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

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

CrossMark

OPEN ACCESS

RECEIVED
3 January 2022

REVISED
4 July 2022

ACCEPTED FOR PUBLICATION
7 July 2022

PUBLISHED
5 August 2022

Original content from this work may be used under the terms of the Creative Commons Attribution 4.0 licence.

Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.

PAPER

Modelling efficient BB84 with applications for medium-range, terrestrial free-space QKD

Thomas Brougham* and **Daniel K L Oi***

Computational Nonlinear and Quantum Optics, SUPA Department of Physics, University of Strathclyde, Glasgow G4 0NG, United Kingdom

* Authors to whom any correspondence should be addressed.

E-mail: t.brougham@strath.ac.uk and daniel.oi@strath.ac.uk

Keywords: free-space optics, QKD, quantum communication

Abstract

Terrestrial free-space (FS) quantum key distribution (QKD) is ideally suited for deployment in dense urban environments. The transition from laboratory to commercial deployment, however, raises a number of important engineering and deployment issues. Here, we investigate these issues for efficient BB84 using a weak coherent pulse-decoy state protocol. We calculate expected key lengths for different environmental conditions and when the scope for optimisation of protocol parameters is restricted due to practical considerations. In particular, we find that for a fixed receiver basis choice probability, it can be advantageous to allow the transmitter to have a different basis choice probability depending on varying channel loss and background light levels. Finally, we examine the effects of pulse intensity uncertainty finding that they can dramatically reduce the key length. These results can be used to determine the loss budget for the FS optics of a QKD systems and assist in their design.

1. Introduction

Quantum key distribution (QKD) allows for the secure distribution of cryptographic keys, where in principle, the security is guaranteed by the laws of physics [1–3]. This is in contrast to current public key methods, where the security is based on the difficulty of mathematical problems such as factoring or the discrete logarithm of elliptic curves [3, 4]. Such schemes are rendered insecure by a quantum computer, which can efficiently solve the hidden abelian subgroup problem that underlies efficient solutions to factoring and discrete logarithms [5]. The development of QKD is thus vital to protect our communication infrastructure and provide forward security without reliance on computational complexity assumptions.

In free-space (FS) QKD, signals are sent via line-of-sight transmission, e.g. between two ground stations or between a satellite and ground station. Satellite-based FS-QKD has attracted a great deal of attention due to its potential to allow QKD over global distances [6–19]. In contrast, ground based FS-QKD typically operates over short to medium distances, ideal for deployment in dense urban spaces where it may be difficult and costly to deploy ad hoc short range fibre links. FS-QKD between either buildings or existing towers should allow secure communication in a more flexible manner. A prototype of such a network is being constructed as part of the AirQKD project [20]. Here, we present high-level analysis of terrestrial FS-QKD operational trade-offs with particular consideration of how finite key statistical effects and uncertainties impact upon their design.

The development of a commercial ground based FS-QKD network faces significant challenges [21]. Firstly, the system has to operate under diverse environmental conditions such as varying background light levels, meteorological visibilities[1], and levels of turbulence, etc [22]. Furthermore, engineering or economic factors constrain the design and component choice. Components or operating settings may be standardised rather than optimised for each link scenario. For example, this could result in fixed or common protocol parameters such as basis bias and weak coherent pulse (WCP) intensities set at the factory instead of being

[1] Here, visibility refers to atmospheric transmittance [27].

© 2022 The Author(s). Published by IOP Publishing Ltd on behalf of the Institute of Physics and Deutsche Physikalische Gesellschaft

optimised for each deployment at greater cost. Hence, determining the performance of a fixed-setting FS-QKD system over a wide range of operating conditions and finding robust sets of protocol parameters are important practical considerations for real-world applications.

To ensure security, it is crucial to take into account finite statistical fluctuations and uncertainties during operation. A vital step for all QKD protocols is to use the transmitted data to estimate parameters, e.g. such as the quantum bit error rate (QBER), yields from vacuum and single photon emissions, and phase errors [23–25]. In practical use, the transmission window (or *integration time*) is finite and will be predetermined or limited due to operational considerations such as key refresh tempo or latency. Finite statistical effects can lead to sharp cutoffs in the positive secret key region as a function of channel loss and background count, thus selection of block accumulation lengths and integration times should be balanced against operational requirements.

QKD protocols based on WCPs requires knowledge of their intensities and these must be stabilized to what is intended. This is achieved by using power monitors to monitor the power and adjusting [26]. However, for any measurement there is an uncertainty associated with this. In a laboratory setting this uncertainty can be reduced and controlled. But in real world deployment, we must expect there to be a non-negligible uncertainty. If we are to ensure security, we must increase the amount of privacy amplification to take account of this uncertainty. We study this effect and show that it leads to both a reduction of the secure key length and a reduction of the region of parameter space for which a secret key can be extracted.

In this paper, we perform a systematic study of efficient BB84 across different environmental conditions, for fixed protocol parameters and study the effects of uncertainties in the intensities. In principle, the results can also be applied to fibre QKD, though will be of lesser utility as their operating conditions tend to be more stable compared with a terrestrial FS-QKD link that will be subject to large variations in loss and background light throughout the day. Geographic variation between FS-QKD links also requires modelling of the performance for a wide range of conditions and typical operating points. The outline of the manuscript is as follows. In section 2 we describe the channel and QKD setup; which serves to introduce the main physical parameters. In section 3 we explain the protocol and how this can be implemented physically in a real system. Results for optimizing the length of the secret key under different conditions are presented in section 4. Next, we study the effects of fixing protocol parameters on the optimization of the secure key length in section 5. We then investigate the effects of uncertainty in the WCP intensities in section 6. Finally, we discuss the findings in section 7. Preliminary versions of some of these result can also be found in [28].

2. The free-space system

We consider a FS optical line-of-sight system between a transmitter (Alice) and receiver (Bob) with a 100 MHz pulsed source of phase randomized polarisation encoded WCPs with signals states: vertical (0°), horizontal (90°), diagonal (45°) and anti-diagonal (135°), V, H, D and A, respectively. For the purposes of a high-level system performance model, we assume that side-channel leakage is negligible [29]. In practice, any implementation should be evaluated for such vulnerabilities, non-idealities characterised, and their effects taken into account in the final security analysis.

In a deployed system the maximum integration time will normally be preset and cannot be easily increased without increased memory or processing. It is thus vital to evaluate system performance over a range of integration times, or transmission block sizes that are the product of the pulse repetition rate and the integration time. The secure key length is determined by the total number of pulses transmitted and received, not the transmission rate, hence we consider a fixed repetition rate with different integration times to determine the number of pulses sent. Results for different repetition rates and transmission times can be easily inferred, keeping other parameters fixed.

FS channels suffer losses due to beam spreading (i.e. diffraction or geometrical losses), absorption, and scattering [30]. Turbulence will also cause the beam to both wander and distort [31, 32], reducing the coupling of the modes to the collection device. Sway of the transmitters and receivers together with additional pointing errors also adds to loss. These effects could be mitigated by active correction methods [33]. Other source of loss are imperfect mode coupling into the detector, detector efficiencies, and losses within the transmitter and receivers optics.

The losses in the transmitter can be mitigated, provided they can be well characterized. For security, what matters is that the emitted signal intensities exiting the transmitter aperture and into the Eve-controlled quantum channel are as specified. We can compensate for internal transmitter losses by producing WCPs with greater intensities at the source so that when they leave the exit aperture, they have

Table 1. A table of parameters that we keep constant throughout modelling.

After-pulse probability	p_{ap}	1×10^{-3}
Source's repetition rate	f_s	100 MHz
Correctness parameter	ϵ_c	10^{-15}
Secrecy parameter	ϵ_s	10^{-9}

the required intensity. Scattered light within the transmitter needs to be prevented from escaping else it could leak side-channel information.

We assume that transmitter losses are compensated by the above method hence we only need to consider the remaining contribution that we group together to obtain a total system loss η_{loss}. Let p_d be the total probability that a photon emitted from the transmitter is detected at the receiver, we characterise the channel optoelectronic efficiency by the total system loss (in dB) defined as

$$\eta_{loss} = -10\log_{10}(p_d). \tag{1}$$

We also consider *extraneous counts* due to detector dark counts or from stray-light where p_{ec} is the probability per pulse. Another source of errors is due to errors in the polarization states or their measurement and we characterise these by the *intrinsic quantum bit error rate* or $QBER_I$ that is independent of channel loss. We also account for detector after-pulsing where we assume the value $p_{ap} = 10^{-3}$, consistent with values used in previous modelling of fibre and FS QKD systems [36, 40]. For convenience, fixed modelling parameter are listed in table 1.

The photon statistics of the WCP signal states are described by a Poissonian distribution $P(n) = \exp(-\mu)\mu^n/n!$ where μ is the mean number of photons per pulse. An eavesdropper can perform a photon number splitting attack on the multiphoton emissions [34, 35]. To counter this, we use the so-called decoy state method to estimate the number of received vacuum and single photon emission events [23–25].

3. The QKD protocol

3.1. Outline of protocol

We employ the efficient BB84 WCP decoy state protocol with 3 intensities μ_1, μ_2 and μ_3 that are randomly and independently chosen [36].[2] Alice prepares WCPs with polarization chosen from one of two bases: $X \in \{H, V\}$ and $Z \in \{D, A\}$. With probability P_X^A Alice chooses the X basis, and with probability $P_Z^A = 1 - P_X^A$ she chooses the Z basis, in efficient BB84 the two bases need not be chosen with equal probability. Instead, the probability is found by optimizing the protocol so as to maximize the secure key length. With the basis chosen, Alice randomly and uniformly encodes bit values 0 or 1 onto the appropriate polarization state, where: $V, D \equiv 0$ and $H, A \equiv 1$, before choosing the intensity of each pulse: $k \in \{\mu_1, \mu_2, \mu_3\}$ with probability p_k. The intensity values can be any values that satisfy the relations: (i) $\mu_1 > \mu_2 > \mu_3$ and (ii) $\mu_1 > \mu_2 + \mu_3$. Bob randomly chooses to measure the polarization in either the basis X or Z, with probability P_X^B and $P_Z^B = 1 - P_X^B$, respectively.

After transmission Alice and Bob perform basis sifting through authenticated public announcement where they retain only those results corresponding to received pulses when they chose the same basis. Alice and Bob will then have n_X sifted X basis bits and n_Z sifted Z basis.

For the sifted bits, Alice publicly announces her choice of intensities for each WCP allowing Bob to tag each bit with its transmitted intensity. Let $n_{X(Z),k}$ denote the number of bits in the $X(Z)$ basis that originated from a pulse of intensity k. The secret key is constructed using only the sifted bits from the X basis, while the bits from the Z basis are used for parameter estimation. All the data from the Z basis is publicly announced, which allows Alice and Bob to calculate the number of errors in this basis: m_Z. Additionally, they can calculate the number of errors in bits that originate from pulses with intensity k, $m_{Z,k}$. Using these results, one can calculate the phase error ϕ_X using equations (4) and (5) of [36].

Alice and Bob's sifted bit string for the X basis will differ due to errors, which are corrected in the reconciliation stage, to produce the identical bit strings called the *raw key*. Error correction can be performed using a number of schemes [3], all of which requires public communication between that leaks λ_{EC} bits. Alice and Bob then perform a verification step to ensure their raw keys are identical with

[2] In other literature, this is also known as the two-decoy state protocol.

probability at least $1-\epsilon_c$, where ϵ_c is a pre-agreed correction parameter [36], here chosen to be $\epsilon_c = 10^{-15}$. The final stage is privacy amplification [2, 3, 43] that reduces the key to length ℓ bits.

3.2. Secure key length

From the analysis of [36], the final composable secure key length is given by

$$\ell = \left\lfloor s_{X,0} + s_{X,1}(1-h(\phi_X)) - \lambda_{\mathrm{EC}} - 6\log_2\frac{21}{\epsilon_s} - \log_2\frac{2}{\epsilon_c}\right\rfloor, \tag{2}$$

where $s_{X,0}$ is the estimated number of bits coming from vacuum events, $s_{X,1}$ is the number of bits originating from single photons, ϵ_s is the security parameter and $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy. A protocol is said to be $\varepsilon = \epsilon_s + \epsilon_c$ secure if it is ϵ_c-correct and ϵ_s-secret [43]. For all calculations presented we use $\epsilon_c = 10^{-15}$ and $\epsilon_s = 10^{-9}$.

The quantities $s_{X,0}$, $s_{X,1}$ and ϕ_X can be calculated using equations (1) to (5) from [36]. In that paper, there are correction terms due to finite statistical fluctuations appearing in the quantities $n^{\pm}_{X(Z),k}$ and $m^{\pm}_{Z,k}$, which we define below in equation (3). In [36] the correction terms are calculated using the Hoeffding bound [37] but it is possible to improve them using a modified version of the Chernoff bound [38, 39] as described in [40]. For the current analysis we use

$$n^{\pm}_{X(Z),k} = \frac{e^k}{p_k}\left[n_{X(Z),k} \pm \delta^{\pm}_{n_{X(Z),k}}\right], \tag{3}$$

$$m^{\pm}_{X(Z),k} = \frac{e^k}{p_k}\left[m_{X(Z),k} \pm \delta^{\pm}_{m_{X(Z),k}}\right], \tag{4}$$

where $k \in \{\mu_1, \mu_2, \mu_3\}$ and

$$\delta^{+}_{Y} = \beta + \sqrt{2\beta Y + \beta^2}, \qquad \delta^{-}_{Y} = \frac{\beta}{2} + \sqrt{2\beta Y + \frac{\beta^2}{4}}, \tag{5}$$

where $\beta = \ln(1/\varepsilon)$ and Y can equal either $n_{X(Z),k}$ or $m_{X(Z),k}$ [39].

The environmental parameters η_{loss}, p_{ec} and $\mathrm{QBER_I}$ appear within the expressions for $n_{X(Z),k}$ and $m_{X(Z),k}$, which feed into equations (3) and (5). For more details on how the environmental factors are incorporated within the model, see appendix E or [40].

The error correction term λ_{EC} is equal to the classical information exchanged during the reconciliation stage, this is included in the estimate of the amount of privacy amplification needed. In practice, we can keep track of the bits exchanged and thus λ_{EC} is known and not subject to statistical uncertainty. However, to model the systems performance we need an estimate of λ_{EC} and we use the sophisticated estimate introduce in [42], as discussed in [40].

3.3. Unequal basis choice

In efficient BB84, it is standard to choose $P^A_X = P^B_X$ and optimised for the channel conditions [41]. In practice, however, it often straightforward for Alice to vary her basis probabilities but difficult for Bob. This is because Alice can encode polarization states using four separate WCP emitters. Changing P^A_X amounts to changing the probability of Alice choosing the X basis signals. In contrast, Bob's measurement is typically realized by beam-splitter that randomly sends photons to one of two polarization measurement setups, to measure either in the basis X or Z. While a variable beam-splitter could be used in a laboratory, it would be more economical and practical in a mass produced commercial system to use a fixed beam-splitter.

To understand why setting $P^A_X \neq P^B_X$ is helpful in the case of Bob's receiver being fixed, consider the sifting stage. Before sifting, Alice and Bob shared N bits. The fraction of these bits discarded in the sifting stage is $P^A_X P^B_Z + P^A_Z P^B_X$. The fraction of bits retained in the X basis is $P^A_X P^B_X$, while $P^A_Z P^B_Z$ is the fraction in the Z basis. To maximize the key length, we want $P^A_X P^B_X$ close to one, while still allowing enough bits in the Z basis to accurately estimate the parameters. If P^B_X is fixed and $P^A_X = P^B_X$, we have no control of the sifting ratios. We thus generalize the protocol by allowing Alice and Bob to have different basis choice probabilities. This change in the protocol affects the numbers $n_{X(Z),k}$ and $m_{X(Z),k}$ seen in a given run. The change, however, does *not* affect either the key length formula, (2), or crucially, the security analysis [36, 43].

3.4. Optimization of the protocol

For a given value of the integration time, source repetition rate, η_{loss}, $\mathrm{QBER_I}$ and p_{ec}, we will calculate the secure key length. Initially, this involves optimizing the secure key length by varying the parameters: $\{P^A_X, p_{\mu_1}, p_{\mu_2}, \mu_1, \mu_2\}$. The value of P^B_X will either be set equal to P^A_X or will be fixed. The smallest intensity, μ_3 should be set to zero, but to avoid numerical issues, we instead use a very small value, $\mu_3 = 10^{-9}$. The

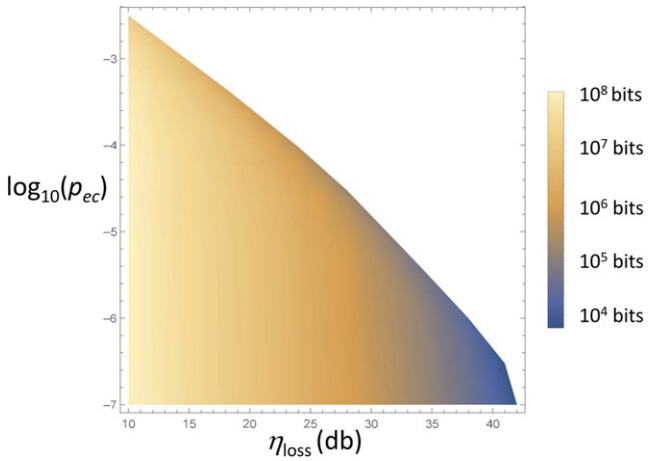

Figure 1. A 3D plot showing values of the secret key for different values of the total system loss, η_{loss}, and the $\log_{10}(p_{ec})$. The plot is for $QBER_I = 0.005$ and an integration time of 60 s.

details of the optimization are the same as those presented in [40] with the exception that now the channel loss is assumed to be fixed in time.

In section 5 we fix P_X^B and the intensities $\{\mu_1, \mu_2, \mu_3\}$. The numerical optimization of the secure key length now involves varying only the parameters: $\{P_X^A, p_{\mu_1}, p_{\mu_2}\}$, this only requires changing the way that the unbiased random number stream, e.g. from a quantum random number generator, are processed to derive the source input data. The approach is the same as before, but where now we input fixed values for P_X^B, μ_1, μ_2 and μ_3 which we assume are set and calibrated at the factory. The values of P_X^B chosen correspond to splitting rations of commercially available beam-splitters. The fixed values for the intensities are picked by a process of trial and error as well as through studying typical values found in the cases where they were optimized. The aim was not to find the optimal choice of fixed intensities, but instead to show that good choices existed over a range of channel conditions. As such the values of fixed values of intensities described in section 5 were not numerically optimized, but instead found using a process of trial and error.

4. System performance

For the design of FS optical systems, one must know the total loss budget, i.e. the maximum η_{loss} one can tolerate, while still producing a secure key. We evaluate the secure key length for different values of η_{loss}, p_{ec} and $QBER_I$. The results we present allow one to both evaluate the system performance under a wide range of environmental conditions and to determine a total loss budget for a given set of circumstances.

Consider a system operating with an integration time of 60 s (link refresh period), $QBER_I = 0.5\%$, $P_X^A = P_X^B$ and repetition rate of 100 MHz. A plot showing the region where one obtains secret keys is shown in figure 1 where we have numerical optimised all protocol parameters at each point, as discussed in section 3.4. The shaded region shows where one obtains a nonzero value for the secret key. We observe that ℓ, when non-zero, is large, even for relatively large losses. An important feature of the plot is that a slight increase in p_{ec} or η_{loss} can cause a sharp drop off in the secret key or reduce it to zero. This is illustrated more clearly in figure 2 where we plot ℓ against η_{loss}, for different values of $QBER_I$ and p_{ec}. An important feature is the sharp drop of ℓ to zero resulting from finite statistical corrections [40].

From figure 1 we observe that the effect of increasing p_{ec} becomes more pronounced as η_{loss} increases, this is due to two reasons. Firstly, increasing the loss decreases the total counts and thus increasing finite statistical fluctuations in the parameters. Errors due to p_{ec} thus become more significant. Secondly, as we increase η_{loss}, the fraction of the total counts corresponding to extraneous counts increases. This increases both the QBER and the phase error, ϕ_X. Figure 1 strongly suggest that p_{ec} greatly impacts the secure key length.

It is also important to understand the effect of the intrinsic QBER, $QBER_I$ on ℓ. In figure 2 we see that increasing $QBER_I$ causes ℓ to decrease. Furthermore, increasing both $QBER_I$ and p_{ec} causes ℓ to drop to zero for smaller values of the total loss. We see however, that increasing $QBER_I$ from 0.005 to 0.01 does not affect ℓ as greatly as increasing p_{ec}.

The sharp drop off of ℓ to zero is important when designing QKD systems. Is vital to know the range of parameters for which $\ell > 0$. In figure 3 we plot the region of values for η_{loss} and p_{ec} where $\ell > 0$. The regions are plotted for different values of $QBER_I$. It is evident that increasing $QBER_I$ not only decreases ℓ, as

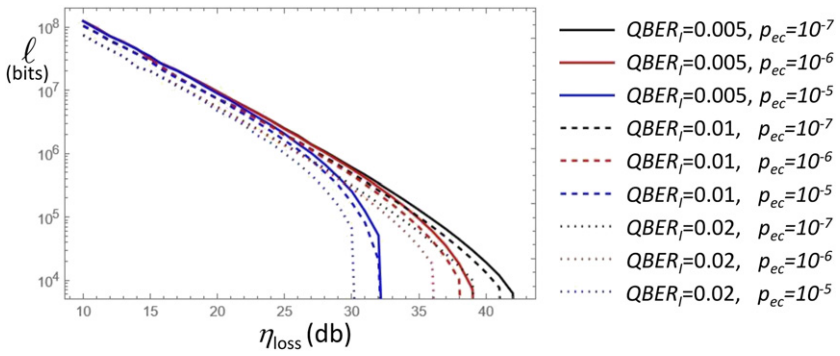

Figure 2. A plot of ℓ, the secure key length (bits), against η_{loss}, the total system loss. We plot for different values of QBER_I and different values of p_{ec}. The solid lines correspond to $\text{QBER}_\text{I} = 0.005$, the dashed lines are for $\text{QBER}_\text{I} = 0.01$, while the dotted lines are for $\text{QBER}_\text{I} = 0.02$. The black curves are for $p_{\text{ec}} = 10^{-7}$, the red curves are for $p_{\text{ec}} = 10^{-6}$, while the blue curves are for $p_{\text{ec}} = 10^{-5}$.

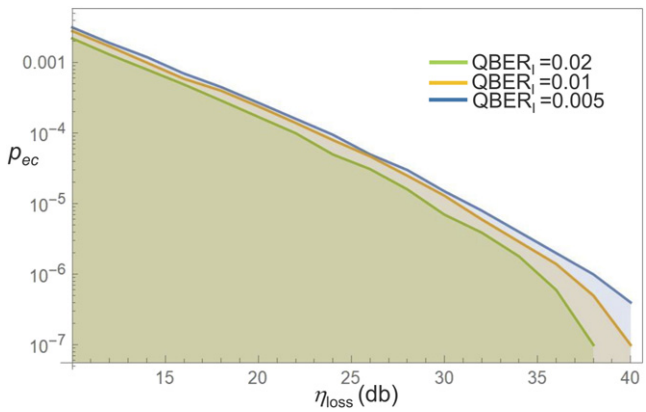

Figure 3. A plot showing the region where $\ell > 0$, i.e. when we can extract a secure key.

shown in figure 2, it also leads to a decrease in the regions where one can extract a secret key. Notice, however, for moderate values of η_{loss} the difference in regions for values of QBER_I equal to 0.5% and 1% is small. This suggests that if the QKD network is expected to operate in conditions where η_{loss} is below 35 dB, then the effort to decrease QBER_I below 1% might not yield great rewards. Instead, more attention should be focussed on reducing p_{ec}.

For different values of QBER_I. All curves are for an integration time of 60 s. The coloured lines represent the boundary for $\ell > 0$, while the shaded coloured regions also corresponds to $\ell > 0$.

The integration time also affects the secret key rate (SKR). Doubling the integration time doubles the raw key bits, this may be expected to also double ℓ but several effects can lead to a super-linear increase. A greater integration time also yields more data for parameter estimation, hence we can estimate the parameters with less error and obtain a smaller correction due to the finite statistics, illustrated in figure 4. In this plot, all curves correspond to $\text{QBER}_\text{I} = 0.005$. Both the blue and black curves are for a total system loss of $\eta_{\text{loss}} = 32$ dB. The extraneous count probabilities are $p_{\text{ec}} = 10^{-6}$ for the blue curve and $p_{\text{ec}} = 10^{-5}$ for the black curve. In contrast, the red curve is for $p_{\text{ec}} = 10^{-5}$ and $\eta_{\text{loss}} = 34$ dB. If increasing the integration time had no effect on parameter estimation, then the SKR would be constant as integration time increases. However, as we see in figure 4, the SKR increases with integration time. In both the black and red curves, $\ell = 0$ initially. However, by increasing the integration time we eventually obtain a nonzero secret key. Furthermore, in all three curves, while the SKR continues to increase as the integration time increases, the rate of increase slows, suggesting that it will plateau for a sufficiently large integration times. These results dramatically illustrate the effects of finite statistics. For integration time of 60 s, the errors within parameter estimation could lead to $\ell = 0$. However, by increasing the integration time we can extract a secret key.

These results show that if possible, one should avoid using several short transmission windows. Instead, one should use fewer, but longer transmission windows. This would necessitate increasing the systems memory and changing the key generation cycle to accommodate the production of large amounts of key,

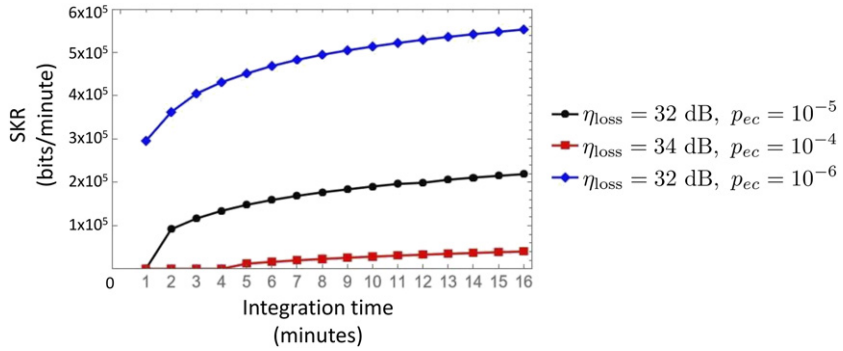

Figure 4. A plot showing the SKR, i.e. secret bits per minute, against the integration time. The blue curve is for $\eta_{\rm loss} = 32$ dB and $p_{\rm ec} = 10^{-6}$, the black curve is for $\eta_{\rm loss} = 32$ dB and $p_{\rm ec} = 10^{-5}$ and the red curve is for $\eta_{\rm loss} = 34$ dB and $p_{\rm ec} = 10^{-4}$. All three curves where generated with $\mathrm{QBER_I} = 0.005$.

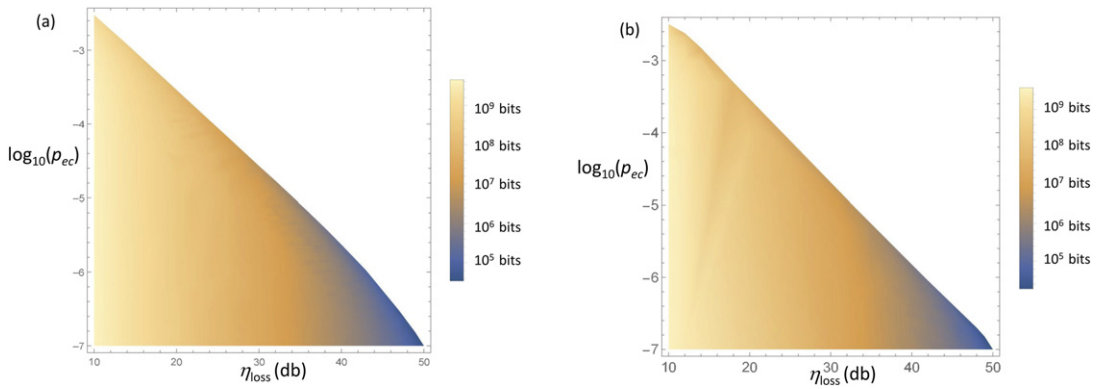

Figure 5. A 3D plot showing values of the secret key for different values of the total system loss, $\eta_{\rm loss}$, and the $\log_{10}(p_{\rm ec})$, for an integration time of 30 min. Plot (a) corresponds to $\mathrm{QBER_I} = 0.005$, while (b) is for $\mathrm{QBER_I} = 0.01$. Notice that for the long integration time of 30 min, plots (a) and (b) are very similar. This shows that doubling $\mathrm{QBER_I}$ from 0.005 to 0.01 does not have a strong effect.

over longer intervals. In principle, one could also group several smaller transmission windows together to form a larger integration time. This approach was investigated in [40] in the case of limited satellite overpass time, but here could be used to mitigate against weather induced channel outages. This is valid for finite data security proofs that use smoothed min-entropies, as described in [36].

In view of the previous results, one should use large integration times. For this reason we study the secure key length with an integration time of 30 min. Under the correct circumstances, this will provide a large amount of secret key. One can then use this to distribute multiple secret keys within a QKD network. Figure 5 shows a plot of the secret key against $\eta_{\rm loss}$ and $p_{\rm ec}$, where (a) is for $\mathrm{QBER_I}$ equal to 0.5% and (b) is for $\mathrm{QBER_I}$ equal to 1%. The long integration times means that we can extract secret keys for large losses. For example, for $\mathrm{QBER_I} = 0.005$, we can extract 34 256 bits for $\eta_{\rm loss} = 50$ dB and $p_{\rm ec} = 10^{-7}$. The plots also show the importance of background light. For example, with $p_{\rm ec} = 10^{-3}$ we can only extract a secret key for $\eta_{\rm loss}$ up to 14 dB. An important feature of figure 5 is that plots (a) and (b) are very similar. This demonstrates that increasing $\mathrm{QBER_I}$ from 0.005 to 0.01 has an almost negligible effect for large integration times. This suggests that once $\mathrm{QBER_I}$ has fallen 0.01, there are diminishing returns from its further improvement. For examples of how these results can be used to obtain loss budgets, see appendix A.

5. Performance with fixed parameters

In a real world deployment of a QKD system, it may not be cost effective to produce separate systems with different parameters for different operating conditions due to the additional effort and components required. An obvious issue is that Bob's basis choice is made using a fixed beam splitter. This means that P_X^B will be fixed, unlike in the previous plots where we assumed one could choose any value. In contrast, as we explained in section 3.3, Alice's can easily vary her basis choice probability, P_X^A. In the remainder of the analysis we allow for $P_X^A \neq P_X^B$. We consider a long integration time of 30 min and $\mathrm{QBER_I}$ of 1%. In models

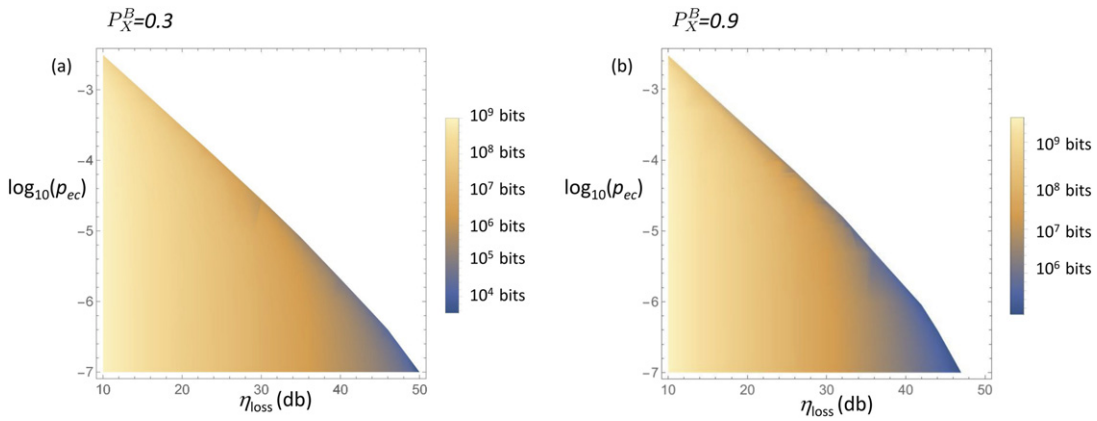

Figure 6. A 3D plot of ℓ plotted for total system loss η_{loss} and $\log_{10}(p_{\text{ec}})$. All plots are for $\text{QBER}_{\text{I}} = 0.01$ and an integration time of 30 min. The receiver basis choice probability is fixed to set values for both plots. In figure (a) we fix $P_X^B = 0.3$, while in (b) we have $P_X^B = 0.9$. This figure illustrates that there can be a trade-off for the choice of P_X^B. Low values for P_X^B give $\ell > 0$ for wider ranges of losses than larger values of P_X^B. However, when a secure key is produced, it tends to be larger when P_X^B is closer to one.

of fibre and satellite QKD systems, a value of 0.5% has often been assumed [36, 40]. The current value for QBER_{I} is more conservative and reflects the fact that a mass produced commercial system may not be as well aligned as current experimental systems.

In figure 6 we present plots of the optimized values for ℓ, where P_X^B is fixed to be a particular value. The optimization is performed by varying the values of $\{P_X^A, p_{\mu_1}, p_{\mu_2}, \mu_1, \mu_2\}$. In figure 6, (a) is for $P_X^B = 0.3$, while (b) is for $P_X^B = 0.9$. Additional plots for $P_X^B = 0.5$ and $P_X^B = 0.7$ are shown in figure 9 of appendix B. One can extract a secret key over a larger range of η_{loss} for smaller values of P_X^B. For instance, for $P_X^B = 0.9$, the largest total system loss for which we can extract a secret key for is $\eta_{\text{loss}} = 47$ dB. In contrast, we can extract secret key up to $\eta_{\text{loss}} = 50$ dB for both $P_X^B = 0.5$ and 0.3. While we can extract a secret key for a wide range of parameter, when we fix P_X^B, figure 6 shows that there is a trade-off for different values of P_X^B. For $P_X^B = 0.9$ we obtain a larger value of ℓ at smaller losses, than we do for $P_X^B = 0.3$. For example, for $\eta_{\text{loss}} =$ 10 dB and $p_{\text{ec}} = 10^{-3}$ we obtain 2.42×10^9 bits when $P_X^B = 0.9$ and 8.68×10^8 bits for $P_X^B = 0.3$. Using $P_X^B = 0.9$ yields a key that is ≈2.8 times greater than using $P_X^B = 0.3$. However, fixing P_X^B to a small value gives $\ell > 0$ over a wider range of losses, but at a cost of providing less secret key bits at lower losses than using larger values for P_X^B. This trade-off results as lower values for P_X^B means P_Z^B is larger thus increasing the number of bits available for parameter estimation. This is important for high losses, but for lower losses this leads to an excess of signals for parameter estimation at the expense of key generation. As only bits in the X-basis are used to construct the final key, having an excess of bits in the Z basis becomes wasteful. The choice of P_X^B is governed by whether we want to design a system to function over wide ranges of loss as possible. And if so, how great a decrease in secure key length are we willing to accept to achieve this robustness.

We have allowed P_X^A to vary and in particular, we do not assume that $P_X^A = P_X^B$. Some optimized values for P_X^A, corresponding to figure 6 are presented in appendix C. In it is observed that P_X^A is generally not equal to P_X^B, which means there is an advantage to allowing $P_X^A \neq P_X^B$. Table 2 corresponds to $P_X^B = 0.3$ and $p_{\text{ec}} = 5 \times 10^{-5}$, it shows that P_X^A is close to one for $\eta_{\text{loss}} = 18$ dB, and decreases as the loss increases. This demonstrates that setting $P_X^B = 0.3$ is sacrificing too much data to parameter estimation. The opposite case is shown in table 5, which corresponds to $P_X^B = 0.9$ and $p_{\text{ec}} = 10^{-6}$. Here we see that for $\eta_{\text{loss}} \geqslant 34$ dB, P_X^A is less than $P_X^B = 0.9$. This occurs because the loss is so great that we need to ensure we have sufficient data in the Z-basis for parameter estimation.

We have shown that allowing P_X^A to differ from P_X^B is beneficial when P_X^B is fixed. However, care must be taken with this observation. We have not shown that one should always optimize *both* P_X^A and P_X^B separately. Instead, we have argued that if P_X^B is fixed, then it is advantageous to allow P_X^A to differ from P_X^B. In fact, one can prove that for any values of P_X^A and P_X^B, one can find different values, where $P_X = P_X^A = P_X^B$, that yields the same ratio of raw bits in each basis and provides a possibly greater total number of sifted bits. The proof of this is presented in appendix D.

Due to deployment in different locations and operation during both night and day, the environmental factors of the system will differ. So far we assumed that signal intensities could be adjusted to accommodate the anticipated operating conditions. In practice this could be both costly and difficult to automatically employ, hence we now investigate the effect of fixing $\{\mu_1, \mu_2, \mu_3\}$. We look at finding fixed values for the intensities that still allow $\ell > 0$ over a wide range of different environmental conditions. As discussed in

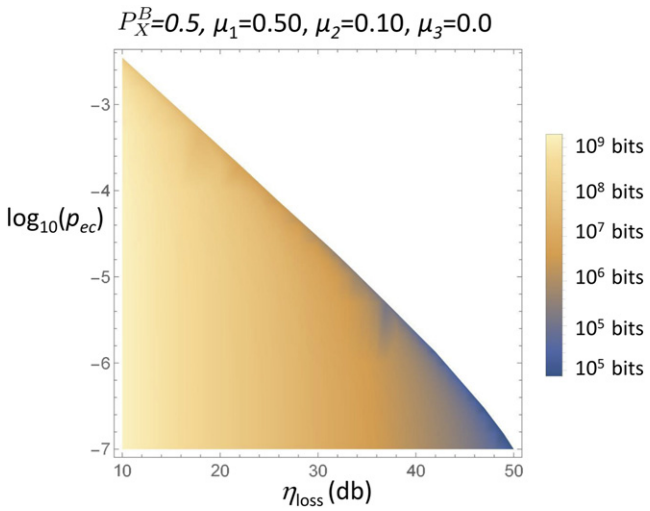

Figure 7. A 3D plot of ℓ plotted for total system loss η_{loss} and $\log_{10}(p_{\text{ec}})$. $\text{QBER}_{\text{I}} = 0.01$, integration time was 30 min, $P_X^B = 0.5$ was fixed, $\mu_1 = 0.50$, $\mu_2 = 0.10$ and $\mu_3 = 0$. Even when both P_X^B and $\{\mu_1, \mu_2, \mu_3\}$ are fixed, we can still choose values that allow one to extract a secure key over a wide range of system parameters.

section 3.4, we use the numerically optimized results for ℓ, with P_X^B fixed, to help find robust values for μ_1 and μ_2, as in figure 7 where ℓ is plotted for $P_X^B = 0.5$ and $\mu_1 = 0.50$, $\mu_2 = 0.10$ and $\mu_3 = 0$. Even when both P_X^B and the intensities are fixed, we can still obtain $\ell > 0$ over a wide ranges of values for η_{loss} and p_{ec}. Furthermore, we obtain significant values for the secure key length. The value $P_X^B = 0.5$ is not special and similar results can be obtained for other commonly available splitting ratios of beamsplitters (appendix B figure 10).

6. Effects of intensity uncertainty on secure key length

In the protocol the pulse intensities need to be well characterized. In a laboratory setting the intensities of the WCPs can be controlled to a high degree. In contrast, this will be difficult in a commercial system deployed within a busy urban environment. Instead, there may be long terms drifts or else systematic offsets from the ideal intensity values. This uncertainty affects the protocol as the security analysis assumes Alice transmits particular values for $\{\mu_j\}$. Bob then uses this information to estimate the vacuum and single photon yields. To ensure security, we must conservatively assume that the values transmitted correspond to those leading to the largest amount of privacy amplification required.

If the WCP intensities can vary by at most a fraction f, the actual mean photon number of the jth intensity lies within the range $[\mu_j - f\mu_j,\ \mu_j + f\mu_j]$. If we neglect the other intensities and model the variation from μ_j by a Gaussian distribution, then we would require that a large variation from μ_j must occur with probability less than ϵ_{sec}, otherwise the security might be compromised. For the full protocol, we use three different WCPs, the weakest pulse the vacuum ($\mu_3 = 0$). Any variation in this will be due to dark counts and stray-light and this is already taken into account in the previous analysis. Instead, we are concerned with the uncertainty in μ_1 and μ_2. If we model these with a multivariable Gaussian, then we require that any fractional variation larger than f occurs with probability less than ϵ_{sec}. The variance of these Gaussian is distinct from the photon statistical fluctuations but is determined by the uncertainty in how well one can set the intensities of the WCPs, an extremely stable laser could still have a large uncertainty in the WCPs intensities due to calibration of the electronic control system.

In practice, we can measure and determine the uncertainties in the WCPs and then deduce the value for the maximum fractional deviation, f. Any larger deviations must occurs with probability less than ϵ_{sec}. From this we obtain a range of values for μ_1 and μ_2. We find combinations of values that lead, in the worst case, to the smallest secure key. As we have no *a priori* information about what are the real values for μ_1 and μ_2, we assume the worst case and perform parameter estimation and privacy amplification with those values of intensities. This ensures the security of the system, but at a cost of reducing the length of the secret key.

Similar approaches have been studied before, but with important differences [45, 46]. In [45], they employed a numerical parameter estimation method with possible values of μ_j whose uncertainties were accounted within the numerical optimization scheme. In [46] the authors use an analytic approach directly incorporating fluctuations within the estimation procedure. Here, we use an analytic estimation procedure

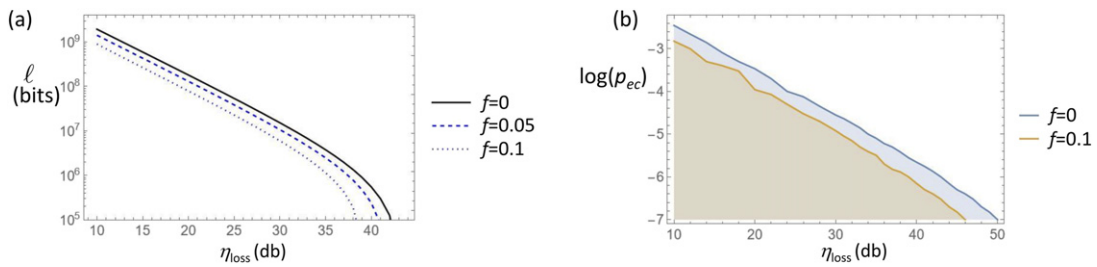

Figure 8. Effects on ℓ due to uncertainties in the WCP intensities. Integration time of 30 min, $\mathrm{QBER_I} = 0.01$, $P_X^B = 0.5$, $\mu_1 = 0.5$, $\mu_2 = 0.1$ and $\mu_3 = 0$. (a) ℓ against total system loss η_{loss} for different values of the fractional uncertainty, f, with $p_{\mathrm{ec}} = 10^{-6}$. The black line corresponds to $f = 0$, i.e. no uncertainty, while the dashed lines is for $f = 0.05$ and the dotted lines are for $f = 0.1$. (b) Regions where $\ell > 0$. x-axis is the total system loss η_{loss} and the y-axis is $\log_{10}(p_{\mathrm{ec}})$.

but take account of fluctuations using numerical optimisation, also considering the case where the nominal intensities are fixed for different losses, not considered in [45, 46]. Additionally, in [45, 46] the same uncertainties are applied to all signals with the same intensity but different polarization, we employ a slightly more involved approach as described below. As such, our results complement the existing literature.

Separate lasers and driving electronics may be used for different signal states, hence we must allow μ_1 and μ_2 to vary independently for both bases and bit values, i.e. they can take different values from the intervals $[\mu_j - f\mu_j,\ \mu_j + f\mu_j]$, $j = 1, 2$. To estimate $s_{X,0}$ and $s_{X,1}$ Bob will need to know μ_1 and μ_2. We assume Bob knows both the intended values and f. As such, he can construct the intervals $[\mu_j - f\mu_j,\ \mu_j + f\mu_j]$, $j = 1$, 2. However, neither Bob or Alice will know the real values for μ_1 and μ_2. During parameter estimation, Bob must choose values for μ_1 and μ_2 that lead to the smallest secret key. To summarize, we choose values for μ_j from $[\mu_j - f\mu_j,\ \mu_j + f\mu_j]$, $j = 1$ and 2, independently for the four signal states H, V, D and A, and also independently for Bob. We then find the smallest possible value for ℓ, which is the worst case value. To guarantee that we have performed sufficient privacy amplification, and thus the protocol is secure, we must use the worst case value for the secure key length.

To find the minimum value of the secret key, we discretise the intervals $[\mu_j - f\mu_j,\ \mu_j + f\mu_j]$. Numerical investigations showed that the minimum always occurred for values of μ_j at the edges of the intervals. This lead us to limit ourselves to three possible values for each μ_j: $\mu_j - f\mu_j$, μ_j and $\mu_j + f\mu_j$, retaining the middle value as a check on our assumption that the end values always yield the minimum. The minimization thus requires evaluating the secure key length for 3^{10} different sets of WCP intensities.

We study the case where we fix both the receiver basis probability and the WCP intensities, illustrated in figure 8. As expected, the effect of uncertainty is to reduce ℓ and in particular, ℓ goes to zero for lower values of η_{loss} as f increases. The effect, for a given value of p_{ec}, is to decrease the total loss budget of about 4 dB which can make a significant difference and must be factored in when designing a QKD system.

7. Conclusions

We have presented an in-depth investigation of the performance of efficient BB84 with the aim of aiding the design of terrestrial FS QKD systems. For fibre-based systems, the channel conditions are relatively stable and controlled, in contrast to a ground based, FS QKD network where daily light levels and environmental conditions can vary site-to-site and from hour-to-hour. This motivates a systematic study of how the secure key length varies with loss and extraneous count rates. For the design of realistic commercial systems, for example see [20], one must also consider fixing protocol parameters though operating in different environments. We examine such factors that are important to the deployment of a ground based QKD network.

For a real system, the signals are transmitted for a finite duration, and thus finite statistical effects are important to the performance. A particularly dramatic example was illustrated in figure 4, where increasing the integration time allowed extraction of a secure key in conditions where this was impossible for smaller integration times. Using a long integration times thus makes a system more robust.

For longer integration times, the secure key length was strongly affected by the probability of an extraneous count, e.g. from background light or a detector dark count. In particular, we found that when the rate of background counts is high, we can tolerate only low losses if we are to generate a secret key. This is an important design consideration. To allow for as large a loss budget as possible, we must reduce the

extraneous counts. For a ground based, FS QKD system, one should either operated in night conditions, or the receivers must be shielded from background light.

For a commercial QKD system, it would be difficult and expensive to customise all system parameters when deploying the system in different conditions. For example, the receiver basis choice is usually implemented with a passive beam-splitter, which will be fixed during production to reduce costs. Similarly, changing the WCP intensities for different locations or channel conditions would require adjustable components and systems, potentially increasing the cost. Adapting the intensities either on a site-by-site basis, or on a session basis adds considerable complication to deployment and operations, further increasing costs. In section 5 we showed that one can fix *both* the receiver's basis choice probability and the WCP intensities, and still extract a secure key over a wide range of different environmental conditions. We also found that a larger secure key is obtained by allowing the transmitters basis choice probability to differ from the receiver's, when the latter was fixed.

Finally, we investigated the effects of uncertainties in the fixed WCP intensities, where we allow for independent uncertainties in all four encoded signal states. If there is any uncertainties, then to ensure security, this needs to be factored in during the privacy amplification stage. We find that uncertainties reduce the secure key length. In particular, it can reduce the region of parameter space for which we can extract a secure key. In some cases the reduction can be of the order of 3–4 dB. As such it is vital to factor in these effects when designing any QKD system.

Acknowledgments

We acknowledge support from Innovate UK project AirQKD (Project Number: 45364). D K L Oi acknowledges support from the UK NQTP, the Quantum Technology Hub in Quantum Communications (EPSRC Grant Ref: EP/T001011/1), and the EPSRC Researchers in Residence Programme at the Satellite Applications Catapult (EPSRC Grant Ref: EP/T517288/1). The authors thank Gerald Bonner, Ross Donaldson, Yoann Noblet and Mike Parker for helpful discussions on the implementation of ground based FS QKD. We also thank Jasminder S Sidhu, Duncan McArthur and Roberto G Pousa for important discussion on simulating and optimizing efficient BB84 with WCPs.

Author contributions

TB developed code and contributed to modelling, discussions, and interpretations of the research. All authors contributed to writing the manuscript. DO developed the idea for the work and contributed to modelling, discussions, and interpretations of the research.

Data availability statement

All data is available on request from authors. SatQuMA code is released under the MIT Licence and is available at https://github.com/cnqo-qcomms/SatQuMA.

Appendix A. Examples of calculating loss budgets for QKD network design

The results presented in sections 4 and 5 can be used to design optical systems needed to realize a ground based, FS QKD. In particular, we can calculate the total loss budget allocated for the FS optics. We illustrate this by some simple examples.

Suppose we plan to setup a QKD link in an area that is prone to fog. The background light levels are measured at various times and used to estimate p_{ec}. At the site, the distance between the transmitter and receiver is 300 m; and the quantum source operates at 850 nm. Using MODTRAN 6 [44] we can calculate the losses due to scattering and absorption for this distance, during different weather conditions. The site is prone to advection fog with a visibility of 800 m, which at 300 m gives a loss of ≈6.4 dB from scattering and absorption.

If we can adapt our choice of both P_X^B and WCP intensities specifically for the site, then we can use the results presented in figure 5. For $p_{\mathrm{ec}} = 10^{-4}$ and $\mathrm{QBER_I} = 0.01$, $\ell > 0$ for values of η_{loss} up to and including $\eta_{\mathrm{loss}} = 22$ dB. Losses from sources other than scattering and absorption, such as from detectors, internal optics, diffraction, turbulence and pointing errors, must be no greater than 15.6 dB. The transmitter and receiver must thus be designed so as to keep these losses below about 15 dB. However, if the extraneous

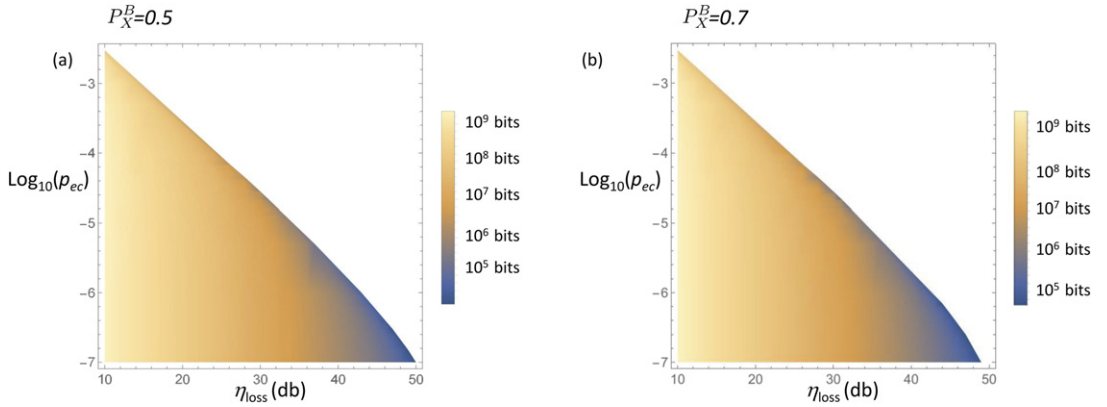

Figure 9. A 3D plot of ℓ plotted for total system loss η_{loss} and $\log_{10}(p_{\text{ec}})$. All plots are for $\text{QBER}_{\text{I}} = 0.01$ and an integration time of 30 min. The receiver basis choice probability is fixed to set values for both plots. In figure (a) $P_X^B = 0.5$ and in (b) $P_X^B = 0.7$.

counts can be reduced by a factor of 4, to $p_{\text{ec}} = 2.5 \times 10^{-5}$, by better design of the transmitter and receiver, then we can extract a key up to $\eta_{\text{loss}} = 26$ dB. This increases the loss budget for the design of the optics to 19.6 dB. This example illustrates that if the QKD link is to be robust to advection fog, then it is crucial to design the receiver and transmitter so as to reduce background light.

In the previous example we assumed that P_X^B and the WCP intensities can both be adapted to the location. In a future commercially deployed systems, such as that planned as part of the AirQKD project [20], both the receiver basis and the set of intensities will be fixed for all units. Furthermore, suppose the design brief requires each link to produce 50 256 bit AES keys every 10 min. For an integration time of 30 min, we need $\ell = 38\,400$ bits. As with the previous example, we assume that the link distance is 300 m and the source is at 850 nm. Furthermore, locations are chosen such that for night operation, p_{ec} is at most 10^{-6}. Using MODTRAN 6 [44], for an urban environment with link distance 300 m, the losses due to scattering and absorption are 0.6 dB. We fix the protocol parameters to $P_X^B = 0.5$, $\mu_1 = 0.5$, $\mu_2 = 0.1$ and $\mu_3 = 0$, which are the same as for plot 7. By assumption, the worst case is $p_{\text{ec}} = 10^{-6}$, for which $\ell > 38\,400$ for η_{loss} up to and including 42 dB. The total loss budget, minus absorption and scattering, is approximately 41 dB.

For $\eta_{\text{loss}} = 42$ dB, we produce over 125 800 bits of key. However, due to finite statistical effects, the key dips to below 38 400 bits for $\eta_{\text{loss}} = 42.5$ dB. If we operate the system right at the edge of the loss budget, then any unexpected increase in say pointing error due to strong winds, will lead to the system falling below its aim of producing 50 AES keys every 10 min. However, as we produce large amounts of key (125 800 bits for η_{loss}), we could store the excesses key. It is thus possible to smooth out any outages by designing the memory and the classical part of the cryptographic infrastructure, using knowledge of the protocol performance under different environmental conditions.

Appendix B. Additional result for different values of P_X^B

In section 5 we investigated fixing the receiver basis choice probability, P_X^B. We demonstrated that P_X^B can be fixed to either 0.3 and 0.9, and $\ell > 0$ for a wide range of values for p_{ec} and η_{loss}. The two values considered for P_X^B correspond to common commercially available beam-splitter splitting ratios. Two other common values are $P_X^B = 0.5$ and 0.7, which we now investigate for completeness. Figure 9 is a 3D plot of ℓ, plotted for η_{loss} and $\log_{10}(p_{\text{ec}})$. Both plots are for an integration time of 30 min and $\text{QBER}_{\text{I}} = 0.01$. In figure 9, (a) is for $P_X^B = 0.5$, while (b) is for $P_X^B = 0.7$. This plot demonstrates that one can obtain a secure key for a wide range of environmental conditions for many different fixed values of P_X^B.

We also investigated fixing both P_X^B and $\{\mu_1, \mu_2, \mu_3\}$. Even when fixing all these parameters, it was still possible to find values such that one could obtain secure key over a wide range of environmental conditions, as shown for $P_X^B = 0.5$ in figure 7. We can also obtain similar results for different values of P_X^B. In figure 10 we plot ℓ against $\log_{10}(p_{\text{ec}})$ and η_{loss}, for an integration time of 30 min and $\text{QBER}_{\text{I}} = 0.01$. In plot (a) $P_X^B = 0.3$, $\mu_1 = 0.785$, $\mu_2 = 0.0455$ and $\mu_3 = 0$, while in (b) $P_X^B = 0.7$, $\mu_1 = 0.50$, $\mu_2 = 0.10$ and $\mu_3 = 0$. The results demonstrate that one can obtain fixed intensities for different choice of P_X^B, which lead to large values of the secure key over wide ranges of environmental parameters.

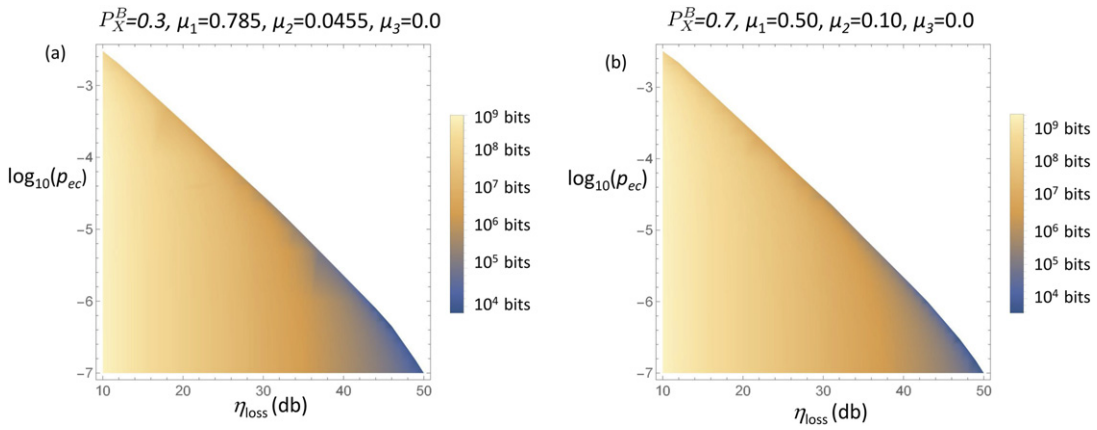

Figure 10. A 3D plot of ℓ plotted for total system loss η_{loss} and $\log_{10}(p_{\text{ec}})$. All plots are for $\text{QBER}_{\text{I}} = 0.01$ and an integration time of 30 min. Both the receiver basis choice probability and the source intensities are fixed to set values for both plots. In figure (a) $P_X^B = 0.3$, $\mu_1 = 0.785$, $\mu_2 = 0.0455$ and $\mu_3 = 0$, while in (b) $P_X^B = 0.7$, $\mu_1 = 0.50$, $\mu_2 = 0.10$ and $\mu_3 = 0$.

Table 2. A table showing the optimized values for P_X^A, when $P_X^B = 0.3$. All values are for $p_{\text{ec}} = 5 \times 10^{-5}$.

η_{loss} (dB)	P_X^B	P_X^A
18	0.3	0.979 64
20	0.3	0.965 25
22	0.3	0.956 72
24	0.3	0.943 19
26	0.3	0.912 83

Table 3. A table showing the optimized values for P_X^A, when $P_X^B = 0.5$. All values are for $p_{\text{ec}} = 5 \times 10^{-5}$.

η_{loss} (dB)	P_X^B	P_X^A
18	0.5	0.954 82
20	0.5	0.960 45
22	0.5	0.951 78
24	0.5	0.941 65
26	0.5	0.896 56

Appendix C. Sample optimized values for P_X^A, when P_X^B is fixed

In this appendix we present some optimized values for P_X^A when P_X^B is fixed. The fact that we allow Alice and Bob to have different basis probabilities is a novel feature of the current analysis. As such, it is worth presenting some results for how P_X^A changes. The results are presented in tables 2–5. All results correspond to an integration time of 30 min and $\text{QBER}_{\text{I}} = 0.01$.

A key feature in all tables is that the optimal secure key length is obtained for $P_X^A \neq P_X^B$. As a general trend, the value of P_X^A tends to decrease as η_{loss} increases. Intuitively, this occurs as for greater values of η_{loss} we have less overall data and thus less data in the Z-basis. To ensure we can perform parameter estimation without error, we need to increase the fraction of data in the Z-basis.

Appendix D. Proof that setting $P_X^A = P_X^B$ yields the optimal raw key length

In section 5 we argued that if P_X^B is fixed, then it is advantageous to allow $P_X^A \neq P_X^B$ and to optimize Alice's basis probability choice independently. Naively, this might be taken to suggest that we should always optimize both P_X^A and P_X^B independently. This, however, is not necessarily true. When *both* Alice and Bob's basis choices are free to vary, then it is sufficient to optimize $P_X = P_X^A = P_X^B$. This follows from the following observation. For any values for P_X^A and P_X^B, there exists a basis probability P_X that yields the same ratio of raw bits in each basis, but where the total sifted bits is greater than or equal to number of raw bits obtained with P_X^A and P_X^B. This means that the optimal raw key can always be found by using $P_X^A = P_X^B = P_X$.

Table 4. A table showing the optimized values for P_X^A, when $P_X^B = 0.7$. All values are for $p_{ec} = 10^{-6}$.

η_{loss} (dB)	P_X^B	P_X^A
32	0.7	0.923 12
34	0.7	0.908 46
36	0.7	0.871 79
38	0.7	0.866 05
40	0.7	0.805 77

Table 5. A table showing the optimized values for P_X^A, when $P_X^B = 0.9$. All values are for $p_{ec} = 10^{-6}$.

η_{loss} (dB)	P_X^B	P_X^A
32	0.9	0.913 67
34	0.9	0.897 87
36	0.9	0.868 97
38	0.9	0.784 94
40	0.9	0.721 54

Suppose we have particular values for P_X^A and P_X^B, where $P_X^A \neq P_X^B$. The fraction of bits retained after basis sifting is

$$F = P_X^A P_X^B + (1 - P_X^A)(1 - P_X^B). \tag{6}$$

The fraction of sifted bits in the X basis relative to the Z basis is $K = P_X^A P_X^B / [(1 - P_X^A)(1 - P_X^B)]$. Consider instead if Alice and Bob both had both chosen the X-basis with probability P_X. The fraction of sifted bits retained is $F' = P_X^2 + (1 - P_X)^2$. For the ratio of bits in each basis to be the same as before we need $P_X/(1 - P_X) = \pm\sqrt{K}$. This yields two values for P_X, we take the value $P_X = \sqrt{K}/(1 + \sqrt{K})$. One can show that

$$F' = \frac{1 + K}{(1 + \sqrt{K})^2}. \tag{7}$$

Equation (6) can be re-written in terms of K as: $F = (1 - P_X^A)(1 - P_X^B)[1 + K]$. Our proposition is false if there exists values for P_X^A and P_X^B such that $F > F'$. Using equation (7) and re-arranging, the condition $F > F'$ can be shown to be equivalent to

$$\sqrt{P_X^A P_X^B} + \sqrt{(1 - P_X^A)(1 - P_X^B)} > 1. \tag{8}$$

The right-hand side of the above equation is of the form of a scalar product between the two vectors: $(\sqrt{P_X^A}, \sqrt{1 - P_X^A})$ and $(\sqrt{P_X^B}, \sqrt{1 - P_X^B})$. From the Cauchy–Schwartz inequality, we have $(\sqrt{P_X^A}, \sqrt{1 - P_X^A}) \cdot (\sqrt{P_X^B}, \sqrt{1 - P_X^B}) \leqslant [P_X^A + 1 - P_X^A][P_X^B + 1 - P_X^B] = 1$. This implies that the inequality (8) can never be satisfied. But this means that the choice of P_X that leads to equation (7) can never yields a smaller total fraction of sifted bits than for $P_X^A \neq P_X^B$, i.e. $F' \geqslant F$. The raw key is thus greater than or equal to the original raw key.

Appendix E. Details for how p_{ec} and $\mathrm{QBER_I}$ contribute to the secure key length

The secure key length, ℓ, is calculated using equations (2), (3) and (5), together with equations (1)–(5) from [36]. The extraneous count probability, p_{ec}, and the intrinsic QBER, $\mathrm{QBER_I}$, induce the errors, which in turn affects ℓ. We detail the relationship in this appendix. The approach is the same as outlined in [40].

The average probability for a pulse of intensity $k \in \{\mu_1, \mu_2, \mu_3\}$ to produce a detection event is given by the equation

$$D_k = (1 + p_{ap})\left[1 - (1 - 2p_{ec})\right] \exp(-\eta_{loss} k). \tag{9}$$

The probability for a pulse of intensity k to yield a bit with an error is given by

$$e_k = p_{ec} + \frac{p_{ap} D_k}{2} + \mathrm{QBER_I}(1 - \exp[-\eta_{loss} k]). \tag{10}$$

The total number of pulses transmitted is the product of the integration time, τ, and the source's repetition rate, f_s.

If the channels parameter, such as η_{loss}, can vary with time, then we partition the integration time into time-slots of width $\Delta\tau$, where this is chosen such that the parameters are approximately constant over this time interval. The number of detection events in the X-basis within the jth time-slot are:

$$n_{X,k}^{(j)} = P_X^A P_X^B p_k D_k(j) f_s \Delta\tau, \tag{11}$$

where p_k is the probability to transmit a pulse with intensity k. The total number of detection events in the X-basis from pulses with intensity k is: $n_{X,k} = \sum_j n_{X,k}^{(j)}$ and the total number of detection events in the X-basis is $n_X = \sum_k n_{X,k}$. The results for the Z-basis have the same form, but with X swapped to Z.

The number of errors in the X-basis, within the jth time-slot, is

$$m_X^{(j)} = \frac{\sum_k p_k e_k(j) n_X^{(j)}}{\sum_k p_k D_k(j)}, \tag{12}$$

where $n_X^{(j)} = \sum_k n_{X,k}^{(j)}$. The total number of errors in the X-basis is $m_X = \sum_j m_X^{(j)}$. The fraction of errors resulting from a pulse of intensity k can be found by weighting $m_X^{(j)}$ by the term $p_k D_k(j)/[\sum_k p_k D_k(j)]$. Similar results can be found for the Z basis. These quantities can be used in equations (3) and (5) together with equations (1)–(5) of [36], to calculate the length of the secure key (2).

ORCID iDs

Thomas Brougham https://orcid.org/0000-0002-9066-1771
Daniel K L Oi https://orcid.org/0000-0003-0965-9509

References

[1] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Proc. IEEE Int. Conf. Comput., Syst. Signal Process* pp 175–9
[2] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 The security of practical quantum key distribution *Rev. Mod. Phys.* **81** 1301–50
[3] Wootter W and Loepp S 2006 *Protecting Information: From Classical Error Correction to Quantum Cryptography* 1st edn (Cambridge: Cambridge University Press)
[4] Hoffstein J, Pipher J and Silverman J H 2014 *An Introduction to Mathematical Cryptography* 2nd (New York: Springer) https://doi.org/10.100/978-1-4939-1711-2
[5] Shor P W 1999 Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer *SIAM Rev.* **41** 303
[6] Schmitt-Manderbach T *et al* 2007 Experimental demonstration of free-space decoy-state quantum key distribution over 144 km *Phys. Rev. Lett.* **98** 010504
[7] Wang J-Y *et al* 2013 Direct and full-scale experimental verifications towards ground-satellite quantum key distribution *Nat. Photon.* **7** 387–93
[8] Liao S-K *et al* 2017 Long-distance free-space quantum key distribution in daylight towards inter-satellite communication *Nat. Photon.* **11** 509–13
[9] Steinlechner F, Ecker S, Fink M, Liu B, Bavaresco J, Huber M, Scheidl T and Ursin R 2017 Distribution of high-dimensional entanglement via an intra-city free-space link *Nat. Commun.* **8** 15971
[10] Fedrizzi A, Ursin R, Herbst T, Nespoli M, Prevedel R, Scheidl T, Tiefenbacher F, Jennewein T and Zeilinger A 2009 High-fidelity transmission of entanglement over a high-loss free-space channel *Nat. Phys.* **5** 389–92
[11] Nauerth S, Moll F, Rau M, Fuchs C, Horwath J, Frick S and Weinfurter H 2013 Air-to-ground quantum communication *Nat. Photon.* **7** 382–6
[12] Takenaka H, Carrasco-Casado A, Fujiwara M, Kitamura M, Sasaki M and Toyoshima M 2017 Satellite-to-ground quantum-limited communication using a 50 kg class microsatellite *Nat. Photon.* **11** 502–8
[13] Liao S-K *et al* 2017 Space-to-ground quantum key distribution using a small-sized payload on Tiangong-2 space lab *Chin. Phys. Lett.* **34** 090302
[14] Xu F, Ma X, Zhang Q, Lo H-K and Pan J-W 2020 Secure quantum key distribution with realistic devices *Rev. Mod. Phys.* **92** 025002
[15] Liao S-K *et al* 2017 Satellite-to-ground quantum key distribution *Nature* **549** 43–7
[16] Yin J *et al* 2020 Entanglement-based secure quantum cryptography over 1120 kilometres *Nature* **582** 501
[17] Oi D K *et al* 2017 Cubesat quantum communications mission *EPJ Quantum Technol.* **4** 6
[18] Sidhu J S *et al* 2021 Advances in space quantum communications *IET Quantum Commun.* **2** 182–217
[19] Pirandola S *et al* 2020 Advances in quantum cryptography *Adv. Opt. Photon.* **12** 1012
[20] British Telecommunications Public Limited Company 2020 *UK Research and Innovation (UKRI)* https://gtr.ukri.org/projects?ref=45364
[21] Liorni C, Kampermann H and Bruß D 2019 Satellite-based links for quantum key distribution: beam effects and weather dependence *New J. Phys.* **21** 093055
[22] Vavoulas A, Sandalidis H G and Varoutas D 2012 Weather effects on FSO network connectivity *J. Opt. Commun. Netw.* **4** 734–40
[23] Lo H-K, Ma X and Chen K 2005 Decoy state quantum key distribution *Phys. Rev. Lett.* **94** 230504
[24] Ma X, Qi B, Zhao Y and Lo H-K 2005 Practical decoy state for quantum key distribution *Phys. Rev.* A **72** 012326
[25] Hayashi M and Nakayama R 2014 Security analysis of the decoy method with the Bennets–Brassard 1984 protocol for finite key lengths *New J. Phys.* **16** 063009

[26] Lucamarini M, Patel K A, Dynes J F, Fröhlich B, Sharpe A W, Dixon A R, Yuan Z L, Penty R V and Shields A J 2013 Efficient decoy-state quantum key distribution with quantified security *Opt. Express* **21** 24550–65
[27] Kamoun F, Chaabani H, Outay F and Yasar A-U-H 2020 A survey of approaches for estimating meteorological visibility distance under foggy weather conditions *Global Advancements in Connected and Intelligent Mobility: Emerging Research and Opportunities* ed F Outay, A Yasar and E Shakshuki (IGI Global) pp 65–92
[28] Brougham T and Oi D K L 2021 Medium-range terrestrial free-space QKD performance modelling and analysis *Proc. SPIE 11881, Quantum Technology* (Driving Commercialisation of an Enabling Science II) p 1188108
[29] Nauerth S, Fürst M, Schmitt-Manderbach T, Weier H and Weinfurter H 2009 Information leakage via side channels in freespace BB84 quantum cryptography *New J. Phys.* **11** 065001
[30] Henniger H and Wilfert O 2010 An introduction to free-space optical communications *Radioengineering* **19** 203
[31] Zhu X and Kahn J M 2002 Free-space optical communication through atmospheric turbulence channels *IEEE Trans. Commun.* **50** 8
[32] Hulea M, Ghassemlooy Z, Rajbhandari S and Tang X 2014 Compensating for optical beam scattering and wandering in FSO communications *J. Lightwave Technol.* **32** 1323–8
[33] Acosta V M, Dequal D and , Schiavon M *et al* 2021 Analysis of satellite-to-ground quantum key distribution with adaptive optics (arXiv:quant-ph/2111.06747)
[34] Hwang W-Y 2003 Quantum key distribution with high loss: toward global secure communication *Phys. Rev. Lett.* **91** 057901
[35] Brassard G, Lütkenhaus N, Mor T and Sanders B C 2000 Limitations on practical quantum cryptography *Phys. Rev. Lett.* **85** 1330 Lütkenhaus N and Jahma M 2002 *New J. Phys.* **4** 44
[36] Lim C C W, Curty M, Walenta N, Xu F and Zbinden H 2014 Concise security bounds for practical decoy-state quantum key distribution *Phys. Rev.* A **89** 022307
[37] Hoeffding W 1963 Probability inequalities for sums of bounded random variables *J. Am. Stat. Assoc.* **58** 13–30
[38] Zhang Z, Zhao Q, Razavi M and Ma X 2017 Improved key-rate bounds for practical decoy-state quantum-key-distribution systems *Phys. Rev.* A **95** 012333
[39] Yin H-L, Zhou M-G, Gu J, Xie Y-M, Lu Y-S and Chen Z-B 2020 Tight security bounds for decoy-state quantum key distribution *Sci. Rep.* **10** 14312
[40] Sidhu J S, Brougham T, McArthur D, Pousa R G and Oi D K L 2022 Finite key effects in satellite quantum key distribution *npj Quantum Inf.* **8** 18
[41] Lo H-K, Chau H F and Ardehali M 2005 Efficient quantum key distribution scheme and a proof of its unconditional security *J. Cryptol.* **18** 133–65
[42] Tomamichel M, Martinez-Mateo J, Pacher C and Elkouss D 2017 Fundamental finite key limits for one-way information reconciliation in quantum key distribution *Quantum Inf. Process.* **16** 280
[43] Renner R 2005 (arXiv:quant-ph/0512258)
[44] Berk A, Conforti P, Kennett R, Perkins T, Hawes F and van den Bosch J 2014 MODTRAN 6: a major upgrade of the MODTRAN radiative transfer code *Proc. SPIE 9088, Algorithms and Technologies for Multispectral, Hyperspectral, and Ultraspectral Imagery* vol XX
[45] Rice P and Harrington J 2009 (arXiv:quant-ph/0901.0013)
[46] Wang Y, Bao W-S, Zhou C, Jiang M-S and Li H-W 2016 Tight finite-key analysis of a practical decoy-state quantum key distribution with unstable sources *Phys. Rev.* A **94** 032335