New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG | IOP Institute of Physics

Device-dependent and device-independent quantum key distribution without a shared reference frame

Joshua A Slater[1], **Cyril Branciard**[2], **Nicolas Brunner**[3,4] **and Wolfgang Tittel**[1]

[1] Institute for Quantum Science and Technology and Department of Physics and Astronomy, University of Calgary, Calgary, T2N 1N4, Canada
[2] Centre for Engineered Quantum Systems and School of Mathematics and Physics, The University of Queensland, St Lucia, QLD 4072, Australia
[3] Département de Physique Théorique, Université de Genève, 1211 Genève, Switzerland
[4] HH Wills Physics Laboratory, University of Bristol, Bristol BS8 1TL, UK
E-mail: wtittel@ucalgary.ca

Received 2 December 2013, revised 30 January 2014
Accepted for publication 21 February 2014
Published 3 April 2014

New Journal of Physics **16** (2014) 043002
doi:10.1088/1367-2630/16/4/043002

Abstract

Standard quantum key distribution (QKD) protocols typically assume that the distant parties share a common reference frame. In practice, however, establishing and maintaining a good alignment between distant observers is rarely a trivial issue, which may significantly restrain the implementation of long-distance quantum communication protocols. Here we propose simple QKD protocols that do not require the parties to share any reference frame, and study their security and feasibility in both the usual device-dependent (DD) case—in which the two parties use well characterized measurement devices—as well as in the device-independent (DI) case—in which the measurement devices can be untrusted, and the security relies on the violation of a Bell inequality. To illustrate the practical relevance of these ideas, we present a proof-of-principle demonstration of our protocols using polarization entangled photons distributed over a coiled 10-km long optical fiber. We consider two situations, in which either the fiber spool's polarization transformation freely drifts, or randomly chosen polarization transformations are applied. The correlations obtained from measurements allow, with high probability, to generate positive asymptotic secret key rates in both the DD and DI scenarios (under the fair-sampling assumption for the latter case).

Keywords: quantum communication, quantum cryptography, quantum implementations, satellite communication

1. Introduction

Quantum key distribution (QKD) [1] is arguably the most developed area in quantum information processing, and has recently reached the commercial level. Currently the main limitation of QKD is the distance between the parties. State of the art experiments have reported key exchanges up to distances of ~250 km [2]. It is a great challenge in this area to reach much longer distances, such as intercontinental distances, and tremendous effort is made in this direction. Significant progress has been recently reported, with promising developments in quantum repeaters [3], as well as in satellite-based quantum communications [4, 5].

The main reason for this challenge to practical implementations of QKD protocols, and more generally all long-distance quantum communication tasks, is the effect of noise and loss. Many studies have been devoted to these problems. There is however another key issue, often overseen, which is the alignment of a common reference frame between the parties. While usually being assumed *a priori* (hence not discussed) in theoretical works, the alignment of a common reference frame is rarely a trivial task in practice. Furthermore, when performing experiments outside of the laboratory, this issue can become highly cumbersome, and may significantly restrain—and even hinder—the implementation of certain quantum protocols. For instance, in fiber-based quantum communications, polarization rotations are induced by unavoidable temperature changes, which makes it challenging to maintain a good alignment for polarization qubits. In the case of phase-encoding, interferometer phases at distant locations must remain locked [6], which, while only depending on local environments and not the channel, is also a challenge over long distances. Also, in satellite-based quantum communications, establishing and maintaining a good alignment between the satellite and the ground station is a challenge [5], given the fast movement of the satellite and the limited amount of time for completing the protocol.

It is therefore relevant to consider quantum communication protocols in which the requirement of a common reference frame can be dispensed with. An elegant solution to this problem is to use decoherence-free subspaces [7, 8]. However, this generally amounts to using high-dimensional quantum systems, the practical implementation of which is challenging—although progress has been achieved recently [9]. It turns out however that one can in fact relax the shared reference frame assumption in certain simple quantum communication protocols that only involve qubits. This approach has received some attention in the context of tests of quantum non-locality [10]: in particular it was recently shown [11, 12], and experimentally illustrated [11, 13], that Bell inequality violations can be guaranteed even if the parties share no common measurement basis. In the context of QKD, Laing and colleagues [14] presented a protocol—dubbed 'reference frame independent', and recently implemented in [15]—which requires the parties to only have one common measurement basis. While the latter approach is well suited and proposes an interesting solution for certain QKD implementations, it is however not adapted to all systems.

Here we propose QKD protocols that do not assume the existence of any shared reference frame. Our protocols can be adapted to any qubit implementation of QKD. We analyze their security and feasibility in two scenarios. In the first, 'device-independent' (DI) case [16, 17], the two communicating parties Alice and Bob use untrusted measurement devices and do not make any assumption on their functioning; the security of the protocol is ensured by the violation of a Bell inequality (for a recent review, see [18]). In the second, standard 'device-dependent' (DD) case, Alice and Bob trust that their devices faithfully implement the prescribed measurements—which further constrains the possible attacks by an eavesdropper, Eve, detectable by Alice and Bob. We show in both cases that if Alice and Bob do not share a common reference frame but measure entangled pairs of quantum systems along randomly orientated measurement bases, they can still expect to generate, with reasonably large probability (which depends on the assumptions for the security analysis), secret keys with positive key rates. We then demonstrate the experimental relevance of these ideas by presenting a proof-of-principle implementation of our protocols using a photonic QKD setup with polarization entangled photons. For all cases under consideration, we could calculate, with non-zero probability, positive (asymptotic) secret key rates as obtained from the preceding security analysis (assuming the fair sampling assumption in the DI case to calculate the violation of a Bell inequality). This suggests that the requirement of a common reference frame can indeed—if need be—be completely dispensed with in experimental QKD, thus opening promising perspectives for long-distance and satellite-based QKD.

2. Device independent protocol

In our first protocol, Alice and Bob can each perform one out of three possible local measurements, labeled by $x = 1, 2, 3$ for Alice and $y = 1, 2, 3$ for Bob, on a shared entangled quantum state ρ_{AB}. All measurements are dichotomic, giving a binary outcome a for Alice and b for Bob. The protocol is device independent in the sense that we shall not make any assumption on which measurements are physically implemented by Alice and Bob's measuring apparatuses, nor of the dimension of the state ρ_{AB}.

After repeating the above operations sufficiently many times, Alice and Bob can, by communicating a random subset of their measurement choices and results, estimate the correlations they share, i.e. the probability distribution $P(a, b|x, y)$. For now we will focus on the *correlators* $E_{xy} = P(a = b|x, y) - P(a \neq b|x, y)$. From these, Alice and Bob can in particular calculate the 36 values (for all x, x', y and y') of the Clauser–Horne–Shimony–Holt (CHSH) [19] parameters

$$S_{xx'yy'} = \left|E_{xy} + E_{xy'} + E_{x'y} - E_{x'y'}\right|. \tag{1}$$

If any of these CHSH values is greater than 2, Alice and Bob can certify that the observed correlations are 'non-local', in the sense that they violate Bell's local causality assumption [20]. Observing quantum non-locality is not only interesting for testing the foundations of quantum theory, it can also have practical applications—in our case of interest it can indeed allow one, for a large enough value of a CHSH parameter together with a large enough value for at least one correlator, to prove the security of QKD protocols in a DI way [16, 17, 21, 22, 25].

Interestingly, it was shown in [11, 12] that if Alice and Bob share a maximally entangled two-qubit state, say the singlet state $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$, and can each choose among three orthogonal measurements, represented for Alice (Bob) by three orthogonal vectors $\vec{a}_x$ $\left(\vec{b}_y\right)$ on the Bloch sphere, there is always at least one of the 36 CHSH values $\mathcal{S}_{xx'yy'}$ that is above the local bound of 2—unless Alice and Bob's orthogonal measurement triads are perfectly aligned. Moreover, if Alice and Bob do not share any common reference frame and the relative orientation of their measurement triads is random, the largest CHSH value they observe is typically quite large: its average value was empirically found to be ~2.6 for random relative orientations drawn from a uniform distribution on the Bloch sphere [11].

This suggests that it should be possible to extract reasonably large secret key rates from the correlations obtained by Alice and Bob, without the requirement that they share a common reference frame (i.e. their orthogonal measurement triads are not pre-aligned). We study this idea below, following the security analyses of both Pironio *et al* [21]—which proves the security against *collective attacks*—and of Masanes *et al* [22]—which considers the security against *general (coherent) attacks*, only assuming *memoryless devices*. Note that full security proofs of DI-QKD, considering the most general attacks, were recently reported [23, 24]. However, these proofs are not robust to noise, hence of limited practical interest, and we do not consider these in this work.

2.1. Device independent security analysis along the lines of Pironio et al [21]

Reference [21] considered a DI-QKD protocol with three inputs for Alice (in our notations, $x = 1, 2, 3$) and two inputs for Bob ($y = 1, 2$). Considering the CHSH parameter $\mathcal{S}_{1212}$ and the correlator E_{31} (see equation (1) above), it was shown that (if $\mathcal{S}_{1212} > 2$) a secret key can be extracted through one-way classical post-processing (from Bob to Alice) from the data obtained when using the settings $x = 3$ and $y = 1$—the 'raw key'—at an asymptotic rate (see details in [21])

$$R \geqslant 1 - h\left[\frac{1 - E_{31}}{2}\right] - h\left[\frac{1 + \sqrt{(\mathcal{S}_{1212}/2)^2 - 1}}{2}\right], \tag{2}$$

where $h(p) = -p\log_2 p - (1 - p)\log_2(1 - p)$ is the binary entropy function. This bound on the secret key-rate ensures the security of the QKD protocol in the DI scenario against *collective attacks* [1], in the limit of infinite key lengths. The term $h\left[\frac{1 - E_{31}}{2}\right]$ represents the (minimum) amount of information that Alice and Bob need to classically exchange in order to correct the errors in their raw keys, while the term $h\left[\frac{1 + \sqrt{(\mathcal{S}_{1212}/2)^2 - 1}}{2}\right]$ is a bound on Eve's Holevo information conditioned on Bob's measurement result. Both need to be reduced through privacy amplification.

The same protocol as in [21] can be run by following the protocol detailed above, in which Alice and Bob do not share a common reference frame (see start of section 2), with three settings for both Alice and Bob, by using any four correlators $E_{x^{(\prime)}y^{(\prime)}}$ to estimate a CHSH parameter $\mathcal{S}_{xx'yy'}$, and any pair of settings $(x_{\text{raw}}, y_{\text{raw}})$ to define the raw key—with the important condition that either $x_{\text{raw}} \in \{x, x'\}$ or $y_{\text{raw}} \in \{y, y'\}$. Let us then define

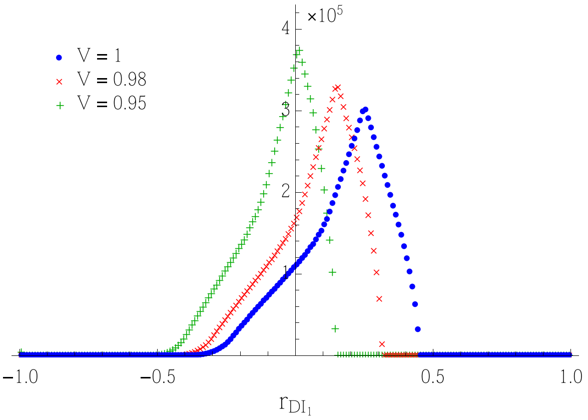

Figure 1. Estimated distribution of the bound r_{DI_1} (3) on the secret key rate (in the DI scenario, following the analysis of [21]—i.e. ensuring security against collective attacks), obtained by generating 10^7 random pairs of orthogonal measurement triads uniformly distributed on the Bloch sphere, to be measured on Werner states of visibilities $V = 1$, 0.98 and 0.95. For each value of V, each data point corresponds to the number of samples (out of 10^7) giving a value r_{DI_1} within an interval of sive $\delta r = 0.01$.

$$r_{DI_1} = \max_{\substack{x,x',y,y',x_{\text{raw}},y_{\text{raw}},\\ \text{s.t.}\,\mathcal{S}_{xx'yy'}>2,\\ x_{\text{raw}}\in\{x,x'\}\,\text{or}\,\,y_{\text{raw}}\in\{y,y'\}}} \left[1 - h\left[\frac{1-E_{x_{\text{raw}}y_{\text{raw}}}}{2}\right] - h\left[\frac{1+\sqrt{(\mathcal{S}_{xx'yy'}/2)^2-1}}{2}\right]\right], \quad (3)$$

corresponding to the rate (2) for the optimal choice of settings used to define the CHSH parameter and the raw key (by convention, if no violation $\mathcal{S}_{xx'yy'} > 2$ is found we define $r_{DI_1} = -1$. From the analysis of [21], if r_{DI_1} is found to be non-negative, then Alice and Bob will indeed be able to extract a secret key with an asymptotic rate of (at least) r_{DI_1}, in the DI scenario, secure against collective attacks[5].

In order to study the experimental feasibility of such a protocol the questions we need to address are the following: How likely is r_{DI_1} to be positive? What are its typical values, and how are they distributed if Alice and Bob's orthogonal measurement triads are randomly chosen?

To answer these questions, we estimated the distribution of r_{DI_1} by generating 10^7 pairs of random orthogonal measurement triads $\{\vec{a}_x\}$ and $\{\vec{b}_y\}$, independently drawn from a uniform distribution on the Bloch sphere. For each pair of triads, we computed the nine correlators E_{xy} assuming that Alice and Bob receives pure (noise-free) maximally entangled states $\rho_{AB} = |\Psi^-\rangle\langle\Psi^-|$ (hence, $E_{xy} = -\vec{a}_x \cdot \vec{b}_y$), and calculated the bound r_{DI_1} (3) on the secret key rate that Alice and Bob can extract. The results of our simulation are plotted on figure 1. We found that ~83.9% of our samples of r_{DI_1} were positive (i.e. we estimate the probability for Alice

[5] Note that instead of throwing some raw data away, Alice and Bob could additionally try to extract some secret key from their measurement results obtained by using other settings than the optimal $(x_{\text{raw}}, y_{\text{raw}})$, if any other choice also leads to a positive bound on the key rate through (2). For simplicity we do not consider this possibility in this paper, and only focus on r_{DI_1} as defined in (3).

and Bob to obtain $r_{DI_1} > 0$ to be ~83.9%), with a maximum value for the distribution of r_{DI_1} observed around $r_{DI_1} \sim 0.25$. The average value of r_{DI_1} was found to be ~0.173; if we post-select only the cases in which $r_{DI_1} > 0$, the average value becomes ~0.226. The maximum value for r_{DI_1} is found to be ~0.450, obtained if two of Alice and Bob's measurement settings coincide (say, $\vec{a}_{x'} = \vec{b}_{y'}$), while the other two pairs of settings, used to define $\mathcal{S}_{xx'yy'}$, are coplanar (with an angle ~0.642 rad from one pair to the other). We also note that for these numerical calculations we have assumed that each measurement triad is fixed for the duration of the measurement. If the measurement alignment were changing during the measurement the only effect would be decreased correlations and Bell violation, leading to lower secret key rates. However, the distributed key would still be secure.

It is also important to study the effect of noise on the secret key rates r_{DI_1}. For that, we similarly estimated the distribution of r_{DI_1} if the measurements are now performed on noisy singlet states (Werner states [26]) $\rho_{AB}^{V} = V|\Psi^-\rangle\langle\Psi^-| + (1 - V)\mathbb{1}/4$ (which gives $E_{xy} = -V\vec{a}_x \cdot \vec{b}_y$), for $V = 0.98$ and 0.95; see figure 1. As expected, the secret key rates are reduced as V decreases. For $V = 0.98$ and $V = 0.95$, the probabilities that $r_{DI_1} > 0$ are, however, still ~72.1% and ~38.0%, respectively. Note in this respect that the violations of a CHSH inequality were found in [11] to be quite robust to noise; for instance, the probability that at least one value of $\mathcal{S}_{xx'yy'}$ is greater than two is still above 99.9% for $V = 0.95$.

2.2. Device independent security analysis along the lines of Masanes et al [22]

[22] provides a different approach to prove the security of a DI-QKD scheme. For the same protocol as in [21], Masanes *et al* proved that (for $\mathcal{S}_{1212} > 0$) a secret key—now secure against *coherent attacks, but under the assumption that their measurement devices are causally independent* (or *memoryless*)—can be extracted at an asymptotic rate [22]

$$R \geqslant -h\left[\frac{1 - E_{31}}{2}\right] - \log_2\left[\frac{1 + \sqrt{2 - (\mathcal{S}_{1212}/2)^2}}{2}\right]. \tag{4}$$

Again, the term $h\left[\frac{1 - E_{31}}{2}\right]$ is due to the necessary error correction, while the term $\log_2\left[\frac{1 + \sqrt{2 - (\mathcal{S}_{1212}/2)^2}}{2}\right]$ is now a bound on the min-entropy of Alice's raw key conditioned on Eve's information. The information of both must be removed through privacy amplification to extract a secret key.

Let us then now define, for our experimental procedure with three settings for Alice and Bob,

$$r_{DI_2} = \max_{\substack{x,x',y,y',x_{\mathrm{raw}},y_{\mathrm{raw}},\\ \mathrm{s.t.}\,\mathcal{S}_{xx'yy'}>2,\\ x_{\mathrm{raw}}\in\{x,x'\}\,\mathrm{or}\,y_{\mathrm{raw}}\in\{y,y'\}}} \left[-h\left[\frac{1 - E_{x_{\mathrm{raw}}y_{\mathrm{raw}}}}{2}\right] - \log_2\left[\frac{1 + \sqrt{2 - (\mathcal{S}_{xx'yy'}/2)^2}}{2}\right]\right]. \tag{5}$$

As before, if r_{DI_2} is found to be non-negative, then Alice and Bob will indeed be able to extract a secret key with a rate (at least) r_{DI_2}.

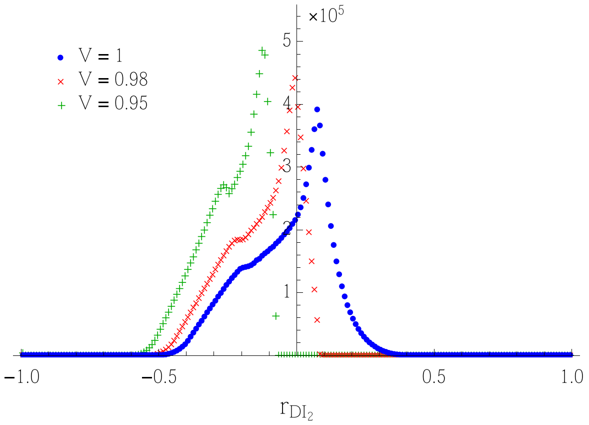

Figure 2. Estimated distribution of the bound r_{DI_2} (5) on the secret key rate for Werner states of visibilities $V = 1$, 0.98 and 0.95 (in the DI scenario, following the analysis of [22]—i.e. showing security against coherent attacks, for memoryless devices), obtained as in figure 1.

Again, we wish to determine how likely it is that r_{DI_2} is positive, and how its typical values and distribution look like when Alice and Bob's orthogonal measurement triads are randomly chosen from a uniform distribution on the Bloch sphere. For that, we estimated the distribution of r_{DI_2} in a similar way as for r_{DI_1}. The results of our simulation are plotted in figure 2. We found that ∼49.0% of our samples of r_{DI_2} were positive, and observed a peak in the distribution of r_{DI_2} for values around ∼0.08. The average value of r_{DI_2} was found to be ~ -0.034; if we post-select only the cases in which $r_{DI_2} > 0$, the average value becomes ∼0.093. The maximum value for r_{DI_2} is obtained if two of Alice and Bob's measurement settings coincide, while the other two pairs of settings, used to define $\mathcal{S}_{xx'yy'}$, are coplanar, at 45° from one another—i.e. they correspond to the optimal choice of settings for testing the CHSH inequality (which was not the case for the optimal settings for r_{DI_1}). In that case, one gets $r_{DI_2} = 1 - h\left(\frac{1-1/\sqrt{2}}{2}\right) \simeq 0.399$.

We also, as before, considered the effect of depolarizing noise on the secret key rates r_{DI_2} (see figure 2). For $V = 0.98$, we found the probability that $r_{DI_2} > 0$ to be ∼18.0%; for $V = 0.95$, however, no positive secret key rate r_{DI_2} is obtained any more.

Note that r_{DI_2} is always smaller than r_{DI_1}. This comes from the different techniques used in the proofs: [22] is based on the calculation of min-entropies to estimate Eve's information, while [21] is based on the calculation of Eve's Holevo information (which involves von Neumann entropies). The security analysis of [22] is more stringent in that it considers more general attacks. It is an open question whether any of the two analyses can be improved to account for more general attacks or to lead to higher bounds on the secret key rates (e.g. whether the higher bound of [21] also holds for the same class of attacks as considered in [22]).

3. Device dependent protocol

We now turn to the more standard device dependent scenario, in which Alice and Bob trust their measurement apparatuses. We assume that the apparatuses implement dichotomic *qubit* measurements, that ρ_{AB} is a two-qubit state, and that the three measurement settings they can each choose from, as before, trustfully correspond to *orthogonal* projective measurements, represented by three orthogonal Bloch vectors $\vec{a}_x$ for Alice, and by three orthogonal Bloch vectors $\vec{b}_y$ for Bob.

It is convenient here to think of Alice's and Bob's measurements along the orthogonal directions $\vec{a}_x$ and $\vec{b}_y$ as the application of an adequate local unitary operation on their respective qubit, followed by a measurement along the axes X, Y, Z of their Bloch spheres[6]. Choosing random orientations for the orthogonal measurement triads $\vec{a}_x$ and $\vec{b}_y$ is equivalent to choosing random local unitary transformations to apply to the two-qubit state ρ_{AB}.

In this view, the QKD protocol we are considering, with a choice of measurement among three orthogonal directions, is nothing but the entanglement-based version of the well-known 6-state protocol [27, 28]. Its standard security analysis can thus directly be applied. The only difference in our case here will concern its typical implementation: we shall not assume that Alice and Bob can (in the ideal case) share an entangled state with any particular symmetries adapted to their measurement bases, but instead, that their qubits undergo some uncontrolled rotations before being measured.

Note already that in the DD scenario, entanglement-based protocols can readily be translated into prepare-and-measure ones [1] (whose practical implementations are typically simpler), and the following analysis would still apply.

3.1. Device dependent security analysis à la 6-state protocol

Following the analysis presented in appendix A of [1], one can show that the asymptotic secret key rate one can extract in the 6-state protocol from the data measured (say) with the settings $x = y = 3$ (corresponding to a σ_z measurement, with the convention that $x, y = 1$ and $x, y = 2$ correspond to σ_x and σ_y measurements, resp.), under one-way classical post-processing, and secure against the most general *coherent attacks* (in the DD scenario) is bounded by

$$R \geqslant 1 - H\left[\left\{\frac{1 + E_{11} + E_{22} - E_{33}}{4}, \frac{1 + E_{11} - E_{22} + E_{33}}{4}, \frac{1 - E_{11} + E_{22} + E_{33}}{4}, \frac{1 - E_{11} - E_{22} - E_{33}}{4}\right\}\right], \tag{6}$$

where $H\left[\{p_i\}\right] = -\sum_i p_i \log_2 p_i$ is the Shannon entropy (and $\{p_i\}$ is a length 4 vector of probabilities).

[6] Alternatively, one can use the orthogonal directions $\vec{a}_x$ and $\vec{b}_y$ to redefine the X, Y, Z axes of Alice and Bob's Bloch spheres, and hence their computational bases, and rewrite ρ_{AB} in these new bases (which indeed amounts to applying local unitaries to ρ_{AB}).

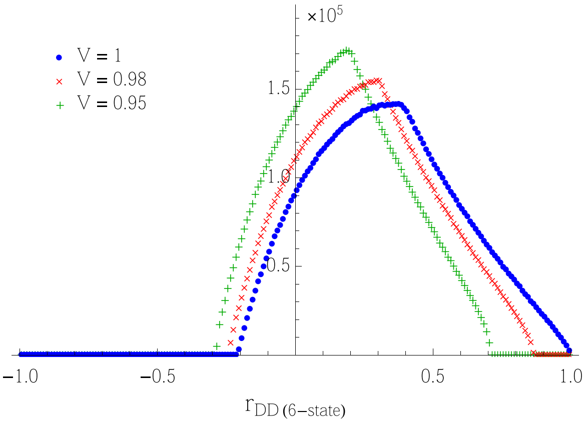

Figure 3. Estimated distribution of the bound $r_{DD\,(6\text{-}state)}$ (7) on the secret key rate for Werner states of visibilities $V = 1$, 0.98 and 0.95 (in the DD scenario, following the analysis '*à la* 6-state protocol'), obtained as in figures 1 and 2.

In our case, the association between each of Alice's three measurement settings and one of Bob's settings is not defined *a priori*, but can be optimized so as to end up with the largest possible secret key rate—that is, we can choose the optimal permutation $\pi(\{1, 2, 3\}) = \{y_1, y_2, y_3\}$ of Bob's settings to be associated to Alice's settings $\{1, 2, 3\}$. Taking into account the fact that equation (6) assumes a given handedness for the orientation of Alice and Bob's settings (that of $\{\vec{x}, \vec{y}, \vec{z}\}$), we define

$$r_{DD\,(6\text{-}state)} = \max_{\substack{\{y_1,y_2,y_3\}\\ =\pi(\{1,2,3\})}} \left[1 - H\left[\left\{ \frac{1 + \sigma_\pi\left(E_{1y_1} + E_{2y_2} - E_{3y_3}\right)}{4}, \frac{1 + \sigma_\pi\left(E_{1y_1} - E_{2y_2} + E_{3y_3}\right)}{4}, \frac{1 + \sigma_\pi\left(-E_{1y_1} + E_{2y_2} + E_{3y_3}\right)}{4}, \frac{1 - \sigma_\pi\left(E_{1y_1} + E_{2y_2} + E_{3y_3}\right)}{4} \right\} \right] \right], \tag{7}$$

where $\sigma_\pi = \pm 1$ is the signature of the permutation π. $r_{DD\,(6\text{-}state)}$ is thus a lower bound on the asymptotic extractable secret key rate of our DD protocol, secure against coherent attacks in the limit of infinitely long keys, obtained from the standard analysis of the 6-state protocol[7].

We again estimated the distribution of the bound $r_{DD\,(6\text{-}state)}$ in a similar manner as before, i.e. if Alice and Bob share (noisy) singlet states and their measurement orientations (or their local unitaries, equivalently—cf above) are chosen at random, uniformly on the Bloch sphere. The results are shown in figure 3. In the noiseless case ($V = 1$) we found that ~89.2% of our

[7] Note that by considering only two of the three settings of both Alice and Bob, one can follow the security analysis for the BB84 protocol [29] (cf e.g. appendix A of [1]), and derive a simpler bound on the asymptotic secret key rate, secure against coherent attacks (and actually proven to give one-sided DI security [30, 31], under the memoryless assumption), given by $r_{DD\,(BB84)} = \max_{x\neq x', y\neq y'}\left[1 - h\left(\frac{1-E_{xy}}{2}\right) - h\left(\frac{1-E_{x'y'}}{2}\right)\right]$. Numerical simulations suggest that this bound is in general only slightly lower than $r_{DD\,(6\text{-}state)}$ (7), and gives comparable distributions to those of figure 3.

samples led to positive secret key rates $r_{DD\,(6\text{-}state)} > 0$. The average value of $r_{DD\,(6\text{-}state)}$ was found to be ∼0.330; if post-selected to the cases in which $r_{DD\,(6\text{-}state)} > 0$, it becomes ∼0.379. The maximum value of $r_{DD\,(6\text{-}state)}$ is 1, obtained e.g. when ρ_{AB} is a pure singlet state and Alice and Bob's measurement axes are perfectly aligned (as in the standard case of the 6-state protocol). For $V = 0.98$ and 0.95, as the key rates decrease, we still found that ∼84.4% and ∼75.6% of our samples, respectively, led to positive secret key rates $r_{DD\,(6\text{-}state)} > 0$.

We note that the key rates obtained from (7), in the DD scenario, are typically larger than those found in the DI scenario considered in the previous section. This was expected, as the assumptions on Eve's possible attacks are more restrictive in the DD scenario. For instance, Eve cannot act on Alice and Bob's measurement apparatuses—which, in the DI scenario, indeed allows her to perform more powerful attacks [21]. An interesting difference between the DD and DI scenarios is the optimal orientations of settings. In the DD scenario, one only aims at maximizing three of the correlators $|E_{xy}|$, and the optimal arrangement does not allow the violation of any Bell inequality; on the other hand, in the DI scenario a trade-off must be found between a large enough violation of a Bell inequality and a large enough correlator $|E_{x_{\text{raw}}y_{\text{raw}}}|$ (cf above). We also note that in real experiments, data acquisition times might be longer than the alignment stability, i.e. the measurement alignment might drift during measurements. In this case, the above security analysis still holds, and the distributed key remain secret. However, Alice and Bob will find decreased correlation, which will lead to decreased secret key rates.

3.2. Improved device dependent security analysis

In the security analysis of the 6-state protocol that leads to the closed form (6), one uses the fact that an upper bound on Eve's information can be obtained, through a 'depolarization process', by restricting oneself to Bell-diagonal states ρ_{AB} (cf appendix A of [1]). While this use of the symmetries of the protocol may be well adapted for standard implementations in which Alice and Bob share a common reference frame and indeed expect their state ρ_{AB} to be (close to) a Bell-diagonal state, the upper bound thus obtained may in general be over-pessimistic, and it may be possible to actually derive larger bounds on the secret key rates—as we now show.

In the experimental situation we consider, Alice and Bob each repeatedly perform one out of three orthogonal qubit measurements. Their full statistics—i.e. their correlators E_{xy}, together with the marginal probabilities $P(a|x)$ and $P(b|y)$ (which are expected to be uniformly 1/2 for maximally entangled two-qubit states, possibly including white noise)—then actually allow them to fully reconstruct the state ρ_{AB}, up to local unitary rotations, through quantum state tomography [32]. This can be used to estimate Eve's information more tightly—e.g., in the ideal case in which the state ρ_{AB} would be found to be a pure state (such as a maximally entangled state), then one can be assured that Eve is not correlated to it.

More precisely, to study the security against *collective attacks*, the information potentially available to an eavesdropper can be represented by a quantum system E that is correlated to Alice and Bob's system in such a way that it 'purifies' the reconstructed state ρ_{AB}—i.e. one can define a purification $\left|\psi_{ABE}\right\rangle$ of ρ_{AB} (a pure 3-partite state such that $\mathrm{Tr}_E\left|\psi_{ABE}\right\rangle\left\langle\psi_{ABE}\right| = \rho_{AB}$), and give the quantum system E to Eve.

Let us denote by $\rho_E = \mathrm{Tr}_{AB}\left|\psi_{ABE}\right\rangle\left\langle\psi_{ABE}\right|$ Eve's partial state and by $\rho_{E|A_x=a}$ her conditional state corresponding to Alice's measurement result $A_x = a$ for the choice of setting x, and let us define Eve's Holevo information conditioned on Alice's outcome as

$$\chi\left(A_x{:}\, E\right) = S\left(\rho_E\right) - \sum_a p\left(A_x = a\right) S\left(\rho_{E|A_x=a}\right), \tag{8}$$

where S denotes the von Neumann entropy $\left[S(\rho) = -\mathrm{Tr}\left(\rho \log_2 \rho\right)\right]$. We similarly define $\chi\left(B_y{:}\, E\right)$ to be Eve's Holevo information conditioned on Bob's measurement result for the choice of setting y. A lower bound on the asymptotic secret key rate one can extract through one-way post-processing from the data $A_{x_{\mathrm{raw}}}$, $B_{y_{\mathrm{raw}}}$ obtained from the measurement of the settings x_{raw} and y_{raw} is then given by the Devetak–Winter bound [33]

$$R \geqslant I\left(A_{x_{\mathrm{raw}}} : B_{y_{\mathrm{raw}}}\right) - \min\left[\chi\left(A_{x_{\mathrm{raw}}} : E\right), \chi\left(B_{y_{\mathrm{raw}}} : E\right)\right], \tag{9}$$

where $I\left(A_{x_{\mathrm{raw}}} : B_{y_{\mathrm{raw}}}\right)$ is the mutual information between Alice's and Bob's measurement results $A_{x_{\mathrm{raw}}}$ and $B_{y_{\mathrm{raw}}}$ which, after randomization of Alice and Bob's marginals (through a simultaneous random flipping of their results), is equal to $I\left(A_{x_{\mathrm{raw}}} : B_{y_{\mathrm{raw}}}\right) = 1 - h\left[\frac{1-E_{x_{\mathrm{raw}}y_{\mathrm{raw}}}}{2}\right]$. The bound (9) ensures the security of the secret key against collective attacks (in the limit of infinitely long keys); using a de Finetti type of argument, one can show that the same secret key rate is also secure against *coherent attacks* [34].

In our case, Alice and Bob still have the possibility to choose the settings from which they will attempt to extract a secret key. Let us accordingly define

$$r_{DD} = \max_{x_{\mathrm{raw}}, y_{\mathrm{raw}}}\left[1 - H\left[\frac{1 - E_{x_{\mathrm{raw}}y_{\mathrm{raw}}}}{2}\right] - \min\left[\chi\left(A_{x_{\mathrm{raw}}} : E\right), \chi\left(B_{y_{\mathrm{raw}}} : E\right)\right]\right], \tag{10}$$

If r_{DD} is found to be non-negative, then Alice and Bob will actually be able to extract a secret key with a rate (at least) r_{DD}—which is larger than the previous bound $r_{DD\,(6\text{-}state)}$ (7).

In the ideal case in which Alice and Bob find that they share noiseless singlet states, the state ρ_{AB} is pure. This implies in particular that Eve's Holevo information is null: $\chi\left(A_{x_{\mathrm{raw}}} : E\right) = \chi\left(B_{y_{\mathrm{raw}}} : E\right) = 0$. The bound r_{DD} (10) on the secret key rate then just depends on the largest correlator (in absolute value) $E_{xy} = -\vec{a}_x \cdot \vec{b}_y$ observed by Alice and Bob. One can show in that case that if Alice's and Bob's three measurements settings are orthogonal, this largest correlator is necessarily greater than $\frac{2}{3}$ (obtained if all scalar products $\vec{a}_x \cdot \vec{b}_y$ are either $\pm\frac{2}{3}$ or $\pm\frac{1}{3}$), and hence $r_{DD} \geqslant 1 - h\left(\frac{1}{6}\right) \simeq 0.350 > 0$; on the other hand, the maximum value 1 of r_{DD} is attained if any two of Alice and Bob's settings are aligned. As in the previous cases, we estimated the distribution of r_{DD} for randomly chosen orientations for Alice and Bob's measurement triads; see figure 4. Its average value was found to be ~0.745.

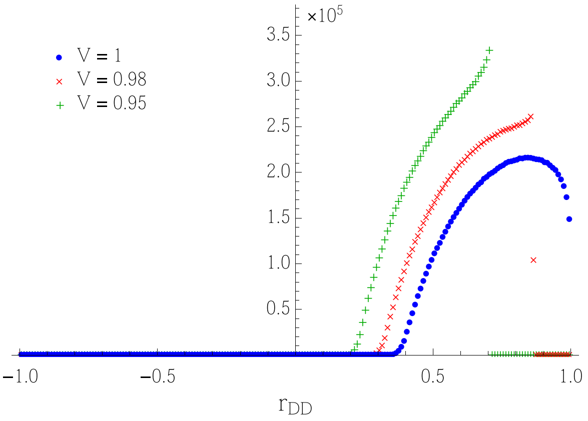

Figure 4. Estimated distribution of the bound r_{DD} (10) on the secret key rate for Werner states of visibilities $V = 1$, 0.98 and 0.95 (in the DD scenario, improving on the standard analysis for the 6-state protocol), obtained as in figures 1–3.

If Alice and Bob determine that they find a noisy Werner state with $V < 1$, they calculate Eve's Holevo information to be (for all x, y) $\chi\left(A_x: E\right) = \chi\left(B_y: E\right) = H\left[\left\{\frac{1+3V}{4}, \frac{1-V}{4}, \frac{1-V}{4}, \frac{1-V}{4}\right\}\right] - h\left[\frac{1-V}{2}\right]$. The distribution of r_{DD}, estimated as before, is also shown on figure 4 for $V = 0.98$ and $V = 0.95$. In both cases we always find positive bounds r_{DD} on the secret key rates (in fact, r_{DD} is always positive for $V \gtrsim 0.875$).

Also, as discussed above, if measurement alignment were to change or drift during actual experiments the only affect would be that Alice and Bob would find a density matrix closer to completely mixed (i.e. the recovered density matrix would be an average over all observed transformations). The result would be for them to overestimate Eve's information and perform more than the necessary privacy amplification, leading to lower secret key rates. Nevertheless, the protocol remains secure. Finally, as Alice and Bob are performing quantum state tomography, they can estimate the transformation in the channel. This means that they could attempt a correction with each iteration of the protocol to increase key rates. Of course, if the transformation is not stable during an iteration of the protocol, they will never be able to perfectly correct it. Also, in practice, there is likely a trade-off between the time spent on alignment and time spent generating key that leads to optimal secret-key generation rates.

4. Proof-of-principle experiments

To demonstrate the practical relevance of our theoretical discussions, we performed a proof-of-principle demonstration of QKD using the four security analyses discussed above. In our experiment Alice generated a sequence of pairs of polarization entangled photons and sent one photon of each pair to Bob via a channel with an unknown polarization transformation. Both parties projectively measured the polarization state of their photon in one of three mutually unbiased bases. Neither Alice nor Bob attempted to align their measurement devices, as we do not want to assume that they share a common reference frame. After collecting sufficient data on each pair of projectors—giving the nine correlators E_{ij} as described above and allowing for the tomography of the quantum state shared by Alice and Bob (for the calculation of r_{DD})—

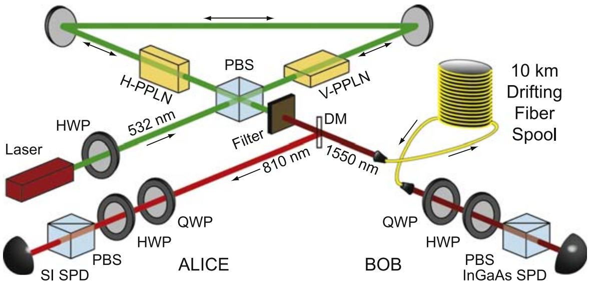

Figure 5. Experimental setup. A horizontally polarized, pulsed (50 ps), 532 nm wavelength laser beam is rotated to diagonal polarization via a half wave-plate (HWP), is then split by a polarizing beam splitter (PBS) and travels both clockwise and counter-clockwise through a polarization Sagnac interferometer. The interferometer contains two type-0, spontaneous parametric down-conversion (SPDC), periodically-poled lithium niobate (PPLN) crystals configured to produce collinear, non-degenerate, 810/1550 nm wavelength photon pairs. The clockwise-travelling, vertically polarized (counter-clockwise travelling, horizontally polarized) pump light passes through the first crystal without interaction (as SPDC is polarization dependent) and may down-convert in the V-PPLN crystal (H-PPLN) to produce two vertically (horizontally) polarized photons. After exiting the interferometer, the remaining pump light is filtered out using a high-pass filter and the entangled photons are separated on a dichroic mirror (DM) and sent to qubit analyzers consisting of waveplates, a PBS and single-photon detectors.

asymptotic secret key rates from each of the above analyses were calculated. Note that our demonstration is proof-of-principle only as we do not randomly select bases nor perform the required error correction or privacy amplification, which is required to generate actual secret keys (and which would require a rigorous finite-key analysis, which would go beyond the scope of this paper). Nor do we close the detection loophole as necessary to generate key for DI-QKD.

4.1. Experimental setup

Figure 5 shows a schematic of our experiments. Alice holds a source of polarization-entangled qubits and a qubit analyzer (details below). Her entanglement source is based on two spontaneous parametric downconversion (SPDC) crystals in a polarizing Sagnac interferometer, described and characterized previously in [35, 36]. Diagonally polarized pump light from a pulsed 532 nm wavelength laser is placed in a superposition of traveling clockwise (CW) and counter-clockwise (CCW) around the Sagnac interferometer. In the CCW path, vertically polarized pump light passes unaffected through the first SPDC crystal, which is oriented to down-convert horizontally polarized pump light, and then produces pairs of vertically polarized photons in the second SPDC crystal. Similarly, the CW path produces pairs of horizontally polarized photons. Each pair consists of one photon at around 810 nm wavelength and one photon at around 1550 nm. By recombining the two paths at the output of the interferometer, and keeping pump powers sufficiently low, Alice generates a two-qubit state close to the $|\Phi^{+}\rangle$ Bell state[8]. Performing quantum state tomography based on a maximum likelihood optimization [32] with the source revealed an average tangle of $\mathcal{T} = 0.85 \pm 0.02$ (note that $\mathcal{T} = 1$ implies a

[8] Note that all maximally entangled two-qubit states (such as $|\Phi^{+}\rangle$) are equivalent, up to a local unitary transformation, to the singlet state $|\Psi^{-}\rangle$ considered in the previous sections.

maximally entangled state and that we observed the tangle to oscillate between 0.82 and 0.88 over the course of the experiment); this value of the tangle corresponds, for an ideal Werner state, to an average visibility of about $V = 0.95 \pm 0.01$. Note that the coherence time of the photon pairs, compared to the duration/coherence time of the pump, is sufficiently short to ensure that multi-photon pair emissions are produced in uncorrelated product states, meaning that photon-number attacks are not a significant concern in our experiments.

During experiments, Alice separates the two entangled photons with a dichroic mirror and measures the 810 nm photon directly with her qubit analyzer, which consists of waveplates, a polarizing beam splitter (PBS) and a free-running silicon avalanche photo-diode (APD). Alice also sends the 1550 nm photon to Bob via a 10 km fiber spool with approx. 6 dB loss, which serves as the quantum channel with unknown and varying polarization transformation, and, in parallel, generates an electronic signal to inform Bob of the incoming photon. Bob then projectively measures the photon with his own qubit analyzer, also consisting of waveplates, a PBS and a gated InGaAs APD. Measurement results from both Alice and Bob are recorded on the same PC for analysis.

4.2. Experimental results

To demonstrate the feasibility of QKD without a shared reference frame with our setup, we performed two experiments. In both experiments Alice and Bob collected statistics on one of the nine correlators for 2 min and then either Alice or Bob would change measurement settings[9]. Hence, 18 min were required to collect statistics on all nine correlators. Note that the polarization transformation of the fiber link drifted noticeably during this time, but, as discussed earlier, this has no affect on the security of the distributed key. In the first experiment, Alice and Bob cycled through the measurement settings for nearly three hours while the polarization transformation of the fiber spool was allowed to freely drift, which generated nine complete iterations through the measurements of the correlators. For our second experiment, we inserted three waveplates into the channel connecting Alice and Bob to randomly vary the polarization transformation and measured the nine correlators for each transformation.

In the first (free-drifting) experiment we analyzed the nearly three hours of data with a sliding 18 min window: We first analyzed the nine correlators and performed state tomography with the data within a window beginning at time $t = 0$ and going to $t = 18$ min. We then repeatedly stepped the window forward by 2 min, yielding a total of 73 sets of data (e.g. the second data set is between $t = 2$ min and $t = 20$ min, etc), and analyzed each set independently. For each data set we calculated the asymptotic secret key rates r_{DI_1}, r_{DI_2}, $r_{DD\,(6\text{-}state)}$ and r_{DD} one could extract in each of the four scenarios, according to equations (3), (5), (7) and (10), respectively. In order to illustrate the role of the CHSH violation in the DI scenario and the importance of having large correlators, we also calculated the maximal CHSH value[10]

[9] In fact, as Alice and Bob each have one detector, each 2 min correlator measurement is composed of four 30 s projection measurements that are used to later calculate the correlator. This makes the observation of double clicks and their appropriate treatment during post-processing [1] impossible.

[10] Note that we do not claim that this maximal $\mathcal{S}_{\max}$ value is necessarily the one that grants the maximum secret key rate (as the latter also depends on the correlator $E_{x_{\rm raw}y_{\rm raw}}$; cf equations (3) and (5)). However, as having a large value of $\mathcal{S}_{\max}$ (>2) is a necessary condition for positive DI secret key rates, we will use the $\mathcal{S}_{\max}$ value as an indicator of the ability to generate key in the DI scenario.

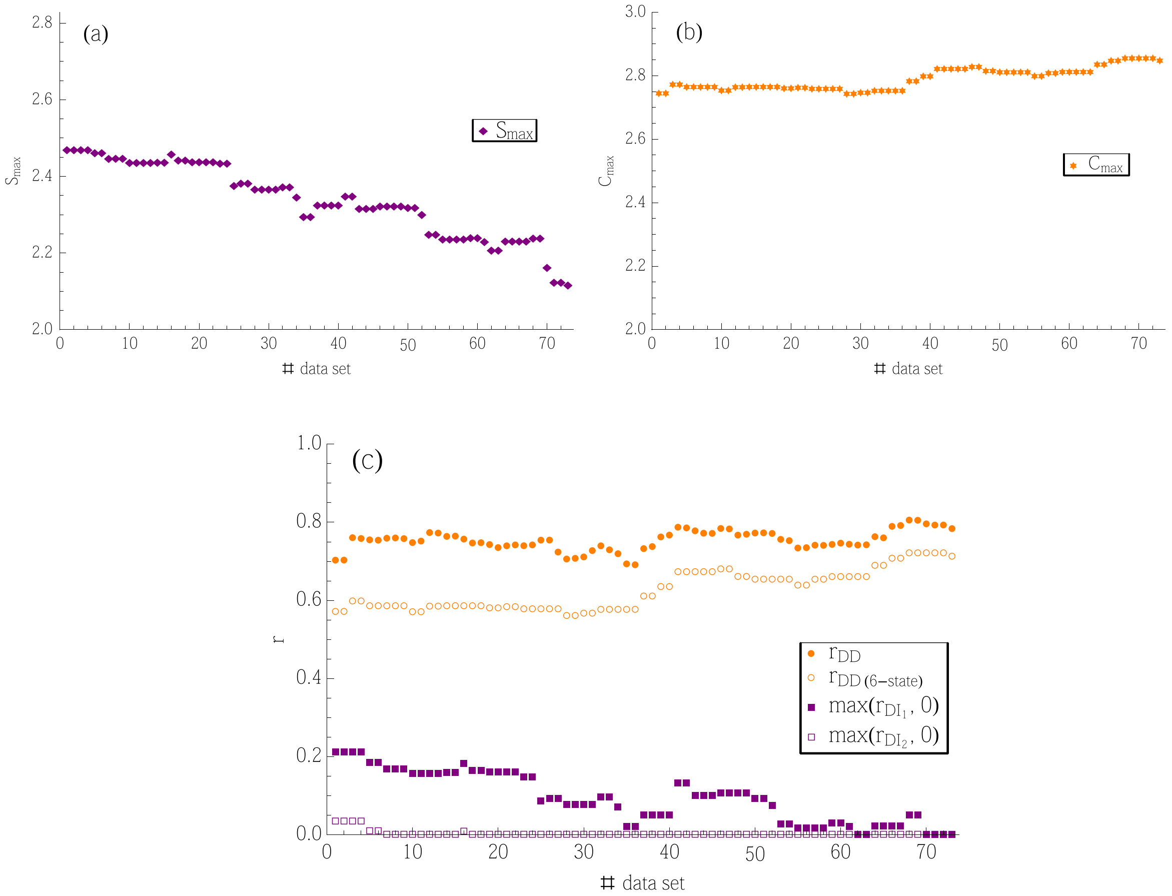

Figure 6. Results from our free-drifting experiment, as a function of time (for each of our 72 data sets; see main text). (a)–(b) Our figures of merit: the maximal CHSH value $\mathcal{S}_{\max}$ and the maximal sum of correlators $C_{\max}$, as defined in the main text. (c) Asymptotic secret key rates r_{DI_1}, r_{DI_2}, $r_{DD\,(6\text{-}state)}$ and r_{DD} corresponding to each of the four scenarios studied in sections 2 and 3.

$\mathcal{S}_{\max} = \max_{x,x',y,y'} \mathcal{S}_{xx'yy'}$, and the largest sum of three correlators defined as $C_{\max} = \max_{x \neq x' \neq x'', y \neq y' \neq y''} \left|E_{xy}\right| + \left|E_{x'y'}\right| + \left|E_{x''y''}\right|$.

These results are presented in figure 6. Initially, and by chance, the channel transformation turned out to be such that a reasonably high parameter $\mathcal{S}_{\max}$ was found, favoring DI-QKD, but over the course of the experiment, the channel transformation slowly drifted close to a point where Alice's and Bob's measurement bases were aligned. At this point we observed three high correlators (i.e. a large value for $C_{\max}$) and a low parameter $\mathcal{S}_{\max}$, which favours DD-QKD. Indeed, when one examines the key rates as a function of time (i.e. window position) one observes steadily decreasing DI key rates (in fact, r_{DI_2} quickly falls to zero, whereas r_{DI_1} remains positive for longer) and steadily increasing DD key rates.

These observations align with our discussion at the end of section 3.1 in that the alignment of bases optimal for DD- and DI-QKD are different. All our protocols require a source with a high degree of entanglement (characterized, for instance, by a high visibility or high tangle).

However, DD-QKD is optimal when Alice's and Bob's measurement bases are well aligned such that one finds three large-valued correlators with which to generate key, which minimizes key reduction due to error correction. On the other hand, in DI-QKD one requires a set of four correlators that generate a high S-parameter (to minimize the bound on Eve's information and thus key reduction during privacy amplification) with one correlator $E_{x_{\mathrm{raw}}y_{\mathrm{raw}}}$ being large so that error correction is minimal, which are conflicting requirements. This conflicting nature is indeed illustrated in figure 6, where one observes that $\mathcal{S}_{\max}$ decreases in time while C increases—just as r_{DI_1} and r_{DI_2} decrease as $r_{DD\,(6\text{-}state)}$ and r_{DD} increase.

Furthermore, the difference between secret key rates granted by the two DD analyses, $r_{DD\,(6\text{-}state)}$ and r_{DD}, are apparent in figure 6(c). The difference between these techniques, as discussed in section 3.2, is how one bounds an eavesdropper's information: r_{DD} uses the Holevo information based on a reconstruction of the density matrix ρ_{AB} while $r_{DD\,(6\text{-}state)}$ uses three correlators. If the quantum state that Alice and Bob share contains a high tangle, then Eve's Holevo information will be low and thus r_{DD} mainly depends on the strength of the correlator used to generate key. On the other hand, the privacy bound for $r_{DD\,(6\text{-}state)}$ does depend on alignment as three high correlators are needed for key generation. We see that in our results: first, r_{DD} always outperforms $r_{DD\,(6\text{-}state)}$ (as mentioned in section 3.2) and, second, the difference between the two key rates is largest initially (when bases are the most misaligned) and slowly decreases as Alice's and Bob's bases begin to align.

As mentioned above, for our second experiment, we inserted three waveplates into the channel connecting Alice and Bob to randomly vary the polarization transformation. All nine correlators were measured 17 times, and state tomography was performed independently each time. Before each iteration the waveplates were re-positioned based on randomly generated numbers, thus generating a random channel transformation (note that the fiber's own transformation continued to drift as above). In figure 7 we present the results. We again plot the figures of merit $\mathcal{S}_{\max}$ and $C_{\max}$ for each of the 17 measurements, as well as the derived asymptotic secret key rates r_{DI_1}, r_{DI_2}, $r_{DD\,(6\text{-}state)}$ and r_{DD}. For DI-QKD, we found positive secret key rates for r_{DI_1} in ten out of 17 measurements (i.e. with probability of 59%) and one out of 17 measurements (i.e. 6%) for r_{DI_2}. For DD-QKD, we found positive secret key rates for r_{DD} in 17 of 17 measurements (i.e. 100%) and in 15 of 17 measurements (i.e. 88%) for $r_{DD\,(6\text{-}state)}$. Although the size of our experimental sample is too small to really be statistically significant, our observations appear to agree reasonably well with the predictions from the numerical simulations above, assuming a source of entangled Werner states of visibility V slightly larger than 0.95, i.e. a tangle of $\simeq$0.856—in agreement with the measured tangle of the state, which was found to oscillate from 0.82 to 0.88.

Lastly, we again point out that a consistently high tangle, which our experiment maintained (up to the oscillations), is required but not sufficient to generate positive secret key rates. A high-quality source does not guarantee the high S-parameter needed for DI-QKD, nor the high correlators needed for DD-QKD. An appropriate channel transformation is also required.

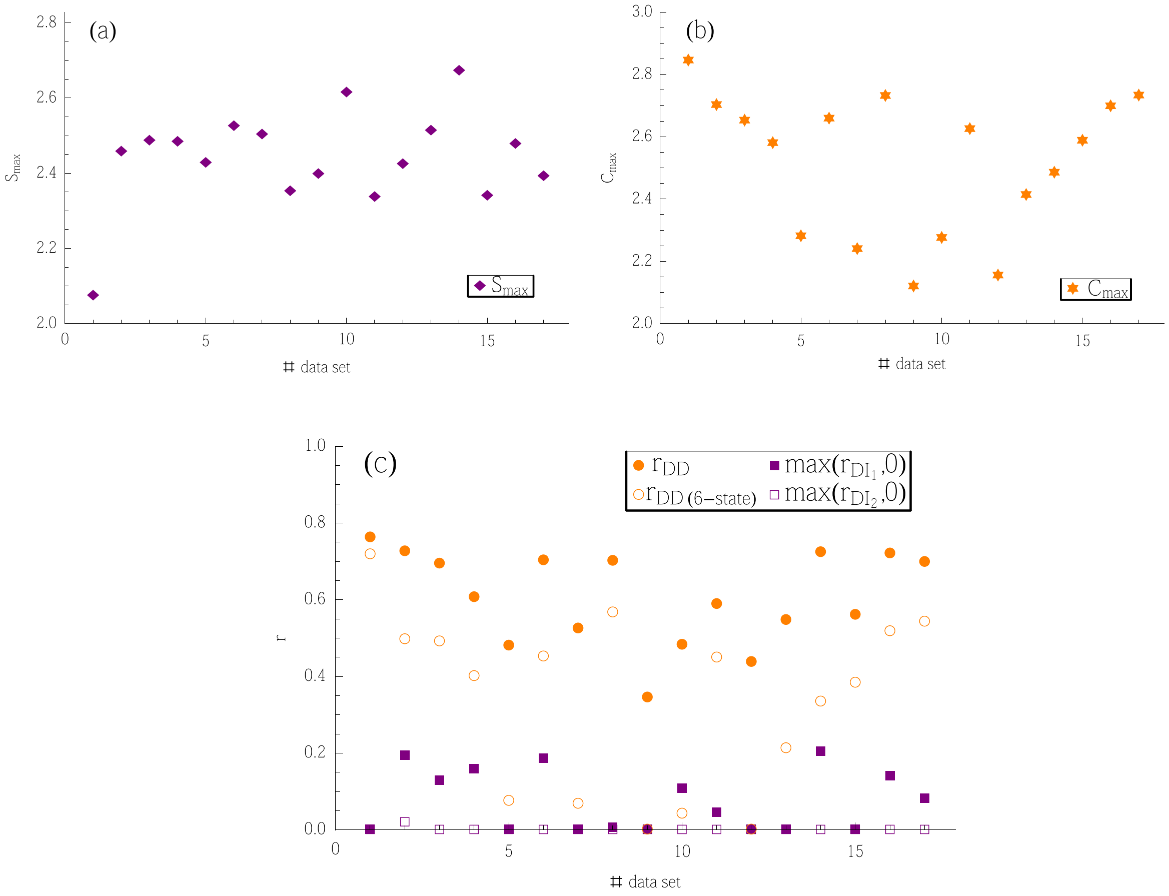

Figure 7. Results from our randomized polarization transformation experiment, for each of our 17 experimental runs (see main text). (a)–(c) as in figure 6.

5. Discussion

We have presented a practical QKD setup in which the requirement of a common reference frame can be completely dispensed with. A proof-of-principle demonstration of our protocols, which covers both the usual device dependent case and the device independent case, was performed over 10 km of spooled fiber. Specifically, we have shown that a secret key can in principle be established, considering both a freely drifting spool and randomly chosen transformations, even in the DI case (assuming fair sampling, and infinitely long keys).

We believe that the present ideas have potential to find applications in future long-distance quantum communication protocols, in particular in situations where the amount time available to perform the protocol is severely constrained, e.g. in satellite based quantum communications. The present results should be considered as a proof-of-principle experiment, and several technical improvements are required, such as implementing random choices of measurement settings, and a finite-key security analysis [37]. For the DI approach, an essential step is to close the detection loophole, which has recently been achieved in fully optical systems [38, 39]. Finally, another challenge consists in devising efficient error-correction protocols for high error rates, as our protocols typically lead to higher error rates compared to the standard approach in which the parties share a common reference frame.

Acknowledgments

This work was supported by a UQ Postdoctoral Research Fellowship, the Swiss National Science Foundation (grant PP00P2_138917), the EU project DIQIP, the National Sciences and Engineering Research Council of Canada (NSERC), Alberta Innovates Technology Futures (AITF), the Canadian Foundation for Innovation (CFI), Alberta Advanced Education and Technology (AAET) and by the Killam Trusts.

References

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

[2] Stucki D, Walenta N, Vannel F, Thew R T, Gisin N, Zbinden H, Gray S, Towery C R and Ten S 2009 *New J. Phys.* **11** 075003

[3] Sangouard N, Simon C, de Riedmatten H and Gisin N 2011 *Rev. Mod. Phys.* **83** 33

[4] Jennewein T 2013 *Phys. World* www.iop.org/news/13/mar/page_59601.html

[5] Bourgoin J-P *et al* 2013 *New J. Phys.* **15** 023006

[6] Dixon A R, Yuan Z L, Dynes J F, Sharpe A W and Shields A J 2010 *Appl. Phys. Lett.* **96** 161102

[7] Cabello A 2003 *Phys. Rev. Lett.* **91** 230403

[8] Bartlett S D, Rudolph T and Spekkens R W 2003 *Phys. Rev. Lett.* **91** 027901

[9] D'Ambrosio V, Nagali E, Walborn S P, Aolita L, Slussarenko S, Marrucci L and Sciarrino F 2012 *Nat. Commun.* **3** 961

[10] Liang Y-C, Harrigan N, Bartlett S D and Rudolph T G 2010 *Phys. Rev. Lett.* **104** 050401

[11] Shadbolt P, Vertesi T, Liang Y-C, Branciard C, Brunner N and O'Brien J L 2012 *Sci. Rep.* **2** 470

[12] Wallman J J and Bartlett S D 2012 *Phys. Rev.* A **85** 024101

[13] Palsson M S, Wallman J J, Bennet A J and Pryde G J 2012 *Phys. Rev.* A **86** 032322

[14] Laing A, Scarani V, Rarity J G and O'Brien J L 2010 *Phys. Rev.* A **82** 012304

[15] Wabnig J, Bitauld D, Li H W, Laing A, O'Brien J L and Niskanen A O 2013 *New J. Phys.* **15** 073001

[16] Mayers D and Yao A 1998 *Proc. 39th IEEE Conf. on Foundations of Computer Science* (Los Alamitos, CA: IEEE) p 503

[17] Acín A, Brunner N, Gisin N, Massar S, Pironio S and Scarani V 2007 *Phys. Rev. Lett.* **98** 230501

[18] Brunner N, Cavalcanti D, Pironio S, Scarani V and Wehner S 2013 arXiv:1303.2849

[19] Clauser J F, Horne M A, Shimony A and Holt R A 1969 *Phys. Rev. Lett.* **23** 880–4

[20] Bell J S 2004 *Speakable and Unspeakable in Quantum Mechanics* 2nd edn (Cambridge: Cambridge University Press)

[21] Pironio S, Acín A, Brunner N, Gisin N, Massar S and Scarani V 2009 *New J. Phys.* **11** 045021

[22] Masanes Ll, Pironio S and Acín A 2011 *Nat. Commun.* **2** 238

[23] Reichardt B W, Unger F and Vazirani U 2013 *Nature* **496** 456–60

[24] Vazirani U and Vidick T 2012 arXiv:1210.1810

[25] Hänggi E and Renner R 2010 arXiv:1009.1833

[26] Werner R F 1989 *Phys. Rev.* A **40** 4277–81

[27] Bruß D 1998 *Phys. Rev. Lett.* **81** 3018–21

[28] Bechmann-Pasquinucci H and Gisin N 1999 *Phys. Rev.* A **59** 4238–48

[29] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing (Bangalore, India)* (New York: IEEE) pp 175–9

[30] Tomamichel M and Renner R 2011 *Phys. Rev. Lett.* **106** 110506

[31] Branciard C, Cavalcanti E G, Walborn S P, Scarani V and Wiseman H M 2012 *Phys. Rev.* A **85** 010301(R)

[32] Altepeter J B, Jeffrey E R and Kwiat P J 2005 *Adv. At. Mol. Phy.* **52** 105–59
[33] Devetak I and Winter A 2005 *Proc. R. Soc.* A **461** 207
[34] Renner R 2007 *Nat. Phys.* **3** 645
[35] Stuart T E, Slater J A, Colbeck R, Renner R and Tittel W 2012 *Phys. Rev. Lett.* **109** 020402
[36] Stuart T E, Slater J A, Bussières F and Tittel W 2013 *Phys. Rev.* A **88** 012301
[37] Scarani V and Renner R 2008 *Phys. Rev. Lett.* **100** 200501
[38] Giustina M *et al* 2013 *Nature* **497** 227–30
[39] Christensen B G *et al* 2013 *Phys. Rev. Lett.* **111** 130406