Currently, quantum key distribution (QKD) using continuous variable (CV) technology has only been demonstrated over short-range terrestrial links. Here we attempt to answer whether CV-QKD over the much longer satellite-to-Earth channel is feasible. To this end, we first review the concepts and technologies that will enable CV-QKD over the satellite-to-Earth channels. We then consider, in the infinite key limit, the simplest-to-deploy QKD protocols, the coherent state (CS) QKD protocol with homodyne detection and the CS-QKD protocol with heterodyne detection. We then focus on the CS-QKD protocol with heterodyne detection in the pragmatic setting of finite keys, where complete security against general attacks is known. We pay particular attention to the relevant noise terms in the satellite-to-Earth channel and their impact on the secret key rates. In system set-ups where diffraction dominates losses, we find that the main components of the total excess noise are the intensity fluctuations due to scintillation, and the time-of-arrival fluctuations between signal and local oscillator. We conclude that for a wide range of pragmatic system models, CS-QKD with information-theoretic unconditional security in the satellite-to-Earth channel is feasible.

I. INTRODUCTION

Quantum key distribution (QKD) provides unconditionally secure key distribution between two parties. Local data sent by a sender, Alice, is encrypted using a key that is guaranteed by quantum mechanics to be securely shared only with the receiving party, Bob. QKD is mainly implemented using optical technology, making it ideal for secure key distribution over a high bandwidth free-space optical (FSO) link.

In discrete variable (DV) QKD applied over fibre the quantum information is usually encoded in a DV of a single photon (e.g. time-bin qubit), with a secure range of order 400 km [1]. However, recently, DV-based QKD using polarization as the DV was demonstrated in a free-space satellite-to-ground channel up to a distance of 1200 km [2]. In [2], a quantum link was established from the low-Earth-orbit (LEO) Micius satellite to the Xinglong ground station. This exciting development is a major step towards realizing global scale secure quantum communications using low-orbit satellites. Indeed, quantum communication through satellite channels is anticipated to be one of the core technologies enabling the so-called quantum internet [3].

However, it is uncertain whether DV or continuous variable (CV) multiphoton technologies (or a combination of CV-DV) will prevail in free-space optical quantum communication. CV protocols have the advantage of high-rate, efficient and cost-effective detection (using homodyne and heterodyne detectors) in comparison to the sophisticated and expensive single-photon detectors used for DV protocols. CV-QKD is also perhaps more compatible with current classical wireless communications technologies. Initially, CV-QKD was proposed with discrete and Gaussian encoding of squeezed states [4–7]. Thereafter, Gaussian-modulated CV-QKD with coherent states was soon developed [8–10].

The simplest-to-deploy CV-QKD protocols are the GG02 protocol introduced in 2002 by Grosshans and Grangier using a homodyne detector [9, 10], and its heterodyne variant (“the no-switching” protocol) [11]. These both involve preparation of a coherent state (CS) using Gaussian modulation [7, 8]. More specifically, the quadratures $X$ and $P$ of the coherent state are randomly modulated according to a Gaussian distribution [8]. In this paper, we refer to GG02 and the no-switching protocol as the CS-Hom protocol and CS-Het protocol, respectively. We state them as the CS-QKD protocols when we refer to them collectively. The CS-QKD protocols have been successfully deployed in fibre with non-zero quantum keys distributed over distances of order 100 km [8, 12, 13].

The question we address in this work is whether the simplest-to-deploy CV-QKD protocols, namely the CS-QKD protocols, will be viable in a real-world LEO satellite-to-Earth channel. Although extensive theoretical work on CV-QKD through terrestrial FSO channels has been done in recent years, e.g. [14–21], the only real-world FSO deployment of any CV-QKD protocol has been over the short distance of 460 m [22]. The larger losses due to diffraction over the much longer satellite-to-Earth channel (as well as disparate turbulence effects) render any extrapolation of the results in [22] far from obvious. This is compounded by the fact that [22] deployed a different form of CV-QKD, namely, a CS uni-dimensional CV-QKD protocol.

Our contributions in this work can be summarized as follows. We identify the most important factors contributing to the total excess noise of the CS-QKD proto-
ocols in the satellite-to-Earth channel. We pay particular
attention to the noise contributions arising from scintillation
and contributions arising from time-of-arrival fluctuations
between the transmitted local oscillator (LO) and the quantum signal. Using our determination of the total excess noise we then consider a lower bound on the secure
key rates anticipated for the CS-QKD protocols deployed
over the satellite-to-Earth channel. We will consider se-
crete rates in the asymptotic signalling limit for both of
the CS-QKD protocols, and in the finite key limit for the
CS-Het protocol.1

The rest of this work is as follows. In Section II we
review the security models required for calculating the
secret key rate of the CS-QKD protocols in a lossy chan-
nel. In Section III we introduce the system model of the
CS-QKD protocols in the satellite-to-Earth channel, and
review well-known contributions to the total excess noise
from the channel and detectors. In Section IV we simu-
late the relative intensity fluctuations and time-of-arrival
fluctuations. In Section V we investigate the impact on
the secret key rate of each noise term. In Section VI we
discuss the security of the CS-QKD protocols in the satellite-to-Earth channel and discuss alternative proto-
cols. Finally, we conclude and summarize our findings in
Section VII.

II. SECURITY ANALYSIS OF CS-QKD IN A
LOSSY CHANNEL

In our security model of the CS-QKD protocols in the
satellite-to-Earth channel, we assume the eavesdropper
Eve has full access to the quantum channel and per-
forms the most general (coherent) attack. The general
attack is when Eve prepares an optimal global ancilla
state, which may not necessarily be separable. Eve can
prepare any ancillary states to interact with the signal
states and make measurements. In particular, Eve can
have access to a quantum memory, which can store the
signal states until she learns information during the clas-
sical post-processing. In our security model, we perform
the analysis in the entanglement based (EB) version of
the CS-QKD protocols, even though in deployment we
will assume the equivalent prepare and measure (PM)
schemes [24, 25]. In deployment, it is straightforward to
convert measurements from one scheme to the other [24].

Unconditional security against the general attack for
the CS-QKD protocols was proven in the asymptotic limit
where an infinite key was assumed [26]. The general at-
tack was proven to reduce to the collective attack using
the de Finetti representation theorem for infinite dimen-
sions [27]. However, in practice, we need to consider the
secret key rate in the finite limit which can only be

1 Currently, a formal proof of security in the finite limit for the
CS-Hom protocol is unavailable.

$\epsilon$-secure, where $\epsilon$ is the probability of failure. Uncon-
tditional security of the CS-Hom protocol in the finite regime is still an open question. However, by exploiting
a new Gaussian de Finetti reduction method, a compos-
able security proof against general attacks for the CS-Het
protocol was recently proven [28].

A. Asymptotic limit

In this section, we review the well-known secret key
rates under general attacks in the asymptotic limit
(which always provides key rates higher than those ob-
tained under general attacks in the finite limit). We
will follow the formalism provided in [29] and references
therein. The covariance matrix describing the Gaussian
modulated coherent state sent from Alice (A) to Bob (B)
has the form,

$$
\gamma_{AB} = \begin{pmatrix}
\sigma_z & \sqrt{\sigma_z} \\
\sqrt{\sigma_z} & I
\end{pmatrix},
$$

(1)

where $I = \text{diag}(1,1)$ is the unity matrix and
$\sigma_z = \text{diag}(1,-1)$ is the Pauli matrix. For the Gauss-
ian modulated CS-QKD protocols, the coefficients of the
covariance matrix are

$$
a = V_A + 1,
$$

$$
b = V_B \frac{\eta_d T}{\mu} (V_A + \chi(T, \eta_d) + 1),
$$

$$
c = \sqrt{\frac{\eta_d T}{\mu}} \sqrt{V_A^2 + 2V_A},
$$

where $V_A$ is Alice’s modulation variance of the quadra-
ture operators, $V_B$ is Bob’s measured quadrature vari-
ance, $0 \leq T \leq 1$ is the transmissivity of the channel, and
$\eta_d$ is the detector quantum efficiency.$^2$ The CS-Hom and
CS-Het protocols correspond to $\mu = 1$ and $\mu = 2$, respec-
tively. The term $\chi(T, \eta_d)$ is defined as all noise terms
other than vacuum noise, expressed in vacuum units. In
the literature it is common to distinguish between noise,
$\chi_d(\eta_d)$, arising from the detector and noise, $\chi_{ch}(T)$, aris-
ing from the channel transmission where [29],

$$
\chi(T, \eta_d) = \chi_{ch}(T) + \frac{\chi_d(\eta_d)}{T},
$$

(3)

and where $\chi_{ch}(T)$ is given by

$$
\chi_{ch}(T) = \frac{1 - T}{T} + \xi_{ch}.
$$

(4)

Here, $\xi_{ch}$ is the channel excess noise from various sources
and $(1 - T)/T$ is due to channel loss. $\chi_d(\eta_d)$ is given by

$$
\chi_d(\eta_d) = \frac{\mu - \eta_d}{\eta_d} + \frac{\mu \xi_d}{\eta_d},
$$

(5)

2 We implicitly assume in all calculations that the vacuum noise
is normalized to 1 by setting $\hbar = 2$. 

---
where $\xi_d$ is the detector excess noise and $(\mu - \eta_d)/\eta_d$ is noise due to detector losses.

The secret key rate$^3$ against general attacks (in bits/pulse) under reverse reconciliation in the asymptotic limit (infinite key length) is given by [29,31]

$$K = \beta I_{AB} - S_{BE},$$

(6)

where $I_{AB}$ is the mutual information between Alice and Bob, $0 \leq \beta \leq 1$ is the reconciliation efficiency, and $S_{BE}$ is the upper bound to the Holevo information between Eve and Bob. In this work we will only consider reverse reconciliation where Bob sends correction information to Alice who corrects the bit values in the key (derived from her quadrature measurement) [32]. The mutual information $I_{AB}$ for the CS-QKD protocol is given by

$$I_{AB} = \frac{\mu}{2} \log_2 \frac{V_A + 1 + \chi(T, \eta_d)}{1 + \chi(T, \eta_d)}.$$  

(7)

Note that from this point forward, we simplify the nomenclature with $\chi(T, \eta_d) := \chi_t$, $\chi_{cb}(T) := \chi_{cb}$ and $\lambda_2(T, \eta_d) := \chi_d$. Note also, the mutual information becomes

$$I_{AB} = \frac{\mu}{2} \log_2 \frac{\eta d T}{\mu} (V_A + \xi_{cb}) + \xi_d + 1,$$

(8)

and in the limit $T \to 0$, $I_{AB(T \to 0)} = \frac{\mu}{2} \log_2 \frac{V_A + \xi_{cb}}{\xi_d + 1}$, as expected.

We use the trusted model throughout the paper, where Eve can only have access to the channel excess noise $\chi_{cb}$. Consequently, in the Holevo information shared between Eve and Bob in [30], we only consider $\chi_{cb}$. Eve’s information after Bob’s measurement is the upper bound on the Holevo information,

$$S_{BE} = S(E) - S(E|B),$$

(9)

where $S(E)$ is the von Neumann entropy of Eve’s state before the measurement on mode $B$ (Bob’s mode) and $S(E|B)$ is conditioned on Bob’s measurement outcome. Eve is assumed to purify the transmitted state $AB$ resulting in a pure Gaussian state. It was shown that for a given covariance matrix describing a Gaussian state, Gaussian attacks are the most optimal attacks that minimize the key rates [33]. Therefore, Eve’s entropy is

$$S(AB) = G(\lambda_1 - \frac{1}{2}) + G(\lambda_2 - \frac{1}{2}),$$

(10)

where $G(x) = (x + 1) \log_2 (x + 1) - x \log_2 x$ and $\lambda_{1,2}$ are the symplectic eigenvalues of the covariance matrix $\gamma_{AB}$.

For CS-QKD protocols, these are given by [29]

$$\lambda_{1,2} = \sqrt{\frac{A' \pm \sqrt{A'^2 - 4B'}}{2}},$$

where

$$A' = (V_A + 1)^2 (1 - 2T) + 2T + T^2 (V_A + 1 + \chi_{cb}),$$

$$B' = T^2 ((V_A + 1)(\chi_{cb} + 1)^2),$$

(11)

and the entropy $S(E|B)$ is

$$S(E|B) = G(\frac{\lambda_3 - 1}{2}) + G(\frac{\lambda_4 - 1}{2}) + G(\frac{\lambda_5 - 1}{2}),$$

(12)

where $\lambda_{3,4,5}$ are the symplectic eigenvalues of the conditional covariance matrix characterizing the state after Bob’s measurement. The eigenvalues $\lambda_{3,4}$ are given by,

$$\lambda_{3,4} = \sqrt{\frac{C' \pm \sqrt{C'^2 - 4D'}}{2}},$$

(13)

where for the CS-Hom protocol $C'$ and $D'$ are given by

$$C'_{hom} = \frac{A' \chi_d + (V_A + 1) \sqrt{B'} + T(V_A + 1 + \chi_{cb})}{T(V_A + 1 + \xi)},$$

$$D'_{hom} = \frac{\sqrt{B'} V_A + 1 + \sqrt{B'} \chi_d}{T(V_A + 1 + \chi)},$$

(14)

respectively, and for the CS-Het protocol $C'$ and $D'$ are given by

$$C'_{het} = \frac{1}{T^2(V_A + 1 + \chi)} [A' \chi_d^2 + B + 1 + 2 \chi_d ((V_A + 1) \sqrt{B'} + T(V_A + 1 + \chi_{cb})) + 2T(V_A^2 + 2V_A)],$$

$$D'_{het} = \frac{(V_A + 1 + \sqrt{B'} \chi_d)^2}{T(V_A + 1 + \chi)},$$

(15)

respectively. Note, $\lambda_5 = 1$ for both protocols. Using [6] and [10-15], it is then straightforward to calculate the secret key rate in the asymptotic limit.

### B. Finite key size effects

We now consider the practical security of the CS-QKD protocols using finite-size analysis. In the security analysis, we consider the Gaussian collective attacks with $\epsilon$-security that was first introduced in [31,35] and extended to general attacks in [28,36,35]. In the infinite limit the knowledge of the relevant parameters are exact, but in the finite limit the parameters are estimated with a finite precision. This precision is related to the probability $\Delta_{PE}$; the true values are not inside the confidence interval calculated from the parameter estimation procedure [31,35]. In the finite limit, the secret key rate in bits/pulse is given by [37]

$$K = \frac{n}{N} (\beta I_{AB} - S_{BE}) - \frac{\sqrt{n}}{N} \Delta_{ABP}(n) - \frac{2}{N} \log_2 \frac{1}{2\epsilon},$$

(16)

$^3$ When we refer to “secret key rate” in this paper, we actually mean a lower bound on the rate.
where \( \epsilon \) is the total failure probability of the protocol, \( S_{BE}^{PE} \) is the upper bound of the Holevo information taking into consideration the finite precision of the parameter estimation, \( N \) is the total number of symbols sent, and \( n = N - n_e \), where \( n_e \) is the number of symbols used for parameter estimation. \( \Delta_{AEP}(n) \) is given by [36, 37]

\[
\Delta_{AEP}(n) = (d + 1)^2 + 4(d + 1)\sqrt{\log_2(2/\epsilon_s)} + 2\log_2(2/(\epsilon^2\epsilon_s)) + 4\epsilon_s d/(\epsilon\sqrt{n}),
\]

where \( d \) is the discretization parameter\(^4\) and \( \epsilon_s \) is a smoothing parameter corresponding to the speed of convergence of the smooth min-entropy. In the finite-size regime, one is limited to \( \epsilon \)-security where \( \epsilon = \epsilon_{EC} + 2\epsilon_s + \epsilon_{PA} + \epsilon_{PE} \), where \( \epsilon_{PA} \) is the failure probability of the privacy amplification procedure, and \( \epsilon_{EC} \) is the failure probability of the error correction. The parameters \( \epsilon_s \) and \( \epsilon_{PA} \) can be optimized computationally [34].

To account for the finite statistics and obtain the value of \( S_{BE}^{PE} \), the previous covariance matrix [2] for Alice and Bob becomes [34, 35].

\[
\gamma_{AB}^{PE} = \begin{pmatrix}
(V_A + 1)I & \sqrt{T_{min}/2} \sqrt{V_A^2 + 2V_A\sigma_z} \\
\sqrt{T_{max}/2} \sqrt{V_A^2 + 2V_A\sigma_z} & (T_{min}/2)(V_A + \xi_{max}) + 1 + \xi_d)
\end{pmatrix},
\]

where \( T_{min} \) and \( \xi_{max} \) are the minimum and maximum values of \( T \) and \( \xi_{ch} \), respectively.

The confidence intervals for \( T \) and \( \xi \) can be calculated from known distributions of the estimators\(^5\) \( \hat{t} \) and \( \hat{\xi} \) to obtain the lower value of the \( T \) interval given by [34, 35],

\[
T_{min} = \left( \hat{t} - z_{\epsilon_{PE}/2}/\hat{\xi} \right)^2,
\]

and the higher value of the \( \xi_{ch} \) interval given by,

\[
\xi_{max} = \left( \hat{\xi}^2 + z_{\epsilon_{PE}/2}/\hat{\xi} \right)^2 - 1 - \xi_d)/\hat{\xi}^2,
\]

where \( z_{\epsilon_{PE}/2} \) satisfies \( 1 - \text{erf}(z_{\epsilon_{PE}/2}/\sqrt{2}) = \epsilon_{PE} \) and \( \text{erf}(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-t^2} dt \). From a theoretical perspective and what we do in this work, we can set the expectation values of the estimators to

\[
E[\hat{t}] = \sqrt{n\eta T},
E[\hat{\xi}^2] = T\eta_d\xi_{ch} + 1 + \xi_d.
\]

Using these values, we can compute \( T_{min} \) and \( \xi_{max} \). To determine \( S_{BE}^{PE} \) in (16) for the CS-Het protocol, we use these values in equations [2]–[13] and [15] (i.e. setting \( T = T_{min} \) and \( \xi_{ch} = \xi_{max} \) in equations [2]–[5]). The mutual information \( I_{AB} \) in (16) is calculated as done before in [7] using \( T \) and \( \xi_{ch} \). Putting all this together, to calculate the secret key rate with finite size effects in (16), we make use of the aforementioned quantities \( S_{BE}^{PE}, I_{AB}, \) and \( \Delta_{AEP}(n) \) in (17).

In going from optimal Gaussian collective attacks to general attacks, only the CS-Het protocol is \( \epsilon \)-secure against general attacks with \( \epsilon' = \frac{\epsilon}{4\alpha} \epsilon \), where [28]

\[
\kappa = \max\{1, n(d_A + d_B)(1 + 2\sqrt{[(\ln(8/\epsilon))/2n]} + (\ln(8/\epsilon)/n)(1 - 2\sqrt{[(\ln(8/\epsilon)/2k)]}) \},
\]

where \( d_A \) and \( d_B \) are the average photon numbers of Alice and Bob’s modes respectively, and \( k \) is the number of modes [28]. However, \( \kappa \approx n \) and thus \( \epsilon \approx \frac{n}{4\alpha} \epsilon' \). We choose \( \epsilon' = 10^{-9} \) and number of symbols used for parameter estimation\(^6\) \( n_e = n = 10^{12} \) which can be obtained in minutes for a source pulse rate of 100 MHz. To obtain the secret key rate under general attacks, it is enough to analyze the security against Gaussian collective attacks with \( \epsilon = 10^{-55} \) and \( \epsilon_{EC} = \epsilon_s = \epsilon_{PA} = \epsilon_{PE} \) [28].

### III. Satellite-to-Earth CS-QKD

We present our system model in Fig. 1. Essentially, a Gaussian modulated coherent state is prepared on the satellite (Alice) and measured at the ground station (Bob) using homodyne or heterodyne detection. At Alice’s location in a LEO satellite at altitude \( H \), a strong laser source generates a coherent state which is divided by an asymmetrical beamsplitter into the local oscillator (LO) and the signal path. The laser source generates pulses at central frequency \( \omega_0 \) of width \( \tau_0 \) and a repetition rate \( f_{rep} \). The laser beam is collimated by a transmitter aperture of diameter \( D_T \). The amplitude and phase corresponding to \( X \) and \( P \) quadratures in the signal path are Gaussian modulated with the Gaussian distribution centred at \( \langle X \rangle = \langle P \rangle = 0 \) with variance \( V_A \).

The LO is then multiplexed with the signal (in a different polarization mode) and sent to Bob. Both the LO and signal are received by an aperture of diameter \( D_R \). Using the LO, Bob monitors the transmissivity \( T \) which has a probability density function PDF \( P_{AB}(T) \) of the channel. The PDF is integrated up to a maximum possible value of \( T = T_{max} \). In general, the form of this PDF is a function of many atmospheric parameters, the transceiver apertures, and distance between the transceivers. In the uplink (Earth-to-satellite) deep fades in the transmissivity

---

\(^4\) \( d \) is the bits of precision encoded by the symbol. In this work, we set \( d = 5 \) as in [37].

\(^5\) In a real-world deployment the maximum-likelihood estimators can be computed from the measurement data to determine \( T_{min} \) and \( \xi_{max} \) [34, 35].

\(^6\) In the rest of the paper, unless stated otherwise, we choose \( n_e = n = 10^{12} \), implying \( n/N = 0.5 \).
FIG. 1: The PM CS-QKD protocols in the satellite-to-Earth channel. A local oscillator (LO) is sent with the signal by Alice which passes through a lossy channel of transmissivity $T$ and channel excess noise $\xi_d$. Bob receives the signal and the LO which he uses to perform the homodyne or heterodyne detection. The former is represented by a $X_B$ quadrature measurement (blue), and the latter by two balanced beamsplitters (purple) and two quadrature measurements (blue $X_B$ and purple $P_B$). The heterodyne/homodyne detector efficiency is $\eta_d$ and the detector excess noise $\xi_d$. An entirely equivalent EB scheme is available.

A. Noise Components

As shown in [4], we separated the noise due to the channel $\chi_{ch}$ and the detector $\chi_d$. Bob’s variance $V_B$ of the quadrature operator in [2] using the definitions in [4] and [5] is

\[
V_B = \frac{\eta_d T}{\mu} (V_A + \chi_{ch} + \chi_d + 1)
\]

\[
= \frac{\eta_d T}{\mu} (V_A + \xi_{ch} + \frac{\mu \xi_d}{\eta_d T}) + 1
\]

\[
= \frac{\eta_d T}{\mu} (V_A + \xi) + 1,
\]

where we define the total excess noise as

\[
\xi := \xi_{ch} + \frac{\mu \xi_d}{\eta_d T}.
\]

The channel excess noise\(^7\) is

\[
\xi_{ch} = \xi_{ta} + \xi_{RIN,Atmos} + \xi_{Background}
\]

\[
+ \xi_{mod} + \xi_{RIN,LO} + \xi_{RIN,Signal},
\]

where the contributions above are the time-of-arrival fluctuations $\xi_{ta}$, relative intensity noise (RIN) due to the atmosphere $\xi_{RIN,Atmos}$, background noise $\xi_{Background}$, modulation noise $\xi_{mod}$, RIN of the LO $\xi_{RIN,LO}$, and RIN of the signal $\xi_{RIN,Signal}$. We refer the reader to Table I for a description of these noise components. We note that the time-of-arrival fluctuations $\xi_{ta}$ and RIN due to the atmosphere, $\xi_{RIN,Atmos}$, have not been determined in the satellite-to-Earth channel. An analysis of these two excess noise components is discussed in the next section.

Similarly, the detector excess noise\(^11\) is

\[
\xi_d = \xi_{ADC} + \xi_{overlap} + \xi_{LO} + \xi_{Leak}
\]

\(^7\) Even in cases where non-constant transmissivity is present, channel post-selection using the LO can render a subset of the channels to lie within an effective constant transmissivity window. QKD rates can then be approximated via summation of rates arising from these subsets.

\(^8\) Note the QKD key rates of [40] are based on the use of an LO generated directly at the receiver (not one transmitted with the signal), and therefore cannot be directly compared with the key rates reported here.

\(^9\) In the limit of $T \to 0$, Bob’s variance of the quadrature operator reduces to $1 + \xi_d$ as expected.

\(^10\) The channel excess noise is defined with respect to the input, and is thus multiplied by the transmissivity $T$ and $\eta_d$ in the covariance matrix.

\(^11\) The detector excess noise is defined with respect to the output and hence $T$ and $\eta_d$ cancel out in the covariance matrix.
where the noise contributions listed are the electronic noise $v_{el}$, analogue-digital converter noise $\xi_{ADC}$, detector overlap $\xi_{overlap}$, LO subtraction noise $\xi_{LO}$, and LO-to-signal leakage $\xi_{Leak}$. We refer the reader to Table II for a fuller description of these noise components.

IV. NOISE SIMULATIONS

In the following section, we use the atmospheric channel to determine the channel excess noise contributions from the intensity fluctuations of the LO and the time-of-arrival fluctuations between the LO and signal. Typical values from the literature of each noise contribution (as well as our own calculations) are summarised in Table II.

A. Relative intensity - Local oscillator

We follow the procedure presented in [24] to derive the contribution to the channel excess noise from the variations in the intensity of the LO, in the context of the satellite-to-Earth channel. At Bob, the signal and LO are mixed on a balanced beamsplitter. Photo-detectors at the outputs measure the intensity and are subtracted to obtain the quadrature measurement. The difference in the number operator describes this measurement

$$\Delta\hat{n}_B = |\alpha_{LO}|(\cos(\theta)\hat{X} + \sin(\theta)\hat{P}),$$

where $|\alpha_{LO}|$ is the coherent amplitude, and $\theta$ is the phase of the quadrature measurement. It is clear that oscillations in the amplitude $|\alpha_{LO}|$ of the LO will introduce an additional excess noise to the protocol. Assuming for simplicity we intend to measure the $\hat{X}$ quadrature ($\theta = 0$). Then the difference in number operator is reduced to $\Delta\hat{n}_B = |\alpha_{LO}|\hat{X}$. Since the fluctuations in intensity and the quadratures are independent random variables, then the variance of the difference in number operator is proportional to the variance of both LO and quadrature operator,

$$\text{Var}(\Delta\hat{n}_B) = \text{Var}(|\alpha_{LO}|\hat{X})$$

$$= \langle|\alpha_{LO}|^2\rangle\langle\hat{X}^2\rangle - \langle|\alpha_{LO}|\rangle^2\langle\hat{X}\rangle^2$$

$$= \langle|\alpha_{LO}|^2\rangle V_A$$

$$= (\text{Var}(|\alpha_{LO}|) + \langle|\alpha_{LO}|\rangle^2)V_A,$$

where $\langle\hat{X}\rangle = 0$ and $\text{Var}(|\alpha_{LO}|) = \langle|\alpha_{LO}|^2\rangle - \langle|\alpha_{LO}|\rangle^2$ is determined by the intensity fluctuations of the LO and $V_A$ denotes the variance of the quadrature without considering the effects of the variation of intensity in the LO (i.e. Alice’s modulation variance). To derive the variance in the measurement of the $\hat{X}$ quadrature considering all the effects, we rewrite $\text{Var}(\Delta\hat{n}_B)$ assuming a constant intensity LO with amplitude $\langle|\alpha_{LO}|\rangle$, and that the RIN in the quadrature measurement is characterized by the variance $V_{RIN,LO}(X)$.

$$\text{Var}(\Delta\hat{n}_B) = \text{Var}(\langle|\alpha_{LO}|\rangle\hat{X})$$

$$= \langle|\alpha_{LO}|\rangle^2 V_{total}(\hat{X})$$

$$= \langle|\alpha_{LO}|\rangle^2 (V_A + V_{RIN,LO}(\hat{X})).$$

where $V_{total}(\hat{X})$ is the total variance including $V_A$ and the variance of the quadrature operator due to the RIN of the LO. Comparing both (29) and (30) we get

$$\langle|\alpha_{LO}|\rangle^2 V_{RIN,LO}(\hat{X}) = \text{Var}(\langle|\alpha_{LO}|\rangle)V_A.$$  

Finally, the resulting noise component is

$$\xi_{RIN} = \frac{\text{Var}(\langle|\alpha_{LO}|\rangle)}{\langle|\alpha_{LO}|\rangle^2} V_A.$$  

We identify two main sources in the fluctuations of the intensity of the LO. One is the fluctuations inherent to the laser when it is generated and the second is the fluctuations caused by the atmospheric fading channel. Since these two random effects are independent, then the noise component due to intensity fluctuations of the LO becomes the sum of the two contributions $\xi_{RIN} = \xi_{RIN,LO} + \xi_{RIN,Atmos}$. In [24] the noise term due to the fluctuations of the laser is derived and given for a realistic setup with commonly available lasers. The contribution to the total excess noise is $\xi_{RIN,LO} \approx 0.00035V_A$. In Table II $\xi_{RIN,LO}$ is shown for a modulation variance of $V_A = 5$.

Analysing $\xi_{RIN,Atmos}$, we note that the intensity of the LO is measured over the aperture used by the receiver. That is, we consider the total power $P$ over the aperture surface $\mathcal{D}$,

$$P_D = \iint_{\mathcal{D}} |I(x,y)|^2 dxdy,$$

where $I(x,y)$ is the irradiance of the LO expressed in Cartesian coordinates with the aperture centred at $(x,y) = (0,0)$. In [32], the term $\frac{\text{Var}(\langle|\alpha_{LO}|\rangle)}{\langle|\alpha_{LO}|\rangle^2}$ is the normalized intensity variance known as the scintillation index $\sigma_{SI}^2$. We can quantify the scintillation index averaged over the aperture surface $\mathcal{D}$ with diameter $D_R$

$$\sigma_{SI}^2(D_R) = \frac{\langle P_D^2 \rangle}{\langle P_D \rangle^2} - 1.$$  

Then the $\xi_{RIN,Atmos}$ noise component can be rewritten as

$$\xi_{RIN,Atmos} = \sigma_{SI}^2(D_R)V_A.$$  

$\xi_{RIN,LO} = \frac{1}{2} RIN_{LO} \times B_{LO} \times V_A$ where $RIN_{LO} = 1.4 \times 10^{-7}$ Hz$^{-1}$ is the RIN and $B_{LO} = 10$ KHz is the optical bandwidth of the LO [24].
The finite response time of the balanced homodyne/heterodyne detector introduces the noise component \( \xi_{\text{det}} \). This noise component is an intrinsic noise that depends on the parameters of the laser [24].

### Table I: Noise components of the total excess noise \( \xi \) of CS-QKD the satellite-to-Earth channel.

| \( \xi \)     | Channel excess noise component | Description                                                                                                                                 |
|--------------|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| \( \xi_{\text{ta}} \) | Time-of-arrival fluctuations | \( \xi_{\text{ta}} \) is the noise component due to the differential modifications between signal and LO pulses in the satellite-to-Earth channel. Predictions for this noise component in a terrestrial free-space channel were made in [50], but not for the satellite-to-Earth channel. We will quantify this noise component in the next section. |
| \( \xi_{\text{RIN,Atmos}} \) | RIN of LO due to atmosphere | \( \xi_{\text{RIN,Atmos}} \) is the noise component due to the scintillation caused by atmospheric fluctuations. We will quantify this noise in the next section. |
| \( \xi_{\text{RIN,LO}} \) | RIN of the LO | The noise term \( \xi_{\text{RIN,LO}} \) is due to the power fluctuations of the laser before modulation. This noise component is an intrinsic noise that depends on the parameters of the laser [24]. |
| \( \xi_{\text{mod}} \) | Modulation noise | The noise term \( \xi_{\text{mod}} \) is due to the voltage fluctuations in the modulation of the coherent state at Alice [11]. The signal generator translates bit information to a voltage which is amplified to drive the modulator [24]. The phase of the quadrature is proportional to the applied voltage. Subsequently, the voltage deviation introduced by the signal generator introduces modulation noise. |
| \( \xi_{\text{Background}} \) | Background noise | Part of the channel excess noise for the satellite-to-Earth channel is photon leakage from the background \( \xi_{\text{background}} \) to the quantum signal and LO [12]. |
| \( \xi_{\text{RIN,Signal}} \) | RIN of the signal | Excess noise due to power fluctuations of the laser translates to the RIN of the signal \( \xi_{\text{RIN,Signal}} \). This noise component is proportional to the absolute power variance for a given optical bandwidth of the signal laser [24]. In comparison to the RIN of the LO due to the laser, the RIN of the signal is considerably smaller [24]. |
| \( \xi_{\text{d}} \) | Detector excess noise component |                                                                                                                                           |
| \( \xi_{\text{el}} \) | Electronic noise | The term \( \xi_{\text{el}} \) is electronic noise that is due to other noise sources of the detector including thermal noise and clock jitter affecting the detector. Shot-noise-limited homodyne measurement requires sufficient LO power to reduce the effect of the electronic noise by increasing the signal-to-noise ratio (SNR) [24] [43]. |
| \( \xi_{\text{ADC}} \) | Analogue-digital converter (ADC) quantization noise | \( \xi_{\text{ADC}} \) is due to digitizing the output voltage, required by all CV-QKD systems [24] [44] [45]. This noise term can be suppressed by increasing the number of bits. |
| \( \xi_{\text{overlap}} \) | Pulse overlap | The finite response time of the balanced homodyne/heterodyne detector causes an electrical pulse overlap \( \xi_{\text{overlap}} \) [46]. Large peak powers for shorter pulses can saturate the diodes, causing a non-linear response. This can be suppressed by ensuring \( \tau_{\text{overlap}} \gg 1 \), where \( \tau_{\text{overlap}} \) is the pulse width. |
| \( \xi_{\text{LO}} \) | LO fluctuations during subtraction | The incomplete subtraction of the output signals by the homodyne/heterodyne detector introduces the noise component \( \xi_{\text{LO}} \) [24] [46]. |
| \( \xi_{\text{Leak}} \) | Leakage noise | Part of the total excess noise is the photon leakage from the LO to the signal when the signal is multiplexed with the LO [44] [46]. This term largely depends on the system design. However, in the polarization-frequency-multiplexing scheme, this is assumed negligible [47]. |

The value of \( \sigma^2_{\text{SI}}(D_R) \) can be obtained for weak atmospheric turbulence by using the atmospheric models presented in the Appendix, and calculating the first and second order statistical moments of the irradiance [48]. The result is

\[
\sigma^2_{\text{SI}}(D_R) = 8.70 k^{7/6} (H - h_0)^{5/6} \sec^{11/6}(\zeta)
\times \operatorname{Re} \int_{h_0}^H C_n^m(h) \left[ \left( \frac{kD_R^2}{16H} + \frac{h - h_0}{H - h_0} \right)^{5/6} - \left( \frac{kD_R^2}{16H} \right)^{5/6} \right] dh
\]  

(36)

where \( k = \omega_0/c \) is the wavenumber of the laser frequency \( \omega_0 \) (c is the speed of light), \( \zeta \) is the zenith angle, \( H \) is the altitude of the satellite at zenith angle \( \zeta = 0 \), \( h_0 = 0 \) km is the altitude of the receiver ground station, and \( C_n^m(h) \) is the refractive index structure of the atmosphere (see Appendix). In Fig. 2 we present the values of \( \sigma^2_{\text{SI}}(D_R) \) for different receiver aperture diameters and zenith angles. We see the importance of using a large aperture in the receiver, since not only is it essential for increasing the transmissivity of the channel but also to reduce the fluctuations on intensity which translates to excess noise. The values of \( \xi_{\text{RIN,Atmos}} \) are calculated for the receiver aperture diameter \( D_R = 1 \text{ m} \) and \( D_R = 3 \text{ m} \) at \( \zeta = 60^\circ \) and altitude \( H = 500 \text{ km} \) are given in Table II. These
are $\xi_{RIN,Atmos} = 0.01$ and 0.003, respectively. For the rest of this paper, unless otherwise specified, we use the former value for $D_R = 1 \text{ m}$.

### B. Time-of-arrival fluctuations

Now we derive the pulse deformations due to transmission through the satellite-to-Earth channel, used in the calculation of the time-of-arrival fluctuations of our Table II in [49] an analysis based on the mutual coherence function (MCF) is made, where the two-frequency MCF is defined by the average of all ensemble of pulses (see equations (11)-(28) in [49]). The MCF represents the product of the free space optical fields and the turbulence factor based on the first and second order Rytov approximation. Since LEO satellites are positioned at a high enough altitude we can treat the propagation of the wave as in the far-field regime. In this regime the wave as seen by the receiver corresponds to a plane wave.

In the far-field regime corresponding to the Fresnel parameter $\Omega = \omega_0 W_0^2 / (2 Lc) << 1$ where $W_0$ is the beam-waist, $L$ is the total distance travelled by the pulse, and $c$ is the speed of light. The beam-waist is determined by the transmitter aperture diameter which is a fundamental system parameter, as it dominates over many of the effects occurring during optical propagation. The temporal mean intensity in the far-field regime is obtained by averaging over the bandwidth of the MCF at the same radial position and time. From [49], the result is

\[
\langle I(r, L, t') \rangle \approx \frac{\tau_0^2}{\tau_1} \left( \frac{W_0^2}{2 Lc} \right)^2 \frac{\tau_0^4}{\tau_1^2 \left[ \tau_0^2 + (W_0 r/Lc)^2 \right]} \exp \left\{ -\frac{\omega_0^2 \tau_0^2 (W_0 r/Lc)^2}{2 \tau_0^4 + (W_0 r/Lc)^2} \right\} \times \exp \left\{ -\frac{2(t'-L/c-\tau_0^2/2Lc)^2}{\tau_1^2} \right\},
\]

where $t'$ is the time, $r$ the radial coordinate over the wavefront of the pulse, $\tau_0$ is the initial pulse width, and the broadened pulse width $\tau_1$ is

\[
\tau_1 = \sqrt{\tau_0^2 + 8 \alpha},
\]

\[
\alpha = \frac{0.391(1 + 0.171 \delta^2 - 0.287 \delta^{5/3})\nu_1 \sec(\xi)}{c^2},
\]

and where $\nu_1$ is the following integral (which we evaluate numerically),

\[
\nu_1 = \int_{h_0}^{H} C_n^2(h) L_0(h)^{5/3} dh.
\]

Here $\delta = \frac{L}{L_0}$ where $L_0$ and $L_0$ denote the outer and inner scales, respectively. The inner and outer scales are introduced alongside the atmospheric model described in the Appendix. Any optical pulse sent through the atmosphere, will incur deformations due to variations of the refractive index of atmospheric turbulence. To fully analyse the pulse deformations we consider two effects:

### Table II: Excess noise break-down affecting satellite-to-Earth CS-QKD during daylight.

| Parameter | Description | Ref. |
|-----------|-------------|------|
| $\xi_{ch}$ | Channel excess noise | 0.0186; 0.0126 |
| $\xi_{ta}$ | Time-of-arrival fluctuations | 0.006 |
| $\xi_{RIN,Atmos}$ | RIN of LO due to atmosphere | 0.01; 0.003 |
| $\xi_{RIN,LO}$ | Relative intensity noise of LO | 0.0018 |
| $\xi_{mod}$ | Modulation noise | 0.0005 |
| $\xi_{Background}$ | Background noise | 0.0002 |
| $\xi_{RIN,Signal}$ | Relative intensity noise of signal | $< 0.0001$ |
| $\xi_d$ | Detector noise | 0.0133 |
| $\nu_d$ | Electronic noise | 0.013 |
| $\xi_{ADC}$ | Analogue-digital converter noise | 0.0002 |
| $\xi_{overlap}$ | Detector overlap | $< 0.0001$ |
| $\xi_{LO}$ | LO subtraction noise | $< 0.0001$ |
| $\xi_{Leak}$ | LO to signal leakage | $< 0.0001$ |

| Parameter | Ref. |
|-----------|------|

FIG. 2: Aperture averaged scintillation index for different receiver aperture diameters and zenith angles.
the broadening of the pulse, and the changes on the time-of-arrival of the pulse. Both of these effects are characterised by the value of $\tau_1$. First, the broadening of the pulse will cause an attenuation of the average light intensity of the received signal by a factor of $\tau_0/\tau_1$ [30]. In Fig. 3 we show the ratio $\tau_0/\tau_1$ as a function of $\tau_0$ for the satellite-to-Earth channel with the parameters specified above. We see that the pulse broadening becomes considerable only for pulse widths $\tau_0 < 0.1$ ps. However, for a pulse width $\tau_0 = 130$ ps commonly used in CV-QKD systems consistent with a 100 MHz repetition rate [43], the pulse broadening effect is negligible.

The second, and more relevant effect is the variation of the time-of-arrival $t_a$ at the detector between the signal and the LO pulses. As shown in [24], the statistical properties of the time-of-arrival are obtained from the temporal statistical moments of the complex envelope describing the pulse. The analysis shows that the time-of-arrival mean and variance equal $\langle t_a \rangle = L/c$ and $\sigma_{t_a}^2 = \frac{\sigma^2}{4}$, respectively. In satellite-to-Earth CS-QKD, the fluctuations of the time-of-arrival caused by the atmospheric channel contribute to the total excess noise as an additional amount [50]

$$\xi_{ta} = 2V_A \omega_0^2 (1 - \rho_{ta}) \sigma_{t_a}^2,$$

where $\rho_{ta}$ is the timing correlation coefficient between LO and the signal. We set the correlation coefficient between signal and LO to $\rho_{ta} = 1 - 10^{-13}$ as in [50]. The noise component due to time-of-arrival fluctuations (40) increases with the pulse width $\tau_1$. In Table 1 we determine the value for this noise component to be $\xi_{ta} = 0.006$ for a pulse width of $\tau_0 = 130$ ps and central frequency $\omega_0 = 2\pi \times 200$ THz (corresponding to a wavelength of 1550 nm).

The LO generated by Alice must have sufficient intensity at Bob such that he can perform a heterodyne/homodyne measurement. Typically, $10^8$ photons per pulse are required at Bob’s side. With a 100 MHz pulse repetition rate and pulse width of 130 ps, the required LO average power for a 20 dB channel loss (a typical loss considered here) at Alice’s side is 130 mW (at 1550 nm). We have chosen the repetition rate to coincide with current detector technology [43]. There are readily available coherent laser sources with these specifications. We assume the ground station has a state-of-the-art homodyne detector as in [40].

In Fig. 3 we compare the noise components contribution for daytime operation. As $T$ gets smaller, the term $\frac{\xi d}{\eta d}$ in [24] would dominate, but for the purpose of this figure, we compare each noise component on equal footing by setting $T = 1$ and $\eta_d = 1$. In this figure, we adopt the following values for the noise components. The electronic noise $\nu_d = 0.013$ is the dominant noise component. The next dominant noise component is the relative intensity noise due to the atmosphere. For the purpose of the noise analysis, we assume the realistic scenario, where the satellite zenith angle is $\zeta = 60^\circ$ (which is sufficient for a 2–3 minutes flyby [2]), a transmitter aperture diameter of $D_T = 0.3$ m and a receiver aperture diameter of $D_R = 1$ m with an altitude $H = 500$ km, implying a relative intensity noise of $\xi_{RIN,atmos} = 0.01$.

The next dominant noise component is the time-of-arrival fluctuations. We set the correlation coefficient between signal and LO to $\rho_{ta} = 1 - 10^{-13}$ as in [50]. Fig. 3 suggests that for pulse widths $\tau_0 > 0.1$ ps, the pulse broadening due to weak turbulence is negligible and $\tau_1 \approx \tau_0$. Thus, the excess noise due to time-of-arrival fluctuations is $\epsilon_{ta} = 0.006$. As expected, this noise component doesn’t depend on the receiver aperture diameter.

Furthermore, $\xi_{RIN,LO}$ is 6% of the total excess noise. ADC noise is negligible (1%) as part of the detector noise component. All other noises $\xi_{RIN,Signal}$, $\xi_{LO}$ and $\xi_{Leak}$ are less than 1% of the total excess noise with the exception of the modulation noise which is 2% [24]. Therefore, the predicted channel excess noise is $\xi_{ch} = 0.0186$ and the detector excess noise $\xi_d = 0.0133$.

V. SECREET KEY RATES OF SATELLITE-TO-EARTH CS-QKD

In Fig. 5 we calculate the secret key rate in the asymptotic limit against the transmissivity $T$ for both CS-Hom and CS-Het protocols using the parameters in Table III. Unless otherwise specified, for the rest of the paper, we use the parameters in Table III. The transmissivity on the x-axis is converted to units of $dB$ using the formula $-10 \times \log_{10} T$. We compare the channel excess noises of $\xi_{ch} = 0$ and that of our specified satellite-to-Earth

| $D_R$ | $H$ | $\zeta$ | $\eta_d$ | $\beta$ | $V_A$ | $\tau_0$ | $\lambda$ | $\xi_{ch}$ | $\xi_d$ |
|-------|-----|--------|---------|--------|-------|---------|--------|---------|-------|
| 1 m   | 500 km | 60°    | 0.95    | 0.95   | 5     | 130 ps  | 1550 nm | 0.0186  | 0.0133 |

TABLE III: System parameters.
FIG. 4: Pie chart of noise contributions to $\xi = \xi_{ch} + \frac{\mu \xi}{2 T}$ for CS-Hom protocol ($\mu = 1$) in the satellite-to-Earth channel for daylight operation. We have used values from Table I with laser pulse width $\tau_0 = 130$ ps and state-of-the-art homodyne detector specifications with $N_{LO} = 10^8$. The dominant noise term is the electronic noise at 40%, followed by RIN due to the atmosphere at 31%, the time-of-arrival fluctuations at 19% and the RIN of the LO at 6%.

channel. For the chosen parameter values, corresponding to a realistic experimental scenario, the difference in the secret key rate between CS-Hom and CS-Het is only evident at low loss in which the CS-Het protocol performs marginally better. The modulation variance $V_A$ is an adjustable parameter that can be optimized to maximize the secret key rate with the total excess noise and transmissivity $T$. However, in atmospheric channels the transmissivity can fluctuate (although here we assume not) and the optimal value of $V_A$ at one time may not be the optimal value at another time. Unless the goal is to maximize the secret key rate each run, additional resources to optimize $V_A$ are not necessary. In our system, we choose a value of $V_A = 5$ which is in the range of optimality for the values of transmissivity in the satellite-to-Earth channel.

In Fig. 6 we calculate the secret key rate in the finite case against the transmissivity $T$. As seen in Fig. 6 for the CS-Het protocol, the loss that can be tolerated (compared to the asymptotic limit) is less in the finite size regime for $n = 10^{10}$ and $n = 10^{12}$. In this same figure, we compare the key rates for collective and general attacks using the failure probability $\epsilon = 10^{-9}$ and $\epsilon' = 10^{-55}$ ($\epsilon' = 10^{-9}$), respectively. It is evident that the general attack does not tolerate as much loss. Note it is straightforward to convert all key rate into units of bits/s
by multiplying by the laser pulse repetition frequency.\textsuperscript{13}

In Table [IV] the individual impact of each noise term on the secret key rate under collective Gaussian attacks is shown\textsuperscript{14} in the finite size regime with $n = 10^{12}$.

The background noise during daylight is approximately 1\% of the total excess noise for 1550 nm light ($0.0002$)\textsuperscript{12}. In DV-QKD, background noise from daylight can be mitigated using small spatial filtering coupled with advanced adaptive optics \textsuperscript{[33]}. It was noted in \textsuperscript{8} that optical systems used in CV-QKD could also use small spectral bandwidth. Consequently, the background noise can be filtered, allowing for daylight operation. Daylight CV technology was demonstrated in \textsuperscript{54}, but there are no corresponding studies for CV-QKD.

We find that the background noise component during daylight in CS-QKD in the satellite-to-Earth channel has negligible impact on the secret key rate, in agreement with \textsuperscript{42}. For night-time operation, the secret key rate would be unchanged with $\xi_{\text{Background}} < 10^{-7}$. Thus, the secret key rate in Fig. 3 is a lower bound, and night-time operation would improve the key rates, but is not essential.

We consider how increasing the size of the receiver aperture improves the secret key rates under general attacks. For a larger receiver aperture of $D_R = 3$ m, we obtain a smaller channel excess noise of $\xi_{ch} = 0.0126$ and detector excess noise of $\xi_{d} = 0.0133$. At the transmissivity $T = 15$ dB, a secret key rate of $2.6 \times 10^{-3}$ bits/pulse is attained under general attacks for this larger receiver aperture. $T = 15$ dB is readily achievable in the satellite-to-Earth channel using this larger receiver aperture. For example, for the transmitter aperture of $D_T = 0.3$ m at transceiver separation 1200 km the beam width at the ground is 12 m (and a diffraction limited divergence of 10 µrad), giving a diffraction loss of 22 dB for receiver aperture $D_R = 1$ m (see discussion below for Micius). Extrapolating from these parameters, the receiver aperture diameter of $D_R = 2.3$ m gives a diffraction loss of 15 dB. For this receiver aperture of $D_R = 2.3$ m, the channel excess noise is $\xi_{ch} = 0.015$ and a secret key rate of $2.4 \times 10^{-3}$ bits/pulse is attained under general attacks.

We consider how the secret key rate changes with the system parameters in Table [IV]. For example, doubling the pulse period to $\tau_0 = 260$ ps, will give a channel excess noise of $\xi_{ch} = 0.033$. However, the secret key rate is barely changed (i.e. $1.0 \times 10^{-3}$ bits/pulse). We also find that from $V_A = 2$ to $V_A = 8$, the result doesn’t significantly change. Hence, this main result is not sensitive to parameters we have chosen for the figures.

As we grew close to the completion of our study, two other works related to CV-QKD over satellite-to-Earth channels appeared \textsuperscript{[38, 55]}. Different from our study, these latter works had a focus on the large-scale fading effects on the QKD key rates, and different excess noise contributions. They therefore apply to different system models than the diffraction-only loss models we explored here. However, collectively the works of \textsuperscript{38, 55} and ours illustrate clearly that CV-QKD in the satellite-to-Earth channel is feasible.

Although our focus has been to demonstrate the viability of the CS-QKD protocols in satellite-to-Earth channel, it is perhaps interesting to compare our results directly with Micius. In our calculations of the secret key rates, we have assumed that transmissivity is constant.\textsuperscript{15} That is, transmissivity fluctuations due to atmospheric turbulence and beam-wandering are assumed small in comparison to diffraction losses \textsuperscript{[54]}. As just mentioned above, in the Micius satellite QKD experiment, the satellite-to-Earth channel loss due to diffraction was 22 dB at a maximum distance of 1200 km with a transmitter aperture of $D_T = 0.3$ m, a field divergence of 10 µrad and receiver aperture of $D_R = 1$ m \textsuperscript{[2]}. Additional loss occurred via atmospheric absorption and turbulence (3 to 8 dB), and loss due to pointing error (< 3 dB). This gave an average total loss of 30 ± 3 dB. In calculations of the Micius QKD key rate, the failure probability was set to $\epsilon = 10^{-9}$ which gave a key rate of $1.38 \times 10^{-5}$ bits/pulse. In comparison, for our CS-Het protocol at the same security setting and same losses we find zero key rate under general attacks. It is only for losses less than 25 dB that we find non-zero rates under general attacks. We do caution however, that direct comparisons of these two very different technologies (DV vs. CV) are limited in value because the security assumptions are different. We also point out the Micius security analysis disregards information leakage due to side-channel imperfections \textsuperscript{[2]}. Other assumptions underpinning the Micius key rate are discussed in \textsuperscript{[57]}. However, to be fair, we have also overlooked some assumptions that underpin our CV-QKD analysis. The most important of these are in regard to the LO - an issue we discuss next.

\textsuperscript{13} In real-world cryptography it is the key rate in bits/s that is ultimately of interest. However, conversion from bits/pulse to bit/s must consider the time to decode the finite, but very large, block lengths (multiplying by the pulse repetition rate is only formally valid when the reconciliation time is zero). Optimisation of the bit/s key rate can be non-trivial in some circumstances \textsuperscript{[32]}.

\textsuperscript{14} Note in our calculations we have assumed that the transmissivity remains constant over the block length. Receiving a block length of $10^{12}$ from a 100MHz source would require minutes of transmission time. For block lengths larger than $10^{10}$ it is likely that the impact of satellite motion on transmissivity would need to be considered within the calculations unless a corresponding higher-rate source was utilised.

\textsuperscript{15} The statistical nature of the turbulence only manifests itself in our calculations through the excess noise contributions. In particular, this is through the impact of scintillation on $\xi_{\text{RIN, Atmos}}$ and on the random refractive index perturbations on $\xi_{\text{ta}}$. Under the assumption of diffraction-only losses, the constant transmissivity $T$ of the channel is determined via the system parameters, $D_T, D_R$ and $L$. Of course, these parameters must be set so that the diffraction-only loss assumption is a reasonable one.
VI. LO HACKING

A. Attacks

An underlying assumption implicit in key rates we have determined for the CS-QKD protocols is that the transmission of the LO through the satellite-to-Earth channel is secure and not interfered with. However, clearly this assumption is suspect as an eavesdropper can in principle obtain access to the LO, modify the channel, and subsequently obtain information on the quantum key. Here we briefly discuss this important caveat. We mention some specific attacks, and some countermeasures.

Equal-amplitude attack. In this attack, Eve intercepts both the LO and quantum signal and performs homodyne detections on both [63]. Eve produces two squeezed states with the same intensity level. Bob cannot discover the attack because the expected noise is less than the shot noise level. When Bob compares the difference in his measurement with Alice’s prepared state to the threshold from theoretical security proofs, he mistakenly confirms the channel is secure [63]. Eve has therefore compromised the channel. However, this security loophole can be solved if Bob can monitor the fluctuations in the intensity of the LO [64].

Wavelength attack. In this attack, Eve modifies the intensity transmission of Bob’s beamsplitter by changing the wavelength of the light from Alice. This wavelength attack deems the final keys insecure. However, it was shown in [64] that adding a simple wavelength filter randomly before measuring the intensity of the LO can prevent this attack.

Calibration attack. The device calibration routine of the LO is susceptible to an intercept-resend attack. That is, the eavesdropper manipulates the LO pulses to change the clock pulses used for the detection [62]. Eve changes the shape of the LO pulse which consequently induces a delay in the clock trigger. The homodyne detection will measure a lower intensity. Therefore, there will be a decrease in the response slope between the variance of the homodyne detection and the LO power. As a result, the shot noise will be overestimated and the excess noise underestimated [63]. Countermeasures to this attack involves monitoring the shot noise in real time.

B. Local local oscillators

Motivated by these security loopholes, there has recently been a focus on using true local oscillators or local local oscillators (LLO). In one use of an LLO, a system model is proposed where reference pulses are sent with the signal [64]. In this system model, two lasers are used, one at Alice for generating the quantum signal and another at Bob for the LLO. To establish a common phase reference, Alice sends low intensity pulses to estimate the phase and correct the heterodyne measurement [64, 65]. However, additional excess noise is introduced. Since the LLO and signal are not phase locked, the necessary phase estimation is limited by quantum uncertainty. Additionally, the laser spectral line-width introduces other phase noise related to the timing of the pulses. Currently, no phase compensation method exists for the LLO in FSO channels [63]. Photon leakage from the LLO to the signal is also unavoidable. Keeping the excess noise tolerable places limits on the intensity of the reference pulses needed for efficient homodyne/heterodyne detection.

However, pilot symbols are also subject to manipulation by an adversary, and therefore susceptible to attacks outside the scope of current security proofs (e.g. [67]). What is really required is a system that avoids the use of any reference signals at all for the phase referencing. Only by this means do the assumptions underpinning formal security proofs for the CV-QKD protocols we have discussed here remain intact. Recent work along these lines is given in [63] where publicly announced raw key values are invoked to determine the phase offsets to be applied to the LLO. However, currently even these types of phase determinations for the LLO are not formally proven secure - an issue that hopefully will be addressed in forthcoming works.

VII. CONCLUSION

In this work we investigated the feasibility of the simplest-to-deploy CV-QKD protocols, the CS-QKD protocols, over the satellite-to-Earth channel. We reviewed the security of these two protocols, as well as the components of the total excess noise most relevant to the satellite-to-Earth channel. Through new calculations we

---

### TABLE IV: Individual impact of each noise term on secret key rate under collective Gaussian attacks relative to ideal case of no noise with $K$ in the finite size regime (i.e. the ratio $\frac{K}{K_0} = 1$ for no impact and $\frac{K}{K_0} = 0$ for maximum impact). Other parameter values: $n = 10^{12}$, $\epsilon = 10^{-9}$, modulation variance $V_A = 5$ and reconciliation efficiency $\beta = 0.95$.

| Parameter Description | Value $\frac{K}{K_0}$ @ 10 dB | $\frac{K}{K_0}$ @ 20 dB | $\frac{K}{K_0}$ @ 30 dB |
|-----------------------|-------------------------------|------------------------|------------------------|
| $\xi_{ch}$ Channel excess noise | 0.0186 0.75 | 0.63 0.00 | 0.00 0.00 |
| $\xi_{ta}$ Time-of-arrival fluctuations | 0.006 0.91 | 0.87 0.00 | 0.00 0.00 |
| $\xi_{RIN,Atmos}$ Relative intensity noise due to atmosphere | 0.01 0.85 | 0.79 0.00 | 0.00 0.00 |
| $\xi_{Background}$ Background noise | 0.0097 1.00 | 1.00 0.93 | 0.93 0.93 |
| $\eta_d$ Detector efficiency | 0.95 0.95 | 0.95 0.95 | 0.95 0.95 |
| $\nu_{el}$ Electronic noise | 0.013 0.99 | 0.99 0.81 | 0.81 0.81 |
then determined that the most important sources of noise in our protocols over the satellite-to-Earth channel was the relative intensity noise due to the atmosphere, and the time-of-arrival fluctuations between the signal and LO. We next focused on the CS-QKD protocol with heterodyne detection in the deployable setting of a finite key regime. Given reasonable transceiver aperture sizes, and assuming diffraction as the only source of loss, we found that reasonable QKD key rates under general attacks can be anticipated. We therefore concluded that CV-QKD with information-theoretic unconditional security in the satellite-to-Earth channel is entirely feasible. In closing we noted our information-theoretic security assumptions that the LO is secured from manipulation by an adversary. Future useful work in this area could include formal security proofs of finite-limit CS-QKD with heterodyne detection, and formal proofs of security under LO (or reference pulse) attacks.

Acknowledgments

This research was a collaboration between the Commonwealth of Australia (represented by the Defence Science and Technology Group) and the University of New South Wales through a Defence Science partnerships agreement.
Turbulence in the Earth’s atmosphere is caused by random variation in temperature and pressure. These variations alter the air’s refractive index both spatially and temporally, distorting any optical waves propagating through the atmosphere. Distortions of the pulses transmitted such as beam deformation and beam wandering are one of the main sources of photon loss in the channel. To model the effects of the turbulent atmosphere on the optical signals we use Kolmogorov’s theory of turbulent flow [69]. The strength of the turbulence is characterized by the refractive index structure parameter, $C_n^2$. Kolmogorov’s theory is based upon the insight that turbulence is induced by eddies in the atmosphere. The scale of the turbulence can be characterised by an inner-scale $l_0$, and an outer-scale $L_0$ [33]. Eddies with a size lower than the inner-scale cannot exist since the turbulence at such scales is dissipated into the atmosphere as heat. The outer-scale denotes the upper-bound to the eddy size and is the scale at which energy is injected into the turbulence.

To model the atmospheres vertical profile of the refractive index structure parameter, we use the widely used Hufnagel-Valley model [70],

$$C_n^2(h) = 0.00594(\nu/27)^2(10^{-5}h)^{10} \exp(-h/1000) + 2.7 \times 10^{-16} \exp(-h/1500) + A \exp(-h/100),$$

with $h$ the altitude in meters, $\nu = 21$ the rms wind-speed (m/s), and $A = 1.7 \times 10^{-14}$ the nominal value of $C_n^2(0)$ at the ground. Additionally, measurements made of the scintillation suggest the outer scale $L_0$ changes with the altitude according to the empirical Coulman-Vernin profile [71]

$$L_0(h) = \frac{4}{1 + (h-2500)^2}. \quad (42)$$

Finally, the inner scale is assumed to directly proportional to the outer scale $l_0 = \delta L_0$, with $\delta = 0.005$ [19].

To describe the fluctuations of the refractive index we use a spectral density function [72]

$$\Phi_\phi(\kappa) = 0.49\kappa_0^{-5/3} \exp(-\kappa^2/\kappa_m^2)/(\kappa^2 + \kappa_0^2)^{11/6}, \quad (43)$$

with $\kappa$ the radial spatial frequency on a plane orthogonal to the propagation direction, $\kappa_m = 5.92/l_0$, $\kappa_0 = 2\pi/L_0$, and $\kappa_0$ the Fried parameter for a vertical propagation length [48]

$$r_0 = \left(0.423k_0^2\sec(\zeta)\int_{h_0}^H C_n^2(h)dh\right)^{-3/5}, \quad (44)$$

where $h_0$ and $H$ correspond to the lower and upper altitudes of the propagation path.