Cavity-enabled high-dimensional quantum key distribution

2014 J. Phys. B: At. Mol. Opt. Phys. 47 155501

(http://iopscience.iop.org/0953-4075/47/15/155501)

OPEN ACCESS
IOP Publishing
Journal of Physics B: Atomic, Molecular and Optical Physics
J. Phys. B: At. Mol. Opt. Phys. **47** (2014) 155501 (8pp)
doi:10.1088/0953-4075/47/15/155501

Cavity-enabled high-dimensional quantum key distribution

Thomas Brougham and Stephen M Barnett

School of Physics and Astronomy, Glasgow University, Glasgow, G12 8QQ, UK

E-mail: thomas.brougham@gmail.com

Received 25 February 2014, revised 8 May 2014
Accepted for publication 27 May 2014
Published 28 July 2014

Abstract

High-dimensional quantum key distribution (QKD) offers the possibility of encoding multiple bits of key on a single entangled photon pair. An experimentally promising approach to realizing this is to use energy–time entanglement. Currently, however, the control of very high-dimensional entangled photons is challenging. We present a simple and experimentally compact approach, which is based on a cavity that allows one to measure two different bases: the time of arrival and another that is approximately mutually unbiased to the arrival time. We quantify the errors in the setup, due both to the approximate nature of the mutually unbiased measurement and as a result of experimental errors. It is shown that the protocol can be adapted using a cut-off so that it is robust against the considered errors, even within the regime of up to 10 bits per photon pair.

Keywords: quantum cryptography, quantum communication, quantum optics

(Some figures may appear in colour only in the online journal)

1. Introduction

One of the central insights of quantum information is that quantum mechanics allow for the safe distribution cryptographic keys. This insight has blossomed into the field of quantum key distribution (QKD) [1–4]. Broadly speaking, there are two main types of QKD protocols: entanglement based schemes [5–8] and send and receive protocols, which do not make use of entanglement [9, 10]. In the former, the security is guaranteed by non-locality, whereas in the latter, the security follows by the virtue of the uncertainty principle.

An essential feature of most QKD protocols is the requirement to measure in two or more bases that are mutually unbiased with respect to one another [11]. For the simplest implementations of QKD, this does not pose a significant problem. For example, it is common in QKD to encode information in the polarization of a photon. In this case, the task of measuring in two mutually unbiased bases (MUBs) can be easily achieved by using two polarizing beam splitters. If information is encoded on different optical degrees of freedom, however, then the task of measuring in two MUBs can be experimentally challenging.

The use of high dimensional states within QKD greatly increases the amount of information that can be encoded on each state. For optical implementations of QKD, this allows one to encode multiple bits of secret key on each photon. For example, it has been shown that under reasonable experimental conditions, one can encode over 10 bits per photon [12], which requires control over in excess of 1000 states. Furthermore, high dimensional states have been shown to be more robust to certain types of noise [13, 14]. There are several different photonic degrees of freedom that one can exploit in order to encode multiple bits per photon. One approach is to use the spatial modes of photons generated by spontaneous parametric down conversion. It has been shown, for example, that such photons can be entangled in their orbital angular momentum [15–18]. The difficulty in coupling orbital angular momentum states into fibers suggests that this approach is best used for free space communication, for which atmospheric effects become important [19].

Another approach is to use the arrival time of a photon. The basic idea is to divide the photon's arrival time into discrete time slots or time bins. In principle, if we have M time bins, then we could extract up to $\log_2(M)$ bits per photon. It is possible to generate photon pairs that are

entangled in their arrival time, so called energy–time entanglement. These states have already been used within experimental QKD protocols [8, 20–28, 44]. If such states are to be useful for high-dimensional QKD, then we must be able to measure in a basis that is mutually unbiased with respect to the time of arrival. This is a non-trivial task, however, when the number of time bins is large.

In this paper we present a simple and compact experimental setup for time-bin based high-dimensional QKD protocols. The approach is based on a reconfigured Mach–Zehnder interferometer that acts as a cavity. This setup allows one to project onto a single state that is approximately mutually unbiased to the arrival time. We will show how this can be used within a simple entanglement based QKD protocol. The performance of this protocol is then analysed in the presence of experimental imperfections. A key finding is that the protocol is robust to reasonable experimental errors.

The outline of the paper is as follows. In section 2 we review the problem of implementing a measurement that is mutually unbiased with respect to the time of arrival. The interferometer/cavity based scheme is reviewed in section 3. In section 4 we describe an entanglement based QKD protocol that is based on the cavity. The effects of experimental errors is investigated in section 5. We find that dark counts cause significant errors in the high-dimensional limit. Nevertheless, it is shown that this does not pose a serious problem as one can reduce the effect of such errors by using a simple trick. Finally, we discuss our results in section 6.

2. Mutually unbiased measurements

Suppose we have a d-level system, in which we will measure in one of two orthonormal bases $\left\{ \left| a_m \right\rangle \right\}$ and $\left\{ \left| b_n \right\rangle \right\}$. These bases are mutually unbiased to one another if

$$\left| \left\langle a_m \middle| b_n \right\rangle \right|^2 = 1/d, \tag{1}$$

$\forall\ m, n \in \{1, 2, \ldots, d\}$ [29, 30]. From a physical perspective, MUBs extend the notion of complementary observables to systems that are described using finite dimensional Hilbert spaces [31].

MUBs play a pivotal role in the security of QKD. They are used in most proofs of the security of QKD [32–37]. In particular, they are used in recent security proofs of QKD using qudits (d-level systems) [14, 38, 39]. The d-dimensional system that we will investigate is formed from the arrival time of a photon, which is split into a series of discrete intervals or time bins. There are many physical systems that naturally cause a photon's arrival time to be time-binned. For example, a photon in a cavity or optical network, where the output has a partially reflecting mirror. The photon would then have a finite chance of being emitted or be forced to take another trip of the cavity before it could be emitted again. One can also consider source of entangled photons that are naturally time-binned. One example is a mode-locked laser that pumps a nonlinear crystal that can produce pairs of down-converted photons [22].

Let $|n\rangle$ represent the state corresponding to a photon being in the nth time bin. Measuring the photon's time of arrival will be equivalent to projecting onto the basis $\{|n\rangle\}$. We label the d time slots, and hence also the basis states, from 1 to d. In practice, a timing measurement could have a better resolution than the spacing of each time bin. One could then determine which time bin the photon was in and discard the record of the exact time the photon was detected. Such a measurement procedure is equivalent to projecting onto the basis states $\{|n\rangle\}$.

If we are to exploit the time of arrival for QKD, then we must also measure within another basis that is mutually unbiased with respect to the basis $\{|n\rangle\}$. One such MUB is

$$\left|\varphi_k\right\rangle = \frac{1}{\sqrt{d}} \sum_{n=0}^{d-1} \exp\left(\frac{2\pi i n k}{d}\right) |d-n\rangle, \quad k = 0, 1, \ldots, d-1. \tag{2}$$

It can be seen that $\left|\left\langle m \middle| \varphi_n \right\rangle\right|^2 = 1/d$. One way of realizing a measurement in the basis $\left\{ \left|\varphi_k\right\rangle \right\}$, which works for $d = 2^N$, is to us a linear optical network of Franson interferometers [40, 41]. This approach requires one to align $d-1$ interferometers, which would be challenging even for small values of d. The difficulty in projecting onto the states $\left|\varphi_n\right\rangle$ has led people to consider alternative approaches to securing high dimensional time-binned QKD. One proposed method is to use just a single Franson interferometer [25, 42, 43]. It has been argued that in an entanglement based protocol, a single pair of Franson interferometers would be sufficient to detect any disturbance of the entanglement. It can be shown, however, that this will only be true if one can perform the experiment with a very high value for the visibility[1]. For example, if one were to encode 10 bits per photon, then to secure half of the bits against an attack with multiple temporal peaks, a visibility greater than 99.8% is required [40].

3. Realizing MUBs using a cavity

The problem with realizing a measurement in a basis such as (2) is that it requires us to project onto states which are a superposition of d time bins. The optical network outlined in [40] solves this problem by using various delay lines and beam-splitters, so as to allow photon amplitudes in different time slots to interfere. This inevitably increased the complexity of the experimental setup. In particular, the number of interferometers scales exponentially with the number of bits that one can encode on each photon[2].

[1] We must stress that this is only true when one wants to encode a large number of bits per photon, e.g. 10 bits per photon pair. It has been shown that one can encode 3–4 bits per photon pair securely using a Franson interferometer [44].

[2] The number of interferometers scales linearly with the number of time bins, or equivalently, the dimensions of the Hilbert space [41]. The problem is, however, that the number of bits per photon is the log of the number of time bins. This leads to an exponential scaling of the number of interferometer with the number of bits per photons.

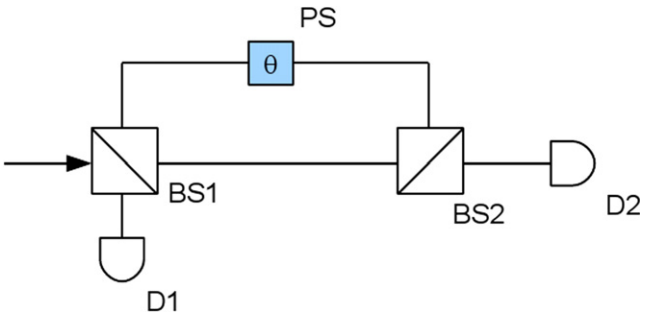

Figure 1. Diagram of the modified Mach–Zehnder interferometer. The elements BS1 and BS2 are both highly reflecting beamsplitters and PS is a phase shifter, which imparts a phase shift of θ. The total phase shift for a single round trip is thus $\phi = \theta + \pi$. Detection of a photon at D2 corresponds to a security check, while detection at D1 gives the time of arrival information and hence the key bits.

An alternative approach is to use a cavity like system. This would allow us to interfere light from different times within the cavity. By carefully designing the cavity, one can use this interference to construct a measurement that is a very good approximation to projecting onto the states $|\varphi_k\rangle$. The approach we take is to use the setup described in in [45]. The cavity is essentially a modified Mach–Zehnder interferometer, as shown in figure 1. The two beam-splitters are both chosen to be highly reflective. The phase shifter imparts a phase shift of θ. In addition to this, reflections at the two beam-splitters will also give a phase shift. For a single round trip of the cavity, a photon would pickup a phase shift of $\phi = \theta + \pi$.

The way this setup works is described in detail in [45]. However, for the sake of completeness, we will give a brief outline[3]. Detecting a photon at D1, within the time slots 1 to d, corresponds to measuring within the time of arrival basis, $\{|n\rangle\}$. We measure within the MUB whenever we detect a photon at D2 within a time slot $N \geqslant d$. To understand why this is, it helps to consider how the interferometer acts on a single photon input.

Suppose we have the single photon state $|\xi\rangle = \sum_k e^{i\gamma_k} |d-k\rangle$. Furthermore, suppose we get a click at D2, within the Nth time-bin, where $N \geqslant d$ and that we do not obtain a click at D1. The fact that we do not see photons at D1 is important. In principle there can be interference at BS1 between the amplitude of the incoming photon and the amplitudes already within the cavity. However, the fact that we do not observe photons at D1 means that we are, in effect, post-selecting a photon that has entered the cavity.

One could image that the photon we detected at D2 could have originated from the dth input slot. It would thus have taken $N-d$ round trips of the cavity before exiting and would thus have acquired a phase of $\exp[i(N-d)\phi]$. Alternatively, the photon could have originated from the $d-1$ time slot. This would have taken $N-d+1$ round trips and acquired a phase of $\exp[i(N-d+1)\phi]$ before exiting the cavity. One can extend this argument to see that each of the d time bins could have been the origin of the photon that was detected. As we have no prior knowledge of the emission time of the photon, the detection of the photon in the output time slot N, will thus correspond to projecting onto some superposition of time-bins. A simple calculation shows that detecting a photon at D2, within a time slot N ($N \geqslant d$) can be equivalent to projecting onto

$$|\Gamma_N(\phi)\rangle = |T_1||T_2|\left(|R_1||R_2|\right)^{N-d} e^{i(N-d)\phi} \times \left[\sum_{n=0}^{d-1} \left(|R_1||R_2|\right)^n e^{in\phi}|d-n\rangle\right], \quad (3)$$

where T_i and R_i are the transmission and reflection coefficients for the ith beam-splitter, with $i = 1, 2$. If we set $\phi = 2\pi k/d$ and make $|R_1|$ and $|R_2|$ close to one, then this state approximates $|\varphi_k\rangle$. However, the closer $|R_1|$ and $|R_2|$ are to one, the longer we must wait to observe a click at D2. This will effect the count rate; for more details see [45]. The prefactor $\left(|R_1||R_2|\right)^{N-d}$ takes account of the fact that the probability of obtaining a click decreases with time. This is a simple consequence of the fact that we are more likely to detect the photon at earlier times. We thus see that obtaining a click within *any* time bin, $N \geqslant d$, corresponds to projecting onto a state that approximates $|\varphi_k\rangle$. If we obtain a click at D2 within a time slot that is less than d, then we do not project onto the desired state as all d components have not full entered the cavity.

As we have stated, if we obtain a click at D2, then we shouldn't observe a click at D1. We are in essence post-selecting on a photon entering the cavity. However, even if all the photon amplitudes enter the cavity, we could still observe a click at D1. One important example is if the single photon state $|\xi\rangle$ was orthogonal to $|\Gamma_N(\phi)\rangle$, then the inference within the cavity should ensure that never register a click at D2, for $N \geqslant d$.

We have not considered the fact that a cavity cannot preserve the coherence of any state indefinitely. In particular, there will come a time for which the coherence between the photon amplitudes, in different time-bins, is lost. For this reason we impose an upper limit for when a click at D2 will project onto (3). Let N' be the last acceptable time slot. The maximum allowed value for N' will depend on the choice of the reflectivities [46]. We see that we only project onto (3) whenever we get a click at D2 within the a time bin N, where $d \leqslant N \leqslant N'$.

The value of the total phase shift ϕ can be altered by adjusting the phase shifter. By choosing $\phi = 2\pi k/d$, we can approximately project onto $|\varphi_k\rangle$. It is thus possible to approximately project onto any of the basis states $\{|\varphi_k\rangle\}$, by simply changing the phase shifter. One can thus obtain the full measurement statistics for the basis $\{|\varphi_k\rangle\}$.

One important point about this scheme is that we can only project onto one of the states $|\varphi_k\rangle$ for a given phase

[3] Issues such as the effects of spectral filtering of the cavity will not be considered. Instead, one should refer to [45] for a discussion on such matters.

setting. This means that it is not suitable for use within QKD protocols where information is encoded on both of the bases, i.e. $\{|n\rangle\}$ and $\left\{\left|\varphi_k\right\rangle\right\}$. Instead, we could use the time of arrival basis to encode the key bits, while using the other MUB to check for an eavesdropper. In this way, our approach is similar to the alternative protocols using within some security proofs in QKD [32]. Another point to note is that we do not measure each basis equally often. The fact that $\left|R_1\right|\left|R_2\right| \approx 1$ implies that we make timing measurements much more often than we make security checks. This is reminiscent of the modified BB84 protocol introduced by Hoi-Kwong Lo *et al* [47]. QKD protocols with an asymmetry in the bases, tend to more efficient than symmetric protocols in the sense that one losses less data during the sifting stage. The price one pays for this is that to ensure security, we require error rates that are lower than for symmetric protocols [47, 48].

4. Entanglement based QKD protocol

We have outlined how one can measure within two different bases using the experimental setup shown in figure 1. In this section we will explain how this setup can be integrated into a time-bin based QKD protocol. If the QKD protocol is to work correctly, then we will also have to investigate how well the states $\left|\Gamma_N(\phi)\right\rangle$, approximate the true MUB states $\left|\varphi_k\right\rangle$.

The setup is compatible with both entanglement based and send and receive protocols. For the sake of definiteness, we shall explain how the experimental setup can be integrated into an entanglement based protocol. This will require both Alice and Bob to each have the interferometer shown in figure 1. The errors within each interferometer will thus be combined. Hence, an entanglement based scenario is a more stringent test of the setup than a send and receive protocol.

Assume that we have two parties, Alice and Bob, that are trying to establish a shared secret key. This will be achieved by Alice generating a two photon entangled state and keeping one of the photons, while sending Bob the other photon. It is important to stress that the source of the entangled photons is under Alice's control. Alice will generate an entangled two photon state of the form

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{d}} \sum_{n=0}^{d-1} |d-n\rangle_A \, |d-n\rangle_B. \tag{4}$$

We see that the arrival time of the two photons are perfectly correlated, i.e., Alice and Bob should always find photons within the same time bin. This correlation will be used to encode the shared random *key bits*. The state, $|\psi\rangle_{AB}$, can also be expressed in the basis $\left|\varphi_k\right\rangle$, which gives the result

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{d}} \sum_{n=0}^{d-1} \left|\varphi_n\right\rangle_A \left|\varphi_{-n}\right\rangle_B, \tag{5}$$

where $\left|\varphi_{-n}\right\rangle = \left|\varphi_{d-n}\right\rangle$. The two-photon state is thus perfectly anti-correlated in the basis (2).

An eavesdropper, Eve, could intercept the photon sent to Bob. Eve's aim is to extract the photon's timing information, as this is where the key bits are encoded. However, this will inevitably disturb the correlation within the basis $\left\{\left|\varphi_k\right\rangle\right\}$. Alice and Bob can thus detect Eve by checking the correlation within the basis $\left\{\left|\varphi_k\right\rangle\right\}$.

A straightforward approach would be the following. Alice and Bob will each have the setup shown in figure 1. The correlation in the basis $\left\{\left|\varphi_k\right\rangle\right\}$ means that if Alice projects onto the state $\left|\varphi_n\right\rangle$, then Bob's photon will be in the state $\left|\varphi_{d-n}\right\rangle$. This implies that if Bob's total phase shift is not set to $\phi = 2\pi(d-n)/d$, then he should not obtain a click at D2 within a time bin N, which is $\geqslant d$. The presence of clicks for uncorrelated phase settings indicate that the correlation in (5) has been disturbed. This would, in turn, imply that Eve is intercepting Bob's photons. The error can thus be defined as the fraction of clicks at D2, that correspond to uncorrelated phase settings. The full statistics for the MUB can be obtained by Alice and Bob each using d settings for their phase shifter. Provided the error introduced by the approximate nature of the MUB measurement is low, then Alice and Bob could use the setup to implement a secure QKD protocol.

An experimentally simpler approach would be for Alice and Bob to use only two phase settings. This is equivalent to projection onto only two of the basis states $\left|\varphi_k\right\rangle$. While this would not provide Alice and Bob with the full statistics for the two MUBs, it would still be suffice to check the correlation in equation (5). There are two advantages to this approach. Firstly, the arrangement is simpler that using d settings for the phase shifter and is thus well suited for establishing how well the setup approximately projects onto the states $\left|\varphi_k\right\rangle$. Secondly, the number of phase settings scales exponentially with the number of bits per photon. For instance, if we wanted to encode up to 10 bits per photon pair, then we would require at least 1024 time-bins and phase settings. Such a large number of different settings requires a large number of experimental runs to acquire a significant amount of data for the security analysis. This problem is compounded by the count rate decreasing for large d, due to the reflectivities needing to be large. For further details on how the count rate varies with d, see [45]. For these stated reasons, we will analyse a protocol that uses only two phase settings. Nevertheless, the results we find can be easily extend to a protocol that uses d settings.

Suppose that Alice's phase settings ϕ_A are either 0 or $2\pi k/d$, then Bob's settings will be $\phi_B = 0$ or $2\pi(d-k)/d$. Let $P_{N'}^{AB}(\phi_A, \phi_B)$ be the total probability for Alice and Bob to both obtain clicks at D2 in time bins within the interval

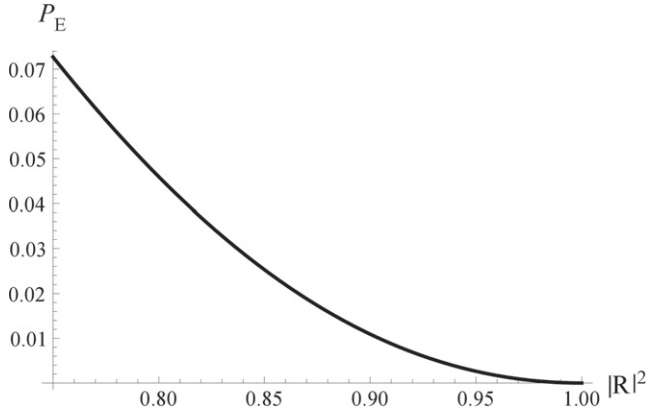

Figure 2. A plot of error probability, P_E, as a function of $|R|^2 = |R_1|^2 = |R_2|^2$, for $d = 1024$ time bins. The value of $k = d/2$, hence $\phi_A = 0$ and $\pi/2$, while $\phi_B = 0$ and $\pi/2$.

$d \leqslant N_{A,B} \leqslant N'$, for the phase settings ϕ_A and ϕ_B, hence

$$P_{N'}^{AB}(\phi_A, \phi_B) = \sum_{m=d}^{N'} \sum_{n=d}^{N'} \left| \left\langle \Gamma_m(\phi_A) \right| \otimes \left\langle \Gamma_n(\phi_B) \right| \psi \rangle_{AB} \right|^2. \quad (6)$$

The probability to obtain an error can then be defined as

$$P_E = \frac{P_{N'}^{AB}\left(0, \frac{2\pi(d-k)}{d}\right) + P_{N'}^{AB}\left(\frac{2\pi k}{d}, 0\right)}{P_{N'}^{AB}(0,0) + P_{N'}^{AB}\left(\frac{2\pi k}{d}, \frac{2\pi(d-k)}{d}\right) + P_{N'}^{AB}\left(0, \frac{2\pi(d-k)}{d}\right) + P_{N'}^{AB}\left(\frac{2\pi k}{d}, 0\right)}. \quad (7)$$

A straightforward calculation shows that

$$P_E = \frac{\left(1 - \left(|R_1|\,|R_2|\right)^2\right)^2}{\left(1 - \left(|R_1|\,|R_2|\right)^2\right)^2 + \left[1 + \left(|R_1|\,|R_2|\right)^4 - 2\left(|R_1|\,|R_2|\right)^2 \cos\left(\frac{2\pi k}{d}\right)\right]}. \quad (8)$$

The probability of error is plotted in figure 2 for $|R_1| = |R_2|$, $d = 1024$ (10 bits per photon) and $k = 512$, which corresponds to $\phi_{A,B} = 0$ and π. The plot shows that P_E decreases as $|R_{1,2}|$ are increased. This confirms the intuition that as $|R_1|$ and $|R_2|$ tend to one, the state (3) becomes a better approximation of the desired state, $|\varphi\rangle$. This means that by choosing sufficiently large values for $|R_1|$ and $|R_2|$, we can make the errors due to the approximate nature of our measurements arbitrarily small. This must be balanced against the fact that the larger $|R_1|$ and $|R_2|$ are, the greater the time needed to acquire the necessary security data. This tradeoff is important for experimental implementations.

One can get a feel for the tradeoff between error and count rate by looking at some examples. For simplicity, we set $|R_1| = |R_2| = |R|$. Suppose we want $P_E = 0.01$ when $d = 1024$; this is achieved when $|R|^2 = 0.904$. The count rate will depend on $P_{N'}^{AB}(\phi_A, \phi_B)$. For $N' = 2048$, we find that the probability for Alice and Bob to both see clicks at D2, for $\phi_A = \phi_B$, is $P_{N'}^{AB}(0,0) = P_{N'}^{AB}(\pi,\pi) = 0.076$. If instead we wanted $P_E = 0.05$, again for $d = 1024$, then we should have chosen $|R|^2 = 0.792$. Using this choice for $|R|$ with a cutoff of $N' = 2048$, we find that $P_{N'}^{AB}(0,0) = P_{N'}^{AB}(\pi,\pi) \approx 0.1$.

The probability of error, P_E, depends on the product of $|R_1|$ and $|R_2|$. We have some freedom, therefore, in the exact choice of the reflectivities. In figure 2 and in the examples in the next section, we set $|R_1| = |R_2|$. There could be situations, however, where it is advantageous to allow the reflectivities to be different. For example, $|R_1|$ determines the probability to make either a timing measurement or to measure within the other basis. It is useful to be able to modify $|R_1|$ without affecting P_E. This can be achieved by choosing $|R_1| \neq |R_2|$.

A further factor to consider is the effect of experimental errors. This is of fundamental importance for all practical QKD schemes. In our case we have the added complications that we have errors even in the absence of experimental noise. It is thus vital that we analyse the robustness of the scheme against experimental imperfections.

5. The effects of experimental errors

The first effect to consider is the that of misalignment in the path length of the interferometer. If the misalignment is too great, then the interference between the different time bins will be completely lost. If the scheme is to function correctly, then the misalignment must be made small. Nevertheless, a small misalignment will still have an effect on the intended interference. One can model this by assuming that the time bins inside the interferometer are shifted in time by a small amount relative to the incoming modes. This will led to the summation in equation (3) being modified. The effect is equivalent to introducing a positive term $\xi \leqslant 1$, such that the term $\left(|R_1|\,|R_2|\right)^n$ in the summation is replaced by $\left(\xi\,|R_1|\,|R_2|\right)^n$. The larger the misalignment is, the smaller ξ will be. The effect of a misalignment on the error probability, can thus be thought of as decreasing the coefficients of transmission and reflection.

Another very important source of errors is in the detectors. Real detectors are inefficient and have dark counts and jitter. We will assume that Alice and Bob's detectors are identical and share the same imperfections. The effects of statistical jitter will be to change the time bin we detect the photons in. With regards to the timing measurement, jitter will set a limit on the sizes of our time bins. The reason for this is that if we chose a width that is small relative to the detectors response, then this will result in significant errors in the timing measurements. The effects of jitter on the security measurements is not so severe. This is because the protocol does not require us to obtain a click within a specific time bin. Similarly, Alice and Bob do not both need to obtain clicks at D2 within the same time slot. However, if we choose the width of the time bins to be too small, then there can be an effect due to jitter making us think we detect a photon in a time slot $N \geqslant d$, when it should have been detected in a time bin before d. This would mean that we have not had a chance to observe interference between all of the time bins. The

effect of this error is small, however, and can be removed complete by either increasing the width of the time-bins or excluding detection events that occur sufficiently near to the dth time slot. The latter option would result in a slightly decreasing the amount data for the security check.

Suppose that Alice and Bob's detectors have an efficiency η, which is less than one. This means that we have a finite probability for not registering photons that are incident on the detectors. Taken in isolation, the effect of detector inefficiencies is just to decrease the probability $P^{AB}_{N'}\left(\phi_A, \phi_B\right)$; the error rate is not increased. In contrast, dark counts will effect the observed error rate. Let q be the probability for Alice and Bob to register a dark count in any given time bin. It is possible for Alice and Bob to both obtain dark counts within the same time bin. These clicks are uncorrelated and can lead to errors. The situation is exacerbated when detector inefficiencies are combined with dark counts. To see why, consider the case where Alice and Bob should both detect photons at D2. The inefficiency of Bob's detector means that he might not register a click, but could instead see a dark count at D3.

The effects of the imperfect detectors will thus change the probability of error from that given in equation (8). Using the fact that $P^{AB}_{N'}\left(2\pi k/d, 0\right) = P^{AB}_{N'}\left(0, 2\pi\left(d-k\right)/d\right)$ and $P^{AB}_{N'}\left(0, 0\right) = P^{AB}_{N'}\left(2\pi k/d, 2\pi\left(d-k\right)/d\right)$, we find that the error probability is

$$P_E\left(N'\right) = \frac{\gamma P^{AB}_{N'}\left(2\pi n/d, 0\right) + Q^2}{\gamma\left[P^{AB}_{N'}\left(2\pi n/d, 0\right) + P^{AB}_{N'}\left(0, 0\right)\right] + 2Q^2}, \quad (9)$$

$$\text{where} \quad \gamma = \eta^2\left(1-\mathrm{Q}\right)^2 + 2\eta\left(1-\eta\right)\mathrm{Q}\left(1-\mathrm{Q}\right),$$

and where $Q = qN'$. The errors in the alignment will be included in the probabilities $P^{AB}_{N'}\left(\phi_A, \phi_B\right)$. We will assume that the error for jitter is either so small that it can be ignored or we disregard clicks in time bins that are sufficiently near to the dth time bin, which changes the probability $P^{AB}_{N'}\left(\phi_A, \phi_B\right)$.

The error probability for 8 and 1024 time bins is plotted in figure 3. In all of the plots we assume that the time bins have a width of 130ps and that the detectors have a dark count rate of 300 counts per second. The probability to see a dark count in any given time bin is thus $q = 3.9 \times 10^{-8}$. In practice, one would have a threshold for tolerable errors. For the sake of illustration, we can take this threshold to be $P_E\left(N'\right) = 0.01$, i.e. 1%. This threshold is indicated in the figure by the red dotted line. An important conclusion to draw from both figures 3(a) and (b), is that $P_E\left(N'\right)$ can be less than 0.01 for suitable values of the reflectivities. For example, for 8 time bins and $\eta = 0.1$, we can obtain an error less than 0.01 by setting $\left|R_1\right|^2 = \left|R_2\right|^2 \geqslant 0.905$. Similarly, the error can be made less than 2% (i.e. $P_E\left(N'\right) = 0.02$) by choosing $\left|R_1\right|^2 = \left|R_2\right|^2 \geqslant 0.89$.

An interesting feature of the curves is the appearance of a trade-off with respect to how the errors vary with the reflectivities. Previously, we found that increasing $\left|R_1\right|$ and $\left|R_2\right|$ would decrease the errors (see figure 2). When dark counts are included, we find that there becomes a point where increasing the reflectivity will eventually make the errors worse. The position of the minium will depend on both the dark count probability q and the efficiency η. The minimum occurs due to the fact that the longer we wait for a click, the more likely we are to see a dark counts. When the reflectivity is large, the photons will spend longer in the interferometer which increases our chances of getting a dark count. This also explains why the error gets worse as η decreases. When η is small, we will lose photons, which increases the average time we must wait to detect a photon.

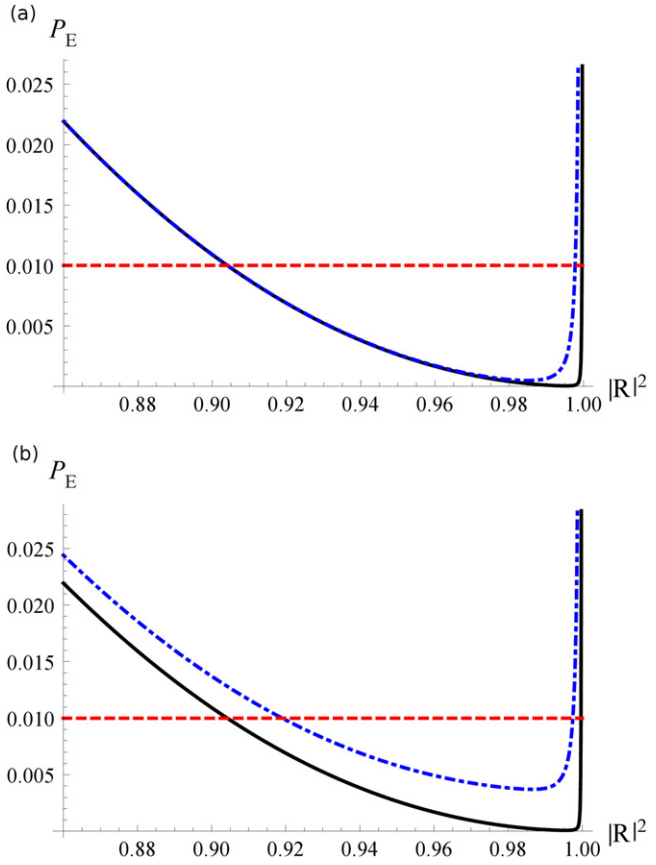

Figure 3. Two plots of error probability, P_E, as a function of $|R|^2 = \left|R_1\right|^2 = \left|R_2\right|^2$. The value of $k = d/2$, hence $\phi_A = 0$ and $\pi/2$, while $\phi_B = 0$ and $\pi/2$. Both plots are for $q = 3.9 \times 10^{-8}$, which corresponds to a dark count rate of 300 counts per second and time bins of width 130ps. Plot (a) is for $d = 8$ time bins and $N' = 800$, while (b) is for $d = 1024$ time bins and $N' = 1200$. In each plot the black line corresponds to the case of $\eta = 1$, while the dotted and dashed blue line is for $\eta = 0.1$. The dotted red line indicate the point where the error probability is 1%.

The effects of dark counts can be minimized if we decrease the time we wait to see a photon in *each experimental run*. One way of achieving this is to decrease N'. Recall that any photons detected in time-bins after N', are not counted as security events. Decreasing N' will thus decrease the error, but at the expense of decreasing the available measurement results. If we are to be sure that an eavesdropper is not intercepting Bob's photons, then we require a sufficient number of security events. We thus see that if we decrease N', then we would need to compensate for the loss of data by performing more experimental runs.

One can gain further insight into this trade-off by looking at a simple example. Consider the case of $d = 1024$, $\eta = 0.1$, $q = 3.9 \times 10^{-8}$, i.e. the parameters used in figure 3(b). In the absence of dark counts, then a typical value for N' would be $N' = 2d = 2048$. For $|R_1|^2 = |R_2|^2 = |R|^2 = 0.92$, the observed error is approximately 1.5%. The cut-off used in figure 3(b) was $N' = 1200$, which lead to an error of less than 1%, when $|R|^2 = 0.92$. The decrease in error is accompanied by a decrease in the count rate of approximately 37%.

6. Conclusion

We have described a compact setup for high-dimensional, time-bin based QKD. This approach offers the promise of encoding multiple key bits on each photon. In particular, entanglement based protocols have been shown to allow for 10 bits to be encoded on each photon pair, under realistic but challenging experimental conditions [12].

The setup was based on a modified Mach–Zehnder interferometer that operated as a cavity. The cavity enables one to implement measurements in two different bases, which were approximately mutually unbiased to each other. We then explained how this could be used within an entanglement based QKD protocol. It was shown that one can encode the key bits within the time of arrival information, while checking for an eavesdropper using the other basis. An important practical point was that we needed only two different phases settings to observe a disturbance in the temporal correlation within an entangled photon pair.

We studied the probability to introduce errors due the approximate nature of the mutually unbiased measurement. It was found that this error could be make arbitrarily low by increasing the reflectivity of the two beam splitters. We also investigated the effects of reasonable errors on the scheme. It was found that presence of dark counts introduce a trade-off in the choice of reflectivity. The effects of dark counts and detector inefficiencies were found to be quite small for a reasonable number of time bins. For larger numbers of time bins, say 1024, then one can decrease the cut-off time for accepted security checks. This will decrease the errors due to dark counts, but at a cost of decreasing the number of valid security events one gets for a given period of time. Crucially, we found that the error could be made as low as 1%. This demonstrates the robustness of the setup to errors.

A key benefit of our protocol is that it is compact and only requires a *single* interferometer each for Alice and Bob. This contrast sharply with alternative approaches to high-dimensional QKD, which would require complicated networks of interferometers. Furthermore, the approach uses mutually unbiased measurements, which ensures that the security can be analysed using existing approaches.

Acknowledgments

We thank Electra Eleftheriadou, Kevin McCusker, Paul Kwiat and Daniel Gauthier for helpful discussions. We also thank Norbert Lütkenhaus for very useful discussions on the effects of errors. This research was supported by the DARPA InPho program through the US Army Research Office award W911NF-10-0395 and by the UK EPSRC grant no. EP/I012451/1.

References

[1] van Assche G 2006 *Quantum Cryptography and Secret-Key Distribution* (Cambridge: Cambridge University Press)
[2] Barnett S M 2009 *Quantum Information* (Oxford: Oxford University Press)
[3] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
[4] Scarani V, Bechmann-Pasquinucci F, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301
[5] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[6] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557
[7] Naik D S, Peterson C G, White A G, Berglund A J and Kwiat P G 2000 *Phys. Rev. Lett.* **84** 4733
[8] Tittel W, Brendel J, Zbinden H and Gisin N 2000 *Phys. Rev. Lett.* **84** 4737
[9] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing (Bangalore, India 1984)* (New York: IEEE) p 175
[10] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121
[11] Bourennane M, Karlsson A and Björk G 2001 *Phys. Rev.* A **64** 012306
[12] Brougham T and Barnett S M 2012 *Phys. Rev.* A **85** 032322
[13] Nikolopoulos G M, Ranade K S and Alber G 2006 *Phys. Rev.* A **73** 032325
[14] Cerf N J, Bourennane M, Karlsson A and Gisin N 2002 *Phys. Rev. Lett.* **88** 127902
[15] Leach J, Bolduc E, Gauthier D J and Boyd R W 2012 *Phys. Rev.* A **85** 060304
[16] Allen L, Barnett S M and Padgett M J 2003 *Optical Angular Momentum* (Bristol: Institute of Physics Publishing)
[17] Gibson G, Courtial J, Padgett M J, Vasnetsov M, Pas'ko V, Barnett S M and Franke-Arnold S 2004 *Opt. Express* **12** 5448
[18] Barreiro J T, Wei T-C and Kwiat P G 2008 *Nat. Phys.* **4** 282
[19] Boyd R W, Rodenburg B, Mirhosseini M and Barnett S M 2011 *Opt. Express* **19** 18310
[20] Marcikic I, de Riedmatten H, Tittel W, Scarani V, Zbinden H and Gisin N 2002 *Phys. Rev.* A **66** 062308
[21] de Riedmatten H, Marcikic I, Scarani V, Tittel W, Zbinden H and Gisin N 2004 *Phys. Rev.* A **69** 050304
[22] Stucki D, Zbinden H and Gisin N 2005 *J. Mod. Opt.* **52** 2637
[23] Ali-Khan I and Howell J C 2006 *Phys. Rev.* A **73** 031801
[24] Barreiro J T, Langford N K, Peters N A and Kwiat P G 2005 *Phys. Rev. Lett.* **95** 260501
[25] Ali-Khan I, Broadbent C J and Howell J C 2007 *Phys. Rev. Lett.* **98** 060503
[26] Mower J, Zhang Z, Desjardins P, Lee C, Shapiro J H and Englund D 2013 *Phys. Rev.* A **87** 062322
[27] Lee C, Mower J, Zhang Z, Shapiro J H and Englund D arXiv:1311.1233
[28] Nunn J, Wright L J, Söller C, Zhang L, Walmsley I A and Smith B J 2013 *Opt. Express* **21** 15959
[29] Schwinger J 1960 *Proc. Natl. Acad. Sci. USA* **46** 570
[30] Wootters W and Fields B D 1989 *Ann. Phys.* **191** 363
[31] Pegg D T, Vaccaro J A and Barnett S M 1990 *J. Mod. Opt.* **37** 1703
[32] Mayers D 2001 *J. Assoc. Comput. Mach.* **48** 351

[33] Lo H-K and Chau H F 1999 *Science* **283** 2050
[34] Biham E, Boyer M, Boykin P O, Mor T and Roychowdhury V 2000 *Proc. 32nd Annual ACM Symp. on Theory of Computing* (New York: ACM) pp 715–24
[35] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[36] Gottesman D, Lo H-K, Lütkenhaus N and Preskill J 2004 *Quantum Inf. Comput.* **4** 325
[37] Tomamichel M, Lim C C W, Gisin N and Renner R 2012 *Nat. Commun.* **3** 634
[38] Sheridan L and Scarani V 2010 *Phys. Rev.* A **82** 030301
[39] Nikolopoulos G M and Alber G 2005 *Phys. Rev.* A **72** 032320
[40] Brougham T, Barnett S M, McCusker K, Kwiat P G and Gauthier D J 2013 *J. Phys. B: At. Mol. Opt. Phys.* **46** 104010
[41] Reck M, Zeilinger A, Bernstein H J and Bertani P 1994 *Phys. Rev. Lett.* **73** 58
[42] Mower J, Wong F N C, Shapiro J H and Englund D 2011 arXiv:1110.4867
[43] Franson J D 1989 *Phys. Rev. Lett.* **62** 2205
[44] Zhang Z, Mower J, Englund D, Wong N C and Shapiro J H 2014 *Phys. Rev. Lett.* **112** 120506
[45] Brougham T and Barnett S M 2013 *Europhys. Lett.* **104** 30003
[46] Milonni P W and Eberly J H 2000 *Laser Physics* (Hoboken, NJ: Wiley)
[47] Lo H-K, Chau H G and Ardehali M 2005 *J. Cryptol.* **18** 133
[48] Gao J, Zhu C and Xiao H 2014 *Europhys. Lett.* **105** 60003