

Fundamental Limits on Quantum Bit Error Rate and Distance in Quantum Key Distribution

Stefano Pirandola Department of Computer Science, *University of York*, York YO10 5GH, United Kingdom

(Received 22 February 2026; revised 26 May 2026; accepted 6 August 2026; published 9 September 2026)

Quantum key distribution (QKD) enables information-theoretic secure communication, yet its ultimate tolerance to noise and achievable transmission distance remain fundamentally constrained. We establish the maximum quantum bit error rate (QBER) compatible with secure QKD and derive corresponding upper bounds on communication distance. Our results follow from a fundamental capacity threshold for qubit Pauli channels and apply to protocols based on two or more mutually unbiased bases, using either single-photon or weak coherent sources. By connecting information-theoretic limits to realistic physical noise models, we obtain universal bounds on achievable distances in fiber and free-space links, including diffraction-limited constraints relevant to deep-space quantum communications. These findings clarify the ultimate noise robustness of QKD and delineate the fundamental boundaries of secure quantum communication.

DOI: [10.1103/3bgy-tpy9](https://doi.org/10.1103/3bgy-tpy9)

Introduction—Quantum key distribution (QKD) [1–3] is one of the most mature quantum technologies, currently being deployed in both research and industrial settings. Yet, QKD is affected by fundamental rate-loss limitations [4,5] which require the use of intermediate repeater stations to form chains or networks of nodes, which may be trusted or untrusted [6–10]. The Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound [5] establishes that $-\log_2(1 - \eta)$ is the maximum possible number of key bits per channel use that can be extracted over a lossy channel with transmissivity η . While this provides the maximum key rate achievable in repeaterless QKD, it does not directly impose a bound on the maximum quantum bit error rate (QBER) that is tolerable by discrete-variable (DV) protocols. This is the main result of this Letter.

We begin by establishing a necessary and sufficient condition under which all two-way assisted capacities of the qubit Pauli channel are strictly positive. Building on this result, we then derive the threshold QBER values required to guarantee the security of a DV-QKD protocol employing either two or three mutually unbiased bases (MUBs). Next, we adopt a standard noise model that relates the QBER to the channel transmissivity and other relevant system parameters. Exploiting this relationship, we translate the QBER threshold conditions into bounds on the maximum transmission distance achievable by DV-QKD protocols

over fiber-based and free-space links. Finally, we extend our analysis from the repeaterless setting to repeater-assisted protocols.

Our investigation not only establishes the fundamental limits of noise robustness for DV-QKD, but also reveals gaps in the existing literature. In particular, we identify the possibility of undiscovered DV-QKD protocols capable of tolerating higher QBERs than those currently known. Furthermore, we show that diffraction-limited free-space implementations can achieve exceptionally long transmission distances, thereby supporting the feasibility of deep-space quantum communications.

Quantum channels in DV-QKD—In DV-QKD protocols, such as the BB84 protocol [1], there are two quantum channels involved, one affecting the system carrier (e.g., a photon or a photon pulse) and the other affecting the degree of freedom that is used for encoding and decoding (e.g., the polarization qubit). The first quantum channel is a bosonic lossy channel that transmits photons with probability η , referred to as the channel transmissivity. The second channel is a qubit Pauli channel. The lossy channel determines the detection rate, while the Pauli channel sets the QBER. Together, they determine the final secret key rate.

A qubit Pauli channel $\mathcal{P}$ acts on a state ρ as follows:

$$\mathcal{P}(\rho) = \sum_{k=0}^3 p_k P_k \rho P_k^\dagger, \quad (1)$$

where $\mathbf{p} := \{p_k\}$ is a probability distribution associated with the Pauli operators $P_k \in \{I, X, Y, Z\}$. Explicitly,

Published by the American Physical Society under the terms of the [Creative Commons Attribution 4.0 International](https://creativecommons.org/licenses/by/4.0/) license. Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad (2)$$

with I being the 2×2 identity matrix.

The Pauli error probabilities can be connected with the values of the QBERs in the encoding bases. If the security of the QKD protocol is based on two MUBs, such as X and Z of the BB84 protocol, we have that the corresponding QBERs, known as bit error rate E_X and phase error rate E_Z , satisfy

$$E_X = p_2 + p_3, \quad E_Z = p_1 + p_2. \quad (3)$$

If the security of the QKD protocol is based on three MUBs, X , Z , and Y , as in the six-state protocol [2], then the associated QBERs satisfy Eq. (3) and the additional relation $E_Y = p_1 + p_3$.

There are some relevant specific examples of Pauli channels. One is the bit-and-phase-flip (BPF) channel corresponding to the case with $p_2 = 0$. Since this channel only induces X and Z errors, it is the simplest model compatible with QKD protocols based on two MUBs. Another relevant channel is the depolarizing one, which is a Pauli channel with equal errors in the three bases. This is typically parametrized as follows:

$$\mathbf{p} = \left\{ 1 - \frac{3p}{4}, \frac{p}{4}, \frac{p}{4}, \frac{p}{4} \right\}, \quad (4)$$

and its action on a qubit state ρ reduces to

$$\mathcal{P}_{\text{depol}}(\rho) = (1 - p)\rho + p \frac{I}{2}. \quad (5)$$

Capacity thresholds—Reference [5] established the ultimate rates for entanglement distribution, quantum information transmission, and QKD in the absence of an intermediate relay. For specific channels, such as the bosonic lossy channel, the bosonic quantum-limited amplifier, and the dephasing and erasure channels, Ref. [5] derived the exact analytical expressions of the two-way assisted entanglement distribution capacity D_2 , the two-way assisted quantum capacity Q_2 , and the two-way assisted secret-key capacity K_2 , showing that these capacities coincide for these channels. Reference [5] also provided lower and upper bounds for the two-way assisted capacities of the Pauli, amplitude damping, and thermal-loss channels.

Let us call $\mathcal{C}_2$ the generic two-way assisted capacity. Depending on the context, this can be D_2 , Q_2 , or K_2 . As a direct consequence of Ref. [5], one obtains equivalent criteria for a quantum channel to satisfy $\mathcal{C}_2 = 0$. For a qubit Pauli channel, we show that

$$\mathcal{C}_2(\mathcal{P}) = 0 \Leftrightarrow p_{\max} := \max\{p_k\} \leq \frac{1}{2}, \quad (6)$$

and, for a depolarizing channel, we therefore have

$$\mathcal{C}_2(\mathcal{P}_{\text{depol}}) = 0 \Leftrightarrow p \geq \frac{2}{3}. \quad (7)$$

The proof in [11] relies on the fact that the two-qubit Choi state of a qubit Pauli channel has nonpositive partial transposition (NPT) [18,19]. Note that this simple proof cannot be extended to higher dimensions since, already for qutrits (3×3), there is bound entanglement. In [11], we also justify the reduction to a Pauli channel, rather than considering a fully general qubit channel, by showing that it represents the worst-case quantum channel compatible with the observed matched-basis QBERs.

Maximum tolerable QBER—We now exploit Eq. (6) to establish the maximum tolerable QBER in repeaterless QKD. Let us start by considering QKD protocols that are based on two MUBs, with observed QBERs E_X and E_Z . As the values of these QBERs gradually increase, the probability of the identity Pauli “error” $p_0 = 1 - (E_X + E_Z) + p_2$ gradually decreases. Also, because the values of the QBERs increase from zero, we have that $p_0 = p_{\max}$. According to Eq. (6), we find that QKD is possible as long as $E_X + E_Z < 1/2 + p_2$. In the worst-case scenario, Eve does not introduce Y errors ($p_2 = 0$), so we have a BPF channel and the maximum QBER is bounded as follows:

$$E_X + E_Z < 1/2. \quad (8)$$

If this inequality is satisfied, then there certainly exists a QKD protocol with a positive key rate. If this is violated, the key rate is certainly zero for any QKD protocol.

Assuming the symmetric condition $E_X = E_Z := E$, we see that Eq. (8) becomes $E < 1/4$. It is interesting to note that this threshold coincides with the QBER induced by an intercept-resend attack against the BB84 protocol. While it may be intuitive to understand that security is not possible above $1/4$, it is less obvious to recognize that a QKD protocol (with suitable data processing) exists with a positive key rate up to $E = 1/4$. Previous studies [20] have identified that BB84 can be made secure up to $E = 18.9\%$ with suitable two-way data processing, and more recently up to $E = 20\%$ [21]. Thus, our result raises the question of identifying a more powerful mechanism (protocol and/or data processing) able to effectively outperform $E = 20\%$ and approach the $1/4$ upper bound limit in the symmetric scenario. Note that this limit applies to single-qubit BB84-like protocols, where the QBER is tested directly on the transmitted qubits, and does not necessarily apply to encoded variants with filtering or postselection [22].

Now consider QKD protocols based on three MUBs, with observed QBERs E_X , E_Z and E_Y . In this case, we repeat the previous reasoning to obtain $p_{\max} = p_0 = 1 - (E_X + E_Z + E_Y)/2$. Therefore, Eq. (6) leads to

$$E_X + E_Z + E_Y < 1. \quad (9)$$

Assuming symmetry $E_X = E_Z = E_Y := E$, we have $E < 1/3$. No QKD protocol based on three MUBs can be secure above this value in symmetric conditions. In fact, one can show that this corresponds to the threshold for an intercept-resend attack. As before, the less obvious point is that this result guarantees the existence of a QKD protocol based on three MUBs able to achieve a positive key rate up to $E = 1/3$. We know that the six-state protocol combined with two-way processing can achieve a QBER of 26.4% [20] and, more recently, the performance was extended to 27.6% [21] and 30% [22]. So it is another open question to discover a more powerful 3-MUB protocol (and/or data processing method) able to exceed $E = 30\%$ and reach $1/3$. More precisely, the threshold $E < 1/3$ can be approached by entanglement-distillation methods requiring a quantum memory [22]. It remains an open question whether the same limit can be saturated by a prepare-and-measure implementation.

Noise model for QBER in DV-QKD—The QBER of a QKD protocol can be related to the total transmissivity η of the lossy channel connecting Alice and Bob. This relation allows one to translate the maximum tolerable QBER into a maximum achievable transmission distance. The exact translation depends on the noise model valid for the QBER, as we discuss below.

Consider the QBER E associated with a generic MUB (X , Z or Y). We can write the minimum value of E compatible with the transmissivity η and the relevant parameters of Alice's source and Bob's detectors. This "irreducible" QBER represents the inevitable error rate arising from loss and device imperfections, and therefore lower bounds any observed QBER. Within the standard adversarial framework of QKD, all such noise is conservatively attributed to Eve and must be treated as channel noise associated with her perturbation of the systems.

Assume that Bob's detector has dark count probability Y_0 and misalignment error probability e_{det} , then the irreducible QBER has the form

$$E = \frac{\gamma e_{\text{det}} + (1 - \gamma)Y_0/2}{\gamma + (1 - \gamma)Y_0}, \quad (10)$$

where the analytical form of $\gamma = \gamma(\eta)$ depends on Alice's source. For a k -photon source, we may write $\gamma(\eta) = 1 - (1 - \eta)^k$, while for an attenuated coherent-state source with intensity μ , we have $\gamma(\eta) = 1 - e^{-\eta\mu}$.

For a decoy-state QKD protocol [23–27] with intensities μ_i and corresponding probabilities q_i , we can identify the intensity $\mu \in \{\mu_i\}$ associated with the best-case QBER. This QBER takes the form E_μ given by the right-hand side of Eq. (10) with $\gamma(\eta) = 1 - e^{-\eta\mu}$. Then, the overall QBER of the protocol E is lower bounded by E_μ . See [11] for more details on QBER modeling.

Maximum distance—By combining the noise models of the previous section with the results on the maximum QBERs, we can bound the maximum distance achievable by QKD protocols under various assumptions. We consider the symmetric scenario where the QBERs associated with the different MUBs are equal to some common value E . This assumption can always be seen as a best-case scenario. In fact, if the QBERs differ, we can take their minimum $E = \min\{E_Z, E_X, \dots\}$ as a common value, thereby resulting in an upper bound on the maximum distance. Thus, our next results will provide distances beyond which QKD protocols are certainly not secure.

For a 2-MUB protocol, we can combine Eq. (10) with the symmetric threshold $E < 1/4$ to get the bound

$$\gamma(\eta) > \Gamma_2 := \frac{Y_0}{1 + Y_0 - 4e_{\text{det}}} \simeq Y_0. \quad (11)$$

Then, for a 3-MUB protocol, the previous formula in Eq. (11) is slightly modified into the following:

$$\gamma(\eta) > \Gamma_3 := \frac{Y_0}{2 + Y_0 - 6e_{\text{det}}} \simeq Y_0/2. \quad (12)$$

Let us set $\Gamma = \Gamma_2$ or Γ_3 depending if we consider 2- or 3-MUB protocols. Then, for a single-photon implementation ($\gamma = \eta$), the bounds can compactly be written as $\eta > \Gamma$. For a practical implementation with an attenuated source of intensity μ (or a decoy-state implementation with best-case intensity μ), we instead have

$$\eta > -\frac{1}{\mu} \ln(1 - \Gamma). \quad (13)$$

The previous lower bounds for the transmissivity η can be written in terms of upper bounds for the distance d between Alice and Bob. First, we notice that we may decompose $\eta = \eta_{\text{eff}}\eta_{\text{ch}}$, where η_{eff} is the setup efficiency, i.e., the product of the transmissivities of Alice's and Bob's setups, while η_{ch} is the actual channel transmissivity, depending on the distance. In a fiber-based implementation, the fiber distance d can be computed assuming a loss-rate α in dB/km, using $\eta_{\text{ch}}(d) = 10^{-\alpha d/10}$. Therefore, by using $\gamma = \gamma[\eta_{\text{eff}}\eta_{\text{ch}}(d)]$ in Eqs. (11) or (12), we can bound the maximum distance achievable in fiber by repeaterless DV-QKD protocols. We may write

$$d < -\frac{10}{\alpha} \log_{10} \Omega, \quad \Omega := \begin{cases} \Gamma/\eta_{\text{eff}} & \text{1-photon,} \\ -\frac{\ln(1-\Gamma)}{\eta_{\text{eff}}\mu} & \text{attenuated.} \end{cases} \quad (14)$$

We can now derive numerical results. We assume high efficiency $\eta_{\text{eff}} = 0.9$, low-loss fiber $\alpha = 0.17$ dB/km, low dark counts 10^{-8} (compatible with SNSPD detectors), and low misalignment error $e_{\text{det}} = 1\%$. We find the results in Table I, which represent distances beyond which no key can

TABLE I. Examples of maximum fiber distance for various protocols (see text for the parameters used).

2-MUB		3-MUB	
1 photon	$\mu = 0.3$	1 photon	$\mu = 0.3$
466 km	436 km	484 km	454 km

be extracted (for the chosen parameters). Note that the current distance records for repeaterless QKD experiments are not far from these values [28].

It is interesting to note how the maximum distance depends on the dark counts, as shown in Fig. 1. Because $Y_0 \ll 1$, we have the approximations in Eqs. (11) or (12). For single-photon protocols, this means $d \simeq -\log_{10} Y_0$.

Maximum free-space distance—In free space, optical links are more generally described as fading channels, since pointing errors and large-scale turbulence induce random beam wandering across the receiver aperture [29–31]. For our upper bound, we ignore the fading process and consider the maximum transmissivity of the free-space link. Its value is determined by diffraction, small-scale turbulence, and atmospheric absorption. In general, we may decompose $\eta_{\text{ch}} = \eta_{\text{fs}}\eta_{\text{atm}}$.

On the ground, the atmospheric component can be modeled by the Beer-Lambert extinction equation

$$\eta_{\text{atm}}(d) = \exp[-\alpha(h)d], \quad (15)$$

where d is the horizontal path length in the atmosphere, and $\alpha(h)$ is the extinction factor at the altitude h [32–34]. A good approximation valid for the optical wavelength of $\lambda = 800$ nm at near sealevel is $\alpha(h) = \alpha_0 \exp(-h/H)$, where $\alpha_0 \simeq 5 \times 10^{-3} \text{ km}^{-1}$ and $H = 6.6 \text{ km}$ [29,35]. For a satellite link, the atmospheric extinction varies with the altitude. For a satellite at slant distance $d = d(h, \theta)$, where

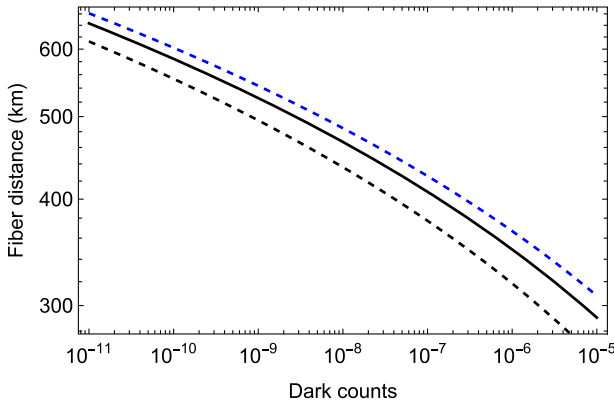


FIG. 1. Maximum fiber-distance in km versus dark count probability for a 2-MUB protocol with a single-photon source (solid black line), an attenuated source with intensity $\mu = 0.3$ (dashed black line), and intensity $\mu = 2$ (dashed blue line). We assume $\eta_{\text{eff}} = 0.9$, $\alpha = 0.17 \text{ dB/km}$, and $e_{\text{det}} = 1\%$.

h is the altitude and $\theta \leq 1$ is the zenith angle, we can write $\eta_{\text{atm}}(d) \simeq [\eta_{\text{atm}}^{\text{zen}}(h)]^{\sec(\theta)}$, where $\eta_{\text{atm}}^{\text{zen}}$ is the transmissivity at the zenith position. For $h > 30 \text{ km}$, we can approximate $\eta_{\text{atm}}^{\text{zen}} \simeq 0.967$ at $\lambda = 800 \text{ nm}$ [30].

The free-space component η_{fs} is associated with beam waist broadening induced by diffraction and small-scale turbulence (inner-scale turbulence effects). Approximate analytical formulas can be written for weak and strong regimes of turbulence, while the intermediate behavior can only be explored numerically [36,37]. Starting from the adopted turbulence model, one can write or numerically evaluate the spot size of the beam at distance d and compute $\eta_{\text{fs}}(d)$. Then, by using $\gamma = \gamma[\eta_{\text{eff}}\eta_{\text{fs}}(d)\eta_{\text{atm}}(d)]$ in Eqs. (11) or (12), we can bound the maximum distance for free-space QKD, which can be applied to ground-based or ground-satellite implementations.

Here, we derive an upper bound which only accounts for diffraction (extension to turbulence is discussed in [11]). This bound applies to all free-space implementations, but is specifically meaningful for deep-space communications. This diffraction-limited bound can be derived by using $\eta_{\text{atm}}(d) \leq 1$ and

$$\eta_{\text{fs}}(d) \leq \eta_{\text{diff}}(d) = 1 - e^{-2a_R^2/w_d^2} \simeq \frac{2a_R^2}{w_d^2}, \quad (16)$$

where a_R is the radius of the receiver circular aperture, and w_d is the beam spot size at distance d . We have

$$w_d^2 = w_0^2 \left[(1 - d/R_0)^2 + (d/d_R)^2 \right] \geq w_0^2 (d/d_R)^2, \quad (17)$$

where w_0 is the field spot size of the Gaussian beam generated by Alice, with carrier wavelength λ and curvature R_0 , while $d_R := \pi w_0^2 \lambda^{-1}$ is the Rayleigh range [38–41]. In this way, we get the following diffraction-limited upper bound for the maximum QKD distance

$$d < \frac{\pi w_0 a_R}{\lambda} \sqrt{\frac{2}{\Omega'}}, \quad \Omega' := -\ln(1 - \Omega) \simeq \Omega, \quad (18)$$

where Ω takes the expressions in Eq. (14), depending on the use of single-photon or attenuated QKD sources.

Let us investigate the limits induced by this bound assuming $\eta_{\text{eff}} = 0.9$, $Y_0 = 10^{-8}$ and $e_{\text{det}} = 1\%$ as before. Consider Alice sending a collimated Gaussian beam ($R_0 = +\infty$) of wavelength $\lambda = 800 \text{ nm}$ and waist $w_0 = 30 \text{ cm}$, and Bob using an aperture of radius $a_R = 10 \text{ cm}$. Adopting a single-photon 2-MUB protocol, we get $d < 1.54 \times 10^6 \text{ km}$, compatible with the distance of the James Webb Space Telescope (at the Sun-Earth L2 Lagrange point). As discussed in [11], this diffraction-limited bound is also an excellent approximation in the presence of turbulence when we consider the downlink. By

contrast, in uplink, the effect of turbulence is nonnegligible, and the distance is reduced by 1 order of magnitude.

Repeater-based protocols—In order to extend the results to repeater-based protocols, we can leverage Ref. [42]. Let us assume that Alice and Bob are connected by N repeaters, so we have $N + 1$ links. Each link i induces a lossy channel and a Pauli channel $\mathcal{P}_i$. For each $\mathcal{P}_i$ with probabilities $\{p_k^i\}$, we consider $p_{\max}^i = \max_k p_k^i$. For the entire sequence of Pauli channels $\{\mathcal{P}_i\}$, we take the bottleneck value $p_{\max}^{\min} := \min_i p_{\max}^i$. As briefly explained in [11], the end-to-end two-way assisted capacity of the repeater chain $\mathcal{C}_2(\{\mathcal{P}_i\})$ satisfies

$$p_{\max}^{\min} \leq 1/2 \Rightarrow \mathcal{C}_2(\{\mathcal{P}_i\}) = 0. \quad (19)$$

As before, this condition can be translated into a threshold for the maximum QBER. If each link on the chain implements a 2-MUB protocol with QBERs E_Z^i and E_X^i , we must have

$$\max_i \{E_X^i + E_Z^i\} < 1/2. \quad (20)$$

If this threshold is violated, then no key rate can be extracted. However, since the converse implication in Eq. (19) does not hold, we cannot assert the existence of a repeater-based protocol that achieves a positive key rate when the total QBER approaches $1/2$. An analogous situation arises if the chain implements 3-MUB protocols, in which case the corresponding bound would be written as $\max_i \{E_X^i + E_Z^i + E_Y^i\} < 1$.

Finally, these results admit a straightforward interpretation in terms of maximum transmission distance. In particular, the distance constraint identified for the repeaterless configuration also governs the longest individual segment within a repeater chain.

Conclusions—In this Letter, we established the maximum tolerable QBER for DV-QKD protocols and bounded their maximum distance in both fiber-based and free-space implementations. We considered protocols based on two or more MUBs, and whose implementation employs either single-photon or weak coherent (attenuated) sources. While we derived the main results for the repeaterless configuration, we also showed that their extension to the repeater-based setting is immediate.

Our results imply the existence of undiscovered BB84-like protocols and/or data processing methods that are able to overcome the best performance known so far. Identifying such protocols and/or methods is left as an open question for the community. In the free-space scenario, we showed that geometric diffraction imposes a fundamental upper bound on the maximum transmission distance; nevertheless, this limit remains sufficiently large to enable long-range implementations, including deep-space quantum communications.

Acknowledgments—This work was supported by the Integrated Quantum Networks (IQN) Research Hub (EPSRC, Grant No. EP/Z533208/1).

Data availability—There are no publicly available research data or software supporting this manuscript. Requests for further information or data should be sent to the authors.

-
- [1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.
 - [2] D. Bruss, Optimal eavesdropping in quantum cryptography with six states, *Phys. Rev. Lett.* **81**, 3018 (1998).
 - [3] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani *et al.*, Advances in quantum cryptography, *Adv. Opt. Photonics* **12**, 1012 (2020).
 - [4] S. Pirandola, R. Garcia-Patron, S. L. Braunstein, and S. Lloyd, Direct and reverse secret-key capacities of a quantum channel, *Phys. Rev. Lett.* **102**, 050503 (2009).
 - [5] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, *Nat. Commun.* **8**, 15043 (2017).
 - [6] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate-distance limit of quantum key distribution without quantum repeaters, *Nature (London)* **557**, 400 (2018).
 - [7] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, Twin-field quantum key distribution with large misalignment error, *Phys. Rev. A* **98**, 062323 (2018).
 - [8] Z.-W. Yu, X.-L. Hu, C. Jiang, H. Xu, and X.-B. Wang, Sending-or-not-sending twin-field quantum key distribution in practice, *Sci. Rep.* **9**, 3080 (2019).
 - [9] C. Jiang, Z.-W. Yu, X.-L. Hu, and X.-B. Wang, Unconditional security of sending or not sending twin-field quantum key distribution with finite pulses, *Phys. Rev. Appl.* **12**, 024061 (2019).
 - [10] C. Cui, Z.-Q. Yin, R. Wang, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, Twin-field quantum key distribution without phase postselection, *Phys. Rev. Appl.* **11**, 034053 (2019).
 - [11] See Supplemental Material at <http://link.aps.org/supplemental/10.1103/3bgy-tpy9> for details on the zero-capacity thresholds, the reduction to a Pauli channel, QBER noise modeling, the inclusion of turbulence, and the extension of the zero-capacity thresholds to repeater chains, which includes Refs. [12–17].
 - [12] R. E. Hufnagel and N. R. Stanley, Modulation transfer function associated with image transmission through turbulent media, *J. Opt. Soc. Am.* **54**, 52 (1964).
 - [13] G. C. Valley, Isoplanatic degradation of tilt correction and short-term imaging systems, *Appl. Opt.* **19**, 574 (1980).
 - [14] L. C. Andrews and R. L. Phillips, *Laser Beam Propagation Through Random Medium*, 2nd ed. (SPIE, Bellingham, 2005).
 - [15] S. M. Rytov, Diffraction of light by ultrasonic waves, *Izv. Akad. Nauk SSSR, Ser. Fiz.* **2**, 223 (1937).

- [16] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight, Quantifying entanglement, *Phys. Rev. Lett.* **78**, 2275 (1997).
- [17] V. Vedral and M. B. Plenio, Entanglement measures and purification procedures, *Phys. Rev. A* **57**, 1619 (1998).
- [18] A. Peres, Separability criterion for density matrices, *Phys. Rev. Lett.* **77**, 1413 (1996).
- [19] M. Horodecki, P. Horodecki, and R. Horodecki, Separability of mixed states: Necessary and sufficient conditions, *Phys. Lett. A* **223**, 1 (1996).
- [20] D. Gottesman and H.-K. Lo, Proof of security of quantum key distribution with two-way classical communications, *IEEE Trans. Inf. Theory* **49**, 457 (2003).
- [21] H. F. Chau, Practical scheme to share a secret key through a quantum channel with a 27.6% bit error rate, *Phys. Rev. A* **66**, 060302(R) (2002).
- [22] X.-B. Wang, Quantum key distribution with two-qubit quantum codes, *Phys. Rev. Lett.* **92**, 077902 (2004).
- [23] W.-Y. Hwang, Quantum key distribution with high loss: Toward global secure communication, *Phys. Rev. Lett.* **91**, 057901 (2003).
- [24] X.-B. Wang, Beating the photon-number-splitting attack in practical quantum cryptography, *Phys. Rev. Lett.* **94**, 230503 (2005).
- [25] X.-B. Wang, Decoy-state protocol for quantum cryptography with four different intensities of coherent light, *Phys. Rev. A* **72**, 012322 (2005).
- [26] H.-K. Lo, X. Ma, and K. Chen, Decoy state quantum key distribution, *Phys. Rev. Lett.* **94**, 230504 (2005).
- [27] D. Rusca, A. Boaron, F. Grünenfelder, A. Martin, and H. Zbinden, Finite-key analysis for the 1-decoy state QKD protocol, *Appl. Phys. Lett.* **112**, 171104 (2018).
- [28] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussi eres, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, Secure quantum key distribution over 421 km of optical fiber, *Phys. Rev. Lett.* **121**, 190502 (2018).
- [29] S. Pirandola, Limits and security of free-space quantum communications, *Phys. Rev. Res.* **3**, 013279 (2021).
- [30] S. Pirandola, Satellite quantum communications: Fundamental bounds and practical security, *Phys. Rev. Res.* **3**, 023130 (2021).
- [31] S. Pirandola, Composable security for continuous variable quantum key distribution: Trust levels and practical key rates in wired and wireless networks, *Phys. Rev. Res.* **3**, 043014 (2021).
- [32] C. F. Bohren and D. R. Huffman, *Absorption and Scattering of Light by Small Particles* (John Wiley & Sons, Inc., New York, 2008).
- [33] H. Kaushal, V. K. Jain, and S. Kar, *Free Space Optical Communication* (Springer, New York, 2017).
- [34] S. Q. Duntley, The reduction of apparent contrast by the atmosphere, *J. Opt. Soc. Am.* **38**, 179 (1948).
- [35] D. Vasylyev, W. Vogel, and F. Moll, Satellite-mediated quantum atmospheric links, *Phys. Rev. A* **99**, 053830 (2019).
- [36] H. Yura, Short term average optical-beam spread in a turbulent medium, *J. Opt. Soc. Am.* **63**, 567 (1973).
- [37] R. L. Fante, Electromagnetic beam propagation in turbulent media, *Proc. IEEE* **63**, 1669 (1975).
- [38] A. Siegman, *Lasers* (University Science Books, Mill Valley, CA, 1986).
- [39] O. Svelto, *Principles of Lasers*, 5th ed. (Springer, New York, 2010).
- [40] L. C. Andrews, W. B. Miller, and J. C. Ricklin, Geometrical representation of Gaussian beams propagating through complex paraxial optical systems, *Appl. Opt.* **32**, 5918 (1993).
- [41] L. C. Andrews, W. B. Miller, and J. C. Ricklin, Spatial coherence of a Gaussian-beam wave in weak and strong optical turbulence, *J. Opt. Soc. Am. A* **11**, 1653 (1994).
- [42] S. Pirandola, End-to-end capacities of a quantum communication network, *Commun. Phys.* **2**, 51 (2019).