Security against eavesdropping in quantum cryptography

Norbert Lütkenhaus
Department of Physics and Applied Physics, University of Strathclyde, John Anderson Building, 107 Rottenrow, Glasgow G4 0NG, Scotland

(Received 2 June 1995; revised manuscript received 12 February 1996)

A sharp estimate is given for the amount of Shannon information and expected collision probability. This estimate is valid for all eavesdropping strategies described by a generalized measurement and restricted to the Hilbert space of the one-photon state. The optimal generalized measurement is explicitly given. [S1050-2947(96)00907-9]

PACS number(s): 03.65.−w, 42.79.Sz, 89.70.+c

I. INTRODUCTION

It is well known that a binary message can be unbreakably encoded using a key consisting of a random sequence of zeros and ones [1]. Sender and receiver have to share the knowledge of that key. The only threat to this way of encoding messages is that the key may be subject to spying during distribution and storage.

Quantum cryptography is a way to circumvent these problems as it allows the secure creation of a key at the time and place it is needed. I will give only a short introduction to quantum cryptography. For more detailed descriptions see, for example, [2–4]. The scenario in which the key establishment takes place is depicted in Fig. 1. The sender of a message, Alice, is connected to the receiver Bob by two channels. The first channel shows classical behavior as, for example, a radio transmitter does, and the second is a quantum channel such as an optical fiber transporting single photons. An eavesdropper Eve has full access to the information flow on the classical channel but she can listen only and cannot tamper with the signals. On the other hand she can tamper with the signals on the quantum channel but the information is not fully accessible to her because of the measurement's back reaction onto the system and the impossibility of cloning quantum states [5].

There are several ways to implement a quantum cryptographical system by means of the two channels [6–9]. The first was proposed by Bennett and Brassard [2] and I will concentrate on this scheme, abbreviated as BB84, in this article. In the BB84 protocol two sets of orthogonal photon states are used. The overlap of type $|\langle\phi_1|\phi_3\rangle|^2$ between states from different sets is $\frac{1}{2}$. As an example we may think of the first set as vertical and horizontal linear polarized photon states and of the second set as right and left circular polarized photon states.

In the first step of establishing the key Alice sends a random sequence of signals built up from the four possible signal states, each appearing with equal probability. Bob possesses two measurement apparatuses adapted to the two sets of signal states. He may distinguish either between vertical and horizontal linear polarized photons or between right and left circular polarized photons. For each of the signals sent to him by Alice he chooses with equal probability an apparatus to use. The results of the measurements can be divided into two sets. The first set of signals and measurement results are those where the signal fits the measurement apparatus, resulting in a deterministic outcome of the measurement. The other set contains those photons where the measurement apparatus does not fit, resulting in purely probabilistic results. Alice and Bob now use as a second step the radio transmitter and announce for each photon sent the set of signals it was chosen from, linear or circular polarized, and the apparatus used to measure it. This is enough to distinguish the deterministic from the nondeterministic outcomes. In a third step they discard all the probabilistic measurement outcomes. The remaining data form the so-called *sifted key* [10].

In case Eve attempts to measure the signal as it passes through the quantum channel she will, on average, corrupt part of the signal. This becomes clear as there is no nondemolition measurement which can operate reliably on nonorthogonal states. Nonorthogonality is crucial here [11]. Alice and Bob may thus perform a test for the presence of Eve by comparing a fraction of their remaining deterministic data consisting of the actual signal and the actual measurement outcome. If they find discrepancies they know about the presence of Eve and must try to establish a new key. On the other hand, the absence of errors shows that the transmission was not eavesdropped upon and the remaining data may be used for encoding of the actual message. The encoded message will be sent via the radio transmitter or other suitable classical channel.

The BB84 scheme in this form works only on a noiseless quantum channel. Noise will inevitably lead to errors in the compared data during the last step. To get the scheme working again we have to extend it to cope with a mild form of eavesdropping which will lead to a disturbance of the signal comparable to that caused by noise. This has been treated by different authors. In particular, a recent discussion of the effects of von Neumann measurements performed by Eve has been given by Ekert *et al.* [12]. By von Neumann measurements I mean those described by a collapse of the wave function into an eigenstate of a Hermitian operator. The key

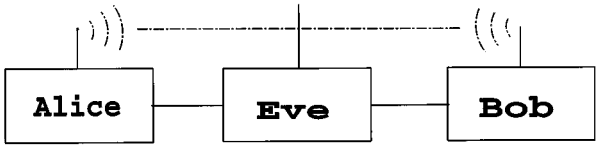

FIG. 1. The setup with quantum and classical channels.

ingredient is to define a quantity describing the disturbance of the system and to relate this to the information Eve gets by interacting with the system. Alice and Bob may then measure the disturbance and infer an estimate on Eve's Shannon information or expected collision probability about the key. The Shannon information is of importance in estimating the amount of information available to Eve in the context of using a Wyner wiretap channel [13]. The expected collision probability is of importance in deleting Eve's information about the key after some error correction. Eve's information is deleted by the process of privacy amplification [14,15] at the cost of the length of the key.

In this paper I present a sharp estimate for the Shannon information and the expected collision probability Eve can gain by performing *general measurements* on single-photon states as they pass from Alice to Bob. The paper is organized as follows in Sec. II the basic quantities describing the key establishing process are defined and I introduce measures for the Shannon information, the expected collision probability, and for the disturbance of the transmission. Section III introduces generalized measurements, the *positive operator measures* (POM). In Sec. IV I give a sharp estimate of Eve's information in the case that all operations are done in the Hilbert space of a one-photon state. In Sec. V the optimal strategy of the eavesdropper is given. A simple model for noise is applied in Sec. VI to demonstrate the consequence of the estimates.

II. BASIC QUANTITIES

The system is described by the joint probabilities of Alice sending a specific signal and Bob finding a specific outcome of a measurement. We denote the signals of the first alphabet as $|\phi_1\rangle$ and $|\phi_2\rangle$ and the signals of the second alphabet as $|\phi_3\rangle$ and $|\phi_4\rangle$. The corresponding measurements are characterized by two projectors each. The first one by $E_1=|\phi_1\rangle\langle\phi_1|$ and $E_2=|\phi_2\rangle\langle\phi_2|$ and the second one by projectors E_3 and E_4 onto the states $|\phi_3\rangle$ and $|\phi_4\rangle$. In terms of a representation we may choose

$$|\phi_1\rangle=\begin{pmatrix}1\\0\end{pmatrix}\quad |\phi_2\rangle=\begin{pmatrix}0\\1\end{pmatrix}, \tag{1}$$

$$|\phi_3\rangle=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}\quad |\phi_4\rangle=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}. \tag{2}$$

This representation reflects the fact that the Hilbert space of the polarization of a single photon is equivalent to that of a spin-$\frac{1}{2}$ particle. For the following calculations the notion of a single photon and a spin-$\frac{1}{2}$ particle is interchangeable. For example, the signal states $|\phi_1\rangle$ and $|\phi_2\rangle$ can then be viewed as spin-up and spin-down states, respectively. We define the matrix $\mathcal{P}_{AB}$ to be the matrix of the joint probabilities for sending signal i and receiving signal j. They are of the type $\frac{1}{4}\mathrm{Tr}_{\mathcal{H}}(\rho_i\frac{1}{2}E_j)$. Here ρ_i is the density matrix corresponding to the state $|\phi_i\rangle$. I denote by the symbol $\mathrm{Tr}_{\mathcal{H}}(.)$ the trace over the two-dimensional Hilbert space. The factor $\frac{1}{4}$ is the probability of sending signal ρ_i and the factor $\frac{1}{2}$ is due to the fact that Bob chooses with equal probability between the two measurement apparatus. We find for the BB84 protocol

$$\mathcal{P}_{AB}=\frac{1}{8}\left(\begin{array}{cccc|c} E_1 & E_2 & E_3 & E_4 & \frac{1}{8}\mathrm{Tr}_{\mathcal{H}}(\rho_i E_j)\\ \hline 1 & 0 & \frac{1}{2} & \frac{1}{2} & \phi_1\\ 0 & 1 & \frac{1}{2} & \frac{1}{2} & \phi_2\\ \frac{1}{2} & \frac{1}{2} & 1 & 0 & \phi_3\\ \frac{1}{2} & \frac{1}{2} & 0 & 1 & \phi_4 \end{array}\right). \tag{3}$$

By analogy with this definition we define the entries of the matrix $\mathcal{P}_{AEB}$ to be the same joint probabilities for the outcomes of the measurements, but this time in the presence of either Eve or noise on the channel. This means that we generalize the matrix elements $\frac{1}{4}\mathrm{Tr}_{\mathcal{H}}(\rho_i\frac{1}{2}E_j)$ to $\frac{1}{8}\mathrm{Tr}_{\mathcal{H}}(\widetilde{\rho}_i E_j)$, where $\widetilde{\rho}_i$ denotes the corrupted signal. By comparing signals and outcomes one can actually determine the matrix $\mathcal{P}_{AEB}$, while the matrix $\mathcal{P}_{AB}$ is a theoretical idealized object.

A. Shannon information

The string of Eve's measurement results contains a certain amount of Shannon information I about the key sent by Alice. We are interested in the Shannon information per signal of the key after the announcement of the used alphabets, and thus we keep the signals belonging to different alphabets separated. In general the Shannon information per bit I is given by [16]

$$I(\mathcal{P})=\sum_i H\left(\sum_k \mathcal{P}^{ik}\right)+\sum_k H\left(\sum_i \mathcal{P}^{ik}\right)-\sum_{ik} H(\mathcal{P}^{ik}), \tag{4}$$

where

$$H(\alpha)=-\alpha\log_2\alpha \tag{5}$$

and the $\mathcal{P}^{ik}$ are the joint probabilities of sending a signal i and receiving a signal k. All logarithms refer to base 2 so that information is expressed in bits per signal. In the situation where we calculate the information Eve receives, i represents the four signal states $|\phi_i\rangle$, and the range of values of k represents all the possible outcomes of a measurement performed by Eve.

The information $I(\mathcal{P})$ is a convex function over the set of probability matrices with fixed *a priori* probabilities for each signal [16]. This allows us to use Jensen's inequality

$$I\left(\sum_i p_i\mathcal{P}_i\right)\leqslant\sum_i p_i I(\mathcal{P}_i), \tag{6}$$

which estimates the information gain of a mixture of strategies, used in parallel with probability p_i and resulting in joint probability matrices $\mathcal{P}_i$, by the average of the information gain associated with the single strategies. If we combine two separate measurement outcomes into a single new one the information decreases [16]. That means that combining two rows or columns by replacing them with their sum will

decrease the amount of Shannon information. Any permutation within either the signals or the outcomes will not change the amount of information.

Next I consider the case in which the set of outcomes can be separated into two subsets such that the *a priori* probability of the signals across both subsets of outcomes separately are, up to a fixed factor of p and $1-p$, respectively, the *a priori* probabilities across the whole set of outcomes. This means that the measurement apparatus can be viewed as consisting of two apparatuses used interchangeably with the probabilities p and $1-p$. In this case we find that the information gained by the use of the composed system is equal to the sum of the information gained by the subsystems, weighted with the probability of their use. This is expressed as

$$I([p\mathcal{P}_1,(1-p)\mathcal{P}_2])=pI(\mathcal{P}_1)+(1-p)I(\mathcal{P}_2), \tag{7}$$

where $[\ldots,\ldots]$ denotes the composed matrix. We obtain a similar property by interchanging signals and outcomes which allows us to separate information with respect to two subsets of signal states.

B. Expected collision probability

Eve's information about the key consists of two parts. The first is the string of outcomes of the measurements performed by Eve on the signals and the second is the knowledge about the correlation of those outcomes to the signals. This knowledge can be quantified. The easiest way Eve can guess the key from her measurement data is in the case of a von Neumann measurement to call one outcome '0' and the other '1.' It is, however, not obvious how to transfer this to the general positive operator measure situation, described later, which deals with several different possible outcomes. The solution lies in the possibility of assigning a probability to all keys possibly sent by Alice to be the one originally sent. This is the conditional probability $p(x|y)$ that x is the key when Eve measured the string of outcomes y. This probability can be calculated from the known probability that a given signal triggers one of the outcomes. A possible attack by Eve on the message is to try several keys chosen according to the probability distribution $p(x|y)$. It is intuitively clear that a sharply peaked probability distribution over the set of possible keys will help Eve to decode the message as this will affect the decoding time. The *collision probability* $p_c(y):=\Sigma_x p^2(x|y)$ is the probability of drawing the same key x twice.

The *expected collision probability* is defined as $\langle p_c(y)\rangle:=\Sigma_y p(y)p_c(y)$ with $p(y)$ as the probability for Eve to find outcome string y. In a forthcoming paper [15] it is shown that this quantity plays a central role in the process of privacy amplification. In the case of a lowest upper bound τ in the sense

$$1+\log_2\langle p_c(y)\rangle^{\frac{1}{n}}\leqslant\tau \tag{8}$$

can be given for a key of length n and $\tau\in[0,1)$, we can cut out Eve's Shannon information on the key by shortening it during privacy amplification. A reduction of the key length by $n\tau+s$ bits, where s is a safety parameter, leaves Eve with a total Shannon information of less than $s^{-s}/\ln 2$ bit on the new key of length $n(1-\tau)-s$.

In the case of the BB84 protocol we can formulate the expression for the expected collision probability using the joint probabilities for sending a specific signal and receiving a specific outcome and using the total probability of the specific outcomes. More precisely we are interested in the expected collision probability after the public announcement of the alphabets used. For this purpose we introduce a parallel notation $|\psi_\alpha\rangle$ for the signals by ψ_α where $\psi=0,1$ is the logical value of the signal and α indexes the alphabet. We identify $|0_1\rangle\equiv|\phi_1\rangle$, $|1_1\rangle\equiv|\phi_2\rangle$, $|0_2\rangle\equiv|\phi_3\rangle$ and $|1_2\rangle\equiv|\phi_4\rangle$. Eve receives the signals k_α consisting of the outcome k of a measurement performed by her and the later acquired knowledge about the alphabet used, which is indicated again by α.

In order to reexpress the expected collision probability in terms of the joint probabilities $p(\phi_\alpha,k_\alpha)$ and the probabilities $p(k_\alpha)$ we use the fact that the transmission of each photon is independent of the others. Then we find the conditional probability $p(x|y)$ for the whole key to be the product of the conditional probability for each single key signal and outcome, that is,

$$p(x|y)=\prod_i\left(\frac{p(\psi_\alpha,k_\alpha)}{p(k_\alpha)}\right)_i, \tag{9}$$

where in the ith factor ψ_α and k_α are the ith signal of x and the ith outcome of y. We next define numbers M_{k_α} and $m_{0_\alpha k_\alpha}$. For a sequence of n signals Eve will find in the sequence of outcomes y the outcome k_α a total of M_{k_α} times. Of those M_{k_α} signals the number of $m_{0_\alpha k_\alpha}$ will be triggered by the signal $|0_\alpha\rangle$. The remaining $(M_{k_\alpha}-m_{0_\alpha k_\alpha})$ are triggered by the state $|1_\alpha\rangle$. With this notation we find, taking into account the different permutations of strings, that

$$\begin{aligned}p_c(y)=\sum_x p^2(x|y)&=\sum_{m_{0_\alpha k_\alpha}\leqslant M_{k_\alpha}}\prod_{k_\alpha}\binom{M_{k_\alpha}}{m_{0_\alpha k_\alpha}}\\&\times\left(\frac{p(0_\alpha,k_\alpha)}{p(k_\alpha)}\right)^{2M_{k_\alpha}}\left(\frac{p(1_\alpha,k_\alpha)}{p(k_\alpha)}\right)^{2(M_{k_\alpha}-m_{0_\alpha k_\alpha})}\\&=\prod_{k_\alpha}\left[\left(\frac{p(0_\alpha,k_\alpha)}{p(k_\alpha)}\right)^2+\left(\frac{p(1_\alpha,k_\alpha)}{p(k_\alpha)}\right)^2\right]^{M_{k_\alpha}}.\end{aligned}$$

To calculate the expected collision probability we need the probabilities $p(M)$ that Eve receives the set of numbers M_{k_α} as measurement outcomes. This probability is given by

$$p(M)=\frac{n!}{M_{0_1}!M_{0_2}!M_{1_1}!\ldots M_{k_\alpha}!\ldots}\prod_{k_\alpha}p(k_\alpha)^{M_{k-\alpha}}. \tag{10}$$

The expectation value is taken over all values of the M_{k_α} with $\Sigma_{k_\alpha}M_{k_\alpha}=n$. We used the probabilities $p(k_\alpha)$ for triggering the different outcomes k_α by the equally distributed signal states.

As a result we find the expression for the expected collision probability as

$$\langle p_c(y)\rangle = \left(\sum_{k,\alpha,\psi} \frac{p(\psi_\alpha,k_\alpha)^2}{p(k_\alpha)} \right)^n . \tag{11}$$

We will later concentrate on the relative expected collision probability

$$\langle p_c(y)\rangle^{\frac{1}{n}} = \sum_{k,\alpha,\psi} \frac{p(\psi_\alpha,k_\alpha)^2}{p(k_\alpha)} \tag{12}$$

as this is the quantity needed to find the estimating parameter τ corresponding to the minimum fraction of bits to be discarded during privacy amplification.

C. Disturbance

We are now in a position to look for a measure of the disturbance affecting the signals during the transmission on the quantum channel. The simplest measures are based on the joint probabilities of signals sent and outcomes measured. These joint probabilities can be measured directly by Alice and Bob by comparing a fraction of their signals and measured outcomes.

To maximize the sensitivity of the measure of the disturbance we monitor all of these joint probabilities and define the disturbance based on the measured joint probabilities $\mathcal{P}_{AEB}$ and the theoretical predicted probabilities $\mathcal{P}_{AB}$ as

$$D := \|\mathcal{P}_{AB} - \mathcal{P}_{AEB}\|_F , \tag{13}$$

where the Frobenius norm (or Schur or Hilbert-Schmidt norm) of a real matrix $M=\{M_{ij}\}$ is defined [17] as

$$\|M\|_F := \left(\sum_{ij} {M_{ij}}^2 \right)^{1/2} . \tag{14}$$

Other choices are possible, for example, related to the measure of fidelity [18], the definition

$$D_f := \mathrm{Tr}_{\mathcal{P}}(\mathcal{P}_{AB} - \mathcal{P}_{AEB}), \tag{15}$$

where the trace is taken over the matrix indices given as the index of the signals sent and the outcomes measured. In Sec. III we show that $D \geqslant (1/\sqrt{2})\, D_f$. The measure D_f depends only on the diagonal elements of $\mathcal{P}_{AB}$ and $\mathcal{P}_{AEB}$ while D depends on all of them. It follows that D is a stronger measure of disturbance than D_f in that it is more sensitive to intervention by Eve. The optimal choice of the disturbance measure can be determined only in connection with a good model for the expected measured joint probabilities (that is, in connection with a good noise model for the channel). Such an analysis is beyond the scope of this paper.

The disturbance D is zero if and only if all measured joint probabilities equal their theoretical predictions, that is, $\mathcal{P}_{AB}=\mathcal{P}_{AEB}$. The Frobenius norm satisfies

$$\|\alpha M\|_F = |\alpha| \|M\|_F$$

and the triangle inequality

$$\Big| \|M\|_F - \|N\|_F \Big| \leqslant \|M+N\|_F \leqslant \|M\|_F + \|N\|_F . \tag{16}$$

Another feature of the Frobenius norm is that it is invariant under unitary transformations, that is,

$$\|M\|_F = \|UM\|_F = \|MV\|_F = \|UMV\|_F , \tag{17}$$

with U and V unitary. This property makes the Frobenius norm convenient to use in connection with the singular value decomposition. Every real matrix M ($M \in \mathbb{R}^{m\times n}$) can be represented in the form [17]

$$M = USV \tag{18}$$

with U and V unitary. The matrix S is a quasidiagonal in the sense that for $S=\{s_{ij}\}$ we find

$$s_{ij} = \begin{cases} 0 & i \neq j \\ s_i & i = j \end{cases} \quad \text{with } s_i \geqslant 0 . \tag{19}$$

The diagonal elements s_i are called the singular values of the matrix M and are uniquely determined up to a permutation. For a symmetric matrix these singular values are the eigenvalues of the matrix. Since the Frobenius norm is invariant under unitary transformations we find

$$\|M\|_F = \|S\|_F = \sqrt{\sum_i s_i^2} . \tag{20}$$

There are two main properties of the disturbance D which we will use later on. The first concerns a mixture of different strategies, which Eve uses with probability p_i and result in the matrices $\mathcal{P}^{(i)}_{AEB}$, leading to a combined $\mathcal{P}_{AEB} = \Sigma_i p_i \mathcal{P}^{(i)}_{AEB}$. The disturbance caused by this eavesdropping strategy can be estimated by the disturbance of each substrategy by

$$D\left(\sum_i p_i \mathcal{P}_i \right) \leqslant \sum_i p_i D(\mathcal{P}_i) \tag{21}$$

using the triangle inequality (16). A mixing of strategies may thus result in a lower disturbance. The other property of the disturbance D is that it is invariant under any permutations of the signals or of the outcomes.

III. POM AND WHAT HAPPENS TO THE SIGNAL

A. POM

A *positive operator measure* [19–21] on a Hilbert-space $\mathcal{H}$ is defined to be a set of positive Hermitian operators which add up to the identity on the Hilbert-space $\mathcal{H}$,

$$\sum_i F_i = \mathbb{1}_{\mathcal{H}} . \tag{22}$$

Each F_i corresponds to an outcome of a measurement. The probability p_i of the ith outcome of a measurement performed on a signal with density matrix ρ is given by

$$p_i = \mathrm{Tr}_{\mathcal{H}}(\rho F_i). \tag{23}$$

As long as we restrict our description to a situation where single-photon states reach Eve and Eve forwards another single-photon state we can use the two-dimensional Hilbert space of the polarization of a single photon. Then we can simplify the definition to the following: A POM is given by

a set of Hermitian complex 2×2 matrices with eigenvalues ranging in the interval $[0,1]$ whose sum is the two-dimensional identity matrix.

A trivial example is the POM representing a von Neumann measurement which is described by two orthogonal projection operators. They can be represented in a suitable basis of the two-dimensional Hilbert space as

$$F_1=\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix},\quad F_2=\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}. \tag{24}$$

A first advantage of using POMs is that we can describe quite simply and generally eavesdropping strategies where Eve chooses for each signal one strategy out of a set of von Neumann measurements or does not interfere at all. For example, the POM with

$$F_1=\begin{pmatrix}\frac{1}{3} & 0\\ 0 & 0\end{pmatrix},\quad F_2=\begin{pmatrix}0 & 0\\ 0 & \frac{1}{3}\end{pmatrix}, \tag{25}$$

$$F_3=\begin{pmatrix}\frac{1}{6} & \frac{1}{6}\\ \frac{1}{6} & \frac{1}{6}\end{pmatrix},\quad F_4=\begin{pmatrix}\frac{1}{6} & -\frac{1}{6}\\ -\frac{1}{6} & \frac{1}{6}\end{pmatrix},$$

$$F_5=\begin{pmatrix}\frac{1}{3} & 0\\ 0 & \frac{1}{3}\end{pmatrix},$$

describes a strategy where Eve measures with equal probability either in the $\{\phi_1,\phi_2\}$ basis (F_1,F_2), or in the $\{\phi_3,\phi_4\}$ basis (F_3,F_4), or does not interfere F_5. The noninterference is described by a POM element proportional to the identity matrix and corresponds to at most noting that there is a photon but not measuring its states. As a major difference from the von Neumann measurements the elements of a POM need not be proportional to a projection operator. For example, the matrix

$$\widetilde{F}=\begin{pmatrix}\frac{1}{2} & 0\\ 0 & \frac{1}{3}\end{pmatrix} \tag{26}$$

may be an element of a POM. It can be represented by the decomposition

$$\widetilde{F}=\frac{1}{2}\left[\frac{2}{3}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}+\frac{1}{3}\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\right], \tag{27}$$

which can be seen as a mixture of two strategies used with probability $\frac{1}{3}$ and $\frac{2}{3}$, respectively. The first is a pure counting as represented by the first matrix while the second matrix represents the measuring of the overlap with a pure state. However, the observer does not know by which strategy the outcome which represents $\widetilde{F}$ was triggered. To give this knowledge to Eve, she has to perform a measurement which splits $\widetilde{F}$ up into the two possible POM elements on the right-hand side.

One might hope that all POM sets can be viewed as consisting of a mixture of von Neumann projector elements and the identity operation. This is, however, not true [22]. An example is the POM with three elements given by projectors which are rotated by an angle of $2\pi/3$,

$$\begin{pmatrix}\frac{1}{3} & 0\\ 0 & 0\end{pmatrix},\quad \begin{pmatrix}\frac{1}{3}\cos\frac{2\pi}{3} & \frac{1}{3}\sin\frac{2\pi}{3}\\ -\frac{1}{3}\sin\frac{2\pi 3}{3} & \frac{1}{3}\cos\frac{2\pi}{3}\end{pmatrix},$$

$$\begin{pmatrix}\frac{1}{3}\cos\frac{4\pi}{3} & \frac{1}{3}\sin\frac{4\pi}{3}\\ -\frac{1}{3}\sin\frac{4\pi}{3} & \frac{1}{3}\cos\frac{4\pi}{3}\end{pmatrix}. \tag{28}$$

All POMs can be represented as a set of projection operators in a higher-dimensional Hilbert space [23]. Up to now it is not clear whether all POMs can be physically realized in a measurement apparatus. However, it is widely accepted [19] that all measurement apparatus can be characterized by a POM. This is obvious at least for a mixture of von Neumann measurements as shown in the example (25). In Appendix A, I give a POM which describes a more complicated measurement on a two-level system. For further examples see [19]. All measurements and, hence, all eavesdropping strategies can therefore be described by a POM. Given the POM we can calculate Eve's Shannon information I and expected collision probability $\langle p_c\rangle$. For this we only need to calculate the joint probabilities for the outcomes of the type $\frac{1}{4}\mathrm{Tr}_{\mathcal{H}}(\rho_i F_k)$.

B. Back reaction of a POM measurement onto the system

Up to now we have not considered the back reaction of a POM measurement onto the measured system. I report some results derived by Davies and Kraus [20,21] which describe the most general measurements, their outcome, and the corresponding back reaction. The assumption for this description is that the measurement has the property to be completely positive [21]. This property may be viewed [24] as allowing the existence of a third system of arbitrary dimension in addition to the measuring device and the system under investigation. This requirement is naturally fulfilled [24,25] since by randomly choosing the signals $|\phi_i\rangle$ the initial state of the combined system of eavesdropper and signal is given as a product state $\rho_i\otimes\rho_E$ with an eavesdropper state ρ_E independent of the signal states. This assures complete positivity. The basic object of this description is a set of matrices A_k. The index set K is partitioned into n subsets K_i. The matrices A_k are any complex matrices which satisfy the restriction that the elements F_i defined by

$$\widetilde{F}_i=\sum_{k\in K_i}A_k^{\dagger}A_k \tag{29}$$

make up a POM.

Given any such set of matrices A_k we can describe the back reaction onto a system with a density-matrix ρ as a change to the density-matrix $\widetilde{\rho}$ after the measurement. In the case of a nonselective measurement considered here the density matrix is given by

$$\widetilde{\rho}=\sum_{k\in K} A_k \rho A_k^\dagger . \tag{30}$$

A nonselective measurement always forwards the measured system and does not suppress it depending on the outcome of the measurement. The probability p_i of the outcome i is given by

$$p_i=\mathrm{Tr}_{\mathcal{H}}\left(\rho \sum_{K_i} A_k^\dagger A_k \right). \tag{31}$$

It is always true that the set with the elements

$$F_i=A_i^\dagger A_i \quad i\in K \tag{32}$$

forms a POM [21]. As far as the disturbance is concerned it does not matter which subset of K is grouped into which POM element since the disturbed density matrix (30) contains the sum over the whole set. For the information gained by the measurement the grouping does matter. Thus an eavesdropping strategy is characterized by a set of A matrices together with a partition of this set to form the POM describing the outcome of the measurements.

IV. SECURITY AGAINST POM ATTACK

In this section, I give an estimate of the amount of Shannon information and expected collision probability Eve can gain by applying an eavesdropping strategy which resends one-photon states to Bob. Thus she performs nonselective measurements. The signal states sent by Alice are one-photon states as well and thus the description of the measurement is given by the previously summarized formalism. In this calculation we deal with the BB84 protocol only. It can be easily generalized to other cryptographical protocols which use nonorthogonal basis sets of orthogonal signals which no longer have the overlap $\frac{1}{2}$.

A. Disturbance

As a preparation we deal with the disturbance alone. The disturbance is a function of the joint probabilities $\mathcal{P}_{AEB}^{ij}$ of Alice sending signal i and Bob receiving signal j. These joint probabilities are given by

$$\mathcal{P}_{AEB}^{ij}=\frac{1}{8}\sum_k \mathrm{Tr}_{\mathcal{H}}(A_k \rho_i A_k^\dagger E_j). \tag{33}$$

Eve's original strategy is described by A matrices which can be represented in the form

$$A_k=\sqrt{a_k}U_k+(\sqrt{b_k}-\sqrt{a_k})U_k P_k \tag{34}$$

with non-negative real numbers a_k and b_k satisfying $0\leqslant a_k \leqslant b_k$, U_k being unitary matrices and P_k being one-dimensional projection operators. The properties (29) and (22) imply

$$\sum_k (a_k+b_k)=2. \tag{35}$$

In the following I show that a replacement of the original strategy by the one given by

$$\widetilde{A}_k=\sqrt{a_k}U_k+(\sqrt{b_k}-\sqrt{a_k})U_k\overline{P_k} \tag{36}$$

does not change the disturbance. Here and in the following chapters over-lined objects are orthogonal complements, for example, $\overline{P_k}=\mathbb{1}-P_k$.

I insert Eq. (34) into (36) and find after some manipulation

$$\begin{aligned}\mathcal{P}_{AEB}^{ij}=\sum_k \{&\tfrac{1}{8}\sqrt{a_k b_k}\mathrm{Tr}_{\mathcal{H}}(U_k\rho_i U_k^\dagger E_j)+\tfrac{1}{8}\sqrt{a_k}(\sqrt{b_k}-\sqrt{a_k})\\ &\times[\mathrm{Tr}_{\mathcal{H}}(U_k P_k \rho_i P_k U_k^\dagger E_j)-\mathrm{Tr}_{\mathcal{H}}(U_k\overline{P_k}\rho_i\overline{P_k}U_k^\dagger E_j)]\\ &+\tfrac{1}{8}(\sqrt{b_k}-\sqrt{a_k})^2\mathrm{Tr}_{\mathcal{H}}(U_k P_k\rho_i P_k U_k^\dagger E_j)\}.\end{aligned} \tag{37}$$

We make use of the decomposition of the type

$$\mathrm{Tr}_{\mathcal{H}}(U_k P_k \rho_i P_k U_k^\dagger E_j)=\mathrm{Tr}_{\mathcal{H}}(P_k\rho_i)\mathrm{Tr}_{\mathcal{H}}(P_k U_k^\dagger E_j U_k) \tag{38}$$

and of identities of type

$$\mathrm{Tr}_{\mathcal{H}}(P_k\rho_i)=\mathrm{Tr}_{\mathcal{H}}(\overline{P_k}\,\overline{\rho_i}) \tag{39}$$

to find

$$\begin{aligned}\mathcal{P}_{AEB}^{ij}=\sum_k \{&\tfrac{1}{8}\sqrt{a_k b_k}\mathrm{Tr}_{\mathcal{H}}(U_k\overline{\rho_i}U_k^\dagger\overline{E_j})+\tfrac{1}{8}\sqrt{a_k}(\sqrt{b_k}-\sqrt{a_k})\\ &\times[\,\mathrm{Tr}_{\mathcal{H}}(U_k\overline{P_k}\,\overline{\rho_i}\,\overline{P_k}U_k^\dagger\overline{E_j})-\mathrm{Tr}_{\mathcal{H}}(U_k P_k\overline{\rho_i}P_k U_k^\dagger\overline{E_j})]\\ &+\tfrac{1}{8}(\sqrt{b_k}-\sqrt{a_k})^2\,\mathrm{Tr}_{\mathcal{H}}(U_k\overline{P_k}\,\overline{\rho_i}\,\overline{P_k}U_k^\dagger\overline{E_j})\}.\end{aligned} \tag{40}$$

This shows that using the strategy described by $\widetilde{A_k}$ together with a toggling of lines and rows, belonging to orthogonal signals and measurement projectors, in the joint probability matrix $\mathcal{P}_{AEB}^{ij}$ leaves this matrix invariant. This is because the orthogonal complements of signals are contained in the set of signals and the same is true for the projection operators E_i describing Bob's measurement. The matrix $\mathcal{P}_{AB}$ turns out to be invariant under this toggling. Thus changing the strategy does not affect the value of the measured disturbance and we find

$$D[\{A_k\}_k]=D[\{\widetilde{A_k}\}_k]. \tag{41}$$

The notation $\{.\}_k$ is used to indicate that the index runs over all k. Now we can show that the disturbance decreases by mixing both strategies with equal probability. This is proven by using (21) and (41) to find

$$\begin{aligned}D[\{A_k\}_k]&=\tfrac{1}{2}D[\{A_k\}_k]+\tfrac{1}{2}D[\{\widetilde{A_k}\}_k]\\ &\geqslant D\left[\left\{\frac{1}{\sqrt{2}}A_k\right\}_k\cup\left\{\frac{1}{\sqrt{2}}\widetilde{A_k}\right\}_k\right].\end{aligned} \tag{42}$$

Applying a decomposition (34), (36) in the same way as in (40) we find for the disturbance

$$D\left[\left\{\frac{1}{\sqrt{2}}A_k\right\}_k \cup \left\{\frac{1}{\sqrt{2}}\widetilde{A_k}\right\}_k\right]$$
$$= \frac{1}{8}\Big\| \mathrm{Tr}_{\mathcal{H}}(\rho_i E_j) - \sum_k \left[\sqrt{a_k b_k}\,\mathrm{Tr}_{\mathcal{H}}(\rho_i U_k^\dagger E_j U_k)\right]$$
$$- \sum_k \left(\frac{(\sqrt{b_k}-\sqrt{a_k})^2}{2}\left[\mathrm{Tr}_{\mathcal{H}}(U_k P_k \rho_i P_k U_k^\dagger E_j)\right.\right.$$
$$\left.\left. + \mathrm{Tr}_{\mathcal{H}}(U_k \overline{P_k} \rho_i \overline{P_k} U_k^\dagger E_j)\right]\right)\Big\|_{\mathrm{F}}. \tag{43}$$

Since the Frobenius norm is strongly connected to singular values we have a closer look at the eigensystem of the matrix we are taking the Frobenius norm of. We find that there are two eigenvectors associated with the eigenvalue zero. These are the vectors $\frac{1}{2}(1,1,1,1)$ and $\frac{1}{2}(1,-1,1,-1)$. The existence of the eigenvectors is purely due to the fact that we use two sets of orthogonal signals and corresponding measurement operators. These two eigenvectors form the *structural eigensystem*. The orthogonal complement is two dimensional which means that the whole matrix has at most two nonvanishing singular values denoted by σ_1 and σ_2. We use this fact to make the estimate

$$D[\mathcal{P}_{AB}-\mathcal{P}_{AEB}] = \left[\sum_{i=1}^{2} (\sigma_i[\mathcal{P}_{AB}-\mathcal{P}_{AEB}])^2\right]^{1/2} \tag{44}$$
$$\geqslant \frac{1}{\sqrt{2}}\sum_{i=1}^{2} \sigma_i[\mathcal{P}_{AB}-\mathcal{P}_{AEB}] \tag{45}$$
$$= \frac{1}{\sqrt{2}}\sum_{i=1}^{4} \sigma_i[\mathcal{P}_{AB}-\mathcal{P}_{AEB}]. \tag{46}$$

To come from the first to the second line I used the inequality $x^2+y^2 \geqslant (x+y)^2/2$ for all real x,y. In the last step I denoted by σ_3 and σ_4 the two structural eigenvalues of value zero and thus extended the range of the summation to that over all singular values.

For any matrix M the sum over its singular values σ_i is again a matrix norm with all the properties of a matrix norm, satisfying especially the triangle inequality. The triangle equation leads to the inequality

$$\sum_i \sigma_i[M] = \frac{1}{2}\left(\sum_i \sigma_i[M] + \sum_i \sigma_i[M^{\mathrm{T}}]\right)$$
$$\geqslant \tfrac{1}{2}\sum_i \sigma_i[\mathrm{M} + \mathrm{M}^{\mathrm{T}}] \geqslant \mathrm{Tr}_{\mathcal{P}}(M). \tag{47}$$

Here M^{T} is the transposed matrix of M. Note that the fidelity disturbance measure D_f appears in this expression as

$$D \geqslant \frac{1}{\sqrt{2}} D_f$$
$$= \frac{1}{\sqrt{2}}\mathrm{Tr}_{\mathcal{P}}\left(\mathcal{P}_{AB} - \mathcal{P}_{AEB}\left[\left\{\frac{1}{\sqrt{2}}A_k\right\}_k \cup \left\{\frac{1}{\sqrt{2}}\widetilde{A_k}\right\}_k\right]\right). \tag{48}$$

With this result and using the notation $\mathrm{Tr}_{\mathcal{P}}(.)$ to denote the trace over the probability matrix elements formed by the indices i and j we find

$$D\left[\left\{\frac{1}{\sqrt{2}}A_k\right\}_k \cup \left\{\frac{1}{\sqrt{2}}\widetilde{A_k}\right\}_k\right]$$
$$\geqslant \frac{1}{8\sqrt{2}}\mathrm{Tr}_{\mathcal{P}}[\mathrm{Tr}_{\mathcal{H}}(\rho_i E_j)]$$
$$- \sum_k \left(\sqrt{a_k b_k}\frac{1}{8\sqrt{2}}\mathrm{Tr}_{\mathcal{P}}[\mathrm{Tr}_{\mathcal{H}}(\rho_i U_k^\dagger E_j U_k)]\right)$$
$$- \sum_k \left\{\frac{(\sqrt{b_k}-\sqrt{a_k})^2}{2}\frac{1}{8\sqrt{2}}\right.$$
$$\left.\times \mathrm{Tr}_{\mathcal{P}}[\mathrm{Tr}_{\mathcal{H}}(U_k P_k \rho_i P_k U_k^\dagger E_j) + \mathrm{Tr}_{\mathcal{H}}(U_k \overline{P_k} \rho_i \overline{P_k} U_k^\dagger E_j)]\right\}. \tag{49}$$

We now deal with the three parts of this expression independently. The first part can be directly calculated using the signal representations (1) and (2) to be

$$\frac{1}{8\sqrt{2}}\mathrm{Tr}_{\mathcal{P}}[\mathrm{Tr}_{\mathcal{H}}(\rho_i E_j)] = \frac{1}{2\sqrt{2}}. \tag{50}$$

The second term can be estimated using $\mathrm{Tr}_{\mathcal{H}}(\rho_i U_k^\dagger E_j U_k) \leqslant 1$, since this expression can be interpreted as overlap between two states. From this we find that

$$\sum_k \left(\sqrt{a_k b_k}\frac{1}{8\sqrt{2}}\mathrm{Tr}_{\mathcal{P}}[\mathrm{Tr}_{\mathcal{H}}(\rho_i U_k^\dagger E_j U_k)]\right) \leqslant \frac{1}{2\sqrt{2}}\sum_k \sqrt{a_k b_k}. \tag{51}$$

The third term can be estimated, with the help of the inequality proven in Appendix B, to be

$$\frac{1}{8\sqrt{2}}\mathrm{Tr}_{\mathcal{P}}[\mathrm{Tr}_{\mathcal{H}}(U_k P_k \rho_i P_k U_k^\dagger E_j) + \mathrm{Tr}_{\mathcal{H}}(U_k \overline{P_k} \rho_i \overline{P_k} U_k^\dagger E_j)] \tag{52}$$
$$\leqslant \frac{1}{4\sqrt{2}} + \frac{1}{2\sqrt{2}}[(c_k-\tfrac{1}{2})^2 + (d_k-\tfrac{1}{2})^2]^{1/2}[(\widetilde{c}_k-\tfrac{1}{2})^2 + (\widetilde{d}_k-\tfrac{1}{2})^2]^{1/2}. \tag{53}$$

Here we have defined the overlaps $\mathrm{Tr}_{\mathcal{H}}(\rho_2 P_k) =: c_k$, $\mathrm{Tr}_{\mathcal{H}}(\rho_4 P_k) =: d_k$, $\mathrm{Tr}_{\mathcal{H}}(E_2 U_k P_k U_k^\dagger) =: \widetilde{c}_k$ and $\mathrm{Tr}_{\mathcal{H}}(E_4 U_k P_k U_k^\dagger) =: \widetilde{d}_k$. These two pairs of overlaps satisfy the inequality

$$(d-\tfrac{1}{2})^2+(c-\tfrac{1}{2})^2 \leqslant \tfrac{1}{4}, \tag{54}$$

proven in Appendix C. From this, the third term can be estimated to be

$$\sum_k \left(\frac{(\sqrt{b_k}-\sqrt{a_k})^2}{2} \frac{1}{8\sqrt{2}} \mathrm{Tr}_{\mathcal{P}}[\mathrm{Tr}_{\mathcal{H}}(U_k P_k \rho_i P_k U_k^\dagger E_j) + \mathrm{Tr}_{\mathcal{H}}(U_k \overline{P_k} \rho_i \overline{P_k} U_k^\dagger E_j)] \right) \tag{55}$$

$$\leqslant \frac{3}{8\sqrt{2}} \sum_k \frac{(\sqrt{b_k}-\sqrt{a_k})^2}{2}. \tag{56}$$

We put all three results together to find

$$D[\mathcal{P}_{AB}-\mathcal{P}_{AEB}] \geqslant \frac{\sqrt{2}}{16} \sum_k \frac{(\sqrt{b_k}-\sqrt{a_k})^2}{2}. \tag{57}$$

This result can be rewritten using the ratio $\epsilon_k := \frac{a_k}{b_k}$ as

$$D[\mathcal{P}_{AB}-\mathcal{P}_{AEB}] \geqslant \frac{\sqrt{2}}{16} \sum_k \frac{a_k+b_k}{2} \frac{(1-\sqrt{\epsilon_k})^2}{1+\epsilon_k}. \tag{58}$$

With this we have estimated the disturbance caused by an eavesdropper. The estimate depends no longer on the specific projection operators used in the A matrices of Eve's strategy.

B. Shannon information

For a given set of A matrices Eve will receive the maximal amount of Shannon information by choosing a POM where each POM element corresponds to exactly one A matrix [16]. I denote the elements of this POM by

$$F_k := A_k^\dagger A_k.$$

From (34) it then follows that the POM elements take the form

$$F_k = a_k \mathbb{1} + (b_k - a_k) P_k \qquad a_k < b_k. \tag{59}$$

I show first that a change of the original strategy to the one described by the A matrices $\widetilde{A_k}$ resulting in the POM

$$\widetilde{F_k} = a_k \mathbb{1} + (b_k - a_k) \overline{P_k} \qquad a_k < b_k \tag{60}$$

does not change the amount of Shannon information gained. The information I is a function of the joint probabilities $\mathcal{P}_{AE}^{ik}$ of Alice sending a signal i and Eve finding the outcome k. For this we find

$$\mathcal{P}_{AE}^{ik} = \tfrac{1}{4}\mathrm{Tr}_{\mathcal{H}}(\rho_i F_k) = \tfrac{1}{4}a_k + \tfrac{1}{4}(b_k-a_k)\mathrm{Tr}_{\mathcal{H}}(\rho_i P_k) = \tfrac{1}{4}a_k + \tfrac{1}{4}(b_k-a_k)\mathrm{Tr}_{\mathcal{H}}(\overline{\rho_i}\,\overline{P_k}) = \tfrac{1}{4}\mathrm{Tr}_{\mathcal{H}}(\overline{\rho_i}\widetilde{F_k}). \tag{61}$$

The signals are pure states and $\overline{\rho_i}$, as the orthogonal complement of ρ_i, is a signal state as well. The use of the second strategy described by $\widetilde{F_k}$ just toggles again lines and rows belonging to orthogonal signals and POM elements with orthogonal projector parts in the joint probability matrix. This toggling does not affect the information I. Thus we find

$$I[\{F_k\}_k] = I[\{\widetilde{F_k}\}_k]. \tag{62}$$

This result implies that an equal mixture of both strategies does not affect the amount of Shannon information either as we find from (7) and (62) that

$$I[\{F_k\}_k] = \tfrac{1}{2}I[\{F_k\}_k] + \tfrac{1}{2}I[\{\widetilde{F_k}\}_k] = I[\{\tfrac{1}{2}F_k\}_k \cup \{\tfrac{1}{2}\widetilde{F_k}\}_k]. \tag{63}$$

The union of the sets describing the two single strategies gives the description of the alternative statistical use of the two strategies. By reordering the elements of this POM we see that this can also be viewed as a statistical mixture of using the strategies consisting of the two POM elements F_k/a_k+b_k and $\widetilde{F_k}/a_k+b_k$ with the probability $a_k+b_k/2$. This means

$$I\left[\left\{\frac{1}{2}F_k\right\}_k \cup \left\{\frac{1}{2}\widetilde{F_k}\right\}_k\right] = I\left[\bigcup_k \frac{a_k+b_k}{2}\left\{\frac{F_k}{a_k+b_k}, \frac{\widetilde{F_k}}{a_k+b_k}\right\}\right] \tag{64}$$

$$= \sum_k \frac{a_k+b_k}{2} \times I\left[\left\{\frac{F_k}{a_k+b_k}, \frac{\widetilde{F_k}}{a_k+b_k}\right\}\right]. \tag{65}$$

The missing subscript k at the curly brackets indicates now that only the two named operators form the POM while k is kept fixed. We can calculate the terms $I[\{F_k/a_k+b_k, \widetilde{F_k}/a_k+b_k\}]$ using (59) and the definitions of c_k, d_k and ϵ_k from the section above. We find the result

$$I[\{F_k\}_k] = \sum_k \frac{a_k+b_k}{2}\Big[1 - \log_2(1+\epsilon_k) + \frac{1}{2(1+\epsilon_k)} \times \{(\epsilon_k + c_k - \epsilon_k c_k)\log_2(\epsilon_k + c_k - \epsilon_k c_k) + (1-c_k+\epsilon_k c_k)\log_2(1-c_k+\epsilon_k c_k) + (\epsilon_k + d_k - \epsilon_k d_k)\log_2(\epsilon_k + d_k - \epsilon_k d_k) + (1-d_k+\epsilon_k d_k)\log_2(1-d_k+\epsilon_k d_k)\}\Big]. \tag{66}$$

The above expression for the Shannon information can be shown to be convex in all the overlaps c_k and d_k which satisfy the inequalities (54). Therefore the maximum of the information exists and is taken on the boundary of the parameter space described by the overlaps. This boundary can be parametrized by

$$c_k = \tfrac{1}{2}(1+\cos\varphi_k), \quad d_k = \tfrac{1}{2}(1+\sin\varphi_k). \tag{67}$$

It can be shown that the expression (66) is maximal if $\varphi_k \in \{0, \frac{1}{2}\pi, \pi, \frac{3}{2}\pi\}$. The maximum value is then given by

$$I[\{F_k\}_k] \leqslant \sum_k \frac{a_k+b_k}{2} \frac{1}{2}\left(1-\log_2(1+\epsilon_k)+\frac{\epsilon_k}{1+\epsilon_k}\log_2\epsilon_k\right). \tag{68}$$

Thus we have been able to give an upper limit on the information by optimizing Eve's strategy and retaining as the only variables the parameters a_k+b_k and ϵ_k of the A matrices. These parameters are the same as in the estimate of the disturbance.

Next we show that it would be favorable for Eve to use a constant value of ϵ_k for all k. For that we note that we can vary the sum a_k+b_k independently of the values ϵ_k. We take any two ϵ_k, here renamed as α and β, and vary them depending on a continuous parameter s is such a way, that the disturbance D is unchanged. In the following calculation we suppress the other ϵ_k in the arguments. We may without loss of generality assume that $\alpha<\beta$ and $\frac{dD[\alpha(s),\beta(s)]}{ds}>0$. We show in Appendix D, that

$$\frac{d\beta(s)}{ds} \leqslant 0 \quad \text{and} \quad \frac{dI[\alpha(s),\beta(s)]}{ds} \geqslant 0. \tag{69}$$

This means that for a fixed disturbance the estimated information can always be increased by moving the values of two ϵ_k closer to each other. Clearly the optimal case is the one, where all ϵ_k have the same value. We denote this value by $\tilde{\epsilon}$. This means that we now have the two inequalities

$$D \geqslant \frac{\sqrt{2}}{16}\frac{(1-\sqrt{\tilde{\epsilon}})^2}{1+\tilde{\epsilon}} \tag{70}$$

$$I \leqslant 1-\log_2(1+\tilde{\epsilon})+\frac{\tilde{\epsilon}}{1+\tilde{\epsilon}}\log_2\tilde{\epsilon}. \tag{71}$$

Alice and Bob can measure the actual disturbance D_m by comparing a fraction of their exchanged signals. The inequality

$$D_m \geqslant \frac{\sqrt{2}}{16}\frac{(1-\sqrt{\tilde{\epsilon}})^2}{1+\tilde{\epsilon}} \tag{72}$$

leads to a lower bound of $\tilde{\epsilon}$ as

$$\tilde{\epsilon} \geqslant \overline{\epsilon} := \left(\frac{1-4\sqrt{(\sqrt{2}-8D_m)D_m}}{1-8\sqrt{2}D_m}\right)^2. \tag{73}$$

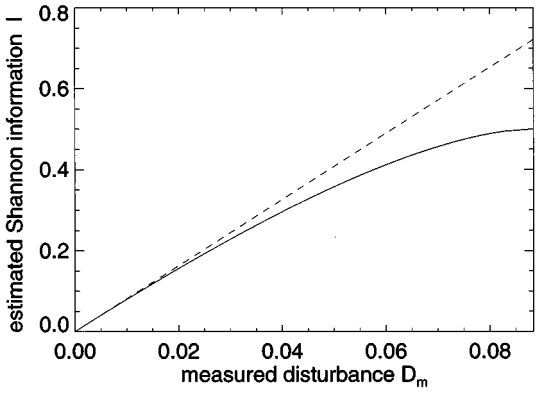

FIG. 2. The estimated Shannon information in the sharp (continuous line) and the linear estimates (dashed line) as a function of the measured disturbance D_m.

This lower bound on the other hand implies an upper bound on the Shannon information

$$I \leqslant 1-\log_2(1+\overline{\epsilon})+\frac{\overline{\epsilon}}{1+\overline{\epsilon}}\log_2\overline{\epsilon} \tag{74}$$

since the right-hand side is monotonically decreasing in ϵ. It can be shown that this estimate can be further estimated by the linear relation

$$I \leqslant \frac{4\sqrt{2}}{\ln 2} D_m, \tag{75}$$

where ln2 is the natural logarithm of 2. For small D_m, this estimate is nearly as good as the estimate (74) which will later be shown to be sharp. The sharp bound and the linear approximation are plotted in Fig. 2 as a function of the measured disturbance.

C. Expected collision probability

The expected collision probability will be maximized, as shown in Appendix E, by using a strategy with a one-to-one correspondence between POM elements and A matrices. We can then use the same decomposition of the POM element (59) as before. We use this expression to find

$$p(k_\alpha) = \frac{a_k+b_k}{4} \tag{76}$$

for the total probability of occurrence of k_α, that is, of outcome k while alphabet α was used, and

$$\sum_{\psi=0,1} p(\psi_\alpha,k_\alpha)^2 = \tfrac{1}{16}[a_k+(b_k-a_k)\mathrm{Tr}_{\mathcal{H}}(\rho_{0_\alpha}P_{k_\alpha})]^2+\tfrac{1}{16}[a_k+(b_k-a_k)\mathrm{Tr}_{\mathcal{H}}(\rho_{1_\alpha}P_{k_\alpha})]^2 \tag{77}$$

$$= \tfrac{1}{8}a_kb_k+\frac{1}{16}(b_k-a_k)^2[\mathrm{Tr}_{\mathcal{H}}(\rho_{0_\alpha}P_{k_\alpha})^2+\mathrm{Tr}_{\mathcal{H}}(\rho_{1_\alpha}P_{k_\alpha})^2 \tag{78}$$

for the joint probabilities occurring in (12). Then the relative expected collision probability is given by executing the sums over α and ψ in (12)

$$\langle p_c(y)\rangle^{\frac{1}{n}}=\sum_k \frac{a_k+b_k}{2}\,\frac{4a_kb_k+(b_k-a_k)^2[(1-c_k)^2+c_k^2+(1-d_k)^2+d_k^2]}{2(a_k+b_k)^2} \tag{79}$$

$$=\sum_k \frac{a_k+b_k}{2}\,\frac{4\epsilon_k+(1-\epsilon_k)^2[(1-c_k)^2+c_k^2+(1-d_k)^2+d_k^2]}{2(1+\epsilon_k)^2}. \tag{80}$$

Here again I used the definitions of c_k, d_k, and ϵ_k as above and c_k and d_k are again limited by the inequality (54). The last expression for the information estimate is, again, convex in all c_k and d_k. On the boundary of the allowed parameter space [parameterized by (67)] it takes on the form

$$\langle p_c(y)\rangle^{1/n}\leqslant\sum_k \frac{a_k+b_k}{2}\,\frac{4\epsilon_k+\frac{3}{2}(1-\epsilon_k)^2}{2(1+\epsilon_k)^2}. \tag{81}$$

We repeat the procedures applied to the Shannon information to show that Eve's optimal strategy uses an ϵ_k independent of k. For details see Appendix D. Following the procedures there we arrive at the final estimate for the expected collision probability depending on the measured disturbance D_m:

$$\langle p_c(y)\rangle^{1/n}\leqslant\frac{3+2\overline{\epsilon}+3\overline{\epsilon^2}}{4(1+\overline{\epsilon})^2}. \tag{82}$$

Here the quantity $\overline{\epsilon}$ is the same as for the Shannon information given by Eq. (73).

The resulting minimum fraction of bits to be discarded in the privacy amplification is then given from (8) by

$$\tau=\log_2\frac{3+2\overline{\epsilon}+3\overline{\epsilon^2}}{2(1+\overline{\epsilon})^2}. \tag{83}$$

An upper bound to this estimate is the linear upper approximation

$$\tau\leqslant\frac{8\sqrt{2}}{\ln 2}D_m \tag{84}$$

which is, as for the estimate of the Shannon information, very close to the more accurate estimate for a small deviation D_m. Both estimates are plotted as a function of the measured disturbance D_m in Fig. 3.

V. OPTIMAL EAVESDROPPER STRATEGY

In this section, I give an eavesdropper strategy which will indeed gain the estimated information for a given resulting disturbance. This strategy is described by A matrices which involve projection operators in the same symmetry which is shown by the signal states. They are represented by projections onto the vector

$$\begin{pmatrix}\sin\dfrac{\varphi+\theta}{2}\\ \cos\dfrac{\varphi+\theta}{2}\end{pmatrix}, \tag{85}$$

with $\theta\in\{0,\pi/2,\pi,3\pi/2\}$. The angle $\varphi+\theta$ can be viewed as spin direction or, alternatively, the angle $\varphi+\theta/2$ as an angle of the polarization plane of a photon. We denote by $P_\theta(\varphi)$ the projector on the corresponding vector. We now use a strategy described by the A matrices

$$A_k=\left[\frac{\epsilon_{opt}}{2(1+\epsilon_{opt})}\right]^{1/2}\mathbb{1}+\left(\left[\frac{1}{2(1+\epsilon_{opt})}\right]^{1/2}-\left[\frac{\epsilon_{opt}}{2(1+\epsilon_{opt})}\right]^{1/2}\right)P_\theta(\varphi) \tag{86}$$

and the corresponding POM elements

$$F_k=\frac{\epsilon_{opt}}{2(1+\epsilon_{opt})}\mathbb{1}+\frac{1-\epsilon_{opt}}{2(1+\epsilon_{opt})}P_\theta(\varphi). \tag{87}$$

Here the parameter ϵ_{opt} is the ratio of lesser to the greater eigenvalue of the eigenvalues of the POM elements. The resulting disturbance can be shown to be

$$D=\frac{\sqrt{2}}{16}\,\frac{(1-\sqrt{\epsilon_{opt}})^2}{1+\epsilon_{opt}}.$$

Thus we find that the equality $\overline{\epsilon}=\epsilon_{opt}$ holds independently of φ. The main reason for that is that by use of the symmet-

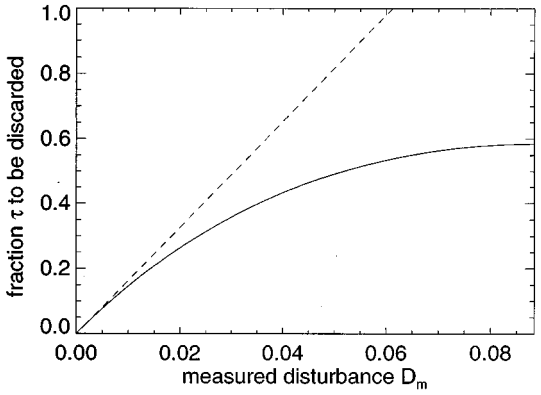

FIG. 3. The fraction τ of bits to be discarded before the error correction in the sharp (continuous line) and the linear estimates (dashed line) as a function of the measured disturbance D_m.

ric projectors the matrix $\mathcal{P}_{AEB}$ becomes symmetric and so the singular values are the eigenvalues of the matrix. Second, the nonstructural eigenvalues are equal so that the equality holds in the estimate (44).

On the other hand we find for the expected Shannon information and the fraction τ the expressions

$$I=1-\log_2(1+\epsilon_{opt})+\frac{\epsilon_{opt}}{1+\epsilon_{opt}}\log_2\epsilon_{opt} \tag{88}$$

and

$$\tau=\log_2\frac{3+2\epsilon_{opt}+3\epsilon_{opt}^2}{2(1+\epsilon_{opt})^2}, \tag{89}$$

which proves that all of the inequalities leading to the estimates (74) and (83) are sharp in the sense that the equalities are satisfied for the optimal strategy presented here.

VI. NOISY CHANNELS

We have obtained our estimate of an eavesdropper's knowledge about the key at this stage depending on the actual measured disturbance D_{min}. I will now investigate the situation of a noisy channel. Any implementation of a quantum cryptographical system will show an error rate c because of dark counts or misalignment. To be on the safe side, these errors have to be thought of as being caused by an eavesdropper. The error rates have to be small enough so that the according (74) and (82) estimated amount of Eve's Shannon information and expected collision probability still allows Alice and Bob to establish a secret key.

The noisy channel is modeled by replacing the signal states $|\phi_i\rangle$ by

$$|\phi_i\rangle\langle\phi_i|\rightarrow(1-c)|\phi_i\rangle\langle\phi_i|+c|\overline{\phi_i}\rangle\langle\overline{\phi_i}|. \tag{90}$$

Here, again, overlined states are the orthogonal complements. By calculating the joint probabilities of signals and outcomes between Alice and Bob using these signal states and the results taking the place of the matrix $\mathcal{P}_{AEB}$, we find a measured disturbance

$$D_m=\frac{\sqrt{2}}{4}c. \tag{91}$$

On the other hand the Shannon information shared by Alice and Bob after announcement of the alphabets used, but before discarding any bits, is given by

$$I_{AB}=\tfrac{1}{2}[1+c\log_2 c+(1-c)\log_2(1-c)]. \tag{92}$$

The transition from the *raw key* to the *sifted key* [12] by discarding all the bits where the alphabets used by Alice and Bob do not match will not change Eve's amount of Shannon information and expected collision probability since the correlation between signals and Eve's measurement outcomes are the same for the discarded and the retained bits. In contrast, the Shannon information shared by Alice and Bob does increase by this operation since here the signal-outcome correlations differ for the two sets. For the sifted key we find the Shannon information $I_{AB}^{(s)}$ to be

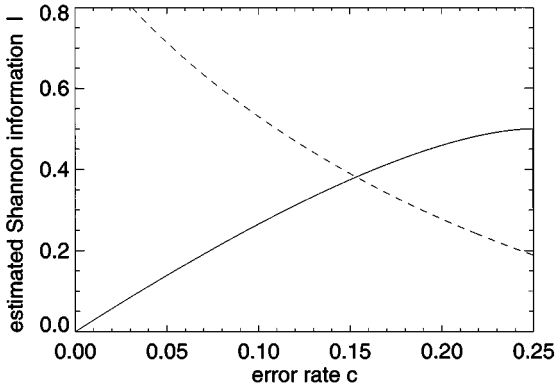

FIG. 4. The estimated Shannon information in the sharp estimate as a function of the error rate c of our noise model (solid line). The dashed line shows the amount of Shannon information shared by Alice and Bob. No error correction is applied.

$$I_{AB}^{(s)}=1+c\log_2 c+(1-c)\log_2(1-c). \tag{93}$$

A Wyner wiretap construction [13] is possible if the Shannon information shared by Alice and Bob exceeds that of Eve. Both relevant quantities are plotted in Fig. 4. We see that for $c\leqslant 0.15$, corresponding to a noise-induced error rate of 15%, a Wyner wiretap (if it can be realized) will work on this system.

For current implementations the only known way for a secure communication employing quantum cryptography uses the privacy amplification [26]. For this Alice and Bob first have to perform error correction. Discarding the errors will change the expected relative collision probability since signals triggering an outcome k for Eve will in general lead to asymmetric error rates depending on the choice of that signal and Eve can take this into account. In this way the expected relative collision probability may increase. In order to get a feeling for this I compare the expected collision probability before and after error correction in the case where Eve applies a strategy consisting of projections onto the four vectors (85) with $\varphi=\pi/4$. The joint probabilities before error correction are given via the expression $\frac{1}{8}\mathrm{Tr}_{\rho_i P_k}$ to be

$$\mathcal{P}_{AE}=\begin{pmatrix} 0.0183 & 0.1067 & 0.1067 & 0.0183 \\ 0.1067 & 0.0183 & 0.0183 & 0.1067 \\ 0.0183 & 0.0183 & 0.1067 & 0.1067 \\ 0.1067 & 0.1067 & 0.0183 & 0.0183 \end{pmatrix}, \tag{94}$$

and lead to an expected collision probability of

$$\langle p_c(y)\rangle^{1/n}=\tfrac{3}{4}, \tag{95}$$

and the fraction of bits to be discarded as

$$\tau=\log_2\tfrac{3}{2}. \tag{96}$$

A signal ρ_i which triggered Eve's outcome k will trigger the correct outcome for Bob with the probability

$$\frac{\mathrm{Tr}_{\mathcal{H}}(P_k\rho_i P_k\rho_i)}{\mathrm{Tr}_{\mathcal{H}}(\rho_i P_k)}. \tag{97}$$

Therefore the joint probabilities after error correction are given by

$$\frac{1}{N}\mathrm{Tr}_{\mathcal{H}}(P_k\rho_i P_k\rho_i) \tag{98}$$

with the normalization factor $N:=\Sigma_{i,k}\mathrm{Tr}_{\mathcal{H}}(P_k\rho_i P_k\rho_i)$. The values of the joint probabilities for the corrected string are then

$$\mathcal{P}_{AE}^{(C)}=\begin{pmatrix} 0.0036 & 0.1214 & 0.1214 & 0.0036 \\ 0.1214 & 0.0036 & 0.0036 & 0.1214 \\ 0.0036 & 0.0036 & 0.1214 & 0.1214 \\ 0.1214 & 0.1214 & 0.0036 & 0.0036 \end{pmatrix}, \tag{99}$$

leading to the expected collision probability

$$\langle p_c(y)^{(C)}\rangle^{1/n}=\tfrac{17}{18}, \tag{100}$$

and the fraction of bits to be discarded as

$$\tau^{(C)}=\log_2\tfrac{17}{9}. \tag{101}$$

A more systematic study is under way and the results will be published elsewhere.

The noise model introduced here is only a first test of the practicability for constructing quantum cryptographical systems. More general noise models are needed to optimize the construction of such systems. However for purposes of application to real data transfer we will not need these models as we are able to estimate the quantities τ and $I^{(s)}$ directly from the *measured* D_m and the fraction of bits discarded during the error correction.

VII. CONCLUSION

In this paper I have established estimates for the Shannon information and the expected collision probability an eavesdropper can gain in an attack on the Bennett-Brassard protocol. The present analysis applies before error correction takes place and depends on a measured disturbance or noise on the system. I have shown that these estimates are sharp and have given an explicit characterization of the optimal eavesdropper strategy in terms of A matrices and POM elements of a generalized measurement.

The estimate of the Shannon information indicates an allowed noise level of 15%, but up to now there has been no algorithm to make use of the required Wyner wiretap channel concept. However, this work suggests the possibility of performing privacy amplification to give provable security on a noisy channel for *all error rates* provided Alice and Bob can perform an error correction. These estimates will allow us to control the theoretical security of experimental systems and to improve the construction of forthcoming experiments by means of more elaborate models of noise and errors induced by the components of the setup.

ACKNOWLEDGMENTS

I thank Stephen M. Barnett for the introduction to quantum cryptography, discussion of the results, and for help transforming the results into this paper, and Simon Phoenix and Paul Townsend for discussion of the results. Special thanks also to Michael Hall for introducing me to the work of Kraus and Davies. This work was funded by the German Academic Exchange Service (DAAD) under the HSPII AUFE program.

APPENDIX A: TWO-LEVEL SYSTEM

This appendix deals with the description of a measurement on a two-level system in terms of a POM. The measurement is done by connecting the original two-level system S to another two-level system M. After an interaction described by a general interaction Hamiltonian $H=\theta\sigma_S\sigma_M$ we perform a von Neumann measurement on the system M. The outcome probabilities of this measurement can be described by a POM defined on the Hilbert space of the original system S before the interaction.

We denote by E_i the two projectors describing the von Neumann measurement performed on M after the evolution and by F_i the two POM elements describing the von Neumann measurement on the level of the system S before the evolution. The density operators of S and M before the measurement process and evolution are denoted by ρ_S,ρ_M and the ones before the measurement but after the evolution by $\widetilde{\rho}_S,\widetilde{\rho}_M$. The density-matrix ρ_{MS} of the combined system has the initial value $\rho_{MS}(0)=\rho_M\otimes\rho_S$. By σ_S,σ_M I denote the spin matrices on S and M, that means $\sigma=\Sigma_i n_i\sigma^i$ where the σ^i are Pauli spin matrices and the n_i are the three Cartesian components of a unit vector

The measurement on M after the interaction leads to the probability P_i for the outcome i as

$$\begin{aligned} P_i&=\mathrm{Tr}_M[E_i\widetilde{\rho}_M(t)]=\mathrm{Tr}_{MS}[(E_i\otimes\mathbb{1}_S)\widetilde{\rho}_{MS}(t)] \\ &=\mathrm{Tr}_{MS}[(E_i\otimes\mathbb{1}_S)e^{i\theta\sigma_S\sigma_M}(\rho_M\otimes\rho_S)e^{-i\theta\sigma_S\sigma_M}] \\ &=\mathrm{Tr}_S(\{[\sin^2\theta\mathrm{Tr}_M(\sigma_M E_i\sigma_M\rho_M) \\ &\quad+\cos^2\theta\mathrm{Tr}_M(E_i\rho_M)]\mathbb{1}_S\}\rho_S) \\ &\quad+\mathrm{Tr}_S(\{i\sin\theta\cos\theta\mathrm{Tr}_M([E_i,\sigma_M]\rho_M)\sigma_S\}\rho_S). \end{aligned} \tag{A1}$$

In the last step I used the identity

$$e^{i\theta\sigma_S\sigma_M}=\cos\theta\,\mathbb{1}_{MS}+i\sin\theta\sigma_S\sigma_M, \tag{A2}$$

which can be proven by the Taylor expansion. From this calculation we find the POM describing the measurement by comparing (A1) with the general form for an outcome probability $P_i=\mathrm{Tr}_S(F_i\rho_S)$, as

$$\begin{aligned} F_i&=[\sin^2\theta\,\mathrm{Tr}_M(\sigma_M E_i\sigma_M\rho_M)+\cos^2\theta\,\mathrm{Tr}_M(E_i\rho_M)]\mathbb{1}_S \\ &\quad+i\sin\theta\cos\theta\,\mathrm{Tr}_M([E_i,\sigma_M]\rho_M)\sigma_S. \end{aligned} \tag{A3}$$

The elements of this POM differ from multiples of the identity matrix only if

$$\begin{aligned} \mathrm{Tr}_M([E_i,\sigma_M]\rho_M)&\equiv\mathrm{Tr}_M([\sigma_M,\rho_M]E_i) \\ &\equiv\mathrm{Tr}_M([\rho_M,E_i]\sigma_M)\neq 0. \end{aligned}$$

APPENDIX B: ESTIMATE OF PROJECTION PART

The expression

$$\frac{1}{8\sqrt{2}}\mathrm{Tr}_{\mathcal{P}}[\mathrm{Tr}_{\mathcal{H}}(U_kP_k\rho_iP_kU_k^{\dagger}E_j)+\mathrm{Tr}_{\mathcal{H}}(U_k\overline{P_k}\rho_i\overline{P_k}U_k^{\dagger}E_j)] \tag{B1}$$

can be written as

$$\sqrt{2}\,\mathrm{Tr}_{\mathcal{P}}(\mathcal{P}_{AE}\mathcal{P}_{EB}) \tag{B2}$$

with matrices $\mathcal{P}_{AE}=\frac{1}{4}\mathrm{Tr}_{\mathcal{H}}(P_{k_1}\rho_i)$ and $\mathcal{P}_{EB}=\frac{1}{4}\mathrm{Tr}_{\mathcal{H}}(U_kP_{k_i}U_k^{\dagger}E_j)$ where I have redefined $P_{k_0}:=P_k$ and $P_{k_1}:=\overline{P_k}$. The matrix $\mathcal{P}_{AE}$ can be always represented using numbers $c,d\in[0,1]$ by

$$\mathcal{P}_{AE}=\frac{1}{4}\begin{pmatrix}1-c & c\\ c & 1-c\\ 1-d & d\\ d & 1-d\end{pmatrix} \tag{B3}$$

$$=\frac{\sqrt{2}}{4}\frac{1}{2}\begin{pmatrix}1\\1\\1\\1\end{pmatrix}\otimes\frac{1}{\sqrt{2}}(1,1)$$

$$+\frac{1}{\sqrt{2}}[(c-\tfrac{1}{2})^2+(d-\tfrac{1}{2})^2]^{1/2}u_{cd}\otimes\frac{1}{\sqrt{2}}(1,-1). \tag{B4}$$

Here we used the unit vector

$$u_{cd}:=\frac{1}{\sqrt{2}\left[\left(c-\frac{1}{2}\right)^2+\left(d-\frac{1}{2}\right)^2\right]^{1/2}}\begin{pmatrix}\frac{1}{2}-2\\ c-\frac{1}{2}\\ \frac{1}{2}-d\\ d-\frac{1}{2}\end{pmatrix}$$

$$\otimes\frac{1}{\sqrt{2}}(1,-1).$$

The transposed matrix $\mathcal{P}_{EB}^{\mathrm{T}}$ can be represented in the same way with numbers $\tilde{c},\tilde{d}$ replacing c,d. With that we find

$$\sqrt{2}\,\mathrm{Tr}(\mathcal{P}_{AE}\mathcal{P}_{EB})=\frac{1}{4\sqrt{2}}\times\frac{1}{2}\begin{pmatrix}1\\1\\1\\1\end{pmatrix}\otimes(1,1,1,1) \tag{B5}$$

$$+\frac{1}{2\sqrt{2}}[(c-\tfrac{1}{2})^2+(d-\tfrac{1}{2})^2]^{1/2}[(\tilde{c}-\tfrac{1}{2})^2$$

$$+(\tilde{d}-\tfrac{1}{2})^2]^{1/2}\langle u_{cd}|u_{\tilde{c}\tilde{d}}\rangle u_{cd}\otimes u_{\tilde{c}\tilde{d}} \tag{B6}$$

and can read the singular values

$$\sigma_S=\frac{1}{4\sqrt{2}} \tag{B7}$$

$$\sigma_{NS}=\frac{1}{2\sqrt{2}}[(c-\tfrac{1}{2})^2+(d-\tfrac{1}{2})^2]^{1/2}[(\tilde{c}-\tfrac{1}{2})^2$$

$$+(\tilde{d}-\tfrac{1}{2})^2]^{1/2}|\langle u_{cd}|u_{\tilde{c}\tilde{d}}\rangle|. \tag{B8}$$

This knowledge of the singular values and the estimate $|\langle u_{cd}|u_{\tilde{c}\tilde{d}}\rangle|\leq 1$ allows us to estimate the third term of Eq. (49) by

$$\sqrt{2}\,\mathrm{Tr}_{\mathcal{P}}(\mathcal{P}_{AE}\mathcal{P}_{EB})\leq\sqrt{2}\sum_i\ \sigma[\mathcal{P}_{AE}\mathcal{P}_{EB}] \tag{B9}$$

$$\leq\frac{1}{4\sqrt{2}}+\frac{1}{2\sqrt{2}}[(c-\tfrac{1}{2})^2$$

$$+(d-\tfrac{1}{2})^2]^{1/2}[(\tilde{c}-\tfrac{1}{2})^2+(\tilde{d}-\tfrac{1}{2})^2]^{1/2}. \tag{B10}$$

This is the expression given in the text.

APPENDIX C: INEQUALITY FOR OVERLAPS

The quantities c and d are restricted by quantum mechanics. This restriction depends on the overlap b between the two alphabets given as $b=|\langle\phi_1|\phi_3\rangle|^2$ and which takes the value $\frac{1}{2}$ for the Bennett Brassard protocol. The restriction takes the form

$$1-c-d+2cd-2\sqrt{cd(1-c)(1-d)}\leq b\leq 1-c-d+2cd$$

$$+2\sqrt{cd(1-c)(1-d)} \tag{C1}$$

and is derived by inserting the constructive identity $|\Psi\rangle\langle\Psi|+|\overline{\Psi}\rangle\langle\overline{\Psi}|$ into the definition of b and using the triangle inequality. This restriction is equivalent to

$$\frac{(d-c)^2}{1-b}+\frac{(1-c-d)^2}{b}\leq 1. \tag{C2}$$

For the Bennett-Brassard protocol with $b=\frac{1}{2}$ it simplifies further to

$$\left(d-\frac{1}{2}\right)^2+\left(c-\frac{1}{2}\right)^2\leq\frac{1}{4}. \tag{C3}$$

APPENDIX D: CHANGE ALONG THE PATH $\{\alpha(s),\beta(s)\}$

We change two ratio parameters α and β depending on a continuous parameter s in such a way, that the estimate for the disturbance remains unchanged. Without loss of generality we assume that $\alpha\leq\beta$ and $dD[\alpha(s),\beta(s)]/ds>0$. The demand for the disturbance estimate to remain constant can then be formulated as

$$\frac{\partial D[\alpha,\beta]}{\partial\alpha}\frac{d\alpha(s)}{ds}+\frac{\partial D[\alpha,\beta]}{\partial\beta}\frac{d\beta(s)}{ds}=0. \tag{D1}$$

With the use of

$$\frac{\partial D[\alpha,\beta]}{\partial\alpha}=-\frac{\sqrt{2}}{16}p_{\alpha}\frac{1-\alpha}{\sqrt{\alpha}(1+\alpha)^2}, \tag{D2}$$

where p_α is the probability of the outcome connected to α and the abbreviation

$$D'[\alpha]:=\frac{\sqrt{2}}{16}\frac{1-\alpha}{\sqrt{\alpha}(1+\alpha)^2}$$

we find

$$\frac{d\beta(s)}{ds}=-\frac{D'[\alpha]}{D'[\beta]}\frac{d\alpha(s)}{ds}. \tag{D3}$$

We note that $\frac{d\beta(s)}{ds}$ is negative since $D'[\alpha]$ is a positive function.

Next we investigate under which circumstances the amount of a Shannon information I increases, that is $dI_S/ds\geqslant 0$, for all possible values of α and β. This is the condition that

$$\frac{\partial I[\alpha,\beta]}{\partial\alpha}\frac{d\alpha(s)}{ds}+\frac{\partial I[\alpha,\beta]}{\partial\beta}\frac{d\beta(s)}{ds}\geqslant 0 \tag{D4}$$

is satisfied parallel to Eq. (D3). We find the expression

$$\frac{\partial I[\alpha,\beta]}{\partial\alpha}=\frac{1}{2}p_\alpha\frac{\log_2\alpha}{(1+\alpha)^2} \tag{D5}$$

which leads with the definition of the positive function

$$I'[\alpha]:=-\frac{1}{2}\frac{\log_2\alpha}{(1+\alpha)^2}$$

to the condition

$$\frac{I'[\alpha]}{D'[\alpha]}\leqslant\frac{I'[\beta]}{D'[\beta]}. \tag{D6}$$

Since this condition has to be fulfilled for all values of α and β with $\alpha\leqslant\beta$ this is equivalent to

$$\frac{\partial}{\partial\alpha}\frac{I'[\alpha]}{D'[\alpha]}\geqslant 0.$$

Inserting the introduced functions we find this condition to be

$$\frac{8\sqrt{2}}{\ln 2}\times\frac{2\alpha-(1+\alpha)\ln\alpha-2}{\sqrt{\alpha}(1-\alpha)^2}\geqslant 0, \tag{D7}$$

which can be shown to be fulfilled for $\alpha\in[0,1]$.

In the same way using

$$\frac{\partial\langle p_c\rangle^{1/n}[\alpha,\beta]}{\partial\alpha}=-p_\alpha\frac{1-\alpha}{(1+\alpha)^3}$$

we find the condition

$$\frac{8}{\sqrt{2}}\times\frac{1-\alpha}{\sqrt{\alpha}(1+\alpha)^2}\geqslant 0. \tag{D8}$$

This condition is obviously fulfilled. These two results show that the upper limit of the Shannon information and the expected collision probability is maximized by choosing the ratios ϵ_k as constants independent of the index k.

APPENDIX E: ACQUIRING ADDITIONAL KNOWLEDGE

In this section I show that the expected collision probability will always grow, in the context of the BB84 protocol, when more detailed knowledge is acquired. The basic description of this situation is that a measurement outcome k to POM element F_l can be replaced by two new outcomes l' and l'' described by $F_{l'}$ and $F_{l''}$ satisfying $F_l=F_{l'}+F_{l''}$. Here I will focus on the description in terms of the joint probabilities p_ik between signals i and measurement outcomes k. For the measurement outcome which gets split up we find $p(i,l)=p(i,l')+p(i,l'')$ for all signals i.

To prove that the expected collision probability never decreases in such a situation I use two steps. In the first step I split all the initial joint probabilities $p(i,l)$ into the same fractions $p(i,l')=\mu p(i,l)$ and $p(i,l'')=(1-\mu)p(i,l)$ which can be viewed as splitting a column of the matrix $\mathcal{P}_{ik}=\{p(i,k)\}$ into two proportional columns. I will show that this does not affect the expected collision probability. In the second step I show that the expected collision probability will generically increase when we change these joint probabilities in such a way that the sum over all signals $p(k)$ stays the same for the two new outcomes.

The first step is done by writing the expected collision probability down as

$$\langle p_c\rangle=\sum_{\substack{k\\ i=1,2}}p(k)\frac{p(i,k)^2}{p(k)^2}, \tag{E1}$$

where k in this context includes the choice of the alphabet α and the two signals are the two possible ones given the alphabet used.

By doing the split of the joint probabilities of the outcome l we find that $p(l')=\mu p(l)$ and $p(l'')=(1-\mu)p(l)$. We pick out the part of the expected collision probability referring to the outcomes l' and l'' to find

$$p(l')\frac{p(i,l')^2}{p(l')^2}+p(l'')\frac{p(i,l'')^2}{p(l'')^2}=p(l)\frac{p(i,l)^2}{p(l)^2}. \tag{E2}$$

Thus the expected collision probability remains unchanged under this split.

The basic step of changing the split of a column of $\mathcal{P}$ into proportional columns into a split in arbitrary columns is done by changing the probabilities depending on a parameter δ,

$$p(1,l')=\mu p(1,l)+\delta\quad p(1,l'')=(1-\mu)p(1,l)-\delta \tag{E3}$$

$$p(2,l')=\mu p(2,l)-\delta\quad p(2,l'')=(1-\mu)p(2,l)+\delta. \tag{E4}$$

The relevant terms of the expected collision probability then are

$$g(\delta) := \frac{[\mu p(1,l)+\delta]^2+[\mu p(2,l)-\delta]^2}{\mu[p(1,l)+p(2,l)]} + \frac{[(1-\mu)p(1,l)-\delta]^2+[(1-\mu)p(2,l)+\delta]^2}{(1-\mu)[p(1,l)+p(2,l)]}.$$

The derivative

$$\frac{\partial}{\partial\delta}g(\delta) = \frac{4\delta}{(1-\mu)\mu[p(1,l)+p(2,l)]}$$

shows that the minimal value is reached for $\delta=0$, which is the proportional split. That means that the collision probability can only increase for any other splits of an outcome. Therefore Eve's optimal strategy consists of a POM where each POM element is of the form $F_k=A_k^\dagger A_k$.

[1] G. S. Vernam, J. Am. Inst. Electr. Eng. **45**, 109 (1926).

[2] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.

[3] R. J. Hughes, D. M. Alde, P. Dyer, G. G. Luther, G. L. Morgan, and M. Schauer, Contemp. Phys. **36**, 149 (1995).

[4] S. J. D. Phoenix and P. D. Townsend, BT Tech. J. **11**, 65 (1993); S. J. D. Phoenix and P. D. Townsend, Contemp. Phys. **36**, 165 (1995).

[5] W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).

[6] C. H. Bennett, Phys. Rev. Lett. **685**, 3121 (1992).

[7] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995).

[8] S. M. Barnett and S. Phoenix, Phys. Rev. A **48**, R5 (1993).

[9] S. J. D. Phoenix, Phys. Rev. A **48**, 96 (1993).

[10] B. Huttner and A. K. Ekert, J. Mod. Opt. **41**, 2455 (1994).

[11] K. J. Blow and S. J. D. Phoenix, J. Mod. Opt. **40**, 33 (1993).

[12] A. K. Ekert, B. Huttner, G. M. N. Palma, and A. Peres, Phys. Rev. A **50**, 1047 (1994).

[13] A. D. Wyner, Bell Syst. Tech. J. **54**, 1355 (1975).

[14] G. B. C. H. Bennett and J. M. Robert, SIAM J. Comput. **17**, 210 (1988).

[15] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, IEEE Trans. Inf. Theo. **41**, 1915 (1995).

[16] E. B. Davies, IEEE Trans. Inf. Theo. **IT-24**, 596 (1978).

[17] B. Noble and J. W. Daniel, *Applied Linear Algebra*, 3rd ed. (Prentice-Hall, New Jersey, 1988).

[18] B. Schumacher, Phys. Rev. A **51**, 2738 (1995).

[19] C. W. Helstrom, *Quantum and Estimation Theory* (Academic, New York, 1976).

[20] E. B. Davies, *Quantum Theory of Open Systems* (Academic, London, 1976).

[21] K. Kraus, *States, Effects, and Operations*, Lecture Notes in Physics Vol. 190 (Springer, Berlin, 1983).

[22] A. S. Kholevo, Probl. Inf. Transm. (USSR) **9**, 110 (1973).

[23] M. A. Naĭmark, Izv. Akad. Nauk SSSR, Ser. Mat. **4**, 277 (1940), Russian, English summary. For a summary of the contents see [19].

[24] P. Pechukas, Phys. Rev. Lett. **73**, 1060 (1994).

[25] M. Hall (private communications).

[26] C. H. Bennett, F. Bessette, and L. Savail, J. Crypt. **5**, 3 (1992).