$, and therefore is expected to go down. Towards quantifying this effect, the most we can do is give an upper bound on the trace distance between the states that achieve the minimum in the smaller and the larger sets. Unfortunately, the exact effect of this on the conditional smooth min-entropy is not at all straightforward to estimate, for the following reason. While the min-entropy of a state without conditioning can be related in a straightforward manner to its spectrum (in fact it is exactly equal to the negative logarithm of the largest eigenvalue), the min-entropy conditioned on subsystem can only be upper-bounded. Therefore, given two states whose trace distance is bounded, not much can be said about the difference in their min-entropies conditioned on a subsystem.

2. The final security parameter is weakened by a term linear in n. Again, this disadvantage owes its origin to the difficulty in estimating the difference in the conditional min-entropies of states in terms of their trace distance. The "advantage" discussed earlier is that by paying this price in the security parameter we can avoid this difficult problem of estimating the entropy change. However, it would be in our interest to be able to eliminate this linear term by finding a way to improve the calculation, particularly because the parameter ϵ_{MI} is not tunable but characteristic of the device used.

Overcoming these disadvantages is an important aspect of the improvement required in our understanding of device imperfections in QKD. Apart from this, another important aspect is to model the imperfections more realistically and in a manner better-suited for calibration. We hope that this work acts as a first step in this direction.

Closing remarks and open problems

In the present work, we have undertaken the endeavour of bridging various types of gaps between the theoretical framework of quantum key-distribution (QKD) and its practical implementations. Specifically, we have addressed various limitations in the way preparation and measurement devices are modelled in QKD. Our progress has been the following:

1. In Chapter 1, we have presented some advances in the theory of squashing models, specifically in the understanding of the role of classical post-processing. We have then applied our understanding to derive a squashing model for the detection device used in the phase-encoded BB84 (PEBB84) QKD scheme.

2. In Chapter 2, we have discussed a general approach to deriving bounds on security-related parameters in optical QKD in cases where squashing models do not exist. Further, we have employed this approach to devise an estimation method in the case of PEBB84.

3. In Chapter 3, we have formulated a heuristic scheme for incorporating the effects of device imperfections on the security and performance of QKD as laid down in the information-theoretic framework developed by Renner. The present scheme uses a limited model for imperfections, based on the diamond-norm distance between measurement operations. The analysis used therein entails an increase in the security failure-rate by a term polynomial in the key-length.

Given the state of affairs described above, we identify the following as the most important among the problems remaining (or emerging) from our work:

1. Advancements in understanding the role of post-processing in particular, and squashing in general, which might provide a universally-applicable toolbox of squashing models, eliminating the need for detailed search and analysis in every particular application.

2. Converting the approach of statistical estimation into a more definite method, applicable universally without the need to devise suitable statistical observables in each application.

3. In general, we still work with many simplifications in modelling optical systems: absence of dark counts, assumption of equal efficiencies in all detectors, etc. It is important to eliminate these simplifying assumptions.

4. Improvements on the methods used in finding bounds on entropies, so that the linear worsening of the failure-rate under the limited imperfection model can be eliminated. More ambitiously, generalizing the model of imperfections so that it is both closer to reality and suitable for use in calibrating devices.

We conclude the thesis with the hope that the problems stated above are tackled, and eventually solved, using the work presented herein as a first step.

Appendices

Appendix A

Input-output relations for the phase-encoded BB84 detection setup

Here we derive input-output relations for the measurement device used in the phase-encoded BB84 (PEBB84) scheme.

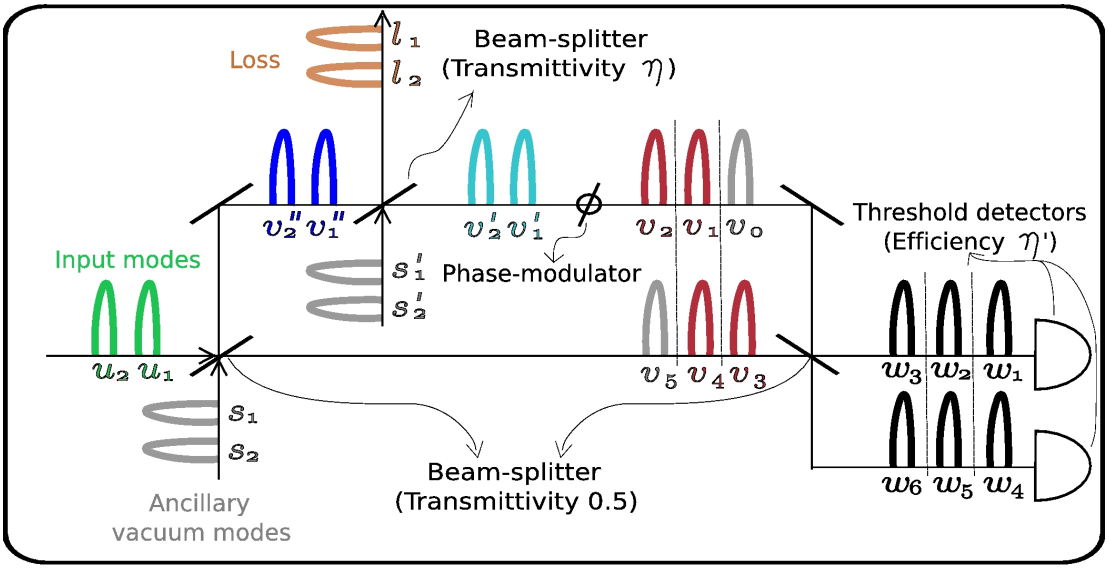
The detection setup on the receiver's side consists of a Mach-Zehnder interferometer with an adjustable phase-modulator (Fig. A.1(a)). Two successive pulses with annihilation operators u_1 and u_2 (green) make up two orthogonal modes[1] at the input (time being the relevant degree of freedom distinguishing the two modes). The output of the interferometer, which consists of six modes labelled by w, is fed to two threshold detectors. Our aim here is to find the output as a function of the input.

The two input modes u_1 and u_2, along with two ancillary input modes s_1 and s_2 which are forced to be in the vacuum state (all ancillary vacuum modes are shown in grey), are transformed by a 50-50 beam-splitter into the two lower v modes (red) and the two v'' modes (dark blue):

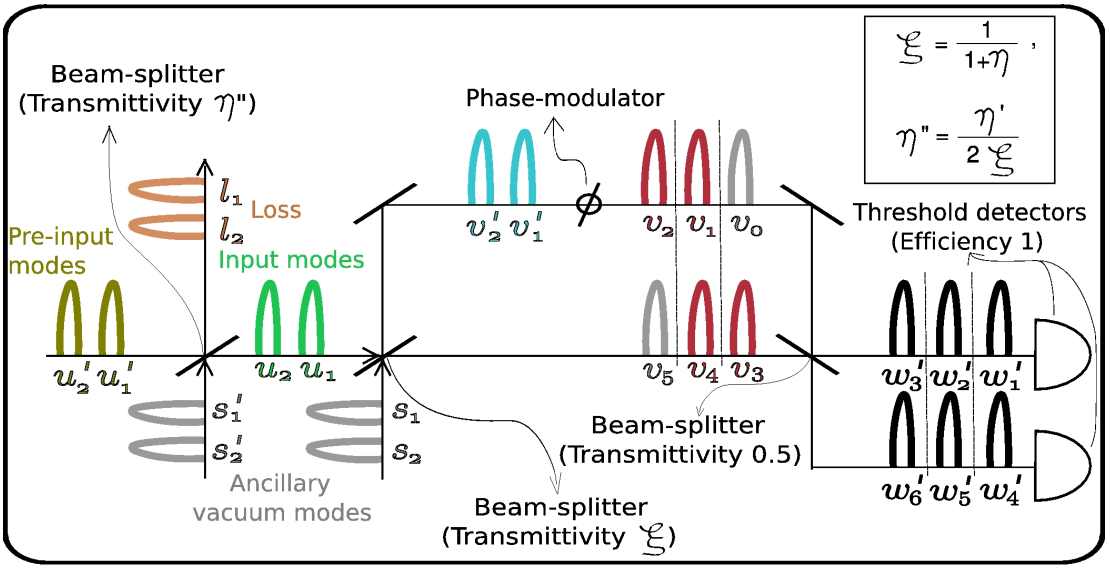
$$\begin{aligned}\begin{pmatrix} v_1'' \\ v_3 \end{pmatrix} &= \begin{pmatrix} 1/\sqrt{2} & -1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix}\begin{pmatrix} u_1 \\ s_1 \end{pmatrix}, \\ \begin{pmatrix} v_2'' \\ v_4 \end{pmatrix} &= \begin{pmatrix} 1/\sqrt{2} & -1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix}\begin{pmatrix} u_2 \\ s_2 \end{pmatrix}. \end{aligned} \tag{A.1}$$

The lossy phase-modulator, with transmittance η, is modeled by a beam-splitter of the same transmittance followed by a lossless phase-modulator. The two v'' modes and two ancillary vacua s' modes pass through the beam-splitter to give rise to the two v' modes (light blue) and two loss modes (l, brown):

[1] Throughout this thesis, we use the symbol for the annihilation operator of a certain mode as an appellation for the mode itself.



(a) Model of detection setup with imperfections: Two input modes u pass through a Mach-Zehnder interferometer with a $(1-\eta)$-lossy phase-modulator in the longer arm, and finally give rise to 6 output w modes, detected by two threshold detectors of equal efficiency η'.



(b) Model of detection setup with imperfections moved to channel: The loss is removed from the longer arm and the detectors replaced with perfectly-efficient ones; To compensate, a loss η'' is inserted in the channel and the first Mach-Zehnder beam-splitter transmittance is changed to ξ.

Figure A.1: Model of the measurement device (a) with its imperfections and (b) after the imperfections have been outsourced to the channel.

$$\begin{pmatrix} v_1' \\ l_1 \end{pmatrix} = \begin{pmatrix} \sqrt{\eta} & -\sqrt{1-\eta} \\ \sqrt{1-\eta} & \sqrt{\eta} \end{pmatrix} \begin{pmatrix} v_1'' \\ s_1' \end{pmatrix},$$
$$\begin{pmatrix} v_2' \\ l_2 \end{pmatrix} = \begin{pmatrix} \sqrt{\eta} & -\sqrt{1-\eta} \\ \sqrt{1-\eta} & \sqrt{\eta} \end{pmatrix} \begin{pmatrix} v_2'' \\ s_2' \end{pmatrix}. \tag{A.2}$$

The two v' modes pass through the lossless phase-modulator, which introduces a phase ϕ_B, and give rise to the upper two modes v. The basis choice for measurement is exercised by selecting either 0 or $\pi/2$ for the phase ϕ_B:

$$\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} \mathrm{e}^{-i\phi_B} & 0 \\ 0 & \mathrm{e}^{-i\phi_B} \end{pmatrix} \begin{pmatrix} v_1' \\ v_2' \end{pmatrix}. \tag{A.3}$$

Note that there is a negative sign in the phase, because we are writing the relation in terms of annihilation operators. Thereafter, the four v modes, along with two more ancillary vacuum modes v_0 and v_5, pass through the second 50-50 beam-splitter and give rise to the w modes. Note that the top two v modes lag behind the bottom modes in precisely such a way as to give rise to an interference between v_1 and v_4:

$$\begin{pmatrix} w_1 \\ w_4 \end{pmatrix} = \begin{pmatrix} 1/\sqrt{2} & -1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix} \begin{pmatrix} v_0 \\ v_3 \end{pmatrix},$$
$$\begin{pmatrix} w_2 \\ w_5 \end{pmatrix} = \begin{pmatrix} 1/\sqrt{2} & -1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix} \begin{pmatrix} v_1 \\ v_4 \end{pmatrix},$$
$$\begin{pmatrix} w_3 \\ w_6 \end{pmatrix} = \begin{pmatrix} 1/\sqrt{2} & -1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix} \begin{pmatrix} v_2 \\ v_5 \end{pmatrix}. \tag{A.4}$$

Finally, the six w modes are detected by two threshold detectors, which gives three time bins over two detectors. Certain important assumptions made about the detectors are:

1. The two detectors have the same efficiency, which we call η'.
2. The detectors are able to resolve each time slot, i.e., the dead-time is less than the rate of pulses arriving.
3. There are no dark counts.

Carrying out the linear transformations, we find

$$\begin{aligned}
w_1 &= \frac{1}{\sqrt{2}}v_0 - \frac{1}{2}u_1 - \frac{1}{2}s_1, \\
w_{2,\phi_B} &= \frac{\mathrm{e}^{-i\phi_B}\sqrt{\eta}}{2}u_1 - \frac{\mathrm{e}^{-i\phi_B}\sqrt{\eta}}{2}s_1 - \mathrm{e}^{-i\phi_B}\sqrt{\frac{1-\eta}{2}}s_1' - \frac{1}{2}u_2 - \frac{1}{2}s_2, \\
w_{3,\phi_B} &= \frac{\mathrm{e}^{-i\phi_B}\sqrt{\eta}}{2}u_2 - \frac{\mathrm{e}^{-i\phi_B}\sqrt{\eta}}{2}s_2 - \mathrm{e}^{-i\phi_B}\sqrt{\frac{1-\eta}{2}}s_2' - \frac{1}{\sqrt{2}}v_5, \\
w_4 &= \frac{1}{\sqrt{2}}v_0 + \frac{1}{2}u_1 + \frac{1}{2}s_1, \\
w_{5,\phi_B} &= \frac{\mathrm{e}^{-i\phi_B}\sqrt{\eta}}{2}u_1 - \frac{\mathrm{e}^{-i\phi_B}\sqrt{\eta}}{2}s_1 - \mathrm{e}^{-i\phi_B}\sqrt{\frac{1-\eta}{2}}s_1' + \frac{1}{2}u_2 + \frac{1}{2}s_2, \\
w_{6,\phi_B} &= \frac{\mathrm{e}^{-i\phi_B}\sqrt{\eta}}{2}u_2 - \frac{\mathrm{e}^{-i\phi_B}\sqrt{\eta}}{2}s_2 - \mathrm{e}^{-i\phi_B}\sqrt{\frac{1-\eta}{2}}s_2' + \frac{1}{\sqrt{2}}v_5.
\end{aligned} \tag{A.5}$$

Since we are interested in the working of the device only when all the auxiliary modes (s_1, s_2, s_1', s_2', v_0 and v_5) are in the vacuum state, we will always be projecting onto the vacuum states on these modes. Therefore, in all our calculations, we can use the following *effective* annihilation operators, where we have simply deleted all terms involving the auxiliary modes, instead of the ones above:

$$\begin{aligned}
w_1 &= -\frac{1}{2}u_1, \\
w_{2,\phi_B} &= \frac{\mathrm{e}^{-i\phi_B}\sqrt{\eta}}{2}u_1 - \frac{1}{2}u_2, \\
w_{3,\phi_B} &= \frac{\mathrm{e}^{-i\phi_B}\sqrt{\eta}}{2}u_2, \\
w_4 &= \frac{1}{2}u_1, \\
w_{5,\phi_B} &= \frac{\mathrm{e}^{-i\phi_B}\sqrt{\eta}}{2}u_1 + \frac{1}{2}u_2, \\
w_{6,\phi_B} &= \frac{\mathrm{e}^{-i\phi_B}\sqrt{\eta}}{2}u_2.
\end{aligned} \tag{A.6}$$

Note that while the expressions in (A.5) define annihilation operators of normalized and independent modes, those in (A.6) are not normalized annihilation operators. However, we can use them in all our calculations in the same manner as we use normalized annihilation operators, and the resulting factors would naturally represent the probabilities involved.

The next step is to replace the above model of the measurement device with a model where all imperfections are outsourced to the channel. For this, we note the following:

1. Because we assume that both threshold detectors have the same efficiency η', it is possible to replace them in the model with detectors with unit efficiency, and model the efficiency by placing a beam-splitter of transmittance η' in the channel, before the input modes. Essentially, this means any detection setup with perfectly efficient detectors at the end, but which results in output modes $\sqrt{\eta'}w$ just before the perfect detectors, is equivalent to the one above.

2. Since the only physically meaningful entity is the final statistics of detection outcomes, and not the meta-modes within the model of the measurement device, we are allowed to make a different model for the detector, provided the final statistics of detection outcomes is the same as before. One step towards the new model, that is to say, moving the detectors' efficiency to the channel, has been discussed above. In the next step, we move the phase-modulator loss to the channel. But now, since we have removed loss in an asymmetric manner between the two arms of the interferometer, we must compensate by skewing the first beam-splitter of the interferometer. The following equations will make this point clear; the essence is that the final $\sqrt{\eta'}w$ must not change.

Let us insert a beam-splitter of ratio η'' in the channel, and make the transmittance of the first beam-splitter of the interferometer ξ, where both the new parameters are yet to be determined. Carrying out similar calculations as before, we get

$$\begin{aligned}
w'_1 &= -\sqrt{\frac{\eta''\xi}{2}}u_1, \\
w'_{2,\phi_B} &= \mathrm{e}^{-i\phi_B}\sqrt{\frac{\eta''(1-\xi)}{2}}u_1 - \sqrt{\frac{\eta''\xi}{2}}u_2, \\
w'_{3,\phi_B} &= \mathrm{e}^{-i\phi_B}\sqrt{\frac{\eta''(1-\xi)}{2}}u_2, \\
w'_4 &= \sqrt{\frac{\eta''\xi}{2}}u_1, \\
w'_{5,\phi_B} &= \mathrm{e}^{-i\phi_B}\sqrt{\frac{\eta''(1-\xi)}{2}}u_1 + \sqrt{\frac{\eta''\xi}{2}}u_2, \\
w'_{6,\phi_B} &= \mathrm{e}^{-i\phi_B}\sqrt{\frac{\eta''(1-\xi)}{2}}u_2.
\end{aligned} \tag{A.7}$$

Now requiring $w' = \sqrt{\eta'}w$, we find that we can satisfy this by assigning

$$\xi = \frac{1}{1+\eta} \tag{A.8}$$

and

$$\eta'' = \frac{\eta'}{2\xi}. \tag{A.9}$$

Now that we have pushed all imperfections of the measurement device's model to the channel, we can consider the modes after the η'' beam-splitter as the input.

References

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

[2] C. H. Bennett. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, 68(21):3121–3124, may 1992.

[3] V. Scarani, A. Acín, G. Ribordy, and N. Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.*, 92:057901, 2004.

[4] K. Inoue, E. Waks, and Y. Yamamoto. Differential phase shift quantum key distribution. *Phys. Rev. Lett.*, 89:037902, 2002.

[5] N. Lütkenhaus. Security against eavesdropping in quantumcryptography. *Phys. Rev. A*, 54:97–111, 1996.

[6] E. Biham and T. Mor. Bounds on information and the security of quantum cryptography. *Phys. Rev. Lett.*, 79:4034, 1997.

[7] D. Gottesman and H.-K. Lo. From quantum cheating to quantum security. *Phys. Today*, 53:22–27, 11 2000.

[8] P. W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85:441–444, 2000.

[9] M. Christandl, R. Renner, and A. Ekert. A generic security proof for quantum key generation. quant-ph/0402131, 2004.

[10] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim. The universal composable security of quantum key distribution. In Joe Kilian, editor, *Second Theory of Cryptography Conference, TCC 2005, Cambridge, MA, USA, February 10-12, 2005.*, volume 3378 of *Lecture Notes in Computer Science*, pages 386–406, Berlin, 2005. Springer.

[11] B. Kraus, N. Gisin, and R. Renner. Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication. *Phys. Rev. Lett.*, 95(8):080501, Aug 2005.

[12] R. Renner. *Security of Quantum Key Distribution*. PhD thesis, ETH Zürich, 2005.

[13] P. D. Townsend, S. J. Phoenix, K. J. Blow, and S. M. Barnett. Design of quantum cryptography systems for passive optical networks. *Electr. Lett.*, 30(22):1875–1876, 1994.

[14] C. Marand and P. T. Townsend. Quantum key distribution over distances as long as 30 km. *OL*, 20(16):1695–1697, 1995.

[15] W. T. Buttler, R. J. Hughes, P. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons. Free-space quantum-key distribution. *Phys. Rev. A*, 57:2379–2382, 1998.

[16] P. D. Townsend. Experimental investigation of the performance limitsfor first telecommunications-window quantum cryptography systems. *IEEE Photonics Technology Letters*, 10:1048–1050, 1998.

[17] R. J. Hughes, G. L. Morgan, and C. G. Peterson. Practical quantum key distribution over a 48-km optical fiber network. *J. Mod. Opt.*, 47:533–547, 2000.

[18] N. Lütkenhaus. Security of quantum cryptography with realistic sources. *Acta Phys. Slovaca*, 49:549–556, 1999.

[19] N. Lütkenhaus. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A*, 61:052304, 2000.

[20] H. Inamori, N. Lütkenhaus, and D. Mayers. Unconditional security of practical quantum key distribution. quant-ph/0107017, 2001.

[21] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson. Practical free-space quantum key distribution over 10 km in daylight and at night. *New J. Phys.*, 4:43, 2002.

[22] M. Curty and N. Lütkenhaus. Effect of finite detector efficiencies on the security evaluation of quantum key distribution. *Phys. Rev. A*, 69:042321, 2004.

[23] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81:1301–1350, 2009.

[24] H.-K. Lo, X. Ma, and K. Chen. Decoy state quantum key distribution. *Phys. Rev. Lett.*, 94:230504, 2005.

[25] B. Ma, X.and Qi, Y. Zhao, and H.-K. Lo. Practical decoy state for quantum key distribution. *Phys. Rev. A*, 72:012326, 2005.

[26] Toyohiro Tsurumaru and Kiyoshi Tamaki. Security proof for quantum-key-distribution systems with threshold detectors. *Phys. Rev. A*, 78:032302, 2008.

[27] Normand J. Beaudry, Tobias Moroder, and Norbert Lütkenhaus. Squashing models for optical measurements in quantum communication. *Phys. Rev. Lett.*, 101:093601, 2008.

[28] Chi-Hang Fred Fung, H. F. Chau, and Hoi-Kwong Lo. Universal squash model for optical communications using linear optics and threshold detectors. *Phys. Rev. A*, 84:020303, Aug 2011.

[29] Dominic Mayers and Andrew Yao. Quantum cryptography with imperfect apparatus. In *Proceedings of the 39th Annual Symposium on Foundations of Computer Science*, FOCS '98, pages 503–509, Washington, DC, USA, 1998. IEEE Computer Society.

[30] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill. Security of quantum key distribution with imperfect devices. *Quant. Inf. Comp.*, 4(5):325, 2004.

[31] G Berlin, G Brassard, F Brussieres, and N Godbout. Fair loss-tolerant quantum coin flipping. *Phys. Rev. A*, 80:062321, 2009.

[32] N. Lütkenhaus. Estimates for practical quantum cryptography. *Phys. Rev. A*, 59:3301–3319, 1999.

[33] Masato Koashi. Unconditional security of coherent-state quantum key distribution with a strong phase-reference pulse. *Physical Review Letters*, 93(12):120501, 2004.

[34] Toyohiro Tsurumaru. Squash operator and symmetry. *Phys. Rev. A*, 81:012328, 2010.

[35] Tobias Moroder, Otfried Gühne, Normand J Beaudry, Marco Piani, and Norbert Lütkenhaus. Entanglement verification with realistic measurement devices via squashing operations. *Phys. Rev. A*, 81:052342, 2010.

[36] M.-D. Choi. Completely positive linear maps on complex matrices. *Linear Algebr. Appl.*, 10(3):285–290, 1975.

[37] C. Gobby, Z.L. Yuan, and A.J. Shields. Quantum key distribution over 122km of standard telecom fiber. *Appl. Phys. Lett.*, 84:3762–3764, 2004.

[38] N. Lütkenhaus and M. Jahma. Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack. *New J. Phys.*, 4:44, 2002.

[39] N. Lütkenhaus. *Generalised Measurements and Quantum Cryptography*. PhD thesis, University of Strathclyde, Glasgow, 1996.

[40] M. Koashi, Y. Adachi, T. Yamamoto, and N. Imoto. Security of entanglement-based quantum key distribution with practical detectors. arXiv:0804.0891, 2008.

[41] I. Devetak and A. Winter. Distillation of secret key entanglement from quantum states. *Proc. of the Roy. Soc. of London Series A*, 461(2053):207–235, 2005.

[42] Matthias Christandl, Robert König, and Renato Renner. Postselection technique for quantum channels with applications to quantum cryptography. *Phys. Rev. Lett.*, 102:020504, Jan 2009.