

High error-rate quantum key distribution for long-distance communication

Muhammad Mubashir Khan^{1,4}, Michael Murphy²
and Almut Beige³

¹ The School of Computing, University of Leeds, Leeds LS2 9JT, UK

² Institut für Quanteninformationsverarbeitung, Universität Ulm,
Albert-Einstein-Allee 11, 89081 Ulm, Germany

³ The School of Physics and Astronomy, University of Leeds,
Leeds LS2 9JT, UK

E-mail: mmkhan@comp.leeds.ac.uk

New Journal of Physics **11** (2009) 063043 (16pp)

Received 16 January 2009

Published 22 June 2009

Online at <http://www.njp.org/>

doi:10.1088/1367-2630/11/6/063043

Abstract. In the original BB84 protocol by Bennett and Brassard, an eavesdropper is detected because his attempts to intercept information result in a quantum bit error rate (QBER) of at least 25%. Here we design an alternative quantum key distribution protocol, where Alice and Bob use two mutually unbiased bases with one of them encoding a '0' and the other one encoding a '1'. The security of the scheme is due to a minimum index transmission error rate (ITER) introduced by an eavesdropper that increases significantly for higher-dimensional photon states. This allows for more noise in the transmission line, thereby increasing the possible distance between Alice and Bob without the need for intermediate nodes.

⁴ Author to whom any correspondence should be addressed.

Contents

1. Introduction	2
2. Alternative design	4
3. Eavesdropping	7
3.1. The ITER	7
3.2. The QBER	8
4. Optimal choices of e, f and g	10
4.1. The $N = 2$ case	10
4.2. The $N = 4$ case	11
4.3. The general case	12
4.4. Possible implementation	13
5. Conclusions	14
Acknowledgments	15
References	15

1. Introduction

The aim of quantum cryptography is to establish a shared, secret and random sequence of bits between a sender, called *Alice* and a receiver, called *Bob* [1]. This sequence constitutes a perfect cryptographic key, a so-called one-time pad, and allows Alice and Bob to securely encrypt a message of the same length. The cryptographic key is obtained solely via the transmission of photons and classical communication. Each bit is encoded in the state of a single photon and read out by Bob upon arrival via a quantum measurement. Random switching between different bases makes it impossible for an eavesdropper, called *Evan*, to predict the states used in the protocol. All his attempts to intercept photons result in a significant *quantum bit error rate* (QBER). This guarantees a high level of security, since Evan's presence is detected easily when Alice and Bob compare a number of test bits.

Under ideal conditions, the exchange of single photons allows Alice and Bob to establish a cryptographic key over an arbitrarily long distance. In practice, cryptographic setups consist of imperfect single-photon sources, lossy transmission lines, and photon detectors with dark count rates. Alice and Bob must hence apply classical information processing tools like error correction and privacy amplification [2, 3] to their data in order to obtain identical secret keys. However, cryptographic protocols are only secure as long as it is possible to detect the presence of an eavesdropper. System errors could cloud Evan's presence; especially since he could simply replace parts of the equipment with high-quality components. This makes it impossible to tolerate large system errors and limits the possible distance between Alice and Bob.

Recently, Rosenberg *et al* [4, 5] reported the creation of a secure cryptographic key over a distance of 144.3 km of optical fiber. Their scheme is based on a decoy state protocol [6]–[8] which is immune to photon number splitting attacks and highly resistant to Trojan horse attacks [9]. It is expected that improvements in filtering of blackbody photons might allow for an extension of the fiber to 250 km. In the mean time, Takesue *et al* [10] and Stucki *et al* [11] created a secure cryptographic key over a distance of 200 km of optical fiber. These experimental setups are believed to be the longest terrestrial quantum key distribution

fiber-links yet demonstrated. Comparable distances have been achieved in free space. For example, Schmitt-Manderbach *et al* [12] securely distributed a cryptographic key over a 144 km free-space link.

In this paper, we design a novel quantum key distribution protocol whose efficiency and minimum error rate in the case of eavesdropping increase with the dimension of the photon states used by Alice and Bob. In this way, we increase the threshold for tolerable system errors without sacrificing the security of the protocol and hence increase the possible distance between Alice and Bob. In principle, single photons could be purified with the help of quantum repeaters [13]. Proposals for their implementation (see e.g. [14, 15]) and other noise reducing links [16]–[18] have been made but their experimental implementation and their practical integration into cryptographic networks remains to be seen.

The above-mentioned long-distance quantum key distribution schemes [4, 5, 10, 12] are all based on the BB84 protocol by Bennett and Brassard [19]. In BB84, Alice encodes her bits in two-dimensional photon states. These can be obtained using polarization encoding. However, a more natural choice is time-bin encoding, which affords better protection of the photons against decoherence [20]. Alice and Bob independently vary their bases between two possibilities. A key bit is obtained whenever both use the same basis. This means, on average, every second photon contributes a bit to the cryptographic key. Using a simple intercept–resend strategy, an eavesdropper introduces a QBER of at least 25% into the communication.

In the following, we assume that Alice and Bob use time-bin or path encoded N -dimensional photon states. As in BB84, Alice and Bob randomly vary their bases between two mutually unbiased bases [21]. However, contrary to BB84, Alice and Bob detect the presence of an eavesdropper by calculating the *index transmission error rate* (ITER). As we shall see below, for $N = 2$, Evan causes a minimum ITER of 25%. In the case of four-dimensional photon states, this error rate becomes 37.5%. When increasing N further, the minimum ITER approaches 50%. The efficiency of the protocol in units of transmitted bits per photon is the same as the minimum ITER in case of eavesdropping. The states required by the proposed key distribution scheme can be realized using a symmetric Bell multiport beam splitter [22]. Before the transmission, the path encoding of the output states of the Bell multiport beam splitter should be switched to the above-mentioned time-bin encoding [20].

Several generalizations of quantum cryptographic schemes to higher dimensions have already been proposed. The papers [23]–[29] are generalizations of the original BB84 protocol [19] based on the encoding of information in higher-dimensional alphabets. However, recently it has been shown [31]–[33] that the security of the BB84 protocol is entirely compromised if Alice and Bob share, for example, four-dimensional photon states in this way [34]. Beige *et al* [35, 36] propose two alternative quantum cryptographic protocols using four-dimensional photon states, which, under ideal conditions, allow Alice and Bob to communicate directly but whose minimum error rates in the case of eavesdropping are relatively low.

Here we show that there are other possible cryptographic schemes in higher dimensions. As in [35, 36], Alice and Bob use two bases e and f with all states of e encoding a ‘0’ and all states of f encoding a ‘1,’ even when N is larger than two. This means, contrary to [19], [23]–[29], all vectors of the same basis encode the same bit. Moreover, a bit can be transmitted only when Alice and Bob use *different* bases. The quantum key distribution scheme considered in this paper is designed such that no conditions have to be posed on the states of e and f , thereby giving us a lot of flexibility when maximizing the relevant minimum error rate introduced by Evan.

For simplicity, we consider only intercept–resend eavesdropping attacks. This is not the only possible eavesdropping attack, but security against this is considered a strong indication for the general security of a quantum cryptographic protocol.

In the special case of $N = 2$, the cryptographic scheme proposed in this paper is essentially equivalent to the SARG quantum key distribution protocol [30] with the parameter χ chosen equal to $1/\sqrt{2}$. This protocol is tailored to be robust against photon number splitting attacks. In the SARG protocol, Alice publicly announces which one of the four different sets of states $\mathcal{A}_{+,+}$, $\mathcal{A}_{+,-}$, $\mathcal{A}_{-,+}$ and $\mathcal{A}_{-,-}$ she used, while our protocol requires her only to announce either ‘ $i = 1$ ’ or ‘ $i = 2$ ’. This difference is due to a redundancy in the SARG protocol.

There are five sections in this paper. In section 2, we introduce the notations used throughout this paper. In section 3, we calculate the ITER and the QBER for the quantum key distribution protocol introduced in section 2 as a function of the states used by Alice, Bob and Evan analytically. Afterwards, we determine their minima in the presence of intercept–resend eavesdropping attacks for different N s numerically. Geometrical considerations suggest that Alice and Bob should use two mutually unbiased bases. Section 4 analyses a concrete protocol based on this idea and shows that mutually unbiased bases indeed guarantee a high ITER and a high QBER in case of eavesdropping. Finally, we summarize our results in section 5.

2. Alternative design

In quantum cryptography there are conventionally three parties, Alice, Bob and Evan. Alice wants to transmit a sequence of secret bits to Bob. To do so, she prepares single photons in certain states and sends them to Bob. Bob measures the state of each incoming photon. Afterwards, Alice and Bob exchange information via classical communication. At the same time, Evan tries to catch the secret bits without revealing his presence. For example, he measures the state of every transmitted photon and listens in to the classical communication between Alice and Bob. The cryptographic protocol is secure as long as Evan’s attempts to obtain information result in an error rate which can be detected easily.

Let us start by introducing *sufficient* conditions for such a protocol to work:

1. Bob should measure the incoming photons in a randomly chosen basis. Otherwise, Evan simply uses the same measurement basis and the bit error rate remains zero. This means Bob should randomly switch between *at least* two sets of basis states. In the following we assume that this is the case and denote these bases

$$e \equiv \{|e_i\rangle : i = 1, \dots, N\} \quad \text{and} \quad f \equiv \{|f_i\rangle : i = 1, \dots, N\}. \quad (1)$$

Here N is the dimension of the photon states. The only condition imposed on e and f is that they form a basis.

2. Similarly, Alice should encode the information that she wants to transmit to Bob such that it cannot be deduced easily by Evan. To obtain a nonzero error rate in case of eavesdropping, she should either use non-orthogonal states (as in B92 [37]) or randomly switch between *at least* two sets of basis states (as in BB84 [19]). For simplicity, we assume in the following that Alice prepares each photon randomly in one of the basis states of e and f .
3. In order to establish strong correlations between Alice’s input state and Bob’s measurement outcome, Alice needs to reveal some information via classical communication. This information should be enough for Alice and Bob to obtain a shared secret key bit but not

Table 1. Bob's interpretation of his measurement outcomes as a function of the index announced by Alice. The parameters η_{ij} and μ_{ij} can assume the values '0', '1' or '×' indicating whether a '0', a '1' or no bit is transmitted.

Index announced by Alice	State measured by Bob									
	$ e_1\rangle$	$ e_2\rangle$	$ e_N\rangle$	$ f_1\rangle$	$ f_2\rangle$	$ f_N\rangle$
1	η_{11}	η_{12}	η_{1N}	μ_{11}	μ_{12}	μ_{1N}
2	η_{21}	η_{22}	η_{2N}	μ_{21}	μ_{22}	μ_{2N}
...
...
N	η_{N1}	η_{N2}	η_{NN}	μ_{N1}	μ_{N2}	μ_{NN}

enough for the eavesdropper to deduce it. One possibility is that Alice announces which basis, e or f , she used (as in BB84 [19]). Another possibility is that Alice reveals the index i of the respective basis state (as in [35, 36]). This does not reveal any information about the key as long as the states $|e_i\rangle$ and $|f_i\rangle$ with the same index i encode different bits. In this paper, we consider this second approach and show that it can guarantee relatively high error rates in the presence of an eavesdropper.

4. We now have a closer look at how Bob should interpret his measurement outcomes after Alice told him the index i of her basis state. He can do this by using a table like table 1. If Alice announces that she prepared the photon in a state with index i , Bob obtains ' η_{ij} ' when he measures $|e_j\rangle$ and he obtains ' μ_{ij} ' when he measures $|f_j\rangle$. The parameters η_{ij} and μ_{ij} in the table assume three different values, '0', '1', or '×', depending on whether Bob obtains a '0', a '1', or no key bit is transmitted.

Suppose Alice sends a photon prepared in $|e_1\rangle$ in order to transmit a '0'. This implies

$$\eta_{11} = \text{'0' or '×'} \quad (2)$$

in order to avoid that Bob obtains a wrong key bit. The state $|f_1\rangle$ has to encode a '1' in this case. Otherwise, Evan knows that a '0' is transmitted, when ' $i = 1$ ' is announced. Consequently,

$$\mu_{11} = \text{'1' or '×'}. \quad (3)$$

Moreover, if Alice announces ' $i = 1$ ' and Bob measures $|f_j\rangle$ with $j \neq 1$, then he knows for sure that she prepared her photon in $|e_1\rangle$. Analogously, if Alice announces ' $i = 1$ ' and Bob measures $|e_j\rangle$ with $j \neq 1$, then he knows that Alice prepared $|f_1\rangle$. Alice and Bob should therefore choose

$$\eta_{1j} = \text{'1'} \quad \text{and} \quad \mu_{1j} = \text{'0'}, \quad \text{for all } j \neq 1. \quad (4)$$

There is no need for Bob to ignore a measurement outcome with $j \neq 1$ since he always knows which key bit the photon encodes in this case.

5. It is indeed possible (cf equations (2)–(4)) that table 1 contains no crosses and that every detected photon transmits one bit of the cryptographic key. However, the minimum error rate in the case of eavesdropping is already known to be relatively low in this case [35, 36]. We therefore assume here that Bob ignores the cases where his measured state has the index i announced by Alice and choose

$$\eta_{ii} = \mu_{ii} = \text{'×'}. \quad (5)$$

Table 2. Bob's interpretation of his measurement outcomes as a function of the index announced by Alice for $N = 4$. All states of e encode a '0', while all states of f encode a '1'. A key bit is obtained whenever the index of Bob's state is different from Alice's index.

Index announced by Alice	States measured by Bob							
	$ e_1\rangle$	$ e_2\rangle$	$ e_3\rangle$	$ e_4\rangle$	$ f_1\rangle$	$ f_2\rangle$	$ f_3\rangle$	$ f_4\rangle$
1	×	1	1	1	×	0	0	0
2	1	×	1	1	0	×	0	0
3	1	1	×	1	0	0	×	0
4	1	1	1	×	0	0	0	×

This means a key bit can only be obtained when Bob's measurement basis is different from the one used by Alice to prepare the photon. One can easily check that Alice and Bob always obtain the same secret key bit under ideal conditions.

6. For symmetry reasons, Alice should have equally many states to encode a '0' as she has to encode a '1'. Without restrictions we therefore assume in the following that all the states of e encode a '0' while all states of f encode a '1'. This means, Bob obtains a '1' whenever he measures a state $|e_j\rangle$ with j different from Alice's index i . Analogously, he obtains a '0' when he measures a state $|f_j\rangle$ with $j \neq i$.

The final protocol is summarized in table 2 for the case where Alice and Bob communicate using four-dimensional photon states. For arbitrary N , the entire scheme works as follows:

1. Alice generates a random key sequence of classical bits and randomly assigns each bit value a random index $i = 1, 2, \dots, N$.
2. Alice then uses this sequence and sends single photons prepared accordingly either in $|e_i\rangle$ or $|f_i\rangle$ to Bob.
3. Bob measures the state of every incoming photon, thereby randomly switching the measurement basis between e and f .
4. Alice publicly announces the random sequence of indices i used to establish the cryptographic key.
5. Bob interprets his measurement outcomes accordingly, using, for example, table 2, if $N = 4$. He obtains a key bit whenever his index is different from the index announced by Alice.
6. Bob tells Alice which photon measurements have been successful and provide a bit of the secret key.
7. Finally, Alice and Bob determine whether an eavesdropper introduced an error into their communication. Whenever this error rate is sufficiently small, Alice and Bob can assume that no eavesdropping has occurred.

Note that no conditions are imposed on e and f in this section other than them being bases. This gives us a lot of flexibility when maximizing the security of the corresponding cryptographic protocol. In fact, the only difference between the above protocol and the direct communication scheme introduced in [35, 36] is that we avoid the assumption of $\langle e_i | f_i \rangle$ being

zero. Alice and Bob therefore have to discard their measurement outcomes when both their states have the same index. As we shall see below, the payoff for the corresponding loss in efficiency is a relatively high error rate in the presence of an eavesdropper.

3. Eavesdropping

In the quantum key distribution protocol proposed here, the index i of the photon state in transmission is the only publicly announced information. This index does not reveal any information about the corresponding key bit since it equally likely encodes a ‘0’ as it encodes ‘1’. An eavesdropper can therefore only learn about the cryptographic key by performing quantum measurements on the transmitted photons. In the following, we assume that Evan measures the state of every photon using a basis g which is optimal for his purpose. Afterwards, he forwards his measurement outcome to Bob. This eavesdropping strategy is known as an *intercept–resend* attack. Although it is not the most general eavesdropping attack, the corresponding error rate is a strong indication for the security of a cryptographic protocol. Our aim is to increase the minimum error rate introduced by an eavesdropper above the 25% of the original BB84 protocol [19]. As already mentioned above, there are different types of errors that Alice and Bob can consider.

3.1. The ITER

In the following, i denotes again the index of the photon state prepared by Alice and j is the index of the basis vector measured by Bob. When Alice and Bob use different bases, j can assume any value between 1 and N , even in the absence of any eavesdropping. However, when Alice and Bob use the same basis, i and j should be the same. To detect Evan’s presence, Alice and Bob could therefore do the following: Alice should randomly select some photons that should not be used to obtain key bits. For these photons, she tells Bob exactly which states she prepared. Comparing this information with his own measurement outcomes, Bob can then easily calculate the ITER.

An index transmission error occurs when a photon prepared in $|e_i\rangle$ ($|f_i\rangle$) is measured at Bob’s end as $|e_j\rangle$ ($|f_j\rangle$) with $i \neq j$. Assuming that Alice prepares the $2N$ basis states of e and f with the same frequency and that Bob measures e and f with the same frequency, we find that the ITER of the proposed protocol equals

$$P_{\text{ITER}} = \frac{1}{2N} \sum_{i=1}^N \sum_{k=1}^N \sum_{j \neq i} \left[|\langle e_i | g_k \rangle|^2 \cdot |\langle g_k | e_j \rangle|^2 + |\langle f_i | g_k \rangle|^2 \cdot |\langle g_k | f_j \rangle|^2 \right] \quad (6)$$

for a given set of bases e , f and g . The states $|g_k\rangle$ denote Evan’s possible measurement outcomes, which are forwarded to Bob without alteration. In principle, Evan could change the state of the transmitted photon by guessing which state Alice prepared. However, this strategy is not expected to reduce the above error rate significantly. A nonzero overlap between the basis states of e and f ensures that there is always a certain probability to guess incorrectly.

To simplify equation (6) we take the normalization of all the relevant basis vectors into account which implies

$$\sum_{j=1}^N |\langle g_k | e_j \rangle|^2 = \sum_{j=1}^N |\langle g_k | f_j \rangle|^2 = \sum_{k=1}^N |\langle g_k | e_j \rangle|^2 = \sum_{k=1}^N |\langle g_k | f_j \rangle|^2 = 1. \quad (7)$$

Table 3. Minimum ITER and minimum QBER as a function of N introduced by Evan in an intercept–resend eavesdropping attack when Alice and Bob use optimal bases e and f . Both error rates are obtained from a numerical simulation which randomly generates 100 000 f s and 100 000 g s and calculates all the corresponding values for P_{ITER} and P_{QBER} using equations (8) and (11).

Dimension N	ITER	QBER
2	0.2500	0.5000
3	0.3340	0.4959
4	0.4003	0.4759
5	0.4965	0.4389
6	0.5843	0.4379

Substituting these identities into equation (6), the expression for the ITER simplifies to

$$P_{\text{ITER}} = 1 - \frac{1}{2N} \sum_{i=1}^N \sum_{k=1}^N \left[|\langle g_k | e_i \rangle|^4 + |\langle g_k | f_i \rangle|^4 \right]. \quad (8)$$

The same expression is obtained when calculating this error rate by subtracting the probability of not making an error under the condition that Alice and Bob use the same basis from unity.

While Alice and Bob want the error rate in equation (8) to be as large as possible, Evan wants it to be as small as possible. Both parties, with Alice and Bob on one side and Evan on the other side, try to optimize the choice of the bases e , f and g accordingly. Table 3 shows the results of a numerical solution of this double-optimization problem for different dimensions N . To obtain this table, the basis e is kept fixed and a large number of bases f is generated randomly. For each f we then generate another large set of random bases g and determine the minima of the corresponding error rates using equation (8). This is illustrated in figure 1 for the $N = 4$ case. The ITER in table 3 is the maximum of all the obtained minimum error rates.

For $N = 2$, we find that the minimum ITER introduced by an eavesdropper equals 25% when Alice and Bob use an optimal choice of e and f , as in the original BB84 protocol [19]. However, when Alice and Bob increase the dimension N of their photon states, the minimum ITER increases. One can easily see that 50% constitutes an upper bound for the minimum ITER by considering the case where Evan measures the incoming photons either in the e or in the f basis. Using this eavesdropping strategy, the states of at least half of the transmitted photons remain unaffected.

3.2. The QBER

Alternatively, Alice and Bob can detect a potential eavesdropper by calculating the usual QBER. To do so, both randomly select a certain number of control bits from the obtained key sequence and compare them openly. Note that a key bit is obtained when the index j of the state measured by Bob and the index i of the state prepared by Alice are different. Bob interprets his measurement result correctly only when both states belong to a different bases. A quantum bit error hence occurs when Bob measures $|e_j\rangle$ ($|f_j\rangle$), while Alice prepared $|e_i\rangle$ ($|f_i\rangle$) with $i \neq j$.

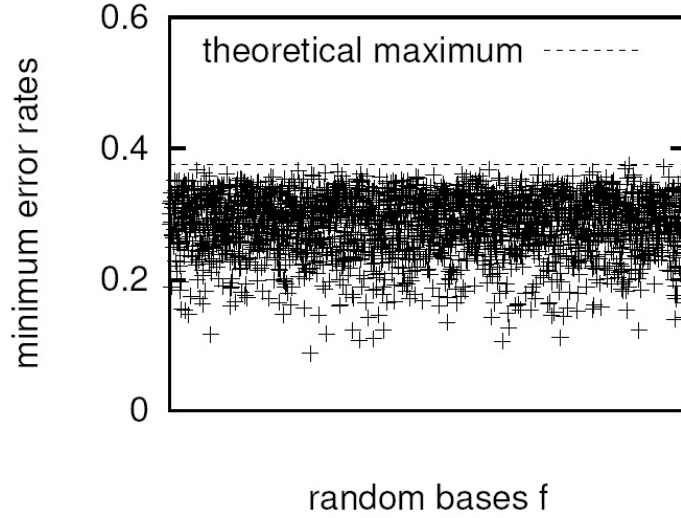


Figure 1. Illustration of the numerical calculation of the minimum ITER introduced by Evan for $N = 4$ and 2 500 random choices of f . The crosses are the minima obtained after generating 10^6 g s and comparing the corresponding ITERs given by equation (8) for each f . The dotted line shows the theoretical maximum of 37.5% of these minima (cf equation (21)).

Using equation (6), the QBER for a given set of bases e , f and g can be written as

$$P_{\text{QBER}} = \frac{P_{\text{ITER}}}{2P_{\text{IC}}}, \quad (9)$$

where the *index-change* (IC) probability P_{IC} ,

$$P_{\text{IC}} = \frac{1}{4N} \sum_{i=1}^N \sum_{k=1}^N \sum_{j \neq i} [|\langle e_i | g_k \rangle|^2 \cdot |\langle g_k | e_j \rangle|^2 + |\langle f_i | g_k \rangle|^2 \cdot |\langle g_k | f_j \rangle|^2 + |\langle e_i | g_k \rangle|^2 \cdot |\langle g_k | f_j \rangle|^2 + |\langle f_i | g_k \rangle|^2 \cdot |\langle g_k | e_j \rangle|^2], \quad (10)$$

is the probability that the index j of Bob's state is different from the index i of Alice's state. Using the identities in equation (7), we find that the QBER in equation (9) equals

$$P_{\text{QBER}} = \frac{2N - \sum_{i=1}^N \sum_{k=1}^N [|\langle e_i | g_k \rangle|^4 + |\langle f_i | g_k \rangle|^4]}{4N - \sum_{i=1}^N \sum_{k=1}^N [|\langle e_i | g_k \rangle|^2 + |\langle f_i | g_k \rangle|^2]}. \quad (11)$$

The third column in table 3 shows the minimum QBER introduced by an eavesdropper, when Alice and Bob use optimal bases e and f , for different dimensions N . As in section 3.1, these probabilities have been obtained by comparing probabilities for a large set of randomly generated bases f and g .

Even for $N = 2$, the minimum QBER can be as high as 50%. A more detailed analysis of the corresponding protocol shows that Alice and Bob can realize this scenario by choosing e and f almost identical, independent of Evan's choice of measurement basis g . However, the price they pay for this very high QBER is a steep drop in the efficiency of their quantum key

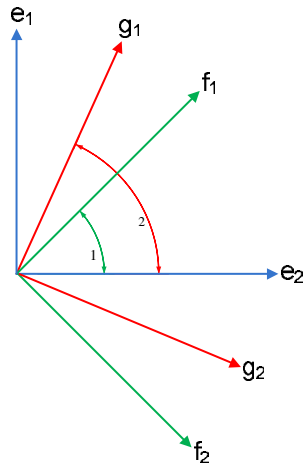


Figure 2. Basis vectors used by Alice, Bob and Evan in the $N = 2$ protocol. To maximize the minimum error rate introduced by Evan in case of an intercept–resend attack, Alice and Bob should choose $\phi_1 = \frac{1}{4}$. This yields an error rate of 25%, independent of Evan’s choice of ϕ_2 .

distribution. In the extreme case, where $|e_1\rangle \equiv |f_1\rangle$ and $|e_2\rangle \equiv |f_2\rangle$, it becomes impossible to generate secret key bits, since Alice’s and Bob’s state always have the same index i , at least in the absence of any eavesdropping. In the following, we assume therefore that Alice and Bob use the ITER in order to detect the presence of an eavesdropper.

4. Optimal choices of e , f and g

We now address the question of how Alice and Bob can take advantage of the high ITERs shown in table 3 by having a look at possible realizations of the proposed quantum key distribution protocol. First, we consider the $N = 2$ case, which suggests an optimal strategy for Alice and Bob in higher dimensions. Moreover, we discuss in this section what Evan can do to best cloud his presence.

4.1. The $N = 2$ case

The problems that Alice, Bob and Evan have to solve in the $N = 2$ case in order to optimize their strategies are exactly the same as in BB84 [19]. Suppose Alice and Bob choose (cf figure 2)

$$|e_1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |e_2\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad (12)$$

while $|f_1\rangle$ and $|f_2\rangle$ are, without restrictions, given by

$$|f_1\rangle = \begin{pmatrix} \cos \phi_1 \\ \sin \phi_1 \end{pmatrix}, \quad |f_2\rangle = \begin{pmatrix} -\sin \phi_1 \\ \cos \phi_1 \end{pmatrix}. \quad (13)$$

Moreover, we write the states of Evan’s optimal measurement basis as

$$|g_1\rangle = \begin{pmatrix} \cos \phi_2 \\ \sin \phi_2 \end{pmatrix}, \quad |g_2\rangle = \begin{pmatrix} -\sin \phi_2 \\ \cos \phi_2 \end{pmatrix}. \quad (14)$$

Substituting these states into equation (8), we find

$$P_{\text{ITER}} = \frac{1}{4} \left[\sin^2(2(\phi_1 - \phi_2)) + \sin^2(2\phi_2) \right]. \quad (15)$$

In order to maximize the minimum of this probability with respect to ϕ_2 , Alice and Bob should choose $\phi_1 = \frac{1}{4}\pi$. In this case, $\sin^2(2(\phi_1 - \phi_2))$ becomes the same as $\cos^2(2\phi_2)$. This error rate equals 25% independent of Evan's choice of ϕ_2 . For the eavesdropper, every possible strategy is hence an optimal one.

In other words, for $N = 2$, Alice and Bob's optimal choice for e and f are two *mutually unbiased* bases [21]. This means, upon measurement, a photon prepared in any of the basis states of e is found with equal probability in any of the basis states of f and vice versa. As shown in figure 2, e and f should be as far away from each other as possible. A straightforward generalization of this result to higher dimensions suggests that Alice and Bob should always use two mutually unbiased bases e and f .

4.2. The $N = 4$ case

Let us now have a closer look at the case where Alice and Bob communicate with four-dimensional photon states. To obtain two mutually unbiased bases, they could choose for example

$$|e_1\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad |e_2\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad |e_3\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad |e_4\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \quad (16)$$

while the states of f are given by

$$|f_1\rangle = \frac{1}{2} \begin{pmatrix} 1 \\ 1 \\ -1 \\ -1 \end{pmatrix}, \quad |f_2\rangle = \frac{1}{2} \begin{pmatrix} -1 \\ 1 \\ 1 \\ -1 \end{pmatrix}, \quad |f_3\rangle = \frac{1}{2} \begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix}, \quad |f_4\rangle = \frac{1}{2} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}. \quad (17)$$

To find an optimal intercept–resend strategy for the eavesdropper, we assume that he measures states which lie on a line between the closest states of the e and the f basis. More concretely, we choose

$$|g_i\rangle = \frac{\cos \alpha |e_i\rangle + \sin \alpha |f_i\rangle}{\left(1 + \frac{1}{2} \sin(2\alpha)\right)^{1/2}}. \quad (18)$$

One can easily check that the $|g_i\rangle$'s are normalized and pairwise orthogonal. This applies since the indices of the basis states in equations (16) and (17) have been chosen accordingly. Using equation (8), we find that the ITER introduced by Evan now equals

$$P_{\text{ITER}} = \frac{3}{8} \left[1 + \frac{\sin^2(2\alpha)}{(2 + \sin(2\alpha))^2} \right]. \quad (19)$$

Since the second term in the brackets is always positive, one can easily see that $P_{\text{ITER}} \geq 37.5\%$. Indeed, the best strategy for Evan is to choose $\sin(2\alpha) = 0$. This means, Evan should measure either e or f .

Figure 3 shows the error rate introduced by Evan for the above choice of e and f and for a large set of randomly generated g s with $N = 4$. It confirms that P_{ITER} is always above 37.5%,

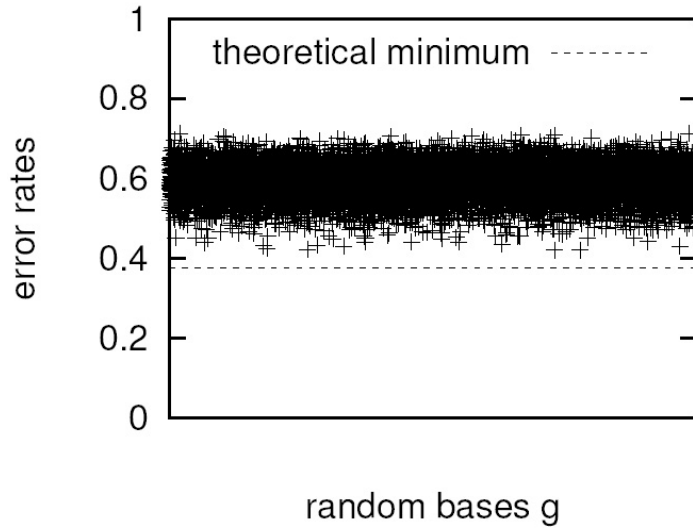


Figure 3. Numerical calculation of the error rates introduced by Evan for 10^5 randomly generated four-dimensional g s, while the states of e and f are as in equations (16) and (17). We see that these rates are always above their theoretical minimum (cf equation (21)) of 37.5% (dotted line), which is obtained when Evan measures either e or f .

if Alice and Bob use two mutually unbiased bases. This applies even when no assumption on the form of the states of g is made, as we do for our analytical calculations in equation (18). A comparison of $P_{\text{ITER}} = 37.5\%$ with the result in table 3 for $N = 4$ confirms that this error rate corresponds to (or is at least very close to) an optimal strategy of Alice, Bob and Evan. Both results agree within the error limits of the underlying numerical calculation.

4.3. The general case

Let us now have a look at the optimal choice of e , f and g for the general case where Alice and Bob use N -dimensional photon states. As suggested at the end of section 4.1, we assume that Alice and Bob use two mutually unbiased bases. More concretely, we assume that their states are given by

$$e_{ij} = \delta_{ij} \quad \text{and} \quad f_{ij} = \frac{1}{\sqrt{N}} \omega_N^{(i-1)(j-1)} \quad \text{with} \quad \omega_N = \exp\left(\frac{2i\pi}{N}\right), \quad (20)$$

$|e_i\rangle \equiv (e_{i1}, e_{i2}, \dots, e_{iN})^T$ and $|f_i\rangle \equiv (f_{i1}, f_{i2}, \dots, f_{iN})^T$. One can easily check that e and f are orthonormal and mutually unbiased. We then generate a large set of random g s and calculate the corresponding error rates P_{ITER} using equation (8). Table 4 shows the maxima of these rates as a function of N . The given error rates hence correspond to Evan's optimal intercept-resend eavesdropping strategy.

A comparison of the ITERs in table 4 with the ITERs in table 3 confirms that using two mutually unbiased bases e and f is (at least close to) an optimal strategy for Alice and Bob. For $N = 2$, we find again that the minimum error rate introduced by Evan equals 25%. For $N = 3$ this rate equals 33%, and for higher-dimensional photon states, the values in the third column of table 4 approach their predicted maximum of 50% (cf section 3). The second column has

Table 4. Minimum ITER introduced by an eavesdropper in the case of an intercept–resend attack when Alice and Bob use the mutually unbiased bases e and f of equation (20). The second column is the result of a numerical simulation, which generates 5 000 000 g s, calculates the respective error rates using equation (8), and determines their minimum. Third column shows the theoretical values given by equation (21).

Dimension N	ITER (numerics)	ITER (analytics)
2	0.2500	0.2500
3	0.3333	0.3333
4	0.3794	0.3750
5	0.4529	0.4000
6	0.5348	0.4167
7	0.6214	0.4286
8	0.6707	0.4375

been obtained from a numerical optimization of Evan’s strategy. Since it is a relatively hard computational problem to find the best eavesdropping measurement basis g numerically, the errors in this column are relatively large, especially for large N .

Let us now have a closer look at the best intercept–resend eavesdropping strategy for Evan. The discussion of the $N = 4$ case in section 4.2 suggests that Evan should measure either e or f in order to minimize the bit transmission error rate. If e and f are mutually unbiased, then the probability of detecting a photon in $|e_i\rangle$ equals $1/N$ when Alice prepares an f -state. Analogously, the probability of detecting a photon in $|f_i\rangle$ equals $1/N$ when Alice prepares an e -state. Substituting this into equation (8) yields

$$P_{\text{ITER}} = \frac{N - 1}{2N}. \quad (21)$$

For completeness we mention that the corresponding QBER (cf equation (11)) equals 33% independent of N . A comparison with a numerical evaluation of the ITER confirms that measuring either e or f and forwarding the respective measurement outcome to Bob is indeed an optimal (or at least a close to optimal) strategy for Evan, if Alice and Bob test his presence by calculating this error rate.

Let us conclude this subsection by commenting on the efficiency of the described quantum key distribution scheme. As in BB84, Alice and Bob randomly switch between two sets of basis states. Here a key bit can only be obtained when both use a *different* basis. Moreover, the index of the state measured by Bob should be different from the index of Alice’s state. The probability for this to happen and hence the mean number of bits per transmitted photon equals

$$P_{\text{success}} = \frac{N - 1}{2N}. \quad (22)$$

This expression is exactly the same as the ITER in equation (21).

4.4. Possible implementation

In order to implement the above protocol, Alice needs a single-photon source. As in BB84, the photon can come from a parametric down conversion crystal, a very weak laser pulse, or an

on-demand single-photon source. Using path encoding, the states of f can be prepared easily with the help of a Bell multiport beam splitter. Such a beam splitter may consist of a network of beam splitters and phase plates [38, 39], which have to be interferometrically stable. It can also be made by splicing N optical fibers [40]. Spliced fibre constructions are commercially available and can include between three and thirty input and output ports.

The main feature of a symmetric $N \times N$ Bell multiport beam splitter is that a photon entering any of its input ports is redirected with equal likelihood to any of its N possible output ports. One way for Alice to prepare the state $|e_i\rangle$ in equation (20) is to bypass the beam splitter and to send a single photon directly to output port i . In this case, preparing the state $|f_i\rangle$ in equation (20) only requires to send a single photon into input port i [22]. Bob can use the same setup as Alice to decode the key bit. To measure f , he should send the incoming photon first through a Bell multiport beam splitter and then detect it in one of the N output ports. To measure e , he can simply bypass this step. During the transmission, the path encoding should be switched to time-bin encoding, which promises a better protection of the photons against decoherence [20].

5. Conclusions

In this paper, we propose a quantum key distribution protocol where Alice and Bob use higher-dimensional photon states. The scheme does not encode information in a higher-dimensional alphabet [23]–[29] and is not a straightforward generalization of the original BB84 protocol [19]. Instead, Alice and Bob use two bases e and f with all e -states encoding a ‘0’ and all f -states encoding a ‘1’. Under ideal conditions, a key bit is obtained when Alice and Bob use different bases. In section 2, no conditions are imposed on the states of e and f , which gives us the flexibility to maximize the error rate introduced by an eavesdropper in the case of an intercept–resend attack. This is not the only possible eavesdropping strategy but security against this is a strong indication for the general security of a cryptographic protocol.

In section 3, we generate large sets of random basis states and determine the minimum ITER introduced by an eavesdropper numerically. For $N = 2$, this error rate equals the 25% QBER of the BB84 protocol [19]. However, the minimum ITER rapidly approaches 50% in higher dimensions (cf table 3). A detailed analysis of the $N = 2$ and 4 cases suggests that Alice and Bob should use two mutually unbiased bases e and f . The best an eavesdropper can do to hide his presence is to measure the transmitted photons either in e or f . This hypothesis is consistent with the numerical results in section 4 (cf table 4). Finally, we point out that the proposed quantum key distribution protocol can be implemented for example with the help of a symmetric Bell multiport beam splitter [22] and switching from path to time-bin encoding during the transmission. The mean number of key bits per transmitted photon turns out to be exactly the same as the minimum error rate introduced by Evan (cf equation (22)).

In section 3, we point out that it is in principle possible to obtain a minimum QBER close to 50%, even for $N = 2$. This requires Alice and Bob to use two bases e and f , which are almost identical. Unfortunately, this strategy corresponds to a very low efficiency of the proposed cryptographic protocol. For $e \equiv f$, the key transmission rate drops to zero. Analytic expressions for the QBER and the efficiency of the bit transmission in the presence of an eavesdropper for a given set of bases can be found in equations (10) and (11).

Acknowledgments

We thank H Zbinden for helpful comments. MMK thanks J Xu for encouraging discussions and acknowledges funding from the NED University of Engineering and Technology, Karachi, Pakistan. AB thanks the project students S So and P Woodward for their initial participation in this project and acknowledges a James Ellis University Research Fellowship from the Royal Society and the GCHQ. This project was supported in part by the UK Engineering and Physical Sciences Research Council through the QIP IRC and the EU Research and Training Network EMALI.

References

- [1] Gisin N, Ribordy G G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
- [2] Deutsch D, Ekert A, Josza R, Macchiavello C, Popescu S and Sanpera A 1996 *Phys. Rev. Lett.* **77** 2818
- [3] Ho H-K and Chau H F 1999 *Science* **283** 2050
- [4] Rosenberg D, Harrington J W, Rice P R, Hiskett P A, Peterson C G, Hughes R J, Lita A E, Nam S W and Nordholt J E 2007 *Phys. Rev. Lett.* **98** 010503
- [5] Rosenberg D *et al* 2008 Practical long-distance quantum key distribution system using decoy levels arXiv:0806.3085
- [6] Hwang W-Y 2003 *Phys. Rev. Lett.* **91** 057901
- [7] Wang X-B 2005 *Phys. Rev. Lett.* **94** 230503
- [8] Lo H-K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
- [9] Gisin N, Fasel S, Kraus B, Zbinden H and Ribordy G 2006 *Phys. Rev. A* **73** 022320
- [10] Takesue H, Nam S W, Zhang Q, Hadfield R H, Honjo T, Tamaki K and Yamamoto Y 2007 *Nat. Photonics* **1** 343
- [11] Stucki D, Barreiro C, Fasel S, Gautier J-D, Gay O, Gisin N, Thoma Y, Trinkler P, Vannel F and Zbinden H 2009 High speed coherent one-way quantum key distribution prototype *New J. Phys.* at press (arXiv:0809.5264)
- [12] Schmitt-Manderbach T *et al* 2007 *Phys. Rev. Lett.* **98** 010504
- [13] Briegel H J, Dür W, Cirac J I and Zoller P 1998 *Phys. Rev. Lett.* **81** 5932
- [14] Childress L, Taylor J M, Sørensen A S and Lukin M D 2006 *Phys. Rev. Lett.* **96** 070504
- [15] van Loock P, Ladd T D, Sanaka K, Yamaguchi F, Nemoto K, Munro W J and Yamamoto Y 2006 *Phys. Rev. Lett.* **96** 240501
- [16] Jacobs B C, Pittman T B and Franson J D 2002 *Phys. Rev. A* **66** 052307
- [17] Sherson J F, Krauter H, Olsson R K, Julsgaard B, Hammerer K, Cirac J I and Polzik E S 2006 *Nature* **443** 557
- [18] Yuan Z S, Chen Y A, Zhao B, Chen S, Schmiedmayer J and Pan J-W 2008 *Nature* **454** 1098
- [19] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing, Bangalore* (New York: IEEE) pp 175–9
- [20] Marcikic I, de Riedmatten H, Tittel W, Scarani V, Zbinden H and Gisin N 2002 *Phys. Rev. A* **66** 062308
- [21] Wootters W K and Fields B D 1989 *Ann. Phys.* **191** 363
- [22] Lim Y L and Beige A 2005 *Phys. Rev. A* **71** 062311
- [23] Bechmann-Pasquinucci H and Peres A 2000 *Phys. Rev. Lett.* **85** 3313
- [24] Bechmann-Pasquinucci H and Tittel W 2000 *Phys. Rev. A* **61** 062308
- [25] Cerf N J, Bourennane M, Karlsson A and Gisin N 2002 *Phys. Rev. Lett.* **88** 127902
- [26] Bourennane M, Karlsson A, Björk G, Gisin N and Cerf N F 2002 *J. Phys. A: Math. Gen.* **35** 10065
- [27] Bruß D and Macchiavello C 2002 *Phys. Rev. Lett.* **88** 127901
- [28] Sych D, Grishanin B and Zadkov V 2004 *Laser Phys.* **14** 1314
- [29] Walborn S P, Lemelle D S, Tasca D S and Souto Ribeiro P H 2008 *Phys. Rev. A* **77** 062323
- [30] Scarani V, Acin A, Ribordy G and Gisin N 2004 *Phys. Rev. Lett.* **92** 057901

- [31] Acin A, Gisin N and Masanes L 2006 *Phys. Rev. Lett.* **97** 120405
- [32] Scarani V, Gisin N, Brunner N, Masanes L, Pino S and Acin A 2006 *Phys. Rev. A* **74** 042339
- [33] Magniez F, Mayers D, Mosca M and Ollivier H 2005 Self-testing of quantum circuits arXiv:quant-ph/0512111 (appendix A)
- [34] Acin A, Brunner N, Gisin N, Massar S, Pironio S and Scarani V 2007 *Phys. Rev. Lett.* **98** 230501
- [35] Beige A, Englert B-G, Kurtsiefer C and Weinfurter H 2002 *J. Phys. A: Math. Gen.* **35** L407
- [36] Beige A, Englert B-G, Kurtsiefer C and Weinfurter H 2002 *Acta Phys. Pol. A* **101** 357
- [37] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121
- [38] Reck M, Zeilinger A, Bernstein H J and Bertani P 1994 *Phys. Rev. Lett.* **73** 58
- [39] Zukowski M, Zeilinger A and Horne M A 1997 *Phys. Rev. A* **55** 2564
- [40] Pryde G J and White A G 2003 *Phys. Rev. A* **68** 052315