

Quantum Communications via Satellite with Photon Subtraction

Mingjian He¹, Robert Malaney¹ and Jonathan Green²

Abstract—Non-Gaussian continuous-variable quantum states represent a pivotal resource in many quantum information protocols. Production of such states can occur through photonic subtraction processes either at the transmitter side prior to sending a state through the channel, or at the receiver side on receipt of a state that has traversed the channel. In the context of quantum protocols implemented over communication channels to and from Low-Earth-Orbit (LEO) satellites it is unclear what photonic subtraction set-up will provide for the best performance. In this work we show that for a popular version of continuous-variable Quantum Key Distribution (QKD) between terrestrial stations and LEO satellites, photon subtraction at the transmitter side is the preferred set-up. Such a result is opposite to that found for fiber-based implementations. Our results have implications for all future space-based missions that seek to take advantage of the opportunities offered by non-Gaussian quantum states.

I. INTRODUCTION

Quantum Communications via satellite offers a paradigm shift in our ability to deploy quantum information protocols over very large scales, e.g. [1]–[4]. Propagation through the atmosphere to and from LEO satellites can overcome the scourge of the roughly 100km limited distance that plagues point-to-point optical-fiber optical links and free-space-optical links. Indeed, in the past few years great strides have been made in regard to actual deployments of quantum communications via satellites [5]–[9]. These latter works on satellite-based quantum communications are largely based on the deployment of discrete-variable (DV) quantum information protocols, a technology that is dependent on the production of single-photon states.

Continuous-variable (CV) technology offers a different pathway to the implementation of quantum information protocols. The main advantage of CV technology over DV technology is that detection can be realized by more reliable, and more efficient homodyne (or heterodyne) detectors e.g., [10]–[13]. Indeed, it is argued by many that relative to DV detectors, CV based-detectors offer the promise of a more pragmatic route to higher secret key rates for certain QKD protocols, e.g. [14].

Currently, no experimental deployment of space-based CV quantum technology has been carried out, but this is expected to change soon (see [4] for review). CV technologies are largely based around so-called Gaussian states, e.g. [12], [13] - quantum states in which the quasi-probability distribution (the Wigner function) of the electromagnetic-field quadratures follow a Gaussian distribution. However, the use of non-Gaussian

states in the implementation of CV quantum information protocols has also garnered interest, e.g. [15]–[19]. Non-Gaussian operations such as photon subtraction (PS) [20]–[26] on a mode of an incoming two mode squeezed vacuum (TMSV) state can lead to higher levels of entanglement, potentially higher secret (QKD) key rates, as well as forming a pivotal resource for quantum error correction.

In this work we will focus on single PS as a means to produce non-Gaussian states. We will be specifically focussed on the question as to whether PS at the transmitter offers a better pathway to improved QKD (higher secret key rates) when propagation between ground stations and LEO satellites is considered. The answer to this question has important implications not only for future space-based implementations of CV-QKD protocols, but also potentially for other space-based quantum information protocols that utilize non-Gaussian states.

The structure of the remainder of this paper is as follows. In Section II, the nature of the quantum channel between terrestrial stations and LEO satellites is described. In Section III, a model for CV-QKD with PS at the transmitter is described, whilst in Section IV a system for PS at the receiver is described. In Section V our performance analysis is described, and in Section VI our simulation results are presented, comparing key rates produced from both systems.

II. EARTH-SATELLITE CHANNELS

We consider the model of single uplink and single downlink satellite channels in an entanglement-based version of a CV-QKD protocol.¹ Our quantum information carrier will be a pulsed optical beam. For the uplink, we assume that Alice first prepares a TMSV state ($A_0 - B_0$) at a ground station, subsequently sending one of her modes (B_0) to the satellite. For the downlink, the TMSV is prepared on the satellite with B_0 being sent to the ground station.

For optical signals in the uplink channel, the dominant loss mechanism will be beam-wander caused by turbulence in the Earth's atmosphere [27]. Assuming the beam spatially fluctuates around the receiver's center point, the fading of the signal as a consequence of the beam-wander can be described by a distribution of transmission coefficients (amplitude attenuation) η . The probability density distribution of these coefficients, $p(\eta)$, can be approximated by the log-negative Weibull distribution, given by [29] [30]

Mingjian He and Robert Malaney (email: r.malaney@unsw.edu.au) are with the School of Electrical Engineering and Telecommunications, the University of New South Wales, Sydney, NSW, Australia. Jonathan Green is with Northrop Grumman Mission Systems, San Diego, California, USA. Approved For Public Release #18-1963; Unlimited Distribution. Dated 9/13/18.

¹Each entanglement-based QKD protocol has an equivalent prepare and measure scheme that will give, in theory, exactly the same results.

$$p(\eta) = \frac{2L^2}{\sigma_b^2 \lambda \eta} \left(2 \ln \frac{\eta_0}{\eta}\right)^{\left(\frac{2}{\lambda}\right)-1} \exp\left(-\frac{L^2}{2\sigma_b^2} \left(2 \ln \frac{\eta_0}{\eta}\right)^{\left(\frac{2}{\lambda}\right)}\right) \quad (1)$$

for $\eta \in [0, \eta_0]$, with $p(\eta) = 0$ otherwise. Here, σ_b^2 is the beam wander variance, λ is the shape parameter, L is the scale parameter, and η_0 is the maximum transmission value. The latter three parameters are given by

$$\begin{aligned} \lambda &= 8h \frac{\exp(-4h)I_1[4h]}{1-\exp(-4h)I_0[4h]} \left[\ln \left(\frac{2\eta_0^2}{1-\exp(-4h)I_0[4h]} \right) \right]^{-1}, \\ L &= \beta_r \left[\ln \left(\frac{2\eta_0^2}{1-\exp(-4h)I_0[4h]} \right) \right]^{-(1/\lambda)}, \\ \eta_0^2 &= 1 - \exp(-2h), \end{aligned} \quad (2)$$

where $I_0[\cdot]$ and $I_1[\cdot]$ are the modified Bessel functions, and where $h = (\beta_r/W)^2$, with β_r being the aperture radius and W the beam-spot radius. Here we set $\beta_r = W = 1$ unit length (which for typical configurations is 1 meter).

In the downlink satellite channel diffraction effects are anticipated to dominate. This is largely because beam-wander in the downlink is relatively suppressed since the beam-width, on entry into the atmosphere from space, is generally broader than the scale of the turbulent eddies [27]. As such, with well-engineered designs² losses in the downlink can be as small as 5-10 dB, compared to the 20-30 dB losses that can be anticipated for well-engineered uplink channels. For simplicity, we model all losses by varying σ_b .

To investigate the effect of the PS we mainly consider three schemes. The first scheme is where there is no PS (No-PS). The second scheme is PS at the transmitter side (T-PS), where the PS is performed immediately after Alice prepares her TMSV state. The last scheme is PS at the receiver side (R-PS), where Bob performs the PS after he receives the mode from Alice, but before his homodyne measurement. We adopt the QKD protocol of [31], modified as required for our additional T-PS scheme. Reverse reconciliation at Alice, in which both Alice and Bob undertake homodyne measurements is always used. We will assume the asymptotic limit in the number of measurements taken.

III. PHOTON SUBTRACTION AT TRANSMITTER SIDE

The system model for the CV-QKD protocol with photon subtraction is illustrated in Fig. 1. We assume that Alice first prepares a TMSV $A_0 - B_0$ at her ground station (for brevity we just describe the uplink). She then sends one of her modes (B_0) through a PS process in which B_0 interacts with a mode C_0 at a beam-splitter with transmissivity (intensity attenuation) T_S . One of the exiting modes (C) is sent to a photodetector

²This involves properly-dimensioned lenses, use of state-of-the-art adaptive optics, and use of feedback from concurrent classical channel measurements. On the latter measurements we note fluctuations caused by turbulence are in the kHz range (compared to the Mhz rate of the laser pulses), thus allowing for channel-coefficient measurements to be made dynamically (within the coherence time of the channel) by a ground receiver.

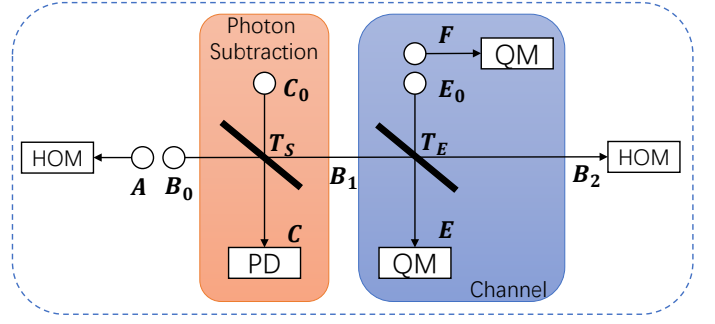


Fig. 1. Photon subtraction at transmitter side (T-PS). Here Alice (ground station) prepares a TMSV ($A_0 - B_0$), sending B_0 through a PS process using a beam-splitter with transmissivity T_S . The exiting mode C is sent to a photodetector, whilst the exiting B_1 is sent to Bob (the satellite). The channel is controlled by Eve using a second beam-splitter with transmissivity T_E .

(PD), whilst the other (B_1) is sent to Bob (the satellite). In the following we take mode C_0 to be a vacuum state.³

In this work we assume that Eve performs a collective attack.⁴ The channel can then be modeled by Eve feeding one mode, E_0 , of a TMSV state ($E_0 - F$) prepared by her into a beam-splitter with transmissivity T_E , with B_1 being fed into the other input mode of the beam-splitter. After passing through Eve's beam-splitter, Eve retains the quantum state $F - E$, E being one of the output modes of her beam-splitter. The other output mode of the beam-splitter is forwarded to Bob. Setting $T_E = \eta^2$, we assume that Eve sets T_E so as to follow a probability density function given by equations (1)-(2). Following its traversal through the channel Bob then receives an "attenuated" version of B_1 , namely B_2 .

Note that PS is not a Gaussian operation, but rather an operation that transforms a Gaussian state into a non-Gaussian state. Because of this, the state following the PS cannot be fully described by the first and second moment of the quadrature operators \hat{x} and \hat{q} of the electromagnetic field. As such, a somewhat more complex state description is required relative to that used for quantum protocols based on Gaussian states. We now describe this more complex quantum state.

Using the Fock basis, Alice's initial TMSV state $|\psi\rangle_{AB_0}$ has the form

$$|\psi\rangle_{AB_0} = \sum_{n=0}^{\infty} \alpha_n |n, n\rangle_{AB_0},$$

with

$$\alpha_n = \sqrt{\frac{\alpha^{2n}}{(1 + \alpha^2)^{n+1}}},$$

³We note that a PS at the transmitter in the context of a somewhat different QKD protocol from that studied here has been investigated for the Earth-satellite channel [28].

⁴A collective attack is where Eve creates a series of ancillary modes with a member from this series independently entangling with each incoming mode sent by Alice. Following Bob's measurements Eve then takes an optimal collective measurement on her series of ancillary modes. In the asymptotic limit, security under collective attacks can be shown to be equivalent to security under coherent attacks (for many protocols) in which Eve's ancillary modes are no longer constrained to interact independently with Alice's modes.

where α^2 is the mean photon number of Alice's mode. We note that $\alpha^2 = \sinh^2 r$, where r is the squeezing parameter of the two-mode squeezing operator

$$S(\xi) = \exp\left(\xi \hat{a} \hat{b} - \xi \hat{a}^\dagger \hat{b}^\dagger\right), \quad \xi = r e^{i\theta},$$

where θ represents the orientation of the squeezing, and where \hat{a} and \hat{a}^\dagger represent the annihilation and creation operators, respectively, of mode A . Here, we assume $\theta = 0$.

Result 1: The quantum state after the channel can be written as

$$|\psi\rangle_{TPS} = -\frac{1}{\sqrt{P_1}} \sum_{n=1}^{\infty} \sum_{k=0}^{n-1} \sum_{m=0}^{\infty} \sum_{l=0}^m s_{n,k,m,l} \times |n, n-1-k+l, k+m-l, m\rangle_{AB_2EF},$$

where $s_{n,k,m,l} = \alpha_n \beta_m (-1)^k r_{n,1}^{TS} r_{n-1,k}^{TE} r_{m,l}^{TE} z_{n-1,k,m,l}$, and the other variables introduced above are defined in the following proof.

Proof: Initially we have the following description of the combined $AB_0C_0B_1C$ mode

$$\begin{aligned} |\psi\rangle_{AB_0C_0B_1C} &= \sum_{n=0}^{\infty} \alpha_n |n, n\rangle_{AB_0} |0, 0, 0\rangle_{C_0B_1C} \\ &= \sum_{n=0}^{\infty} \alpha_n \frac{(\hat{b}_0^\dagger)^n}{\sqrt{n!}} |n, 0\rangle_{AB_0} |0, 0, 0\rangle_{C_0B_1C}. \end{aligned}$$

The presence of the beam-splitter at the PS stage alters this combined mode to the form

$$\begin{aligned} &\sum_{n=0}^{\infty} \alpha_n \frac{(\sqrt{T_S} \hat{b}_1^\dagger - \sqrt{1-T_S} \hat{c}^\dagger)^n}{\sqrt{n!}} |n, 0\rangle_{AB_0} |0, 0, 0\rangle_{C_0B_1C} \\ &= \sum_{n=0}^{\infty} \alpha_n \sum_{k=0}^n (-1)^k r_{n,k}^{TS} |n, 0\rangle_{AB_0} |0, n-k, k\rangle_{C_0B_1C}, \end{aligned}$$

where $r_{n,k}^T = \sqrt{\binom{n}{k}} (\sqrt{T})^{n-k} \sqrt{1-T}^k$. We assume that the subtraction is for the single photon case (i.e. $k = 1$ and $C = |1\rangle$). Tracing out mode B_0 , C , and C_0 we have,

$$|\psi\rangle_{AB_1} = -\frac{1}{\sqrt{P_1}} \sum_{n=1}^{\infty} \alpha_n r_{n,1}^{TS} |n, n-1\rangle_{AB_1},$$

where

$$P_1 = \sum_{n=1}^{\infty} \left(\alpha_n r_{n,1}^{TS} \right)^2$$

is the probability of subtracting one photon. Similar to Alice, Eve's initial TMSV state is,

$$|\psi\rangle_{E_0F} = \sum_{m=0}^{\infty} \beta_m |m, m\rangle_{E_0F}$$

with

$$\beta_m = \sqrt{\frac{\beta^{2m}}{(1+\beta^2)^{m+1}}},$$

where β^2 is the mean photon number of Eve's mode - a parameter used to simulate the channel noise.

As it passes the channel, mode B_1 evolves to mode B_2 . Prior to Eve acting on the incoming states we have the following description of the combined $AB_1E_0EFB_2$ mode

$$\begin{aligned} |\psi\rangle_{AB_1E_0EFB_2} &= -\frac{1}{\sqrt{P_1}} \sum_{n=1}^{\infty} \alpha_n r_{n,1}^{TS} |n, n-1\rangle_{AB_1} \\ &\quad \otimes \sum_{m=0}^{\infty} \beta_m |m, m\rangle_{E_0F} |0, 0\rangle_{B_2E}. \end{aligned}$$

The presence of the beam-splitter at Eve alters this combined mode to the form

$$\begin{aligned} &-\frac{1}{\sqrt{P_1}} \sum_{n=1}^{\infty} \alpha_n r_{n,1}^{TS} \frac{(\sqrt{T_E} \hat{b}_2^\dagger - \sqrt{1-T_E} \hat{e}^\dagger)^{n-1}}{\sqrt{(n-1)!}} |n, 0\rangle_{AB_1} \\ &\quad \otimes \sum_{m=0}^{\infty} \beta_m \frac{(\sqrt{T_E} \hat{e}^\dagger + \sqrt{1-T_E} \hat{b}_2^\dagger)^m}{\sqrt{m!}} |0, m\rangle_{E_0F} |0, 0\rangle_{B_2E} \\ &= -\frac{1}{\sqrt{P_1}} \sum_{n=1}^{\infty} \alpha_n r_{n,1}^{TS} \sum_{k=0}^{n-1} (-1)^k r_{n-1,k}^{TE} \\ &\quad \times \sum_{m=0}^{\infty} \beta_m \sum_{l=0}^m r_{m,l}^{TE} z_{n-1,k,m,l} \\ &\quad \times |n, n-1-k+l, k+m-l, m, 0, 0\rangle_{AB_2EFB_1E_0}, \end{aligned}$$

where

$$z_{n,k,m,l} = \sqrt{\binom{n-k+l}{l}} \sqrt{\binom{k+m-l}{k}}.$$

Rearranging the summation and tracing out B_1 and E_0 we arrive at the Result 1.

IV. PHOTON SUBTRACTION AT RECEIVER SIDE

If the photon subtraction occurs at the receiver side instead of the transmitter side (Fig. 2), a different outcome is achieved for the final state - a result previously derived in [31]. We simply provide that result here (the proof follows a similar path to that given for PS at the transmitter). However, we note the work of [31] considers the fixed-attenuation channel only, and therefore the results of that work cannot be directly utilized for the Earth-satellite channels we are concerned with here.

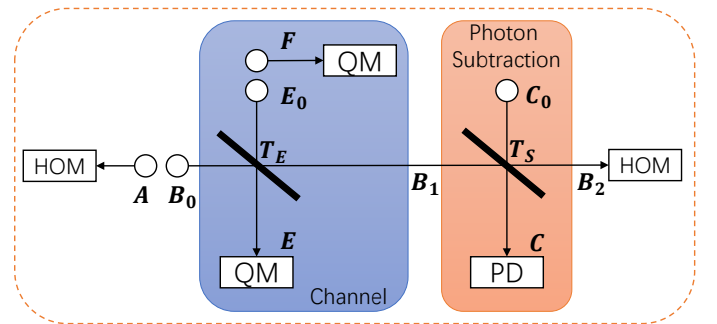


Fig. 2. Photon subtraction at receiver side (R-PS). Here Alice (ground station) prepares a TMSV ($A_0 - B_0$), sending B_0 through a channel controlled by Eve using a beam-splitter with transmissivity T_E . The exiting mode B_1 is sent by Eve to Bob (the satellite) who undertakes a PS process on B_1 using a beam-splitter with transmissivity T_S , leading to B_2 .

Prior to the PS at the receiver the quantum state is given by

$$\begin{aligned} |\psi\rangle_{AB_1EF} &= \sum_{n=0}^{\infty} \sum_{k=0}^n \sum_{m=0}^{\infty} \sum_{l=0}^m \alpha_n \beta_m (-1)^k r_{n,k}^{TE} r_{m,l}^{TE} z_{n,k,m,l} \\ &\quad \times |n, n-k+l, k+m-l, m\rangle_{AB_1EF}. \end{aligned}$$

After the channel, Bob performs PS on B_1 , leading to the B_2 mode. This latter mode is subsequently used in Bob's homodyne detection.

Result 2: The photon subtracted quantum state at the receiver can be written

$$|\psi\rangle_{RPS} = \frac{1}{\sqrt{P_1}} \sum_{n=0}^{\infty} \sum_{k=0}^n \sum_{m=0}^{\infty} \sum_{l=0}^m s'_{n,k,m,l} \times |n, n-1-k+l, k+m-l, m\rangle_{AB_2EF},$$

where $s'_{n,k,m,l} = \alpha_n \beta_m (-1)^k r_{n-k+l,1}^{T_S} r_{n,k}^{T_E} r_{m,l}^{T_E} z_{n,k,m,l}$ and P_1 is a new normalization constant (cf. Eq. (19) of [31]).

V. PERFORMANCE ANALYSIS

A. Covariance Matrix

Before moving into our investigation of the secret key rate we note that the covariance matrix of a given state $|\psi\rangle_{AB}$ with two modes A and mode B , can be written as

$$\mathbf{M}_{AB} = \begin{bmatrix} V_A \mathbf{I} & C_{AB} \sigma \\ C_{AB} \sigma & V_B \mathbf{I} \end{bmatrix},$$

where $\mathbf{I} = \text{diag}(1, 1)$, $\sigma = \text{diag}(1, -1)$. Here,

$$V_A = \langle \psi | 1 + 2\hat{a}^\dagger \hat{a} | \psi \rangle_{AB}$$

is the variance of mode A (likewise V_B), and

$$C_{AB} = \langle \psi | \hat{a} \hat{b} + \hat{a}^\dagger \hat{b}^\dagger | \psi \rangle_{AB}$$

is the covariance between mode A and mode B .

Consider next the variances of mode A and mode F following PS at the transmitter. Using the above, we can see that the variances of mode A and F can be given as,

$$\begin{aligned} V_A &= \langle \psi | 1 + 2\hat{a}^\dagger \hat{a} | \psi \rangle_{TPS} \\ &= 1 - \frac{2}{\sqrt{P_1}} \langle \psi | \sum_{n=1}^{\infty} \sum_{k=0}^{n-1} \sum_{m=0}^{\infty} \sum_{l=0}^m n s_{n,k,m,l} \\ &\quad \times |n, n-1-k+l, k+m-l, m\rangle_{AB_2EF}, \end{aligned}$$

$$\begin{aligned} V_F &= \langle \psi | 1 + 2\hat{f}^\dagger \hat{f} | \psi \rangle_{TPS} \\ &= 1 - \frac{2}{\sqrt{P_1}} \langle \psi | \sum_{n=1}^{\infty} \sum_{k=0}^{n-1} \sum_{m=0}^{\infty} \sum_{l=0}^m m s_{n,k,m,l} \\ &\quad \times |n, n-1-k+l, k+m-l, m\rangle_{AB_2EF}, \end{aligned}$$

respectively. Likewise, the covariance between two different modes, say E and F , can be given by

$$\begin{aligned} C_{EF} &= \langle \psi | \hat{e} \hat{f} + \hat{e}^\dagger \hat{f}^\dagger | \psi \rangle_{TPS} \\ &= -\frac{1}{\sqrt{P_1}} \langle \psi | \varphi \rangle, \end{aligned}$$

where

$$\begin{aligned} |\varphi\rangle &= \sum_{n=1}^{\infty} \sum_{k=0}^{n-1} \sum_{m=0}^{\infty} \sum_{l=0}^m s_{n,k,m,l} \sqrt{m+1} \sqrt{k+m-l+1} \\ &\quad \times |n, n-1-k+l, k+m-l+1, m+1\rangle_{AB_2EF} + \\ &\quad \sum_{n'=1}^{\infty} \sum_{k'=0}^{n'-1} \sum_{m'=0}^{\infty} \sum_{l'=0}^{m'-1} s_{n',k',m',l'} \sqrt{m'} \sqrt{k'+m'-l'} \\ &\quad \times |n', n'-1-k'+l', k'+m'-l'-1, m'-1\rangle_{AB_2EF}. \end{aligned}$$

Similar variance and covariance terms can be derived for PS at the receiver. These terms can be calculated numerically simply by using the fact that $\langle n, k, m, l | n', k', m', l' \rangle = \delta_{nkm, n'k'm'l'}$. The usefulness of such terms will become evident when we calculate the keys rates, an issue we turn to next.

B. The Secret Key Rate

Under a collective attack, the key rate is related to the difference of $I(A : B_2)$ - the mutual information between mode A and mode B_2 ; and $\chi(B_2 : EF)$ - the Holevo information that Eve can extract from her measurement [13]. More specifically, we can say, the key rate (per pulse generated by the source laser) is,

$$K(T_E) = P [f I(A : B_2) - \chi(B_2 : EF)],$$

where f is the decoding reconciliation efficiency, and P is the probability of subtracting one photon in the PS. However, calculation of the key rate for a non-Gaussian state is analytically not tractable since the non-Gaussian state has more than two non-zero moments. To make progress, we utilize the Gaussian state (metrics of which will be indicated by the subscript G) that produces the same covariance matrix \mathbf{M} as the non-Gaussian state $|\psi\rangle_{AB_2EF}$. This provides a lower bound for the key rate by the theorem of Gaussian optimality [32]. Emphasizing that all key rates discussed from this point on are bounds, we have⁵

$$K(T_E) \geq P [f I_G(A : B_2) - \chi_G(B_2 : EF)],$$

where [13]

$$I_G(A : B_2) = \frac{1}{2} \log_2 \frac{V_{B_2}}{V_{B_2|A}},$$

and the conditional variance $V_{B_2|A}$ is

$$V_{B_2|A} = V_{B_2} - \frac{C_{AB_2}^2}{V_A}.$$

For Eve's stolen information, we can write

$$\chi_G(B_2 : EF) = \sum_i g(v_i^{EF}) - \sum_j g(v_j^{EF|B_2}),$$

where

$$g(v) = \frac{v+1}{2} \log_2 \frac{v+1}{2} - \frac{v-1}{2} \log_2 \frac{v-1}{2}.$$

In the above, v^{EF} and $v^{EF|B_2}$ are the symplectic eigenvalues of the covariance matrices \mathbf{M}_{EF} and $\mathbf{M}_{EF|B_2}$, respectively, where [13]

$$\mathbf{M}_{EF|B_2} = \mathbf{M}_{EF} - \begin{bmatrix} C_{EB_2} \mathbf{I} \\ C_{FB_2} \sigma \end{bmatrix} \begin{bmatrix} V_{B_2}^{-1} & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} C_{EB_2} \mathbf{I} \\ C_{FB_2} \sigma \end{bmatrix}^T.$$

Finally, we can now determine the bound on the key rate achieved in the satellite lossy channel by taking the average over all possible transmission coefficient values, namely, $K_{avg} = \int p(\eta) K(\eta^2) d\eta$. Allowing the initial squeezing to be dependent on η allows for further optimization of the key rate - an issue we ignore for simplicity.

VI. SIMULATION RESULTS

For comparison purposes we first consider a non-variable attenuation channel, before comparing the performance of our three schemes for the satellite channel we have discussed

⁵Note, the beam-splitter attack we use is the most pragmatic, but it is slightly sub-optimal. Under an optimal attack (purification), the key rate will be approximately 1.1dB lower for all our schemes.

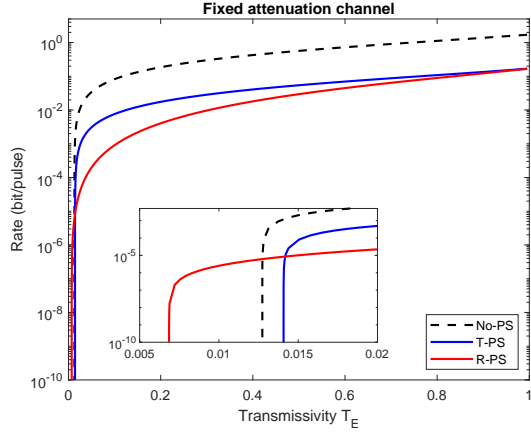


Fig. 3. The key rate vs. transmissivity.

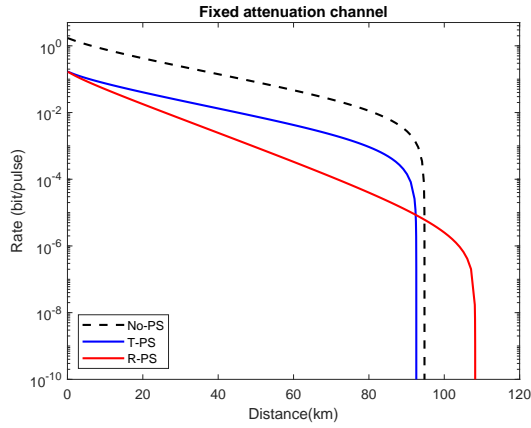


Fig. 4. The key rate vs. distance.

earlier in the paper. Unless otherwise stated, the parameters utilized in the calculations shown are $\alpha^2 = 1.3$, $\beta^2 = 0.001$, $f = 0.95$, and $T_S = 0.9$ (for simplicity a detector efficiency of 1 is assumed). The infinite summation limits are constrained to 20 for n and m [33].

As stated, we first consider a fixed attenuation channel. Here we fix the value of α^2 for all attenuation conditions. We plot the key rate against transmissivity in Fig. (3), and against distance in Fig. (4). In Fig. (4) we assume that the channel has a fixed attenuation of 0.2dB/km. The results of Figs. (3)-(4) show that the R-PS scheme has the longest key distribution range at a cost of a reduced key rate. That is, the R-PS scheme is in some sense the most robust against channel attenuation (provides a non-zero key rate at the largest distance). We further compare the performance of the three schemes as a function of the noise β^2 and the mean photon number α^2 (i.e. $\sinh^2 r$, r being the squeezing parameter) - the results of which are shown in Figs. (5) and (6), respectively. Note, that in these figures the rates are not plotted in the logarithmic domain so the comparison in the small rate region is not as apparent. As can be seen, for some parameter space we find distances where the T-PS scheme shows better key rate performance than the other schemes. We also find the T-PS and R-PS schemes can outperform the No-PS scheme in some parameter space (again we caution that optimisation of the initial squeezing can alter

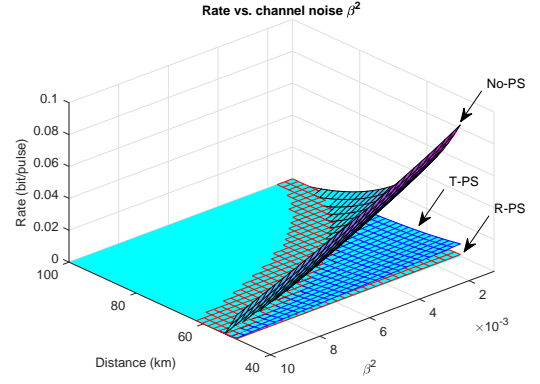


Fig. 5. The key rate over the fixed channel for different noise conditions. The top, middle, and bottom layers are No PS, T-PS and R-PS, respectively.

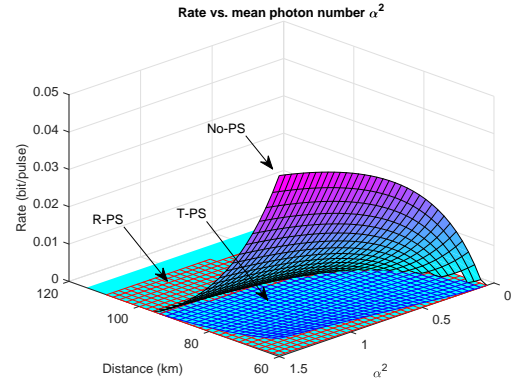


Fig. 6. The key rate over the fixed channel for different mean photon number. The top, middle, and bottom layers are No PS, T-PS and R-PS, respectively.

these conclusions).

We next investigate the key rates of the three schemes in the variable Earth-satellite channel, calculating their average key rates under different average channel fluctuations, quantified using σ_b within equations (1)-(2). These results are shown in Fig. (7). The No-PS case shows better performance in terms of key rate for the entire range of channel conditions - a result not found for the fixed attenuation case. The PS cases (T-PS and R-PS) are impacted by the low probability of obtaining a subtracted photon in any given pulse, and this effect dominates when channel averaging over the fading channel is accounted for. The blue dashed curve (marked normalized) in Fig. (7) show the impact of a quantum memory in place such that the low probability for PS can be negated. Here the schemes are assumed to be *a priori* storing the required states in memory, then sending the same rate of quantum states into the satellite channel on-demand. A close up at low σ_b is shown in Fig. (8) for different noise conditions. These latter results show the rates possible in very-high quality downlinks from the satellite-to-Earth.⁶

A main aim of our study was to determine whether PS at the

⁶ Note that $\sigma_b = 1$ corresponds to approximately 5dB of loss. Such low loss rates are possible for well-engineered systems in which diffraction of the beam is the major factor contributing to photon loss.

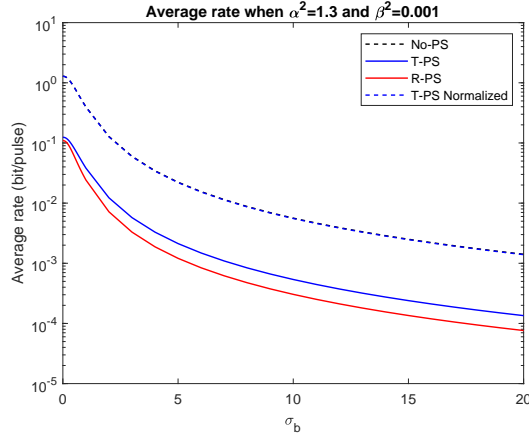


Fig. 7. The key rate averaged over the satellite channel as a function of the standard deviation of the beam wandering for range 0-20.

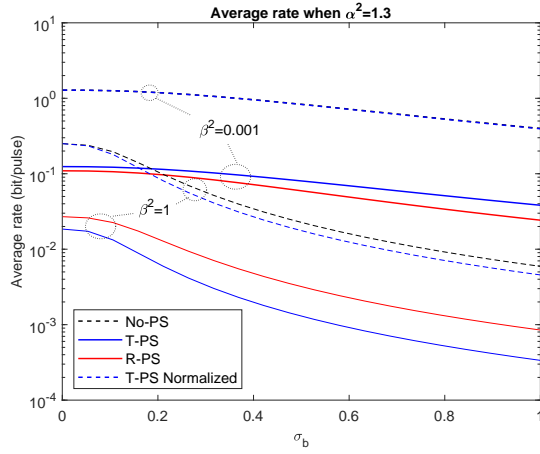


Fig. 8. A close up of the key rate averaged over the satellite channel as a function of the standard deviation of the beam wandering for the range 0-1.

transmitter-side outperforms PS at the receiver-side for a range of Earth-Satellite channels (where no instantaneous channel-dependent optimisation of squeezing occurs at the transmitter). Figs. (7)-(8) provide an answer to this question - yes. This result holds for all anticipated channel conditions (only at unrealistic noise levels is the opposite found).

VII. CONCLUSIONS

We have studied the use of non-Gaussian CV quantum states - created via photon subtraction - in the context of a straightforward QKD protocol. More specifically, we have studied the lower-bounds on secret key rates delivered by such states. Contrary to what is found in fixed attenuation channels (such as optical fiber), we find that for the variable-channels anticipated for Earth-satellite communications, photon subtraction at the transmitter, for an initially fixed squeezing, outperforms photon subtraction at the receiver for all realistic conditions. The authors acknowledge support from the UNSW, the CSC, and Northrop Grumman.

REFERENCES

- [1] R. Bedington, J. M. Arrazola, and A. Ling, "Progress in satellite quantum key distribution," *Npj Quantum Information* 3, 30, (2017).
- [2] N. Hosseinihahaj and R. Malaney, "Gaussian entanglement distribution via satellite," *Phys. Rev. A* 91, 022304 (2015).
- [3] N. Hosseinihahaj and R. Malaney, "Quantum key distribution over combined atmospheric fading channels," in *Proceedings of IEEE Int. Conf. on Communications (ICC)*, pp. 7413-7419, (2015).
- [4] N. Hosseinihahaj, et al., "Satellite-based CV quantum communications: State-of-the-art and a predictive outlook," *IEEE Communications Surveys & Tutorials*, doi:10.1109/COMST.2018.2864557 (2018).
- [5] S. Liao, et al., "Satellite-to-ground QKD," *Nature* 549, pp. 43-47 (2017).
- [6] J. Yin, et al., "Satellite-based entanglement distribution over 1200 kilometers," *Science* 356, pp. 1140-1144 (2017).
- [7] J.-G. Ren, et al., "Ground-to-satellite quantum teleportation," *Nature* 549, pp. 70-73 (2017).
- [8] K. Gunthner, et al., "Quantum-limited measurements of optical signals from a geostationary satellite," *Optica* 4, 611 616 (2017).
- [9] H. Takenaka, et al., "Satellite-to-ground quantum-limited comms. using a 50-kg-class microsatellite," *Nat. Phot.* Vol. 11, pp. 502-508 (2017).
- [10] F. Grosshans, et al., "High-rate quantum cryptography using Gaussian modulated coherent states," *Nature* 421, 238 (2003).
- [11] V. Scarani, et al., "The security of practical quantum key distribution," *Rev. Mod. Phys.* 81, 1301 (2009).
- [12] R. Garcia-Patron, Ph.D. thesis, Universite Libre de Bruxelles, (2007).
- [13] C. Weedbrook, et al., "Gaussian quantum information," *Rev. Mod. Phys.* 84, 621 (2012).
- [14] S. Pirandola, et al., "MDI-QKD: Continuous - versus discrete-variables at metropolitan distances," *Nature Photonics* 9, 773-775 (2015).
- [15] A. Leverrier, and P. Grangier, "CV quantum-key-distribution protocols with a non-Gaussian modulation," *Phys. Rev. A* 83, 042312 (2011).
- [16] P. Huang, G. He, J. Fang, and G. Zeng, "Performance improvement of continuous-variable quantum key distribution via photon subtraction," *Phys. Rev. A* 87, 012317 (2013).
- [17] Z. Li, et al., "Non-Gaussian post-selection and virtual photon subtraction in CV quantum key distribution," *Phys. Rev. A* 93, 012310 (2016).
- [18] L. F. M. Borelli, et al., "Quantum key distribution using CV non-Gaussian states," *Quantum Information Processing* 15, 893 (2016).
- [19] N. Hosseinihahaj and R. Malaney, "Entanglement generation via non-Gaussian transfer over atmospheric fading channels," *Phys. Rev. A* 92, 062336 (2015).
- [20] T. Opatrny, G. Kurizki, and D.-G. Welsch, "Improvement on teleportation of continuous variables by photon subtraction via conditional measurement," *Phys. Rev. A* 61, 032302 (2000).
- [21] A. Kitagawa, et al., "Entanglement evaluation of non-Gaussian states generated by photon subtraction," *Phys. Rev. A* 73, 042310 (2006).
- [22] Y. Yang and F.-L. Li, "Entanglement properties of non-Gaussian resources generated via photon subtraction and addition and CV quantum-teleportation improvement," *Phys. Rev. A* 80, 022315 (2009).
- [23] S. L. Zhang, and P. van Loock, "Distillation of mixed-state CV entanglement by photon subtraction," *Phys. Rev. A* 82, 062316 (2010).
- [24] K. P. Seshadreesan, J. P. Dowling, and G. S. Agarwal, "Non-Gaussian entangled states and quantum teleportation of Schrodinger-cat states," *Phys. Scr.* 90, 074029 (2015).
- [25] T. J. Bartley and I. A. Walmsley, "Directly comparing entanglement-enhancing non-Gaussian operations," *New J. Phys.* 17, 023038 (2015).
- [26] Y. Zhao, et al., "Improvement of two-way CV QKD with virtual photon subtraction," *Quantum Information Processing* 16, 184 (2017).
- [27] L. C. Andrews and R. L. Phillips, "Laser Beam Propagation through Random Media", SPIE Press Book (2005).
- [28] N. Hosseinihahaj and R. Malaney, Continuous variable quantum key distribution with Gaussian and non-Gaussian entangled states over satellite-based channels," *IEEE Globecom*, Washington DC, USA (2016).
- [29] D. Y. Vasylyev, A. A. Semenov, and W. Vogel, "Towards global quantum communication: Beam wandering preserves quantumness," *Phys. Rev. Lett.* 108, 220501 (2012).
- [30] V. C. Usenko, et al., "Entanglement of Gaussian states and the applicability to QKD over fading channels," *New J. Phys.* 14, 093048 (2012).
- [31] K. Lim, C. Suh, and J. K. Rhee, "Longer distance continuous variable quantum key distribution protocol with photon subtraction at receiver," arXiv 1802.07915v1 (2018).
- [32] R. Garcia-Patron and N. J. Cerf, "Unconditional optimality of Gaussian attacks against CV-QKD," *Phys. Rev. Lett.* 97, 190503 (2006).
- [33] Due to an error in our previous simulation code the curves shown here are slightly different from an earlier version of this work. This article updates the published Globecom 2018 version of this work.