Satellite-to-Ground Discrete Modulated Continuous Variable Quantum Key Distribution: The $M$-PSK and $M$-QAM Protocols in Low Earth Orbit

Mikhael Sayat, Biveen Shajilal, Sebastian P. Kish, Syed M. Assad, Ping Koy Lam, Nicholas Rattenbury, John Cater

Abstract—The Gaussian modulated continuous variable quantum key distribution (GM-CVQKD) protocol is known to maximise the mutual information between two parties during QKD. However, the reconciliation efficiency significantly decreases in low signal-to-noise ratio (SNR) regimes. In contrast, the more resilient discrete modulated CVQKD (DM-CVQKD) protocol has better reconciliation efficiencies in low SNR regimes. In this paper, we study the Phase Shift Keying ($M$-PSK) and Quadrature Amplitude Modulation ($M$-QAM) DM-CVQKD protocols along with the GM-CVQKD protocol over a satellite-to-ground link in the low SNR regime. We use a satellite-to-ground link model which takes into account geometric, scintillation, and scattering losses from the link distance, atmospheric turbulence, and atmospheric aerosols, respectively. In addition, recent multidimensional (MD) and multilevel coding and multistage decoding (MLC-MSD) reconciliation method models in combination with multiedge-type low-density parity-check (MET-LDPC) code models have been used to determine the reconciliation efficiency. The results show that the 4-PSK and 8-PSK protocols outperform GM-CVQKD in both the asymptotic and finite size limit of collective attacks by producing positive key rates at larger link distances and lower elevation angles when the SNR is low. In addition, the $M$-QAM protocol produces larger positive secret key rates compared to $M$-PSK in the asymptotic limit.

Index Terms—quantum key distribution, continuous variable, discrete modulation, Gaussian modulation, satellite communication, quantum communication.

I. INTRODUCTION

QUANTUM key distribution (QKD) [1] is a method of sharing a secret key between two parties, Alice and Bob, where eavesdropping by Eve can be inferred by quantum mechanics. The most significant advancement of QKD in space-based applications was the demonstration of discrete variable QKD (DVQKD), which uses the available degrees of freedom of single photons to encode a key between optical ground stations on Earth and the Micius satellite [2]. Despite its successful deployment in space, its use of expensive and inefficient single photon detectors for detection poses challenges for its popularisation and commercialisation [3]. An appealing alternative is continuous variable QKD (CVQKD) which uses multi-photon technologies to encode the key in the continuous X and P quadratures of light [3, 4]. Its use of homodyne or heterodyne detection is more cost-effective, more compatible with standard telecommunication optical networks, and more efficient, offering higher secret key rates. CVQKD experiments have predominantly been restricted to fibre-based systems in the laboratory where a secret key rate of 14.2 Mbit/s over 15 km optical fibre has been demonstrated using a local local oscillator [5]. The first demonstration of fibre-based CVQKD over 100 km was performed by controlling and suppressing excess noise [6]. A secret key rate of 2.1 Gbit/s has been achieved using 10-channel wavelength division multiplexing in the weak turbulence regime [7], and a secret key rate greater than 1.68 Gbit/s can be reached in a lossless and excess noise free system that uses two polarisations, six wavelengths, and four orbital angular momentum for multiplexing [8]. A study of atmospheric effects on quantum communications over 1.6 km of free-space was performed and the experimental setup is capable of CVQKD [9]. However, there has only been one demonstration of free-space CVQKD which occurred over 460 m in an urban environment and achieved a secret key rate of 0.152 kbit/s using polarised coherent states with unidimensional Gaussian modulation [10].

The two modulation approaches for CVQKD to encode a key are Gaussian modulation (GM-CVQKD) [3] and discrete modulation (DM-CVQKD) [11] where implementations can be found in [12] and [13], respectively. The GM-CVQKD protocol achieves greater mutual information between Alice and Bob than the DM-CVQKD protocol, leading to higher achievable secret key rates in high signal-to-noise-ratio (SNR) regimes [14]. However, in low SNR regimes, GM-CVQKD has lower reconciliation efficiencies between Alice and Bob, making it nonoperational in low SNR regimes; restricting its large secret key rates to small distances [11, 15]. Post-selection methods, in which classical and quantum post-processing methods increase the SNR, have been employed to combat this problem [16, 17, 18].

DM-CVQKD, on the other hand, although exhibiting lower correlations between Alice and Bob (which leads to lower secret key rates compared to GM-CVQKD at higher SNR regimes [19]), is capable of higher reconciliation efficiencies at lower SNR regimes [15]. This is because noise does not affect its modulation as much as in GM-CVQKD since it relies on the sign of the quadrature, allowing for the use of error-correcting codes at low SNR regimes leading to higher reconciliation efficiencies. DM-CVQKD is therefore a favourable protocol in satellite-to-ground CVQKD where low SNR is prevalent due to the large link distance and accumulated losses and excess noise.

In this work, the feasibility of low Earth orbit (LEO) satellite-to-ground DM-CVQKD (orbit altitudes of 160-1000 km) is investigated. The $M$-PSK protocol that assume
Gaussian optimality under collective attacks [11, 19, 20, 21, 22] and the M-QAM protocol which does not assume Gaussian optimality under collective attacks are studied for LEO satellite-to-ground CVQKD. The rest of the paper is structured as follows. Section II introduces the M-PSK protocol. Section III introduces the M-QAM protocol. Section IV introduces the LEO satellite to optical ground station link model. Section V discusses the achievable secret key rates of the M-PSK and M-QAM DM-CVQKD protocols and discusses the resulting trends in SKR from parameter variation. Section VI concludes the work presented in the paper.

II. THE M-PSK DM-CVQKD PROTOCOL

In this section, we study the M-PSK DM-CVQKD protocol for $M = 2, 4, 8$ with security under collective attacks and assuming Gaussian optimality.

A. Optical Phase Space Representation

In the 2-PSK protocol, Alice sends one of two coherent states with equal probability (0.5). In the 4-PSK protocol, Alice sends one of four coherent states with equal probability (0.25). In the 8-PSK protocol, Alice sends one of eight coherent states with equal probability (0.125). This is summarised below [23]:

- $\mathcal{S}_2 = \{ |\alpha\rangle, |\alpha e^{i\pi}\rangle \}$
- $\mathcal{S}_4 = \{ |\alpha\rangle, |\alpha e^{i\pi/2}\rangle, |\alpha e^{i3\pi/4}\rangle \}$
- $\mathcal{S}_8 = \{ |\alpha\rangle, |\alpha e^{i\pi/4}\rangle, |\alpha e^{i3\pi/4}\rangle, |\alpha e^{i\pi/2}\rangle \}$

The M-PSK ($M = 2, 4, 8$) protocols use coherent states with a magnitude $\alpha$ and are represented in the optical phase space as shown in Figure 1.

![Fig. 1: Constellation diagrams of the 2,4,8-PSK protocols](image)

(a) 2-PSK  (b) 4-PSK  (c) 8-PSK

The DM-CVQKD covariance matrix which describes the discretely modulated coherent state sent from Alice to Bob with security under collective attacks, has the same form as the Gaussian modulation scheme [19],

$$
\gamma_{AB} = \begin{bmatrix} (V_A + 1)I & \sqrt{TZ\sigma_z} \\ \sqrt{TZ\sigma_z} & T(V_A + 1 + \chi_{\text{line}})I \end{bmatrix}
$$

where $V_A$ is the modulation variance of Alice, $T$ is the overall transmittance between Alice and Bob, and $\chi_{\text{line}}$ is the noise in the channel line expressed in shot noise units. $I$ and $\sigma_z$ are the identity matrix, $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, and the Pauli matrix, $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, respectively. The correlation coefficient, $Z_n$, varies between each M-PSK protocol:

- $Z_2 = \alpha^2(\sinh^2(\zeta_0) + \sinh^2(\zeta_1) + \sinh^2(\zeta_2) + \sinh^2(\zeta_3) + \sinh^2(\zeta_4))$
- $Z_4 = 2\alpha^2 \sum_{k=0}^{3}(\sinh^2(\zeta_k) - \sinh^2(\zeta_{1-k}))$
- $Z_8 = 2\alpha^2 \sum_{k=0}^{7}(\sinh^2(\zeta_k) - \sinh^2(\zeta_{8-k}))$

The parameter $\zeta_k$ varies for each M-PSK protocol: 2-PSK protocol:

- $\zeta_0 = \frac{1}{2}e^{-\alpha^2}\cosh(\alpha^2)$
- $\zeta_1 = \frac{1}{2}e^{-\alpha^2}\sinh(\alpha^2)$

4-PSK protocol:

- $\zeta_{0,2} = \frac{1}{2}e^{-\alpha^2}(\cosh(\alpha^2) \pm \sinh(\alpha^2))$
- $\zeta_{1,3} = \frac{1}{2}e^{-\alpha^2}(\sinh(\alpha^2) \pm \sinh(\alpha^2))$

8-PSK protocol:

- $\zeta_{0,4} = \frac{1}{2}e^{-\alpha^2}(\cosh(\alpha^2) \pm 2\cos(\alpha^2) \cosh(\alpha^2/\sqrt{2}) \cosh(\alpha^2/\sqrt{2}))$
- $\zeta_{1,5} = \frac{1}{2}e^{-\alpha^2}(\sinh(\alpha^2) \pm 2\sin(\alpha^2) \sinh(\alpha^2 \sqrt{2}) \pm \sqrt{2}\sin(\alpha^2) \sinh(\alpha^2 \sqrt{2}) \cosh(\alpha^2 \sqrt{2}))$
- $\zeta_{2,6} = \frac{1}{2}e^{-\alpha^2}(\cosh(\alpha^2) - \sin(\alpha^2) \pm 2\sin(\alpha^2) \sinh(\alpha^2 \sqrt{2}))$
- $\zeta_{3,7} = \frac{1}{2}e^{-\alpha^2}(\sinh(\alpha^2) - \sin(\alpha^2) \pm \sqrt{2}\cos(\alpha^2) \cosh(\alpha^2 \sqrt{2}) \cosh(\alpha^2 \sqrt{2}))$

where $\alpha = \sqrt{\frac{V_A}{Z_n}}$. In the case of Gaussian modulation, the correlation coefficient would be $Z_G = \sqrt{V_A^2 + 2V_A}$.

B. Secret Key Rate Calculation

The asymptotic limit secret key rate (SKR) [bits/pulse] is calculated as

$$
SKR_{\text{asy}} = \beta I_{AB} - S_{BE},
$$

where $\beta$ is the reconciliation efficiency, $I_{AB}$ is the mutual information between Alice and Bob, and $S_{BE}$ is the Holevo information which upper bounds the Holevo information that represents the maximum mutual information between Eve and Bob in the protocol [11]. The mutual information for homodyne and heterodyne detection is calculated as

$$
I_{AB,\text{hom}} = \frac{1}{2} \log_2 \left( \frac{(V_A + 1) + \chi_{\text{tot}}}{1 + \chi_{\text{tot}}} \right),
$$

$$
I_{AB,\text{het}} = \log_2 \left( \frac{(V_A + 1) + \chi_{\text{tot}}}{1 + \chi_{\text{tot}}} \right),
$$

where the total excess noise, $\chi_{\text{tot}}$, combines both the channel noise, $\chi_{\text{line}} = \frac{1}{T} - 1 + e_{\text{ch}}$ (where $e_{\text{ch}}$ is the channel excess noise), and detection excess noise, $\chi_{\text{hom/het}}$, and is expressed as $\chi_{\text{tot}} = \chi_{\text{line}} + \chi_{\text{hom/het}}$ [19]. In this case, the detection noise varies between homodyne and heterodyne detection where $\chi_{\text{hom}} = \frac{(1-\eta) + e_{\text{det}}}{\eta}$ and $\chi_{\text{het}} = \frac{1 + (1-\eta) + 2e_{\text{det}}}{\eta}$, respectively. Here, $\eta$ is the detector efficiency and $e_{\text{det}}$ is the detector excess noise (Table I). The Holevo information is calculated as

$$
S_{BE} = G \left( \frac{\lambda _1 - 1}{2} \right) + G \left( \frac{\lambda _2 - 1}{2} \right) - G \left( \frac{\lambda _1 - 1}{2} \right),
$$

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

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

where

$$A = (V_A + 1)^2 + T^2(V_A + 1 + \chi_{\text{line}})^2 - 2TZ^2,$$

$$B = (T(V_A + 1)^2 + T(V_A + 1)\chi_{\text{line}} - T^2Z^2).$$

$\lambda_{3,4}$ is calculated as

$$\lambda_{3,4} = \sqrt{\frac{1}{2}(C \pm \sqrt{C^2 - 4D})},$$

where

$$C_{\text{hom}} = A_{\chi_{\text{hom}}} + (V_A + 1)\sqrt{B} + T(V_A + 1 + \chi_{\text{line}}),$$

$$D_{\text{hom}} = \sqrt{B} \frac{V_A + 1 + \sqrt{B}_{\chi_{\text{hom}}}}{T(V_A + 1 + \chi_{\text{tot}})},$$

for homodyne detection, and

$$C_{\text{het}} = \frac{A_{\chi_{\text{het}}}^2 + B + 1 + 2TZ^2}{T(V_A + 1 + \chi_{\text{tot}})^2},$$

$$D_{\text{het}} = \frac{(V_A + 1 + \sqrt{B}_{\chi_{\text{het}}})^2}{T(V_A + 1 + \chi_{\text{tot}})}$$

for heterodyne detection.

The SKR calculation (Equation 2-9) is for the idealistic asymptotic limit in which an infinite number of symbols are sent between Alice and Bob, and provides an upper bound to the achievable SKRs. The finite size limit secret key rate, which represents a realistic case in which a finite number of symbols are sent between Alice and Bob [23], is calculated as

$$\text{SKR}_{\text{fin}} = f(1 - \text{FER})(1 - v)[\beta I_{AB} - S_{BE} - \delta n_{\text{privacy}}],$$

(10)

where $f$ is the laser repetition rate, FER is the frame error rate, $v$ is the fraction of the number of symbols excluded for channel parameter estimation, and $\delta n_{\text{privacy}}$ represents the proportion of the key further attributed to information gained by the eavesdropper to reflect the validity of estimated channel parameters in determining the Holevo information. $\delta n_{\text{privacy}}$ is calculated as

$$\delta n_{\text{privacy}} = \frac{(d + 1)^2}{N} + \frac{4(d + 1)}{N} \sqrt{\log_2\left(\frac{2}{\epsilon_s}\right)}$$

$$+ \frac{2 \log_2\left(\frac{2}{\epsilon_s}\right)}{N} \frac{4\epsilon_s d}{\epsilon_s \sqrt{N}} +$$

$$+ \frac{2 \log_2\left(\frac{2}{\epsilon_s}\right)}{N} \frac{4\epsilon_s d}{\epsilon_s \sqrt{N}},$$

(11)

where $d$ is a discretisation parameter, $\epsilon_s$ is a smoothing parameter, $\epsilon$ is a security parameter representing the probability that the key is not secret, and $n$ is the difference between the total symbols sent ($N$) between Alice and Bob and the amount used for channel parameter estimation, the details of which can be found in [16] and [24].

### TABLE I: Excess Noise in Daylight [24]. The values are normalised to shot noise and have the unit Shot Noise Units (SNU).

| Source Value (SNU) | Value (SNU) |
|--------------------|-------------|
| Time-of-arrival fluctuations | 0.0060 |
| Atmospheric relative intensity noise in local oscillator | 0.0100 |
| Excess relative intensity noise in local oscillator | 0.0018 |
| Noise, modulation noise | 0.0005 |
| $\chi_{\text{tot}}$, background noise | 0.0002 |
| Relative intensity noise in signal | 0.0001 |
| Detector overlap | 0.0001 |
| Local oscillator subtraction noise | 0.0001 |
| Local oscillator to signal leakage | 0.0001 |

### C. Reconciliation Efficiency

The reconciliation efficiency, $\beta$, is defined as the efficiency of reconciliation methods in reconciling the secret key between Alice and Bob. The primary argument favouring DM-CVQKD over GM-CVQKD is that its operations have significantly greater reconciliation efficiencies in lower SNR regimes [11]. This is crucial in satellite-to-ground QKD where the signal suffers from attenuation and excess noise. These detrimental effects are injected in and between Alice (satellite) and Bob (receiver), from the hardware used, link distance, and atmosphere.

Reconciliation methods can be split into Multidimensional (MD) reconciliation and Multilevel Coding and Multistage Decoding (MLC-MSD) reconciliation [23]. MLC-MSD reconciliation is employed for CVQKD with Gaussian modulations and operate at SNRs greater than 0 dB, while MD reconciliation is employed for CVQKD with discrete modulations and operate at SNRs less than 0 dB. Low-density parity-check (LDPC) codes can be used with MD and MLC-MSD reconciliation [23]. Multilevel-type LDPC (MET-LDPC) codes are regarded to be suitable for both MD and MLC-MSD reconciliation.

Consistent with the claim that reconciliation efficiencies for DM-CVQKD are higher in lower SNR regimes [11], the most recent practical MD reconciliation efficiencies and FER asymptotically approach 100% as the SNR decreases [23]. The models and experimental results of the dependency of $\beta$ and FER on the SNR in (Equation 12) [23] have been used to calculate and analyse the satellite-to-ground DM-CVQKD and GM-CVQKD SKRs in the asymptotic and finite size limit. These experimental results use a code block length of $N = 10^6$. The coefficients, $c_i$, for $\beta$ are displayed in Table II. The calculation of the FER uses the coefficients $m_1 = 0.8218$, $m_2 = -19.46$, and $m_3 = -298.1$ as in Equation 12.

$$\beta_{\text{MLC-MSD/MD}} = c_1^{\text{SNR}} - c_3^{\text{SNR}},$$

$$\text{FER} = \frac{1}{2}(1 + m_1 \arctan(m_2 \text{SNR} + m_3)).$$

(12)

The SNR is calculated as

$$\text{SNR} = 10 \log_{10} \left(\frac{T^2}{|\alpha|^2 + (1 - T)\chi_{\text{tot}}}\right),$$

(13)

and depends on $\alpha$, transmittance ($T$) and excess noise ($\chi_{\text{tot}}$) between Alice and Bob. Note that $\beta_{\text{MLC-MSD}}, \beta_{\text{MD}}$, and FER...
as in Equation 12 are only valid when they have a value between 0 and 1.

**TABLE II: Coefficients of β**

| Coefficient | MLC-MSD | MD       |
|--------------|---------|----------|
| $c_1$        | 0.9655  | -0.0825  |
| $c_2$        | 0.0001507 | 0.1834  |
| $c_3$        | -0.04696 | 0.9821  |
| $c_4$        | -0.2238 | -0.00002815 |

### III. The M-QAM DM-CVQKD Protocol

The previous $M$-PSK protocol is only secure from an eavesdropper performing collective attacks. In [25], a security proof for the $M$-PSK and $M$-QAM DM-CVQKD protocols without Gaussian optimality under collective attacks from an eavesdropper in the asymptotic limit was developed. Unfortunately, using the security proof and given the the transmittances and excess noise in a typical satellite-to-ground link (Table I), $M$-PSK is not capable of producing a positive SKR. A more attractive protocol is $M$-QAM as it produces positive SKRs in lower transmittances and higher levels of excess noise.

#### A. Optical Phase Space Representation

In $M$-QAM, $M$ coherent states are modulated to be distributed equidistantly with each other on the optical phase space. By assigning a non-uniform probability on each coherent state, $M$-QAM can be tailored to a discretised Gaussian distribution to further increase the mutual information between Alice and Bob.

The modulated coherent state is described as

$$
\alpha_{k,l} = \frac{\alpha \sqrt{2}}{\sqrt{m-1}} \left( k - \frac{m-1}{2} \right) + i \frac{\alpha \sqrt{2}}{\sqrt{m-1}} \left( l - \frac{m-1}{2} \right),
$$

where $M = m^2$ and the coherent states are equidistantly spaced between $-\sqrt{m-1}$ and $\sqrt{m-1}$ in the phase and amplitude quadratures. Here, $k = l = 0, 1, ..., (m-1)$. The probability of each coherent state, $p_{k,l}$, can follow either a binomial distribution,

$$
p_{k,l} = \frac{1}{2^{2(m-1)}} \binom{m-1}{k} \binom{m-1}{l},
$$

or a discrete Gaussian distribution,

$$
p_{k,l} \sim \exp\left(-\nu \left(x^2 + p^2\right)\right),
$$

where $x = \frac{\alpha \sqrt{2}}{\sqrt{m-1}} \left(k - \frac{m-1}{2}\right)$ and $p = \frac{\alpha \sqrt{2}}{\sqrt{m-1}} \left(l - \frac{m-1}{2}\right)$. Here, $\nu$ is a free parameter which is optimised to maximise the SKR. For example, Figure 2 shows a 16-QAM, 64-QAM, and 256-QAM on the optical phase space with the probability of each modulated coherent state based on the binomial distribution. It can be seen that a greater amount of coherent states used approximates the Gaussian distribution better as in Figure 2.

#### B. Secret Key Rate Calculation

The asymptotic limit SKR is calculated as in Equation 2. However, the mutual information is calculated as

$$
I_{AB,\text{hom}} = \frac{1}{2} \log_2 \left(1 + \frac{TV_A}{2 + T\epsilon}\right),
$$

$$
I_{AB,\text{het}} = \log_2 \left(1 + \frac{TV_A}{2 + T\epsilon}\right).
$$

The Holevo information is determined from the covariance...
matrix given by,
\[ \Gamma_{AB} = \begin{bmatrix} (V_A + 1) & Z^* \sigma_z \\ Z^* \sigma_z & (1 + T V_A + T \epsilon) I \end{bmatrix}. \] (18)

The Holevo information is therefore,
\[ S_{BE} = G \left( \frac{\lambda_1 - 1}{2} \right) + G \left( \frac{\lambda_2 - 1}{2} \right) - G \left( \frac{\lambda_3 - 1}{2} \right), \] (19)
where \( \lambda_1 \) and \( \lambda_2 \) are the symplectic eigenvalues of the covariance matrix, \( \Gamma_{AB} \). The symplectic eigenvalue, \( \lambda_3 \), is calculated as
\[ \lambda_{3,\text{het}} = V_A + 1 - \frac{Z^* 2}{2 + T V_A + T \epsilon}, \] (20)
for homodyne and heterodyne detection, respectively. For an arbitrary modulation, the lower bound of the correlation coefficient, \( Z^* \), can be calculated as
\[ Z^* (T, \epsilon) = 2 \sqrt{T} \text{Tr} \left( \tau^2 \hat{a} \tau^2 \hat{a}^\dagger \right) - \sqrt{2T \epsilon w}, \] (21)
where \( \hat{a} \) and \( \hat{a}^\dagger \) are the annihilation and creation operators, respectively, \( \epsilon \) is the total excess noise, and \( \tau \) is the density matrix of the modulation,
\[ \tau = \sum_k p_k |\alpha_k\rangle \langle \alpha_k|, \] (22)

where \( w \) is defined as
\[ w = \sum_k p_k \left( |\langle \alpha_k| \hat{a}_\tau |\alpha_k\rangle|^2 - |\langle \alpha_k| \hat{a}_\tau |\alpha_k\rangle|^2 \right). \] (23)

Although \( M \)-QAM is still a DM-CVQKD protocol, its assignment of a probability following a Gaussian distribution to each modulated coherent state raises the question of whether or not it is still capable of high reconciliation efficiencies in low SNR regimes. Lower order \( M \)-QAM is definitely more capable of higher reconciliation efficiencies compared to higher order \( M \)-QAM. However, since \( M \)-QAM approximates a Gaussian distribution, it can be argued that it is not capable of having high reconciliation efficiencies. In addition, the calculation of SKRs in the finite size limit for \( M \)-QAM is still an open question. As a result, only the SKRs in the asymptotic limit will be studied in a satellite-to-ground context.

### IV. Satellite-to-Ground Channel Model

Clouds, atmospheric turbulence, and atmospheric aerosols are the three sources of signal degradation in the atmosphere that cause the transmittance of the signal to decrease through attenuation. The model developed considers the following: geometric losses due to the distance between Alice (satellite) and Bob (optical ground station (OGS)) and hardware used, scintillation losses due to the atmospheric turbulence, scattering losses due to atmospheric aerosols. Clouds are not included in the model as they effectively destroy the signal and act as a blockade, completely attenuating the signal. The solution to this is accurate cloud coverage analyses and OGS network site diversity [26] to spatiotemporally maximise channel links between Alice and Bob regardless of environmental condition. In addition, weather conditions such as rain, snow, and hail effectively destroy the signal and can cause damage to the OGS telescope [27]. Therefore, in the presence of clouds, rain, snow, and hail, satellite-to-ground CVQKD is not ideal.

Atmospheric losses depend on the thickness of the atmosphere or the atmospheric mass the signal propagates through. On average, 95% of the total atmospheric mass is within the first 20 km from ground to zenith [28], [29] and so atmospheric losses can approximately be confined to this range.

Figure 3 displays the channel link between the satellite and OGS where the total link distance and effective atmospheric thickness is a function of the elevation angle. The model assumes a uniform atmospheric thickness of 20 km. The total link distance, \( L_{\text{tot}} \), and effective atmospheric thickness, \( L_{\text{atm,eff}} \), can be calculated as

\[ L_{\text{tot}} = (R_E + L_{\text{zen}})^2 + (R_E + L_{\text{OGS}})^2 - 2(R_E + L_{\text{zen}})(R_E + L_{\text{OGS}}) \cos (\alpha_1)^2 \]
\[ \alpha_1 = \arcsin \left( \frac{\cos (\theta) (R_E + L_{\text{OGS}})}{R_E + L_{\text{zen}}} \right) + (90 - \theta), \]
\[ L_{\text{atm,eff}} = (R_E + L_{\text{atm}})^2 + (R_E + L_{\text{OGS}})^2 - 2(R_E + L_{\text{atm}})(R_E + L_{\text{OGS}}) \cos (\alpha_2)^2 \]
\[ \alpha_2 = \arcsin \left( \frac{\cos (\theta) (R_E + L_{\text{OGS}})}{R_E + L_{\text{atm}}} \right) + (90 - \theta) \]
where \( R_E \) is the radius of Earth, \( L_{\text{OGS}} \) is the altitude of the OGS, \( L_{\text{zen}} \) is the altitude of the satellite at zenith (90° elevation angle), \( L_{\text{atm}} \) is the atmospheric thickness containing 95% of atmospheric mass, and \( \theta > 0 \) is the elevation angle.

#### A. Geometric Losses

Geometric losses arise from the link distance and optical hardware used in the transmission and reception of the signal, and can be estimated from [30].

\[ A_{\text{geo}} = 10 \log_{10} \left( \frac{L_{\text{tot}}^2 \lambda^2}{D_t^2 D_r^2 T_i (1 - L_{\text{dp}}) T_r} \right) \text{[dB]} \] (25)

which depends on the total link distance (\( L_{\text{tot}} \)), wavelength \( \lambda \), transmitter and receiver aperture diameter \( (D_t, D_r) \), transmitter and receiver efficiencies \( (T_i, T_r) \), and pointing loss \( (L_{\text{dp}}) \) which is attributed to the inefficiency of the acquisition, pointing, tracking (APT) system of the OGS as well as beam wandering. The equation assumes that the receiver is in the far field of the transmitter \( (L_{\text{tot}} \geq \frac{D_r D_t}{\lambda}) \), the transmitter is diffraction limited, and there is no attenuation from the atmosphere which enables the later addition of atmospheric losses (scattering and scintillation losses) in the overall model.

#### B. Scattering Losses

Atmospheric aerosols attenuate the signal through three regimes of scattering [31]: Rayleigh scattering caused by air molecules, Mie scattering caused by haze and fog, and geometrical scattering caused by rain, snow etc. For the wavelength used in DM-CVQKD, 1550 nm, the effects of Rayleigh...
C. Scintillation Losses

Atmospheric turbulence causes refractive index variations in the atmosphere and distorts the optical wavefront of the laser, leading to intensity fluctuations and losses in the received signal seen as speckles on an imaging detector [25]. This is a phenomenon known as scintillation and can be measured by the scintillation index, \( \sigma_v^2 \). As the receiver involves a telescope, it is assumed to have an aperture diameter larger than the irradiance correlation width (lateral intensity coherence length) of the speckles. Therefore, aperture averaging is utilised, decreasing the adverse effects of scintillation [33].

The losses related to scintillation with aperture averaging is described in Equation [27] which depends on the scintillation index, \( \sigma_v^2 \), and the probability, \( p_{thr} \), that the received power is below the minimum required power to register a signal, \( p_{thr} \) is equivalent to the fraction of link outage time. Here, it is assumed that the received signal is a spherical wave. The resulting loss as a function of the scintillation index is given by [33].

\[
A_{sci} = 4.343 \left( \text{erf}^{-1}(2p_{thr}) - 1 \right) \left[ 2 \ln(\sigma_v^2 + 1) \right]^{1/2} - \frac{1}{2} \ln(\sigma_v^2 + 1) \text{[dB]}.
\]

The scintillation index can be calculated using Equation 28 which depends on the Rytov variance (\( \sigma_R^2 \)), the effective atmosphere thickness (\( L_{atm,eff} \)), and the refractive index structure parameter (\( C_n^2 \)). Here, \( k = \frac{2\pi}{\lambda} \) is the wave number, \( d = D_r \left( \frac{\pi}{2L_{atm,eff}} \right)^{1/2} \), \( D_r \) is the aperture diameter of the receiver, and \( \lambda \) is the wavelength.

\[
\sigma_v^2(D_r) = \exp \left\{ \frac{0.20\sigma_R^2}{1 + 0.18d^2 + 0.20(\sigma_R^2)^{1/2} + 0.21\sigma_R^2 \left[ 1 + 0.24(\sigma_R^2)^{1/2} \right]^{1/2} + 1 + 0.90d^2 + 0.21d^2(\sigma_R^2)^{1/2}} \right\} - 1,
\]

\[
\sigma_R^2 = 2.25k^2 \int_0^{L_{atm,eff}} C_n^2(z)(L_{atm,eff} - z)^{1/2} \text{d}z.
\]

The refractive index structure parameter, \( C_n^2 [m^{-2}] \), defines the intensity of turbulence in the atmosphere. Although this can be calculated more accurately through models such as the Hufnagel-Valley models [34], \( C_n^2 \) is set as a constant parameter [27] where \( C_n^2 = 10^{-16} \) corresponds to low turbulence levels, \( C_n^2 = 10^{-14} \) medium turbulence levels, and \( C_n^2 = 10^{-13} \) high turbulence levels.

V. SATELLITE-TO-GROUND DM-CVQKD SKR ANALYSIS

In this section, the SKR of satellite-to-ground DM-CVQKD is analysed with M-PSK and M-QAM modulation in combination with typical daylight excess noise values (Table 1) and the losses applied on the total link distance and effective atmosphere thickness. The overall total attenuation based on losses is defined as

\[
A_{tot} = A_{geo}(L_{tot}) + A_{scat}L_{atm,eff} + A_{sci}(L_{atm,eff}) \text{[dB]}.
\]
and the transmittance is calculated as the non-logarithmic inverse of it. Of the three sources of attenuation, geometric loss is the most dominant due to the large distance between the satellite and OGS. In calculating geometric losses, the assumption that the receiver is in the far field of the transmitter is governed by $L \geq \frac{D_r \lambda}{4}$. In situations where this inequality does not hold, the SKR calculated has been omitted. However, the general trend should still apply. The reconciliation efficiency was also used in calculating the performance of DM-CVQKD and was compared to GM-CVQKD performance in long-distance low-SNR satellite-to-ground links using the appropriate reconciliation method (MD for DM-CVQKD, MLC-MSD for GM-CVQKD) for the calculation of the SKR.

Several parameters were varied for the analysis of the $M$-PSK and $M$-QAM DM-CVQKD protocols under different satellite orbits (Table III). The two values for the visibility and the refractive index structure parameter correspond to good atmospheric conditions where the visibility is high and there is low atmospheric turbulence ($V = 200$ km, $C_n^2 = 10^{-16}$) and bad atmospheric conditions where visibility is low and there is high atmospheric turbulence ($V = 20$ km, $C_n^2 = 10^{-13}$). Two values of the receiver aperture diameter were also used to observe the changes in achievable SKR. The modulation variance for discrete and Gaussian modulation were chosen to be close to optimal ($V_A = 0.5$ SNU for $M$-PSK, $V_A = 2$ SNU for $M$-QAM, $V_A = 5$ SNU for Gaussian modulation). The SKRs for DM-CVQKD and GM-CVQKD were calculated as a function of the satellite altitude at zenith at different elevation angles (30°, 60°, 90°) in reference to the satellite altitude at zenith.

**TABLE III: CVQKD Link Parameters**

| Parameter                          | Value (Unit)          |
|------------------------------------|-----------------------|
| Detection                          | Homodyne (M-PSK)      |
| Modulation Variance ($V_A$)        | 0.5 SNU (M-PSK)       |
|                                   | 2 SNU (M-QAM)         |
|                                   | 5 SNU (Gaussian)      |
| Laser repetition rate (f)          | 50 MHz                |
| Channel Parameter Estimation Fraction (u) | 0.1               |
| Discretisation parameter (d)       | 5                    |
| Smoothing parameter ($\epsilon_s$)  | $2 \times 10^{-56}$  |
| Security parameter (e)             | $1 \times 10^{-55}$  |
| Wavelength ($\lambda$)             | 1550 nm               |
| Transmitter Aperture Diameter ($D_t$) | 0.3 m                |
| Receiver Aperture Diameter ($D_r$)  | 1.2 m                |
| Transmitter, Receiver Optics Efficiency ($T_1$, $T_r$) | 0.9, 0.9 |
| Pointing Loss Efficiency / APT Efficiency ($L_{pt}$) | 0.1            |
| OGS Elevation ($L_{OGS}$)          | 0 km                  |
|                                    | 1.029 km (Mt. John)   |
| Atmosphere Thickness (95% mass)    | 20 km                 |
|                                    | 20 km (Bad)           |
|                                    | 200 km (Good)         |
| Refractive Index Structure Parameter ($C_n^2$) | $10^{-13}$ m$^{-2}$ (Bad) |
|                                    | $10^{-16}$ m$^{-2}$ (Good) |
| Probability Threshold ($p_{thr}$)   | 10$^{-6}$             |
| Code block length                  | $10^6$                |

/ Total number of symbols sent ($N$)

**A. M-PSK Satellite-to-Ground SKRs**

This section shows the calculated SKRs for satellite-to-ground $M$-PSK under collective attacks from Eve. Since it only includes a small number of coherent states (2, 4, 8-PSK), homodyne detection has been used for the analyses in defence of simplification for real-life implementation.

The results in Figure 4 show that for a receiver aperture diameter of 1 m and good atmospheric conditions, DM-CVQKD significantly outperforms GM-CVQKD by having the ability to produce positive SKRs at larger distances both in the asymptotic and finite size limit. However, these are only for the 4-PSK protocol and 8-PSK protocol, with the 8-PSK protocol achieving greater distances than the 4-PSK protocol. The 2-PSK protocol does not produce a positive SKR and is therefore unsuitable for LEO satellite-to-ground downlinks. As expected, a smaller elevation angle produces a smaller SKR as the signal travels through a larger link distance and effective atmosphere thickness where it suffers from greater attenuation. In bad atmospheric conditions, the link distance in which positive SKRs in the asymptotic limit are achievable is significantly decreased (Figure 3). In the finite size limit, during bad atmospheric conditions, no positive SKR is achieved. This is evidence of the inability of CVQKD to operate under bad atmospheric conditions which leads to significant signal attenuation.

In Figure 4, we can see that in the finite size limit, with $N = 10^6$, the link distance for which a positive SKR is achievable significantly decreases to a maximum satellite orbit altitude of approximately 250 km. At this altitude, active propulsion is required adding to the required complexities of a CVQKD LEO satellite. However, this can be ameliorated by increasing the receiver aperture diameter. Increasing the receiver aperture diameter from 1 m to 2 m increases the maximum satellite altitude which can produce positive SKRs from 250 km to 650 km (Figure 6). Note that the steep cutoff in the calculated finite size limit SKRs are due to the FER equaling zero, leading to a SKR value of zero.

The finite size limit SKR calculation can also be presented as a function of elevation angle for a satellite at a certain orbit altitude. For this purpose, we assessed the orbit of the International Space Station (ISS), which has an average orbit altitude at zenith of 417.5 km, and studied two passes, shown in Figure 7 which occurred on 9th August 2022, over the University of Canterbury’s Mt. John Observatory in New Zealand (Latitude = -43.9853°, Longitude = 170.4641°, Altitude = 1.029 km). The first pass had a duration of 663 s with a maximum elevation angle of 87.6°. The second pass had a duration of 662 s with a maximum elevation angle of 57.2°. Note that the calculation had the same link parameter values as in Table III with a receiver diameter aperture, $D_r$, of 2 m and OGS altitude, $L_{OGS}$, of 1.029 km. The SKR was calculated using our model and assuming good atmospheric conditions for both passes. The results show that DM-CVQKD can produce positive SKRs from a minimum elevation angle of 52° while GM-CVQKD can produce positive SKR from 59°. This means that in the second pass, GM-CVQKD is unsuitable. The SKR profiles for the first and second pass are shown in Figure 8 and Figure 9 respectively.

Multiplying the calculated SKR and the time the ISS is at a certain elevation angle gives the total number of bits of the secret key. The elevation angle has been discretised with a
resolution of 1° in Figure 7 to determine the temporal position of the ISS. For the first pass, the secret key has:

- 345 Mbit for the GM-CVQKD protocol,
- 126 Mbit for the 8-PSK DM-CVQKD protocol,
- 105 Mbit for the 4-PSK DM-CVQKD protocol.

For the second pass, the secret key has:
- 0 bits for the GM-CVQKD protocol,
- 25 Mbit for the 8-PSK DM-CVQKD protocol,
- 20 Mbit for the 4-PSK DM-CVQKD protocol.

Although GM-CVQKD is capable of generating a larger secret key, it only does so at larger elevation angles when the SNR is high. In contrast, DM-CVQKD is capable of generating a secret key at both high elevation angles and low elevation angles where GM-CVQKD cannot. This is emphasised in the second pass, displayed in Figure 7 and Figure 9, which has lower elevation angles. In this situation, GM-CVQKD is not capable of generating a secret key but DM-CVQKD can with the 4-PSK and 8-PSK protocols.

B. \( M \)-QAM Satellite-to-Ground SKRs

This section shows the calculated SKRs for satellite-to-ground \( M \)-QAM without Gaussian optimality under collective attacks from Eve. Since the \( M \)-QAM protocol uses more coherent states in both quadratures, it is impractical to use homodyne detection. It is more efficient and accurate to use heterodyne detection to detect the modulations in the amplitude and phase quadratures. Thus, we have assumed heterodyne detection in our SKR calculations for \( M \)-QAM.
Fig. 7: ISS passes over Mt. John Observatory. The first pass had a maximum elevation angle of 87.6°. The second pass had a maximum elevation angle of 57.2°. Dr = 2 m. Lgeo = 1.029 km.

Fig. 8: SKR for ISS pass over Mt. John Observatory with maximum elevation angle 87.6°. Dr = 2 m. Homodyne detection. Lgeo = 1.029 km.

The results show that by optimising the free parameter v, a probability distribution based on the discrete Gaussian distribution leads to larger SKRs compared to a probability distribution based on the binomial distribution. Furthermore, M-QAM is capable of producing positive SKRs in larger link distances and can achieve them in lower altitude medium Earth orbits (MEO) compared to M-PSK. This is due to more coherent states used and the use of probability distributions to approximate the Gaussian distribution, which is known to maximise the SKR. Consequently, 256-QAM produces larger secret key rates than 64-QAM.

The results are for the asymptotic limit and assume an infinite amount of symbols are sent between the transmitter and receiver. This is not the case in a LEO/MEO-to-ground link and the SKRs are smaller in reality. However, they provide an upper bound of achievable SKRs. As solutions for the finite size limit remains an open question, so does the variability between asymptotic limit and finite size limit M-QAM SKRs in a satellite-to-ground context. As asymptotic limit M-QAM SKRs are much larger than asymptotic limit M-PSK SKRs, once can argue that the same trend holds with finite size limit SKRs. However, it could also be argued that because larger order M-QAM protocols approximate a Gaussian distribution much closer, the inherent advantage of DM-CVQKD, in which the reconciliation efficiency is larger in low SNR regimes, does not hold. In this case, 64-QAM will be able to produce positive SKRs at lower elevation angles than 256-QAM as 256-QAM approximates the Gaussian distribution closer.

As expected, like the SKRs in M-PSK, lower elevation angles yield lower SKRs while good atmospheric conditions and a larger receiver aperture diameter yield larger SKRs.
Fig. 10: Asymptotic limit SKRs of 64-QAM with probabilities based on a binomial and discrete Gaussian distribution in (a) good atmospheric conditions with $D_r = 1$ m, (b) bad atmospheric conditions with $D_r = 1$ m, and (c) bad atmospheric conditions with $D_r = 2$ m. Solid line indicates $\theta = 90^\circ$, dashed line indicates $\theta = 60^\circ$, dash-dotted line indicates $\theta = 30^\circ$. Heterodyne detection.

Fig. 11: Asymptotic limit SKRs of 256-QAM with probabilities based on a binomial and discrete Gaussian distribution in (a) good atmospheric conditions with $D_r = 1$ m, (b) bad atmospheric conditions with $D_r = 1$ m, and (c) bad atmospheric conditions with $D_r = 2$ m. Solid line indicates $\theta = 90^\circ$, dashed line indicates $\theta = 60^\circ$, dash-dotted line indicates $\theta = 30^\circ$. Heterodyne detection.
C. SKR Trends from Parameter Variation Analysis

An analysis of the parameters leads to the following observed trends:

- Increasing the laser repetition rate increases the SKR for a given link distance.
- Decreasing the proportion of symbols needed for channel parameter estimation increases the SKR for a given link distance. However, this comes at a cost of less accurate estimated channel parameters and therefore a decrease in knowledge of the amount of information Eve can access.
- Decreasing the value for allowable information for Eve in the finite size limit (δ_h^{privacy}) increases the SKR for a given link distance. This implies that there is greater accuracy in the estimated amount of information Eve has (Holevo information), which stems from greater accuracy in channel parameter estimation.
- Increasing the transmitter and receiver aperture diameter as well as the transmitter and receiver optics efficiencies increases the maximum link distance and therefore satellite orbit altitude. This results from the decrease in losses during state preparation and measurement.
- Decreasing the pointing loss increases the maximum link distance and therefore satellite orbit altitude. This requires a more accurate APT system as well as less beam wandering between Alice and Bob.
- Increasing the OGS elevation increases the maximum link distance and therefore satellite orbit altitude. This results from the decrease in attenuation from a decrease in link distance and effective atmosphere thickness as Bob is effectively closer to Alice.
- Operating in good atmospheric conditions where there is greater visibility and smaller refractive index structure parameter increases the maximum link distance and therefore satellite orbit altitude. This results from the decrease in attenuation due to less atmospheric scattering and turbulence.
- Protocols with a larger number of coherent states lead to larger SKRs. However, protocols that approximate the Gaussian distribution closer will produce smaller SKRs.

VI. Conclusions

Although Gaussian modulation based CVQKD is known to maximise the secret key rate between Alice and Bob, the dynamic reconciliation efficiency, governed by practical error correction codes, in Gaussian modulations decreases as the SNR decreases. In this work, we show that DM-CVQKD outperforms GM-CVQKD in the context of LEO satellite-to-ground CVQKD, which is predominantly in the low SNR regime, by producing positive SKRs at greater distances and lower elevation angles. Furthermore, higher order DM-CVQKD which have more coherent states and approximate a Gaussian distribution such as 64-QAM and 256-QAM produce larger SKRs in the asymptotic limit. However, their performance in the finite size limit and ability to have large reconciliation efficiencies remains an open question. For a given OGS, LEO satellite passes are unlikely to always reach elevation angles near 90°. Having only GM-CVQKD creates missed opportunities for satellite-to-ground CVQKD. Therefore, using DM-CVQKD or incorporating a hybrid CVQKD system which utilises DM-CVQKD allows more opportunities for CVQKD.

REFERENCES

[1] H.-K. Lo and H. F. Chau, “Unconditional security of quantum key distribution over arbitrarily long distances,” Science, vol. 283, no. 5400, pp. 2050–2056, mar 1999.
[2] J. Yin, Y. H. Li, S. K. Liao, M. Yang, Y. Cao, L. Zhang, J. G. Ren, W. Q. Cai, W. Y. Liu, S. L. Li, R. Shu, Y. M. Huang, L. Deng, L. Li, Q. Zhang, N. L. Liu, Y. A. Chen, C. Y. Lu, X. B. Wang, F. Xu, J. Y. Wang, C. Z. Peng, A. K. Ekert, and J. W. Pan, “Entanglement-based secure quantum cryptography over 1,120 kilometres,” Nature, vol. 582, no. 7813, pp. 501–505, 2020.
[3] F. Lautenbach, C. Pacher, C. H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hubel, “Continuous-Variable Quantum Key Distribution with Gaussian Modulation—The Theory of Practical Implementations,” Advanced Quantum Technologies, vol. 1, no. 1, pp. 1–37, 2018.
[4] R. Garcia-Patron and N. J. Cerf, “Unconditional optimality of gaussian attacks against continuous-variable quantum key distribution,” Phys. Rev. Lett., vol. 97, p. 190503, Nov 2006.
[5] S. Ren, S. Yang, A. Wonfor, R. Penty, and I. White, “Experimental demonstration of high key rate and low complexity CVQKD system with local local oscillator,” Optics InfoBase Conference Papers, vol. Part F174-, pp. 3–5, 2020.
[6] D. Huang, P. Huang, D. Lin, and G. Zeng, “Long-distance continuous-variable quantum key distribution by controlling excess noise,” Scientific Reports, vol. 6, pp. 1–9, 2016.
[7] Z. Qu and I. B. Djordjevic, “High-speed free-space optical continuous-variable-quantum key distribution based on Kramers-Kronig scheme,” IEEE Photonics Journal, vol. 10, no. 6, pp. 1–7, 2018.
[8] ——, “High-speed free-space optical continuous-variable quantum key distribution enabled by three-dimensional multiplexing,” Optics Express, vol. 25, no. 7, p. 7917, 2017.
[9] B. Heim, C. Peuntinger, N. Killoran, I. Khan, C. Wittmann, C. Marquardt, and G. Leuchs, “Atmospheric continuous-variable quantum communication,” New Journal of Physics, vol. 16, 2014.
[10] S. Y. Shen, M. W. Dai, X. T. Zheng, Q. Y. Sun, G. C. Guo, and Z. F. Han, “Free-space continuous-variable quantum key distribution of unidimensional Gaussian modulation using polarized coherent states in an urban environment,” Physical Review A, vol. 100, no. 1, 2019.
[11] A. Leverrier and P. Grangier, “Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation,” Phys. Rev. Lett., vol. 102, p. 180504, May 2009.
[12] F. Grosshans and P. Grangier, “Continuous variable quantum cryptography using coherent states,” Phys. Rev. Lett., vol. 88, p. 057902, Jan 2002.
[13] Y. Shen, H. Zou, L. Tian, P. Chen, and J. Yuan, “Experimental study on discretely modulated continuous-variable quantum key distribution,” Physical Review A - Atomic, Molecular, and Optical Physics, vol. 82, no. 2, pp. 1–7, 2010.
[14] A. Leverrier and P. Grangier, “Continuous-variable quantum key distribution protocols with a discrete modulation,” 2010.
[15] Q. Liao, G. Xiao, C.-G. Xu, Y. Xu, and Y. Guo, “Discretely modulated continuous-variable quantum key distribution with an untrusted entanglement source,” Phys. Rev. A, vol. 102, p. 032604, Sep 2020.
[16] N. Hosseineidehaj, A. M. Lance, T. Symul, N. Walk, and T. C. Ralph, “Finite-size effects in continuous-variable quantum key distribution with Gaussian postselection,” Physical Review A, vol. 101, no. 5, 2020.
[17] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, “Continuous Variable Quantum Cryptography: Beating the 3 dB Loss Limit,” Physical Review Letters, vol. 89, no. 16, pp. 14–17, 2002.
[18] H. Zhong, Y. Guo, Y. Mao, W. Ye, and D. Huang, “Virtual zero-photon catalysis for improving continuous-variable quantum key distribution via Gaussian post-selection,” Scientific Reports, vol. 10, no. 1, pp. 1–12, 2020.
[19] H. Zhang, J. Fang, and G. He, “Improving the performance of the four-state continuous-variable quantum key distribution by using optical amplifiers,” Phys. Rev. A, vol. 86, p. 022338, Aug 2012.
[20] A. Becir, F. A. A. El-Orany, and M. R. B. Wahiddin, “Continuous-variable quantum key distribution protocols with eight-state discrete modulation,” 2010.

[21] I. B. Djordjevic, “Optimized-eight-state cv-qkd protocol outperforming gaussian modulation based protocols,” IEEE Photonics Journal, vol. 11, no. 4, pp. 1–10, 2019.

[22] W. Zhao, R. Shi, Y. Feng, and D. Huang, “Unidimensional continuous-variable quantum key distribution with discrete modulation,” Physics Letters A, vol. 384, no. 2, p. 126061, 2020.

[23] H. Mani, T. Gehring, P. Grabenweger, B. Omer, C. Pacher, and U. L. Andersen, “Multiedge-type low-density parity-check codes for continuous-variable quantum key distribution,” Phys. Rev. A, vol. 103, p. 062419, Jun 2021.

[24] S. P. Kish, E. Villasenor, 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, vol. 2, no. 3, pp. 1–16, 2020.

[25] A. Denys, P. Brown, and A. Leverrier, “Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation,” Quantum, vol. 5, p. 540, Sep. 2021.

[26] F. Bennet, K. Ferguson, K. Grant, E. Kuzins, N. Rattenbury, and S. Schediwy, “An Australia/New Zealand optical communications ground station network for next generation satellite communications,” in Free-Space Laser Communications XXXII, H. Hemmati and D. M. Boroson, Eds., vol. 11272, International Society for Optics and Photonics. SPIE, 2020, pp. 1 – 7.

[27] S. S. Muhammad, P. Köhldorfer, and E. Leitgeb, “Channel modeling for terrestrial free space optical links,” Proceedings of 2005 7th International Conference on Transparent Optical Networks, ICTON 2005, vol. 1, pp. 407–410, 2005.

[28] Z. Zuo, Y. Wang, D. Huang, and Y. Guo, “Atmospheric effects on continuous-mediated continuous-variable quantum key distribution,” Journal of Physics A: Mathematical and Theoretical, vol. 53, no. 46, 2020.

[29] M. Aspelmeier, T. Jennewein, M. Pfennigbauer, W. R. Leeb, and A. Zeilinger, “Long-Distance Quantum Communication With Entangled Photons Using Satellites,” IEEE Journal on Selected Topics in Quantum Electronics, vol. 9, no. 6, pp. 1541–1551, 2003.

[30] I. I. Kim, B. McArthur, and E. J. Korevaar, “Comparison of laser beam propagation at 785 nm and 1550 nm in fog and haze for optical wireless communications,” Optical Wireless Communications III, vol. 4214, pp. 26–37, 2001.

[31] M. Grabner and V. Kvicera, “Fog attenuation dependence on atmospheric visibility at two wavelengths for FSO link planning,” 2010 Loughborough Antennas and Propagation Conference, LAPC 2010, no. November, pp. 193–196, 2010.

[32] D. Gigan, “Fading-loss assessment in atmospheric free-space optical communication links with on-off keying,” Optical Engineering, vol. 47, no. 4, p. 046001, 2008.

[33] L. C. Andrews, R. L. Phillips, D. Wayne, T. Leclerc, P. Sauer, R. Crabbs, and J. Kiriazes, “Near-ground vertical profile of refractive-index fluctuations,” in Atmospheric Propagation VI, L. M. W. Thomas and G. C. Gilbreath, Eds., vol. 7324, International Society for Optics and Photonics. SPIE, 2009, pp. 11 – 22.

Biveen Shajilal received the M.Sc. degree in Photonics from the Cochin University of Science and Technology, Kerala, India. He is a doctoral candidate at the Department of Quantum Science and Technology, Australian National University. His research interests include quantum states of light, quantum communications, quantum entanglement and quantum information.

Sebastian P. Kish was awarded a Ph.D. in Physics from The University of Queensland, Australia, in 2019. Sebastian is currently a postdoctoral fellow at The Australian National University and previously held a research associate position at UNSW. His research interests include quantum communications, quantum information and quantum entanglement.

Syed M. Assad received the B.Sc degree with a double major in physics and computational science from the National University of Singapore, and the joint Ph.D. degree in realization of harmonic entanglement between a light beam and its second harmonic, and theoretical proofs of security for quantum key distribution protocols from the National University of Singapore and The Australian National University in 2011. He was with the National University of Singapore as a Teaching Assistant and the Centre for Quantum Technologies as a Research Assistant with the Quantum Optics Group, The Australian National University, since 2011, where he is currently leading the Secure Communications Team. He is a member of the Centre of Excellence for Quantum Computation and Communication Technology.

Ping Koy Lam received a BSc degree with a double major in mathematics and physics from The University of Auckland, an MSc degree in theoretical physics and a PhD degree in experimental physics from The Australian National University (ANU). He was a Process Engineer with Sony (audio electronics) and Hewlett-Packard (semiconductor LED) for three years prior to his post-graduate studies with ANU. He was a recipient of the Australian Institute of Physics Bragg Medal and the Australian National University Crawford Prize for his PhD dissertation in 1999. He was awarded the British Council Eureka Prize for inspiring science (2003) and the University of New South Wales Eureka Prize for innovative research (2006). He is currently the chief quantum scientist at the Agency for Science, Technology, And Research (A*STAR) in Singapore. He has authored around 260 articles on his research in quantum physics.

Nicholas Rattenbury was awarded a Ph.D. in Physics from The University of Auckland, New Zealand, in 2004. Nicholas leads research in free space optical communications, astrodynamics and time-domain astrophysics.

Mikhael Sayat received the B.E. (Hons.) degree in Mechatronics Engineering and B.Sc. degree in Physics from the University of Auckland, New Zealand in 2021. He was the recipient of the 2022 New Zealand Space Scholarship to intern at NASA JPL. He is a doctoral candidate at the University of Auckland and is currently at the Department of Quantum Science and Technology, Australian National University. His research interests include quantum key distribution, space-based quantum communications, and quantum networks.

John Cater was awarded a B.E. with Honours in Mechanical Engineering from the University of Auckland, New Zealand in 1997, and a Ph.D. from Monash University in Australia in 2003. John leads research in aerospace engineering; his interests include electric propulsion for small satellites and modelling of thermal protection systems for reentry of spacecraft.