Quantum Noise in Optical Communication Systems: Limitations and Opportunities

Konrad Banaszek(1), Karol Łukanowski(1), Michał Jachura(1), Marcin Jarzyna(1)

(1) Centre for Quantum Optical Technologies, CeNT, University of Warsaw, 02-097 Warszawa, Poland, k.banaszek@uw.edu.pl

Abstract *Quantum fluctuations fundamentally affect optical signal regeneration and detection. This results in ultimate quantum limits on the performance of optical communication links and enables innovative physical layer security solutions such as quantum key distribution. ©2023 The Author(s)*

Introduction

The continuing efforts to improve the performance of optical communication systems will ultimately encounter the barrier of quantum fluctuations inherently present in optical signal processing and detection. Quantum physics offers quantitative characterisation of the resulting limitations, even if conventional modulation and detection techniques are replaced by more advanced strategies enabled by emerging or future quantum technologies. This paper examines the ultimate Gordon-Holevo (GH) limit on the capacity of optical links,[1]–[4] including multispan configurations with optical amplifiers,[5]–[8] as well as reviews selected concepts of quantum key distribution (QKD),[9]–[12] where quantum fluctuations enable secure communication.

Channel model

In a canonical model shown in Fig. 1, an optical signal with average input power P and slot rate (bandwidth) B undergoes attenuation characterised by a power transmission factor τ followed by addition of excess Gaussian noise with a power spectral density (PSD) $\mathscr{N}$. It is convenient to quantify the input signal strength and the noise strength with respective PSDs expressed in photon numbers per unit time-bandwidth area:

$$\bar{n} = P/(Bhf_c), \qquad n_\mathrm{n} = \mathscr{N}/(hf_c), \tag{1}$$

where $h = 6.626 \cdot 10^{-34}\ \mathrm{J}\cdot\mathrm{Hz}^{-1}$ is Planck's constant and f_c is the signal carrier frequency. The attainable information rate R reads R $= B \cdot$ C,

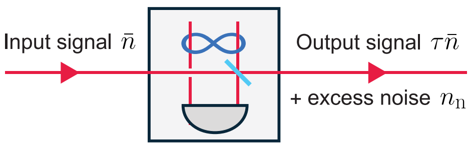

Fig. 1: Canonical channel model. The setup inside the box realizes a QKD eavesdropping strategy using an entangled twin-beam state (∞) and a receiver saturating the GH limit.

where C is the channel capacity per slot (spectral efficiency). Conventional references for the channel capacity derived from the Shannon-Hartley theorem[13] correspond to scenarios where information is encoded respectively in one (S1) or two (S2) field quadratures and read:

$$\mathrm{C}_{\mathrm{S1}} = \frac{1}{2}\log_2\left(1 + \frac{4\tau\bar{n}}{2n_\mathrm{n}+1}\right), \tag{2}$$

$$\mathrm{C}_{\mathrm{S2}} = \log_2\left(1 + \frac{\tau\bar{n}}{n_\mathrm{n}+1}\right). \tag{3}$$

It has been assumed that information-carrying quadratures are read out using coherent, shot-noise-limited (SNL) detection which contributes terms $+1$ to the denominators in (2) and (3). The Shannon capacities for a loss-only channel with no excess noise, $n_\mathrm{n} = 0$, are depicted in Fig. 2.

Gordon-Holevo capacity limit

From the quantum physics perspective, scenarios leading to the Shannon limits (2) and (3) are overly restrictive. In addition to optical fields with a well defined complex amplitude, described in quantum mechanics by so-called coherent states, one may consider also input symbols prepared in non-classical states, such as squeezed states or photon number (Fock) states.[14] Furthermore,

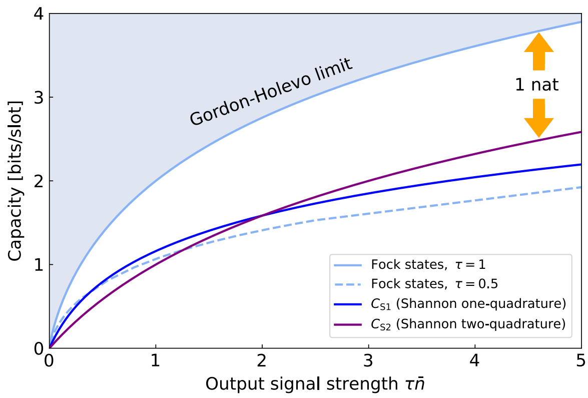

Fig. 2: Capacities for a loss-only channel.

conventional detection of field intensity or quadratures can be replaced by more elaborate receivers,[15] aiming e.g. at minimising the probability of error when discriminating the symbol values,[16]–[20] or detecting jointly multiple symbols.[21]–[23] Optimisation over all ensembles of input symbols under the average power constraint and physically feasible detection strategies yields the ultimate Gordon-Holevo (GH) capacity limit[1]–[3]

$$\mathrm{C}_{\mathrm{GH}} = g(\tau\bar{n} + n_{\mathrm{n}}) - g(n_{\mathrm{n}}), \tag{4}$$

where $g(x) = (x+1)\log_2(x+1) - x\log_2 x$. Because $g(0) = 0$, the expression $g(\tau\bar{n})$ gives the GH limit of a loss-only channel, indicated in Fig. 2 by the edge of the shaded region. For large arguments, $x \gg 1$, the function $g(x)$ admits the expansion $g(x) = \log_2(1+x) + \log_2 \mathrm{e} + O(x^{-1})$, which implies that in the case of a loss-only channel with a strong output signal one has

$$\mathrm{C}_{\mathrm{GH}} \approx \mathrm{C}_{\mathrm{S2}} + \log_2 \mathrm{e}, \qquad \tau\bar{n} \gg 1,\ n_{\mathrm{n}} = 0, \tag{5}$$

which gives the quantum advantage equal to 1 nat ≈ 1.44 bit of information per slot. In the special case of a lossless and noiseless channel the GH limit can be saturated by encoding information in Fock states and using at the output photon number resolved detection that identifies unambiguously the input state. As seen in Fig. 2, this strategy no longer works for a lossy channel.[24]

When the excess noise is strong, $n_{\mathrm{n}} \gg 1$, the large-argument expansion of $g(x)$ can be applied to both terms in Eq. (4) which gives:

$$\mathrm{C}_{\mathrm{GH}} \approx \mathrm{C}_{\mathrm{S2}} \approx \log_2\left(1 + \frac{P}{B\mathscr{N}}\right), \qquad n_{\mathrm{n}} \gg 1. \tag{6}$$

In the second step the detection shot noise has been neglected compared to the excess noise, which yields the standard Shannon expression for the capacity of a noisy Gaussian channel.

Under severe power limitations the photon starved regime with $\tau\bar{n} \ll 1$ is reached. Taking $\tau\bar{n} \to 0$ one obtains $\mathrm{C}_{\mathrm{GH}} \approx \tau\bar{n}\log_2(1 + n_{\mathrm{n}}^{-1})$. The resulting information rate can be recast as

$$\mathrm{R}_{\mathrm{GH}} \approx \frac{\tau P}{h f_c} \cdot \log_2\left(1 + \frac{h f_c}{\mathscr{N}}\right), \qquad \tau\bar{n} \to 0, \tag{7}$$

where the first factor specifies the received photon flux, and the second factor is the GH limit on the photon information efficiency (PIE). With vanishing excess noise, $\mathscr{N} \to 0$, the PIE can take in principle an arbitrarily high value.[25],[26] A generic example of a scalable photon-efficient modulation format is pulse position modulation (PPM).[27]

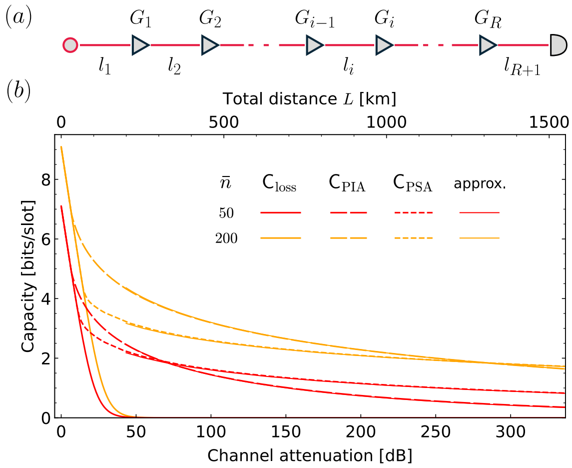

Fig. 3: A multispan link with optical signal regeneration (a); Optimized GH capacity limits for distributed amplification (b).

Amplified multispan links

Consider a link consisting of $R+1$ spans that connect R regeneration nodes as shown in Fig. 3(a). If the optical signal is regenerated at the ith node using a phase-insensitive amplifier (PIA) with gain G_i, at least $G_i - 1$ noise photons have to be contributed by the amplification process.[28] When PIAs operate at the quantum limit, this leads to the following recursive relations for the channel transmission τ_i and the excess noise $n_{\mathrm{n},i}$ up to the point right after the ith node:[7]

$$\begin{aligned} \tau_i &= G_i \exp(-\alpha l_i)\tau_{i-1}, \\ n_{\mathrm{n},i} &= G_i \exp(-\alpha l_i) n_{\mathrm{n},i-1} + G_i - 1. \end{aligned} \tag{8}$$

Here l_i is the length of the ith span and α is the attenuation per unit length. A natural constraint is that the combined signal and noise power does not exceed the input value $\bar{n}$ at any point of the link, $\tau_i\bar{n} + n_{\mathrm{n},i} \leq \bar{n}$.

Fig. 3(b) depicts the optimized GH limit on the link capacity as a function of distance in the case of distributed amplification, $l_i \to 0$. Apart from short distances, where the 1 nat quantum advantage for a loss-only channel prevails over regeneration, the optimal strategy is to keep the signal amplified to the maximum value permitted by the total power constraint for most of the distance. For short span lengths, $\alpha l_i \ll 1$, and high powers, $\bar{n} \gg 1$, the requirement to maintain the total power implies the gain $G_i \approx 1 + \alpha l_i(\bar{n} - 1)/\bar{n}$. Inserting this value into Eqs. (8) and taking the limit of distributed amplification gives the solution over the link distance L of the form: $\tau = \exp(-\alpha L/\bar{n})$,

$n_{\mathrm{n}} = (1-\tau)\bar{n}$. As soon as the excess noise contributed by amplification overwhelms the shot noise, $n_{\mathrm{n}} \gg 1$, it becomes sufficient to use the Shannon limit (3), which after simplification yields

$$\mathsf{C}_{\mathrm{PIA}} \approx -\log_2\big(1-\exp(-\alpha L/\bar{n})\big). \tag{9}$$

It is seen that the decrease of capacity with distance is reduced by a factor $1/\bar{n}$.

An analogous analysis can be carried out[8] in the case of a multispan link with phase-sensitive amplifiers (PSAs).[29] For large distances the nearly optimal strategy is to modulate one field quadrature, subject it to amplification to bring the combined signal and noise power back to the input value, and coherently detect the information-carrying quadrature. In the limit of distributed amplification the capacity is well approximated by

$$\mathsf{C}_{\mathrm{PSA}} \approx -\frac{1}{2}\log_2\big(1-\exp[-\alpha L/(4\bar{n})]\big). \tag{10}$$

Although the capacity is reduced by an overall factor $1/2$, its decrease with distance is slower by an additional factor 4 in the exponent compared to Eq. (9) which prevails for very long links as seen in Fig. 3.

Quantum key distribution

The purpose of quantum key distribution (QKD)[10]–[12] is to generate a secure key between two parties: the sender (Alice) and the recipient (Bob), that will be unknown to an adversary (Eve) that can access the channel or even replace the actual physical channel with an elaborate eavesdropping mechanism. The key can be distilled from partly correlated random variables in possession of Alice and Bob, provided that Eve has less knowledge about Alice's variable (direct reconciliation) or Bob's variable (reverse reconciliation) than the mutual knowledge between Alice and Bob. Asymptotically the knowledge is quantified in terms of mutual information $\mathsf{I}(\cdot;\cdot)$.

An exemplary QKD protocol is Alice modulating the complex field amplitude composed of two conjugate quadratures according to a phase-invariant Gaussian distribution $\mathcal{CN}(0,\bar{n})$. For a loss-only channel and conventional SNL detection of both quadratures by Bob, their mutual information reads $\mathsf{I}(A;B) = \log_2(1+\tau\bar{n})$. If Eve has access to the entire fraction $1-\tau$ of the signal that is not received by Bob, her maximum knowledge about Alice's variable is given by the GH limit, $\mathsf{I}(A;E) = g\big((1-\tau)\bar{n}\big)$. Consequently, the channel transmission threshold to distill a secure key by Alice and Bob exceeds 50%. However, Eve has less knowledge about Bob's outcomes, $\mathsf{I}(B;E) = g\big((1-\tau)\bar{n}\big) - g\big((1-\tau)\bar{n}/(1+\tau\bar{n})\big)$, which enables key generation below that threshold in the reverse reconciliation scenario.[9] For strong input signal, $\bar{n} \gg 1$, and high attenuation, $\tau \ll 1$, assuming perfect reconciliation the attainable key scales linearly with channel transmission:

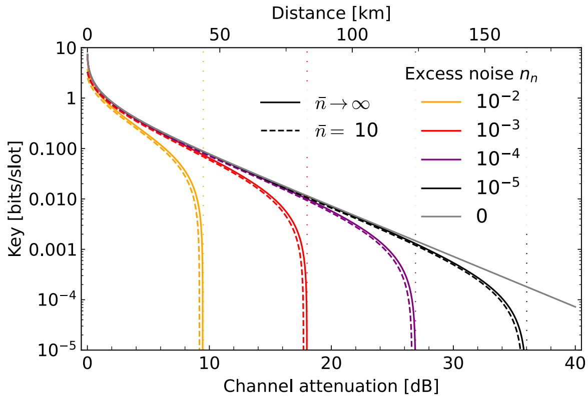

Fig. 4: Secure key as a function of channel transmission.

$$\mathsf{K} = \mathsf{I}(A;B) - \mathsf{I}(B;E) \approx \frac{\tau}{2}\log_2 \mathrm{e}. \tag{11}$$

In the most pessimistic scenario, the physical channel is replaced by Eve with a quantum processor, as illustrated with Fig. 1, and the security analysis assumes the optimal eavesdropping strategy compatible with the effective channel characteristics observed by Alice and Bob. As shown in Fig. 4, the result for passive eavesdropping on a loss-only channel holds for transmissions down to a cut-off value that depends on the excess noise contribution.

Conclusions

Quantum physics indicates multifold ways to boost the performance of optical communication systems and equip them with extra functionalities, such as physical layer security. These enhancements depend essentially on reaching quantum-limited operation of optoelectronic components and implementing advanced signal processing strategies, especially in the optical domain.

Acknowledgements

We thank R.-J. Essiambre, N. Fabre, M. Notarnicola, and our collaborators for insightful discussions. This work was supported by the project “Quantum Optical Technologies” carried out under the International Research Agendas Programme of the Foundation for Polish Science co-financed by the European Union through the European Regional Development Fund.

References

[1] J. P. Gordon, "Quantum effects in communications systems", *Proc. IRE*, vol. 50, pp. 1898–1908, 1962. DOI: 10.1109/JRPROC.1962.288169.

[2] A. S. Holevo, "The capacity of the quantum channel with general signal states", *IEEE Trans. Inf. Theory*, vol. 44, pp. 269–273, 1998. DOI: 10.1109/18.651037.

[3] V. Giovannetti, R. García-Patrón, N. J. Cerf, and A. S. Holevo, "Ultimate classical communication rates of quantum optical channels", *Nature Photon.*, vol. 8, pp. 796–800, 2014. DOI: 10.1038/nphoton.2014.216.

[4] K. Banaszek, L. Kunz, M. Jachura, and M. Jarzyna, "Quantum limits in optical communications", *J. Lightwave Technol.*, vol. 38, pp. 2741–2754, 2020. DOI: 10.1109/JLT.2020.2973890.

[5] A. Yariv, "Signal-to-noise considerations in fiber links with periodic or distributed optical amplification", *Opt. Lett.*, vol. 15, pp. 1064–1066, 1990. DOI: 10.1364/OL.15.001064.

[6] C. Antonelli, A. Mecozzi, M. Shtaif, and P. J. Winzer, "Quantum limits on the energy consumption of optical transmission systems", *Journal of Lightwave Technology*, vol. 32, no. 10, pp. 1853–1860, 2014. DOI: 10.1109/JLT.2014.2309721.

[7] M. Jarzyna, R. Garcia-Patron, and K. Banaszek, "Ultimate capacity limit of a multi-span link wirth phase-insensitive amplification", in *45th European Conference on Optical Communication*, Dublin, Ireland, 2019. DOI: 10.1049/cp.2019.0742.

[8] K. Łukanowski, K. Banaszek, and M. Jarzyna, "Quantum limits on the capacity of multispan links with phase-sensitive amplification", *J. Lightwave Technol.*, pp. 1–9, 2023. DOI: 10.1109/JLT.2023.3256585.

[9] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, "Continuous variable quantum cryptography: Beating the 3 dB loss limit", *Phys. Rev. Lett.*, vol. 89, p. 167 901, 2002. DOI: 10.1103/PhysRevLett.89.167901.

[10] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Du šek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution", *Rev. Mod. Phys.*, vol. 81, pp. 1301–1350, 2009. DOI: 10.1103/RevModPhys.81.1301.

[11] F. Laudenbach, C. Pacher, C.-H. F. Fung, *et al.*, "Continuous-variable quantum key distribution with gaussian modulation-the theory of practical implementations", *Advanced Quantum Technologies*, vol. 1, p. 1 800 011, 2018. DOI: 10.1002/qute.201800011.

[12] S. Pirandola, U. L. Andersen, L. Banchi, *et al.*, "Advances in quantum cryptography", *Adv. Opt. Photon.*, vol. 12, pp. 1012–1236, 2020. DOI: 10.1364/AOP.361502.

[13] C. E. Shannon, "A mathematical theory of communication", *Bell System Technical Journal*, vol. 27, pp. 379–423, 623–656, 1948.

[14] C. Gerry and P. Knight, *Introductory Quantum Optics*. Cambridge University Press, 2004. DOI: 10.1017/CBO9780511791239.

[15] I. A. Burenkov, M. V. Jabir, and S. V. Polyakov, "Practical quantum-enhanced receivers for classical communication", *AVS Quantum Science*, vol. 3, p. 025 301, 2021. DOI: 10.1116/5.0036959.

[16] R. L. Cook, P. J. Martin, and J. M. Geremia, "Optical coherent state discrimination using a closed-loop quantum measurement", *Nature*, vol. 446, pp. 774–777, 2007. DOI: 10.1038/nature05655.

[17] K. Tsujino, D. Fukuda, G. Fujii, *et al.*, "Quantum receiver beyond the standard quantum limit of coherent optical communication", *Phys. Rev. Lett.*, vol. 106, p. 250 503, 2011. DOI: 10.1103/PhysRevLett.106.250503.

[18] C. R. Müller, M. A. Usuga, C. Wittmann, *et al.*, "Quadrature phase shift keying coherent state discrimination via a hybrid receiver", *New Journal of Physics*, vol. 14, no. 8, p. 083 009, Aug. 2012. DOI: 10.1088/1367-2630/14/8/083009.

[19] F. E. Becerra, J. Fan, and A. Migdall, "Photon number resolution enables quantum receiver for realistic coherent optical communications", *Nature Photonics*, vol. 9, pp. 48–53, 2015. DOI: 10.1038/nphoton.2014.280.

[20] M. T. DiMario, L. Kunz, K. Banaszek, and F. E. Becerra, "Optimized communication strategies with binary coherent states over phase noise channels", *npj Quantum Information*, vol. 5, no. 1, Jul. 2019. DOI: 10.1038/s41534-019-0177-4.

[21] S. Guha, "Structured optical receivers to attain superadditive capacity and the Holevo limit", *Phys. Rev. Lett.*, vol. 106, p. 240 502, 2011. DOI: 10.1103/PhysRevLett.106.240502.

[22] M. M. Wilde, S. Guha, S.-H. Tan, and S. Lloyd, "Explicit capacity-achieving receivers for optical communication and quantum reading", in *2012 IEEE International Symposium on Information Theory Proceedings*, 2012, pp. 551–555. DOI: 10.1109/ISIT.2012.6284251.

[23] K. Banaszek and M. Jachura, "Structured optical receivers for efficient deep-space communication", in *2017 IEEE International Conference on Space Optical Systems and Applications (ICSOS)*, 2017, pp. 34–37. DOI: 10.1109/ICSOS.2017.8357208.

[24] K. Łukanowski and M. Jarzyna, "Capacity of a lossy photon channel with direct detection", *IEEE Trans. Commun.*, vol. 69, pp. 5059–5068, 2021. DOI: 10.1109/TCOMM.2021.3075714.

[25] M. Jarzyna, "Classical capacity per unit cost for quantum channels", *Phys. Rev. A*, vol. 96, p. 032 340, 2017. DOI: 10.1103/PhysRevA.96.032340.

[26] K. Banaszek, L. Kunz, M. Jarzyna, and M. Jachura, "Approaching the ultimate capacity limit in deep-space optical communication", in *Free-Space Laser Communications XXXI*, H. Hemmati and D. M. Boroson, Eds., SPIE, Mar. 2019. DOI: 10.1117/12.2506963.

[27] M. Jarzyna, P. Kuszaj, and K. Banaszek, "Incoherent on-off keying with classical and non-classical light", *Opt. Express*, vol. 23, no. 3, pp. 3170–3175, 2015. DOI: 10.1364/OE.23.003170.

[28] C. M. Caves, "Quantum limits on noise in linear amplifiers", *Phys. Rev. D*, vol. 26, pp. 1817–1839, Oct. 1982. DOI: 10.1103/PhysRevD.26.1817.

[29] S. L. I. Olsson, H. Eliasson, E. Astra, M. Karlsson, and P. A. Andrekson, "Long-haul optical transmission link using low-noise phase-sensitive amplifiers", *Nature Communications*, vol. 9, p. 2513, 2018. DOI: 10.1038/s41467-018-04956-5.