# Review Report

Photonic Engineering for CV-QKD over Earth-Satellite Channels

**Authors:** Mingjian He, Robert Malaney, and Jonathan Green
**Reviewer:** Mayar Tharwat

## Contents



## 1 Overview

The main challenge addressed by the study in [1] is investigating which engineered-photonic non-Gaussian state, increases the secret key rate in satellite systems that connects the terrestrial receivers with Low-Earth-Orbit satellites, to enhance QKD performance in these systems for more secure communications. The investigated photonic states are the non-Gaussian photon-added states and photon-subtracted states, derived from two mode squeezed vacuum states. In a previous study done by the same authors, they investigated the performance of a CV-QKD protocol using a single-photon-subtracted state over an Earth-satellite channel, determining whether transmitter or receiver photonic subtraction is preferred [2]. The authors found that substracting photons at the transmitter, outperforms photon subtraction at the receiver. In this study, the authors extended their work to investigate more effects that can produce higher key rates. Four main effects on the key rate are considered in this study: multiple-photon-subtracted states, multiple-photon-added states, optimization of the input TMSV states at the transmitter, and studying some important physical factors that affect the beam to develop a model for the probability density function (PDF) of the transmissivity of the fading channel.

This study is interesting because there is no previous study has taken into account these effects collectively all at once, looking for higher secret key rates over Earth-satellite channels. This study is important because enhancing Earth-satellite QKD is much needed as terrestrial QKD is challenging due to distance limitation of optical-fiber networks, which is around 100 km for a practical QKD protocol. However, Earth-satellite QKD has the potential for much less propagation losses, which could scale quadratically in free-space optical links, in comparison with the exponential propagation loss in optical-fibers links.

*Why did the authors choose to work with Continuous-Variable (CV) over Discrete variable (DV)?* The authors claimed that CV would draw a more realistic route to higher secret key rates because of efficient CV detectors, which I agree with. DV come with the pain of single photon detectors, as we know dark counts phenomenon for example, is quite problematic to implement a practical QKD. However, homodyne detection for example in CV-QKD protocols, is a realistic method that can potentially provides higher secret key rates for a more practical application of QKD.

*Why did the authors choose to work with non-Gaussian states over Gaussian states?* The authors claimed that CV using non-Gaussian states can potentially allow for a higher level of entanglement and it's a pivotal resource for quantum information tasks such as quantum error correction. Studies in the literature agree with the authors statements, a study done in [4] showed that it's impossible to distil Gaussian states with only Gaussian operations, and this is a disadvantage if we want to use CV entanglement using Gaussian states in CV-based QKD protocols, because entanglement distillation is often quite needed to increase the entanglement shared between the two parties, correcting whatever errors occurred in the states due to losses while communicating. Interestingly, many of the channels errors are actually Gaussian in nature, which was showed in this study [5]. Because it's impossible to distilling Gaussian states with Gaussian operations, non-Gaussian operations are then can be used to perform entanglement distillation, enhancing CV-QKD protocols.

# 2 Methods

## 2.1 Channel model

The authors adapted the direct vertical link model for the satellite-earth channel. To model the losses in the optical beam of the channel, three effects were considered: beam-wandering, beam-broadening, and beam-deformation. Refer to figure (1), the beam-wandering is what causing the deviation of center of the beam, and beam-broadening enlarges the profile of the beam, and beam-deformation changes the shape of the profile of the beam overall. In the first picture of this figure, the inner circle is what the beam looks like at the transmitter before any losses, the outer circle represents the aperture of the detector. After the losses are introduces, we get the second picture, where the orange eclipse is what the beam looks like at the receiver.

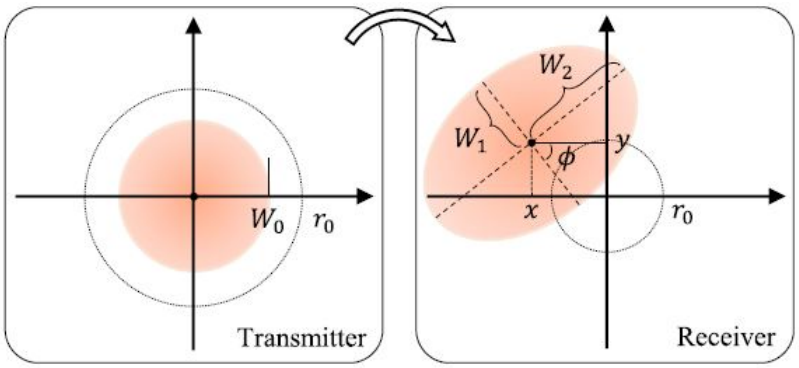



Figure 1: Beam-profile evolution over the Earth-satellite channel. Taken from [1]

The authors used this formula from [3], to model the losses of the beam profile:

$$T_E = T_0 \exp\left\{ - \left[ \frac{\sqrt{x^2 + y^2}/r_0}{R(\frac{2}{W_{\text{eff}}(\phi - \phi_0)})} \right]^{\lambda(2/W_{\text{eff}}(\phi - \phi_0))} \right\}$$

Where $W_{eff}$ is the effective spot-radius, and $T_0$ is the maximal attainable transmissivity achieved when (x, y) = (0, 0). $R(.)$ and $\lambda(.)$ are some scaling and shaping functions.

## 2.2 Generating Non-Gaussian states

This study uses photon addition and subtraction methods on the two-mode squeezed vacuum (TMSV) state for generating non-Gaussian states. First, lets start by describing the TMSV state. TMSV state with a mode A and $B_0$, is created by applying the two-mode squeezing operator $\hat{S}(r) = exp[r(\hat{a}\hat{b} - \hat{a}^\dagger\hat{b}^\dagger)/2]$ to two vacuum states, represented in Fock stats:

$$|TMSV\rangle = \hat{S}(r)\,|0,0\rangle = \sum_{n=0}^{\infty} a_n\,|0,0\rangle_{AB_0} \tag{1}$$

where $r$ is the squeezing factor, and $\{\hat{a}, \hat{b}\}$ are the two modes boson operators.

And,

$$a_n = \sqrt{\frac{\alpha^{2n}}{(1+\alpha^2)^{n+1}}} \tag{2}$$

Where $\alpha^2$ is the mean photon number of the TMSV state.

The Photon-Subtracted State (PSS) can be produced by inserting a mode, $B_0$, of state $|TMSV\rangle$ and an ancillary mode $C_0 = |0\rangle$ into the two inputs of a beam splitter as in figure 2(a). On the other hand, Photon-Added State (PAS) can be generated by inserting the ancillary mode $C_0 = |N\rangle$, figure 2(b).

The two outputs of the beam-splitter are B and C. T-PS scheme results in N subtracted photons PSS state when $C = |N\rangle$, where PAS operation results in $C = |0\rangle$.

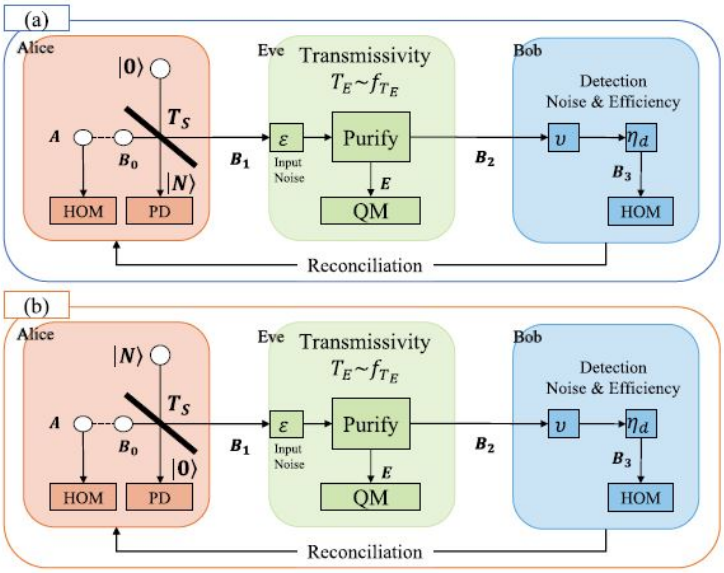



Figure 2: (a) The T-PS scheme. (b) The T-PA scheme. [1]

## 2.3 CV-QKD Protocol

The QKD protocol described in this study is an entanglement-based CV-QKD protocol, with reverse reconciliation. The protocol goes as follows:

1. Alice prepares her TMSV state $\rho_{AB_0}$ in both T-PS and T-PA schemes.
2. Alice produces the state $\rho_{AB_1}$ by applying the non-Gaussian operation (in both T-PS and T-PA schemes) to her state $\rho_{AB_0}$.
3. Alice then sends mode $B_1$ to Bob.
4. Bob finally performs a homodyne detection.

Note that the homodyne detection Bob performs is actually an imperfect homodyne detection with a detection thermal noise $\nu$ and an efficiency $\eta$. This imperfection is modeled by first interacting mode $B_2$ with with variance $\nu$ at a beam splitter with transmissivity $\eta_d$. Then the output mode $B_3$ is then injected into a perfect homodyne detector.

As shown in figure 2, this protocol assumes that Eve can hide herself by mimicking the anticipated noise conditions $\epsilon$ and the channel transmissivity $T_E$.

### 2.4 Key rate calculation

To calculate the key rate, the lower bounded formula for key size in the asymptotic limit is used:

$$K \geq P_N[\eta_r I(A:B_3) - \chi(E:B_3)] \tag{3}$$

In this formula, $P_N$ is the success probability of adding (or subtracting) N photons to (or from) the state, and $\eta_r$ is the reverse reconciliation efficiency.

The first term $I(A:B_3)$ is the mutual information between Alice and Bob:

$$I(A:B_3) = H(A) - H(A|B_3) = \frac{1}{2} log_2 \frac{V_A}{V_{A|B_3}} \tag{4}$$

where $V_A$ is the variance of Alice's mode, and $V_{A|B_3}$ is the conditioned variance of Alice's mode with the homodyne measurement of Bob. Further, the authors were able to calculate the mutual information between Alice and Bob in terms of the channel transmissivity $T_E$, rxpressed as:

$$I(A:B_3) = \frac{1}{2} log_2 \frac{1}{1 - \frac{\eta_d T_E z^2}{\eta_d T_E xy + cx}} \tag{5}$$

where $c = \eta_d[(1 - T_E) + T_E\epsilon] + (1 - \eta_d)\nu$

The second term $\chi(E:B_3)$ in eq (4) is the Holevo bound for Eve's imformation, and this is the quantity by which the key needs to be shortened with to obtain a good secret key.

$$\chi(E:B_3) = S(E) - S(E|B_3) = \sum_{i=1}^{2} g(\lambda_i) - \sum_{i=3}^{5} g(\lambda_j) \tag{6}$$

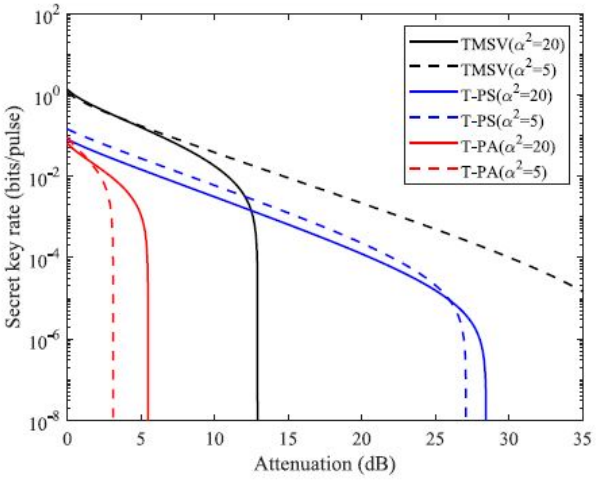
such that, $g(\lambda_i)$ and $g(\lambda_j)$ are some function of $\lambda_i$ and $\lambda_j$ which represents the eigenvalues of the pure state $\rho_{AB_2}$, and the eigenvalues of Alice's state conditioned on Bob's measurement, respectively.

Finally, putting eq (5) and eq (6) in the key rate formule eq (4) , one can calculate the secret key rate for any channel with transmissivity $T_E$.

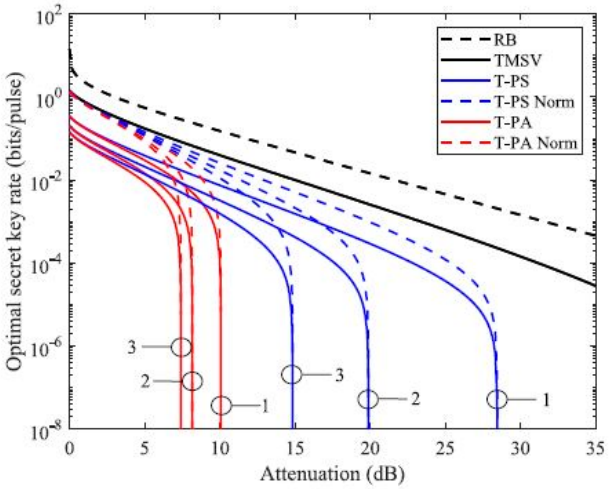
## 3 Results

For the simulation experiments, the authors adopted noise and efficiency parameters from [6] and [7] respectively. The authors considered two different values for mean photon number of the TMSV state ($\alpha^2 = 20$, $\alpha^2 = 5$), corresponding to the entanglement level. Such that, increasing the photon mean number corresponds to a higher entanglement level. Refer to figure (3a), the authors first compared the key rates of the different schemes over channels with fixed-attenuation. We observe from this graph that the state TMSV($\alpha^2 = 5$) does generally better over the whole range of the channel attenuation. For the non-Gaussian states in T-PS and T-PA scenarios, we observe that T-PS ($\alpha^2 = 5$) does slightly better than T-PS ($\alpha^2 = 20$) when the channel attenuation is less than around $26dB$. Also, it's clear that T-PA scenario does far worse compared to the other two.

Then, the authors wanted to optimize the key rate by optimizing $\alpha^2$ and the beamsplitter transmitivity $T_S$ simultaneously. The results obtained for the optimal secret key rate is represented in figure (3b). Where RB is 'Repeaterless Bound' which represents the upper bound for the channel without a repeater, and the blue and the red dashed lines represent the case where a quantum memory device is at the transmitter. Again We observe that the state TMSV has the highest key rate over the whole range of the channel attenuation. Also, we note that T-PA scenario has always worse performance than the scenario of T-PS scheme.




(a) Secret key rate over the fixed-attenuation channel, with beamsplitter transmitivity $T_s = 0.7$ and photon number N=1. [1]




(b) Optimal secret key rate over the fixed-attenuation channel. Note that the numbers '1','2','3' represent the number of the subtracted or added photons (N).

The second main simulation of this study is to investigate fading channels for CV-QKD protocols. The authors adopted parameters from the study in [8] to simulate the atomspheric turbelnce and its effect on the secret key rate.

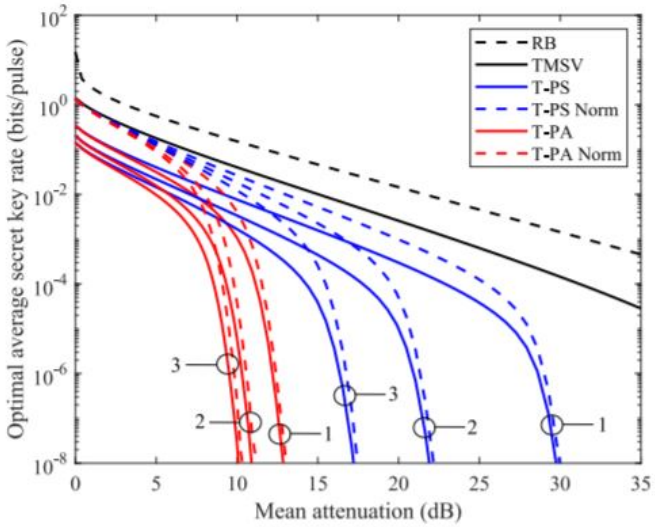



Figure 3: Average key rate optimized for mean channel transmissivity. Note that the numbers '1','2','3' represent the number of the subtracted or added photons (N) [1].

Considering the three channel effects, beam-wandering, beam-broadening, and beam-deformation, discussed in section (2.1), results in figure (3) represents the average key rate optimized for the mean channel transmissivity. Again, we observe that the state TMSV has the highest key rate over the whole range of the channel attenuation, and T-PA scenario has worse performance than the scenario of T-PS scheme.

From these results, the authors shows that PSS state with an initial TMSV state that has an optimized mean photon number $\alpha^2 \approx 10$ and downlink channel attenuation with $5-10dB$, provides a key rate of $10^{-2}$ bits/pulse. However, for an uplink channel with attention $20-30dB$, the optimal mean photon number $\alpha^2 \approx 5-10$, provides an optimized key rate that is around $10^{-4}$ bits/pulse. Further, these values are expected to be higher for actual secret key rate because the lower bound of the key rate formula is used to evaluate the performance, hence, the actual secret key rate might be higher.

# 4 Conclusion

In conclusion, the authors chose Photon-Subtracted State (PSS) as their preferred state, as PSS has the highest average key rate compared to the other non-Gaussian states they considered in their study, and as a result, PSS state would make a good candidate for CV-QKD protocols that are based on using non-Gaussian states for satellite communications. The paper's conclusion is consistent with their results I represented in the previous section.

In general, I like the paper as it is well organized in a clear and logical flow. The authors specifically did a great job in highlighting the important results in each simulation arriving at conclusions that are relevant to the goal of the paper. However, there are some incidents where the authors make claims without giving the intuition why this claim is true or giving references for the readers to justify their claims. For example, in the simulation results section of their paper, the authors considered two different values for mean photon number of the TMSV state, and they claimed that these value correspond to the entanglement level, but the readers were given no intuition for why is this true. Also, in the same section, the authors justified that the T-PA scheme is always worse than the T-PS scheme, by claiming that this is because Eve can obtain more information from the PAS than the PSS, again the readers were given no intuition behind this claim.

# References


[1] He M, Malaney R, Green J. Photonic engineering for CV-QKD over earth-satellite channels. . 2019. https://arxiv.org/abs/1902.09175v3. Accessed Apr 3, 2020. doi: 10.1109/ICC.2019.8762003.

[2] M. He, R. Malaney, and J. Green, "Quantum communications via satellite with photon subtraction," in 2018 IEEE Globecom Workshops, Dec 2018

[3] D. Vasylyev, A. Semenov, and W. Vogel, "Atmospheric quantum channels with weak and strong turbulence," Physical Review Letters, vol. 117, no. 9, 090501, 2016.

[4] 1. Eisert J, Scheel S, Plenio MB. Distilling gaussian states with gaussian operations is impossible. Phys Rev Lett. 2002;89(13):137903.

[5] Holevo, A.S. One-mode quantum Gaussian channels: Structure and quantum capacity. Probl Inf Transm 43, 1–11 (2007). https://doi.org/10.1134/S0032946007010012

[6] P. Huang, G. He, J. Fang, and G. Zeng, "Performance improvement of continuous-variable quantum key distribution via photon subtraction," Physical Review A, vol. 87, no. 1, 012317, 2013.

[7] K. Lim, C. Suh, and J.-K. K. Rhee, "Continuous variable quantum key distribution protocol with photon subtraction at receiver," in Proc. of the International Conference on Quantum Cryptography 2017. Proceedings of the International Conference on Quantum Cryptography, 2017.

[8] D. Vasylyev, A. Semenov, and W. Vogel, "Atmospheric quantum channels with weak and strong turbulence," Physical Review Letters, vol. 117, no. 9, 090501, 2016.