

# Security in the Multi-Dimensional Fibonacci Protocol

David S. Simon,<sup>1,2</sup> Casey Fitzpatrick,<sup>1</sup> and Alexander V. Sergienko<sup>1,3,4</sup>

<sup>1</sup>*Dept. of Electrical and Computer Engineering,*

*Boston University, 8 Saint Mary's St., Boston, MA 02215*

<sup>2</sup>*Dept. of Physics and Astronomy, Stonehill College, 320 Washington Street, Easton, MA 02357*

<sup>3</sup>*Photonics Center, Boston University, 8 Saint Mary's St., Boston, MA 02215*

<sup>4</sup>*Dept. of Physics, Boston University, 590 Commonwealth Ave., Boston, MA 02215*

Security against simple eavesdropping attacks is demonstrated for a recently proposed quantum key distribution protocol which uses the Fibonacci recursion relation to enable high-capacity key generation with entangled photon pairs. No transmitted pairs need to be discarded in reconciliation; the only pairs not used for key generation are those used for security-checking. Although the proposed approach does not allow eavesdropper-induced errors to be detected on single trials, it can nevertheless reveal the eavesdropper's action on the quantum channel by detecting changes in the distribution of outcome probabilities over multiple trials, and can do so as well as the BB84 protocol. The mutual information shared by the participants is calculated and used to show that a secret key can always be distilled.

PACS numbers: 03.67.Dd,62.23.St,42.25.Fx

## I. INTRODUCTION

In quantum key distribution (QKD), two legitimate users of the system, Alice and Bob, attempt to generate a shared encryption key in such a way that the laws of quantum mechanics prevent an unauthorized eavesdropper, Eve, from obtaining the key without revealing her presence. Restricting ourselves here to systems that use pairs of entangled photons, the most common approach is the Ekert protocol [1], which is itself an entangled version of the earlier BB84 protocol [2]. An embodiment of this approach using photon polarization works as follows. Alice and Bob each receive half of the entangled pair from a common source. Often the source is in Alice's lab, but it may be under the control of a third party (or even under the control of Eve herself). As the photons arrive, Alice and Bob each randomly choose one of two bases in which to make a linear polarization measurement. One basis consists of horizontal and diagonal polarization states ( $|H\rangle$  and  $|V\rangle$ ), the other involves diagonal states ( $|↗\rangle$ ) and ( $|↘\rangle$ ) polarized at  $45^\circ$  from the horizontal and vertical. They then communicate on a classical (possibly public) channel in order to compare their bases (but not the results of their measurements), discarding those trials in which they used different bases.

In the simplest possible eavesdropping attack, Eve also makes a polarization measurement of one photon as it en route to Bob. She must guess randomly which measurement basis to use. If she guesses correctly, measuring in the same basis as Alice and Bob, then she gains full information about the polarization state and therefore has complete information about the state of the corresponding key segment. Half of the time she guesses incorrectly, in which case her outcome is completely random and uncorrelated with Alice's result. When she sends on the photon, Bob's results will also be completely randomized in the original basis. This disturbance in Bob's results allows Eve's actions to be revealed. Alice and Bob ran-

domly select a subset of their results for a security check, exchanging the results of their measurements as well as the basis used on these trials. If Eve intercepts a fraction  $\eta$  of Bob's photons she introduces an error rate of  $\frac{\eta}{4}$  between Alice's outcomes and Bob's in the security-checking subset.

The polarization states have an effective Hilbert space of dimension 2, allowing a single bit of the key to be extracted in each polarization measurement. There have been a number of attempts to generalize the procedure above with other physical degrees of freedom that have higher-dimensional effective Hilbert spaces, thereby allowing more than one bit of the key to be generated per photon [3–7], as well as improved ability to detect eavesdroppers. One particularly promising way [8–10] to achieve this goal is to use the photon's orbital angular momentum (OAM) [11–13] instead of polarization. The OAM about the propagation axis is quantized,  $L_z = l\hbar$ , where the topological charge  $l$  can take on any integer value. If a range of OAM values of size  $N$  is used as the alphabet (for example  $l = 1, 2, \dots, N$  or  $l = -\frac{N-1}{2}, \dots, +\frac{N-1}{2}$  for even  $N$ ), then each photon can be used to determine up to  $\log_2 N$  bits of the key. Although in principle such schemes allow unlimited numbers of bits per photon, their experimental complexity increases rapidly with increasing  $N$ . For the most part we will work in this paper with arbitrary  $N$ , but in order to make the discussion more concrete we will at some points restrict ourselves to an alphabet of size  $N = 8$  (capable of achieving  $\log_2 8 = 3$  bits per photon). The generalization to higher values of  $N$  is straightforward.

In [14], an approach to high-dimensional QKD was proposed based on a novel entangled light source [15–19] that produces output with absolute values of the OAM spectrum restricted to the Fibonacci sequence. (Recall that the Fibonacci sequence starts with initial values  $F_1 = 1$  and  $F_2 = 2$ , generating the rest of the sequence via the recurrence relation  $F_{n+2} = F_{n+1} + F_n$ .) These states

pump a nonlinear crystal, leading to spontaneous parametric down conversion (SPDC), in which a small proportion of the input photons are split into entangled signal and idler output photons. After the crystal, any photons with non-Fibonacci values of OAM are filtered out. Angular momentum conservation and the Fibonacci recurrence relation conspire to force the two output photons to have OAM values that are adjacent Fibonacci numbers (for example  $F_m$  and  $F_{m+1}$ ). These photons can then be used to generate a secret key, as detailed in the next section.

The Fibonacci protocol requires the ability to distinguish between single OAM eigenstates and pairwise superpositions of eigenstates. This cannot be done unambiguously on a single trial; however, as shown in [28], an interferometric approach allows statistical discrimination of the possibilities over multiple trials. Using this approach, we show in this paper that the outcome probability distributions can be built up in such a way that eavesdropping alters them in a detectable manner. In this way, an eavesdropper can be revealed over multiple trials even though it may not be possible to identify errors on any individual trial. This is especially important because even without eavesdropping there is some probability of error in discriminating between states in individual trials, due to the non-orthogonality of the relevant superposition states. This complication must be dealt with in the reconciliation stage. BB84 and most other protocols rely on the rate of errors in individual outcomes for security, but here we must rely on statistical changes wrought by the eavesdropper's actions over many trials. As a result, rather than using eavesdropper-induced error rates as a measure of eavesdropper detection, it is more appropriate here to use probability-based measures such as the disturbance  $\mathcal{D}$  [21], which is defined in section V.

Section II reviews the procedure for implementing the Fibonacci protocol in the context of OAM measurements. The effect of eavesdropping is examined in section III. Details of the means of dealing with the superposition states are described in section IV, with calculations of various measures of security carried out in section V and conclusions in Section VI. A brief discussion of key reconciliation over a classical channel is given in Appendix A, and detailed expressions for the probability distributions of outcomes for the protocol appear in Appendix B.

## II. SETUP FOR KEY DISTRIBUTION

Here, we review the Fibonacci protocol [14]. The protocol discussed here is a slightly improved variation on the original proposal of [14], making use of the apparatus described in more detail in [28]. Note that no trials need to be discarded in the scheme described, aside from those used for security checking. This is in contrast to the original version of the Fibonacci protocol [14] where  $\frac{1}{4}$  of the trials were discarded during reconciliation and the BB84/Ekert protocol, where  $\frac{1}{2}$  must be discarded.

The Fibonacci protocol allows multiple key bits to be generated per photon. The required basis modulation can be done in a completely passive manner, and switching only has to be done between two fixed bases, so that the complexity of the setup increases much more slowly with increasing  $N$  than in other OAM-based QKD methods, such as [7].

The basic setup is shown schematically in Fig. 1. The source on the left (see [14] for more detail) uses a down conversion source and scattering from an aperiodic spiral nanoarray [15–19] to create an entangled superposition of states with Fibonacci-valued OAM states in the two output directions:

$$\psi = \sum_n (|F_{n-1}\rangle_A |F_{n-2}\rangle_B + |F_{n-2}\rangle_A |F_{n-1}\rangle_B), \quad (1)$$

where the index  $n$  runs over the indices of the allowed Fibonacci numbers in the pump beam:  $|\Psi\rangle_{pump} = \sum_n |F_n\rangle$ . Alice and Bob each receive one photon from the entangled pair. In each of their labs is a 50/50 beam splitter which randomly directs the photon to one of two types of detection stages. The stage labeled “L-type” detection consists of an OAM sorter [22–24] followed by a set of single-photon detectors. The OAM sorter sends OAM eigenstates with different  $l$  values into different outgoing directions, so that they will be registered in different detectors, thus allowing  $l$  to be determined. The other type of detection (labeled “D type”) is used to distinguish different superpositions  $|S_n\rangle$  of the form

$$|S_n\rangle = \frac{1}{\sqrt{2}}(|F_{n-1}\rangle + |F_{n+1}\rangle). \quad (2)$$

The detection of such superposition states can be accomplished in several ways [25–27]. One complication with the D-type detection is that adjacent superposition states, such as  $\frac{1}{\sqrt{2}}(|F_{n-1}\rangle + |F_{n+1}\rangle)$  and  $\frac{1}{\sqrt{2}}(|F_{n+1}\rangle + |F_{n+3}\rangle)$  are not orthogonal, meaning that the two states cannot be unambiguously distinguished from each other. This adds complications to the classical exchange and alters the corresponding detection probabilities; however we will see below that this extra complication is well compensated by increased the key-generating capacity. Moreover, the degree of complication does not grow with the size of the alphabet used, so that the benefits outweigh the complications by a larger amount as the range of  $l$  values increases.

It is necessary to keep the possible key values uniformly distributed, so that Eve can't obtain any advantage from knowledge of the nonuniform distribution. To do this it will be necessary to make sure that the spectrum of signal and idler values is broader than the alphabet of values actually used for the key, since the nonorthogonality of the superposition states means that measurements can broaden the range of outgoing values (see section III).

It should be noted that photons are lost from the setup only once, in the filtering after the crystal; the spiral before the crystal simply redistributes the energy among

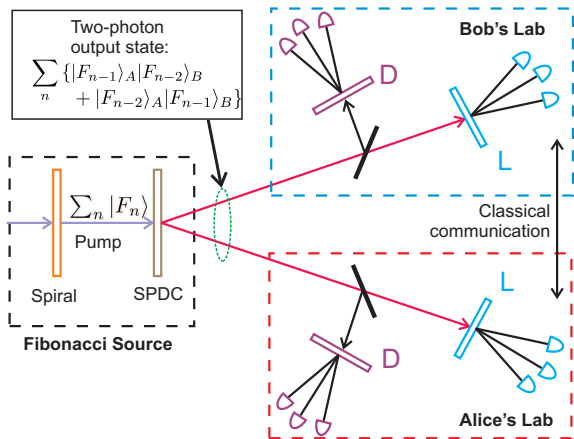


FIG. 1: Schematic setup for generating cryptographic key with Fibonacci-valued OAM states.

the available modes through interference effects, with no net loss of photons or energy. As a result, event rates should be at levels comparable to other entangled photon protocols.

For illustration purposes, we will often restrict ourselves to the case  $N = 8$ . Assume that the pump spectrum is broad enough to be approximately flat over a sufficient span to produce signal and idler OAM values of uniform probability over the range  $F_{m_0}$  to  $F_{m_0+N-1}$ , for some  $m_0$ . The outcomes for  $\mathbb{L}$ -type detection (OAM eigenstates) that will be used for key generation by Alice and Bob are then simply  $|F_{m_0}\rangle, |F_{m_0+1}\rangle, \dots, |F_{m_0+N-1}\rangle$ . For example, if the values  $N = 8$ ,  $m_0 = 2$  are chosen, then the utilized states are

$$\begin{aligned} |l_A\rangle, |l_B\rangle &= \{|F_2\rangle, |F_3\rangle, |F_4\rangle, \dots, |F_9\rangle\} \\ &= \{|2\rangle, |3\rangle, |5\rangle, |8\rangle, |13\rangle, |21\rangle, |34\rangle, |55\rangle\}. \end{aligned} \quad (3)$$

The outcomes for  $\mathbb{D}$ -type detection (two-fold OAM superposition states) used by Alice and Bob for key generation run from

$$|S_{m_0}\rangle = \frac{1}{\sqrt{2}} \{|F_{m_0-1}\rangle + |F_{m_0+1}\rangle\} \quad (4)$$

to

$$|S_{m_0+N-1}\rangle = \frac{1}{\sqrt{2}} \{|F_{m_0+N-2}\rangle + |F_{m_0+N}\rangle\}. \quad (5)$$

Detection either of the states  $|F_n\rangle$  or  $|S_n\rangle$  by Alice will correspond to a key value  $K = F_n$ . Unfortunately, Alice and Bob will not necessarily agree on the same key unless further classical information is exchanged to reconcile their values. One possible method for reconciliation is discussed in appendix A.

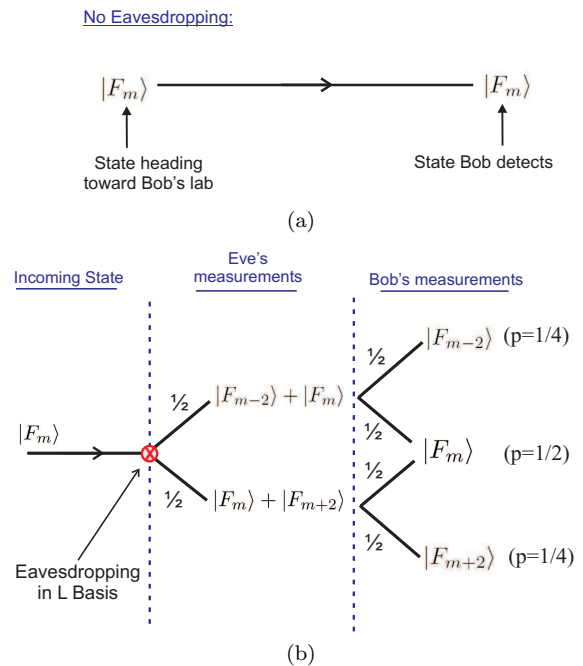


FIG. 2: Outcome probabilities for eigenstates. (a) When there is no eavesdropping and Bob measures in the  $\mathbb{L}$  basis, an incoming eigenstate should be detected correctly 100% of the time. (b) When Eve measures in the  $\mathbb{D}$  basis, each eigenstates can result in two different superposition detections. If she sends one of these superpositions on to Bob, the net result is that there are now three eigenstates that he could detect.

### III. EFFECT OF EAVESDROPPING: QUALITATIVE DISCUSSION

If an eavesdropper is acting on the photon heading to Bob, she does not know which type of detection ( $\mathbb{D}$  or  $\mathbb{L}$ ) will occur in Alice's and Bob's labs. If Alice detects an eigenstate, then the state arriving at Bob's end should be a superposition, whereas if Alice detects a superposition then the state heading toward Bob should be an eigenstate. If Eve makes a  $\mathbb{D}$ -type measurement when Bob's photon is in an  $\mathbb{L}$  state or if she makes an  $\mathbb{L}$ -type measurement when Bob's photon is in a  $\mathbb{D}$  state, a disturbance is made in the statistical distribution of Alice and Bob's joint outcomes, which will become apparent when he compares a random subset of his trials with Alice's. In more detail:

(i) Suppose Eve makes a  $\mathbb{D}$ -type measurement on a photon which is actually in the eigenstate  $|F_m\rangle$ . She will detect one of the two superpositions  $|F_m\rangle + |F_{m-2}\rangle$  or  $|F_m\rangle + |F_{m+2}\rangle$ , each with 50% probability, and send on a copy of it. If Bob receives one of these superpositions and makes an  $\mathbb{L}$  measurement, he will see one of the values  $F_m$ ,  $F_{m-2}$ , or  $F_{m+2}$ , with respective probabilities of  $\frac{1}{2}$ ,  $\frac{1}{4}$ ,  $\frac{1}{4}$ . In Eve's absence, he should only see  $F_m$  with 100% probability (see Fig. 2).

(ii) On the other hand, suppose Eve makes an  $\mathbb{L}$ -type

measurement on a photon which is actually in the superposition state  $|F_m\rangle + |F_{m-2}\rangle$ . She will detect one of the two eigenstates  $|F_m\rangle$  or  $|F_{m-2}\rangle$ , each with 50% probability, and send on a copy of it. If Bob receives one of these eigenstates and makes a  $\mathbb{D}$  measurement, he will see one of the superpositions  $|F_m\rangle + |F_{m-2}\rangle$ ,  $|F_m\rangle + |F_{m+2}\rangle$ , or  $|F_{m-2}\rangle + |F_{m-4}\rangle$ , with respective probabilities of  $\frac{1}{2}$ ,  $\frac{1}{4}$ ,  $\frac{1}{4}$  (see fig. 3). Thus, it seems that Bob sees the same result whether Eve interferes or not. However, by adding an additional interferometric element to the setup, we will see (section IV) that Bob will be able to distinguish between the two cases.

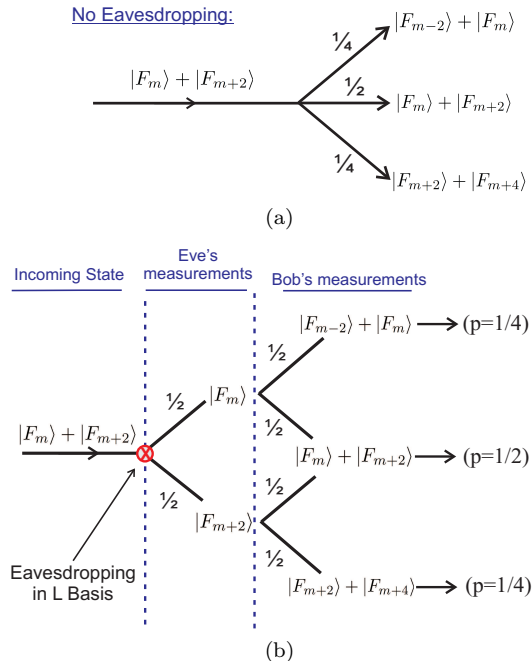


FIG. 3: Outcome probabilities for superposition states. (a) When there is no eavesdropping, an incoming superposition state leads to three possible outcomes when Bob makes a measurement in the superposition ( $\mathbb{D}$ ) basis: the state can be identified correctly with probability  $\frac{1}{2}$ , or it can be misidentified as one of the other two allowed superpositions that have nonzero overlap with it. (b) When Eve measures in the  $\mathbb{L}$  basis, each of the two possible eigenstates that result can lead to two different superpositions. The net result is that there are three outcomes that have nonzero overlap with the two eigenstates, so that the same probabilities occur as in figure (a), unless an addition is made to the apparatus (section IV).

It will be desirable to arrange the probabilities of the possible outcomes into a matrix. However, as seen above, the process of measurement can cause the range of states present in the system to spread. States that are within the range of our alphabet can lead to measurements outside the allowed range (for example, the in-range state  $|S_{m_0+N-1}\rangle$  can be measured as the out-of-range  $|S_{m_0+N}\rangle$ , since these two states have nonzero overlap). Similarly, states that are initially outside the desired range can lead to in-range measurements. This

spreading is greater when Eve is present and introducing additional measurements. So to account for this and to maintain the uniform distribution of key values, we allow states beyond the desired range to propagate in the system and include additional rows and columns in the probability matrix to describe the probability that the measured state is out of range of the allowed alphabet. This will be seen explicitly in section V and Appendix B. Note that we only need to include events in which at least one of the legitimate participants sees a value out of range; we can exclude events where the measurements are out of range for both of them.

#### IV. DISCRIMINATING SUPERPOSITION STATES

The discrimination of OAM eigenstates in the  $\mathbb{L}$  basis is straightforward and simply requires an OAM sorter. Discrimination of superposition states in the  $\mathbb{D}$  basis is more complicated. As shown in [28], the setup of figure 4 is capable of sorting the superposition states. A pair of photon-counting detectors  $C_n$  and  $D_n$  is used at the output ports of the final nonpolarizing beam splitters. If  $C_n$  fires during the key-generating trials, we count that as an  $|S_{n-1}\rangle$  detection. Due to destructive interference,  $D_n$  should not fire for  $|S_{n-1}\rangle$  input, so its firing will count as an  $|F_n\rangle$  detection. Then the scheme of Appendix A is used to reconcile Alice's and Bob's trials by classical information exchange in order to arrive at an unambiguously agreed-upon key. During the security checks, we then look at the distribution of counts in  $C_n$  and  $D_n$  separately in order to detect eavesdropper-induced deviations from the expected probability distributions. In order to achieve the indistinguishability required for interference, the OAM of each photon is shifted to zero after the sorting by a spiral phase plate or by other means. Measurements with detectors  $C_n$  and  $D_n$ , respectively, are equivalent to looking for nonzero projections onto the states

$$|C_n\rangle = \frac{i}{\sqrt{2}} (|F_n\rangle + |F_{n-2}\rangle) = i|S_{n-1}\rangle \quad (6)$$

$$|D_n\rangle = \frac{1}{\sqrt{2}} (|F_n\rangle - |F_{n-2}\rangle). \quad (7)$$

These two sets of states are also mutually nonorthogonal:  $\langle C_n | D_m \rangle = -\frac{i}{2} (\delta_{m,n-2} - \delta_{m,n+2})$ .

There are then multiple possible output states for Alice and Bob. Each can measure in the  $\mathbb{L}$  basis and obtain one of the  $|F_n\rangle$  states, or they can measure in the  $\mathbb{D}$  basis and register one of the  $|C_n\rangle$  or  $|D_n\rangle$  states. Their joint output probabilities for these states can then be found by taking the incoming state, applying the appropriate projection operator ( $|F_n\rangle\langle F_n|$ ,  $|C_n\rangle\langle C_n|$ ,  $|D_n\rangle\langle D_n|$ ), and then taking the inner product of the resulting projection with the initial state. The effect of Eve's intervention on Bob's channel can be dealt with by inserting similar additional projection operators representing Eve's measurements.

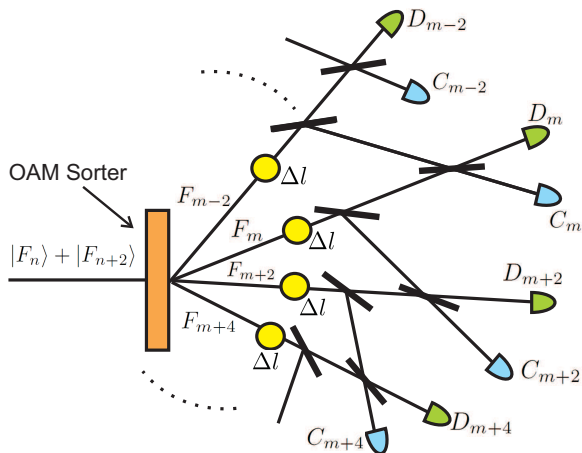


FIG. 4: A portion of a detection unit for statistically detecting superpositions of OAM states, analogous to the polarization version of the previous figure. The sorter separates different OAM values, which are then shifted to zero OAM by spiral wave plates or holograms (the yellow circles). From the top downward, the OAM shifts shown change the incoming OAM value by  $\Delta l = -F_{m-2}, -F_m, -F_{m+2}, -F_{m+4}$ . Superpositions of the form  $|F_m\rangle + |F_{m+2}\rangle$  cause constructive interference at the  $C_m$  detectors and destructive interference at the  $D_m$  detectors, while OAM eigenstates lead to equal detection rates at both types.

These extra projection operators tend to spread the probability distributions out, causing them to be nonzero for combinations of outcomes that previously had vanishing probabilities. As a result, Eve's actions can be revealed by these alterations in the outcome probabilities.

## V. MUTUAL INFORMATION AND SECURITY

For the detection events described in the previous sections, we may now construct the probability distributions.

We begin by making some definitions.  $P_{ij}$  will be the joint probability that Alice measures outcome  $i$  and Bob measures outcome  $j$  in the absence of eavesdropping. (In other words, these are the *expected* probabilities.)  $P_{Eij}$  will be the *observed* probabilities for the same outcomes in the presence of eavesdropping. The index  $i$  labels Alice's outcomes.  $i = 1$  represents an  $\mathbb{L}$ -type measurement with the measured value out of range of the desired alphabet, while values  $2 \leq i \leq N + 1$  correspond to the event that Alice measured in the  $\mathbb{L}$  basis and found state  $|F_{m_0+i-2}\rangle$ ; similarly,  $1 \leq j \leq N + 1$  represents Bob detecting an out-of-range value or measuring state  $|F_{m_0+j-2}\rangle$  in the eigenbasis. Value  $i = N + 2$  represents Alice making an out-of-range detection in the  $\mathbb{D}$  basis, while values of  $i$  in the range  $N + 3 \leq i \leq 3N + 2$  represent Alice measuring in the diagonal superposition basis and seeing an event in the  $C$  and  $D$  detectors. Specifically,  $i = N + 2k + 3$  represents the firing of  $C_{m_0+k}$ ,

and  $i = N + 2k + 4$  represents the firing of  $D_{m_0+k}$ , for  $k = 0, \dots, N - 1$ ; similarly for Bob with  $j$  values in the same range.  $P_i^{(A)}$  and  $P_j^{(B)}$  will be the expected marginal probabilities,  $P_i^{(A)} = \sum_j P_{ij}$  and  $P_j^{(B)} = \sum_i P_{ij}$ , with similar definitions for  $P_{Ei}^{(A)}$  and  $P_{Ej}^{(B)}$ .

First, we give the expected probabilities for the states in the two beams (before Bob's measurement) in the absence of eavesdropping. Columns label Alice's measurements, while rows label Bob's. The matrix of outcome probabilities then has the form

$$P_0 = \frac{1}{4} \begin{pmatrix} L_0 & C_0 \\ C_0^T & D_0 \end{pmatrix}, \quad (8)$$

where explicit expressions for the submatrices  $L_0$ ,  $C_0$ , and  $D_0$  may be found in Appendix B.

The matrices  $L_0$  and  $D_0$  represent, respectively, the events on which both Alice and Bob measured in the  $\mathbb{L}$  basis or both in the  $\mathbb{D}$  basis.  $C_0$  represents events in which Alice and Bob measured in different bases, one  $\mathbb{L}$  and one  $\mathbb{D}$ . The factor of  $\frac{1}{4}$  in eq. 8 is due to the fact that each of the four combinations of detection type ( $\mathbb{L}\mathbb{L}$ ,  $\mathbb{D}\mathbb{D}$ ,  $\mathbb{L}\mathbb{D}$ , and  $\mathbb{D}\mathbb{L}$ ) has a probability of  $\frac{1}{4}$  in a given trial.

Now let  $\eta$  be the proportion of trials on which Eve eavesdrops, i.e. the fraction of the photons on which she makes measurements. Assume she also randomly measures (with equal probabilities) in the  $\mathbb{L}$  or  $\mathbb{D}$  basis. Then the probability matrix for Alice and Bob's outcomes will change according to:

$$P_0 \rightarrow P = (1 - \eta)P_0 + \eta P_E, \quad (9)$$

where

$$P_E = \frac{1}{4} \begin{pmatrix} L' & C' \\ F' & D' \end{pmatrix} \quad (10)$$

The entries in  $P_E$  give the probability that Eve's actions will induce a change in the measured value, given that she intervened on that particular trial. The new submatrices  $L'$ ,  $C'$ ,  $D'$ , and  $F'$  may be found in Appendix B. We assume for simplicity that Eve only acts on Bob's channel, not Alice's. The more general case can be treated in a similar manner. Note that  $F'$  no longer needs to be equal to  $C'^T$  due to the asymmetry introduced by this assumption. We define the change in the probability matrix due to eavesdropping,

$$\Delta P = P - P_0 \quad (11)$$

$$= \frac{\eta}{4} \begin{pmatrix} L' - L_0 & C' - C_0 \\ F' - C_0^T & D' - D_0 \end{pmatrix}. \quad (12)$$

The *disturbance* [21] introduced by the eavesdropper can be used as a measure of how much effect she is having on the outcomes of the communication. The disturbance  $\mathcal{D}$  is defined to be

$$\mathcal{D} = \sqrt{\sum_{ij} (\Delta P_{ij})^2}. \quad (13)$$

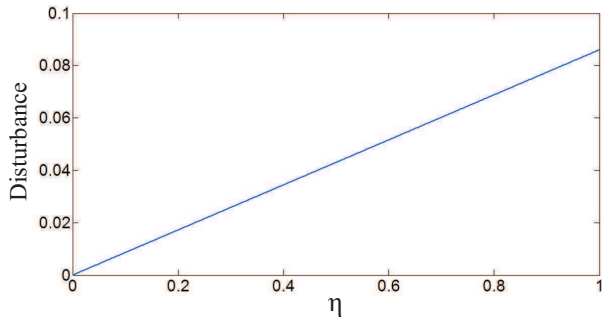


FIG. 5: The disturbance to the probability distribution, plotted against the eavesdropping fraction,  $\eta$ .

For binary protocols like BB84 the disturbance simply equals the eavesdropper-induced error rate, so  $\mathcal{D}$  is an appropriate generalization to protocols for which there are more than two possible outcomes per measurement. Using the probability matrices of Appendix B,  $\mathcal{D}$  can be readily calculated. From eqs. 12 and 13 it should clearly be linear in the eavesdropping fraction  $\eta$ , as verified in the plot of fig. 5. The disturbance reaches similar values to those found in [21] for the BB84 protocol.

From the probability distributions, the mutual information shared by Alice and Bob can also be computed:

$$I_{AB} = H_A + H_B - H_{AB} \quad (14)$$

$$\begin{aligned} &= - \sum_i P_{A,i} \log_2 P_{A,i} - \sum_j P_{B,j} \log_2 P_{B,j} \\ &\quad + \sum_{ij} P_{i,j} \log_2 P_{i,j}. \end{aligned} \quad (15)$$

The information per trial gained by Eve can also be found. First note that the probability that she measures in the correct basis is  $\frac{1}{2}$ . If she guesses the correct basis then she can determine the correct value for Bob with certainty; if she guesses the wrong basis, she only has a 50% chance of determining the correct value. So on a given trial, her probability of obtaining the correct value is  $\frac{3}{4}$ . Therefore, her information gain per trial (her average mutual information with Alice) is:

$$I_{AE} = (\text{prob. that Eve listens in on trial}) \quad (16)$$

$$\cdot (\text{probability trial is not discarded})$$

$$\cdot (\text{info. gained per eavesdropping})$$

$$= \eta \cdot r(\eta) \cdot I_{AB}, \quad (17)$$

where the fraction  $r(\eta)$  of trials retained is given in Appendix B.

These two information measures are plotted in fig. 6 as a function of eavesdropping fraction  $\eta$ . It can be seen that the mutual information per trial gained by Eve is always less than the mutual information shared between Alice and Bob, so that a secure key can always be distilled from the exchange. The secret key rate  $K = I_{AB} - I_{AE}$

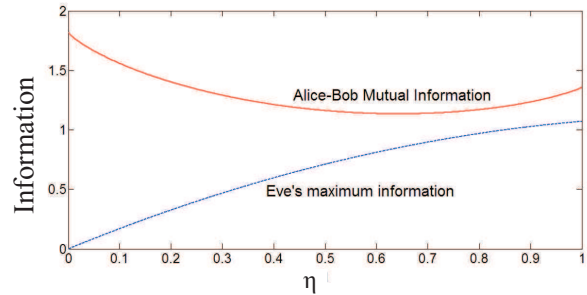


FIG. 6: The mutual information (upper red curve) shared between Alice and Bob, and the information gain per trial by Eve (lower blue curve) as functions of  $\eta$ .

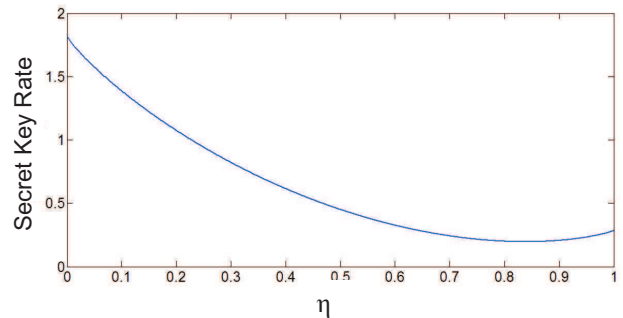


FIG. 7: The secret key generation rate  $\kappa$  versus eavesdropping fraction  $\eta$ .

is shown in fig. 7 as a function of  $\eta$  and as a function of disturbance in fig. 8. The slight upturn in the Alice-Bob mutual information at large  $\eta$  in Fig. 6 seems to be due to the fact that Eve's interference causes the outcomes to be more spread out (there are more nonzero entries in  $P_E$  than in  $P_0$ ), and more uniform distributions lead to increased information gains per measurement. Due to the concave shape of the binary entropy function, such an effect can also happen in schemes using binary qubits, if the error rate is able to exceed 50%.

## VI. CONCLUSIONS

In this paper, we have constructed the joint probability distributions for Alice and Bob's measurement outcomes in the Fibonacci protocol, both in the absence of eavesdropping and for the case of simple intercept-resend attacks. For the case of three bits per photon, it has been demonstrated that a secure key can be distilled and that the eavesdropper's presence can be revealed. For larger alphabets (more key bits per photon), the mutual information shared by Alice and Bob increases logarithmically with alphabet size, while the amount of classical information that needs to be exchanged stays constant.

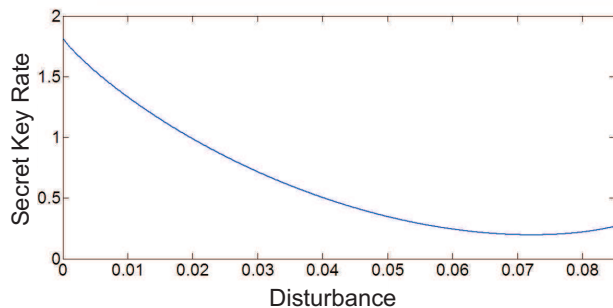


FIG. 8: The secret key rate  $\kappa$  as function of disturbance,  $\mathcal{D}$ .

It remains for future investigation to see how the protocol behaves under more sophisticated eavesdropping attacks.

### Acknowledgements

This research was supported by the DARPA QUI-NESS program through US Army Research Office award W31P4Q-12-1-0015

### Appendix A: Reconciliation

In order for Alice and Bob to determine each other's values they must exchange additional information on a classical side channel. Here, a brief description is given of one way to do this. Other methods are also possible. It is necessary to make sure that no eavesdropper can obtain the key from the classical exchange alone.

If Eve intercepts both the classical and quantum exchanges, and if she can store the photon from the quantum channel until she has read the classical channel, then she has complete information about the bit, just as Bob does. However, the disturbances she introduces will then signal her presence, causing the tainted key to be discarded. This is identical to the case in the BB84 or Ekert protocols.

However, in the Fibonacci case a *larger* classical exchange is required, which reduces the average amount of information about the key that remains secret. This reduces the key generation capacity per photon, partially canceling the advantages from the larger Hilbert space. But even in the worst case the classical exchange can be chosen such that the amount of classically revealed information remains less than the amount of information generated by the quantum exchange, allowing the distillation of a secure key [20]. Furthermore, the amount of revealed information is independent of  $N$ , while the total information from the quantum exchange increases with increasing alphabet size like  $\log_2 N$ ; thus this information leakage becomes more and more negligible with increasing  $N$ , as compared to the total information.

When both experimenters measure in the  $\mathbb{L}$  (eigenstate) basis, they should (in the absence of eavesdropping) always receive adjacent Fibonacci numbers, say  $F_n$  and  $F_{n+1}$ , although initially neither of them knows whether they have the lower or higher value in the pair. In order for them to determine this, they must each exchange one bit of information over the classical channel.

One possible way to do this (illustrated for the case  $N = 8$ ,  $m_0 = 2$ ), is for Alice first to send either a 0 or 1 to Bob in the following manner:

$$\begin{array}{l} \text{Alice has:} \\ \text{Alice sends:} \end{array} \left| \begin{array}{c|c|c|c|c|c|c|c} 2 & 3 & 5 & 8 & 13 & 21 & 34 & 55 \\ \hline 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \end{array} \right| \quad (18)$$

Once Bob receives this information he can determine Alice's value, since he already knows it has to be one of the two values adjacent to his. Alice's value can then be used as the key value. For arbitrary  $N$ , the probability of guessing the correct value based on the classical exchange alone decreases with increasing  $N$ :  $P = \frac{2}{N}$ .

Half of the time, Alice and Bob make opposite types of measurements, one  $\mathbb{L}$  and one  $\mathbb{D}$ . Suppose, for example, Alice measures the value  $F_5 = 8$  in the  $\mathbb{L}$  basis, while Bob measures in  $\mathbb{D}$ . In principle, he should receive the superposition state  $\frac{1}{\sqrt{2}}(|5\rangle + |13\rangle)$ ; however, since non-orthogonal states can not be uniquely distinguished, there is a 25% chance that Bob will instead measure the superposition  $\frac{1}{\sqrt{2}}(|2\rangle + |5\rangle)$  and 25% that he will find  $\frac{1}{\sqrt{2}}(|13\rangle + |34\rangle)$ . To arrive at an unambiguous value shared by both participants, there are several possible procedures. One possibility (again described for the case  $N = 8$ ,  $m_0 = 2$ ) is for Alice to send Bob *two* bits of information, according to the following table:

$$\begin{array}{l} \text{Alice has:} \\ \text{Alice sends:} \end{array} \left| \begin{array}{c|c|c|c|c|c|c|c} 2 & 3 & 5 & 8 & 13 & 21 & 34 & 55 \\ \hline 01 & 10 & 00 & 01 & 10 & 00 & 01 & 10 \end{array} \right| \quad (19)$$

Bob then knows Alice's value unambiguously, so that they can agree to use her value as the key segment; again, there is no need for Bob to send any classical information in this case. As  $N$  increases, the number of key bits generated per photon grows but the amount of classical information exchanged remains fixed.

Finally, Alice and Bob can both make a  $\mathbb{D}$  measurement. Suppose that Alice sends two bits of classical information, which could be:

$$\begin{array}{l} \text{Alice has:} \\ \text{Alice sends:} \end{array} \left| \begin{array}{c|c|c|c|c|c|c|c|c|c|c|c} S_1 & S_2 & S_3 & S_4 & S_5 & S_6 & S_8 & S_9 & S_{10} & S_{11} & \dots \\ \hline 00 & 00 & 01 & 01 & 10 & 10 & 11 & 11 & 00 & 00 & \dots \end{array} \right| \quad (20)$$

Examination of the probability matrices (eqs. 27-28) makes clear that, armed with knowledge of his own superposition, Bob can unambiguously determine Alice's value, while an outsider eavesdropper on the classical channel again has a decreasing probability of guessing the correct value as  $N$  increases. Once Alice and Bob agree that Alice has superposition  $|S_n\rangle$ , they then adopt the value  $F_n$  as the key value.

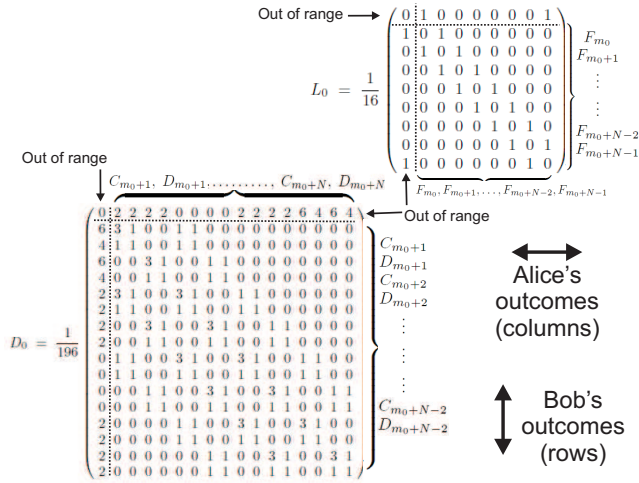


FIG. 9: The labeling of rows and columns is shown for the probability submatrices. Different rows correspond to different outcomes for Bob, while columns correspond to Alice's outcomes. The first row and column label detection of outcomes not included in the range of the alphabet used for key generation. The remaining rows and columns of  $L_0$  label allowed eigenstates, and those of  $D_0$  alternately label  $C_n$  and  $D_n$  detection events signalling allowed superposition states. Similarly,  $C_0$  has eigenstate events running horizontally, with  $C_n$  and  $D_n$  events vertically.  $L_0$ ,  $C_0$ , and  $D_0$  are respectively  $(N+1) \times (N+1)$ ,  $(N+1) \times (2N+1)$ , and  $(2N+1) \times (2N+1)$  matrices.

## Appendix B: Probability Matrices

Here we give explicit expressions for the joint probability distributions seen by Alice and Bob for their out-

comes, with and without eavesdropping. See section V for the relevant definitions. The labeling of the rows and columns is shown in fig. 9.

To compute the probabilities in the absence of eavesdropping, first consider the projections of the biphoton state  $|\psi\rangle$  after the crystal (eq. 1) onto the states that can be detected at the various detectors on Alice's side:

$$|\Psi_{F_n}^A\rangle = |F_n\rangle_A {}_A\langle F_n|\psi\rangle \quad (21)$$

$$= \frac{1}{\sqrt{2}}|F_n\rangle_A (|F_{n-1}\rangle_B + |F_{n+1}\rangle_B) \quad (22)$$

$$|\Psi_{D_n}^A\rangle = |D_n\rangle_A {}_A\langle D_n|\psi\rangle \quad (23)$$

$$= -\frac{i}{2}|D_n\rangle_A \times (|F_{n-3}\rangle_B + 2|F_{n-1}\rangle_B + |F_{n+1}\rangle_B) \quad (24)$$

$$|\Psi_{C_n}^A\rangle = |C_n\rangle_A {}_A\langle C_n|\psi\rangle \quad (25)$$

$$= \frac{1}{2}|C_n\rangle_A (|F_{n+1}\rangle_B - |F_{n-3}\rangle_B), \quad (26)$$

with similar expressions for the states  $|\Psi_{F_n}^B\rangle$ ,  $|\Psi_{C_n}^B\rangle$ ,  $|\Psi_{D_n}^B\rangle$  on Bob's side. Then (up to an overall constant that can be fixed by the requiring the probabilities to sum to one) the matrix for the probabilities of joint detections by Alice and Bob can be built up entry by entry by computing the various products  $\langle\Psi_{X_n}^A|\Psi_{Y_m}^B\rangle$ , for  $X, Y = C, D, F$ . We give here the results for  $N = 8$ ; the generalization to larger  $N$  is straightforward. The results are:

$$L_0 = \frac{1}{16} \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \quad C_0 = \frac{1}{72} \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 2 & 4 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 4 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 4 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 4 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 4 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 4 & 0 & 0 & 0 & 1 \\ 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 4 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 4 & 0 \end{pmatrix} \quad (27)$$

$$D_0 = \frac{1}{196} \begin{pmatrix} 0 & 2 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & 2 & 6 & 4 & 6 & 4 \\ 6 & 3 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 6 & 0 & 0 & 3 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 3 & 1 & 0 & 0 & 3 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 3 & 1 & 0 & 0 & 3 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 3 & 1 & 0 & 0 & 3 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 3 & 1 & 0 & 0 & 3 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 2 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 3 & 1 & 0 & 0 & 3 & 1 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 3 & 1 & 0 & 0 & 3 & 1 \\ 2 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{pmatrix} \quad (28)$$



Eve's measurements will alter Bob's outcome probabilities. If  $\eta$  be the proportion of trials she intercepts, then the probability matrix for Alice and Bob's outcomes will change according to  $P_0 \rightarrow P = \eta P_E + (1 - \eta)P_0$ , where  $P_E$  describes the change in probability due to Eve's intervention on a given trial. The various joint probabilities are computed as before, but with additional projection operators inserted into Bob's line to represent Eve's action. For example, when Alice and Bob measure in the  $\mathbb{L}$  basis and Eve measures in the  $\mathbb{D}$  basis, the probability that Alice detects  $F_p$  and Bob detects  $F_n$  has extra terms

added to it of the form

$$\sum_m \left\{ \langle \Psi_{F_p}^A | \Psi_{C_m}^B \rangle | \langle C_m | F_n \rangle |^2 + \langle \Psi_{F_p}^A | \Psi_{D_m}^B \rangle | \langle D_m | F_n \rangle |^2 \right\}; \quad (29)$$

these extra terms correspond to the possible outcomes of Eve's measurement. Similar expressions apply to find the rest of the probabilities. The net result (for  $N = 8$ )

is:  $P_E = \frac{1}{4} \begin{pmatrix} L' & C' \\ F' & D' \end{pmatrix}$ , where the new submatrices are

$$L' = \frac{1}{122} \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 1 & 6 & 6 & 11 \\ 11 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 6 & 5 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 6 & 0 & 5 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 5 & 0 & 5 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 5 & 0 & 5 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 5 & 0 & 5 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 5 & 0 & 5 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 5 & 0 & 5 & 0 \end{pmatrix} \quad F' = \frac{1}{1380} \begin{pmatrix} 0 & 5 & 5 & 5 & 5 & 45 & 45 & 91 & 91 \\ 39 & 12 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 52 & 28 & 0 & 4 & 0 & 0 & 0 & 0 & 0 \\ 39 & 0 & 12 & 0 & 1 & 0 & 0 & 0 & 0 \\ 52 & 0 & 28 & 0 & 4 & 0 & 0 & 0 & 0 \\ 13 & 26 & 0 & 12 & 0 & 1 & 0 & 0 & 0 \\ 32 & 20 & 0 & 28 & 0 & 4 & 0 & 0 & 0 \\ 13 & 0 & 26 & 0 & 12 & 0 & 1 & 0 & 0 \\ 32 & 0 & 20 & 0 & 28 & 0 & 4 & 0 & 0 \\ 1 & 12 & 0 & 26 & 0 & 12 & 0 & 1 & 0 \\ 4 & 28 & 0 & 20 & 0 & 28 & 0 & 4 & 0 \\ 1 & 12 & 0 & 26 & 0 & 12 & 0 & 1 & 0 \\ 4 & 0 & 28 & 0 & 20 & 0 & 28 & 0 & 4 \\ 1 & 0 & 1 & 0 & 12 & 0 & 26 & 0 & 12 \\ 4 & 0 & 4 & 0 & 28 & 0 & 20 & 0 & 28 \\ 1 & 1 & 0 & 12 & 0 & 26 & 0 & 12 & 0 \\ 4 & 4 & 0 & 28 & 0 & 20 & 0 & 28 & 0 \\ 1 & 0 & 1 & 0 & 12 & 0 & 26 & 0 & 12 \\ 4 & 0 & 4 & 0 & 28 & 0 & 20 & 0 & 28 \end{pmatrix} \quad (30)$$

$$C' = \frac{1}{664} \begin{pmatrix} 0 & 27 & 15 & 27 & 15 & 13 & 9 & 13 & 9 & 3 & 3 & 3 & 3 & 3 & 3 & 3 \\ 6 & 10 & 6 & 0 & 0 & 14 & 6 & 0 & 0 & 10 & 6 & 0 & 0 & 3 & 3 & 0 \\ 6 & 0 & 0 & 10 & 6 & 0 & 0 & 14 & 6 & 0 & 0 & 10 & 6 & 0 & 0 & 3 \\ 6 & 3 & 3 & 0 & 0 & 10 & 6 & 0 & 0 & 14 & 6 & 0 & 0 & 10 & 6 & 0 \\ 6 & 0 & 0 & 3 & 3 & 0 & 0 & 10 & 6 & 0 & 0 & 14 & 6 & 0 & 0 & 10 \\ 22 & 0 & 0 & 0 & 0 & 3 & 3 & 0 & 0 & 10 & 6 & 0 & 0 & 14 & 6 & 0 \\ 22 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 3 & 0 & 0 & 10 & 6 & 0 & 0 & 14 \\ 42 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 3 & 0 & 10 & 6 & 0 & 0 \\ 42 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 3 & 0 & 10 & 6 & 0 \end{pmatrix} \quad (31)$$

$$D' = \frac{1}{4294} \begin{pmatrix} 0 & 103 & 120 & 28 & 36 & 28 & 36 & 4 & 8 & 4 & 8 & 28 & 36 & 28 & 36 & 103 & 120 \\ 163 & 0 & 0 & 61 & 68 & 1 & 1 & 0 & 0 & 13 & 18 & 0 & 0 & 1 & 2 & 0 & 0 \\ 60 & 0 & 0 & 14 & 16 & 1 & 1 & 0 & 0 & 13 & 14 & 0 & 0 & 1 & 2 & 0 & 0 \\ 34 & 61 & 68 & 0 & 0 & 61 & 68 & 0 & 0 & 13 & 18 & 0 & 0 & 1 & 2 & 0 & 0 \\ 30 & 14 & 16 & 0 & 0 & 14 & 16 & 0 & 0 & 13 & 14 & 0 & 0 & 1 & 2 & 0 & 0 \\ 34 & 0 & 0 & 61 & 68 & 0 & 0 & 61 & 68 & 0 & 0 & 13 & 18 & 0 & 0 & 1 & 2 \\ 30 & 0 & 0 & 14 & 16 & 0 & 0 & 14 & 16 & 0 & 0 & 13 & 14 & 0 & 0 & 1 & 2 \\ 6 & 13 & 18 & 0 & 0 & 61 & 68 & 0 & 0 & 61 & 68 & 0 & 0 & 13 & 18 & 0 & 0 \\ 6 & 13 & 14 & 0 & 0 & 14 & 16 & 0 & 0 & 14 & 16 & 0 & 0 & 13 & 14 & 0 & 0 \\ 6 & 0 & 0 & 13 & 18 & 0 & 0 & 61 & 68 & 0 & 0 & 61 & 68 & 0 & 0 & 13 & 18 \\ 6 & 0 & 0 & 13 & 14 & 0 & 0 & 14 & 16 & 0 & 0 & 14 & 16 & 0 & 0 & 13 & 14 \\ 34 & 1 & 2 & 0 & 0 & 13 & 18 & 0 & 0 & 61 & 68 & 0 & 0 & 61 & 68 & 0 & 0 \\ 30 & 1 & 2 & 0 & 0 & 13 & 14 & 0 & 0 & 14 & 16 & 0 & 0 & 14 & 16 & 0 & 0 \\ 34 & 0 & 0 & 1 & 2 & 0 & 0 & 13 & 18 & 0 & 0 & 61 & 68 & 0 & 0 & 61 & 68 \\ 30 & 0 & 0 & 1 & 2 & 0 & 0 & 13 & 14 & 0 & 0 & 14 & 16 & 0 & 0 & 14 & 16 \\ 163 & 0 & 0 & 0 & 0 & 1 & 2 & 0 & 0 & 13 & 18 & 0 & 0 & 61 & 68 & 0 & 0 \\ 60 & 0 & 0 & 0 & 0 & 1 & 2 & 0 & 0 & 13 & 14 & 0 & 0 & 14 & 16 & 0 & 0 \end{pmatrix} \quad (32)$$

Note that the matrix is no longer symmetric due to the fact that we are assuming Eve has access only to Bob's

line but not Alice's. In particular, this means that  $F'$  is not equal to the transpose of  $C'$ .

- International Conference on Computers, Systems, and Signal Processing, Bangalore, 175 (1984).
- [3] D. Bruß, *Phys. Rev. Lett.* **81**, 3018-3021 (1998).
- [4] H. Bechmann-Pasquinucci, A. Peres, *Phys. Rev. Lett.* **85**, 3313-3316 (2000).
- [5] M. Bourennane, A. Karlsson, G. Björk, *Phys. Rev. A* **64**, 012306 (2001).
- [6] N. J. Cerf, M. Bourennane, A. Karlsson, N. Gisin, *Phys. Rev. Lett.* **88**, 127902 (2002).
- [7] S. Groblacher, T. Jennewein, A. Vaziri, G. Weihs, A. Zeilinger, *New J. Phys.* **8**, 1 (2006).
- [8] A. Mair, A. Vaziri, G. Weihs, A. Zeilinger, *Nature* **412**, 313 (2001).
- [9] A. Vaziri, G. Weihs, and A. Zeilinger, *Phys. Rev. Lett.* **89**, 240401 (2002).
- [10] D. S. Simon, A. V. Sergienko, *New J. Phys.* **16** 063052 (2014).
- [11] S. Franke-Arnold, L. Allen, M. Padgett, *Laser Photon. Rev.* **2**, 299313 (2008).
- [12] L. Allen, M. W. Beijersbergen, R. J. C. Spreeuw, J. P. Woerdman, *Phys. Rev. A* **45**, 8185-8189 (1992).
- [13] G. Molina-Terriza, J. P. Torres, L. Torner, *Nat. Phys.* **3**, 305-310 (2007).
- [14] D. S. Simon, J. Trevino, N. Lawrence, L. dal Negro, A. V. Sergienko, *Phys. Rev. A* **87**, 032312 (2013).
- [15] S. F. Liew, H. Noh, J. Trevino, L. Dal Negro, H. Cao, *Optics Express* **19**, 23631-23642 (2011).
- [16] J. Trevino, H. Cao, L. Dal Negro, *Nano Letters*, **11**, 2008-2016 (2011).
- [17] J. Trevino, S. F. Liew, H. Noh, H. Cao, L. Dal Negro, *Optics Express*, **20**, 3015-3033 (2012).
- [18] L. Dal Negro, N. Lawrence, J. Trevino, *Optics Express* **20**, 18209 (2012).
- [19] N. Lawrence, J. Trevino, L. Dal Negro, *J. of App. Phys.* **111**, 113101 (2012).
- [20] I. Csiszár, J. Körner, *IEEE Transactions on Information Theory*, Vol. IT-24, 339-348 (1978).
- [21] N. Lütkenhaus, *Phys. Rev. A* **54**, 97 (1996).
- [22] J. Leach, M. J. Padgett, S. M. Barnett, S. Franke-Arnold, J. Courtial, *Phys. Rev. Lett.* **88**, 257901 (2002).
- [23] G. C. G. Berkhout, M. P. J. Lavery, J. Courtial, M. W. Beijersbergen, M. J. Padgett, *Phys. Rev. Lett.* **105**, 153601 (2010).
- [24] M. P. J. Lavery, D. J. Robertson, G. C. G. Berkhout G. D. Love, M. J. Padgett, J. Courtial, *Optics Express* **20**, 2110-2115 (2012).
- [25] Y. Miyamoto, D. Kawase, M. Takeda, K. Sasaki, S. Takeuchi, *J. Opt.* **13**, 064027 (2011).
- [26] B. Jack, A. M. Yao, J. Leach, J. Romero, S. Franke-Arnold, D. G. Ireland, S. M. Barnett, M. J. Padgett, *Phys. Rev. A* **81**, 043844 (2010).
- [27] D. Kawase, Y. Miyamoto, M. Takeda, K. Sasaki, S. Takeuchi, *Phys. Rev. Lett.* **101**, 050501 (2008).
- [28] D. S. Simon, C. Fitzpatrick, A. V. Sergienko, *Phys. Rev. A* **91**, 043806 (2015).