

Use of a Local Local Oscillator for the Satellite-to-Earth Channel

S. P. Kish¹, E. Villaseñor¹, R. Malaney¹, K. A. Mudge² and K. J. Grant²

¹School of Electrical Engineering & Telecommunications,
The University of New South Wales, Sydney, NSW 2052, Australia.

²Cyber and Electronic Warfare Division,
Defence Science and Technology Group, Edinburgh, SA 5111, Australia.

Abstract—Continuous variable quantum key distribution (CV-QKD) offers information-theoretic secure key sharing between two parties. The sharing of a phase reference frame is an essential requirement for coherent detection in CV-QKD. Due to the potential attacks related to transmitting the local oscillator (LO) alongside quantum signals, there has been a focus on using local LOs (LLOs) to establish a shared phase reference. In this work, we develop a new noise model of a current state-of-the-art LLO scheme in the context of the satellite-to-Earth channel. In doing this, we encapsulate detailed phase-screen calculations that determine the coherent efficiency - a critical parameter in free-space CV-QKD that characterizes the wavefront aberrations caused by atmospheric turbulence. Using our new noise model we then determine the CV-QKD key rates for the satellite-to-Earth channel, secure under general attacks in the finite-size regime of the LLO scheme. Our results are of practical importance for next-generation quantum-enabled satellites that utilize multi-photon technology as opposed to single-photon technology.

I. INTRODUCTION

Quantum key distribution (QKD) offers information-theoretic secure key distribution between two parties [1]. However, it is uncertain which of the two versions of QKD—discrete-variable (DV) QKD using single-photon technology or continuous-variable (CV) QKD using multi-photon technology will prevail. CV-QKD is appealing because it can be implemented with current off-the-shelf technology [2]. However, accurate and precise phase recovery is required for the coherent detection of CV-QKD protocols [3]. This is particularly the case since the sharing of a phase reference is an essential requirement in CV-QKD, in order to sift signals to information bits. The subsequent phase noise associated with the phase recovery contributes to the excess noise ξ —an important parameter determining the performance of CV-QKD.

The traditional and simplest implementation (which we refer to as the transmitted local oscillator (TLO) scheme) of establishing a shared phase reference is the transmission of the local oscillator (LO) from Alice to Bob which acts as a fixed phase reference for the quantum signal detection. However, the TLO scheme is not without issues, as an eavesdropper can in

principle obtain access to the LO, modify it, and subsequently obtain information on the quantum key. Attacks of this form on the LO have been extensively studied including equal-amplitude attacks [4], wavelength attacks [5] and calibration attacks [6], [7]. Another disadvantage of the TLO scheme is that the LO is attenuated during channel transmission, and shot-noise limited coherent detection may not be attained for lossy channels [8].

Recently, there has been a focus on using *local local oscillators* (LLO) for which the security issues of sending the LO are eliminated¹ by generating the LO locally at Bob's trusted device [8]. Unlike the TLO scheme, LLO schemes do not require phase or frequency lock ahead of time. In one use of an LLO, a scheme is proposed where reference pulses (or pilot tones) are sent with the signal [8]. We refer to these sequential schemes as the S-LLO scheme which was proposed in [8] and demonstrated experimentally in 25 km optical fibre independently in [9] & [10]. In this scheme, 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 reference pulses (RPs) to estimate the phase and correct the signal [8]. However, additional excess noise is introduced by the phase estimation process. Since the LLO and signal are not phase locked, there is considerable *phase drift* caused by the de-synchronized lasers in addition to the quantum-limited phase noise.

The phase drift noise contribution to the excess noise is one of the drawbacks in practical implementation of the S-LLO scheme [8]–[10]. Regardless of these practical issues, there are fundamental security issues associated with this phase drift noise, which opens up the S-LLO scheme to attacks by an eavesdropper [11]–[13]. Recently, much effort has been directed to minimizing phase drift using phase compensation methods in the S-LLO scheme [14], [15]. However, a design proposal by [16] called the delay-line LLO (D-LLO), uses

¹We note, that even though the security aspects of an LLO appear intuitively attractive—no formal security analysis on par with known CV-QKD information-theoretic proofs (which do not consider phase referencing issues) is available. Consideration of the formal security for LLO-based protocols and system models under circumstances where the eavesdropper prepares ancillary states that become entangled with both reference pulses and quantum signals would be useful in this regard.

balanced interferometers to eliminate the phase drift by ensuring self-coherence between signal and reference pulse. Further improvement of the D-LLO was demonstrated in optical fibre [17] & [18] by using multiplexing techniques to reduce photon leakage from the reference to signal pulse. In this work, we consider the D-LLO scheme to be a current state-of-the-art LLO scheme. However, it is not known how the D-LLO scheme would be adapted to the satellite-to-Earth channel.

The contributions of this work are the following:

- We develop a practical noise model of a current state-of-the-art LLO scheme (the D-LLO scheme) in the satellite-to-Earth channel.
- We numerically simulate the wavefront aberrations characterized by the coherent efficiency γ in the satellite-to-Earth channel with and without adaptive optics (AO).
- We calculate for the first time the expected information-theoretic secure key rates under general attacks in the finite-size regime of the D-LLO scheme in the satellite-to-Earth channel.

The remainder of this article is organized as follows. In Section II, we adapt the D-LLO scheme from [17] to the satellite-to-Earth channel. In this same section, we introduce the noise model, including contributions due to the turbulent atmosphere. In the same section, we introduce analytic solutions for the reference pulse intensity to minimize the excess noise in the D-LLO scheme. In Section III, we simulate γ in the satellite-to-Earth channel with and without AO using techniques found in [19]. In Section IV, we calculate the achievable key rates under general attacks in the finite-size regime of the D-LLO scheme in the satellite-to-Earth channel with the values of γ . Lastly, we summarize the article and discuss future directions in the conclusion.

II. NOISE MODEL FOR LLO CV-QKD IN THE SATELLITE-TO-EARTH CHANNEL

In the *free-space* optical (FSO) channel CV-QKD, contributions to the excess noise are quite different from those seen in optical fibre [8]–[10], [16], [20]. In particular, there are studies of TLO CV-QKD protocols in FSO channels that suggest excess noise due to time-of-arrival fluctuations caused by atmospheric turbulence cannot be ignored [21]–[24]. Fluctuations of the pulse intensity due to scintillation also contributes to the excess noise ξ . In [16], these terms due to the atmospheric channel in LLO schemes were not taken into account.

Unlike the TLO scheme, *wavefront aberrations* caused by propagation through atmospheric turbulence of the signal contributes to the excess noise in the LLO schemes [19]. This excess noise contribution is characterized by the coherent efficiency γ , determined by interfering the signal and the LO at the coherent detector. It is well known in coherent classical communication, that AOs can correct wavefront aberrations and significantly decrease the bit error rate [25]. Recently, performance improvements using AO have been shown to improve key rates under collective attacks in the asymptotic limit in CV-QKD systems [26], [27]. However, the impact of γ

on the secret key rate under general attacks in the deployable setting of the finite regime is yet to be investigated.

A. System model

We present our system model of the D-LLO CV-QKD protocol in Fig. 1. A Gaussian modulated coherent state (GMCS) of variance V_A is prepared on the satellite (Alice) and measured at the ground station (Bob) using heterodyne detection. At Alice's location in a LEO satellite at altitude H , a strong laser source L_A generates pulses (of wavelength λ , beam-waist w_0 and duration τ_0) separated by $2/f$ where f is the repetition rate. A balanced interferometer is used to create self-coherence between signal and reference pulses delayed by $1/f$. The signal is modulated by an amplitude modulator (AM) and phase modulator (PM). The reference and signal pulses are polarization-multiplexed by a polarizing beam-splitter (PBS). After passing through a lossy channel of transmissivity T and channel excess noise ξ_{ch} , the reference and signal pulses are de-multiplexed at Bob's side. The signal is further delayed by $1/f$ and a heterodyne detector is used with the LLO. Both signal and reference pulses are received by an aperture of diameter D_R . We set the aperture size D_R such that the effects of beam-wandering and elliptical deformation can be neglected. Henceforth, we will assume T is constant and is dominated only by diffraction loss.

For the LLO, high intensity pulses are generated by the laser L_B . These pulses pass through a balanced interferometer to produce self-coherent pulses delayed by $1/f$. The LLO is split by a balanced beamsplitter to the two heterodyne detectors used to measure the quadratures of the reference and signal pulses, respectively. Bob receives the reference pulses which he uses to determine the phase by performing the heterodyne detection using the LLO. Another heterodyne detector is used to measure the quadrature of the signal. The heterodyne detector efficiency of both detectors is η_d and the detector excess noise is ξ_d . The signal wavefront undergoes aberrations by atmospheric turbulence, causing a mismatch at the coherent detection. This is characterized by the coherent efficiency given by

$$\gamma = \frac{\frac{1}{2} \iint_{\mathcal{D}_R} [E_{LO}^* E_S + E_{LO} E_S^*] ds|^2}{\iint_{\mathcal{D}_R} |E_{LO}|^2 ds \iint_{\mathcal{D}_R} |E_S|^2 ds}, \quad (1)$$

where \mathcal{D}_R is the receiver aperture surface, E_S is the electric field of the signal pulse, and E_{LO} is the electric field of the LO that remains undisturbed by the turbulence.

The coherent efficiency γ is effectively the normalized intensity of the wavefront aberration of the signal interfering with the LLO. An AO unit can be inserted to correct the wavefront aberrations of the signal by means of a deformable mirror that is assumed to be controlled faster than the frequency of fluctuations.

B. Channel excess noise

The excess noise is given by

$$\xi = \xi_{ch} + \frac{2\xi_d}{\eta_d T}, \quad (2)$$

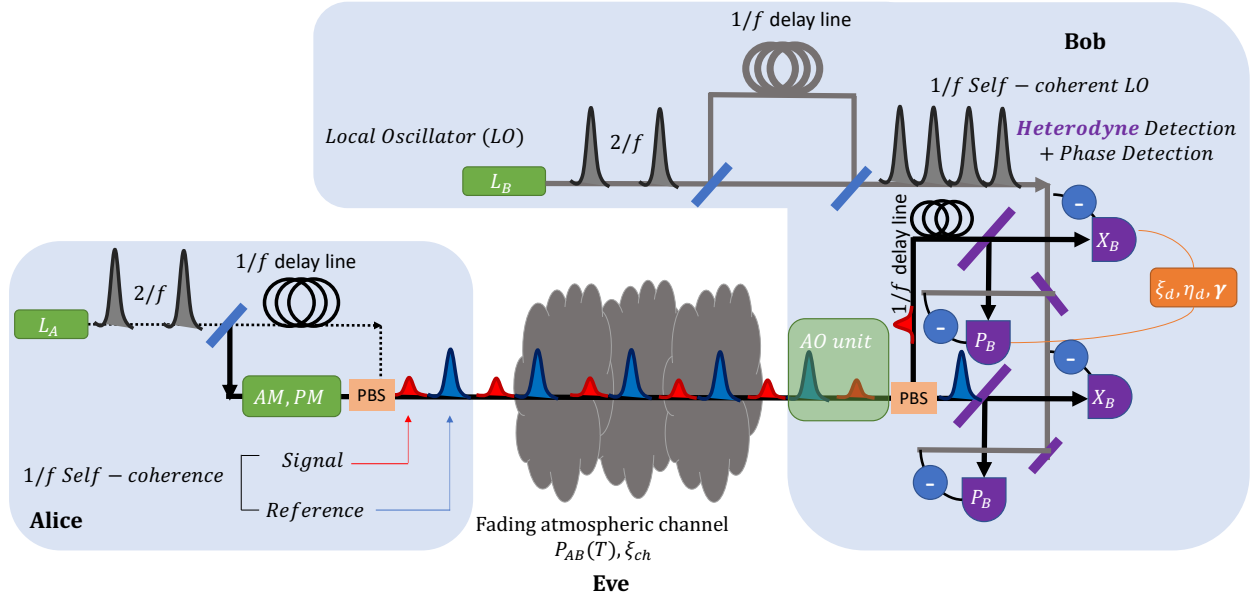


Figure 1: The D-LLO protocol in the satellite-to-Earth channel. Alice's laser L_A generates pulses separated by $2/f$ where f is the repetition rate. A balanced interferometer is used to create self-coherent signal and reference pulses delayed by $1/f$. The signal passes through the amplitude modulator (AM) and phase modulator (PM). The reference and signal pulses are recombined with a polarizing beam-splitter (PBS) and pass through a lossy channel of transmissivity T and channel excess noise ξ_{ch} . For the LO, pulses generated by laser L_B pass through a balanced interferometer to create self-coherent pulses delayed by $1/f$. Bob receives the signal and the reference pulse which are separated. One of the two heterodyne detectors is used to determine the phase of the reference pulse used to correct the signal. The other heterodyne detector is used to detect the signal. The heterodyne detector efficiency is η_d and the detector excess noise ξ_d . γ is the coherent efficiency due to the wavefront aberration of the signal mixing with the LO which is corrected by an AO unit.

f	w_0	D_R	H	η_d	V_A	τ_0	λ	ξ_{ch}
100 MHz	0.15 m	1 m	500 km	0.95	1.5	130 ps	1550 nm	0.0172

Table I: System parameters.

where ξ_{ch} is the channel excess noise which comprises of

$$\begin{aligned} \xi_{ch} = & \xi_{ta} + \xi_{RIN,Atmos} + \xi_{Background} \\ & + \xi_{mod} + \xi_{RIN,LO} + \xi_{RIN,Signal} + \xi_{Leak} + \xi_{Phase}, \end{aligned} \quad (3)$$

where the terms on the RHS are the time-of-arrival fluctuations ξ_{ta} , relative intensity noise (RIN) of RP due to the atmosphere $\xi_{RIN,Atmos}$, background noise $\xi_{Background}$, modulation noise ξ_{mod} , RIN of the LO $\xi_{RIN,LO}$, RIN of the signal due to atmosphere $\xi_{RIN,Signal}$, reference-to-signal leakage ξ_{Leak} and the phase noise after phase correction ξ_{Phase} .

C. Detector excess noise

The detector excess noise is given by

$$\xi_d = \frac{2v_{el}}{\gamma} + \xi_\gamma + \xi_{tech}, \quad (4)$$

where the noise contributions listed are the electronic noise v_{el} , coherent efficiency noise contribution ξ_γ and the technical noise ξ_{tech} . ξ_γ is given by [21]

$$\xi_\gamma = \frac{1 - \gamma}{\gamma}. \quad (5)$$

Wavefront aberrations are particularly important in LLO schemes because of the interference of the aberrated signal and un-aberrated LLO wavefront at the detector. In the TLO scheme, both signal and LO are aberrated by the same amount for colinear propagation and this term is $\xi_\gamma = 0$. In the D-LLO scheme, polarization- and time- multiplexing are used to isolate the signal from the reference pulse as in [17]. The remaining photon leakage is given by:

$$\xi_{Leak} = \frac{|\alpha_R|}{R_e + R_{po}}, \quad (6)$$

where R_e is the finite extinction ratio of the pulse generation at Alice and R_{po} is the finite extinction ratio of the polarization beamsplitter (PBS) at Bob. Typical values for R_e and R_{po} are between 30 dB and 60 dB.

The technical noise is given by

$$\xi_{tech} = \xi_{ADC} + \xi_{overlap} + \xi_{LO}, \quad (7)$$

where the noise contributions are analogue-digital converter noise ξ_{ADC} , detector overlap $\xi_{overlap}$ and LO subtraction noise ξ_{LO} . In this D-LLO scheme, a separate heterodyne

detector is used to detect the signal. The ADC quantization noise is limited by the maximum amplitude of the signal pulse, instead of the reference pulse as would be the case if one heterodyne detector is used. Subsequently, $\xi_{ADC} = \frac{|\alpha_s|^2}{12 \times 2^n}$, where $|\alpha_s|^2$ is the signal intensity and $n = 10$ is the number of bits. Since the signal intensity is at least 2 orders of magnitude smaller than the reference pulse, ξ_{ADC} is negligible.

D. Phase estimation error

In the D-LLO scheme, there are two independent laser sources, one at Alice and one at Bob. The reference pulse $|\alpha_R\rangle$ is sent along with the modulated signal pulse $|\alpha_S\rangle$.

Bob performs a heterodyne detection to determine the phase θ_S of the signal relative to his LO using the reference pulse. Bob uses the reference pulse and LO to measure the phase θ_R , and then applies the correction on the signal. After phase compensation, the phase noise for the GMCS protocol ξ_{phase} can be written as [16]

$$\xi_{Phase} = 2V_A(1 - e^{-V_{est}/2}), \quad (8)$$

where V_{est} is the remaining phase error between reference and signal pulse after phase compensation. The phase accumulated by the signal coherent state is

$$\theta_S = \theta_{src}^A + \theta_S^{ch} + \theta_{mod} - \theta_{src}^B, \quad (9)$$

where θ_{src}^A is the phase of Alice's source, θ_S^{ch} is the phase introduced by the channel, θ_{mod} is the modulation phase and θ_{src}^B is the phase of the LO pulse at Bob's side. The phase of the reference pulse is

$$\theta_R = \theta_{src}^A + \theta_{delay}^A - (\theta_{src}^B + \theta_{delay}^B), \quad (10)$$

where θ_{delay}^A and θ_{delay}^B are the phase delays $1/f$ of the reference pulse and LO, respectively. Note, both the reference and signal are generated at the same source with the phase θ_{src}^A . The remaining phase error $V_{est} = \text{Var}(\hat{\theta}_S - \theta_{mod})$ comprises of

$$V_{est} = V_{error} + V_{drift} + V_{channel}, \quad (11)$$

where V_{error} is the fundamental phase estimation error given by the standard quantum limit:

$$V_{error} = \frac{\xi_{ch} + 2\frac{1+\xi_d}{\eta_d T}}{|\alpha_R|^2}, \quad (12)$$

Noise term	Description	D-LLO
ξ_{ta}	Time-of-arrival fluctuations	$0.0012V_A$
$\xi_{RIN,Atmos}$	RIN of RP due to atmosphere	$0.002V_A$
$\xi_{RIN,LO}$	RIN of LO	$0.00035V_A$
$\xi_{RIN,Signal}$	RIN of signal due to atmosphere	< 0.0001
ξ_{error}	Phase estimation error	$\frac{\xi_{ch} + 2\frac{1+\xi_d}{\eta_d T}}{ \alpha_R ^2} V_A$
ξ_{Leak}	Photon leakage to signal	$\frac{ \alpha_R ^2}{R_e + R_{po}}$
ξ_γ	Wavefront aberrations	$\frac{1-\gamma}{\gamma}$
ξ_{el}	Electronic noise	$\frac{2v_{el}}{\gamma}$
ξ_{tech}	Technical noise	0.005

Table II: Excess noise contributions in the satellite-to-Earth channel using the system parameters in Table I.

where α_R is the amplitude of the reference pulse prepared by Alice. Unlike the S-LLO scheme, in the D-LLO scheme, there are two balanced interferometers assuring self-coherence between signal and reference pulses. Consequently, the phase drift noise is eliminated $V_{drift} = 0$. Since the reference pulse does not pass through the modulator, the AM dynamics noise component only depends on the signal intensity and therefore, can be neglected. Lastly, the noise of the channel $V_{channel}$ is due to the differences in path length or equivalently the time-of-arrival fluctuations V_{ta} between the signal and reference pulse.

E. Optimal reference pulse intensity

In this section, we determine the optimal reference pulse intensity. The most significant difference between noise components in the TLO and LLO is noise ξ_{LE} due to photon leakage from the reference to signal pulses. The larger the reference pulse intensity, the larger ξ_{LE} . However, there is a trade-off with the fundamental quantum phase noise² $\xi_{error} = V_A V_{error}$ which decreases with increasing reference pulse intensity. The reference pulse intensity can be optimized to minimize the excess noise.

The photon leakage contributes the noise component $\frac{|\alpha_R|^2}{R_e + R_{po}}$, such that

$$\xi_{ch} = \frac{|\alpha_R|^2}{R_e + R_{po}} + V_A \frac{\xi_{ch} + 2\frac{1+\xi_d}{\eta_d T}}{|\alpha_R|^2} + \xi_{other}, \quad (13)$$

with the derivative w.r.t. $N_R = |\alpha_R|^2$ given by,

$$\frac{d\xi_{ch}}{dN_R} = \frac{1}{R_e + R_{po}} - V_A(\xi_{ch} + 2\frac{1+\xi_d}{\eta_d T})/N_R^2 = 0, \quad (14)$$

from which it follows that the optimal value for the reference pulse intensity as prepared by Alice (i.e. $T = 1$) is

$$N_R = \sqrt{(R_e + R_{po})(\xi_{ch} + 2\frac{1+\xi_d}{\eta_d})V_A}, \quad (15)$$

and the minimum excess noise,

$$\xi_{ch} = 2 \times \sqrt{\frac{V_A}{R_e + R_{po}}(\xi_{ch} + 2\frac{1+\xi_d}{\eta_d})} + \xi_{other}. \quad (16)$$

For detector efficiency $\eta_d = 0.95$, $V_A = 1.5$, $R_e = 60$ dB and $R_{po} = 30$ dB (see reference [17]) the initial reference pulse intensity generated by Alice is $N_R \approx 55,000$. For the rest of the paper, we use these parameters to minimize ξ_{ch} . We summarize the excess noise contributions in Table II.

III. NUMERICAL SIMULATION OF THE COHERENT EFFICIENCY

Using the system parameters shown in Table I we use numerical methods to obtain the field of the signal involved in calculating the values of γ (equation (1)). The numerical methods consist of the use of Fourier algorithms to simulate

²Note from this point forward, we make the approximation $\xi_{phase} = 2V_A(1 - e^{-V_{est}/2}) \approx V_A(V_{drift} + V_{error} + V_{ta} + V_{RIN,Atmos})$ and assume that $V_{est} < 0.1$.

laser-beam propagation through a turbulent atmosphere. The evolution of the laser-beam is simulated using the open-source software *PROPER* [28], and the turbulent atmosphere is modelled using phase screens in combination with several atmospheric models.

To account for the use of an AO system, we assume the existence of hardware, i.e. a deformable mirror, which can apply a correction to each pulse. Each AO correction is represented in the basis of the Zernike polynomials, where the effectiveness of AO ultimately depends on the maximum order, n_{max} , of polynomials used to construct each correction. Higher values of n_{max} yield higher values of γ . A detailed description of the numerical methods used can be found in [19]. In Table III we show the resulting mean values of γ (10,000 iterations were used), with and without AO, for $\zeta = 0^\circ$, and for $\zeta = 60^\circ$. When AO is used, an order $n_{max} = 14$ is considered.

IV. PRACTICAL LLO SECRET KEY RATE IN THE SATELLITE-TO-EARTH CHANNEL

For the Gaussian modulated coherent state protocol with heterodyne detection, the secret key rate³ under general attacks

³When we refer to “secret key rate” in this article, we actually mean a lower bound on the rate.

ζ	γ	γ with AO
0°	0.484	0.843
60°	0.375	0.677

Table III: Coherent efficiency γ in the satellite-to-Earth channel.

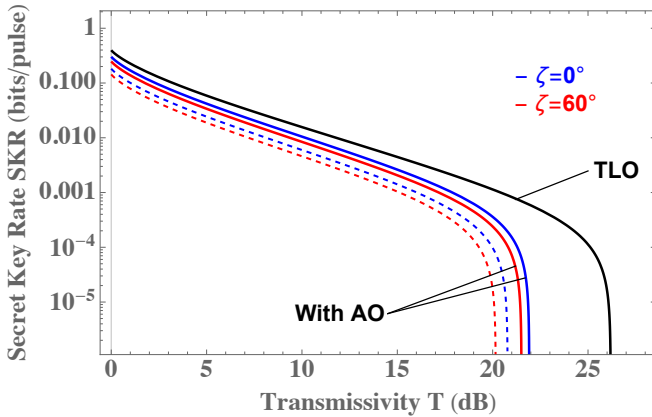


Figure 2: Secret key rate under general attacks in the finite-size regime for $V_A = 1.5$ comparison for the coherent efficiencies in the satellite-to-Earth channel from Table III. The optimal value for the reference pulse intensity to minimize excess noise is used.

in the deployable setting of the finite regime (in bits/pulse) is given by [29]

$$K = \frac{n}{N}[\beta I_{AB} - S_{BE}^{\epsilon_{PE}}] - \frac{\sqrt{n}}{N} \Delta_{AEP}(n) - \frac{2}{N} \log_2 \frac{1}{2\epsilon}, \quad (17)$$

where I_{AB} is the mutual information between Alice and Bob, $0 \leq \beta \leq 1$ is the reconciliation efficiency, $S_{BE}^{\epsilon_{PE}}$ 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 [29], [30]

$$\Delta_{AEP}(n) = (d+1)^2 + 4(d+1)\sqrt{\log_2(2/\epsilon_s)} + 2\log_2(2/(\epsilon^2\epsilon_s)) + 4\epsilon_s d/(\epsilon\sqrt{n}), \quad (18)$$

where d is the discretization parameter⁴, ϵ_s is a smoothing parameter corresponding to the speed of convergence of the smooth min-entropy, and ϵ_{PA} is the failure probability of the privacy amplification procedure. The parameters ϵ_s and ϵ_{PA} can be optimized computationally [31]. In the finite-size regime, one is limited to ϵ -security where $\epsilon = \epsilon_{EC} + 2\epsilon_s + \epsilon_{PA} + \epsilon_{PE}$ is the total failure probability of the protocol, and where ϵ_{EC} is the failure probability of the error correction.

Based on the equations for I_{AB} and $S_{BE}^{\epsilon_{PE}}$ in [24], we calculate the secret key rate against general attacks in the finite-size regime with the block size $n = 10^{12}$, $n/N = 0.5$, $\beta = 0.95$ and failure of probability (for general attacks) $\epsilon = 10^{-55}$. We use the trusted model in which the channel excess noise is untrusted and the detector excess noise is trusted. We use the values of the channel excess noise contributions in Table II which are obtained for our system model in the satellite-to-Earth channel. We have used the values from [24] to determine the variances V_{ta} and $V_{RIN,Atmos}$ and hence the excess noise contributions $\xi_{ta} = V_{ta}V_A$ and $\xi_{RIN,Atmos} = V_{RIN,Atmos}V_A$, respectively. We note that the time-of-arrival fluctuations contribution would be unchanged for the D-LLO with the exception that it is physically the timing between RP and signal. The reference pulse and signal intensity fluctuates due to the atmospheric turbulence, which adds the same amount of excess noise contribution $\xi_{RIN,Signal}$ and $\xi_{RIN,Atmos}$ as would be the case for the TLO scheme. Similarly, the intrinsic RIN of the LO $\xi_{RIN,LO}$ remains the same. Next, we use the value of (16) for the given $R_e = 60$ dB and $R_{po} = 30$ dB. The electronic noise is set to $v_{el} = 0.01$ and technical noise $\xi_{tech} = 0.005$.

In Fig. 2, we plot the secret key rate under general attacks in the finite-size regime versus the transmissivity in units of dB (i.e. $-10\log_{10} T$) at the zenith angles $\zeta = 0$ and $\zeta = 60^\circ$. The RP intensity is optimized to minimize the excess noise, and similarly $V_A = 1.5$ is chosen to maximize the secret key rate. For the zenith angle⁵ $\zeta = 60^\circ$, we find non-zero key rates

⁴ d is the bits of precision encoded by the symbol. In this work, we set $d = 5$ as in [29].

⁵We take the zenith angle $\zeta = 60^\circ$ to be the worst case scenario. In deployment, the satellite likely spends more time over the duration of the communication link at $\zeta < 60^\circ$.

of the D-LLO scheme up to a channel loss of 20 dB without AO and 22 dB with AO.

We also plot the key rate of the TLO scheme for comparison. For the TLO scheme, we used the noise model in [24] and the same system parameters. Evidently, the TLO performs much better overall and is feasible up to channels losses of 26 dB. However, the D-LLO scheme without AO is still feasible for channel losses up to 20 dB (22 dB with AO) which is readily achievable for diffraction dominated channel losses of 15 dB with transceiver aperture diameter $D_T = 0.3$ m, receiver aperture diameter $D_R = 3$ m and far-field divergence of $10 \mu\text{rad}$ [24].

V. CONCLUSION

In this work, we developed a practical noise model of a current state-of-the-art LLO scheme (the D-LLO scheme) in the satellite-to-Earth channel. We numerically simulated the coherent efficiency characterizing the wavefront aberration due to atmospheric turbulence in the satellite-to-Earth channel. Next, we calculated the expected secret key rates under general attacks in the deployable setting of the finite-size regime, showing that non-zero key rates can be obtained in diffraction-dominated satellite-to-Earth channels. In addition, we found that AO can reduce the excess noise to the point that an observable improvement of the key rates is forthcoming. In conclusion, we find that CV-QKD with an LLO in the satellite-to-Earth channel is indeed feasible. This work extends the scope of our previous work on a TLO scheme to an LLO scheme – the latter providing more security against practical attacks.

ACKNOWLEDGMENT

This research was funded through a Quantum Technologies Research Network Grant through the Defence Science & Technology Group, Australian Government.

REFERENCES

- [1] R. Bedington, J. M. Arrazola, and A. Ling, "Progress in satellite quantum key distribution," *npj Quantum Information*, vol. 3, no. 1, p. 30, 2017.
- [2] F. Laudenbach et al., "Continuous-variable quantum key distribution with gaussian modulation—the theory of practical implementations," *Advanced Quantum Technologies*, vol. 1, no. 1, p. 1800011, 2018.
- [3] K. Günthner et al., "Quantum-limited measurements of optical signals from a geostationary satellite," *Optica*, vol. 4, no. 6, pp. 611–616, 2017.
- [4] X.-C. Ma, S.-H. Sun, M.-S. Jiang, and L.-M. Liang, "Local oscillator fluctuation opens a loophole for eavesdropping in practical continuous-variable quantum-key-distribution systems," *Phys. Rev. A*, vol. 88, p. 022339, 2013.
- [5] J.-Z. Huang et al., "Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack," *Phys. Rev. A*, vol. 87, p. 062329, 2013.
- [6] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, "Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 87, p. 062313, 2013.
- [7] J.-Z. Huang et al., "Quantum hacking on quantum key distribution using homodyne detection," *Phys. Rev. A*, vol. 89, p. 032304, 2014.
- [8] D. Huang, P. Huang, D. Lin, C. Wang, and G. Zeng, "High-speed continuous-variable quantum key distribution without sending a local oscillator," *Opt. Lett.*, vol. 40, no. 16, pp. 3695–3698, 2015.
- [9] B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, "Generating the local oscillator 'locally' in continuous-variable quantum key distribution based on coherent detection," *Phys. Rev. X*, vol. 5, p. 041009, 2015.
- [10] D. B. S. Soh et al., "Self-referenced continuous-variable quantum key distribution protocol," *Phys. Rev. X*, vol. 5, p. 041010, 2015.
- [11] W. Zhao, R. Shi, and D. Huang, "Practical security analysis of reference pulses for continuous-variable quantum key distribution," *Scientific Reports*, vol. 9, no. 1, p. 18155, 2019.
- [12] B. Huang, Y. Huang, and Z. Peng, "Practical security of the continuous-variable quantum key distribution with real local oscillators under phase attack," *Opt. Express*, vol. 27, no. 15, pp. 20621–20631, 2019.
- [13] R. Shengjun et al., "Reference pulse attack on continuous variable quantum key distribution with local local oscillator under trusted phase noise," *J. Opt. Soc. Am. B*, vol. 36, no. 3, pp. B7–B15, 2019.
- [14] Y. Guo et al., "Phase estimation and compensation for continuous-variable quantum key distribution," *International Journal of Theoretical Physics*, vol. 58, no. 5, pp. 1613–1625, 2019.
- [15] M. Zou, Y. Mao, and T.-Y. Chen, "Phase estimation using homodyne detection for continuous variable quantum key distribution," *Journal of Applied Physics*, vol. 126, no. 6, p. 063105, 2019.
- [16] A. Marie and R. Alléaume, "Self-coherent phase reference sharing for continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 95, p. 012316, 2017.
- [17] T. Wang, P. Huang, Y. Zhou, W. Liu, and G. Zeng, "Pilot-multiplexed continuous-variable quantum key distribution with a real local oscillator," *Phys. Rev. A*, vol. 97, p. 012310, 2018.
- [18] T. Wang et al., "High key rate continuous-variable quantum key distribution with a real local oscillator," *Opt. Express*, vol. 26, no. 3, pp. 2794–2806, 2018.
- [19] E. Villaseñor, R. Malaney, K. A. Mudge, and K. J. Grant, "Atmospheric effects on satellite-to-ground quantum key distribution using coherent states," *arXiv:2005.10465*, 2020 (unpublished).
- [20] S. Ren et al., "Noise and security analysis of trusted phase noise continuous variable quantum key distribution using a local local oscillator," in *2019 IEEE 20th International Workshop on Signal Processing Advances in Wireless Communications*, 2019, pp. 1–5.
- [21] S. Wang, P. Huang, T. Wang, and G. Zeng, "Atmospheric effects on continuous-variable quantum key distribution," *New Journal of Physics*, vol. 20, no. 8, p. 083037, 2018.
- [22] D. Dequal et al., "Feasibility of satellite-to-ground continuous-variable quantum key distribution," *arXiv:2002.02002*, 2020 (unpublished).
- [23] M. Li and T. Wang, "Continuous-variable quantum key distribution over air quantum channel with phase shift," *IEEE Access*, vol. 8, pp. 39 672–39 677, 2020.
- [24] S. P. Kish, E. Villaseñor, R. Malaney, K. A. Mudge, and K. J. Grant, "Feasibility assessment for practical continuous variable quantum key distribution over the satellite-to-earth channel," *Quantum Engineering*, p. e50, e50 QUE-2020-0013.R1.
- [25] H. Jian et al., "Effectiveness of adaptive optics system in satellite-to-ground coherent optical communication," *Opt. Express*, vol. 22, no. 13, pp. 16 000–16 007, 2014.
- [26] Y. Wang et al., "Performance improvement of free-space continuous-variable quantum key distribution with an adaptive optics unit," *Quantum Information Processing*, vol. 18, no. 8, p. 251, 2019.
- [27] G. Chai, P. Huang, Z. Cao, and G. Zeng, "Suppressing excess noise for atmospheric continuous-variable quantum key distribution via adaptive optics approach," *New Journal of Physics*, 2020 (in press).
- [28] J. E. Krist, "PROPER: an optical propagation library for IDL," in *Optical Modeling and Performance Predictions III*, M. A. Kahan, Ed., vol. 6675, International Society for Optics and Photonics. SPIE, 2007, pp. 250 – 258.
- [29] C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, "Continuous-variable measurement-device-independent quantum key distribution: Composable security against coherent attacks," *Phys. Rev. A*, vol. 97, p. 052327, 2018.
- [30] A. Leverrier, "Composable security proof for continuous-variable quantum key distribution with coherent states," *Phys. Rev. Lett.*, vol. 114, p. 070501, 2015.
- [31] A. Leverrier, F. Grosshans, and P. Grangier, "Finite-size analysis of a continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 81, p. 062343, 2010.