Medium-range terrestrial free-space QKD performance modeling and analysis

Brougham T.[a] and Oi D. K. L. [a]

[a]SUPA Department of Physics, University of Strathclyde, Glasgow G4 0NG, UK

ABSTRACT

Medium-range terrestrial free-space quantum key distribution systems enable widespread secure networked communications in dense urban environments, where it would be infeasible to install a large number of short optical fibre links. Such networks need to perform over a wide range of conditions and their design has to balance key rate maximisation versus robust key generation over the greatest range of circumstances. Practicalities, such as manufacturability and deployment, further constrain the design space. Here, we examine challenges in translating experiment into engineering reality and identify efficient BB84 weak coherent pulse-decoy state protocol parameter regimes suitable for medium-range QKD systems considering likely system performance and environmental conditions.

Keywords: QKD, free-space optics

1. INTRODUCTION

Quantum key distribution (QKD) enables the distribution of cryptographic keys where, in principle, the security is based on the laws of physics.[1–3] Free-space (FS) implementations of QKD are currently being explored, for example a common approach is satellite QKD, which allows a secret key to be distributed over global distances.[4–7] An alternative application is terrestrial FS-QKD aimed at short range communication between fixed locations.[8,9] One motivation is the deployment of QKD networks in dense urban locations, where it is difficult to install new short range fibre links compatible with QKD operation. Instead, one could deploy a network of short range FS-QKD transmitters and receivers in a manner that is reminiscent of planned 5G networks. This approach is currently being explored in the AirQKD project funded by Innovate UK involving academic and industrial partners and led by BT.[10]

A real world FS-QKD network will need to operate in a diverse range of conditions.[11] It is thus important to study the performance of a system in different environmental settings. Furthermore, the transition from laboratory test system to commercially viable system brings many challenges. Apart from the uncontrolled environment conditions, another problem is the need for system cost reduction. It is common when designing a system to optimize operations, such as using particular protocol parameters, for fixed conditions. Different conditions would require changing the system parameters for best performance, for example changing the signal basis probabilities and the pulse intensities. To achieve this would require greater system and operational complexity hence increasing capital and service costs. This raises the question: is it possible to fix the basis probabilities and pulse intensities so as to allow the system to operate over a wide range of conditions? We will demonstrate that this is possible.

The aim of this work is not to model one particular FS setup or operating point, but instead to model the performance of a common QKD protocol under a diverse range of environmental conditions. These results can be used to inform the design of an FS-QKD system. For example, when designing the FS optics, one needs to know the *loss budget*, i.e. the total system loss one can tolerate, while still producing a secret key. The results we present allow the loss budget to be found given a range of expected background light levels. In these investigations, we find that finite data size of a real world systems leads to finite statistical effects in the

Further author information: (Send correspondence to T. Brougham.)
T. Brougham: E-mail: t.brougham@strath.ac.uk,
D. Oi: E-mail: daniel.oi@strath.ac.uk

parameter estimation stage. This leads to the secret key going to zero much quicker than expected. In particular, plots of the secret key length against total system loss show a sharp dropoff. We explore this important effect. Another key finding is to demonstrate that one can still extract secret key over a wide range of environmental conditions, even when the protocol parameters are fixed.

The outline of the manuscript is as follows. In section 2, we explain how we model the FS system and channel. In particular, we introduce the variables that characterize the system. In section 3 we explain the QKD protocol we analysis: efficient BB84 with decoy states.[12,13] This protocol was chosen as it has low sifting losses and is more efficient in situations where we have a finite data set.[14] Furthermore, the use of decoy states avoids the need for a single photon source. It has also been shown to increase the range of the system.[15] In section 4 we explore the system performance, when we can vary all system parameters. The system performance when parameters are fixed is investigated in section 5. Finally, the results are discussed in section 6.

2. THE SYSTEM

To construct a ground based FS-QKD network one needs multiple nodes that exchange a secret key with each other. The performance of the link between each node sets limits on the performance of the network. As such, we focus only on a single link of the FS-QKD network. A FS link is composed of transmitter (Alice) and receiver (Bob), as shown in Fig. 1. The transmitter will send key bits for a fixed time, known as the *integration time.* Each bit is encode on the polarization state of laser pulse. We use four different linear polarization states: horizontal, vertical, diagonal and anti-diagonal. For the secret key length, the important factor is the total number of pulses transmitted. This equals the product of the laser repetition rate and the integration time. We can thus vary the total number of pulses transmitted by either varying the repetition rate or the integration time. Throughout this manuscript, we keep the laser repetition rate fixed to 100 MHz and instead vary the integration time. Results for different repetition rates can be inferred from the presented results.

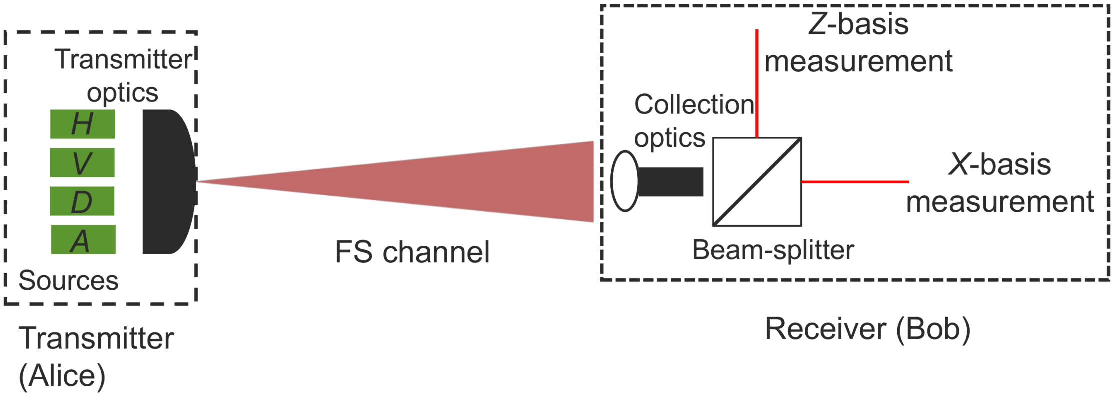

Figure 1. A schematic diagram showing a typical FS-QKD system. The transmitter (Alice) consists of 4 emitters of phase randomized weak coherent pulses of the following polarizations: horizontal (H), vertical (V), diagonal (D) and anti-diagonal (A). The signals are mode matched in their spatial, spectral, and temporal degrees of freedom to avoid side-channel information that can compromise security. The receiver (Bob) collects the photons using a suitable arrangement of optical elements (the collection optics). The beam-splitter chooses which polarization basis Bob will measure in (see section 3 for more details). We denote the $\{H, V\}$ ($\{D, A\}$) as the Z basis (X-basis)

In a FS optical system there are many sources of loss.[11] In the FS quantum channel, we have losses due to scattering, absorption, diffraction (geometrical) losses and turbulence. Additionally, there are also losses due to detector loss, internal optics, mode coupling to detectors and due to errors in beam tracking. The last source of loss could results from the swaying of the place the transmitter / receivers are mounted. We characterize all these loss combined together by introducing p_d, the probability that a transmitted photon is detected. From this we derive the total loss in decibels: total loss (dB) $= -10\log_{10}(p_d)$.

In addition to losses, there will be errors in the transmitted bits. One important source of errors is extraneous counts, which are detection events that don't come from a source photon. Extraneous counts result from detector dark counts and from stray photons (background photons). We characterize this by introducing p_{ec} the probability of a extraneous count. This can be calculated by recording the number of extraneous counts within some time-interval, when the source is not operating. Another source of errors is due to misalignments in the internal optics. We characterize this by introducing the internal quantum bit error rate $QBER_I$.[14,16] The final source of errors is due to after-pulsing. As we will be gating the detectors on and off, we should be able to keep this low. For all modeling, we assume the after-pulse probability is $p_{ap} = 10^{-3}$. A summary of the parameters that describe the system and source is given in table 1.

Table 1. A table showing the parameters that the describe the FS system. Variables with an asterisk by their name correspond to quantities that don't change in the modelling.

System variable	**Symbol**	**typical value**
Combined loss for whole system	total loss	10 - 50dB
Extraneous count probability	p_{ec}	10^{-7} - 3×10^{-3}
Intrinsic quantum bit error rate	$QBER_I$	0.005 - 0.01
After-pulse probability*	p_{ap}	10^{-3}
Laser repetition rate*	rep. rate	100MHz
Mean photon number per pulse	μ_j	10^{-9} - 1.0

3. EFFICIENT BB84 WITH DECOY STATES

In this section we explain the efficient BB84 protocol that we analysis.[12,16] Efficient BB84 is a variant on the original BB84 protocol.[1] One uses two polarization bases $X = \{H, V\}$ or $Z = \{D, A\}$, where H, V, D and A respectively mean horizontal, vertical, diagonal and anti-diagonal. Alice randomly chooses to encode in either the X or Z basis with probability $P(X)$ and $P(Z) = 1 - P(X)$. Bob then measures randomly in the X or Z basis, with probabilities $P(X)$ and $P(Z)$. This means that the basis reconciliation factor, i.e. the probability that both Alice and Bob use the same basis, is $P^2(X) + P^2(Z)$. In the original BB84 protocol, $P(X) = P(Z) = 1/2$. However, in efficient BB84, we allow $P(X)$ and $P(Z)$ to be differ and instead choose their values so as to maximize the secret key length. The advantage is before Alice and Bob would choose different bases with probability 1/2, where as in efficient BB84, this occurs with probability $2P(X)P(Z)$.

Rather than using a single photon source, we use weak coherent pulses (WCP), with a repetition rate of 100MHz. While the use of WCP brings benefits in terms of speed, range and cost, they introduce a new source of attack: the photon number splitting attack.[15] This attack takes account of the fact that a WCP has a non-zero probability to contain more than one photon. An attacker could siphon these additional photons without disturbing the polarization state of the photons. To protect against this attack, we need to precisely characterize the number of detector clicks arising from single photons and vacuum events. To achieve this we use WCP with three different intensity values: $\{\mu_1, \mu_2, \mu_2\}$, where μ_j is the mean photon number of the pulse. The estimation procedure requires that $\mu_1 > \mu_2 + \mu_3$ and $\mu_2 > \mu_3$. This is known as a decoy state protocol with two decoy states.[13,16] In spite of the term "decoy", all three WCP intensities have key bits encoded in them and can contribute to the secure key.

We now outline the steps of the protocol.[16]

1. Alice choose her encoding basis, either X or Z, and the intensity of her WCP. Let p_k be the probability that she choose intensity μ_k for her WCP. Recall, there are three possible intensities μ_j, $j = 1, 2, 3$ where $\mu_1 > \mu_2 + \mu_3$ and $\mu_2 > \mu_3$. Alice then encodes a key bits, 0 or 1, with equal probability on her chosen basis. A typical encoding scheme is $0 \rightarrow H$, $1 \rightarrow V$, $0 \rightarrow D$ and $1 \rightarrow A$.

2. Bob randomly chooses a basis to measure the transmitted WCP. In practice, the basis choice is made passively using a non-polarizing beam-splitter. The basis measurement can then be make using an appropriate arrangement of wave-plates and a polarizing beam-splitter.[3]

3. After all the pulses have been transmitted, Bob publicly announce in which time-slots he detected a photon and what basis he measured in. Alice then announces her basis choice and the WCP intensity, but not the value of the key bit.

4. Alice discards her bits corresponding to when Bob didn't record a detection. After this, both Alice and Bob discard the bits where they used different bases.

5. Alice and Bob then publicly announce their Z basis values, while keeping the X basis bits secret. The final secret key is constructed only from data collected in the X basis. The Z basis is used for estimation of the channel parameters: quantum bit error rate (QBER), single photon yield, vacuum yield and phase error (number of errors in detected single photon events).[16] When estimating these parameters, the finite nature of the statistics plays an important role. For more details on the finite statistical estimation see.[14]

6. Next error correction must be performed to obtain identical keys for Alice and Bob. Alice and Bob could estimate the QBER or use a simulate version as detailed in.[16] Either way, if the QBER is not too high, they can correct the errors using a one-way reconciliation protocol.[3, 17] This will require them to publicly exchange parity bits, which yields information to an eavesdropper. The amount of information leaked, λ_{EC}, can be estimated using the approach detailed in.[17] They will then perform a parity check to ensure they have the same raw key.[3] With high probability, they now share the same bit string.

7. Finally, Alice and Bob perform privacy amplification on their key.[7, 18]

The final secret has length, ℓ, which is given by the formula[16]

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

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 ϵ_c is the correctness parameter. The term ϕ_X is the phase error rate, i.e. due to eavesdropper induced errors corresponding to single photon events, and is estimated using data from the Z-basis. The function $h(\phi_X)$ is the binary entropy: $h(q) = -q\log_2(q) - (1-q)\log_2(1-q)$. The quantities $s_{X,0}$, $s_{X,1}$ and ϕ_X can be calculated using equations (1) to (5) from.[16] In that paper, there are correction terms due to finite statistical fluctuations in the quantities $n^{\pm}_{X(Z),k}$ and $m^{\pm}_{Z,k}$. It is possible to improve upon these result by using a modified version of the Chernoff bound[19, 20] that is outlined in detail in.[14] The security proof outlined in[16] uses the composable security framework, in which a protocol is said to be $\varepsilon = \epsilon_s + \epsilon_c$ secure if it is ϵ_c-correct and ϵ_s-secret.[18] For all calculations presented we use $\epsilon_c = 10^{-15}$ and $\epsilon_s = 10^{-9}$.

4. SYSTEM PERFORMANCE WHEN OPTIMIZING ALL PROTOCOL PARAMETERS

In this section we calculate the secret key length, ℓ, for a range of environmental conditions. To do this we optimize the secret key length by varying the following protocol parameters: $\{P(X), p_1, p_2, \mu_1, \mu_2\}$, where p_j is the probability to prepare the pulse with mean photon number μ_j. To help estimate the number of vacuum events, we need μ_3 to have a small value,[16] we thus set $\mu_3 = 10^{-9}$ for all modeling. We perform the optimization for different values of the total loss and p_{ec}. For details of the optimization procedure see.[14] A version of the code used, called SatQuMA, has been released.[21]

Consider an integration time of 60 seconds and $QBER_I = 5 \times 10^{-3}$. In Fig. 1 we plot a 2D heat map showing how the secret key length depends the total loss and p_{ec}. A secret key can be extracted for a wide range of losses, provided p_{ec} is small enough. The size of the secret key depends on the total loss and p_{ec}. For example, when the total loss is 25dB and $p_{ec} = 10^{-5}$, then $\ell = 2.80 \times 10^6$ bits. Additionally, for a total loss of 34dB and

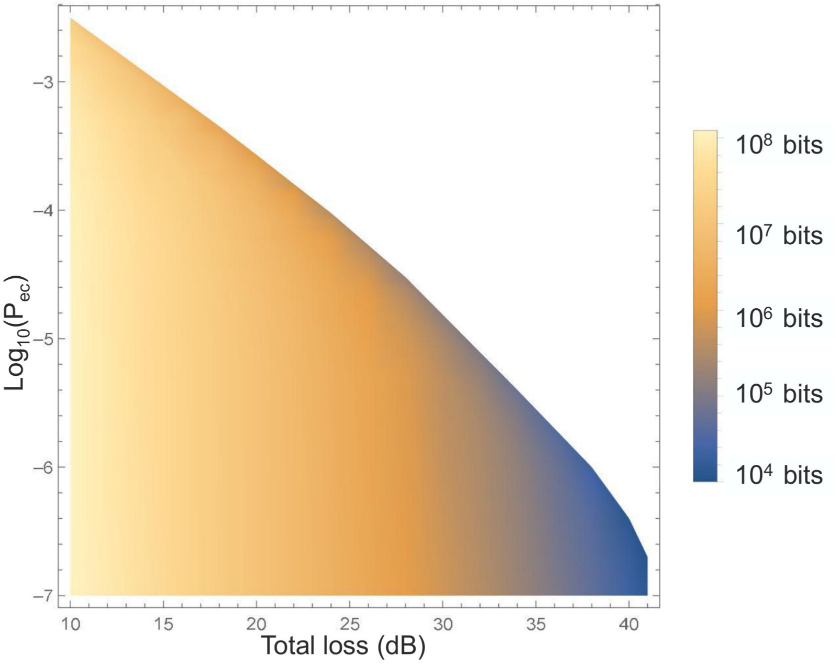

Figure 2. A plot showing values of the secret key for different values of the total loss and $\log_{10}(p_{ec})$, where p_{ec} is the probability of an extraneous count. The plot is for $QBER_I = 0.005$ and an integration time of 60 seconds.

$p_{ec} = 10^{-6}$, then $\ell = 1.43 \times 10^5$ bits. Notice that even for a loss as great as 34dB, we can still extract a key of the order of 10^5 bits.

One feature of Fig. 2 is the quick drop of in the secret key rate. For example, for $p_{ec} = 10^{-4}$, we have $\ell = 1.90 \times 10^6$ bits for a total loss of 22dB. But this drops to zero if we increase the loss by 2dB. To investigate this further, we plot individual curves for the the secret key length against total loss, for different values of p_{ec}. This is shown in Fig. 3 for $p_{ec} = 10^{-4}$, 10^{-5}, 10^{-6} and 10^{-7}. Here we see that the secret key length does indeed sharply drop to zero. This is seen clearly for both $p_{ec} = 10^{-4}$ and $p_{ec} = 10^{-5}$. This occurs because the phase error, ϕ_X, (the estimated error in single photon events), sharply increases. As the loss increases, one would expect the number of errors to increase. However, what is peculiar here is the sharp nature of the increase. One possible reason is due to errors in estimating ϕ_X. Following the process outlined in,[14,16] we take account of the finite sample size in our estimates. The finite sample size leads to large fluctuations in our estimates. For security reasons, if the estimated value of ϕ_X lies in a range of possible values, we must choose the worst possible value. Increasing the loss will both decrease the sample size and increase the fraction of bits with errors. The dramatic drop in the secret key length thus occurs when both the increase in errors and the finite statistical fluctuations conspire to give bad estimates of ϕ_X.

If the previous interpretation of the sharp drop-off in secret key is correct, then increasing the integration time should alleviate the problem. However, care must be taken when increasing the integration time. To understand why, consider the effect of doubling the integration time. This will double the sample size and one would naively expect this to double the secret key length. To avoid this issue, rather than investigating the secret key length we use the *secret key rate*, denoted as R. We define R to be the secret key per minute of integration time. Note the R defined here is *not* the asymptotic secret key rate, but includes inefficiencies due to finite sample size. In Fig. 4 we plot R against integration time, for $p_{ec} = 10^{-4}$, $QBER_I = 0.005$ and $\eta = 32$dB. Notice for an integration time of one minute, $R = 0$, i.e. we cannot extract a secret key. However, for larger integration times we can extract a secret key, and furthermore, R increases with time due to reduced finite-key effects. These features of Fig. 4 occurs because increasing the integration time increases the statistical sample. The fluctuations due to finite statistics will decreases as we increase the integration time. This suggests that we should always choose

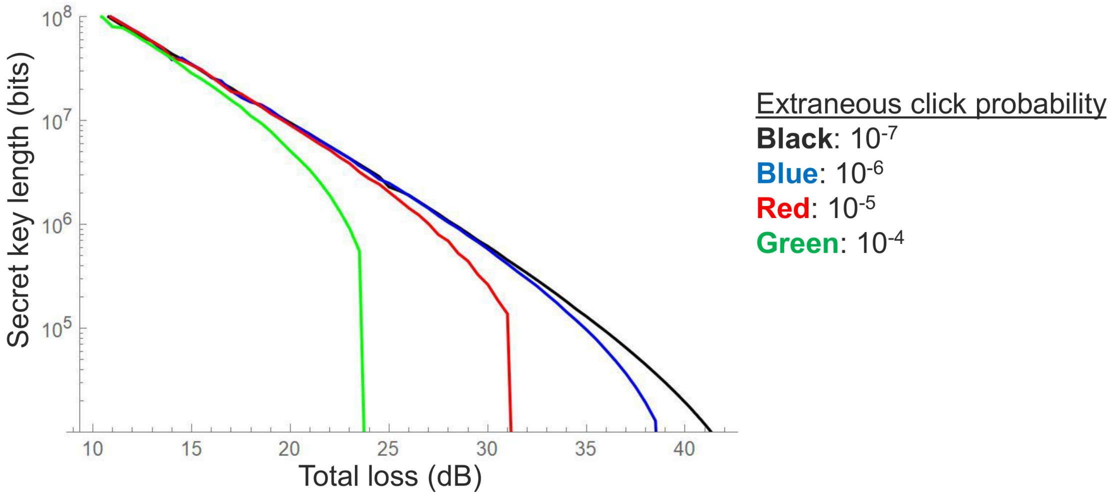

Figure 3. A plot the secret key length plotted against the total loss for different values of the extraneous count probability, p_{ec}. The black curve is for $p_{ec} = 10^{-7}$, the blue curve is for $p_{ec} = 10^{-6}$, the red curve is for $p_{ec} = 10^{-5}$ and the green curve is for $p_{ec} = 10^{-4}$. All curves are plotted with $QBER_I = 0.005$ and an integration time of 60 seconds.

the integration time to be as large as possible. In a realistic application, the integration time could be limited by the internal memory or by weather or some other environmental factor. Nevertheless, the results of this section stress the importance of using as large an integration time as possible.

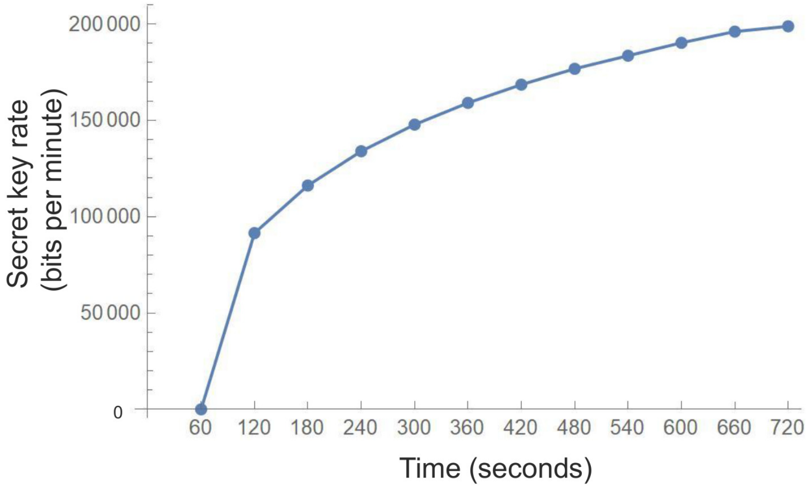

Figure 4. A plot showing the rate of secret key bits per minute, R, against the integration time. The curve is for $\eta = 32$ dB, $p_{ec} = 10^{-4}$ and $QBER_I = 0.005$. The curve shows that simply by increasing the integration time, we can go from $R = 0$ to extracting a secret key.

All of the results thus far have been for $QBER_I = 5 \times 10^{-3}$. Increasing the internal error will, as expected, decrease the secret key length. It would also be expected to decrease the region of values for p_{ec} and total loss, for where we can extract a secret key. This is again confirmed numerically. However, increasing $QBER_I$ to 0.01 does not significantly decrease the cut-off point for extracting a secret key, for loss up to 30dB. While $QBER_I = 0.005$ is not unrealistic for laboratory settings, using the increased value of 0.01 is preferable for modeling potential commercial systems with relaxed source and receiver quality demands.

5. SYSTEM PERFORMANCE WITH FIXED PARAMETERS

In the previous section all the results correspond to cases where we optimize the parameters $\{P(X), p_1, p_2, \mu_1, \mu_2\}$, for every different value of the total loss and p_{ec}. This is the best possible situation. However, in practice it might not be straightforward to vary each of these parameters. For instance, the optimal set of laser intensities $\{\mu_1, \mu_2, \mu_3\}$ are different for different extraneous counts levels and different losses. However, it is not enough to be able to change these values, we also need the new values to be stable and reliable. This would require a complex and expensive system. In practice, it would be preferable to find a fixed set of values for $\{\mu_1, \mu_2, \mu_3\}$ that provide a good secret key length under a wide range of different conditions.

A similar issues occurs for the receiver's basis choice. The transmitter can choose between different bases by having a set of different lasers for each encoding. For the receiver, a common approach is to make the basis choice passively using a beam-spitter, as illustrated in Fig 1. The splitting ratio of this beam-splitter is fixed and thus Bob cannot vary $P(X)$. The receivers basis probability must be fixed in our modeling. In standard efficient BB84, as explained in section 3, the transmitter and receiver basis choice probabilities are the same. However, it is easier for the transmitter to change their probability to choose a given basis. Suppose we allow the two probabilities to differ. Let $P^A(X)$ denote the transmitter (Alice's) probability to choose basis X, while $P^B(X)$ is the receiver (Bob's) probability to choose the basis X. To see why this could be an advantage, suppose $P^B(X) = 0.7$, and $P^B(Z) = 0.3$. For $P^A(X) = P^B(X)$, then about 15.5% of the sifted raw bits will be in the Z. If we operate the QKD system in an area where loss can increase, then we may find that an increase in the total loss will result in us not being able to extract a secret key. However, if $P^A(X) \neq P^B(X) = 0.7$, then we could increase $P^A(Z)$ so as to compensate for the loss and thus obtain sufficient bits to estimate the parameters reliably. The alternative would be to keep $P^A(X) = P^B(X)$, but then to alway choose $P^B(Z)$ large. This would, however, needlessly reduce the secret key length in times when the total loss is lower.

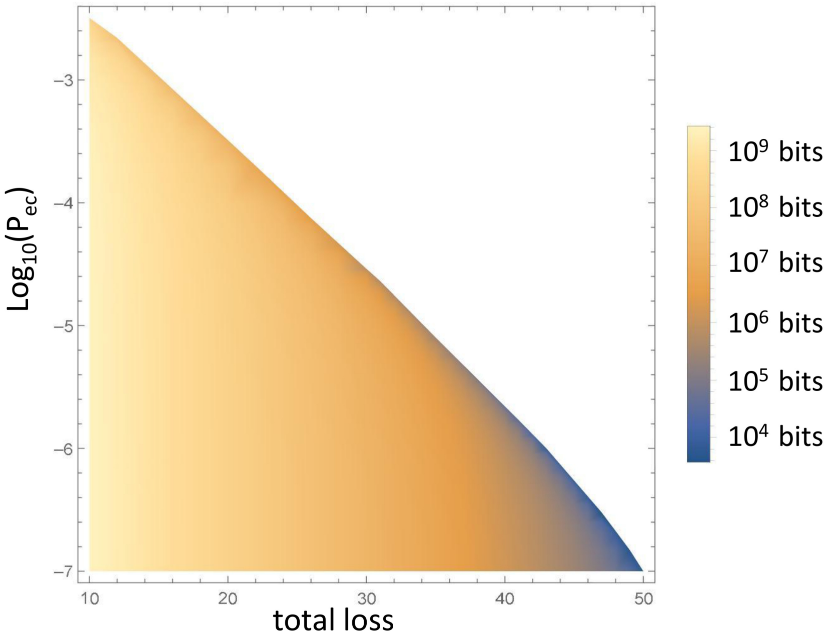

Figure 5. A plot showing values of the secret key for different values of the total loss and $\log_{10}(p_{ec})$, where p_{ec} is the probability of an extraneous count. The plot is for $P^B(X) = 0.7$, $\mu_1 = 0.5$, $\mu_2 = 0.1$ and $\mu_3 = 10^{-9}$; $QBER_I = 0.01$ and an integration time of 30 minutes.

The question we now examine is whether it is possible to fix $\{\mu_1, \mu_2, \mu_3\}$ and $P^B(X)$, and still extract a secret key over a wide range of environmental conditions. In the following calculations we optimize the secret key length by varying the parameters $\{P^A(X), p_1, p_2\}$, where p_j is the probability to prepare a pulse of intensity

μ_j. Following the discussion of last section, we choose a large value for the integration time, 30 minutes. The intrinsic QBER is taken to be $QBER_I = 0.01$, to account for greater errors in a non-laboritory setting. These values of integration time and $QBER_I$ are choose to match expected values used in modeling within the AirQKD project. We assume the transmitter uses a beam-splitter with 70-30 splitting ratio, such that $P^B(X) = 0.7$. By trial and error, we can obtain suitable values for the mean photon number of the pulses. In Fig. 5 we plot a 2D heat map showing how the secret key length depends on the total loss and p_{ec}. This plot was for $\mu_1 = 0.5$, $\mu_2 = 0.1$ and $\mu_3 = 10^{-9}$.

In Fig. 5, we see that one can extract a secret key for high losses. In fact, because the integration time is so large, we can extract a key up to 50dB. Notice also, that for $p_{ec} = 10^{-5}$, we can extract a secret key of 4.96×10^5 bits for a total loss of 34dB. The results demonstrate that we can fix both the laser intensities and the receiver basis probability, and still extract a secret key over a wide range of values for the total loss and p_{ec}. One point to address is whether allowing the receiver's basis to vary yields an advantage. In Fig. 5, we optimized the value of $P^A(X)$. Some sample optimized values are given in table 2. This shows that there is an advantage to letting $P^A(X)$ differ from $P^B(X)$, in this case. However, one must be careful in interpreting this observation. We have not shown that one should optimize *both* $P^A(X)$ and $P^B(X)$. Instead, we have argued that if $P^B(X)$ is fixed, then it is advantageous to allow $P^A(X) \neq P^B(X)$.

Table 2. A table showing the optimalized values for $P^A(X)$, when $P^B(X) = 0.7$.

Total loss (dB)	p_{e}	$P^A(X)$
18	5×10^{-5}	0.966
20	5×10^{-5}	0.957
22	5×10^{-5}	0.943
24	5×10^{-5}	0.919
26	5×10^{-5}	0.863

From table 2 we see that $P^A(X)$ is larger than $P^B(X)$. This suggests that for this value of p_{ec} and range of losses examined, we have fixed $P^B(X)$ at too low a value. We can find values for $P^A(X)$ that are lower than 0.7. For example, for $p_{ec} = 2 \times 10^{-6}$ and a total loss of 40dB, we find $P^A(X) = 0.579$. This suggests that for high losses, we might be better to have fixed $P^B(X)$ at a lower value. Nevertheless, the current results do show that one can fix protocol parameters and still obtain secret key over a rather wide range of losses and extraneous count levels.

One important application of the current results is in designing the FS optics for a FS-QKD system. If one is to achieve this we need to know the loss budget for the system. That is the total amount of loss we can tolerate while still extracting a secret key. Suppose we need to design a system to operate where the p_{ec} can vary from 10^{-4} to 10^{-5}. At the value of $p_{ec} = 10^{-4}$, we can extract a secret key for at most a loss of 22dB. While for $p_{ec} = 10^{-5}$, we can extract a key of 4.96×10^5, for a loss of 34dB, but no key for 35dB. The loss budgets in this case varies from 22-34dB, depending on the extraneous count rate.

6. CONCLUSION

Terrestrial FS-QKD networks are attractive for realizing short to medium range QKD networks, ideally suited for deployment within a dense urban environment where it would be expensive to build new custom fibre links. However, there are many challenges including the need to operate in a diverse range of environmental conditions and the desirability for reduced system complexity by using fixed system protocol and system parameters. The secure links still need to be robust against changing environmental conditions. Here, we have modeled a FS-QKD system using efficient BB84 and WCP with decoy states. We have presented performance results for different total losses and amounts of extraneous counts. This study will help with the design of FS optics needed to implement FS-QKD. For instance, if one can measure the typical background light levels, and thus p_{ec}, one can then determine the loss budget, i.e. the values of total loss one can tolerate and still extract a secret key.

One factor affecting the key length was the integration time. Intuitively, doubling the integration time should at least double the key length. We found, however, that the secret key rate can increase by more. This resulted from finite data effects within the estimation procedure. Increasing the integration time give a greater sample size and thus allowed the parameters to be estimated more reliably. This in turn increases the amount of secret key. The findings suggest that the integration time should be choosen to be as large as possible given the constraints of the system.

We also considered the effect of fixing the transmitters probability to choose a basis, $P^B(X)$. Additionally, we looked at fixing the set of laser intensities used in the decoy state protocol. We found that even with $P^B(X)$ and the intensities fixed, it was possible to chose values such that one could extract a secret key for a large range of different conditions. This is an important finding as in a real world system it would be difficult or expensive to vary $P^B(X)$ and the set of laser intensities. We also found that if the receiver basis probability is fixed, then it can still be advantageous to vary the transmitter basis probability. In many implementations, the transmitter basis choice is made by exciting different lasers, which prepare different polarization states. In contrast, the receiver basis choice is made by a fixed beam-splitter. It is thus possible to vary the transmitter basis probability is straightforward to fashion.

The results presented help with the design of commercially viable FS-QKD systems. Nevertheless, there are other factors that need further investigation. Firstly, one should investigate different values for $P^B(X)$. The one we presented was aimed at balancing performance in low and high loss regimes. However, if we know apriori that we will be working either high (or low) loss regime, then using a smaller (or larger) value for $P^B(X)$ could be advantageous. A more detailed study is required to evaluate the various trade-offs. Furthermore, we have not discussed the effect of uncertainties in the protocol parameters. The intensities of the WCPs need to be specified in the QKD protocol. Uncertainties in the intensities can be reduced by careful calibration in a laboratory setting. But in a commercial system operating in different environments, controlling uncertainties might not be easy. As such, it is important to study the effects of such uncertainties. The current authors will present such an analysis in a forthcoming manuscript. Nevertheless, the current work highlights that as QKD moves from the laboratory to real world deployment, it is vital to consider constraints that arise from the practicalities associated with manufacturability and deployment.

ACKNOWLEDGMENTS

We acknowledge funding from Innovate UK as part of AirQKD project-45364. We also thank our AirQKD collaborators at Fraunhofer UK Centre for Applied Photonics and Heriot-Watt for important discussions, especially G. Bonner, R. J. Donaldson and Y. Noblet. We also acknowledge very helpful discussions with our coFlleagues at Strathclyde: J. S. Sidhu, D. McArthur and R. G. Pousa. DKLO is supported by the EPSRC Quantum Communications Hub (EP/T001011/1) and is an EPSRC Researcher in Residence at the Satellite Applications Catapult (EP/T517288/1).

REFERENCES

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Proc. IEEE Int. Conf. Comput., Syst. Signal Process.* , pp. 175–179, 1984.

[2] V. Scarani, H. Bechmann-Pasquinucci, and et al., "The security of practical quantum key distribution," *Rev. Mod. Phys.* **81**, p. 1301, 2009.

[3] W. Wootter and S. Loepp, *Protecting Information: From Classical Error Correction to Quantum Cryptography*, Cambridge University Press, Cambridge, first ed., 2006.

[4] S. K. Liao, W. Q. Cai, W. Y. Liu, and et al., "Satellite-to-ground quantum key distribution," *Nature* **549**, pp. 43–47, 2017.

[5] J. Yin, Y.-H. Li, and et al., "Entanglement-based secure quantum cryptography over 1,120 kilometres," *Nature* **582**, p. 501, 2020.

[6] D. K. L. Oi, A. Ling, G. Vallone, and et al., "Cubesat quantum communications mission," *EPJ Quantum Technol.* **4**, p. 6, 2017.

[7] S. Sidhu, S. K. Joshi, M. Gündoğan, T. Brougham, D. Lowndes, L. Mazzarella, and et al., "Advances in space quantum communications," *IET Quant. Comm.* , pp. 1–36, 2021.

[8] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, and et al., "Entanglement-based quantum communication over 144 km.," *Nature Phys* **3**, p. 481–486, 2006.

[9] H. Chun, I. CIhoi, G. Faulkner, and et al., "Handheld free space quantum key distribution with dynamic motion compensation," *Opt. Express* **25**, pp. 6784–6795, 2017.

[10] "UK Research and Innovation, project - AIRQKD." https://gtr.ukri.org/projects?ref=45364.

[11] C. Liorni, H. Kampermann, and D. Bruß, "Satellite-based links for quantum key distribution: beam effects and weather dependence," *New J. Phys.* **21**, p. 093055, 2019.

[12] H.-K. Lo, H. F. Chau, and M. Ardehali, "Efficient quantum key distribution scheme and proof of its unconditional security," *J. of Cryptology* **18**, p. 133–165, 2005.

[13] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Phys. Rev. A* **72**, p. 012326, 2005.

[14] J. S. Sidhu, T. Brougham, D. McArthur, R. G. Pousa, and D. K. L. Oi, "Finite key effects in satellite quantum key distribution," *arXiv:2012.07829* , 2020.

[15] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Phys. Rev. Lett.* **91**, p. 057901, 2003.

[16] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, "Concise security bounds for practical decoy-state quantum key distribution," *Phys. Rev. A* **89**, p. 022307, 2014.

[17] M. Tomamichel, J. Martinez-Mateo, C. Pacher, and D. Elkouss, "Fundamental finite key limits for one-way information reconciliation in quantum key distribution," *Quantum Inf. Process* **16**, p. 280, 2017.

[18] R. Renner, "Security of quantum key distribution." PhD thesis, quant-ph/0512258. 2006.

[19] Z. Zhang, Q. Zhao, M. Razavi, and X. Ma, "Improved key-rate bounds for practical decoy-state quantum-key-distribution systems," *Phys. Rev. A* **95**, p. 012333, 2017.

[20] H. L. Yin, M. G. Zhou, J. Gu, Y. M. Xie, Y. S. Lu, and Z. B. Chen, "Tight security bounds for decoy-state quantum key distribution," *Sci. Rep.* **10**, p. 14312, 2020.

[21] J. S. Sidhu, T. Brougham, D. McArthur, R. G. Pousa, and D. K. L. Oi, "Satellite quantum modelling & analysis software version 1.0: Documentation," *arXiv:2109.01686* , 2021.