Squashing model for detectors and applications to quantum-key-distribution protocols

O. Gittsovich,[1] N. J. Beaudry,[1,2] V. Narasimhachar,[1] R. Romero Alvarez,[1,3] T. Moroder,[1,4] and N. Lütkenhaus[1]

[1]*Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1*

[2]*Institute for Theoretical Physics, ETH Zürich, 8093 Zürich, Switzerland*

[3]*Department of Physics, University of Toronto, Toronto, Ontario, Canada M5S 1A7*

[4]*Naturwissenschaftlich-Technische Fakultät, Universität Siegen, Walter-Flex-Straße 3, D-57068 Siegen, Germany*

(Received 6 November 2013; published 23 January 2014)

We develop a framework that allows a description of measurements in Hilbert spaces that is smaller than their natural representation. This description, which we call a "squashing model," consists of a squashing map that maps the input states of the measurement from the original Hilbert space to the smaller one, followed by a targeted prescribed measurement on the smaller Hilbert space. This framework has applications in quantum key distribution, but also in other cryptographic tasks, as it greatly simplifies the theoretical analysis under adversarial conditions.

DOI: 10.1103/PhysRevA.89.012325 PACS number(s): 03.67.Dd, 03.65.Ta, 03.67.Hk, 42.50.−p

I. INTRODUCTION

Measurements are an essential part of quantum mechanics. In quantum communication, among other fields, various measurements are used to extract information from signals. In quantum cryptographic contexts measurement results often allow the inference of how third parties are correlated with the obtained data. Usually, the quantum advantage of these communication protocols is demonstrated in theoretical protocols utilizing abstract qubit systems, or other low-dimensional systems. However, in physical realizations of quantum communication protocols, no qubit systems are available; instead, one resorts to optical implementations where the signals and measurements are described on infinite-dimensional Hilbert spaces corresponding to optical modes.

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 down-conversion experiments only on the level of vacuum and single-photon pairs. We can do this because we can handle the approximations well on a theoretical level such that theoretical predictions and experimental verifications coincide with high precision.

In quantum cryptographic situations, such as quantum key distribution (QKD) or quantum coin tossing [1–4], this is not good enough. In such contexts, we would have to account for the information that an arbitrary third party could gain about our measurement data. Since experimental verification of third-party information is not possible, we need to be able to provide rigorous bounds on such compromised information. One possibility is to do full calculations in the infinite-dimensional Hilbert spaces [5,6]. Often, this is technically challenging. The other possibility is to do truncations to finite-dimensional subspaces. These can not be in the form of approximations, but as truncations that also hold under adversarial conditions. Again, there are two possibilities. The traditional way would be to provide exact bounds on the effect of truncations and to extend the theoretical qubit analysis to accommodate the effects of the truncation. This approach has been followed, for example, in Ref. [7] in the context of a specific application, while a more general framework of this approach has recently been formulated in Ref. [8]. Here, we show a second way, which was already postulated in Ref. [9], where the term "squashing" was coined for this approach. The squashing method 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 in the truncated Hilbert space. In the context of QKD, this approach means that for a generic QKD protocol with a Bennett-Brassard 1984 (BB84) [1] polarization encoding, we can assume without loss of generality that single photons enter the detection device of the receiver.

Thus, our approach allows a truncation of high-dimensional Hilbert spaces to some low-dimensional target space that also holds under adversarial conditions, as they occur in cryptographic contexts. We build on our earlier work [10] that gave a well-defined notion of a squashing map that allows us to clarify the role of the squashing assumption. Note that Tsurumaru and Tamaki [11,12] independently investigated squashing models and Semenov and Vogel [13] pointed out an important application of squashing models in the context of experiments measuring the Bell parameter.

A rough idea of what a squashing model does is represented in Fig. 1. Each physical measurement device B provides some basic distinguishable events for an input state ρ_{in}, which usually has its support on a high-dimensional Hilbert space. All possible events that can be triggered by the states in the high-dimensional Hilbert space will formally correspond to a positive operator-valued measure (POVM) F_B. If one would feed the measurement device with states from some low-dimensional Hilbert space, then typically the number of possible events will be smaller. We refer the corresponding POVM as to target POVM and denote it by F_Q. Often, however, the events produced by the states from the high- and low-dimensional Hilbert spaces can be related by a classical postprocessing, which is applied to the basic events. A typical example in QKD is a processing of double clicks occurring in the BB84 protocol. The basic events after a particular (classical) postprocessing form a coarse-grained list of events, which then are described by a POVM F_M. We refer to the combination of basic events and postprocessing as the *full measurement*. This classical postprocessing will be an

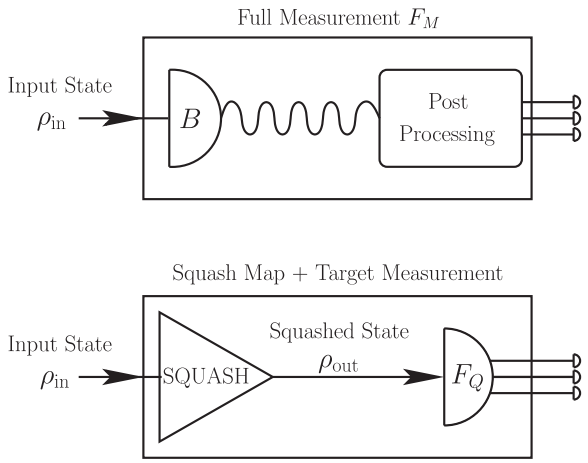

FIG. 1. The full measurement F_M (above) has a general optical input ρ_{in}, which is first measured by a receiver's measurement device B, followed by classical postprocessing. The squashed measurement (below) has the same general optical input ρ_{in}, which is then squashed by a map SQUASH to a smaller 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}.

essential tool in making squashing models work. A squashing model provides an equivalent but simplified description of the full measurement F_M on the high-dimensional Hilbert space in terms of the measurement F_Q on the low-dimensional Hilbert space. The map SQUASH or squashing map (see Fig. 1) provides a direct link between the measurements on the high-dimensional and the truncated Hilbert spaces. Formally, the squashing map takes a state ρ_{in} as input and outputs a "squashed" state ρ_{out} on the truncated Hilbert space. The squashing model is an equivalent description of the full measurement F_M in terms of the squashing map and a target measurement F_Q on a squashed state ρ_{out}. All elements (basic measurement F_B, target measurement F_Q, and classical postprocessing) need to be specified in order to form a well-posed question for the existence of a squashing model. A typical choice for the target measurement will be the restriction of the full measurement to a single-photon input, although our framework is not limited by this particular choice.

In this article, we first extend the formalism introduced in Ref. [10] and provide a rigorous framework for how to find a squashing model for a particular measurement device and which general steps can be used in order to simplify the analysis. For example, we show how to enforce the existence of squashing maps by choosing the postprocessing that introduces additional noise. Second, we review previous results involving the squashing model for the measurement devices which are used in optical implementations of the BB84 [10] and six-state [10,11] QKD protocols with an active detection scheme. Third, we discuss several generalizations of these measurement devices and provide squashing models for them. For instance, we present a squashing model for a generalization of the qubit measurement devices with the passive detection scheme to qudit measurement devices [14–16] and prove that there exists a squashing model for this generalized device. We also consider squashing models for the measurements that accept different temporal modes and are employed in the phase-encoded BB84 (PEBB84) protocol.

This paper is organized as follows. The first part (Secs. II–IV) is devoted to the general framework and discussion of the general properties of the examples presented in the second part (Secs. V–X). Some technical details relevant for our investigations are given in the Appendices.

In Sec. II, we fix the notation and define the quantities that will be frequently used. We will define the squashing model as well. In Sec. III, we present general strategies for finding a squashing map for a general measurement device and discuss possible issues such as nonpositivity of the squashing map. Subsequently, in Sec. IV, we consider common properties of typical linear optical measurement devices, which simplify the construction of the squashing model. In particular, we discuss how the usage of threshold detectors helps to truncate infinite-dimensional Hilbert space of an optical mode and the consequences it has for the application of the general framework to concrete examples.

In Secs. V–VII, we apply the presented theory in order to construct squashing models for several optical measurement devices. These include active measurement devices from the BB84 QKD protocol (Sec. V), from the six-state protocol (Sec. VI), biased active and passive measurements from the BB84 protocol, and passive measurement from the six-state QKD protocol (Sec. VII). In Sec. VIII, we present a squashing model for measurement devices that can be used in the optical implementation of qudit QKD protocols. In Sec. IX, we consider squashing models in the time domain, where the incoming state can carry multiple photons that are distributed over several time modes. We show that this generalization does not affect the existence of a squashing model. Finally, in Sec. X we discuss the squashing model for the measurement device from the phase-encoded BB84 (PEBB84) protocol. This refines the security analysis of the corresponding QKD protocol, which was performed in Refs. [17,18].

II. NOTATION AND STATEMENT OF THE PROBLEM

We first make some preliminary definitions so that we can define a squashing model explicitly. $\mathcal{H}_M$ denotes a high-dimensional Hilbert space. Basic and full measurements on a state $\rho_M \in \mathcal{B}(\mathcal{H}_M)$ are described by POVMs F_B and F_M, respectively. $\mathcal{H}_Q$ denotes the low-dimensional Hilbert space (i.e., the target Hilbert space). The measurement on the states $\rho_Q \in \mathcal{B}(\mathcal{H}_Q)$ (the target measurement) is described by the POVM F_Q. Elements of the corresponding POVM are denoted by $F_X^{(i)}$ with $X \in B,M,Q$, and the indices i run over the set of outcomes for each of the measurements. Observed probabilities for measurement outcomes are given by $p_X^{(i)} = \text{Tr}(F_X^{(i)}\rho)$.

Moving forward to the formal definition of a squashing model, we need to explicitly state what classical postprocessing means. The classical postprocessing is applied to the basic measurement outcomes and allows, for example, to combine different outcomes into one (which we call coarse graining). More precisely, it defines the full measurement by using the basic measurement events such that the POVM F_M contains the same number of elements as the target POVM F_Q. Otherwise, the problem of finding a squashing model is not well defined.

Formally, the postprocessing can be described as a stochastic matrix $\mathcal{P}$ ($\sum_i \mathcal{P}_{ij} = 1, \forall\, j$) which acts on the vector of probabilities of the basic measurement outcomes. The entries of the matrix $\mathcal{P}_{ij} = p(i|j)$ are given by the conditional probabilities which describe the redistribution of the outcomes of the POVM F_B with index j into events of the full measurement POVM F_M with index i.

Summarizing the above discussion, we have the following.

Definition 1. Classical postprocessing: Let $\vec{p}_{\text{bas}}$ be the vector of the outcome probabilities of the basic measurement B. We say that a classical postprocessing (CPP) scheme is defined if there exists a stochastic matrix $\mathcal{P}$ such that

$$\vec{p} = \mathcal{P}\vec{p}_{\text{bas}}, \tag{1}$$

and the number of the outcome probabilities p_j coincides with the number of events provided by the target POVM F_Q.

It is not hard to see that the postprocessing can be considered as a linear transformation of the POVM elements

$$F_M^{(i)} = \sum_j \mathcal{P}_{ij} F_B^{(j)}, \tag{2}$$

where we require that $\vec{p} = \text{Tr}(\rho F_M^i)$ describes the vector of outcome probabilities of the full measurement F_M.

In our discussion, we will not add a postprocessing step to the target measurement, as the choice of target measurement is usually motivated by circumstances. A typical example of this is when a security proof may exist for a fixed given measurement, which one then typically considers as a target measurement in the context of the squashing model. As the target measurement is given by a particular POVM, it may already be a combination of some target measurements and fixed postprocessing of the target events. An example of this situation will be discussed in Sec. X, where we construct a squashing model for the measurement device used in the phase-encoded BB84 QKD protocol and will group certain target measurement events into one (outside clicks).

We will fix the notation and define the CPP and then we will give the formal definition of a squashing model.

Definition 2. Squashing model: Let F_B and F_Q be the POVMs that describe outcomes of a measurement performed by a physical device B on states in high- and low-dimensional Hilbert spaces, respectively. Let $\mathcal{P}$ be a CPP scheme that defines a full measurement POVM F_M. Then, we say that there exists a squashing model for the device B and the CPP $\mathcal{P}$ if there exists a map Λ_B such that

(1) for any state ρ_M the linear constraints

$$\text{Tr}\big(F_M^{(i)}\rho_M\big) = \text{Tr}\big(F_Q^{(i)}\Lambda_B[\rho_M]\big), \quad \forall\, i \tag{3}$$

are satisfied;

(2) Λ_B is a completely positive (CP) map; we call it a "squashing map".

Remark 3. Linear constraints on POVM elements: We introduce the adjoint map $\Lambda_B^\dagger$ to find that Eq. (3) implies

$$\text{Tr}\big(F_M^{(i)}\rho_M\big) = \text{Tr}\big(\Lambda_B^\dagger\big[F_Q^{(i)}\big]\rho_M\big), \quad \forall\, i. \tag{4}$$

This has to hold for any state ρ_M. Therefore,

$$\Lambda_B^\dagger\big[F_Q^{(i)}\big] = F_M^{(i)}, \quad \forall\, i = 1, \ldots, N_Q, \tag{5}$$

which can be seen as linear constraints on the map $\Lambda_B^\dagger$. The adjoint map has to satisfy

$$\Lambda_B^\dagger[\mathbb{1}_Q] = \mathbb{1}_M, \tag{6}$$

which is the unital property of the adjoint of the squashing map and assures that Λ_B is completely positive and trace preserving (CPTP).

In order to gain more insight into the formal definition of the squashing model, we make a few more remarks. The definition of the squashing model consists of two essential parts. In order to provide a squashing model for a given measurement device B, a particular low-dimensional Hilbert space must be chosen. Second, one has to agree on a meaningful postprocessing, as defined in Definition 1. The classical postprocessing can be seen as a freedom available to search for a squashing model. That is, the postprocessing fixes the full measurement and has to satisfy the linear constraints in Eq. (3), which has to be fulfilled by the squashing map Λ_B. In fact, as we will see later on, for any choice of the POVMs F_B and F_Q there always exists a CPP scheme for which a squashing model exists. However, as we will also see, such a squashing model may not be meaningful and would correspond to a very noisy outcome of the measurement. The squashing map Λ_B has to be a CPTP map. Therefore, its existence, given the constraints, can be investigated by exploiting the Choi-Jamiołkowski isomorphism [19,20]. Note that variations of squashing models that require only positive but not completely positive maps have been investigated and utilized in Ref. [21].

III. GENERAL STRATEGY TO FIND A SQUASHING MODEL

The formal definition of the squashing model already provides some intuition for how to investigate the question of whether a squashing model exists for a given measurement device. The goal of this section is to provide a step-by-step strategy to search for a squashing map for any particular case.

A. Basic and target POVMs

In our considerations, we always assume that the exact physical model of the actual measurement device is known, so the POVM F_B is fixed. The choice of the target measurement depends on the choice of the truncated Hilbert space and is always motivated by circumstances. For example, a theoretic analysis of a communication protocol with a specific POVM F_Q might already exist and we would like to link an optical implementation with basic events F_B to this analysis. So, the main choice that has to be made to set up a well-defined search for a squashing map is that of the postprocessing of the basic events into the full measurement events.

B. Constraints on CPP schemes

We pointed out before that any valid classical postprocessing scheme has to assure that the number of events of the full and the target measurements coincide. There are further limitations on what types of classical postprocessing that can lead to a successful squashing map. We note that the set of the target POVM elements $F_Q^{(i)}$ may be linearly dependent which

means that there may exist some complex numbers α_i, such that

$$\sum_{i=1}^{N_Q} \alpha_i F_Q^{(i)} = 0. \tag{7}$$

Each set of POVM elements of the corresponding basic measurement add up to the identity on the operator space. This also means that the full measurement (including postprocessing) must have the same linear dependency. This has implications for the postprocessing of the basic events, as this linear dependence has to be respected by the postprocessing $\mathcal{P}$ one is looking for. Due to the linearity of $\Lambda_B^\dagger$ and the linear constraints in Eq. (5), we can write

$$\sum_i \alpha_i F_Q^{(i)} = 0 \Leftrightarrow \sum_i \alpha_i F_M^{(i)} = 0 \Leftrightarrow \sum_{i,j} \alpha_i \mathcal{P}_{ij} F_B^{(j)} = 0. \tag{8}$$

The simplest example of the situation where the target POVM elements are linearly dependent is the qubit measurement in the BB84 QKD protocol. There, the sum of the elements of either basis is proportional to the identity operator and therefore it is not hard to find scalars α_i such that Eq. (7) holds.

Using the vectorization of the POVM elements, it is convenient to rewrite Eq. (8) as

$$\sum_i \alpha_i \mathrm{vec}\big(F_M^{(i)}\big) = 0 \Leftrightarrow \sum_{i,j} \alpha_i \mathcal{P}_{ij} \mathrm{vec}\big(F_B^{(j)}\big) = 0, \tag{9}$$

where the vectorization $\mathrm{vec}(\cdots)$ gives an isomorphism between the linear bounded operators and vectors in corresponding spaces. Considering $\mathrm{vec}(F_B^{(i)})$ for any i as an ith column of a matrix and writing $\vec{\alpha} = (\alpha_1, \ldots, \alpha_{N_Q})^T$ gives $\mathbf{F}_Q \vec{\alpha} = 0 \Leftrightarrow \mathbf{F}_M \vec{\alpha} = 0 \Leftrightarrow \mathbf{F}_B(\mathcal{P}^T \vec{\alpha}) = 0$. In summary, we have the following observation.

Observation 4. Valid CPP schemes: A valid postprocessing that allows for the existence of a squashing map is a stochastic matrix such that its transpose maps the null space of the matrix, built from the vectorizations of the basic POVM elements $\mathbf{F}_B^{(i)}$, onto the null space of the matrix, built from the vectorizations of the target POVM elements $\mathbf{F}_Q^{(i)}$:

$$\mathcal{P}^T : \mathrm{Null}(\mathbf{F}_Q) \to \mathrm{Null}(\mathbf{F}_B). \tag{10}$$

Note that this condition incorporates both the validity of a CPP scheme, as stated in Definition 1, and the requirement that the linear dependencies of the POVM elements on the truncated and initial Hilbert spaces has to be respected. Hence, if this condition is satisfied, then there always exists a linear map connecting the full and the target measurements.

C. Determining the existence of a squashing map: Complete positivity

The last constituent of a squashing model is the positivity of the squashing map (the linear map from the previous section). In order to check for positivity, we employ the Choi-Jamiołkowski isomorphism [19,20]

$$\tau \equiv \mathbb{1}_Q \otimes \Lambda_B^\dagger(|\psi^+\rangle\langle\psi^+|) \geqslant 0, \tag{11}$$

where τ is called the Choi matrix and $|\psi^+\rangle = \frac{1}{\sqrt{d_Q}} \sum_i |i\rangle|i\rangle$ is a normalized maximally entangled state. This isomorphism is formulated directly from the action of the adjoint map $\Lambda_B^\dagger$. The property of complete positivity of the map $\Lambda_B^\dagger$ is then equivalently expressed by the positivity of the corresponding Choi matrix.

The linear constraints on the map $\Lambda_B^\dagger$ are best expressed in terms of the so-called natural representation τ^R (see Appendix A for details). The direct link between the full and the target measurements in the natural representation is given by

$$\tau^R \mathrm{vec}\big(F_Q^{(i)}\big) = \mathrm{vec}\big(F_M^{(i)}\big). \tag{12}$$

Note that this automatically includes the condition for the map $\Lambda_B^\dagger$ to be unital, as can be checked by summing over the index i.

As a consequence, one can reformulate the problem of looking for a completely positive squashing map as a special instance of semidefinite programming (feasibility problem) [22]:

$$\text{Find } \tau \geqslant 0, \quad \text{s.t.} \quad \tau^R \mathrm{vec}\big(F_Q^{(i)}\big) = \mathrm{vec}\big(F_M^{(i)}\big). \tag{13}$$

It is clear from the provided construction that the positivity of the Choi matrix (and therefore of the squashing map) crucially depends on the choice of the classical postprocessing. In fact, as we will see in the next section and in Sec. VI C, if positivity is not achieved by the basic measurement it can be always repaired by choosing another valid postprocessing, although this will typically be at some price in terms of protocol performance.

D. Enforcing existence of squashing maps by noisy postprocessing

In this section, we point out two important facts: (i) We can always find a squashing model for any pair of target and basic measurements by choosing a suitable (although very noisy) postprocessing which we call a *trivial squashing model* (Proposition 5). (ii) Despite the fact that this trivial squashing model might, at first sight, appear useless, we can use its completely positive squashing map in order to restore the positivity of another squashing map that appears to be nonpositive and therefore construct a *nontrivial squashing model*. That will be the essence of the *restoring theorem* (Theorem 7).

To be more specific, we provide an example for how a noisy squashing model can be used and then turn to the general case. A typical situation where we look for squashing models has the property that the target measurement corresponds to a restriction of the basic measurement to some simple subspaces, for example, those of single-photon signals. In these cases, one will usually try to make a smart choice of postprocessing, namely, such that the postprocessing retains this property, i.e., the restriction of the full measurement to the specified subspaces results in the target measurement. An example of such a CPP scheme arises in the context of the six-state measurements (defined in Sec. VI) where one makes a random assignment of double clicks (when two detectors fire simultaneously), while keeping the single-click events unchanged. As we will see, the squashing map constructed for this CPP scheme is not completely positive (Sec. VI B). However, this positivity problem can be overcome by statistically mixing the smart postprocessing (where single-click events are unchanged) with a noisy postprocessing that will also reassign single-click outcomes (see Sec. VI C).

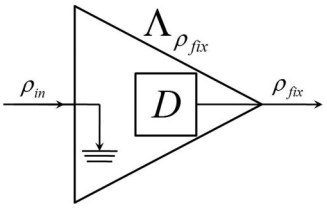

FIG. 2. Squashing map $\Lambda_{\rho_{\text{fix}}}$ that disregards the input and outputs a fixed state ρ_{fix}, which is prepared by a device D.

To start out, we introduce a postprocessing which allows the existence of a trivial squashing model.

Proposition 5. (Trivial squashing map): Let $F_B^{(i)}$ be any complete set of POVM elements that characterize the basic measurement and let $F_Q^{(j)}$ be some complete set of POVM elements that characterize the target measurement. Let the classical postprocessing be such that it redistributes all basic events according to some *a priori* fixed probabilities, which are derived from a density matrix ρ_{fix} as $p_Q^{(i)} = \text{Tr}(\rho_{\text{fix}} F_Q^{(i)})$ and which do not depend on the input state. Then, there always exists a squashing model such that its map $\Lambda_{\rho_{\text{fix}}}$ acts trivially on any input state ρ_{in}, i.e., $\Lambda_{\rho_{\text{fix}}}[\rho_{\text{in}}] = \rho_{\text{fix}}$.

Proof. The statement of the proposition is a link between positivity of a squashing map for any type of basic and target measurements and a certain classical postprocessing. An idea of how such a postprocessing scheme can be constructed, and which squashing map it corresponds to, is presented in Fig. 2. We apply a postprocessing which ignores the measurement result and assigns an outcome with fixed *a priori* probabilities $p_Q^{(i)} = \text{Tr}(\rho_{\text{fix}} F_Q^{(i)})$ compatible with some fixed quantum state ρ_{fix}. We define a map $\Lambda_{\rho_{\text{fix}}}$ such that $\Lambda_{\rho_{\text{fix}}}[\rho_{\text{in}}] = \rho_{\text{fix}}$ for any ρ_{in}. By construction, this map is completely positive and fulfills the linear constraints of Eq. (5). ■

Before we show how this type of the squashing map is useful, we need to point out an important property of its Choi matrix.

Remark 6. Properties of the Choi matrix for the trivial squashing map: The minimum eigenvalue of the Choi matrix of the trivial squashing map $\Lambda_{\rho_{\text{fix}}}$ is proportional to the minimum eigenvalue of the state ρ_{fix} with the coefficient of proportionality $1/d_Q$, where d_Q is the dimension of the target Hilbert space $\mathcal{H}_Q$.

Proof. As defined in Proposition 5, $\Lambda_{\rho_{\text{fix}}}[\rho] = \rho_{\text{fix}}$ for any ρ. Therefore, the adjoint map $\Lambda^\dagger_{\rho_{\text{fix}}}$ must satisfy

$$\text{Tr}(\rho_{\text{fix}}\mathcal{O}) = \text{Tr}\big(\rho \Lambda^\dagger_{\rho_{\text{fix}}}[\mathcal{O}]\big) \tag{14}$$

for any bounded operator $\mathcal{O}$. This implies that

$$\Lambda^\dagger_{\rho_{\text{fix}}}[\mathcal{O}] = \text{Tr}(\rho_{\text{fix}}\mathcal{O})\mathbb{1}_M \tag{15}$$

which is reminiscent of the completely depolarizing map. Then, the Choi matrix of the adjoint map is explicitly given by

$$\tau_{\rho_{\text{fix}}} = \mathbb{1}_Q \otimes \Lambda^\dagger_{\rho_{\text{fix}}}(|\psi^+\rangle\langle\psi^+|) = \frac{1}{d_Q}\sum_{ij}|i\rangle\langle j| \otimes \Lambda^\dagger_{\rho_{\text{fix}}}[|i\rangle\langle j|]$$

$$= \frac{1}{d_Q}\sum_{ij}\langle j|\rho_{\text{fix}}|i\rangle|i\rangle\langle j| \otimes \mathbb{1}_M = \frac{1}{d_Q}\rho_{\text{fix}}^T \otimes \mathbb{1}_M, \tag{16}$$

and so the assertion follows. ■

It is clear that choosing such a postprocessing and constructing such a squashing model is not very clever because one loses all useful data from the performed measurement and eventually winds up with a squashing model that produces only noise. Nevertheless, this tool turns out to be very useful in particular cases. In fact, as we will see now, Proposition 5 and Remark 6 together imply that a positive squashing map can always be found by introducing some amount of noise on the measurement data.

Theorem 7. Restoring theorem: Let $F_B^{(i)}$ and $F_Q^{(i)}$ be the basic and the target POVM elements of the corresponding measurement devices, respectively. Let τ be a Choi matrix, such that for classical postprocessing $\mathcal{P}$ the linear constraints in Eq. (13) are satisfied, but $\tau \ngeq 0$. Then, there exists a state ρ_{fix} and another postprocessing $\mathcal{P}'$ with intermediate amount of the added noise p, which provides a squashing map with the Choi matrix

$$\tau'(p) = (1-p)\tau + p\tau_{\rho_{\text{fix}}} \tag{17}$$

that is positive semidefinite whenever p and ρ_{fix} are chosen according to

$$\lambda_{\min}(\tau') \geqslant (1-p)\lambda_{\min}(\tau) + p\lambda_{\min}(\rho_{\text{fix}})/d_Q \geqslant 0. \tag{18}$$

Proof. First we note that due to Proposition 5, a completely noisy postprocessing exists that allows for a completely positive squashing map. Now, we look for an intermediate postprocessing that introduces less noise and where the corresponding Choi matrix is still positive. This intermediate postprocessing will be chosen as a probabilistic mixture of the postprocessing $\mathcal{P}$ and the noisy postprocessing $\mathcal{P}_{\text{noise}}$ from Proposition 5:

$$\mathcal{P}' = (1-p)\mathcal{P} + p\mathcal{P}_{\text{noise}}. \tag{19}$$

For the full measurement POVM elements, this implies

$$F_M'^{(i)} = (1-p)F_M^{(i)} + pF^{(i)}_{\text{noise},M}, \tag{20}$$

so that we can construct an adjoint of the squashing map

$$\Lambda'^\dagger\big[F_Q^{(i)}\big] = (1-p)\Lambda^\dagger\big[F_Q^{(i)}\big] + p\Lambda^\dagger_{\rho_{\text{fix}}}\big[F_Q^{(i)}\big]. \tag{21}$$

The choice of the ρ_{fix} is of crucial importance here. We choose ρ_{fix} to have a full rank, so that the eigenvalues of the Choi matrix in Eq. (16) are all strictly positive.

For $p = 1$, the squashing map Λ' is completely positive (Proposition 5). For the rest of the parameter values, we investigate the positivity of $\tau' = \mathbb{1}_Q \otimes \Lambda'^\dagger(|\psi^+\rangle\langle\psi^+|)$, which satisfies

$$\tau'(p) = (1-p)\tau + p\tau_{\rho_{\text{fix}}}$$

and where $\tau_{\rho_{\text{fix}}}$ is given explicitly by Eq. (16). Since the second term in the last equation is strictly positive, which is guaranteed by our choice of ρ_{fix} and Remark 6, there exists a value of p that is smaller than the trivial value $p = 1$ and for which we still find $\tau' \geqslant 0$ and therefore a nontrivial complete positive squashing map Λ'.

The amount of noise p that guarantees the positivity of τ' can be determined by comparing the minimal eigenvalue of τ (which is negative) and the minimal eigenvalue of ρ_{fix} (which is positive). It follows from one of Weyl's inequalities (see, for example, Chap. III.2 in Ref. [23]) that the minimum eigenvalue

of the sum of Hermitian matrices is lower bounded by the sum of the minimal eigenvalues of each term which implies the positivity condition in Eq. (18):

$$\lambda_{\min}(\tau') \geqslant (1-p)\lambda_{\min}(\tau) + p\lambda_{\min}(\rho_{\text{fix}})/d_Q \geqslant 0.$$

■

To close the section, we comment on the nontriviality of the map constructed in the last theorem. The existence of a positive $\tau'(p)$ for some $p < 1$ implies that there exists a CPP scheme that allows a physical map which preserves some quantum properties of the input state (a specific example will be given in Sec. VI C). This is especially important to know for applications such as verification of entanglement, which has, for example, applications as necessary conditions for QKD [24].

IV. REDUCTIONS FOR SQUASHING MODELS FOR LINEAR OPTICAL DEVICES WITH THRESHOLD DETECTORS

The description of a general linear optical measurement device, that is, a device in which input modes undergo a linear transformation before entering detectors, can be rather complicated. A full description should include several different degrees of freedom. For example, incoming light can consist of several spatially separated or overlapping wave packets with an arbitrary number of photons, each with its various polarization or frequency. However, we restrict our analysis to measurement devices that only respond to particular degrees of freedom. This means that they are invariant in their statistics with a change in degrees of freedom they do not measure. Specifically, in what follows, we consider measurement devices that can have different statistics given a change in photon number and polarization (Secs. V–VIII) or in time (see Sec. IX) or in photon number and relative phase between two spatial modes (Sec. X). This implies that these measurement devices are invariant under changes in all other degrees of freedom, such as frequency.

The existence of common attributes in optical measurement devices makes the application of the general framework discussed in the previous sections easier. The fact that one usually uses threshold detectors turns out to be especially helpful. As we will see shortly, this allows us to decompose the Hilbert space of the incoming signal and to construct the squashing map for N-photon input states for each $N = 0,1,2,3,\ldots$ independently. This will be the first reduction for the linear optical measurement devices.

In addition, we show that for a special type of basic and target measurements, there exists a particular CPP scheme that allows further decomposition in each of the N-photon subspaces that substantially simplifies the squashing-model analysis.

A. Quantum nondemolition (QND) measurements and N-photon subspaces

One essential trick in managing the analysis of squashing models connecting infinite-dimensional mode spaces to finite-dimensional target measurements consists of exploiting the fact that the basic POVM elements of linear optical measurement devices with threshold detectors commute with the POVM elements of the QND measurement of the total number of photons. This allows the reduction of the problem of analyzing input states on an infinite-dimensional Hilbert space to the problem of analyzing input states on an infinite number ($N = 0,1,2,3,\ldots$) of finite-dimensional Hilbert spaces independently. Formally, we can write

$$\text{QND} : \rho \mapsto \bigoplus_{N=0}^{\infty} \rho_N. \tag{22}$$

Based on what was laid out above, we can assume without loss of generality that the squashing map first performs a QND measurement of the total photon number, thus turning the input state into a block-diagonal form with respect to the photon-number subspaces. It implies that we can check for the existence of a squashing model for each subspace separately. An important note here is that a CPP scheme has to be fixed before we start to search for a squashing model on the infinite family of finite-dimensional Hilbert spaces. Each of these squashing models has to share a common CPP scheme.

All of the above can be summarized as follows.

Observation 8. Reduction 1, QND: For a linear optical measurement device with threshold detectors, any squashing map has a block-diagonal form with respect to the photon-number subspaces:

$$\Lambda[\rho] \overset{\text{QND}}{=} \Lambda\left[\bigoplus_{N=0}^{\infty} \rho_N\right] = \bigoplus_{N=0}^{\infty} \Lambda_N[\rho_N]. \tag{23}$$

Note that for any N, the map Λ_N is characterized by the same target measurement and its adjoint maps the target POVM elements onto the full measurement POVM elements projected onto the N-photon subspace. One immediate consequence of the QND measurement is the fact that one can split off the vacuum component and only consider states with $N \geqslant 1$. Indeed, for $N = 0$, one can always choose $\Lambda_0[\rho_0] = |\text{vac}\rangle_Q\langle\text{vac}|$, where $|\text{vac}\rangle$ is the vacuum state in the target Hilbert space. Therefore, the squashing map will output a vacuum state whenever the outcome of the QND measurement is zero and we can restrict ourselves to the case where $N \neq 0$:

$$\bigoplus_{N=0}^{\infty} \Lambda_N[\rho_N] = |\text{vac}\rangle_Q\langle\text{vac}| \oplus \bigoplus_{N=1}^{\infty} \Lambda_N[\rho_N]. \tag{24}$$

This will be referred to as the vacuum flag structure of the squashing map. Note that the map Λ_0 is applied if and only if the outcome of the QND measurement is 0. Later on in Sec. VII D we will become acquainted with another map, which outputs a vacuum state on the target Hilbert space, no matter what the input is. This "vacuum map" should not be confused with the vacuum flag, whose sole role is to split off the vacuum component of the signal.

B. Reduction for natural CPP schemes

For measurement devices with threshold photodetectors, for which the target measurement can be described as a restriction of the basic measurement to the single-photon subspace, the smart choice of a CPP scheme is such that the scheme does not affect the events which could have come from single-photon signals. These events are single clicks. Separating the single clicks from the rest of the events in this way will lead to a CPP scheme which assigns all multiclicks to some single clicks

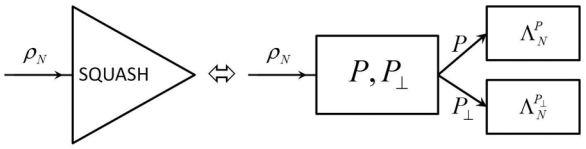

FIG. 3. Action of the squashing map for the special type of CPP scheme preserving the single-click events. The squashing map can be modeled as a photon-number measurement followed by a projective measurement onto a subspace spanned by the pure states that can trigger only single-click events. The number of such states does not depend on the photon number $N \geqslant 1$. Depending on the outcome of these measurements, one either proceeds with a low-dimensional squashing operation Λ_N^P or outputs a completely mixed qubit state.

without performing any operation on single-click outcomes, so that overall full measurement POVM elements are of the form

$$F_M^{(i)} = F_{B,\text{single}}^{(i)} + \sum_j \mathcal{P}_{ij} F_{B,\text{rest}}^{(j)}. \tag{25}$$

For generic linear optical devices, $F_{B,\text{single}}^{(i)}$ has a form of a rank-1 projector on some state $|\Psi_{B,\text{single}}^{(i)}\rangle$. If we denote a space spanned by single-click states by $P = \text{span}\{|\Psi_{B,\text{single}}^{(i)}\rangle\}$, then any state from its orthogonal complement $P_\perp$ triggers a multiclick with certainty. If the projection on P commutes with full measurement POVM elements, we can investigate the existence of the squashing map for P and $P_\perp$ separately. Schematically, this situation is represented in Fig. 3.

In summary we have the following observation.

Observation 9. Reduction 2: Single-click subspace: If a linear optical device with threshold photodetectors is such that

(i) the reduction of the basic POVM elements to a single-photon subspace provides target measurement POVM elements, and

(ii) the projection on the space P, spanned by the states that can trigger only single-click events, commutes with the full measurement POVM elements,

then there exists a CPP scheme that allows a decomposition of the squashing map of the form

$$\Lambda_N = \Lambda_{P,N} + \Lambda_{P_\perp,N}. \tag{26}$$

Both $\Lambda_{P,N}$ and $\Lambda_{P_\perp,N}$ map N-photon states to states on the same target Hilbert space and fulfill the same set of linear constraints.

V. SQUASHING MODEL FOR A MEASUREMENT DEVICE USED IN THE BB84 QKD PROTOCOL

In this section, we consider a measurement device which is used in the optical implementation of the most prominent QKD protocol: the BB84 protocol [1]. This device has been introduced in Ref. [10] as a standard example used to introduce squashing models. We start off by providing a short background on the measurement device in the BB84 QKD protocol, where an observer actively makes the choice of the measurement basis.

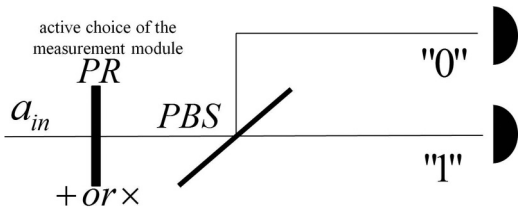

FIG. 4. Active detection scheme. The observer possesses two detector modules and a polarization rotator, which is used to actively choose one or the other detector module. The detector modules are made up of polarizing beam splitters that are able to discriminate two orthogonal linearly polarized modes and ideal threshold detectors for each mode.

A. Active detection scheme for the BB84 measurement

In the active detection scheme for the BB84 measurement, the observer has two detector modules, each adjusted to one of the polarization bases α (see Fig. 4). Before the measurement is performed, one has to decide which detector module will be used. This represents the active nature of the detection scheme.

Note that there is no notion of an *a priori* probability distribution that governs the choice of the measurement basis yet, i.e., the observer has no classical "coin" at his disposal and therefore no randomness for the basis choice. A measurement with such randomness will be discussed in Sec. VII A.

Each detector module is a polarization analyzer and consists of two detectors monitoring two outputs of a polarizing beam splitter, which is able to discriminate between two orthogonal polarizations of linearly polarized light. In every measurement, the observer will register four different events: no click (vac), single-click (sc) in one of the detectors, and two different double clicks (dc), when both detectors ("0" and "1") fire. Assuming ideal threshold detectors, no photon losses and no dark counts, the observed events are described by the following POVM elements:

$$\begin{aligned} F_{\text{vac}} &= \sum_{\alpha=+,\times} |0,0\rangle_\alpha\langle 0,0|, \\ F_{\text{sc}}^{i,\alpha} &= \sum_{N=1}^{\infty} |N\rangle_{i,\alpha}\langle N|, \\ F_{\text{dc}}^{\alpha} &= \sum_{N_0,N_1=1}^{\infty} |N_0,N_1\rangle_\alpha\langle N_0,N_1|, \end{aligned} \tag{27}$$

where $|N\rangle_{i,\alpha}$ denotes a state with N photons in the mode i of the α-polarized *incoming* light (cf. Ref. [5]). Note that for each choice of α, one has a *complete set* of POVM elements and *no* classical probability that may describe the basis choice.

B. BB84 measurement: Reduction of the squashing model

We start off by defining target POVM elements. These correspond to a measurement on zero- and single-photon Hilbert spaces and are given by [cf. Eq. (27)]

$$\begin{aligned} F_{\text{vac}} &= \sum_{\alpha=+,\times} |0,0\rangle_\alpha\langle 0,0|, \\ F_1^{(0,\alpha)} &= |1,0\rangle_\alpha\langle 1,0|, \\ F_1^{(1,\alpha)} &= |0,1\rangle_\alpha\langle 0,1|, \end{aligned} \tag{28}$$

where $\alpha \in \{+,\times\}$ is a label for the basis choice of the polarizing beam splitter.

For a general input state, we apply reductions from Sec. IV in order to reduce the problem. First, in virtue of what is discussed in Sec. IV A, we consider an input state of the BB84 measurement device that contains N photons and by using the flag structure of the vacuum events, we split off the vacuum component. This also simplifies the target space and makes it a space of a qubit with the following POVM elements:

$$F_1^{(0,\alpha)} = |1,0\rangle_\alpha\langle 1,0|, \quad F_1^{(1,\alpha)} = |0,1\rangle_\alpha\langle 0,1|. \tag{29}$$

Second, the target POVM elements [Eq. (29)] are restrictions of the general basic POVM elements to the single-photon subspace. Therefore, we can apply the results of Sec. IV B and choose a CPP scheme that does not affect the single clicks in order to be able to decompose Λ_N into $\Lambda_{P,N}$ and $\Lambda_{P_\perp,N}$.

To perform this decomposition, we fix the CPP scheme by randomly (with equal probability) assigning each of the double-click events to a single-click event within the same basis. It follows directly from Eq. (27) that the full measurement POVM elements on the N-photon subspace are

$$\begin{aligned} F_N^{(b,\alpha)} &= F_{\mathrm{sc},N}^{(b,\alpha)} + \frac{1}{2}F_{\mathrm{dc},N}^{\alpha} \\ &= \frac{(-1)^b}{2}(|N,0\rangle_\alpha\langle N,0| - |0,N\rangle_\alpha\langle 0,N|) + \frac{\mathbb{1}_N}{2}, \end{aligned} \tag{30}$$

where $b \in \{0,1\}$ corresponds to the 0 or 1 outcome of the detection module, and $|l,k\rangle_\alpha$ is a two-mode Fock state with photon numbers l and k with respect to the polarization mode basis α. It is straightforward to see that the restriction of these elements to the $N = 1$ subspace exactly reproduces the target POVM elements.

Now, we see that the full measurement POVM elements in Eq. (30) have the same structure of the POVM elements in Eq. (25). Moreover, projections on the spaces $P = \mathrm{span}\{|N,0\rangle_\alpha, |0,N\rangle_\alpha\}_{\alpha=+,\times}$ and $P_\perp$ commute with the full measurement POVM elements and therefore we can apply Observation 9 in order to search for a squashing map in P and $P_\perp$ separately.

C. BB84 measurement: Positivity of the squashing map

For any $N \geqslant 1$ we can choose $\Lambda_{P_\perp,N}$ to be a trivial map $\Lambda_{\varrho_{\mathrm{fix}}}$ from Proposition 5 and the choice $\varrho_{\mathrm{fix}} = \mathbb{1}_Q/2$. This is in accordance with the chosen CPP scheme, i.e., the probability condition in Eq. (3) is fulfilled. Thus, we have determined the squashing map on the space $P_\perp$ and all that is left to find is a squashing map for the subspace P, whose dimension in this case does not exceed 4 (it is 2 for $N = 1$, 3 for $N = 2$, and 4 for $N \geqslant 3$).

As we mentioned in Sec. III, we need two ingredients for this: (i) we need to construct a linear map preserving linear dependencies as in Eq. (8) and (ii) we need this map to be completely positive.

We start off by writing the linear constraints, which are respected by the chosen CPP scheme,

$$\Lambda_{P,N}^\dagger\left[F_1^{(b,\alpha)}\right] = F_{P,N}^{(b,\alpha)}, \quad \alpha \in \{+,\times\} \tag{31}$$

where $F_1^{(b,\alpha)}$ are the target measurement POVM elements as in Eq. (29) and $F_{P,N}^{(b,\alpha)}$ are the full measurement POVM elements restricted to the subspace P. Using Eqs. (29) and (30), it is not hard to see that the linear dependencies are satisfied:

$$F_1^{(0,\alpha)} + F_1^{(1,\alpha)} = \mathbb{1}_Q \Leftrightarrow F_{P,N}^{(0,\alpha)} + F_{P,N}^{(1,\alpha)} = \mathbb{1}_{P,N}, \forall\, \alpha. \tag{32}$$

Therefore, there exists a linear map $\Lambda_{P,N}^\dagger$ as in Eq. (31).

The complete positivity of $\Lambda_{P,N}^\dagger$ is proven by directly checking the non-negativity of the Choi matrix. First, we use the decomposition of the maximally entangled state in terms of Pauli matrices

$$|\psi^+\rangle\langle\psi^+| = \frac{1}{4}\left(\mathbb{1}_Q \otimes \mathbb{1}_Q + \sum_{\alpha=x,y,z} \sigma_\alpha^T \otimes \sigma_\alpha\right). \tag{33}$$

Therefore, the Choi matrix is given explicitly by

$$\begin{aligned} \tau_{P,N} &= \mathbb{1} \otimes \Lambda_{P,N}^\dagger(|\psi^+\rangle\langle\psi^+|) \\ &= \frac{1}{4}\left(\mathbb{1}_Q \otimes \mathbb{1}_M + \sum_{\alpha=x,y,z} \sigma_\alpha^T \otimes \Lambda_{P,N}^\dagger(\sigma_\alpha)\right). \end{aligned} \tag{34}$$

Second, we note that the Pauli matrices σ_x and σ_z can be written in terms of the target POVM elements: $\sigma_\alpha = F_1^{(0,\alpha)} - F_1^{(1,\alpha)}$, $\alpha = x,z$. The action of the $\Lambda_{P,N}^\dagger$ on σ_y, however, is not fixed by our linear constraints and we can use this freedom in order to enforce the positivity of the Choi matrix $\tau_{P,N}$.

For the upcoming discussion, it is convenient to decompose $\tau_{P,N} = \tau_{P,N,\mathrm{fix}} + \tau_{P,N,\mathrm{open}}$, with

$$\tau_{P,N,\mathrm{open}} = \sigma_y^T \otimes \Lambda_{P,N}^\dagger(\sigma_y). \tag{35}$$

In order to check the positivity of $\tau_{P,N}$, we will consider its matrix representation $M(\tau_{P,N})$ using the nonorthogonal basis vectors

$$\{|\psi_i\rangle \otimes |j\rangle\}_{j=0,1}, \quad |\psi_i\rangle \in \{|N,0\rangle_\alpha, |0,N\rangle_\alpha\}_{\alpha=+,\times}. \tag{36}$$

The matrix $M(\tau_{P,N,\mathrm{fix}})$ only has real entries [its explicit form is given by Eq. (C1)]. The properties of the matrix $M(\tau_{P,N,\mathrm{open}}) = \sigma_y^T \otimes M(\Lambda_{P,N}^\dagger(\sigma_y))$ can be specified further: first, without loss of generality, we can assume that $M(\tau_{P,N,\mathrm{open}})$ only has real entries. If there exists a complex solution $M(\tau_{P,N,\mathrm{open}})$ for $M(\tau_{P,N,\mathrm{fix}}) + M(\tau_{P,N,\mathrm{open}}) \geqslant 0$, then its complex conjugate is also a solution. Then, by linearity the equal weighted average is also a solution and it is a real matrix. Second, since the open part $\tau_{P,N,\mathrm{open}}$ is Hermitian (otherwise the Choi matrix would have complex eigenvalues), we can write $M(\Lambda_{P,N}^\dagger(\sigma_y)) = iS$ where S is some skew-symmetric matrix with six real entries as free parameters. These free parameters can be found such that $M(\tau_{P,N}) \geqslant 0$ holds [see Eq. (C3)]. Therefore, there exists a positive $\tau_{P,N}$ which maps the specified target measurements to the corresponding full measurements.

This implies that there is a squashing map on the space P, which is completely positive and fulfills the linear constraints in Eq. (31). As pointed out above, the squashing map on the complementary space $P_\perp$ also exists. Therefore, for the choice of the classical postprocessing we made, we provided a squashing map for the target measurement in Eq. (29).

This squashing map has been found also by Tsurumaru and Tamaki [11].

In summary in this section, we proved the following.

Theorem 10. Squashing model for BB84 measurement with active basis choice: There exists a squashing model with the qubit target measurement for the BB84 measurement with active basis choice and random equiprobable assignment of double clicks to one of the outcomes (i.e., independent from how often one decides to choose one or the other basis).

VI. ACTIVE DETECTION SCHEME FOR A SIX-STATE MEASUREMENT

In this section, we will focus on a squashing model for a measurement device which is used in optical implementations of the six-state QKD protocol [25]. The six-state measurement is similar to the BB84 measurement, except that there is a third setting to the polarizing beam splitter which splits photons according to a circular basis (labeled as y). The measurement basis is chosen actively by the observer.

A. Six-state measurement: Reduction of the squashing model

In full analogy to the BB84 measurement, we want to make use of the reductions in Sec. IV. First of all, we reduce the problem and consider N-photon incoming signals for $N = 1,2,\ldots$. For the six-state measurement device, we choose the target measurement to be a measurement on the zero- and single-photon Hilbert spaces. After splitting off the vacuum component, the target POVM elements are

$$F_1^{(0,\alpha)} = |1,0\rangle_\alpha\langle 1,0|, \quad F_1^{(1,\alpha)} = |0,1\rangle_\alpha\langle 0,1|, \tag{37}$$

with $\alpha \in \{x,y,z\}$.

As with the BB84 measurement, these POVM elements are restrictions of the basic POVM elements, which suggests to choose the same type of classical postprocessing as we did for the BB84 protocol: the postprocessing of double-click events is randomly assigned again to either single-detection events. The probabilities of the "0" and "1" assignments are equal: $p = \frac{1}{2}$. This CPP scheme fixes the full measurement POVM elements to

$$F_N^{(b,\alpha)} = \frac{(-1)^b}{2}(|N,0\rangle_\alpha\langle N,0| - |0,N\rangle_\alpha\langle 0,N|) + \frac{\mathbb{1}_N}{2}. \tag{38}$$

This CPP scheme allows us to apply the second reduction and restrict our search to a six-dimensional subspace P spanned by $\{|N,0\rangle_\alpha, |0,N\rangle_\alpha\}$, $\alpha = x,y,z$, and its complement $P_\perp$. Similarly to the active BB84 measurement, the projections onto P and $P_\perp$ commute with the full measurement POVM elements in Eq. (38).

B. Six-state measurement: Squashing map

The linear constraints on the squashing map in the six-dimensional subspace P are given by

$$\Lambda_{P,N}^\dagger\left[F_1^{(b,\alpha)}\right] = F_{P,N}^{(b,\alpha)}, \quad \alpha \in \{x,y,z\}. \tag{39}$$

In this case, one can follow the calculation for the BB84 protocol. The only difference is that the matrix $\tau_{P,N}$, that represents the squashing map, is completely determined by the linear constraints since the measurement operators $F_1^{(b,\alpha)}$ form a complete basis for their Hilbert space. However, it can be easily seen that $\Lambda_{P,N}$ can not be positive. First, we can write the adjoint squashing map $\tau_{P,N} = \mathbb{1} \otimes \Lambda_{P,N}^\dagger(|\psi^+\rangle\langle\psi^+|)$ as before. Since the qubit measurements of the six-state protocol are complete, we can write

$$\begin{aligned}\tau_{P,N} &= \mathbb{1} \otimes \Lambda_{P,N}^\dagger(|\psi^+\rangle\langle\psi^+|) \\ &= \frac{1}{4}\left(\mathbb{1}_Q \otimes \mathbb{1}_{P,N} + \sum_{\alpha=x,y,z} \sigma_\alpha^T \otimes \left(F_{P,N}^{(0,\alpha)} - F_{P,N}^{(1,\alpha)}\right)\right).\end{aligned} \tag{40}$$

As in the BB84 case, we can directly apply $\Lambda_{P,N}^\dagger$ to the second subsystem that does the map $F_1^{(b,\alpha)} \mapsto F_{P,N}^{(b,\alpha)}$. In this case, the Choi matrix $\tau_{P,N}$ is completely fixed and has no free parameters since the linear constraints in Eq. (39) have to be respected.

However, the matrix $\tau_{P,N}$ has negative eigenvalues. By writing $\tau_{P,N}$ in a basis of nonorthogonal vectors, which is analogous to that for the BB84 measurement device in Eq. (36),

$$\{|\psi_i\rangle \otimes |j\rangle\}_{j=0,1}, \quad |\psi_i\rangle \in \{|N,0\rangle_\alpha, \quad |0,N\rangle_\alpha\}_{\alpha=x,y,z}, \tag{41}$$

we can calculate the minimum eigenvalues directly. For example, in the three-photon subspace, the state

$$|\theta_-\rangle = \frac{1}{\sqrt{2}}(|3,0\rangle_z \otimes |1\rangle - |0,3\rangle_z \otimes |0\rangle) \tag{42}$$

has the property that $\langle\theta_-|\tau_3|\theta_-\rangle < 0$, which obviously violates the positivity condition of the squashing map. Therefore, we conclude that for the choice of the classical postprocessing we made there is no complete positive squashing map onto target measurement given by Eq. (37).

C. Alternative classical postprocessing and completely positive squashing map

As we mentioned in Sec. III D, the lack of complete positivity of the squashing map is not always a big obstacle and can be overcome by introducing some additional noise to the measurement data. This is done by choosing another CPP scheme. We will apply this trick for the six-state active measurement device and show that the amount of noise one needs to introduce is tolerable in QKD implementations.

We start by describing an alternate classical postprocessing. This will be a mixture of the old postprocessing and the completely noisy postprocessing that corresponds to the random assignment of an outcome regardless of which basic event occurred [cf. Eq. (19)]. For this type of postprocessing, there is a positive squashing map $\Lambda_{\varrho_{\text{fix}}}$ with $\rho_{\text{fix}} = \mathbb{1}_Q/2$ (cf. Theorem 7 and Remark 6).

We use Eq. (17) with $d_Q = 2$ and $\rho_{\text{fix}} = \mathbb{1}_Q/2$ to achieve the Choi matrix for squashing map

$$\tau_{P,N,\text{new}}(p) = (1-p)\tau_{P,N} + \frac{p}{4}\mathbb{1}_Q \otimes \mathbb{1}_{P,N}, \tag{43}$$

where $\tau_{P,N}$ is from Eq. (40). In order to check the positivity of $\tau_{N,\text{new}}(p)$, we can again represent it in the basis of Eq. (41) as a 12×12 matrix of the parameters N and p, and show the positivity of its eigenvalues for $p \geqslant \frac{1}{3}$. The proof is given in Appendix D.

Next, we point out a connection between the parameter p and an additional penalty bit-error rate e in the six-state protocol, which one needs to introduce in order to ensure the positivity of the squashing map.

Remark 11. Connection between white-noise parameter and bit-error rate: The white-noise parameter p corresponds to the double-bit-error rate which one needs to introduce as a penalty for a positive squashing map to exist. That is, $p = 2e$.

Proof. The essential point for this is the fact that for the old full measurement POVMs we have

$$F^{(0,\alpha)}_{N,\text{old}} + F^{(1,\alpha)}_{N,\text{old}} = \mathbb{1}_N. \tag{44}$$

Substituting this equation in Eq. (43) will result in

$$\begin{aligned} F^{(0,\alpha)}_{N,\text{new}} &= (1 - p/2)F^{(0,\alpha)}_{N,\text{old}} + \frac{p}{2}F^{(1,\alpha)}_{N,\text{old}}, \\ F^{(1,\alpha)}_{N,\text{new}} &= (1 - p/2)F^{(1,\alpha)}_{N,\text{old}} + \frac{p}{2}F^{(0,\alpha)}_{N,\text{old}}. \end{aligned} \tag{45}$$

This relates the full measurement POVM elements after additional noisy postprocessing to the elements before the postprocessing. This relation concerns one particular measurement basis and can be interpreted as an additional bit flip with probability $e = p/2$ after all double clicks have been assigned. ■

It follows from the last remark that we need to add 16.67% of noise to our data in order for the squashing map of the six-state protocol to be completely positive. To summarize, we showed that the following statement holds.

Theorem 12. Squashing model for six-state measurement with active basis choice: There exists a squashing model with a qubit target measurement for the six-state measurement with active basis choice (no matter how often one chooses to measure in one of the three bases) for the CPP scheme that randomly (with equal probability) assigns the double clicks to single clicks and flips the single click bit values with probability $\frac{1}{6}$.

To conclude this section, we point out that the recent results by Ma and Lütkenhaus [26] allow us to say that this penalty error rate only needs to be used to estimate the amount of privacy amplification necessary for the protocol. As a matter of fact, we do not actually need to flip any bits and can therefore effectively reduce the amount of information leaking to the eavesdropper. In this case, the squashing model can be used for the protocol with one-way classical communication and one can provide a secret key rate for an error rate up to 6.43% if one uses the infinite-key-limit formula $r = 1 - h(Q) - I_E(Q')$ [see Eq. (A6) in Ref. [27]] with $Q' = (1 - p_{\text{flip}})Q + p_{\text{flip}}(1 - Q)$, where Q is a bit-error rate and p_{flip} the flip probability from Theorem 12.

VII. EXTENSIONS OF SQUASHING MODELS, BIASED ACTIVE BB84 MEASUREMENT, PASSIVE BB84 AND SIX-STATE MEASUREMENTS

This section is devoted to several generalizations of the ideas that were laid out in Secs. IV–VI. First, we investigate a biased active BB84 measurement. Then, we turn our attention to the passive detection scheme (defined below) for the BB84 and six-state measurement devices. Such devices are also often used in practical implementations of QKD protocols, which is often motivated by the fact that a passive detection scheme requires fewer random bits and typically allows higher clock rates (see, e.g. [28,29]).

A. Biased active BB84 measurement

We start off by generalizing the squashing model for the BB84 measurement to a device where the observer chooses the measurement basis according to classical probabilities p_+ and $p_\times$ such that $p_+ + p_\times = 1$. That is, the active "at will" choice of the observer is replaced by a random number generator. This will result only in a coefficient in front of the POVM elements in Eq. (27):

$$\begin{aligned} F_{\text{vac}} &= \sum_{\alpha=+,\times} p_\alpha |0,0\rangle_\alpha\langle 0,0|, \\ F^{i,\alpha}_{\text{sc}} &= p_\alpha \sum_{N=1}^{\infty} |N\rangle_{i,\alpha}\langle N|, \\ F^{\alpha}_{\text{dc}} &= p_\alpha \sum_{N_0,N_1=1}^{\infty} |N_0,N_1\rangle_\alpha\langle N_0,N_1|, \end{aligned} \tag{46}$$

and will not affect the rest of the argument we made in Sec. V. Therefore, we have the following theorem.

Theorem 13. Squashing model for biased active BB84 measurement: There exists a squashing model for the biased active BB84 measurement for which the basis choice is made according to classical probabilities p_+ and $p_\times$ such that $p_+ + p_\times = 1$.

B. Passive detection scheme for the BB84 measurement

In this section, we will present the details for the passive BB84 measurement. The passive six-state measurement can then be generalized straightforwardly. In the passive BB84 measurement, the observer uses a measurement device presented in Fig. 5. The whole measurement device consists of two detection modules that correspond to two detection bases. Both detection modules are positioned at the two output ports of a 50:50 beam splitter. This measurement outputs a bit value and a basis choice.

Interestingly, this type of detection scheme is more sensitive to the signals containing more than one photon. Indeed, because of the 50:50 beam splitter [cf. Eq. (B2)] the POVM

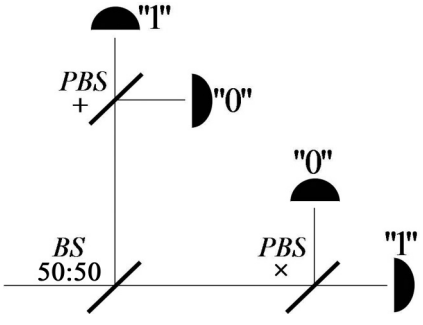

FIG. 5. The device for the passive BB84 measurement. Here, it consists of two detection modules, located at the output ports of a 50:50 beam splitter. Each detection module corresponds to one of the polarization bases.

elements will take the form (see also [5])

$$F_{\text{vac}} = \frac{1}{2}\sum_{\alpha=+,\times} |0,0\rangle_\alpha\langle 0,0|,$$
$$F_{\text{sc}}^{i,\alpha} = \sum_{N=1}^{\infty}\left(\frac{1}{2}\right)^N |N_i\rangle_\alpha\langle N_i|, \quad i=0,1 \tag{47}$$

$$F_{\text{dc}}^{\alpha} = \frac{1}{2}\sum_{N_0,N_1=1}^{\infty} |N_0,N_1\rangle_\alpha\langle N_0,N_1|,$$
$$F_{\text{cc}} = \frac{1}{2}\mathbb{1} + \sum_{\substack{\alpha=+,\times\\ i=0,1}}\sum_{N=1}^{\infty}\left(1-\frac{1}{2^N}\right)|N\rangle_{i,\alpha}\langle N|, \tag{48}$$

where "sc," "dc," and "cc" denote single clicks, double clicks within the same detection module, and cross clicks between different modules, respectively.

C. Relation between active and passive measurement devices via switching

A closer comparison of Figs. 4 and 5 reveals an important relationship between the two detection schemes. First note that the single-click POVM elements are the same (up to an N-dependent coefficient) for both detection schemes. As we will see shortly, this can be crucial for the positivity of the squashing map. In fact, an active detection scheme can be generally represented as a part of the passive detection scheme with a beam splitter which acts as a probabilistic classical switch.

Indeed, the initial beam splitter is only rerouting all photons in one direction or the other direction or splitting up the photons. So, we can think of it like a classical switch which either decides between the two polarization bases like in an active scheme, or splits up the photons thus creating cross clicks. The probability for the first two cases is the same, so we can combine them into the problem of active detection in Fig. 6. Therefore, we can think of the passive detection scheme as of a scheme consisting of two parts: with probability $p(N)$ the system chooses to apply an active detection setup, and with probability $1-p(N)$ the system chooses to create a cross

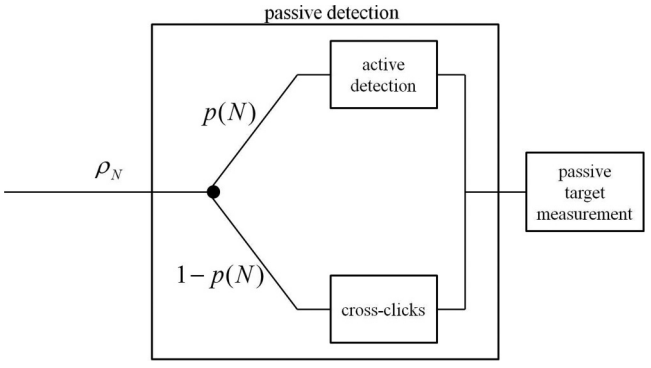

FIG. 6. Active detection scheme as a part of the passive detection scheme. Any passive detection that is due to an input beam splitter can be thought of as a switching between active detection and a cross click. The probability of switching depends only on the number of photons N entering the measurement device.

click. To give an example, for the passive BB84 measurement in Fig. 5 we have $p(N) = \frac{1}{2^N} + \frac{1}{2^N} = \frac{1}{2^{N-1}}$. As we will see now, this structure turns out to be very useful for the construction of squashing models and especially for choosing the right CPP scheme for passive detection devices.

D. Squashing model for the passive BB84 measurement

According to the previous section, we can rely on our knowledge of the active detection scheme and consider the cross-click events separately. As it turns out, since there exists a squashing model for the active detection scheme (see Sec. V), we can either discard all cross clicks or assign them to some bit value with some probability.

To be more precise, let us define two different CPP schemes for the part of the squashing model that deals only with cross clicks (cf. Fig. 6) and hence leads to two different overall squashing maps

$$\Lambda_{N,\text{passive}}^{\text{discard}} = \frac{1}{2^{N-1}}\Lambda_{N,\text{active}} + \left(1-\frac{1}{2^{N-1}}\right)\Lambda_{\text{vac}},$$
$$\Lambda_{N,\text{passive}}^{\text{keep}} = \frac{1}{2^{N-1}}\Lambda_{N,\text{active}} + \left(1-\frac{1}{2^{N-1}}\right)\Lambda_{\mathbb{1}_Q/2}, \tag{49}$$

where the vacuum map Λ_{vac} disregards the input and forwards a vacuum state to the target measurement [not to be confused with the vacuum flag (see the closing remark in Sec. IV A)]. We refer to $\Lambda_{N,\text{passive}}^{\text{discard}}$ as the squashing map corresponding to the overall postprocessing that discards all cross clicks and we refer to $\Lambda_{N,\text{passive}}^{\text{keep}}$ as the squashing map that corresponds to the CPP scheme with random (in this case with equal probabilities, because of the passive target measurement) assignment of cross clicks. Note that in principle we can choose the assignment of cross clicks according to some other (nonuniform) probability distribution. It will only mean that we would need to change ρ_{fix} in $\Lambda_{\rho_{\text{fix}}}$ accordingly, but it will not affect the positivity of the squashing map, as long as ρ_{fix} corresponds to a physical state.

Finally, the positivity of both passive maps in Eq. (49) for the BB84 case follows from the positivity of the maps on the right-hand side of Eq. (49), which is in contrast to the six-state measurement considered in the next section. To summarize, we have the following theorem.

Theorem 14. Squashing model for the passive BB84 measurement: For the passive BB84 measurement, there is a squashing model with a qubit target measurement no matter what the classical postprocessing of the cross clicks is, as long as there is a squashing model with a qubit target measurement for cross-click events.

E. Passive six-state measurement

For the six-state measurement device with the passive detection scheme, we can use the same argument as we did in the last section for the BB84 measurement device. Here, however, we can not rely on the positivity of the squashing map for the active part of the model because as we learned in Sec. VI the map is not completely positive. In virtue of this we can not simply discard all cross clicks and we have to fall back to their random assignment. We still will be using the

map $\Lambda_{N,\text{active}}$, although it is not physical, as a tool to show the complete positivity of the overall map (see following).

Assuming that we assign cross clicks with equal probabilities, we have the overall squashing map of the type

$$\Lambda^{\text{keep}}_{N,\text{passive}} = \frac{1}{3^{N-1}}\Lambda_{N,\text{active}} + \left(1 - \frac{1}{3^{N-1}}\right)\Lambda_{\mathbb{1}_Q/2}. \quad (50)$$

The positivity of this squashing map will be, as per usually, investigated in terms of its Choi matrix:

$$\tau^{\text{keep}}_{N,\text{passive}} = \frac{1}{3^{N-1}}\tau_{N,\text{active}} + \left(1 - \frac{1}{3^{N-1}}\right)\frac{\mathbb{1}_Q \otimes \mathbb{1}_N}{4}. \quad (51)$$

Note that the chosen CPP scheme allows us to apply Reduction 2 here (Observation 9) and consider the Choi matrix only on the single-click subspace P: $\tau_{P,N,\text{passive}}$. The positivity of $\tau_{P,N,\text{passive}}$ was discussed in Eq. (43) where we concluded that this matrix is positive whenever $p(N) = 1 - 1/3^{N-1}$ and takes values $p(N) \in [1/3, 1]$, which is the case for any $N \geqslant 2$. Therefore, all eigenvalues are positive and we have shown the following.

Theorem 15. Squashing model for the passive six-state measurement: For the passive six-state measurement device there exists a squashing model if the classical postprocessing randomly assigns (with equal probability) the double clicks to a bit value within the same basis where the double click has occurred, and assigns the cross clicks randomly (with equal probability) to one of the possible bit values.

VIII. PASSIVE MULTISTATE QUDIT MEASUREMENT DEVICE FOR PRIME-DIMENSIONAL HILBERT SPACES

In the previous section, we discussed squashing models for measurement devices for which it was self-evident to choose a qubit measurement as the target measurement. A possible way to generalize the results of Secs. V and VI is to consider a qudit measurement device as the target instead. Here, we present a general result for the passive detection scheme in the case of a qudit target measurement, with d being a prime number. Note that we only consider passive devices since this generalization includes the six-state measurement device, for which an active choice does not work (see Sec. VI). We will be setting the stage by recapitulating some known facts about mutually unbiased bases (MUBs), and the reader who is familiar with this notion can skip the next section without losing the thread of the paper.

A. Background on mutually unbiased bases

First, we recall the definition of MUBs.

Definition 16. MUB: Let $\{|\psi_1\rangle \ldots |\psi_d\rangle\}$ and $\{|\phi_1\rangle \ldots |\phi_d\rangle\}$ be two orthonormal bases in the Hilbert space $\mathbb{C}^d$. These bases are called *mutually unbiased* if

$$|\langle\psi_i|\phi_j\rangle| = \frac{1}{\sqrt{d}}, \quad \forall\, i,j. \quad (52)$$

The existence of a $d+1$ MUB, if d is a prime number, was proven in Ref. [30]. The proof is constructive. Each basis consists of the eigenvectors of

$$Z_d, X_d, X_d Z_d, X_d (Z_d)^2, \ldots, X_d (Z_d)^{d-1}, \quad (53)$$

where Z_d and X_d are generalized Pauli matrices with the properties

$$Z_d|j\rangle = w^j|j\rangle, \quad X_d|j\rangle = |(j+1) \bmod d\rangle, \quad (54)$$

where ω is the dth root of unity. The basis of Z_d is referred to as the standard basis. It is possible to represent all other matrices in Eq. (53) in terms of the standard basis. This gives an explicit relationship between different bases representations

$$\begin{aligned} Z_d^k &= \sum_{i=0}^{d-1} \omega^{ik} |1\rangle_{i,0}\langle 1|, \\ \left(X_d Z_d^\alpha\right)^k &= \sum_{i=0}^{d-1} \omega^{\alpha k[i+\frac{1}{2}(k-1)]} |1\rangle_{i+k,0,i}\langle 1| \\ &= \sum_{i=0}^{d-1} \omega^{ik} |1\rangle_{i,\alpha+1}\langle 1|, \end{aligned} \quad (55)$$

where $\alpha = 0, \ldots, d-1$.

One more fact that we will be using quite often is that the operators

$$Z_d^\alpha, \left(X_d Z_d^\alpha\right)^k, \quad \alpha = 0, \ldots, d-1, \quad k = 1, \ldots, d-1 \quad (56)$$

form a basis in the space of all operators acting on the Hilbert space of a qudit $\mathcal{B}(\mathcal{H}_d)$.

B. Description of the measurement device: Basic measurement

The measurement device for the multistate protocol is schematically represented in Fig. 7. It measures in $d+1$ different polarization bases. For each basis there are d different polarization states that are detected by one of d threshold photodetectors in a corresponding detection module $\mathcal{M}_\alpha$, $\alpha = 0, \ldots, d$. Note that the described measurement device contains the passive six-state measurement, if one assigns $p_\alpha = \frac{1}{3}$ for $\alpha \in \{x, y, z\}$.

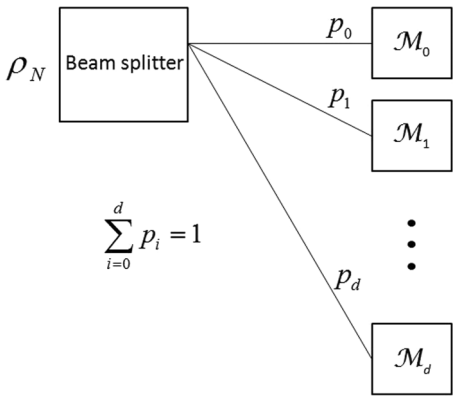

FIG. 7. Scheme of the measurement device for the qudit QKD protocol (where d is a prime number). After passing the input beam splitter, which distributes the signals into $d+1$ arms with probabilities p_α with $\alpha = 0, \ldots, d$, the input state is measured in one of the $d+1$ mutually unbiased bases. Each basis measurement contains d different threshold photodetectors corresponding to d different polarization states within the basis α. There are $d(d+1)$ polarization states in total.

From now on, we will consider the situation where $p_\alpha = 1/(d+1)$ for all $\alpha = 0,\ldots,d$ (possible generalizations will be considered in the closing part, VIII E, of this section). Since our measurement device contains threshold photodetectors, we can perform a QND measurement of the number of photons and split off the vacuum component first (see Observation 8). Hence, we can restrict ourselves to inputs containing $N \geqslant 1$ photons. In the N-photon subspace, the basic POVM elements have the following form (see Appendix E for more details):

$$\begin{aligned} F_N^{i,\alpha} &= (d+1)^{-N}|N\rangle_{i,0}\langle N|, \\ F_{\mathrm{mc},N}^{\alpha} &= (d+1)^{-N}\left(\mathbb{1}_N - \sum_{i=1}^{d}|N\rangle_{i,0}\langle N|\right), \\ F_{\mathrm{cc},N} &= \left(1 - \frac{1}{(d+1)^{N-1}}\right)\mathbb{1}_N, \end{aligned} \tag{57}$$

with $i = 1,\ldots,d$ and $|N\rangle_{i,\alpha}$ is adopted to describe an event of the detection of N photons in the detector i of the detection module $\mathcal{M}_\alpha$. From the structure of the basic POVM elements, it is evident that we have to distinguish between multiclicks (mc) $F_{\mathrm{multi},N}$ and cross clicks (cc) $F_{\mathrm{cc},N}$. The multiclicks happen when different detectors within the same detection module (i.e., the same basis choice) have a click and is a generalization of a double click for $d = 2$. Cross clicks occur when several detectors in at least two different measurements modules (two different bases) have a click.

C. Target measurement, classical postprocessing, and full measurement

The target POVM elements can be easily deduced when we restrict to a single-photon input state [note the analogy to Eq. (37) for the six-state measurement]:

$$F_1^{i,\alpha} = \frac{1}{d+1}|1\rangle_{i,0}\langle 1|, \quad \alpha = 0,\ldots,d; \quad i = 0,\ldots,d-1. \tag{58}$$

It is not hard to see that the target POVM elements are single-photon restrictions of the basic POVM elements in Eq. (57). Therefore, we choose a CPP scheme that does not affect single-click basic POVM elements. Following the same lines as the BB84 and the six-state squashing models, we choose the CPP scheme as follows:

(i) Single clicks are mapped to the same single clicks.

(ii) Multiclicks are assigned equally randomly to one of the $d$it values in the same module $\mathcal{M}_\alpha$.

(iii) Cross clicks are assigned with probability $1/d(d+1)$ to one of the outcomes of the measurement $\mathcal{M}_\alpha$.

The chosen CPP scheme and Eq. (57) imply the following form of the full POVM measurement elements:

$$\tilde{F}_N^{i,\alpha} = F_N^{i,\alpha} + \frac{1}{d}F_{\mathrm{mc},N}^{\alpha} + \frac{1}{d(d+1)}F_{\mathrm{cc},N}. \tag{59}$$

D. Positivity of the squashing map Λ_N

To start off, we note that the chosen postprocessing scheme allows us to use the results of Sec. IV B and precede the squashing map by a projection on the $d(d+1)$-dimensional space $P = \mathrm{span}\{|N_i\rangle_\alpha\}$ because the projection on this space commutes with full measurement POVM elements (Observation 9).

All states in the orthogonal complement $P_\perp$ will produce either multiclicks or cross clicks. In this case, the squashing map will output a completely mixed qudit state $\mathbb{1}_d/d$: $\Lambda_{P_\perp,N}[\rho_N] = \mathbb{1}_d/d$ for all ρ_N. Therefore, we have constructed a squashing map on the subspace $P_\perp$. What is left to construct is a completely positive $\Lambda_{P,N}$. The adjoint of the squashing map must satisfy the linear constraints (3) and (4):

$$\Lambda_{P,N}^{\dagger}\left[\tilde{F}_1^{i,\alpha}\right] = \tilde{F}_{P,N}^{i,\alpha}. \tag{60}$$

We have the following result.

Lemma 17. Complete positivity of $\Lambda_{P,N}^{\dagger}$: On the Hilbert space of interest there exists a completely positive map $\Lambda_{P,N}$ which fulfills the linear constraints in Eq. (60).

Proof. The proof consists of two steps. First, one has to construct a map $\Lambda_{P,N}^{\dagger}$ that fulfills the linear constraints. Second, one needs to prove its complete positivity. To begin with, we note that Eq. (60) defines the map $\Lambda_{P,N}^{\dagger}$ on all target POVM elements $\tilde{F}_1^{i,\alpha} = F_1^{i,\alpha}$, which form a basis in $\mathcal{B}(\mathcal{H}_d)$. This completeness is a starting point for the construction of the squashing map $\Lambda_{P,N}$. As $\Lambda_{P,N}^{\dagger}$ is linear, this defines its action on any input operator. In the second step, we need to prove that the squashing map is completely positive. The proof is technical, and can be found in Appendix F. ■

This lemma finishes the construction of the squashing model for the qudit measurement device with a uniformly distributing input beam splitter.

Theorem 18. Squashing model for the passive multi-state qudit measurement: There exists a squashing model for the full ($d+1$ MUBs) passive multistate qudit measurement device for all prime numbers d.

E. Possible generalizations

In the concluding part of this section, we make some remarks about possible ways to generalize the results for the MUB measurement device. First of all, one may want to allow for different input beam-splitter ratios and choose $p_\alpha \neq 1/(d+1)$. In the following remark, we point out that it is not possible if one wants to keep the CPP scheme of Sec. VIII C unchanged, i.e., where the multiclicks and cross clicks are uniformly distributed.

Remark 19. For the CPP scheme chosen in Sec. VIII C (uniform distribution of the multiclicks and cross clicks) the linear constraints (60) are fulfilled if and only if the output probabilities of the input beam splitter in Fig. 7 are all equal, i.e., $p_\alpha = 1/(d+1)$ for all α.

Proof. See Appendix G.

Note that this remark does not contradict the existence of a squashing model for the passive BB84 measurement, as the CPP scheme used there is not a special case of the CPP scheme of Sec. VIII C. The other possible extension of the result of Theorem 18 is to choose the input beam splitter such that p_α are uniformly distributed over $k < d+1$ output arms and $p_\alpha = 0$ for the rest of the beam-splitter outputs (this situation would include the BB84 measurement device). However, we do not have an analytic proof that a squashing model for such situation exists and leave it as an open question.

IX. SQUASHING MODEL FOR TIME MODES

So far, we have provided examples in which squashing models take multiple-photon signals to single-photon ones. However, there are other degrees of freedom in experimental measurements that we have not accounted for in the squashing models considered so far. For example, measurements typically accept signals over a time window, whose responses from the measurement (such as detector clicks) are grouped together into what is called an event. During the time window of a detection event, it is possible that a measurement receives signals in multiple time modes. In this section, we address the question of the existence of squashing models for measurement devices that accept multiple time modes. First, we provide a squashing model for the multi-time-mode active BB84 measurement device. Based on this result, we prove the existence of the squashing model for the multi-time-mode six-state measurement. Finally, in accordance with Theorem 14, we apply the squashing model of the multi-time-mode active BB84 measurement to the multi-time-mode passive BB84 measurement. Note that the following results will apply to any collection of spatial-temporal modes a detector might be susceptible to, not only time modes.

As we will show, a measurement device that receives an input in many time modes can be thought of as many copies of that same measurement device, each measuring with the same setting (for example, the same basis) and each receives a single-time mode, followed by a suitable postprocessing in order to combine the single-mode devices into the full device. Therefore, it is important to distinguish between two essential groups of basic events (see Fig. 8): *single-time-mode events* and *multi-time-mode events*. Note that single-detector clicks and multi-detector clicks can correspond to a multi-time-mode event.

The situation seems to become rather cumbersome because in general it is unclear what classical postprocessing one should choose. However, if the structure of the measurement device is such that it has a single-time-mode squashing model for a specific classical postprocessing, then there exists an overall classical postprocessing such that a multi-time-mode squashing model exists. We have the following theorem.

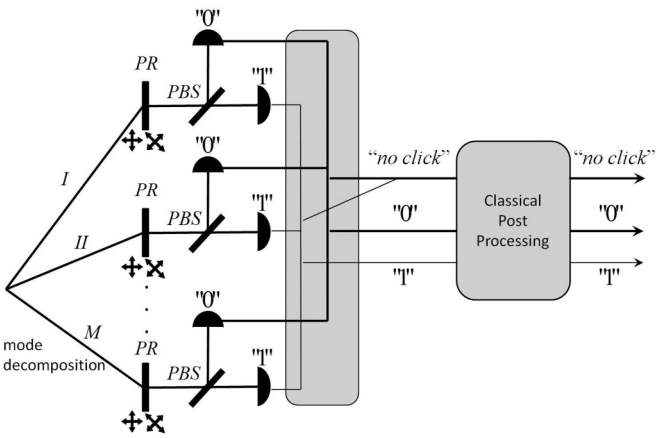

FIG. 8. Overall classical postprocessing for the multi-time-mode squashing model. The overall vacuum or "no-click" event is only registered if all single-time mode measurements output a "no-click" event. If the click pattern in the single-time-mode representation of the multi-time-mode measurement contains only 0's (1's) or vacuum, it is recorded as an overall 0 (1). Any other click pattern is recorded as an overall double click. The classical postprocessing randomly assigns the overall double clicks to the value 0 or 1 in the corresponding basis with equal probability.

Theorem 20. Multi-time-mode squashing model for the active BB84 measurement: There exists a squashing model with a single-mode qubit target measurement for the multi-time-mode active BB84 measurement, no matter how often one chooses to measure in either basis.

Proof. The proof relies on the fact that there exists a squashing model for the single-time-mode device and in particular on the orthogonality of the single-click and double-click subspaces (see Sec. V B).

Classical postprocessing in the time domain. The classical postprocessing in the time domain is defined by grouping events that come from single-time-mode measurements. If there is no click in any of the single-time-mode measurements, we assign an "overall" vacuum to this event. We use "overall" to mean the output of this first step in the classical postprocessing. If the outcome of every single-time-mode measurement is either 0 (1) or no click, we assign it to an overall 0 (1). To any other click pattern we assign an overall double click. These four types of events from a multimode measurement are then forwarded to the classical postprocessing that allows a single-time-mode squashing model.

In summary, the overall classical postprocessing for the multi-time-mode active BB84 measurement device is (cf. Fig. 8) as follows:

(i) If there is no click in any of the single-mode devices, then we call the overall event a "no-click."

(ii) If each single-mode device the event is either 0 (1) or "no click," and there is at least one click event, we call the overall event 0 (1).

(iii) In the case of any other click pattern, we call the event an "overall double click."

(iv) The overall single clicks and vacuum events remain unchanged.

(v) The overall double clicks are assigned with probability $\frac{1}{2}$ to 0 or 1.

CP map for the classical postprocessing in the time domain. In order to prove that there is a CP map that preserves the structure of the incoming state and is compatible with the provided classical postprocessing, we note that according to Sec. IV A we can (without loss of generality) perform a QND measurement of the photon number on each of the single-time modes.

Schematically, the CP map on the overall system can be constructed by the composition of CP maps as shown in Fig. 9. After the QND measurement is done on each of the single-time modes, we combine all time modes into one single-time mode. This is done via a unitary map U_{JC} that depends on the outcome of the QND measurements. It is applied to consecutive pairs of single-time modes (see Fig. 9). The first single-time mode is then forwarded directly to a flag measurement (defined shortly), whereas the second is an input to the next U_{JC}. This flag measurement is a projection on the vacuum state of the first $M-1$ time modes and is performed after the map U_{JC} has been applied on the $M-1$ and M single-time modes. Depending on the outcome of this measurement, a particular

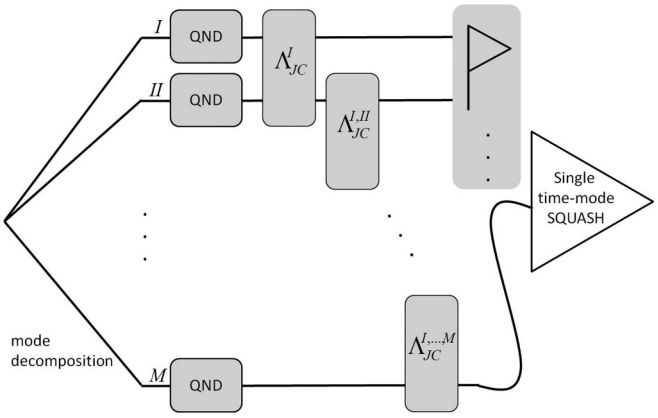

FIG. 9. The CP map compatible with the time-mode classical postprocessing. In the first step, the number of photons is determined in every mode by performing a QND measurement. Then, a unitary map U^{k}_{JC} is applied to the adjacent modes k and $k+1$. This map can be realized via a Jaynes-Cummings interaction, while the atomic degrees of freedom are traced out afterwards. Last is a flag measurement performed on the first $M-1$ time modes. The state of mode M is forwarded as input to the single-time-mode squashing map. Depending on the outcome of the flag measurement, either Λ_P or $\Lambda_{P_\perp}$ is applied.

single-time-mode squashing map is applied to the state in time mode M.

To explain this in more detail, the map U_{JC} can be described by using the Jaynes-Cummings model. This map is unitary but depends on the total photon number in each mode (without this knowledge it is impossible to perform the map). The crucial property of this map is that it preserves the structure of the particular type of incoming states independent of their polarization $\alpha = +,\times$ (cf. Appendix A in Ref. [6]):

$$\begin{aligned} &U^{I,II}_{\mathrm{JC}}[|N_I,0\rangle_\alpha\langle N_I,0| \otimes |N_{II},0\rangle_\alpha\langle N_{II},0|] \\ &\quad = |0,0\rangle_\alpha\langle 0,0| \otimes |N_I+N_{II},0\rangle_\alpha\langle N_I+N_{II},0|, \\ &U^{I,II}_{\mathrm{JC}}[|0,N_I\rangle_\alpha\langle 0,N_I| \otimes |0,N_{II}\rangle_\alpha\langle 0,N_{II}|] \\ &\quad = |0,0\rangle_\alpha\langle 0,0| \otimes |0,N_I+N_{II}\rangle_\alpha\langle 0,N_I+N_{II}|. \end{aligned} \tag{61}$$

Thus, we conclude that any state that produces an overall single click will be mapped to either one of four states:

$$\begin{aligned} &|0,0\rangle_\alpha\langle 0,0|^{\otimes(M-1)} \otimes \left|\sum_{k=1}^{M} N_k,0\right\rangle_\alpha \left\langle \sum_{k=1}^{M} N_k,0\right|, \\ &|0,0\rangle_\alpha\langle 0,0|^{\otimes(M-1)} \otimes \left|0,\sum_{k=1}^{M} N_k\right\rangle_\alpha \left|0,\sum_{k=1}^{M} N_k\right\rangle. \end{aligned} \tag{62}$$

Therefore, if the outcome of the flag measurement is vacuum we know with certainty (due to the unitarity of the map U_{JC}) that the incoming multi-time-mode state would have produced a single click in any single-time-mode measurement. If the outcome of the flag measurement is not the vacuum, then we know with certainty (again due to unitarity) that the incoming state would have produced an overall double click in the multi-time-mode measurement. By virtue of this, we proceed with the single-time-mode squashing map Λ_P from Sec. V if the flag signals vacuum, and $\Lambda_{P_\perp}$ otherwise.

Note that this procedure is compatible with the overall CPP scheme since the CP map in the time domain preserves the structure of the single-click subspace as it can be deduced from Eqs. (61) and (62). Since we are given that there is a squashing model for the single-time-mode measurement, we conclude the proof. ■

Note that the generalization of this result to other measurement devices is not straightforward. On one hand, for qudit measurement devices, the first part of the proof holds regardless of whether or not one measures in MUBs. Then, one needs the final single-mode squashing map to exist in order to claim the existence of the overall map. On the other hand, for most of the passive devices, one would need to come up with a flag that can distinguish between double and cross clicks, because CPP schemes for these devices usually distinguish between these types of clicks (see Sec. VII D).

Nonetheless there are two important corollaries from Theorem 20.

Corollary 21. There is a squashing model with a qubit target measurement for the multimode active six-state measurement with noisy postprocessing.

Proof. The proof repeats the proof of Theorem 20 until the point where one needs to apply the single-time-mode squashing map. In this case, the map from Sec. VI C is applied. ■

Corollary 22. There is a squashing model with a qubit target measurement for the multimode passive BB84 measurement with a CPP scheme that discards all cross-click events.

Proof. Since all cross-click events are thrown away, it is sufficient to have the same flag as in the multimode active BB84 measurement. More precisely, the squashing map is a sequence of three maps. First, all cross clicks are projected onto a multimode vacuum state. Second, the Jaynes-Cummings map is applied and a flag measurement is done. Third, depending on the flag measurement, the squashing map for the single-time-mode active BB84 measurement is applied. ■

X. SQUASHING MODEL FOR THE UNBALANCED PHASE-ENCODED BB84 (PE BB84) MEASUREMENT DEVICE

In the case of the unbalanced phase-encoded BB84 measurement device (PE BB84), the relevant information is always encoded in the phase between two different time modes that enter a Mach-Zehnder interferometer (see Fig. 10). This phase usually takes one of four values $\phi_0 = 0,\pi/2,\pi,3\pi/2$, which is motivated by the corresponding QKD protocol (cf. Ref. [17]). The long arm of the interferometer has a lossy phase modulator, which can be adjusted to $\phi = 0,\pi/2$ and whose loss is modeled by a beam splitter with transmittance t. The signals pass through the interferometer and then the modes are detected by two threshold detectors with equal efficiencies η [see Fig. 10(a)]. Each of the two detectors can accept signals in three different time windows containing the modes (b_1,b_4), (b_2,b_5), and (b_3,b_6), respectively. Due to the structure of the device it is clear that the relevant information about the phase is contained in the second time window since clicks in this time window correspond to the interference between the first and the second input time modes.

The question of the existence of a squashing model for the unbalanced PE BB84 measurement is also practically

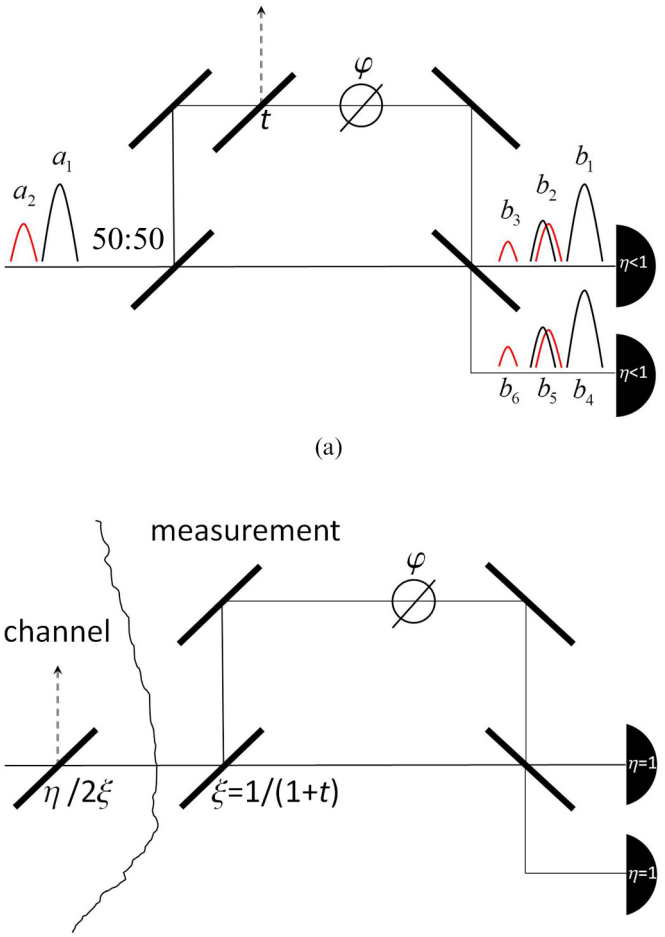

FIG. 10. (Color online) The PE BB84 measurement device. (a) Model of the device with imperfections: Two input modes a carrying a relative phase $\phi_0 = 0,\pi/2,\pi,3\pi/2$ pass through a Mach-Zehnder interferometer with a lossy phase modulator in the longer arm (adjusted to either $\phi = 0$ or $\pi/2$), and finally give rise to six output modes b, detected by two threshold detectors of equal efficiency η. (b) Equivalent model of the device with no imperfections but with some predetection loss, which is absorbed in the channel and is modeled by a beam splitter with transmittance $\eta/2\xi$, and an unbalanced input beam splitter $\xi = 1/(1+t)$.

motivated. A change in the loss of the phase modulator changes the measurement operators. For example, this implies that for the purpose of a security proof, the lossless version of the device, which is equivalent to the polarization BB84 measurement (see Sec. X A), can not be used anymore.

In order to not deal with losses and inefficient threshold detectors directly, we can always consider detection by a lossless interferometer with ideal threshold detectors but unbalanced input beam splitter due to the loss in the phase modulator and additional predetection loss due to the originally inefficient threshold detectors (cf. Ref. [17]). Such a measurement device is presented in Fig. 10(b). Since we are not interested in any predetection losses but solely in the mode of operation of the measurement device, we ignore the loss that is described by the beam splitter with transmittance $\eta/2\xi$ and consider the ideal Mach-Zehnder interferometer with an unbalanced input beam splitter with transmittance ξ.

The POVM elements of the PE BB84 measurement device can be described by the mode operators b_i that are related to mode operators a_i of the incoming signal (cf. Ref. [17]). The input-output relations (up to an unimportant overall phase) for the modes of interest are

$$\begin{aligned} b_1 &= \sqrt{\frac{\xi}{2}}a_1, \quad b_{2,\phi} = e^{-i\phi}\sqrt{\frac{(1-\xi)}{2}}a_1 - \sqrt{\frac{\xi}{2}}a_2, \\ b_3 &= \sqrt{\frac{(1-\xi)}{2}}a_2, \quad b_4 = \sqrt{\frac{\xi}{2}}a_1, \\ b_{5,\phi} &= e^{-i\phi}\sqrt{\frac{(1-\xi)}{2}}a_1 + \sqrt{\frac{\xi}{2}}a_2, \quad b_6 = \sqrt{\frac{(1-\xi)}{2}}a_2. \end{aligned} \tag{63}$$

Having these relations in mind, one can draw a connection to the usual polarization measurement. It is not hard to see that the measurements in the middle time window for different settings of ϕ correspond to polarization measurements in two conjugate bases. Moreover, if one combined clicks in the first and in the third time windows, one would perform a measurement that corresponds to the measurement in the standard basis in the polarization measurement device. Formally, for a lossless phase modulator ($t = 1$), we have the following POVM elements:

$$F_Q^{2,0} = \tfrac{1}{2}|-\rangle\langle -|, \quad F_Q^{5,0} = \tfrac{1}{2}|+\rangle\langle +|, \tag{64}$$

$$F_Q^{2,\pi/2} = \tfrac{1}{2}|y_+\rangle\langle y_+|, \quad F_Q^{5,\pi/2} = \tfrac{1}{2}|y_-\rangle\langle y_-|, \tag{65}$$

$$F_Q^1 + F_Q^4 = \tfrac{1}{2}|0\rangle\langle 0|, \quad F_Q^3 + F_Q^6 = \tfrac{1}{2}|1\rangle\langle 1|, \tag{66}$$

where $F_Q^{T,\phi}$ is the POVM element on single-photon input in the time window T and for the phase modulator set to ϕ. Equations (64) and (65) establish the formal connection of the lossless PE BB84 measurement (in the case where only events from the second time window are taken into account) to the active polarization BB84 measurement.

A. Target POVM elements and connection to the passive BB84 measurement device

We choose the target measurement to be the full measurement restricted to the single-photon and vacuum input. Since the useful events are detected in the second time window, we group the target POVM elements as follows:

$$\begin{aligned} F_Q^{2,\phi} &= |1\rangle_{2,\phi}\langle 1|, \\ F_Q^{5,\phi} &= |1\rangle_{5,\phi}\langle 1|, \\ F_{\mathrm{out},Q} &= \sum_{\substack{i=1,3,4,6 \\ \phi=0,\frac{\pi}{2}}} |1\rangle_{i,\phi}\langle 1|. \end{aligned} \tag{67}$$

The reason why we write the POVM elements here in terms of the output operators b will be more apparent in Sec. X C, where we consider N-photon input states.

In terms of the input states, which we denote by $|0\rangle = a_1^\dagger|\mathrm{vac}\rangle$ and $|1\rangle = a_2^\dagger|\mathrm{vac}\rangle$, respectively, the POVM

element for the outside clicks can be rewritten as

$$F_{\text{out},Q} = (1-\xi)|0\rangle\langle 0| + \xi|1\rangle\langle 1| = F_Q^{2,\phi} + F_Q^{5,\phi},\ \forall\,\phi. \quad (68)$$

This leads us to useful relations between the target POVM elements and the Pauli matrices σ_α, $\alpha = x,y,z$:

$$\begin{aligned} \frac{1}{\sqrt{\xi(1-\xi)}}\left(F_Q^{2,0} - F_Q^{5,0}\right) &= \sigma_x, \\ \frac{1}{\sqrt{\xi(1-\xi)}}\left(F_Q^{2,\frac{\pi}{2}} - F_Q^{5,\frac{\pi}{2}}\right) &= \sigma_y, \\ \frac{1}{2\xi-1}(2F_{\text{out},Q} - \mathbb{1}_2) &= \sigma_z. \end{aligned} \quad (69)$$

B. Classical postprocessing scheme for the PE BB84 measurement device

For a general input state with an undetermined number of photons in the input modes, the basic detection events can be characterized by means of patterns of clicks on the two threshold detectors over the three time windows. The total number of different events for each choice of the phase ϕ of the modulator is $2^6 = 64$. As we demonstrated at the beginning of this section, we can consider a lossless PE BB84 measurement device (cf. Fig. 10) by introducing some additional loss to the channel and an unequal-ratio input beam splitter. It means that a "no-click" pattern never occurs if the incoming signal was not in a vacuum state. Therefore, for two phase settings of interest $\phi = 0$ and $\pi/2$, we have 126 possible basic events.

In what follows, we describe a basic event by a phase setting ϕ 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 corresponds to the index of the output optical mode (see Fig. 10). This combination of indices provides an exact description of which detector has clicked and when.

Since our target measurement is a restriction of the basic measurement to the single-photon subspace, we are interested in a CPP scheme where single clicks are preserved and the rest of the postprocessing involves only multiple clicks. This postprocessing needs to be valid in the terms that were set in Sec. III B.

Using the linear dependency of the target POVM elements in Eq. (68) we performed an exhaustive numerical search for a valid CPP scheme. There are many CPP schemes that are allowed by the linear dependencies. Here, we present the only postprocessing that, as we will show shortly, allows a completely positive squashing map:

(1) Single clicks in either of the detectors in the second time window for either basis choice [i.e., events with $C = (0,1,0,0,0,0)$ or $C = (0,0,0,0,1,0)$] are assigned to the corresponding single-photon events.

(2) Simultaneous clicks in the two detectors in only the second time window for either basis choice [i.e. events with $C = (0,1,0,0,1,0)$] are assigned with probability $\frac{1}{2}$ to each of the single-photon measurement outcomes for the same setting of the phase ϕ.

(3) All events with clicks only in the first and the third time windows (outside clicks) are assigned to an outside single-photon measurement event.

(4) Any event with clicks in both the second and any of the outer time windows is assigned with probability $\frac{1}{2}$ to the outside click event of the single-photon measurement event and with probability $\frac{1}{8}$ onto each of the four other events of the single-photon measurement event.

C. Basic and full measurement POVM elements

Since the PE BB84 measurement device contains threshold detectors, we can use the same argument as in Observation 8, Sec. IV A, and consider the problem on the N-photon subspace. From now on, we will only consider N-photon input states. According to the properties of the target measurement and the choice of the CPP scheme, we will distinguish between the following basic POVM elements:

$$\begin{aligned} F_N^{2,\phi} &= |N\rangle_{2,\phi}\langle N|, \\ F_N^{5,\phi} &= |N\rangle_{5,\phi}\langle N|, \\ F_{\text{in,dc},N}^{\phi} &= \sum_{k=1}^{N-1} |k\rangle_{2,\phi}\langle k| \otimes |N-k\rangle_{5,\phi}\langle N-k|, \\ F_{\text{out},N} &= \sum_{\phi=0,\frac{\pi}{2}} \sum_{\substack{m_i\geqslant 0 \\ \sum_{i=1,3,4,6} m_i = N}} |m_1,m_3,m_4,m_6\rangle_\phi\langle m_1,m_3,m_4,m_6|, \\ F_{\text{in,out},N} &= \mathbb{1}_N - F_{\text{out},N} - \sum_{\phi=0,\frac{\pi}{2}} \left(F_{\text{in,dc},N}^{\phi} + F_N^{2,\phi} + F_N^{5,\phi}\right). \end{aligned} \quad (70)$$

The last three POVM elements correspond to a double click in the second time window for the particular choice of the phase ϕ, $F_{\text{in,dc},N}^{\phi}$, to any click not in the second time window, $F_{\text{out},N}$, and to any cross click between the second and one or both other time windows, $F_{\text{in,out},N}$.

The complementarity condition gives us one more auxiliary POVM element

$$F_{\text{in},N} = \sum_{\phi=0,\frac{\pi}{2}} \left(F_{\text{in,dc},N}^{\phi} + F_N^{2,\phi} + F_N^{5,\phi}\right), \quad (71)$$

where $F_{\text{in},N}$ is a POVM element corresponding to any click in the second time window.

Note that neither $F_{\text{in},N}$ nor $F_{\text{out},N}$ depend on the setting of the phase ϕ in the phase modulator. This can be seen if we write these elements in terms of the incoming modes a_1 and a_2:

$$\begin{aligned} F_{\text{in},N} &= \sum_{r=0}^{N} \xi^{N-r}(1-\xi)^r |r,N-r\rangle\langle r,N-r|, \\ F_{\text{out},N} &= \sum_{r=0}^{N} \xi^{r}(1-\xi)^{N-r} |r,N-r\rangle\langle r,N-r|, \end{aligned} \quad (72)$$

where $|r,N-r\rangle = \frac{1}{\sqrt{r!(N-r)!}}(a_1^\dagger)^r(a_2^\dagger)^{N-r}|\text{vac}\rangle$. With this in mind, we can write the full measurement POVM elements as

$$\begin{aligned} \tilde{F}_N^{b,\phi} &= F_N^{b,\phi} + \frac{1}{2}F_{\text{in,dc},N}^{\phi} + \frac{1}{8}F_{\text{in,out},N}, \\ \tilde{F}_{\text{out},N} &= F_{\text{out},N} + \frac{1}{2}F_{\text{in,out},N}, \\ \phi &= 0, \quad \frac{\pi}{2}; \quad b = 2,5. \end{aligned} \quad (73)$$

D. Positivity of the squashing map

With full measurement elements provided in Eq. (73), we have that the adjoint of the squashing map Λ_N has to fulfill the following linear constraints:

$$\begin{aligned}\Lambda_N^\dagger\big[F_Q^{b,\phi}\big] &= \tilde{F}_N^{b,\phi},\\ \phi = 0,\quad \frac{\pi}{2};\quad b &= 2,5\\ \Lambda_N^\dagger[F_{\mathrm{out},Q}] &= \tilde{F}_{\mathrm{out},N}.\end{aligned} \tag{74}$$

As in the previous examples, we investigate the positivity of the squashing map by investigating the positivity of the corresponding Choi matrix $\tau_N = \mathbb{1}\otimes\Lambda_N^\dagger[|\psi^+\rangle\langle\psi^+|]$. The Choi matrix will have no free parameters since the target POVM elements can be seen as an operator basis on the target Hilbert space. Using the decomposition of the projector $|\psi^+\rangle\langle\psi^+|$ in terms of Pauli matrices [see, e.g., Eq. (33)] and employing the established connection between the Pauli matrices and the target POVM elements [Eq. (69)], we have

$$\begin{aligned}&4(\mathbb{1}\otimes\Lambda_N^\dagger)[|\psi^+\rangle\langle\psi^+|]\\ &= \mathbb{1}_2\otimes\mathbb{1}_N + \frac{1}{\sqrt{\xi(1-\xi)}}\sigma_x\otimes\big(\tilde{F}_N^{2,0}-\tilde{F}_N^{5,0}\big)\\ &\quad - \frac{1}{\sqrt{\xi(1-\xi)}}\sigma_y\otimes\big(\tilde{F}_N^{2,\frac{\pi}{2}}-\tilde{F}_N^{5,\frac{\pi}{2}}\big)\\ &\quad + \frac{1}{2\xi-1}\sigma_z\otimes(2\tilde{F}_{\mathrm{out},N}-\mathbb{1}_N)\\ &= \mathbb{1}_2\otimes\mathbb{1}_N + \frac{1}{\sqrt{\xi(1-\xi)}}\sigma_x\otimes\big(F_N^{2,0}-F_N^{5,0}\big)\\ &\quad - \frac{1}{\sqrt{\xi(1-\xi)}}\sigma_y\otimes\big(F_N^{2,\frac{\pi}{2}}-F_N^{5,\frac{\pi}{2}}\big)\\ &\quad + \frac{1}{2\xi-1}\sigma_z\otimes(F_{\mathrm{out},N}-F_{\mathrm{in},N}).\end{aligned} \tag{75}$$

Here, we used the classical postprocessing equation (73) in order to write the last equation in terms of the basic POVM elements.

When we write the basic POVM elements in terms of input mode operators a_1,a_2 [Eqs. (63)], we can show that $F_N^{b,\phi} = 2^{-N}|N_b\rangle\langle N_b|$ where $|N_b\rangle$ is a normalized vector. Moreover, from the same equations it follows that $|\langle N_2|N_5\rangle|^2 = (2\xi-1)^{2N}$. Therefore, the traceless operator $F_N^{2,\phi}-F_N^{5,\phi} = (|N_2\rangle\langle N_2|-|N_5\rangle\langle N_5|)/2^N$ of rank 2 has eigenvalues $\pm\sqrt{1-(2\xi-1)^{2N}}$.

From Eq. (72) it follows that

$$\begin{aligned}&F_{\mathrm{out},N}-F_{\mathrm{in},N}\\ &= \sum_{r=0}^{N}\left(\frac{\xi^r}{(1-\xi)^{r-N}}-\frac{(1-\xi)^r}{\xi^{r-N}}\right)|r,N-r\rangle\langle r,N-r|.\end{aligned} \tag{76}$$

With these relations in mind, we can easily calculate the minimal eigenvalue of the Choi matrix in Eq. (75) numerically for any finite number N of incoming photons. We use Eq. (76) in order to represent the last term in Eq. (75) as an $(N+1)\times(N+1)$ matrix.

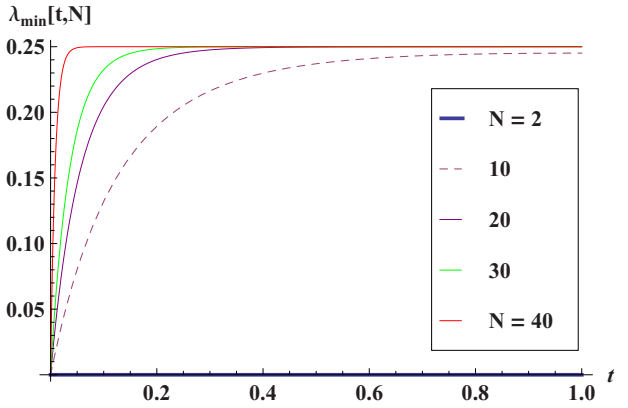

FIG. 11. (Color online) Minimum eigenvalue $\lambda_{\min}(t,N)$ of the Choi matrix τ_N of the adjoint squashing map $\Lambda_N^\dagger$ for the PE BB84 measurement device as a function of the loss t in the phase modulator in the long arm of the Mach-Zehnder interferometer. While for $N=2$ the minimal eigenvalue of τ_N stays constantly zero, it becomes strictly positive for $N>2$ and any $t\in(0,1]$.

In Fig. 11, we present the minimum eigenvalue of the Choi matrix as a function of the loss in the phase modulator t [recall that $\xi = 1/(1+t)$] for different numbers of incoming photons N. One can readily see that for any $t\in(0,1]$, $\lambda_{\min}(t,N)$ is non-negative. In fact, the minimum eigenvalue of the Choi matrix is strictly positive for any $N>2$. Moreover, it is clear from our numerics that $\lambda_{\min}(t,N)$ is a nondecreasing sequence in N for any $t\in(0,1]$, i.e., $\lambda_{\min}(t,N+1)\geqslant\lambda_{\min}(t,N)$ for all $t\in(0,1]$.

We will underpin our numerical findings by investigating asymptotical behavior of $\lambda_{\min}(t,N)$ analytically. We derive a lower bound on the minimal eigenvalue of the Choi matrix τ_N in two steps. First, as in the proof of Theorem 7, we again use Weyl's inequalities in order to derive a lower bound on the sum of the Hermitian matrices in Eq. (75). Second, we use the fact that $\lambda_{\min}(A\otimes B)\geqslant\lambda_{\min}(A)\lambda_{\min}(B)$. After some algebra, the bound for all N is given by

$$\begin{aligned}4\lambda_{\min}[t,N] &\geqslant 1-\frac{2(1+t)}{2^N\sqrt{t}}\sqrt{1-\left(\frac{1-t}{1+t}\right)^{2N}}\\ &\quad-\left(\frac{\frac{1}{(1+t)^{N-1}}-\frac{t^N}{(1+t)^{N-1}}}{1-t}\right)=:f_N(t).\end{aligned} \tag{77}$$

The function $f_N(t)$ is a monotonically increasing sequence of N for any $t\in(0,1]$, i.e., $f_{N+1}(t)-f_N(t)\geqslant 0$. Moreover, it holds that $\lim_{N\to\infty}f_N(t)=1$. Therefore, for any ϵ there exists an N_0 such that for any $N>N_0$, $|f_N(t)-1|<\epsilon$. Since N_0 is finite and for any finite N_0 one can calculate the minimum positive eigenvalue of the Choi matrix explicitly, it follows that, for all $N>N_0$,

$$4\lambda_{\min}(t,N)\geqslant 1-\epsilon\geqslant 0, \tag{78}$$

which concludes the proof of the positivity of the adjoint of the squashing map $\Lambda^\dagger$ and implies the existence of the squashing model for the PE BB84 measurement device with a lossy phase modulator.

XI. APPLICATION OF SQUASHING MODELS TO QKD PROTOCOLS

In this section, we shortly explain the application of squashing models for QKD. We start with the standard usage, followed by an advanced application, first put forward in Ref. [26], which provides slightly better key rates for various protocols. In the end, we exemplify their difference for a BB84 protocol suffering from additional double-click events on the receiver's side. We demonstrate the standard usage of squashing models in the security analysis of QKD using entanglement-based QKD protocols, but all results straightforwardly apply also to prepare-and-measure schemes that do not use physical entanglement.

Let us start with a quick review of the essentials about QKD: An entanglement-based QKD protocol is realized in two phases: in a first phase, the quantum phase, the two legitimate parties Alice and Bob perform measurements on their share of tripartite pure states, which can be thought of as being prepared by the adversary, Eve. In a subsequent second phase, the classical communication phase, Alice and Bob use an authenticated public channel to create a shared secret key from their data. The classical communication phase includes, typically, a sampling of their jointly correlated data that have been created in the quantum phase, a key map, error correction, and privacy amplification. The key map fixes which part of the data becomes key material. In our formulation, we call these data X and we assume without loss of generality that they are in Alice's hand. In error correction, Alice and Bob exchange additional information about X using their available data to make sure that also Bob has a copy of the key material. At this stage, the adversary could still be correlated with X, thus having information about it. Privacy amplification turns the key material X into a secret key K by applying some privacy amplification function out of a predefined set of functions. The resulting key can be shown to be arbitrarily close to a perfectly secure key. For our purpose, we do not need to deal with the exact security statement, or with finite-size effects in QKD. Instead, we deal only with the secret-key rate in what is known as the *infinite-key limit*.

In the security analysis, we can calculate the guaranteed achievable secret-key rate R as number of secret-key bits per bit of key material X as

$$R := \left(\inf_{\rho_{ABE} \in \Gamma_{ABE}} S(X|E) \right) - \delta_{\text{leak}}, \tag{79}$$

where $S(X|E)$ is the conditional von Neumann entropy of Eve on the key material X, minimized over a set of potential underlying states ρ_{ABE} (which can be thought of without loss of generality as pure states). This set is constrained by Alice's and Bob's observations during sampling in the classical communication phase. Each state ρ_{ABE} represents an eavesdropping strategy which leads to particular conditional states ρ_E^x in Eve's hand conditioned on an element x of the key material X. These states summarize that part of Eve's knowledge about the key material which stems from her preparation of (or interaction with) the physical systems on which Alice and Bob perform their measurements. The von Neumann entropy $S(X|E)$ is a function of these states and the probability of occurrence of the elements of X, as influenced by the public communication protocol. The last term δ_{leak} is the information content about the key material X that leaks to Eve during the classical communication phase, including, for example, the number of bits per key material that have been announced publicly during error correction.

Squashing models can now be used to simplify the minimization calculation in the key-rate expression. This is of particular importance for optical implementations of QKD where, for example, Bob performs some type of photon-counting measurements, which need to be described on the infinite-dimensional Hilbert space of optical modes. Thus, the set Γ_{AB_FE} can have a rather complex form: it is given by all pure tripartite quantum states ρ_{ABE} which satisfy the condition that they give the observed correlations of data for Alice and Bob (including postprocessing on Bob's side).

Theorem 23. The key rate R_F using the full measurement can be lower bounded by a key rate using the target measurement R_T as

$$R_F \geqslant R_T := \left(\inf_{\rho_{AB_TE} \in \Gamma_{AB_TE}} S(X|E) \right) - \delta_{\text{leak}}, \tag{80}$$

where ρ_{AB_TE} has now the lower-dimensional target system B_T as one component. The set Γ_{AB_TE} contains all such density matrices which are again constrained by the observed correlations for Alice and Bob. These constraints can now be formulated using the target measurements.

The same statement can be made for the measurement on system A if that measurement admits a squashing model. To verify the theorem, we can follow a simple argument which is illustrated in Fig. 12. As a first step, note that an eavesdropping strategy against the full measurement protocol, as represented by a state ρ_{AB_FE} and shown in Fig. 12(a), is now equivalent to an eavesdropping strategy described by the state $(\mathbb{1}_A \otimes \Lambda_B \otimes \mathbb{1}_E)[\rho_{AB_FE}]$, as the squashing map is applied to system B_F without loss of generality before the target measurement is being performed, as shown in Fig. 12(b). In the next step, we enlarge the set of possible eavesdropping strategies by directly admitting all density matrices of the type ρ_{AB_TE} that are compatible with the observations, thereby dropping the constraint that it must be obtained by applying the squashing map Λ to the full system [see Fig. 12(c)]. As a result of enlarging the set of allowed eavesdropping strategies over which the infimum in Eq. (79) is taken, the resulting key rate can only decrease.

Note that the above theorem applies to the full measurements, that is, Bob performs the postprocessing on his basic measurement results. Next, we draw the attention to the fact that the above key rate can be improved, as shown by Ma and Lütkenhaus in Ref. [26]. The motivation for this improvement comes from the fact that the postprocessing of the basic measurements helps to establish a squashing model to simplify the evaluation of the conditional entropy $S(X|E)$ over all eavesdropping strategies. However, the same postprocessing, typically, increases the amount of communication required during error correction from $\delta_{\text{leak}}^{\text{basic}}$ to $\delta_{\text{leak}} \geqslant \delta_{\text{leak}}^{\text{basic}}$. The key observation in Ref. [26] is that these two points can be separated: we are allowed to use postprocessed data to formulate constraints on ρ_{AB_TE} to evaluate $S(X|E)$, but we do not actually need to apply the postprocessing to our data,

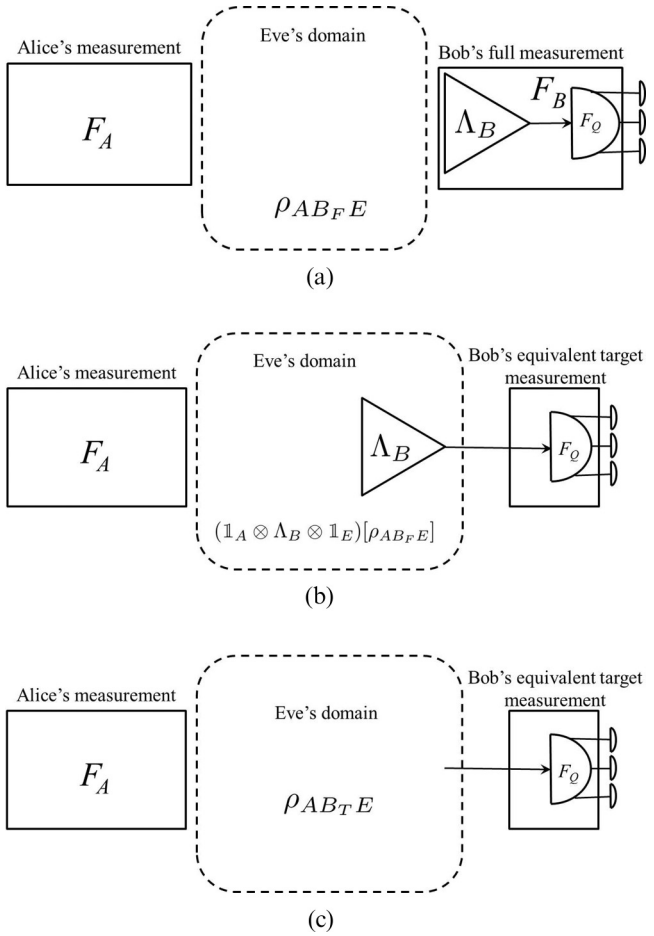

FIG. 12. Explanation of the standard squashing models application in QKD: Case (a) represents a general attack against the full measurement scheme, while case (b) shows the reformulation of the same attack using the squashing model which results from enforcing the application of the squashing map on system B of the general attack. Case (c) then represents a general attack of the scheme using the target measurement, which now clearly contains the case (b), and thus case (a). Thus, the key rate of case (c) is a lower bound of the key rate in case (a), as stated in Theorem 23.

as long as the key material variables X are not affected by the postprocessing. Formally, we can state this as follows.

Theorem 24. For a QKD scheme, which uses basic measurements, postprocessing of the basic measurements that leads to full measurements and allows for squashing model with some target measurement, we can find the key rate

$$R^{\mathrm{imp}}_{AB_T} \geqslant \left(\inf_{\rho_{AB_TE} \in \Gamma_{AB_TE}} S(X|E) \right) - \delta^{\mathrm{basic}}_{\mathrm{leak}}. \tag{81}$$

This key rate holds as long as the key material X is unaffected by the postprocessing. It uses the squashing model to estimate the term involving $S(X|E)$, but shows a reduced value of the term $\delta^{\mathrm{basic}}_{\mathrm{leak}}$ which represents the amount of information on X that leaks during the error correction phase of QKD based on Bob's basic measurement events.

To illustrate the effect, consider an example of the BB84 and compare the key rates when one applies either Theorems 23 or 24. If we assume an initial symmetric data behavior of the type

$$P(X,Y) = \begin{cases} P(0,0) = P(1,1) = \frac{1}{2} P_{\mathrm{single}}(1-e), \\ P(0,1) = P(1,0) = \frac{1}{2} P_{\mathrm{single}} e, \\ P(0,d) = P(1,d) = \frac{1}{2}(1 - P_{\mathrm{single}}), \end{cases} \tag{82}$$

with P_{single} being the probability to obtain a single-click event and e as the error rate within the single-click events. Postprocessing that allows a squashing model for these measurements involves a random assignment of double clicks to the values 0 and 1, which will raise the error rate from e to $e_{PP} := P_{\mathrm{single}} e + \frac{1}{2}(1 - P_{\mathrm{single}})$. Using the squashing model, we find

$$\inf_{\rho_{AB_TE} \in \Gamma_{AB_TE}} S(X|E) \geqslant 1 - h[e_{PP}],$$

where $h[x] = -x \log_2 x - (1-x)\log_2(1-x)$ is the binary entropy function.

Now, let us have a look at the amount of error correction we have to do, as quantified by δ_{leak} (with postprocessing) and $\delta^{\mathrm{basic}}_{\mathrm{leak}}$ (without postprocessing). Assuming that we can reach the Shannon limit for error correction, we find $\delta_{\mathrm{leak}} = h(e_{PP})$, while we have $\delta^{\mathrm{basic}}_{\mathrm{leak}} = h[(1 - P_{\mathrm{single}}) + P_{\mathrm{single}} h_2(e)]$. Consequently, we find for the key rate according to Theorem 23

$$R_{AB_T} = 1 - 2h[e_{PP}],$$

while we can find an improved key rate according to Theorem 24

$$R^{\mathrm{imp}}_{AB_T} = 1 - h[e_{PP}] - h[(1 - P_{\mathrm{single}}) + P_{\mathrm{single}} h_2(e)],$$

which is a strict improvement of the rate due to the concavity of the binary entropy function.

XII. CONCLUSION AND OUTLOOK

In this work, we have further developed the ideas of Ref. [10]. We gave a rigorous definition of the squashing model and precisely defined the role of classical postprocessing in this setting. In summary, the squashing models give us a tool for the truncation of Hilbert spaces under adversarial conditions. More precisely, in the context of quantum communication in the presence of an adversary that can tamper with the transmitted signals by employing their high dimensionality, it is equivalent to the scenario where one only performs the target measurement instead of a high-dimensional measurement. This undoes the adversary's advantage because there is no information that can be gained by making a measurement on the high-dimensional system above what can be gained from the target measurement on the lower-dimensional system. Thus, the squashing models can be effectively applied, for example, in the optical implementations of QKD or coin tossing.

For QKD applications, we constructed squashing models for various types of measurement devices, which are used in optical implementations of corresponding QKD protocols. For instance, this implies that a security proof of these protocols can be generalized from single photons to the multiphoton case.

Several generalizations can be made for results presented in this work. First of all, it would be interesting to generalize the results on the qudit measurement to the case where the

input beam splitter has less than $d+1$ output arms. Our intuition strongly suggests that the squashing model might exist if the number of output arms is strictly less than $d+1$. This is due to the fact that removing the output arms would effectively introduce free parameters in the Choi matrix of the squashing map, which is usually enough to guarantee the complete positivity of the corresponding squashing map (cf. active BB84 and six-state measurements). However, these findings would heavily rely on numerical findings. It would be therefore desirable to find some type of symmetry argument that can be used to tackle this problem analytically.

ACKNOWLEDGMENTS

This research has been supported by NSERC (via the Discovery Program and the Strategic Project Grant FREQUENCY) and the Ontario Research Fund (ORF). O. Gittsovich is grateful for the support of the Austrian Science Fund (FWF) and Marie Curie Actions (Erwin Schrödinger Stipendium J3312-N27). We would like to thank W. Gao, M. Curty, E. Diamant, H.-K. Lo, and M. Peev for many enlightening discussions.

APPENDIX A

In this Appendix, we summarize some known facts about the natural representation of superoperators. Further details on this topic can be found in Ref. [31].

Remark A1. Equivalence of the natural and Choi-Jamiołkowski representations. Let Θ be a superoperator $\Theta(X)=Y$, with $X\in L(\mathcal{H}_A)$ and $Y\in L(\mathcal{H}_B)$ being linear operators. Let $\{|e_m\rangle\}$ and $\{|f_\mu\rangle\}$ denote orthonormal bases in $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. On the one hand, the natural representation of Θ is defined as a map

$$\Gamma_\Theta : \mathrm{vec}(X)\mapsto \mathrm{vec}(\Theta(X)), \tag{A1}$$

where $\mathrm{vec}(X)$ denotes columnwise vectorization of matrix X. Γ_Θ is a linear operator $\Gamma_\Theta\in L(\mathcal{H}_A\otimes\mathcal{H}_A,\mathcal{H}_B\otimes\mathcal{H}_B)$ which can be represented by a matrix

$$\Gamma_{\Theta_{\substack{\mu m\\ \nu n}}}=\langle f_\mu,f_\nu|\Gamma_\Theta|e_m,e_n\rangle. \tag{A2}$$

On the other hand, the Choi-Jamiołkowski representation is defined by the map [19,20]

$$\tau_\Theta : L[L(\mathcal{H}_A),L(\mathcal{H}_B)]\to L(\mathcal{H}_A\otimes\mathcal{H}_B) \tag{A3}$$

and can be represented by a matrix

$$\tau_{\Theta_{\substack{nm\\ \nu\mu}}}=\langle e_n,f_\nu|\tau_\Theta|e_m,f_\mu\rangle. \tag{A4}$$

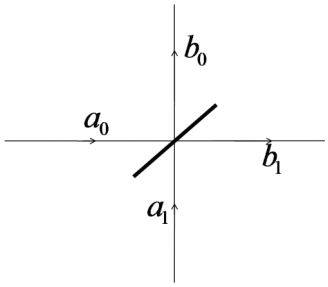

FIG. 13. Beam splitter presented as a four-port device with a_0 and a_1, b_0 and b_1 being the input and output modes, respectively.

One can readily see that Γ_Θ is a reshuffled version of the τ_Θ:

$$\langle f_\mu,f_\nu|\tau_\Theta^R|e_m,e_n\rangle=\langle e_n,f_\nu|\tau_\Theta|e_m,f_\mu\rangle. \tag{A5}$$

APPENDIX B

Beam splitters are well-studied objects in quantum optics [32,33]. They are considered as four-port devices with two input and two output ports (Fig. 13). For a beam splitter with transmittance T and reflectivity R ($R+T=1$), the following relations between the input and output modes hold:

$$\begin{aligned} b_0&=(\sqrt{T}a_1+e^{i\alpha}\sqrt{R}a_0),\\ b_1&=(\sqrt{T}a_0+e^{i(\pi-\alpha)}\sqrt{R}a_1), \end{aligned} \tag{B1}$$

provided an α phase shift between the reflected and transmitted beams. Without loss of generality, one can set $\alpha=0$.

Both the transmittance and the reflectivity of the beam splitter may depend on the frequency, direction of propagation, and on the polarization of the incident light. For usual 50:50 beam splitter, the relations simplify to

$$\begin{aligned} b_0&=\frac{1}{\sqrt{2}}(a_0+a_1),\\ b_1&=\frac{1}{\sqrt{2}}(a_0-a_1). \end{aligned} \tag{B2}$$

APPENDIX C

Here, we give explicit formulas for the matrix representations of the Choi matrices used for the squashing map in the BB84 active basis measurement's squashing model: $M(\tau_{P,N,\mathrm{fix}})$ and $M(\tau_{P,N,\mathrm{open}})$. We also discuss how to solve $M(\tau)\geqslant 0$ to ensure the complete positivity of the squashing map. The Choi matrices are given by

$$M\left(F_{P,N}^{(0,z)}-F_{P,N}^{(1,z)}\right)\equiv M_z=\begin{pmatrix} 1 & 0 & s & s\\ 0 & -1 & -s & (-1)^{N+1}s\\ s & -s & 0 & [1-(-1)^N]s^2\\ s & (-1)^{N+1}s & [1-(-1)^N]s^2 & 0 \end{pmatrix},$$

$$M\left(F_{P,N}^{(0,x)}-F_{P,N}^{(1,x)}\right)\equiv M_x=\begin{pmatrix} 0 & [1-(-1)^N]s^2 & s & -s\\ [1-(-1)^N]s^2 & 0 & s & (-1)^{N+1}s\\ s & s & 1 & 0\\ -s & (-1)^{N+1}s & 0 & -1 \end{pmatrix},$$

$$M(\mathbb{1}_M) = \begin{pmatrix} 1 & 0 & s & s \\ 0 & 1 & s & (-1)^N s \\ s & s & 1 & 0 \\ s & (-1)^N s & 0 & 1 \end{pmatrix},$$

$$M\left[\left(\Lambda_N^P\right)^\dagger(\sigma_y)\right] \equiv iS = i \begin{pmatrix} 0 & x_1 & x_2 & x_3 \\ -x_1 & 0 & x_4 & x_5 \\ -x_2 & -x_4 & 0 & x_6 \\ -x_3 & -x_5 & -x_6 & 0 \end{pmatrix}, \tag{C1}$$

where x_i, $i = 1, \ldots, 6$, are real free parameters and $s = 2^{-N/2}$. The overall 8×8 matrix, which needs to be positive, is then given by

$$M(\tau_{P,N}) = \begin{pmatrix} M(\mathbb{1}_N) + M_z & M_x + S \\ M_x - S & M(\mathbb{1}_N) - M_z \end{pmatrix}$$

$$= \begin{pmatrix} 2 & 0 & 2s & 2s & 0 & \delta_N s^2 + x_1 & s + x_2 & x_3 - s \\ 0 & 0 & 0 & 0 & \delta_N s^2 - x_1 & 0 & x_4 + s & x_5 + (-1)^{N+1} s \\ 2s & 0 & 1 & \delta_N s^2 & s - x_2 & s - x_4 & 1 & x_6 \\ 2s & 0 & \delta_N s^2 & 1 & -s - x_3 & (-1)^{N+1} s - x_5 & -x_6 & -1 \\ 0 & \delta_N s^2 - x_1 & s - x_2 & -x_3 - s & 0 & 0 & 0 & 0 \\ \delta_N s^2 + x_1 & 0 & -x_4 + s & -x_5 + (-1)^{N+1} s & 0 & 2 & 2s & (-1)^N 2s \\ s + x_2 & s + x_4 & 1 & -x_6 & 0 & 2s & 1 & -\delta_N s^2 \\ -s + x_3 & (-1)^{N+1} s + x_5 & x_6 & -1 & 0 & (-1)^N 2s & -\delta_N s^2 & 1 \end{pmatrix}, \tag{C2}$$

where $\delta_N = 1 - (-1)^N$. The matrix $M(\tau_{P,N})$ is positive if and only if each of its principal minors is positive. This fixes all free parameters to be

$$\begin{aligned} x_1 &= x_6 = \delta_N s^2, \\ x_3 &= x_4 = -s, \\ x_2 &= (-1)^N x_5 = s. \end{aligned} \tag{C3}$$

APPENDIX D

Here, we provide some technical details used for the construction of the squashing model of the active six-state measurement device for an intermediate postprocessing in Sec. VI C. In particular, we show the positivity of the matrix $\tau_{P,N,\mathrm{new}}(p)$ from Eq. (43) for $p \geqslant \frac{1}{3}$. First of all, for small integers N we observe that the critical value of p is equal to $\frac{1}{3}$. For example, we need p to exceed this value for $N = 3$ in order matrix to be positive. Then, one can check directly that the matrix of $\tau_{P,N,\mathrm{new}}(p = \frac{1}{3})$ is non-negative for $N = 1, 2, \ldots, 10$. After this is done, one can use the Gerschgorin disk theorem [34] in order to prove that all eigenvalues strictly lie on the positive part of the real axis. One can give an upper bound on each of the disk's (there are 12 of them) radii. Each bound is a monotonically decreasing function of N, and for $N > 10$ the union of 12 disks lies on the part of the complex plane representing the eigenvalues of the matrix $\mathrm{Re}\lambda > 0$. This implies the positivity of the eigenvalues since the matrix is Hermitian and all its eigenvalues are real.

APPENDIX E

Here, we derive the POVM elements for the qudit measurement device from Sec. VIII. Formally, we will use $b^\dagger$ and b to describe creation and annihilation operators of the output and $a^\dagger$ and a to describe creation and annihilation operators of the input of the measurement device from Fig. 7. Assuming that the input state has N photons, we have the following POVM elements in terms of output operators $b^\dagger$ and b:

$$\begin{aligned} F_N^{i,\alpha} &= \frac{1}{N!} (b_{i,\alpha}^\dagger)^N |0\rangle\langle 0| (b_{i,\alpha})^N, \\ F_{\mathrm{mc},N}^{\alpha} &= \sum_{\substack{m_k > 0 \\ \sum m_k = N}} \bigotimes_{i=1}^{d} \frac{1}{m_k!} (b_{i,\alpha}^\dagger)^{m_k} |0\rangle\langle 0| (b_{i,\alpha})^{m_k}, \\ F_{\mathrm{cc},N} &= \mathbb{1}_N - \sum_{\alpha=0}^{d} \left(F_{\mathrm{mc},N}^{\alpha} + \sum_{i=1}^{d} F_N^{i,\alpha} \right). \end{aligned} \tag{E1}$$

Here, $F_N^{i,\alpha}$ denotes a single click in detector i of the detection module $\mathcal{M}_\alpha$ (basis α). $F_{\mathrm{mc},N}^{\alpha}$ denotes a multiclick for which several detectors of the same detection module $\mathcal{M}_\alpha$ have clicked, whereas $F_{\mathrm{cc},N}$ denotes any cross click between different detection modules.

In order to write the POVM elements in terms of input operators $a^\dagger$ and a, one needs to know the input-output relations for the linear optical network. For an unbiased version [$p_\alpha = 1/(d+1)$ for all α] of the beam splitter in Fig. 7, the input and output modes are connected by the Fourier matrix:

$$\begin{aligned} b_{\alpha,q} &= \sum_{\beta=0}^{d} U_{\alpha,\beta} a_{\beta,q}, \quad \text{with} \quad q = 1 \ldots d \\ U_{\alpha,\beta} &= (d+1)^{-\frac{1}{2}} e^{\frac{2\pi i}{d+1} \alpha\beta}. \end{aligned} \tag{E2}$$

Now, we can substitute these relations in Eq. (E1). We note that on the input side only the mode $a_{\beta,q}$, $q = 1 \ldots d$, is occupied. Whence, we can project the rest of the a's on the vacuum state. After some algebra, the POVM elements in terms of

input modes eventually become

$$\begin{aligned} F_N^{i,\alpha} &= (d+1)^{-N}|N\rangle_{i,\alpha}\langle N|, \\ F_{\mathrm{mc},N}^{\alpha} &= (d+1)^{-N}\left(\mathbb{1}_N - \sum_i |N\rangle_{i,\alpha}\langle N|\right), \\ F_{\mathrm{cc},N} &= \left(1 - \frac{1}{(d+1)^{N-1}}\right)\mathbb{1}_N. \end{aligned} \tag{E3}$$

APPENDIX F

In this Appendix, we provide the proof of Proposition 17 from Sec. VIII.

Proof of Proposition 17. The positivity is checked by proving that the Choi matrix of the map $\Lambda_{P,N}^{\dagger}$ is positive semidefinite. If d is a prime number, the maximally entangled state can be decomposed in the the chosen operator basis $\{Z_d^{\alpha},(X_d Z_d^{\alpha})^k\}_{\alpha,k}$, $\alpha = 0,\ldots,d-1$, $k = 1,\ldots,d-1$ [one can see this after some algebra involving Eqs. (55)] as

$$\begin{aligned} |\psi^+\rangle\langle\psi^+| = \frac{1}{d^2}\mathbb{1}_d \otimes \mathbb{1}_d + \frac{1}{d^2}\sum_{k=1}^{d-1} Z_d^{-k} \otimes Z_d^k \\ + \frac{1}{d^2}\sum_{\substack{\alpha=0 \\ k=1}}^{d-1} \left(X_d Z_d^{-\alpha}\right)^k \otimes \left(X_d Z_d^{\alpha}\right)^k. \end{aligned} \tag{F1}$$

Moreover, we point out that one can relate $\{Z_d^{\alpha},(X_d Z_d^{\alpha})^k\}_{\alpha,k}$ to the target POVM elements (58):

$$\begin{aligned} Z_d^k &= (d+1)\sum_{i=0}^{d-1} \omega^{ik} F_1^{0,i}, \\ \left(X_d Z_d^{\alpha}\right)^k &= (d+1)\sum_{i=0}^{d-1} \omega^{ik} F_1^{\alpha+1,i}. \end{aligned} \tag{F2}$$

We prove the positivity in two steps.

Step 1. $N = 1$: When the QND measurement signals that one photon enters the measurement device, the squashing map does not have to do anything and $\Lambda^{\dagger} = \mathbb{1}$. Clearly, it is completely positive in this case.

Step 2. $N \geqslant 2$: When the QND measurement signals the presence of more than one photon in the incoming signal, the squashing map has to be nontrivial. The proof of its complete positivity has several technical steps.

First of all, let us apply $\mathbb{1} \otimes \Lambda_{P,N}^{\dagger}$ to the second term in Eq. (F1). We omit the overall factor of $1/d^2$ for brevity:

$$\begin{aligned} &\sum_{k=1}^{d-1} Z_d^{-k} \otimes \Lambda_{P,N}^{\dagger}\left[Z_d^k\right] \\ &\quad = \sum_{\substack{r,s=0 \\ k=1}}^{d-1} (d+1)^2 \omega^{(s-r)k} \tilde{F}_1^{r,0} \otimes \tilde{F}_{P,N}^{s,0} \\ &\quad = (d+1)^2\left(d\sum_{r=0}^{d-1} \tilde{F}_1^{r,0} \otimes \tilde{F}_{P,N}^{r,0} - \sum_{r,s=0}^{d-1} \tilde{F}_1^{r,0} \otimes \tilde{F}_{P,N}^{s,0}\right), \end{aligned} \tag{F3}$$

where we used the first relation in Eq. (F2) and the identity $\sum_{k=1}^{d-1} \omega^{(s-r)k} = d\delta_{rs} - 1$ for $\omega = e^{\frac{2\pi i}{d}}$. From the form of the basic POVM elements [Eq. (57)] and the form of the full measurement POVM elements [Eq. (59)], it follows that

$$\sum_{r=0}^{d-1} \tilde{F}_{P,N}^{r,\alpha} = \frac{1}{d+1}\mathbb{1}_{P,N} \;\forall\, \alpha. \tag{F4}$$

Note that this can also be concluded by a simple normalization argument: the POVM elements corresponding to clicks in one of the detector modules should sum up to something proportional to the identity. The coefficient of proportionality is equal to the probability $p_{\alpha} = 1/(d+1)$ of the generalized balanced input beam splitter.

Hence,

$$\begin{aligned} &\sum_{k=1}^{d-1} Z_d^{-k} \otimes \Lambda_{P,N}^{\dagger}\left[Z_d^k\right] \\ &\quad = d(d+1)^2 \sum_{r=0}^{d-1} \tilde{F}_1^{r,0} \otimes \tilde{F}_{P,N}^{r,0} - \mathbb{1}_d \otimes \mathbb{1}_{P,N}. \end{aligned} \tag{F5}$$

Second, let us consider the action of $\mathbb{1} \otimes \Lambda_{P,N}^{\dagger}$ on the third term in Eq. (F1), while omitting the overall factor of $1/d^2$ again for brevity:

$$\begin{aligned} &\sum_{\substack{\alpha=0 \\ k=1}}^{d-1} \left(X_d Z_d^{-\alpha}\right)^k \otimes \Lambda_{P,N}^{\dagger}\left[\left(X_d Z_d^{\alpha}\right)^k\right] \\ &\quad = (d+1)^2 \sum_{\substack{r,s,\alpha=0 \\ k=1}}^{d-1} \omega^{(r+s)k} \tilde{F}_1^{r,-(\alpha+1)} \otimes \tilde{F}_{P,N}^{s,\alpha+1} \\ &\quad = d(d+1)^2 \sum_{r,\alpha=0}^{d-1} \tilde{F}_1^{r,-(\alpha+1)} \otimes \tilde{F}_{P,N}^{d-r,\alpha+1} - d\mathbb{1}_d \otimes \mathbb{1}_{P,N}. \end{aligned} \tag{F6}$$

Here, we used the second relation in Eq. (F2), the identity $\sum_{k=1}^{d-1} \omega^{(r+s)k} = d\delta_{d,r+s} - 1$ for $\omega = e^{\frac{2\pi i}{d}}$, and Eq. (F4).

Putting Eqs. (F5) and (F6) together, we arrive at

$$\begin{aligned} &d^2\mathbb{1} \otimes \Lambda_{P,N}^{\dagger}[|\psi^+\rangle\langle\psi^+|] \\ &\quad = d(d+1)^2 \sum_{r=0}^{d-1} \tilde{F}_1^{r,0} \otimes \tilde{F}_{P,N}^{r,0} \\ &\qquad + d(d+1)^2 \sum_{r,\alpha=0}^{d-1} \tilde{F}_1^{r,-(\alpha+1)} \otimes \tilde{F}_{P,N}^{d-r,\alpha+1} - d\mathbb{1}_d \otimes \mathbb{1}_{P,N}. \end{aligned} \tag{F7}$$

The positivity of the last expression is proven by expanding the full measurement POVM elements in terms of the basic POVM elements. For that, we reformulate the first term in

Eq. (F7). According to Eqs. (57) and (G2) for $\alpha = 0$, we have

$$\begin{aligned} & d(d+1)^2 \sum_{r=0}^{d-1} \tilde{F}_1^{r,0} \otimes \tilde{F}_{P,N}^{r,0} \\ &= d(d+1)^2 \sum_{r=0}^{d-1} \tilde{F}_1^{r,0} \otimes \tilde{F}_{\text{any}}^{r,0} \\ &\quad + (d+1)\left(1 - \frac{1}{(d+1)^{N-1}}\right) \sum_{r=0}^{d-1} \tilde{F}_1^{r,0} \otimes \mathbb{1}_{P,N} \\ &= d(d+1)^2 \sum_{r=0}^{d-1} \tilde{F}_1^{r,0} \otimes \tilde{F}_{\text{any}}^{r,0} \\ &\quad + \left(1 - \frac{1}{(d+1)^{N-1}}\right) \mathbb{1}_d \otimes \mathbb{1}_{P,N}, \end{aligned} \tag{F8}$$

where $\tilde{F}_{\text{any}}^{r,0} = F_{P,N}^{r,0} + F_{P,N}^{0}/d$ and we used Eq. (F4) for the qudit part ($N = 1$) of the tensor product.

For the second term in Eq. (F7), we have

$$\begin{aligned} & d(d+1)^2 \sum_{r,\alpha=0}^{d-1} \tilde{F}_1^{r,-(\alpha+1)} \otimes \tilde{F}_{\text{any}}^{d-r,\alpha+1} \\ &= d(d+1)^2 \sum_{r,\alpha=0}^{d-1} \frac{d}{p_{d-\alpha}\, p_{\alpha+1}} \tilde{F}_1^{r,-(\alpha+1)} \otimes \tilde{F}_{\text{any}}^{r,\alpha+1} \\ &\quad + (d+1)\left(1 - \frac{1}{(d+1)^{N-1}}\right) \sum_{r,\alpha=0}^{d-1} \tilde{F}_1^{r,-(\alpha+1)} \otimes \mathbb{1}_{P,N} \\ &= d(d+1)^2 \sum_{r,\alpha=0}^{d-1} \tilde{F}_1^{r,-(\alpha+1)} \otimes \tilde{F}_{\text{any}}^{r,\alpha+1} \\ &\quad + d\left(1 - \frac{1}{(d+1)^{N-1}}\right) \mathbb{1}_d \otimes \mathbb{1}_{P,N}, \end{aligned} \tag{F9}$$

where $\tilde{F}_{\text{any}}^{r,\alpha+1} = F_{P,N}^{d-r,\alpha+1} + F_{P,N}^{\alpha+1}/d$.

Substituting Eqs. (F8) and (F9) into (F7) yields

$$\begin{aligned} & d^2 \mathbb{1} \otimes \Lambda_P^\dagger[|\psi^+\rangle\langle\psi^+|] \\ &= d(d+1)^2 \sum_{r=0}^{d-1} \left(\tilde{F}_1^{r,0} \otimes \tilde{F}_{\text{any}}^{r,0} + \sum_{\alpha=0}^{d-1} \tilde{F}_1^{r,-(\alpha+1)} \otimes \tilde{F}_{\text{any}}^{r,\alpha+1} \right) \\ &\quad + \left(1 - \frac{1}{(d+1)^{N-2}}\right) \mathbb{1}_d \otimes \mathbb{1}_{P,N}. \end{aligned} \tag{F10}$$

While the first term on the right-hand side of the previous equation is strictly positive, the eigenvalues of the second one are all equal to $1 - \frac{1}{(d+1)^{N-2}}$ and are non-negative for any $N \geqslant 2$. This finishes the proof of the second step and of the whole proposition. ■

APPENDIX G

In this Appendix, we provide the proof of Remark 19 from Sec. VIII.

Proof of Remark 19. First note that all basic POVM elements for unequal probabilities p_α generalize from Eq. (57) to

$$\begin{aligned} F_N^{i,\alpha} &= p_\alpha^N |N\rangle_{i,\alpha}\langle N|, \\ F_{\text{mc},N}^{\alpha} &= p_\alpha^N \left(\mathbb{1}_N - \sum_i |N\rangle_{i,\alpha}\langle N| \right), \\ F_{\text{cc},N} &= \left(1 - \sum_{\alpha=0}^{d} p_\alpha^N\right) \mathbb{1}_N. \end{aligned} \tag{G1}$$

According to the postprocessing [Eq. (59)], the full measurement POVM elements then become

$$\begin{aligned} \tilde{F}_N^{i,\alpha} &= p_\alpha^N \left(|N\rangle_{i,\alpha}\langle N| - \frac{1}{d} \sum_{j=1}^{d} |N\rangle_{j,\alpha}\langle N| \right) \\ &\quad + \frac{(d+1)p_\alpha^N + 1 - \sum_{\beta=0}^{d} p_\beta^N}{d(d+1)} \mathbb{1}_N. \end{aligned} \tag{G2}$$

Let us consider the map $\Lambda_{P_\perp,N}$, which is applied when an incoming N-photon state triggers the $P_\perp$ flag, i.e., will with certainty produce a non-single click. We assume that $\Lambda_{P_\perp,N}$ fulfils the linear constraints in Eq. (60). Then, the probability of seeing a click in the ith detector of the detection module $\mathcal{M}_\alpha$ is given by

$$\begin{aligned} p(i,\alpha) &= \text{Tr}\left(\rho_N^\perp \tilde{F}_N^{i,\alpha}\right) = \text{Tr}\left(\Lambda_{P_\perp}[\rho_N^\perp] \tilde{F}_1^{i,\alpha}\right) \\ &= \frac{\text{Tr}\left(\mathbb{1}_D \tilde{F}_1^{i,\alpha}\right)}{d} = \frac{1}{d}, \end{aligned} \tag{G3}$$

where we used the fact $\text{Tr}(A^\dagger B) = \text{Tr}(A B^\dagger)$. The same probability can be reexpressed as

$$p(i,\alpha) = \text{Tr}\left(\rho_N^\perp P_\perp \tilde{F}_N^{i,\alpha} P_\perp^\dagger\right) = \text{Tr}\left(\rho_N^\perp \tilde{F}_{P_\perp,N}^{i,\alpha}\right). \tag{G4}$$

By virtue of Eq. (G2),

$$\tilde{F}_{P_\perp,N}^{i,\alpha} = \frac{(d+1)p_\alpha^N + 1 - \sum_{\beta=0}^{d} p_\beta^N}{d(d+1)} \mathbb{1}_{P_\perp,N}, \tag{G5}$$

and hence

$$p(i,\alpha) = \frac{(d+1)p_\alpha^N + 1 - \sum_{\beta=0}^{d} p_\beta^N}{d(d+1)}. \tag{G6}$$

Finally, a direct comparison of Eqs. (G3) and (G6) implies that

$$\frac{(d+1)p_\alpha^N + 1 - \sum_{\beta=0}^{d} p_\beta^N}{d(d+1)} = \frac{p_\alpha}{d} \tag{G7}$$

must hold for any N and for any α. Taking the limit $N \to \infty$ in the last equation, we immediately see that the only beam-splitter ratio that respects the linear constraints is the one with $p_\alpha = 1/(d+1)$. ■

[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] C. H. Bennett, G. Brassard, and A. K. Ekert, Sci. Am. **267**, 50 (1992).

[3] G. Berlin, G. Brassard, F. Bussieres, and N. Godbout, Phys. Rev. A **80**, 062321 (2009).

[4] G. Berlin, G. Brassard, F. Bussieres, N. Gobout, J. A. Slater, and W. Tittel, Nat. Commun. **2**, 561 (2011).

[5] N. Lütkenhaus, Phys. Rev. A **59**, 3301 (1999).

[6] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).

[7] M. Koashi, Y. Adachi, T. Yamamoto, and N. Imoto, arXiv:0804.0891.

[8] Chi-Hang Fred Fung, H. F. Chau, and H.-K. Lo, Phys. Rev. A **84**, 020303(R) (2011).

[9] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).

[10] N. J. Beaudry, T. Moroder, and N. Lütkenhaus, Phys. Rev. Lett. **101**, 093601 (2008).

[11] T. Tsurumaru and K. Tamaki, Phys. Rev. A **78**, 032302 (2008).

[12] T. Tsurumaru, Phys. Rev. A **81**, 012328 (2010).

[13] A. A. Semenov and W. Vogel, Phys. Rev. A **83**, 032119 (2011).

[14] H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).

[15] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).

[16] T. Durt, D. Kaszlikowski, J. L. Chen, and L. C. Kwek, Phys. Rev. A **69**, 032313 (2004).

[17] A. Ferenczi, V. Narasimhachar, and N. Lütkenhaus, Phys. Rev. A **86**, 042327 (2012).

[18] S. Sunohara, K. Tamaki, and N. Imoto, arXiv:1302.1701.

[19] A. Jamiołkowski, Rep. Math. Phys. **3**, 275 (1972).

[20] M.-D. Choi, Linear Algebr. Applicat. **10**, 285 (1975).

[21] T. Moroder, O. Gühne, N. J. Beaudry, M. Piani, and N. Lütkenhaus, Phys. Rev. A **81**, 052342 (2010).

[22] L. Vandenberghe and S. Boyd, SIAM Rev. **38**, 49 (1996).

[23] R. Bhatia, *Matrix Analysis* (Springer, New York, 1997).

[24] M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004).

[25] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).

[26] X.-F. Ma and N. Lütkenhaus, Quantum Inf. Comput. **12**, 203 (2012).

[27] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[28] J. G. Rarity and P. R. Tapster, Phys. Rev. A **45**, 2052 (1992).

[29] J. G. Rarity, P. C. Owens, and P. R. Tapster, J. Mod. Opt. **41**, 2435 (1994).

[30] S. Bandyopadhyay, P. Boykin, V. Roychowdhury, and F. Vatan, Algorithmica **34**, 512 (2002).

[31] Bengtsson and Życzkowski, *Geometry of Quantum States* (Cambridge University Press, Cambridge, UK, 2006).

[32] B. Yurke, S. L. McCall, and J. R. Klauder, Phys. Rev. A **33**, 4033 (1986).

[33] Z. Ou, C. Hong, and L. Mandel, Opt. Commun. **63**, 118 (1987).

[34] S. Gerschgorin, Bull. Acad. Sci. URSS, Cl. Sci. Math. Nat. **6**, 749 (1931).