


## RESEARCH ARTICLE

# Secret key rates of free-space optical continuous-variable quantum key distribution

Laszlo Gyongyosi<sup>1,2,3</sup>  | Sandor Imre<sup>2</sup>

<sup>1</sup>School of Electronics and Computer Science, University of Southampton, Southampton, UK

<sup>2</sup>Department of Networked Systems and Services, Budapest University of Technology and Economics, Budapest, Hungary

<sup>3</sup>MTA-BME Information Systems Research Group, Hungarian Academy of Sciences, Budapest, Hungary

**Correspondence**

Laszlo Gyongyosi, School of Electronics and Computer Science, University of Southampton, Southampton, SO17 1BJ, UK.

Email: lasgy\_ph@yahoo.com

**Funding information**

Hungarian Scientific Research Fund, Grant/Award Number: OTKA K-112125; Budapesti Műszaki és Gazdaságtudományi Egyetem, Grant/Award Number: BME FIKP-MI/SC; National Research Development and Innovation Office of Hungary, Grant/Award Number: 2017-1.2.1-NKP-2017-00001; National Research, Development and Innovation Fund, Grant/Award Number: TUDFO/51757/2019-ITM, Thematic Excellence Program

**Summary**

In this letter, we derive the maximal achievable secret key rates for continuous-variable quantum key distribution (CVQKD) over free-space optical (FSO) quantum channels. We provide a channel decomposition for FSO-CVQKD quantum channels and study the SNR (signal-to-noise ratio) characteristics. The analytical derivations focus particularly on the low-SNR scenarios. The results are convenient for wireless quantum key distribution and for the quantum Internet.

**KEYWORDS**

cryptography, networking, quantum cryptography, quantum key distribution, security

## 1 | INTRODUCTION

Free-space optical (FSO) quantum links<sup>1-6</sup> provide a tool to implement quantum communications via wireless telecommunication<sup>6-10</sup> network infrastructures. As an integrated component of future quantum Internet<sup>11-16</sup> and long-distance quantum communications,<sup>11,17-29</sup> the FSO quantum channels could play a significant role in the global-scale practical implementations of quantum communications and quantum key distribution (QKD).<sup>1-3,30-36,44-49</sup> QKD systems allow us to utilize the fundamentals of quantum mechanics to realize unconditionally secure communications for legal users. QKD protocols can be decomposed into discrete-variable (DV) and continuous-variable (CV) counterparts.<sup>11,17-27</sup> Continuous-variable quantum key distribution (CVQKD) schemes enable parties to use standard telecommunication

This is an open access article under the terms of the Creative Commons Attribution License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.

© 2019 The Authors. International Journal of Communication Systems published by John Wiley & Sons, Ltd.

devices for experimental implementations.<sup>4-6,11,17-27,43-49</sup> The multicarrier CVQKD has been recently introduced through the adaptive quadrature division modulation (AMQD) scheme.<sup>44</sup> The multicarrier CVQKD injects several additional degrees of freedom into the transmission, which are not available for a standard, single-carrier CVQKD setting.<sup>45-48,50</sup> The achievable secret key rates in a multicarrier CVQKD setting have been proven in Gyongyosi and Imre.<sup>47</sup> The secret key rates confirm the multimode bounds determined in Pirandola et al.<sup>1</sup>

The FSO systems bring several new attributes to both the theoretical and experimental side of CVQKD. An FSO quantum link's special characteristics require a specific mathematical description. The channel characteristics of the FSO quantum links are approachable via the mathematical framework of the GG (gamma-gamma) distribution.<sup>6-10</sup> The secret key rates for CVQKD schemes over FSO links and the performance of free-space quantum links in diverse environmental conditions raise several questions and call for further examination. Another interesting problem is the private classical capacity<sup>4</sup> of a GG link. Without loss of generality, the private classical capacity measures the amount of classical information that can be privately transmitted from a sender (Alice) to a receiver (Bob) in the presence of an eavesdropper (Eve). For further information on the rate-loss scaling in quantum optical communications, we suggest the derivations in Pirandola et al.<sup>1</sup> Our results on the private classical capacity also confirm the bounds of<sup>2</sup> on private quantum communications in a CVQKD setting.

The private classical capacity imposes a theoretical upper bound on the achievable secret key rates in QKD implementations. Since practical QKD implementations operate in the low-SNR regime,<sup>11,17-27,44</sup> we will analyze the behavior of private classical capacity in the low-SNR domain for CVQKD over FSO (referred to as FSO-CVQKD). By theory, the DVQKD and CVQKD implementations require different channel models. For DVQKD, the resulting channel noise distribution is analogous to the binary-symmetric channel (BSC),<sup>23</sup> while for the DVQKD setting, the resulting noise is Gaussian.<sup>11,17-27</sup> Another important difference from traditional crypto systems is that the correlation measure functions are non-traditional. In the theoretical analysis, it is assumed that the legal parties and the eavesdropper have quantum memories and can perform joint measurements,<sup>11,17-27</sup> therefore the Holevo information<sup>4</sup> is the appropriate correlation measure function for deriving the private classical capacity.

Several works have focused on implementations of CVQKD in diverse networking conditions,<sup>11,17,19-27,44</sup> but the question of the achievable secret key rates over FSO quantum links remains open. Consequently, we have chosen to investigate the FSO-CVQKD case because of its significant benefits over DVQKD in practical implementations.

The novel contributions of our paper are as follows:

- *We derive an upper bound for the secret key rates of wireless CVQKD over FSO channels.*
- *We provide a decomposition model for the FSO quantum channel in a CVQKD setting.*
- *We investigate the SNR attributes of the GG-channel and the complementary channel for the information leakage.*

This paper is organized as follows: Section 2 provides the channel model for FSO-CVQKD. Section 3 focuses on the private classical capacity of an FSO link in a CVQKD setting. Finally, Section 4 concludes the results.

## 2 | SYSTEM MODEL

In this section, the general formulas and equations are briefly summarized.

The  $\mathcal{P}(\mathcal{N})$  private classical capacity identifies the maximum rate at which classical information can be transmitted privately (ie, an eavesdropper has no knowledge about the original message) over a quantum channel  $\mathcal{N}$ . To derive the  $\mathcal{P}(\mathcal{N})$  private classical capacity of  $\mathcal{N}$  in the FSO setting, the physical quantum link  $\mathcal{N}$  is divided into logical channels  $\mathcal{N}_{AB}$ ,  $\mathcal{N}_{AE}$ , and  $\mathcal{N}_{BE}$ . Logical channel  $\mathcal{N}_{AB}$  denotes information transmission through the GG quantum channel between Alice ( $A$ ) and Bob ( $B$ ). Logical channels  $\mathcal{N}_{AE}$  and  $\mathcal{N}_{BE}$  are complementary channels that model the information leakage from Alice to eavesdropper Eve ( $E$ ), and the information leakage from Bob to Eve, respectively. In our setting,  $\mathcal{N}_{AE}$  is relevant for the DV case, while  $\mathcal{N}_{BE}$  is important in the reverse reconciliation of CVQKD (Bob starts the reconciliation to minimize information leakage).

Let

$$|\varphi_j\rangle = |x_j + ip_j\rangle, \quad (1)$$

identify a  $j$ th input coherent state (Gaussian state) in the phase space  $S$ , with *i.i.d.* Gaussian random position and momentum quadratures  $x_j \in \mathcal{N}(0, \sigma_{\omega_0}^2)$  and  $p_j \in \mathcal{N}(0, \sigma_{\omega_0}^2)$ , where  $\sigma_{\omega_0}^2$  is the modulation variance. The coherent state  $|\varphi_j\rangle$  in the phase space  $S$  can be modeled as a zero-mean, circular symmetric complex Gaussian random variable

$$z_j \in \mathcal{CN}(0, \sigma_{\omega_{z_j}}^2), \quad (2)$$

with variance

$$\sigma_{\omega_{z_j}}^2 = \mathbb{E}[|z_j|^2] = \mathbb{E}[x_j^2 + p_j^2] = 2\sigma_{\omega_0}^2, \quad (3)$$

and with *i.i.d.* real and imaginary zero-mean Gaussian random components,  $\text{Re}(z_j) \in \mathcal{N}(0, \sigma_{\omega_0}^2)$ ,  $\text{Im}(z_j) \in \mathcal{N}(0, \sigma_{\omega_0}^2)$ .

The transmission of this complex variable over the Gaussian quantum channel  $\mathcal{N}$  can be characterized by the  $T(\mathcal{N}) \in \mathbb{C}$  normalized complex transmittance variable

$$T(\mathcal{N}) = \text{Re}T(\mathcal{N}) + i\text{Im}T(\mathcal{N}), \quad (4)$$

where  $0 \leq \text{Re}T(\mathcal{N}) \leq 1/\sqrt{2}$  is the transmission of the position quadrature and  $0 \leq \text{Im}T(\mathcal{N}) \leq 1/\sqrt{2}$  is the transmission of the momentum quadrature. During the evaluation of the private classical capacity for an FSO setting, we assume that the CVQKD protocol operates in the low-SNR regime,  $\text{SNR} \rightarrow 0$ ,<sup>8</sup> which is precisely the situation for practical CVQKD scenarios.

Utilizing an FSO channel for the transmission of a given input  $z_j$ , logical channel  $\mathcal{N}_{AB}$  is defined as

$$\mathcal{N}_{AB} : T(\mathcal{N})z_j + \epsilon_j, \quad (5)$$

where  $\epsilon_j$  is a zero-mean, circular symmetric complex Gaussian random variable that identifies the Gaussian noise added by Eve;  $\epsilon_j \in \mathcal{CN}(0, \sigma_{\epsilon_j}^2)$ , with variance  $\sigma_{\epsilon_j}^2 = \mathbb{E}[|\epsilon_j|^2] = 2\sigma_{\epsilon_{ve}}^2$ , and with *i.i.d.* real and imaginary zero-mean Gaussian random components,  $\text{Re}(\epsilon_j) \in \mathcal{N}(0, \sigma_{\epsilon_{ve}}^2)$ ,  $\text{Im}(\epsilon_j) \in \mathcal{N}(0, \sigma_{\epsilon_{ve}}^2)$ , while the  $T(\mathcal{N})$  complex transmittance coefficient is as

$$T(\mathcal{N}) = \eta I + i\eta I, \quad (6)$$

where  $\eta$  is the effective photocurrent conversion ratio of the receiver, while  $I$  is the normalized irradiance with the gamma-gamma (GG) probability density<sup>7-10</sup>

$$f(I) = \frac{2(ab)^{\frac{a+b}{2}}}{\Gamma(a)\Gamma(b)} I^{\frac{a+b}{2}-1} K_{a-b}(2\sqrt{abI}), \quad (7)$$

where  $K_\nu(\cdot)$  is the modified Bessel function of the second kind and of order  $\nu$ ,<sup>8</sup>  $\Gamma(\cdot)$  is the Gamma function, while  $a \geq 0$ , and  $b \geq 0$  are the distribution-shaping parameters expressed as

$$a = \left[ \exp\left(\frac{0.49\delta^2}{(1 + 0.18d^2 + 0.56\delta^{12/5})^{7/6}}\right) - 1 \right]^{-1}, \quad (8)$$

and

$$b = \left[ \exp\left(\frac{0.51\delta^2}{(1 + 0.9d^2 + 0.62\delta^{12/5})^{5/6}}\right) - 1 \right]^{-1}, \quad (9)$$

where

$$\delta^2 = 1.23C^2|x_j|^{7/6}l^{11/6} = 1.23C^2|p_j|^{7/6}l^{11/6} \quad (10)$$

is the Rytov variance,  $C^2$  is the altitude-dependent turbulence strength,  $l$  is the length of the link, and  $|k|$  is the optical wave number, while  $d = \sqrt{|k|D^2/4l}$ , where  $D$  is the receiver's aperture diameter.<sup>8</sup> The complementary channel  $\mathcal{N}_{BE}$  for a reverse reconciliation in the CVQKD case is defined as

$$\mathcal{N}_{BE} : \mathcal{N} \left( 0, \sigma_{\mathcal{N}_{BE}}^2 \right), \quad (11)$$

where  $\sigma_{\mathcal{N}_{BE}}^2$  is the noise variance for  $\mathcal{N}_{BE}$ . Assuming that the parties have quantum memories and can perform joint measurement on their quantum registers in the QKD protocol run, the appropriate correlate measure functions for the logical channels  $\mathcal{N}_{AB}$ ,  $\mathcal{N}_{AE}$ , and  $\mathcal{N}_{BE}$  are the Holevo quantities<sup>4</sup>  $\chi_{AB}$ ,  $\chi_{AE}$ , and  $\chi_{BE}$ .

Without loss of generality, for the  $S(\mathcal{N})$  secret key rate over a quantum channel  $\mathcal{N}$ , the following relation holds:

$$S(\mathcal{N}) \leq \lim_{n \rightarrow \infty} \frac{1}{n} P(\mathcal{N}), \quad (12)$$

where  $P(\mathcal{N})$  is the private classical capacity of  $\mathcal{N}$ . Assuming reverse reconciliation in CVQKD with GG channel  $\mathcal{N}_{AB}$  and Eve's Gaussian channel  $\mathcal{N}_{BE}$ ,  $P(\mathcal{N})$  is

$$P(\mathcal{N}) = \lim_{n \rightarrow \infty} \frac{1}{n} \max_{\forall p_i, \rho_i} (f \chi_{AB} - \chi_{BE}), \quad (13)$$

where  $f$  is the reconciliation efficiency,  $\chi_{AB}$  is the Holevo information between Alice and Bob

$$\chi_{AB} = S(\mathcal{N}_{AB}(\rho_{AB})) - \sum_i p_i S(\mathcal{N}_{AB}(\rho_i)) \quad (14)$$

and  $\chi_{BE}$  is the Holevo information between Bob and Eve

$$\chi_{BE} = S(\mathcal{N}_{BE}(\rho_{BE})) - \sum_i p_i S(\mathcal{N}_{BE}(\rho_i)) \quad (15)$$

are the Holevo quantities between Alice and Bob and Bob and Eve;  $S(\rho) = -\text{Tr}(\rho \log(\rho))$  is the von Neumann entropy, while  $\rho_{AB} = \sum_i p_i \rho_i$  and  $\rho_{BE} = \sum_i p_i \rho_i$ . The quantity  $\chi_{BE}$  is the Holevo information between Bob and Eve, which plays a role in a reverse reconciliation CVQKD. We also use this approach to derive  $\mathcal{P}(\mathcal{N})$  for the CVQKD case, since reverse reconciliation is proved to minimize the eavesdropper's Holevo information compared with the direct-reconciliation case.

Thus,  $P(\mathcal{N})$  at a reverse reconciliation with reconciliation efficiency  $f$  is evaluated as

$$P(\mathcal{N}) = \lim_{n \rightarrow \infty} \frac{1}{n} \left( f \left( \max_{\forall p_i, \rho_i} S \left( \mathcal{N}_{AB} \left( \sum_i p_i (\rho_i) \right) \right) - \sum_i p_i S(\mathcal{N}_{AB}(\rho_i)) \right) - S \left( \mathcal{N}_{BE} \left( \sum_i p_i (\rho_i) \right) \right) + \sum_i p_i S(\mathcal{N}_{BE}(\rho_i)) \right), \quad (16)$$

where  $\mathcal{N}(\rho_i)$  represents the  $i$ th output density matrix.

Specifically, the  $D(\cdot \| \cdot)$  quantum relative entropy function between density matrices  $\rho$  and  $\sigma$  is

$$\begin{aligned} D(\rho \| \sigma) &= \text{Tr}(\rho \log(\rho)) - \text{Tr}(\rho \log(\sigma)) \\ &= \text{Tr}[\rho (\log(\rho) - \log(\sigma))]. \end{aligned} \quad (17)$$

The Holevo quantity can be expressed by the quantum relative entropy function as  $\chi = D(\rho_k \| \sigma)$ , where  $\rho_k$  denotes an optimal channel output state (for which the Holevo quantity will be maximal) and  $\sigma = \sum p_k \rho_k$ . The Holevo information  $\chi$  can be derived in terms of  $D(\cdot \| \cdot)$  as

$$\begin{aligned}
\sum_k p_k D(\rho_k \| \sigma) &= \sum_k (p_k \text{Tr}(\rho_k \log(\rho_k))) - \text{Tr}\left(\sum_k (p_k \rho_k \log(\sigma))\right) \\
&= \sum_k (p_k \text{Tr}(\rho_k \log(\rho_k))) - \text{Tr}(\sigma \log(\sigma)) \\
&= S(\sigma) - \sum_k p_k S(\rho_k) = \chi.
\end{aligned} \tag{18}$$

Therefore,  $\chi_{AB}$  is rewritten as

$$\chi_{AB} = S\left(\mathcal{N}_{AB}\left(\sum_i p_i \rho_i\right)\right) - \sum_i p_i S(\mathcal{N}_{AB}(\rho_i)). \tag{19}$$

The quantity  $\chi_{BE}$  measures the Holevo information leaked to Eve from Bob during a reverse reconciliation and is written as

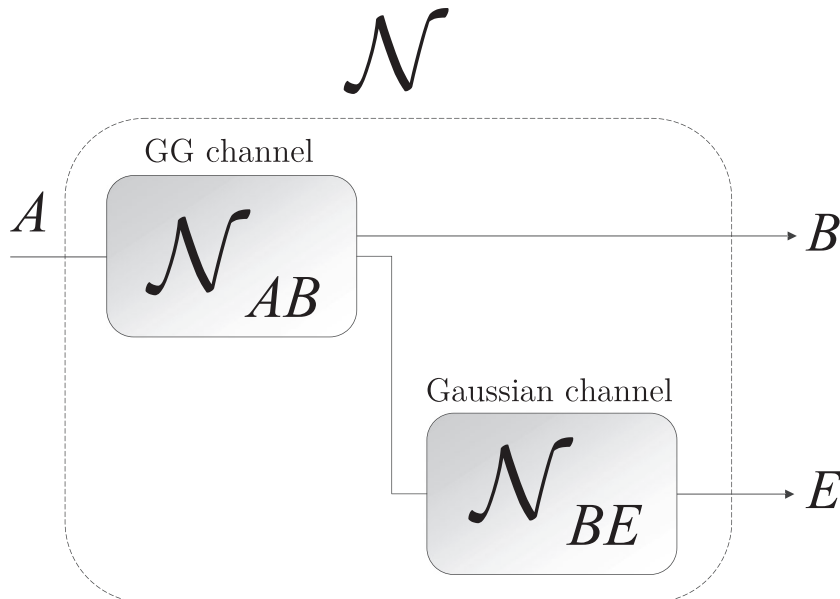
$$\chi_{BE} = S\left(\mathcal{N}_{BE}\left(\sum_i p_i \rho_i\right)\right) - \sum_i p_i S(\mathcal{N}_{BE}(\rho_i)). \tag{20}$$

Using (19) and (20),  $P(\mathcal{N})$  can be expressed as

$$\begin{aligned}
P(\mathcal{N}) &= \lim_{n \rightarrow \infty} \frac{1}{n} \left( f\left(\min_{\rho} \max_{\sigma} D(\rho_k^{AB} \| \sigma^{AB})\right) - \min_{\sigma} \max_{\rho} D(\rho_k^{BE} \| \sigma^{BE}) \right) \\
&= \lim_{n \rightarrow \infty} \frac{1}{n} \left( f(\min_{\sigma} \max_{\rho} D(\rho_k^{AB-BE} \| \sigma^{AB-BE})) \right),
\end{aligned} \tag{21}$$

where  $\rho_k^{AB-BE}$  is the final optimal density matrix, while  $\sigma^{AB-BE}$  refers to the final output average density matrix.

Figure 1 depicts the model of FSO-CVQKD channel  $\mathcal{N}$  used for the derivation of  $P(\mathcal{N})$ .



**FIGURE 1** Decomposition of a physical quantum link  $\mathcal{N}$  into logical channels  $\mathcal{N}_{AB}$  and  $\mathcal{N}_{BE}$  in an FSO-CVQKD setting at a reverse reconciliation. The input system of the link is  $A$ , Bob's system is  $B$ , and Eve's system is  $E$ . The logical channel  $\mathcal{N}_{AB}$  refers to the FSO link between Alice and Bob with the GG characteristics and Gaussian noise. The complementary channel  $\mathcal{N}_{BE}$  is a Gaussian channel between Bob and Eve

### 3 | RESULTS

**Theorem 1.** (Scalability of the secret key rate). At a direct or reverse reconciliation with channels  $\mathcal{N}_{AE}$  and  $\mathcal{N}_{BE}$  between Alice and Eve and Bob and Eve, the  $S(\mathcal{N})$  secret key rate over an FSO link  $\mathcal{N}$  in any CVQKD protocol is scalable by the  $\text{SNR}_{AB}$  of  $\mathcal{N}_{AB}$ .

*Proof.* Let  $\mathcal{N}_{AB}$  be the quantum channel between Alice and Bob. For the transmission of a given  $z_i$ , let the SNR of  $\mathcal{N}_{AB}$  be evaluated as

$$\text{SNR}_{AB} = \frac{2\sigma_{\omega_0}^2}{\sigma_{\mathcal{N}_{AB}}^2}, \quad (22)$$

where  $\sigma_{\omega_0}^2$  is the modulation variance of a quadrature component and  $\sigma_{\mathcal{N}_{AB}}^2 = 2\sigma_{Eve}^2$  is the variance of the Gaussian noise. To evaluate the private classical capacity, we consider three scenarios<sup>8</sup> for the values of coefficients  $a$  and  $b$ . First, assume that<sup>8</sup>  $a + b = \frac{13}{2}$ , which yields

$$\tau \text{SNR}_{AB} \approx e^{-2\sqrt{ab}\left(\frac{\lambda}{\Omega}\right)^{1/4}}, \quad (23)$$

where

$$\tau = \frac{\Gamma(a)\Gamma(b)\Omega}{2\sqrt{\pi}(ab)^2}, \quad (24)$$

while coefficient  $\Omega$  is as

$$\Omega = (\eta \mathbb{E}[I])^2 = \eta^2 \quad (25)$$

and  $\lambda$  is a Lagrange multiplier.<sup>8-10</sup> Then, let  $\lambda_{\text{SNR}}$  be a Lagrange multiplier at an average power constraint  $c$ ,

$$c : 2\tilde{\sigma}_{\omega_0}^2 = \text{SNR}_{AB} = \frac{1}{16(ab)^2} \Omega \text{SNR}_{AB} \log^4 \left( \frac{1}{\tau \text{SNR}_{AB}} \right), \quad (26)$$

where  $2\tilde{\sigma}_{\omega_0}^2$  refers to the average input power<sup>8-10</sup> associated to a  $j$ th input  $z_j$  and  $\gamma = \eta^2 I^2$ .<sup>8-10</sup> The resulting modulation variance  $2\sigma_{\omega_0}^2$  for  $\mathcal{N}_{AB}$  with  $\text{SNR}_{AB}$  is then

$$2\sigma_{\omega_0}^2 \approx \text{SNR}_{AB} \sigma_{\mathcal{N}_{AB}}^2 = 2\frac{1}{\tau} e^{-2\sqrt{ab}\left(\frac{\lambda}{\Omega}\right)^{1/4}} \sigma_{\mathcal{N}_{AB}}^2, \quad (27)$$

which allows us to evaluate  $\mathcal{P}(\mathcal{N})$  at  $a + b = \frac{13}{2}$  via (13), where  $\chi_{AB}$  is the Holevo information between Alice and Bob over  $\mathcal{N}_{AB}$ ,

$$\chi_{AB} \geq \frac{\text{SNR}_{AB}}{16(ab)^2} \Omega \log^4(\tau \text{SNR}_{AB}), \quad (28)$$

while  $\chi_{BE}$  is the Holevo information derived via the Gaussian channel  $\mathcal{N}_{BE}$  between Bob and Eve,

$$\chi_{BE} = \sum_{i=1}^2 G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^4 G\left(\frac{\lambda_i - 1}{2}\right), \quad (29)$$

where

$$G(x) = (x + 1) \log_2(x + 1) - x \log_2 x, \quad (30)$$

and  $\lambda_{1,2}^2 = \frac{1}{2}(A \pm \sqrt{A^2 - 4B})$ ,  $\lambda_{3,4}^2 = \frac{1}{2}(C \pm \sqrt{C^2 - 4D})$ ,  $\lambda_5 = 1$ ,<sup>26,27</sup> where  $A = V^2(1 - 2T) + 2T + T^2(V + \kappa_{line})^2$ ,  $V = \sigma_{\omega_0}^2 + 1$ ,  $\kappa_{line}$  is the total channel-added noise,<sup>26</sup>  $B = T^2(V\kappa_{line} + 1)^2$ ,  $C = \frac{1}{(T(V + \kappa_{tot}))^2} (A\kappa_M^2 + B + 1 + 2\kappa_M(V\sqrt{B} + T(V + \kappa_{line})) + 2T(V^2 - 1))$ , while  $\kappa_{tot}$  is the overall noise  $\kappa_{tot} = \kappa_{line} + \kappa_M \frac{1}{T}$ ,  $\kappa_M$  is the detector-added error,<sup>27</sup>  $D = \left(\frac{V + \sqrt{B}\kappa_M}{T(V + \kappa_{tot})}\right)^2$ , with an  $\text{SNR}_{BE}$  of the Gaussian channel  $\mathcal{N}_{BE}$ , as

$$\text{SNR}_{BE,i} = \frac{2\sigma_{\omega}^{2'}}{2\sigma_{\mathcal{N}_{BE,i}}^2}, \quad (31)$$

where  $2\sigma_{\omega}^{2'}$  is the modulation variance of Bob's noisy  $z'_i$ . Second, let's assume that<sup>8-10</sup>  $a + b > \frac{13}{2}$ , thus after some calculations,  $\lambda_{\text{SNR}_{AB}}$  is as

$$\lambda_{\text{SNR}_{AB}} \approx \frac{m^4 \Omega}{16(ab)^2} \log^4 \left( \frac{2\sqrt{ab}}{m\Omega^{1/4}} (\tau \text{SNR}_{AB})^{-1/m} \right), \quad (32)$$

where  $m < 0$ , and  $\text{SNR}_{AB}$  of  $\mathcal{N}_{AB}$  is

$$\text{SNR}_{AB} \approx \frac{1}{\tau} \lambda^{\frac{a+b}{4} - \frac{13}{8}} e^{-2\sqrt{ab\sqrt{\lambda/\Omega}}}. \quad (33)$$

Thus, the resulting modulation variance  $2\sigma_{\omega_0}^2$  is as

$$2\sigma_{\omega_0}^2 \approx 2\frac{1}{\tau} \lambda^{\frac{a+b}{4} - \frac{13}{8}} e^{-2\sqrt{ab\sqrt{\lambda/\Omega}}} \sigma_{\mathcal{N}_{AB}}^2, \quad (34)$$

from which  $\mathcal{P}(\mathcal{N})$  at  $a + b > \frac{13}{2}$  is yielded from the Holevo information  $\chi_{AB}$  of  $\mathcal{N}_{AB}$ , written as

$$\chi_{AB} \geq \frac{m^4 \text{SNR}_{AB}}{16(ab)^2} \Omega \mathcal{L}_{-1}^4 \left( \frac{2\sqrt{ab}}{m\Omega^{1/4}} (\tau \text{SNR}_{AB})^{-1/m} \right), \quad (35)$$

where  $\mathcal{L}(\cdot)$  is the product logarithm function,  $\mathcal{L}_{-1}$  refers to the lower branch of the function  $\mathcal{L}$ ,<sup>7-10</sup> and  $\chi_{BE}$  is given by (29). Finally, at  $a + b < \frac{13}{2}$ , after some calculations,  $\lambda_{\text{SNR}_{AB}}$  is yielded as

$$\lambda_{\text{SNR}_{AB}} \approx \frac{m^4 \Omega}{16(ab)^2} \log^4 \left( \frac{2\sqrt{ab}}{m\Omega^{1/4}} (\tau \text{SNR}_{AB})^{-1/m} \right), \quad (36)$$

where  $m > 0$ ; thus the resulting modulation variance  $2\sigma_{\omega_0}^2$  is

$$2\sigma_{\omega_0}^2 \approx 2\frac{1}{\tau} \lambda^{\frac{a+b}{4} - \frac{13}{8}} e^{-2\sqrt{ab\sqrt{\lambda/\Omega}}} \sigma_{\mathcal{N}_{AB}}^2, \quad (37)$$

from which  $\mathcal{P}(\mathcal{N})$  at  $a + b < \frac{13}{2}$  is approachable from the Holevo information  $\chi_{AB}$  of  $\mathcal{N}_{AB}$ , where  $\chi_{AB}$  is as follows:

$$\chi_{AB} \geq \frac{m^4 \text{SNR}_{AB}}{16(ab)^2} \Omega \mathcal{L}_0^4 \left( \frac{2\sqrt{ab}}{m\Omega^{1/4}} (\tau \text{SNR}_{AB})^{-1/m} \right), \quad (38)$$

where  $\mathcal{L}_0$  is the principal branch of  $\mathcal{L}$ ,<sup>8</sup> while  $\chi_{BE}$ , as given by (29). The proof is concluded here.  $\square$

The next theorem focuses on the reverse reconciliation case.

**Theorem 2.** (Maximized secret key rate over an FSO link in CVQKD at a reverse reconciliation). The  $\mathcal{P}(\mathcal{N})$  of an FSO channel  $\mathcal{N}$  in a CVQKD setting for  $\text{SNR}_{AB} \rightarrow 0$  of  $\mathcal{N}_{AB}$ , at a reconciliation efficiency  $f$  is

$$\mathcal{P}(\mathcal{N}) = \lim_{n \rightarrow \infty} \frac{1}{n} \max_{\forall i} \left( f \left( \frac{\Omega}{16(ab)^2} \text{SNR}_{AB} \log^4 \left( \frac{1}{\text{SNR}_{AB}} \right) \right) - \chi_{BE} \right). \quad (39)$$

*Proof.* Utilizing parameters of the FSO channel model yields the  $f\chi_{AB}$  quantity for the FSO link  $\mathcal{N}$  in the low SNR regime (eg,  $\text{SNR}_{AB} \rightarrow 0$  for  $\mathcal{N}_{AB}$ ) as

$$f\chi_{AB} \geq f \left( \frac{\Omega}{16(ab)^2} \frac{\sigma_{\omega_0}^2}{\sigma_{\mathcal{N}}^2} \log^4 \left( \frac{\sigma_{\mathcal{N}_{AB}}^2}{\sigma_{\omega_0}^2} \right) \right) \quad (40)$$

with

$$\text{SNR}_{AB} = \frac{2\sigma_{\omega_0}^2}{\sigma_{\mathcal{N}_{AB}}^2} = \frac{\sigma_{\omega_0}^2}{\sigma_{Eve}^2} \approx \frac{1}{\tau} \lambda^{\frac{a+b}{4} - \frac{13}{8}} e^{-2\sqrt{ab\sqrt{\lambda/\Omega}}}, \quad (41)$$

and the  $\lambda_{\text{SNR}_{AB}}$  Lagrange multiplier is evaluated as

$$\lambda_{\text{SNR}_{AB}} = \frac{1}{\tau} \lambda^{\frac{a+b}{4} - \frac{5}{8}} e^{-2\sqrt{ab\sqrt{\lambda/\Omega}}} \frac{1}{\text{SNR}_{AB}}, \quad (42)$$

where

$$\tau = \frac{\Gamma(a)\Gamma(b)\Omega^{\frac{a+b}{4} - \frac{5}{8}}}{2\sqrt{\pi}(ab)^{\frac{a+b}{2} - \frac{5}{4}}}. \quad (43)$$

The Holevo information  $\chi_{BE}$  of Eve is as given by (29), the proof is therefore concluded here.  $\square$

## 4 | CONCLUSIONS

This letter studied the performance of CVQKD over free-space optical quantum channels. The analysis provided the private classical capacity of an FSO link for the CVQKD protocols at a reverse reconciliation. Our derivations were focused on the low-SNR setting. The results prove to be convenient for wireless quantum communications, wireless quantum key distribution and quantum Internet scenarios.

## ACKNOWLEDGEMENTS

The research reported in this paper has been supported by the National Research, Development and Innovation Fund (TUDFO/51757/2019-ITM, Thematic Excellence Program). This work was partially supported by the National Research Development and Innovation Office of Hungary (Project 2017-1.2.1-NKP-2017-00001), by the Hungarian Scientific Research Fund - OTKA K-112125 and in part by the BME Artificial Intelligence FIKP grant of EMMI (BME FIKP-MI/SC).

## STATEMENTS

### ETHICS STATEMENT

This work did not involve any active collection of human data.

### DATA ACCESSIBILITY STATEMENT

This work does not have any experimental data.

### COMPETING FINANCIAL INTERESTS STATEMENT

We have no competing financial interests.

### COMPETING INTERESTS STATEMENT

We have no competing interests.

## AUTHORS' CONTRIBUTIONS

L.GY. designed the protocol and wrote the manuscript. L.GY. and S.I. analyzed the results. All authors reviewed the manuscript.



## ORCID

Laszlo Gyongyosi  <https://orcid.org/0000-0002-4209-7619>

## REFERENCES

1. Pirandola S, Laurenza R, Ottaviani C, Banchi L. Fundamental limits of repeaterless quantum communications. *Nat Commun.* 2017;8:15043. <https://doi.org/10.1038/ncomms15043>
2. Pirandola S, Braunstein SL, Laurenza R, et al. Theory of channel simulation and bounds for private communication. *Quantum Sci Technol.* 2018;3:35009.
3. Pirandola S. Capacities of Repeater-Assisted Quantum Communications. arXiv preprint arXiv:1601.00966; 2016.
4. Gyongyosi L, Imre S, Nguyen HV. A survey on quantum channel capacities. *IEEE Commun Surv Tutor.* 2018;20(2):1149-1205.
5. Lloyd S, Shapiro JH, Wong FNC, Kumar P, Shahriar SM, Yuen HP. Infrastructure for the quantum Internet. *ACM SIGCOMM Comput Commun Rev.* 2004;34(5):9-20.
6. Imre S, Gyongyosi L. *Advanced Quantum Communications—An Engineering Approach.* New Jersey, USA: Wiley-IEEE Press; 2012.
7. Kiasaleh K. Channel Estimation for FSO Channels Subject to gamma-gamma Turbulence. In: Proc. International Conference on Space Optical Systems and Applications (ICSOS). Corsica; 2012.
8. Benkhelifa F, Rezki Z, Alouini MS. Low SNR capacity of FSO links over gamma-gamma atmospheric turbulence channels. *IEEE Commun Lett.* 2013;17:1264-1267.
9. García-Zambrana A, Castillo-Vázquez C, Castillo-Vázquez B. On the capacity of FSO links over gamma-gamma atmospheric turbulence channels using OOK signaling. *EURASIP Journal on Wireless Communications and Networking.* 2010;2010:64. Available: <https://jwcn-urasipjournals.springeropen.com/articles/10.1155/2010/127657>
10. Chatzidiamentis N, Karagiannidis GM. Generalized maximum-likelihood sequence detection for photon-counting free space optical systems. *IEEE Trans Commun.* 2010;58(12):3381-3385.
11. Grosshans F, Grangier P. Reverse Reconciliation Protocols for Quantum Cryptography with Continuous Variables. arXiv:quant-ph/0204127v1; 2002.
12. Van Meter R. *Quantum Networking.* New Jersey: John Wiley and Sons; 2014.
13. Van Meter R, Ladd TD, Munro WJ, Nemoto K. System design for a long-line quantum repeater. *IEEE/ACM Trans Networking.* 2009;17(3):1002-1013.
14. Van Meter R, Satoh T, Ladd TD, Munro WJ, Nemoto K. Path selection for quantum repeater networks. *Netw Sci.* 2013;3(1-4):82-95.
15. Van Meter R, Devitt SJ. Local and distributed quantum computation. *IEEE Comput.* 2016;49(9):31-42.
16. Gyongyosi L, Imre S. Decentralized base-graph routing for the quantum internet. *Phys Rev A.* 2018;98(2):22310.
17. Pirandola S, Mancini S, Lloyd S, Braunstein SL. Continuous variable quantum cryptography using two-way quantum communication. arXiv:quant-ph/0611167v3; 2008.
18. Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing; 1984; Bangalore:175-179.
19. Lim CCW, Curty M, Walenta N, Xu F, Zbinden H. Concise security bounds for practical decoy-state quantum key distributio. *Phys Rev A.* 2014;89:22307.
20. Curty M, Xu F, Cui W, Lim CCW, Tamaki K, Lo HK. Finite-key analysis for measurement-device-independent quantum key distribution. *Nat Com.* 2014;5:3732.
21. Pfister C, Lutkenhaus N, Wehner S, Coles PJ. Sifting attacks in finite-size quantum key distribution. *New J Phys.* 2016;18:53001.
22. Pirandola S, Braunstein SL, Lloyd S. Characterization of collective gaussian attacks and security of coherent-state quantum cryptography. *Phys Rev Lett.* 2008;101:200504.
23. Jouguet P, Kunz-Jacques S. High performance error correction for quantum key distribution using polar codes. arXiv:1204.5882v2; 2012.
24. Weedbrook C, Pirandola S, Garcia-Patron R, et al. Gaussian quantum information. *Rev Mod Phys.* 2012;84:621.
25. Pirandola S, Garcia-Patron R, Braunstein SL, Lloyd S. Direct and reverse secret-key capacities of a quantum channel. *Phys Rev Lett.* 2009;102:50503.
26. Lodewyck SJ, Bloch M, Garcia-Patron R, et al. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Phys Rev.* 2007;76:42305.
27. Qi B, Lim CC. Noise analysis of simultaneous quantum key distribution and classical communication scheme using a true local oscillator. 2017. arXiv:1708.08742v1 76, 042305.
28. Wu X-D, Liao Q, Huang D, Wu XH, Guo Y. Balancing four-state continuous-variable quantum key distribution with linear optics cloning machine. *Chinese Phys B.* 2017;11:101-107.
29. Ou S, Yang K, Chen H-H. Integrated dynamic bandwidth allocation in converged passive optical networks and IEEE 802.16 networks. *IEEE Syst J.* 2010;4:467-476.
30. Laurenza R, Pirandola S. General bounds for sender-receiver capacities in multipoint quantum communications. *Phys Rev A.* 2017;96:32318.
31. Qu Z, Djordjevic I. High-speed free-space optical continuous-variable quantum key distribution enabled by three-dimensional multiplexing. *Opt Express.* 2017;25(7):7919-7928.

32. Grosshans F, Van Assche G, Wenger J, Brouri R, Cerf NJ, Grangier P. Quantum key distribution using gaussian-modulated coherent states. *Nature*. 2003;421:238-241.
33. Kiktenko EO, Pozhar NO, Anufriev MN, et al. Quantum-secured blockchain. *Quantum Sci Technol*. 2018;3:35004.
34. Laudenbach F, Pacher C, Fred Fung C-H, et al. Continuous-variable quantum key distribution with gaussian modulation - the theory of pract implement. *Adv. Quantum Technol*. 2018;1(1):1-37. 1800011
35. Petz D. *Quantum Information Theory and Quantum Statistics*. Heidelberg: Springer-Verlag, Heidelberg; 2008.
36. Pirandola S. End-to-end capacities of a quantum communication network. *Commun Phys*. 2019;2:51.
37. Gyongyosi L, Imre S. A survey on quantum computing technology. *Comp Sci Rev*. 2018;31:51-71. Elsevier, ISSN: 1574-0137. <https://doi.org/10.1016/j.cosrev.2018.11.002>
38. Gyongyosi L, Imre S. Adaptive multicarrier quadrature division modulation for long-distance continuous-variable quantum key distribution. In: Proc. SPIE 9123 Quantum Information and Computation XII. Baltimore; 2014:912307.
39. Gyongyosi L, Imre S. Diversity space of multicarrier continuous-variable quantum key distribution. *Int J Commun Syst*. 2019:e4003. <https://doi.org/10.1002/dac.4003>
40. Gyongyosi L, Imre S. Gaussian quadrature inference for multicarrier continuous-variable quantum key distribution. *Quantum Studies: Mathematics and Foundations*. 2019;1:1-34. Springer Nature, ISSN: 2196-5609, ISSN: 2196-5617.
41. Gyongyosi L, Imre S. Secret key rate proof of multicarrier continuous-variable quantum key distribution. *Int J Commun Syst*. 2019;32(4):e3865.
42. Gyongyosi L, Imre S. Multiple access multicarrier continuous-variable quantum key distribution. *Chaos, Solitons Fractals*. 2018;114:491-505.
43. Gyongyosi L, Imre S. Low-dimensional reconciliation for continuous-variable quantum key distribution. *Appl Sci*. 2018;8(1):87.
44. Jouguet P, Kunz-Jacques S, Leverrier A, Grangier P, Diamanti E. Experimental demonstration of long-distance continuous-variable quantum key distribution. arXiv:1210.6216v1; 2012.
45. Navascues M, Acin A. Security bounds for continuous variables quantum key distribution. *Phys Rev Lett*. 2005;94:20505.
46. Navascues M, Grosshans F, Acin A. Optimality of Gaussian attacks in continuous-variable quantum cryptography. *Phys Rev Lett*. 2006;97:190502.
47. Weedbrook C, Pirandola S, Lloyd S, Ralph T. Quantum cryptography approaching the classical limit. *Phys Rev Lett*. 2010;105:110501.
48. Zhang H, Mao Y, Huang D, Li J, Zhang L, Guo Y. Security analysis of orthogonal-frequency-division-multiplexing-based continuous-variable quantum key distribution with imperfect modulation. *Phys Rev A*. 2018;97:52328.
49. Zhao W, Liao Q, Huang D, Guo Y. Performance analysis of the satellite-to-ground continuous-variable quantum key distribution with orthogonal frequency division multiplexed modulation. *Quant Inf Proc*. 2019;18:39.
50. Gyongyosi L. Singular value decomposition assisted multicarriercontinuous-variable quantum key distribution. *Theo Comp Sci*. 2019;1:1-29. Elsevier, <https://doi.org/10.1016/j.tcs.2019.07.029>

**How to cite this article:** Gyongyosi L, Imre S. Secret key rates of free-space optical continuous-variable quantum key distribution. *Int J Commun Syst*. 2019:e4152. <https://doi.org/10.1002/dac.4152>