

# Squashing Models for Optical Measurements in Quantum Communication

Normand J. Beaudry (1), Tobias Moroder (1) (2), Norbert Lütkenhaus (1) (2)

1: Inst. for Quantum Computing, University of Waterloo, 200 University Ave. W., Waterloo ON N2L 3G1, Canada

2: Universität Erlangen-Nürnberg, Staudtstr. 7/B2, 91058 Erlangen, Germany

(nbeaudry@iqc.ca)

## Abstract

Measurements with photodetectors are naturally described in the infinite dimensional Fock space of one or several modes. A model has been postulated which describes the full mode measurement as a composition of a mapping (squashing) of the signal into a small dimensional Hilbert space followed by a specified target measurement. We present a formalism to investigate whether a given measurement pair of full and target measurements can be connected by a squashing model. We show that a measurement used in the BB84 protocol does allow a squashing description, although the corresponding six-state protocol measurement does not. As a result, security proofs for the BB84 protocol can be based on the assumption that the eavesdropper forwards at most one photon, while the same does not hold for the six-state protocol.

## Introduction

Quantum communication protocols are often constructed with information encoded in qubit signals sent between different parties, and therefore low-dimensional Hilbert spaces only need to be considered for these signals. However, in the experimental implementation of these protocols, signals are realized by photons, which are naturally described by the Fock spaces of spatio-temporal modes. Consider a protocol which uses a source that outputs either the vacuum or single photons, send the signals through a quantum channel, and then they are received by a detector which accepts single photons or the vacuum. In order to use the theoretical tools which may have been developed for this protocol, it would be convenient to be able to link a qubit theory, which applies to this protocol, with an experimental implementation which is realised by optical modes. Here we focus on the side of the detector, where the squashing model can allow such a link.

## Motivation

A typical measurement in quantum communication is the one used in the BB84 QKD protocol [1] called the active detection scheme, in which the incoming light is split by a polarizing beam-splitter, which can be oriented either along the horizontal/vertical basis or in the +45/-45 degree basis. The signal is then sent to a threshold detector which cannot resolve the number of photons by which they are triggered. This measurement can be described as a single Positive Operator Valued Measure (POVM) with non-commuting POVM elements if the basis choice is done at random

with some fixed probabilities. It has been postulated that there exists a squashing model for this set-up, which first maps (squashes) the incoming signal to a one-photon polarization Hilbert space, followed by the same BB84 measurement. A recent important security proof [2] is based on this detector property.

In the context of QKD, one typically assumes the *calibrated device scenario* in which the detection device is trusted and known. Then if a squash model exists, the corresponding squashing map can become part of Eve's attack. Therefore we can assume, without loss of generality, that Eve sends a signal in the Hilbert space  $Q$  to the receiver, Bob. As an example, many security proofs assume that Eve forwards polarized single photons (qubits) or vacuum states to the receiver. If a given full optical implementation of a polarization measurement has a squash model connecting it to the single photon polarization measurement assumed in the security proof, then this proof is also valid for the full optical implementation of the protocol. Additionally, squashing the detection to a finite-dimensional system makes it possible to use the exponentially fast converging de Finetti theorems of Renner [3] on the level of the squashed system, even if the original full system is infinite dimensional.

## Main Achievements

Let us first define a squashing model more precisely. A full measurement,  $F_M$ , described by a POVM with elements  $F_M^{(i)}$  defined on a large (possibly infinite dimensional) Hilbert space  $M$  is said to *admit a squashing model with respect to a target measurement*,  $F_Q$ , with POVM elements  $F_Q^{(i)}$  on a smaller dimensional Hilbert

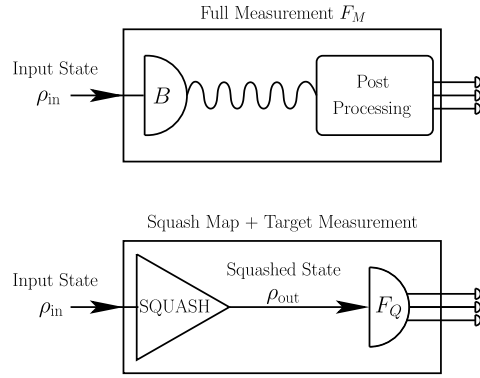


Figure 1: The mode measurement  $F_M$  (above) has a general optical input  $\rho_{in}$ , which is first measured by a receiver's physical detector  $B$ , followed by classical post-processing. The squashed measurement (below) has the same general optical input  $\rho_{in}$ , which is then squashed by a map  $\Lambda$  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  $\rho_{in}$ .

space  $Q$  if a squashing map  $\Lambda$  from  $M$  to  $Q$  exists, such that the composition of the squashing map and the measurement on  $Q$  is statistically equivalent to the measurement on system  $M$ . In other words, the two measurement models in Fig. 1 must act identically for any input signal.

Given this condition, we find a set of linear constraints on a positive operator,  $\tau$ , which provide a set of necessary and sufficient conditions for finding a squashing model connecting a full and target measurement. These conditions can be solved analytically, or they can also be solved numerically via convex optimization techniques such as semidefinite programming.

Let us now consider the optical implementation of the BB84 measurement mentioned above. Double clicks occur in this setup if both detectors fire due to a multiphoton input, while after squashing at most one photon is contained in the signal and so no double-clicks can occur. Therefore, to match the number of possible outcomes, we can choose to map double-clicks of the full mode measurement randomly to the single-click event of one of the two detectors, which has been introduced before in the security analysis of QKD [4, 5]. Under this post-processing we have shown that there exists a squashing model for this measurement [6], which has also been independently obtained by [7]. In the six-state protocol [8, 9], a third measurement setting is introduced to the BB84 measurement above. In this case, we show there is no squashing map for this measurement with the specified post-processing [6].

Another typical detection device is the one used in the BB84 QKD protocol called the passive detection

scheme, where the basis choice is performed instead by a 50/50 beam splitter, and on each end is a polarizing beamsplitter and two threshold detectors. If there is a double click between the two separate ends then there are two possible post-processings of interest that give a squashing model: they can be mapped at random or chosen to be a vacuum outcome. Also, the six-state measurement can also be made to be passive by making the basis choice by a 1:1:1 beam splitter which has three arms measuring in each of the three bases. In this case a squashing map exists, where the double clicks between at least two of the three arms are randomly assigned.

## Conclusion

To summarize, we give necessary and sufficient linear conditions on a positive operator so that a full measurement can be represented by a concatenation of a squashing operation and a lower dimensional target measurement. In application to security proofs of QKD, the existence of a squashing model allows a simple qubit-based security proof to be lifted to one based on the full optical implementation, as is the case for the BB84 active and passive measurements as well as the passive six-state measurement. In the absence of a squashing model a shortcut from the qubit theory to the full optical implementation is not possible, and another method of proving security of the full optical scenario has to be found, such as for the active six-state measurement. Also, the squashing property holds for the detection set-up independent of the use of the detection device, and so the method outlined here will help to simplify the analysis in other quantum communication contexts, including the verification of entanglement of optical modes with threshold detectors.

- [1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.
- [2] X.-F. Ma, C.-H. Fung, and H.-K. Lo, *Phys. Rev. A* **76**, 012307 (2007).
- [3] R. Renner, *Nature Physics* **3**, 645 (2007).
- [4] N. Lütkenhaus, *Phys. Rev. A* **59**, 3301 (1999).
- [5] N. Lütkenhaus, *Phys. Rev. A* **61**, 052304 (2000).
- [6] N. J. Beaudry, T. Moroder, and N. Lütkenhaus, *Phys. Rev. Lett.* **101**, 093601 (2008).
- [7] K. Tsurumaru, T. Tamaki, *Phys. Rev. A* **78**, 032302 (2008).
- [8] D. Bruß, *Phys. Rev. Lett.* **81**, 3018 (1998).
- [9] H. Bechmann-Pasquinucci and N. Gisin, *Phys. Rev. A* **59**, 4238 (1999).