Studying free-space transmission statistics and improving free-space quantum key distribution in the turbulent atmosphere

C Erven\textsuperscript{1,6}, B Heim\textsuperscript{1,2,3,6}, E Meyer-Scott\textsuperscript{1}, J P Bourgoin\textsuperscript{1}, R Laflamme\textsuperscript{1,4}, G Weihs\textsuperscript{1,5} and T Jennewein\textsuperscript{1,6}

\textsuperscript{1} Institute for Quantum Computing, Department of Physics and Astronomy, University of Waterloo, 200 University Avenue West, Waterloo, ON N2L 3G1, Canada
\textsuperscript{2} Max Planck Institute for the Science of Light, Günther-Scharowsky-Strasse 1, Building 24, D-91058 Erlangen, Germany
\textsuperscript{3} Erlangen Graduate School in Advanced Optical Technologies (SAOT), University of Erlangen-Nuremberg, Paul-Gordan-Strasse 6, D-91052 Erlangen, Germany
\textsuperscript{4} Perimeter Institute, 31 Caroline Street North, Waterloo, ON N2L 2Y5, Canada
\textsuperscript{5} Institut für Experimentalphysik, Universität Innsbruck, Technikerstrasse 25, A-6020 Innsbruck, Austria

E-mail: cerven@iqc.ca, bettina.heim@mpl.mpg.de
and thomas.jennewein@uwaterloo.ca

New Journal of Physics 14 (2012) 123018 (17pp)
Received 5 September 2012
Published 11 December 2012
Online at http://www.njp.org/
doi:10.1088/1367-2630/14/12/123018

Abstract. The statistical fluctuations in free-space links in the turbulent atmosphere are important for the distribution of quantum signals. To that end, we first study statistics generated by the turbulent atmosphere in an entanglement-based free-space quantum key distribution (QKD) system. Using the insights gained from this analysis, we study the effect of link fluctuations on the security and key generation rate of decoy state QKD concluding that it has minimal effect in the typical operating regimes. We then investigate the novel idea of using these turbulent fluctuations to our advantage in QKD experiments. We implement a signal-to-noise ratio filter (SNRF) in our QKD system which rejects...
measurements during periods of low transmission efficiency, where the measured quantum bit error rate is temporarily elevated. Using this, we increase the total secret key generated by the system from 78,009 bits to 97,678 bits, representing an increase of 25.2% in the final secure key rate, generated from the same raw signals. Lastly, we present simulations of a QKD exchange with an orbiting low earth orbit satellite and show that an SNRF will be extremely useful in such a situation, allowing many more passes to extract a secret key than would otherwise be possible.

1. Introduction

Quantum key distribution (QKD), one of the first experimentally realizable technologies from the field of quantum information, has by now seen a number of robust implementations both in fibre [1–4] and in free space [5–10]. Indeed, it has already reached the level of maturity so as to be offered as a commercial product from a number of companies [11–14]. While the fastest systems to date are based on fibre transmission media [15], they will remain limited to a transmission distance of about 200 km until reliable quantum repeaters are realized. Even taking into account the expected future advances in fibre, source and detector technology, secure key distribution will still be limited to about 400 km using fibres.

QKD with orbiting satellites has long been proposed as a solution for global key distribution, as evidenced by the growing number of feasibility studies that have been conducted [10, 16–19]. QKD with low earth orbit (LEO) satellites probably represents the most feasible solution since they will have the shortest free-space transmission distance with the lowest losses. However, LEO satellites travel quickly with short orbital periods, limiting the time available to perform QKD during a single pass to the order of 300 s [10, 19]. Thus, it is important to have a thorough understanding of the transmission properties of the free-space channel which the photons will travel through in order to properly evaluate the feasibility of such a system. Also, with such a short time to exchange a key, it is important to extract the most secure key bits from the relatively small number of signals sent and received during a pass.

For these purposes, this paper first examines some recent theoretical works on the transfer of quantum light and entanglement through the turbulent atmosphere; then experimentally determined free-space transmission efficiency curves measured with an entanglement-based free-space QKD system are then analysed; this is followed by a discussion of the implications of...
link fluctuations for decoy state QKD; a method for improving free-space QKD key rates in the turbulent atmosphere through the use of a signal-to-noise ratio filter (SNRF) is then put forward; this is followed by the experimental results of implementing such a filter and their implications for the security of the system.

2. Free-space optical link statistics

The propagation of classical light through a turbulent atmosphere has long been of interest in theoretical investigations, including such diverse phenomena as diffraction, scintillation and the absorption of light by molecules in the atmosphere which produce beam wander and broadening [20–25]. Satellite-based communication has also been investigated in the context of a turbulent atmosphere [24–27]. From these studies it has been shown that the intensity fluctuations due to the turbulent atmosphere can be assumed to be log-normally distributed in the regime of weak fluctuations and strong losses. This has also been confirmed in various experiments (see, e.g., [28]).

Recently, Vasylyev et al [29] and Semenov and Vogel [30, 31] provided a theoretical foundation for studying the influence of fluctuating loss channels on the transmission of quantum and entangled states of light. Like others [28, 32], in [30, 31] they approximate the probability distribution of the (fluctuating) atmospheric transmission coefficient (PDTC) in the case of entanglement distribution according to the log-normal distribution:

$$P(\eta_{atm}) = \frac{1}{\sqrt{2\pi \sigma \eta_{atm}}} \exp \left( -\frac{1}{2} \left( \ln \eta_{atm} + \bar{\theta} \right)^2 \right),$$  

where $\eta_{atm}$ is the atmospheric transmittance, $\bar{\theta} = -\ln \langle \eta_{atm} \rangle$ is the logarithm of the mean atmospheric transmittance and $\sigma$ is the variance of $\theta = -\ln \eta_{atm}$ characterizing the atmospheric turbulence.

Equation (1) only describes in a simplified way the transmission property of an atmospheric channel and ignores any phase (front) fluctuations. This is sufficient for our analysis because our experiments utilize the direct detection of single photons, making the phase nature of the transmission irrelevant.

2.1. Measuring free-space link statistics with entangled photons

To begin with, we measured the free-space transmission efficiency statistics in our entanglement-based QKD system. The system is composed of a compact Sagnac interferometric entangled photon source [33–35] operating at 808 nm, a 1305 m free-space optical link where the outgoing/incoming beam is expanded/contracted by the use of appropriate telescopes (the telescopes have a 75 mm collection lens and a 25:1 magnification), two compact passive polarization analysis modules, quad module silicon avalanche photodiode single photon detectors (Perkin-Elmer SPCM-AQ4C, $\sim$50% detection efficiency, $\sim$400 dark counts per second), time-tagging units, GPS time receivers, two laptop computers and custom written software [7]. We chose to work at a wavelength of 808 nm to take advantage of a peak in the typical atmospheric transmission [19] as well as the high detection efficiency at that wavelength in our detectors. Usually there is a 10 nm interference filter at the entrance of the polarization detector box used to reject background light; however, we remove it for all experiments in this
paper in order to simulate a scenario (such as a satellite link) with a higher background noise level in order to test the usefulness of our SNRF, described later.

Brida et al [36] were the first to suggest using two photon entangled states for the absolute quantum efficiency calibration of photodetectors. We adapt their method here to measure the PDTC of the free-space channel by first performing a local experiment with the same equipment (source, polarization analysers and photon detectors) so that we can measure various other efficiencies of the system. Then through a comparison of the experiments performed locally and over the free space, we can extract the PDTC of the link.

In a local experiment, we expect the number of counts per second seen by Alice (\(N_A\)) and Bob (\(N_B\)) to be given by

\[
N_A = N \eta_A = N \eta_{\text{source}} \eta_{\text{pol}} \eta_{\text{det}} \tag{2}
\]

\[
N_B = N \eta_B = N \eta_{\text{source}} \eta_{\text{pol}} \eta_{\text{det}} \tag{3}
\]

where \(N\) is the total number of pairs produced at the source per second, \(\eta_A\) is Alice’s total transmission efficiency (composed of the source coupling efficiency, \(\eta_{\text{source}}\), polarization analyser efficiency, \(\eta_{\text{pol}}\), and detector efficiency, \(\eta_{\text{det}}\)), and similarly for Bob. Additionally, the expected number of observed coincidences per second (\(N_{\text{coin}}\)) between Alice and Bob, found using a coincidence window (\(\Delta t_{\text{coin}}\)) to identify entangled photon pairs, is given by

\[
N_{\text{coin}} = N \eta_A \eta_B \tag{4}
\]

Dividing the measured coincidence count rate (\(N_{\text{coin}}\)) by the observed singles rate at Alice (\(N_A\)) yields an estimate for the total loss caused by Bob’s optics (\(\eta_B\)) including the source coupling, polarization analyser and photon detectors. Double pair emissions, where two photon pairs are created in the source crystal at once, could lead to corrections in equations (4)–(7) at sufficiently high pump powers. However, for the experiments detailed here, the pumping strength was sufficiently low that double pair emissions were negligible and thus safely ignored.

For experiments performed over the free-space link, the equation for Bob’s singles rate gets modified to

\[
N_B = N \eta_B + N_{\text{background}}
= N \eta_{\text{source}} \eta_{\text{atm}} \eta_{\text{pol}} \eta_{\text{det}} + N_{\text{background}}, \tag{5}
\]

where his total transmission efficiency, \(\eta_B\), now includes a term for the link transmission efficiency, \(\eta_{\text{atm}}\), and an additional term, \(N_{\text{background}}\), is added representing background photons which are collected and measured by Bob’s receiver. The equation for the coincidence rate is similarly modified to

\[
N_{\text{coin}} = N \eta_A \eta_B + N_{\text{accidental}}, \tag{6}
\]

where \(N_{\text{accidental}}\) represents accidental coincidences of Alice’s measurements with the background photons measured by Bob. Fortunately, the accidental rate given to a good approximation by

\[
N_{\text{accidental}} \approx N_A N_B \Delta t_{\text{coin}} \tag{7}
\]

can be easily estimated by finding the number of coincidences between Alice’s measurements and Bob’s measurements shifted by a few coincidence windows and then subtracted from the results.
To find the free-space link PDTC, we divide the coincidence rate ($N_{\text{coin}}$) observed during a link experiment by Alice’s local single photon count rates ($N_A$), which gives the PDTC for Bob’s total loss, $\eta_B$, including all the losses in his equipment. Then, using the estimate from the local experiment, we divide out the losses from Bob’s equipment leaving only the atmospheric transmission, $\eta_{B\text{, atm}}$, allowing us to construct the PDTC for the free-space channel. There is an alternative method for estimating the free-space link PDTC using only the singles rates from an experiment over a free-space link. However, the method just described using coincidences is more accurate than using just the singles rates since the only source of error is the accidental coincidence rate ($N_{\text{accidental}}$) which we can estimate and remove.

We studied three different scenarios with our system for the distribution of entangled photons over free-space channels corresponding to the following conditions: a maximum free-space transmission with optimized pointing and focusing parameters (figure 1(a)), a transmission with artificially increased turbulence using a heat gun to heat the air immediately in front of the sending telescope (figure 1(b)), and a defocused transmission as a way to simulate larger losses (figure 1(c)). For each of these experiments, the data were broken up into blocks of a certain duration which we call the block duration and then the efficiency was estimated for each block using the method described above. These results are then summed up into a histogram, normalized and displayed as the PDTC for that link. In all cases, the distributions are shown with a block duration of 10 ms since it has been shown that this is the typical timescale for atmospheric turbulence [28]. All measurements were made on 24 August 2011 between the hours of 12 and 1 am since the system requires the reduced background experienced at night to operate, with a total data acquisition time for each experiment of 3 min. The temperature was approximately 18 °C with clear visibility in an urban environment with typical city illumination levels.

Figure 1(a) shows that we experienced extremely good atmospheric conditions during the experiments since the observed transmission coefficient for the well-aligned link was very close to a Poissonian distribution. The term Poissonian here really refers to the original graphs of integer photon counts versus the frequency with which they were observed. We would expect the transmission coefficient for a local system without a free-space link to be Poissonian in nature owing to the pair creation process and detection. The fact that we still observe a Poissonian distribution with a free-space link implies that our atmospheric conditions were very good since the presence of the link did not alter the nature of the statistics.

The defocused transmission case, figure 1(c), is also very close to a Poissonian distribution only narrowed with a decreased overall transmittance compared with figure 1(a). This is expected since defocusing the beam increased it to a size larger than the receiver telescope, thus causing fluctuations in the transmission efficiency experienced over the free-space link to be smoothed out (i.e. causing it to be even closer to a Poissonian distribution) while at the same time lowering the overall transmittance since many more photons missed the receiver telescope and consequently were not collected and measured. For the experiment where turbulence was artificially added by letting the beam pass over hot air produced by a heat gun, figure 1(b), the distribution indeed changes towards a log-normal distribution as predicted.

3. Effect of link fluctuations on decoy state quantum key distribution (QKD)

Having investigated the PDTC for a number of different free-space channels in the previous section, we now turn our attention to the question of what effect atmospheric turbulence might
Figure 1. PDTC for the case of (a) an optimized free-space channel, (b) a free-space channel with artificially increased turbulence using a heat gun placed in front of the sending telescope and (c) a free-space channel where the beam is defocused in order to simulate larger losses. The detection (sampling) time was 10 ms.

have on weak coherent pulse QKD with decoy states. Attenuated lasers, while convenient for QKD, do not emit true single photons but rather a mixture of photon number states following a Poissonian distribution. This limits the distance over which QKD can be performed as Eve can perform a photon number splitting attack to gain full information on multi-photon pulses [37]. This attack relies on Eve’s ability to block single photon pulses and thus modifies the channel transmission nonlinearly depending on the photon number. However, this attack can be detected through the use of decoy states of various pulse strengths [38, 39], and an additional step in the security phase which verifies that channel transmission does not depend on the mean
Figure 2. Secure key rate versus the turbulence parameter, $\sigma$, comparing static (solid line) and fluctuating channels (dashed line) with the same mean loss. Average channel losses are indicated for the four curves. Deviation is only apparent at very strong turbulence, meaning that the static channel approximation is sufficient for most cases.

photon number. Thus, it is crucial for free-space QKD systems using decoy states to consider atmospheric fluctuation since the security of the protocol depends strongly on the relative transmission of the various pulse strengths.

Here we investigate whether the assumption of a static channel for determining secure key length is valid when the channel is, in reality, fluctuating. We consider a one-decoy protocol from Ma et al [40], including the ‘tighter bound’ from section E.2, along with the PDTC generated from the photon statistics in atmosphere taken from [28], and with a realistic error correction efficiency of $f(e) = 1.22$ used. Figures 2 and 3 compare the results of a simulation of secure key rates based on a simple static channel versus a channel fluctuating with a log-normal distribution.

Figure 2 shows that approximating a fluctuating channel as a static channel with the same mean loss is sufficient so long as the atmosphere is not extremely turbulent. It should be noted that the turbulence model of Milonni et al [28] begins to fail at extremely high turbulence levels possibly leading to inaccuracies in the extreme right portion of figure 2. Unfortunately, we are unaware of a correct high turbulence free-space link model to replace it within this regime. Nevertheless, we can still draw important conclusions in the usual operating scenarios. Further, at moderate turbulence strengths figure 3 shows that the static channel approximation is valid as long as the channel loss is above $\sim 15$ dB, a typical condition in long distance free-space QKD (see [19] for example scenarios). Therefore, the security of weak coherent pulse QKD with decoy states is not significantly affected by a fluctuating free-space quantum channel as compared to the usual assumed static channel since the differences only arise in a situation where the high turbulence would likely make a successful transmission impossible or with a
Figure 3. Secure key rate versus loss, comparing a static quantum channel (solid line) to a fluctuating free-space quantum channel (dashed line) with the same mean loss. (a) considers a ‘good’ atmosphere with $\sigma = 0.18$, resulting in no deviation between the static and fluctuating channels. (b) considers a ‘bad’ atmosphere with $\sigma = 1.8$, resulting in less secure key for the fluctuating channel at low loss.

link with such low losses that the transmission distance is probably uninteresting. This also paves the way for checking whether the key rates could possibly be improved with an SNRF.

4. Improving QKD with a signal-to-noise ratio filter

Using the link statistics analysis and the data from the experiments above, we now investigate the use of an SNRF in order to increase the final key rate in QKD systems with a turbulent quantum transmission channel. The idea of the SNRF is to throw away data blocks where the signal-to-noise ratio (SNR) was low based on a directly measurable quantity, the signal strength, under the assumption that the noise caused by background events remains constant. While this has the consequence of decreasing the overall raw key rate, it is possible to actually improve the final secret key rate since we omit the blocks where the SNR was lower and correspondingly the quantum bit error rate (QBER) was inflated by the larger relative contribution from the background. We mention that similar filtering techniques have been explored in the continuous variable regime, although the effect of fading on continuous-variable quantum states is very different. Fading and excess noise quickly destroy Gaussian quantum features such as entanglement and purity of states; however, different possibilities have been offered to recover these [41, 42].

We define the SNRF algorithm as follows. One begins by measuring the background contribution of the quantum free-space channel (in terms of a count rate) with the entangled source switched off. Then one defines the singles contribution from the source divided by the background contributions as the dimensionless SNR. One then throws away low SNR blocks where the background contribution is proportionally higher according to a preset SNR threshold. The idea can also be mapped to real coincidences from the source divided by background coincidences where these numbers now implicitly depend on the coincidence window used.
In the following, we implement the equivalent algorithm where rather than using the dimensionless SNR we instead use the singles rates to define our threshold. The SNR threshold is implicitly used in this protocol since the background noise is assumed to remain constant. Thus, examining the optimum singles rate threshold effectively amounts to finding the optimum SNR threshold since one could calculate this number by first measuring the background, subtract it from the total measured singles and then divide the remainder by the measured background to arrive at the SNR. In the remainder of this paper, we will refer to all such equivalent protocols as an SNRF algorithm.

Figure 4 shows (a) Alice’s local rates (red curve) and Bob’s singles count rates measured over the link (blue curve) along with the coincidence count rate (green curve) and (b) the corresponding QBERs measured in the $Z$ (blue curve) and $X$ (green curve) bases when no SNRF is used for the artificially increased turbulence experiment of figure 1(b). Figure 4(c) shows Alice and Bob’s singles and coincidence rates when the optimum SNRF threshold of 95 000 counts per second (discussed below) is applied and panel (d) shows the corresponding QBER. The data points are grouped according to the optimum block duration of 30 ms (thus each data point represents 30 ms worth of data) and a coincidence window of 5 ns is used. Here one can clearly see the high background detection rate experienced by Bob (a situation that will be typical of a QKD link performed to an orbiting satellite) as the flat bottom of his singles rate graph (figure 4(a), blue curve), as well as the wildly varying coincidence rates (figure 4(a), green curve) where the points close to the $x$-axis largely consist of accidental coincidences. From figure 4(a), blue curve, we can estimate Bob’s mean background count rate at roughly 2700 counts per second. Each background count that is registered as a valid coincidence will be uncorrelated with Alice’s measurements and contribute a 50% error rate to the QBER.

The SNRF idea is neatly illustrated here by looking at the many high QBER values, corresponding to the low signal phases in figure 4(b) associated with Bob’s low singles and coincidence rates from the top graph. We know from the experiment corresponding to figure 1(a) for the well-aligned link that the intrinsic QBER is $\sim 2.34\%$; however, the QBER observed for the turbulent link corresponding to figure 1(b) and figures 4(a) and (b) was instead $\sim 5.51\%$. This increase in the measured QBER over the actual QBER of the system will lower the final secret key rates. However, one can see that when the low SNR regions are removed from the singles and coincidence graph (figure 4(c)) using the optimum SNRF, many of the corresponding high QBER blocks (figure 4(d)) are also removed. Thus, we are able to lower the measured QBER from $\sim 5.51$ to $\sim 4.30\%$, a value closer to the intrinsic error rate of the system, allowing the system to generate many more secret key bits than would otherwise be possible.

The secret key rate formula for our system expressed in secret key bits per raw key bit is given by [43]

$$R = \frac{1}{2}(1 - f(e)h_2(e) - h_2(e)),$$

where $f(e)$ is the error correction inefficiency as a function of the error rate, normally $f(e) \geq 1$ with $f(x) = 1$ at the Shannon limit, and $h_2(e) = -e \log e - (1 - e)\log(1 - e)$ is the binary entropy function. For clarity of the argument, we have used the infinite key limit formula; however, the insights gained should transfer to the finite key limit. Looking at equation (8), we can see that a higher QBER is detrimental to the final key rate for two reasons: (a) increased error correction inefficiency and (b) increased privacy amplification. The Cascade algorithm

The $Z$ basis here refers to the basis of the Pauli $\sigma_Z$ operator (i.e. horizontal and vertical polarization), while the $X$ basis refers to the basis of the Pauli $\sigma_X$ operator (i.e. $+45$ and $-45$°C polarization).
Figure 4. Alice’s local single count rate (red curves, the left axis), Bob’s single count rate measured over the link (blue curves, the left axis), the coincidence rate (green curves, the right axis) and QBER in the $Z$ (blue curve) and $X$ (green curve) bases for the high free-space turbulence experiment of figure 1(b) for the case of (a), (b) no SNRF and (c), (d) the optimum SNRF of 95 000 singles per second. The data points are grouped according to the optimum block duration of 30 ms and a coincidence window of 5 ns is used.
[44, 45] and low density parity check codes [46–49] are the two most commonly employed error correction algorithms used in QKD systems. As the QBER climbs the number of parities revealed (and correspondingly the information about the key which has to be accounted for in privacy amplification) increases. This applies even in the ideal case of error correction algorithms operating at the Shannon limit. Privacy amplification is then used after error correction to squeeze out any potential eavesdropper and ensure that the probability that any one besides Alice and Bob knows the final key is exponentially small at the cost of shrinking the size of the final key. Privacy amplification is commonly accomplished by applying a two-universal hash function [50, 51] to the error corrected key and then using equation (8) to determine how many bits from this operation may be kept for the final secret key. Both the number of bits exposed during error correction and the measured QBER are used to determine the final size of the key. Additionally, the secure key rate formula is a nonlinear function of the QBER so that decreasing the QBER does better than a linear improvement in the final key rate [52]. Thus, the fewer the parities revealed during error correction and the lower we can make the measured QBER, the larger the final key will be.

The use of an SNRF could potentially open a loophole in the security proofs for QKD, since we are now discarding data (which is typically not allowed by the proofs) depending on Bob’s measured singles rates. However, we are implementing the SNRF on Bob’s singles rate which is a sum over all his detectors during a block of data, so the SNRF is detector independent. In addition, discarding data should be equivalent to a decrease in channel transmission efficiency (which could happen anyway due to atmospheric effects) and thus should not affect the security proof. One might initially think that measuring the SNRF in real time could thwart a potential eavesdropper; however, any real-time measurement would require a probe beam either of a different wavelength or propagating in a different spatial mode so that it could be easily separated from the signal photons. This difference would easily allow an eavesdropper to fake whatever background they wished on the probe beam while leaving the signal beam untouched. Therefore, for this paper we assume that using an SNRF does not compromise the security of our system; however, we stress that it remains an open question whether security can be proven for this scenario. We also point out that for an entangled QKD protocol, security does not depend on the transmission of the quantum channel; whereas, if one wanted to use an SNRF in a decoy state protocol, which works by measuring the channel gain for each photon number component, the issue of security would be delicate and require careful analysis so as not to open up any security loopholes. We hope that by showing the utility of the SNRF methods we can stimulate work on proving its security. Finally, we also mention the recent work by Usenko et al [53] which theoretically studied the influence of fading on Gaussian states in the framework of the continuous variable QKD filtering ideas mentioned earlier.

5. Experimental results and discussion

After performing some initial simulations which showed the promise of the SNRF idea, we proceeded to implement the algorithm using the data gathered during the artificially increased turbulence experiment of figure 1(b). There are three main parameters which affect the total secret key rate using the SNRF idea: the block duration, the SNRF threshold and the coincidence window. The block duration refers to the timescale on which the SNRF algorithm is applied and its optimum should be related to the timescale of the atmospheric turbulence. The optimum SNRF threshold should be related to the mean background count rates observed during the
Figure 5. The total secret key for the high turbulence free-space experiment of figure 1(b) plotted versus the block duration and the SNRF threshold, using a coincidence window of 5 ns. The optimum block duration was found to be 30 ms, while the optimum SNRF threshold was 95 000 counts per second suitably applied on the timescale of the optimum block duration.

The key rates for the lower SNRF thresholds (closest to the front) in figure 5 essentially show the secret key rate one would expect without implementing the SNRF algorithm (since little if any raw key is thrown away). As the SNRF threshold increases however (moving towards the top in figure 5), one can clearly see that the total secret key rate also increases until reaching a maximum at which point it quickly falls off since the SNRF cuts out too much raw key. Less obvious from the figure, but still important, there is a gradual improvement in the secret key rate as the block duration shrinks until a maximum is reached at which point the secret key rate gradually decreases once again. The optimum parameters for this data set were to use a block duration of 30 ms and an SNRF threshold of 95 000 counts per second suitably applied on the timescale of the optimum block duration which increased the total secret key generated to 97 678 bits from the 78 009 bits generated when no SNRF was used. This represents an increase of 25.2% in the total secret key generated from the same raw key data set.

As mentioned earlier, the secret key rate given by equation (8) is improved due to two effects. Firstly, the intrinsic error rate in the data is smaller, causing the efficiency of the Cascade error correction algorithm [44, 45] used here to be improved from 1.2631 for the case of no SNRF to 1.2202 when an SNRF is used. This increased efficiency translates into fewer bits
Table 1. Measured values for: directly generating key, using the SNRF to generate key, and data discarded by the SNRF, for the high free-space turbulence experiment of figure 1(b).

| Scenario     | Raw key | Sifted key | Secret key | $f$    | QBER (%) |
|--------------|---------|------------|------------|--------|----------|
| No SNRF      | 535 530 | 259 855    | 78 009     | 1.2697 | 5.51     |
| Above SNRF   | 466 441 | 226 279    | 97 678     | 1.2202 | 4.30     |
| Below SNRF   | 69 089  | 33 576     | –          | –      | 13.77    |

revealed during error correction and thus a few bits sacrificed during privacy amplification. Secondly, the QBER measured during error correction is smaller, 4.30% with an SNRF versus 5.51% with none. This translates into less privacy amplification needed to ensure that the final secret key is secure against an eavesdropper.

In order to aid the potential security analysis of our SNRF idea, we also include a few other measured values pertinent to its implementation which are summarized in table 1. For the data set shown in figure 5, we kept 466 441 coincidences which made up our raw key while rejecting 69 089 coincidences generated from data blocks that were below the SNRF threshold. The size of the sifted key, where both Alice and Bob measured in the same basis, was 226 279 bits while 33 576 bits were rejected by the SNRF. As mentioned before, the QBER in this sifted key was 4.30% while the QBER in the rejected data was 13.77%. Here we can clearly see how utilizing the SNRF was able to increase our overall secret key rate by rejecting this small subset which turns out to have a much higher QBER.

While the preceding discussion nicely illustrated the usefulness of using the SNRF idea to produce a larger final key length from the same raw key rates, we now mention two ideas for how one would actually implement the SNRF algorithm in practice. The first idea would be in the case of a static scenario (fixed position free-space links) to use the first few minutes of an experiment to find the optimum SNRF threshold (since finding the optimum requires full knowledge of the measurement results) which would then be used during the rest of the key exchange. For the case of a long distance key exchange with a quickly changing background, one could periodically re-calculate the ideal SNRF threshold in order to continually operate with the optimum threshold. In the case of an exchange with an orbiting satellite, for example, one could periodically re-calculate the optimum every few seconds even as atmospheric conditions changed over the course of the key exchange. The beauty of the SNRF idea is that it can be applied completely offline, as the raw data from the key exchange can be saved and processed with the optimum threshold determined after the satellite has already passed overhead. In addition, the user can apply as fine or coarse grained an analysis as they wish. A second possibility would be to have a catalogue of free-space parameter regimes and the corresponding optimum SNRF thresholds stored in a look-up table. Then one could continually monitor the free-space link statistics over the course of a key exchange (which require only the coincidence events to calculate) and pick the optimum threshold based on the measured free-space PDTC parameters.

Besides these implementation ideas, there are at least two other possibilities for future work to augment the protocol. The ideas are similar with the first being to use an adaptive block duration which expands and contracts depending on the single photon rates being observed. The optimum block duration of 30 ms found in this experiment was in a way a compromise between using larger blocks where fluctuations are averaged over and smaller blocks where there are
unclear statistics. With an adaptive algorithm it would be possible to match the block duration more closely to the actual physical SNR variations during an experiment and thus increase the proportion of good transmission periods kept even more.

The second idea would seek to examine how the signal (singles rate) is correlated with the QBER (for instance, by plotting a 3D frequency (z-axis) histogram of signal (x-axis) versus QBER (y-axis)). With this correlation plot, one could try to predict what the most likely QBER would be for a given signal level. Then one could apply a finer filtering scheme, for instance, grouping data blocks into the three classes: low QBER, medium QBER (<11%) and high QBER (>11%). Certainly the high QBER blocks should be discarded because they actually cost key. But while the medium QBER blocks may still have a QBER higher than that of the intrinsic system due to background light, they would still contribute positively to the key. Processing them separately from the low QBER blocks, however, would allow one to optimize the algorithms used for each subset to make them as efficient as possible.

The full power of the SNRF idea is realized in the cases with a high background where the accidental coincidence rate approaches the same order of magnitude as the QKD signal. Recent work for the case of performing QKD with an orbiting satellite [19] has shown that one will indeed be operating in a high background regime where the SNRF idea will prove very useful. Further to this point, depending on the level of the background noise, the simulations in figure 6 show that the SNRF idea can be used to produce a secret key when the background would otherwise have prevented it. Figure 6 plots the secret key rates for exchanging key with an

Figure 6. The simulated secret key rates for a LEO QKD satellite for various elevation angles and the expected number of background counts and free-space PDTC [19]. We assume that the entangled source on the satellite operates at 100 MHz with an intrinsic QBER of 2.5%. Negative rates in the shaded region below the zero axis would produce no secret key and are shown to emphasize the fact that utilizing the SNRF can produce a positive key rate where otherwise none would be possible.
orbiting LEO QKD satellite carrying an entangled photon source with a pair production rate of 100 MHz and an intrinsic QBER of 2.5% for various elevation angles and the expected number of background counts and free-space PDTC [19]. These initial results show that the SNRF idea would allow us to generate secret key from many more satellite passes occurring at elevation angles of 70° or less; however, a more detailed analysis would have to take into account the statistics of satellite passes over a year which must integrate over the various elevation angles. Nonetheless, the SNRF idea should prove particularly useful, as the most probable passes for a LEO satellite occur at elevation angles much less than 90° which otherwise would render them useless due to the high free-space link fluctuations, high background and low SNR experienced. Thus, we are very confident that the SNRF idea will prove extremely useful in high background situations such as in satellite QKD, long distance terrestrial free-space links or daylight QKD experiments.

6. Conclusions

In conclusion, we have used an entanglement-based free-space QKD system to study the link statistics generated during the fluctuating free-space transmission of entangled photon pairs. Simulating a free-space channel with a large amount of turbulence allowed us to recover the theoretical prediction of a log-normal distribution for the statistics of the transmission coefficient. Using insights from this analysis, we studied the effect of link fluctuations on free-space decoy state QKD and found that the static channel approximation typically assumed is valid for the regimes where such systems are typically operated. Lastly, we studied the implementation of an SNRF in order to increase the overall secret key rate by rejecting measurements during periods of low transmission efficiency which tend to have a larger QBER due to a higher proportion of background events to actual entangled pair detection in the raw key. Using this SNRF, we were able to increase the final secret key rate by 25.2% using the same raw signals for a particular experimental run. Further, we showed simulations that indicate that the SNRF idea will be extremely useful in terrestrial long distance free-space experiments and experiments exchanging a key with a LEO satellite allowing one to generate a secret key from many passes that would otherwise have been useless.

Acknowledgments

Support for this work from NSERC, CSA, CIFAR, CFI, ORF, OCE, ERA and the Bell family fund is gratefully acknowledged. One of us (BH) would like to thank the EU-Canada Programme for Cooperation in Higher Education, Training, and Youth, which sponsored her exchange with the IQC during this project. The authors would like to thank M Toyoshima, B Higgins and N Lütkenhaus for helpful discussions about free-space satellite communication, turbulence induced link fluctuations and the quantum security of such schemes.

Note added. During the final preparation of the manuscript the authors became aware of a similar work [54] which examined the impact of turbulence on long-range quantum and classical channels, and put forward a similar SNR proposal based on measuring a secondary beacon laser. While the work measuring the PDTC of the free-space links is similar, we stress that we have already implemented such an SNRF directly on the detected signal and illustrated the improvements possible.
References

[1] Sasaki M et al 2011 Field test of quantum key distribution in the Tokyo QKD network Opt. Express 19 10387–409
[2] Peev M et al 2009 The SECOQC quantum key distribution network in vienna New J. Phys. 11 075001
[3] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 A framework for practical quantum cryptography Rev. Mod. Phys. 81 1301–50
[4] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Quantum cryptography Rev. Mod. Phys. 74 145–95
[5] Jin X M et al 2010 Experimental free-space quantum teleportation Nature Photon. 4 376–81
[6] Elser D, Bartley T, Heim B, Wittmann Ch, Sych D and Leuchs G 2009 Feasibility of free space quantum key distribution with coherent polarization states New J. Phys. 11 045014
[7] Erven C, Couteau C, Laflamme R and Weihs G 2008 Entangled quantum key distribution over two free-space optical links Opt. Express 16 16840–53
[8] Peloso M P, Gerhardt I, Ho C, Lamas-Linares A and Kurtsiefer C 2009 Daylight operation of a free space, entanglement-based quantum key distribution system New J. Phys. 11 045007
[9] Ursin R et al 2007 Entanglement-based quantum communication over 144 km Nature Phys. 3 481–6
[10] Nordholt J E, Hughes R J, Morgan G L, Peterson C G and Wipf C C 2002 Present and future free-space quantum key distribution Proc. SPIE 4635 116
[11] MagiQ Technologies 2008 www.magiqtech.com
[12] idQuantique 2011 www.idquantique.com
[13] Quintessence Labs 2011 www.quintessencelabs.com
[14] SeQureNet 2011 www.sequrenet.fr
[15] Dixon A R, Yuan Z L, Dynes J F, Sharpe A W and Shields A J 2008 Gigahertz decoy quantum key distribution with 1 mbit/s secure key rate Opt. Express 16 18790–7
[16] Rarity J G, Tapster P R, Gorman P M and Knight P 2002 Ground to satellite secure key exchange using quantum cryptography New J. Phys. 4 82
[17] Aspelmeyer M, Jennewein T, Pfennigbauer M, Leeb W and Zeilinger A 2003 Long-distance quantum communication with entangled photons using satellites IEEE J. Sel. Top. Quantum Electron. 9 1541
[18] Armengol J et al 2008 Quantum communications at ESA—towards a space experiment on the ISS Acta Astronaut. 63 165–78
[19] Bourgoin J P et al 2012 A comprehensive design and performance analysis of LEO satellite quantum communications arXiv:1211.2733
[20] Kolmogorov A N 1941 The local structure of turbulence in incompressible viscous fluid for very large Reynolds numbers Dokl. Akad. Nauk SSSR 30 301–4
[21] Tatarskii V I 1971 The Effects of the Turbulent Atmosphere on Wave Propagation (Springfield, VA: US Department of Commerce)
[22] Fante R L 1975 Electromagnetic beam propagation in turbulent media Proc. IEEE 63 1669–92
[23] Fante R L 1980 Electromagnetic beam propagation in turbulent media: an update Proc. IEEE 68 1424–43
[24] Andrews L C and Phillips R L 2005 Laser Beam Propagation Through Random Media (Bellingham, WA: SPIE Optical Engineering Press)
[25] Andrews L C, Phillips R L and Yu P T 1995 Optical scintillations and fade statistics for a satellite-communication system Appl. Opt. 34 7742–51
[26] Fried D L 1967 Scintillation of a ground-to-space laser illuminator J. Opt. Soc. Am. 57 980–3
[27] Shapiro J H 1984 2011 Scintillation has minimal impact on far-field Bennett–Brassard protocol quantum key distribution Phys. Rev. A 84 032340
[28] Milonni P W, Carter J H, Peterson C G and Hughes R J 2004 Effects of propagation through atmospheric turbulence on photon statistics J. Opt. B: Quantum Semiclass. Opt. 6 S742–5
[29] Vasylyev D Y, Semenov A A and Vogel W 2012 Towards global quantum communication: beam wandering preserves quantumness Phys. Rev. Lett. 108 220501
Semenov A A and Vogel W 2010 Entanglement transfer through the turbulent atmosphere Phys. Rev. A 81 023835
Semenov A A and Vogel W 2009 Quantum light in the turbulent atmosphere Phys. Rev. A 80 021802
Smith F G (ed) 1993 Atmospheric Propagation of Radiation vol 2 (Bellingham, WA: SPIE Optical Engineering Press)
Erven C, Hamel D, Resch K, Laflamme R and Weihs G 2010 Entanglement based quantum key distribution using a bright Sagnac entangled photon source Quantum Communication and Quantum Networking (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering vol 36) ed O Akan, P Bellavista, J Cao, F Dressler, D Ferrari, M Gerla, H Kobayashi, S Palazzo, S Sahni, X Shen, M Stan, J Xiaohua, A Zomaya, G Coulson, A Sergienko, S Pascazio and P Villoresi (Berlin: Springer) pp 108–16
Kim T, Fiorentino M and Wong F N C 2006 Phase-stable source of polarization-entangled photons using a polarization Sagnac interferometer Phys. Rev. A 73 012316
Fedrizzi A, Herbst T, Poppe A, Jennewein T and Zellinger A 2007 A wavelength-tunable fiber-coupled source of narrowband entangled photons Opt. Express 15 15377
Brida G, Genovese M and Novero C 2000 An application of two-photon entangled states to quantum metrology J. Mod. Opt. 47 2099–104
Gottesman D, Lo H-K, Lütkenhaus N and Preskill J 2004 Security of quantum key distribution with imperfect devices Quantum Inf. Comput. 4 325–60
Hwang W Y 2003 Quantum key distribution with high loss: toward global secure communication Phys. Rev. Lett. 91 057901
Lo H K and Ma Chen K X 2005 Decoy state quantum key distribution Phys. Rev. Lett. 94 230504
Ma X, Qi B, Zhao Y and Lo H K 2005 Practical decoy state for quantum key distribution Phys. Rev. A 72 012326
Heersink J, Marquardt C, Dong R, Filip R, Lorenz S, Leuchs G and Andersen U L 2006 Distillation of squeezing from non-gaussian quantum states Phys. Rev. Lett. 96 253601
Dong R, Lassen M, Heersink J, Marquardt C, Filip R, Leuchs G and Andersen U L 2008 Experimental entanglement distillation of mesoscopic quantum states Nature Phys. 4 919–23
Ma X, Fung C H and Lo H K 2007 Quantum key distribution with entangled photon sources Phys. Rev. A 76 012307
Brassard G and Salvail L 1994 Secret-key reconciliation by public discussion Lect. Notes Comput. Sci. 765 410
Sugimoto T and Yamazaki K 2000 A study on secret key reconciliation protocol ‘cascade’ IEICE Trans. Fundam. E83A 1987
Gallager R G 1962 Low density parity check codes IRE Trans. Inform. Theory IT-8 21–8
MacKay D J C and Neal R M 1997 Near Shannon limit performance of low density parity check codes Electron. Lett. 33 457–8
Pearson D 2004 High-speed QKD reconciliation using forward error correction AIP Conf. Proc. 734 299–302
Martinez I L, Chan P, Mo X, Hosier S and Tittel W 2009 Proof-of-concept of real-world quantum key distribution with quantum frames New J. Phys. 11 095001
Carter J L and Wegman M N 1979 Universal classes of hash functions J. Comput. Syst. Sci. 18 143
Krawczyk H 1994 LFSR-based hashing and authentication Advances in Cryptology—CRYPTO’94 (Lecture Notes in Computer Science vol 839) pp 129–39
Clarke P J et al 2011 Analysis of detector performance in a gigahertz clock rate quantum key distribution system New J. Phys. 13 075008
Usenko V C, Heim B, Peuntinger C, Wittmann C, Marquardt C, Leuchs G and Filip R 2012 Entanglement of gaussian states and the applicability to quantum key distribution over fading channels arXiv:1208.4307
Capraro I, Tomello A, Dall’Arche A, Gerlin F, Ursin R, Vallone G and Villoresi P 2012 Impact of turbulence in long range quantum and classical communications arXiv:1207.6931