Limits for quantum communications: From fibres to free space

nodeQ

Stefano Pirandola
nodeQ and UoY

UNIVERSITY of York

EPSRC
Engineering and Physical Sciences Research Council

QUANTUM COMMUNICATIONS HUB

UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME

PT-UK Workshop on Quantum Technologies in Space
(March 31, 2023)

nodeQ and UoY

Software

- Design, optimization and control of quantum-safe networks (QKD and/or PQC)
- Fast QKD data processing (universal, both DV and CV)

Theory

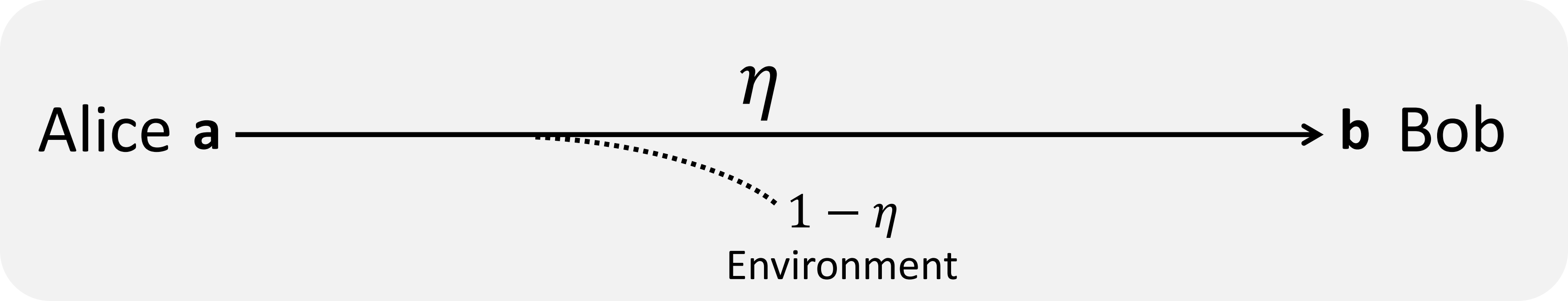
- Optimal performance for quantum-safe comms (fibre, ground free-space, sat)
- Protocols (CV-QKD, MDI, CV-MDI, etc.)

Outline of the seminar

- ☐ Fundamental limits of quantum comms
- ☐ Optimal rates for quantum repeaters
- ☐ Free-space quantum comms: Limits & CV-QKD rates
- ☐ Satellite quantum comms with CVs

Fundamental limits of quantum communications

Consider a lossy communication channel with transmissivity η



Channel can be used for various tasks:

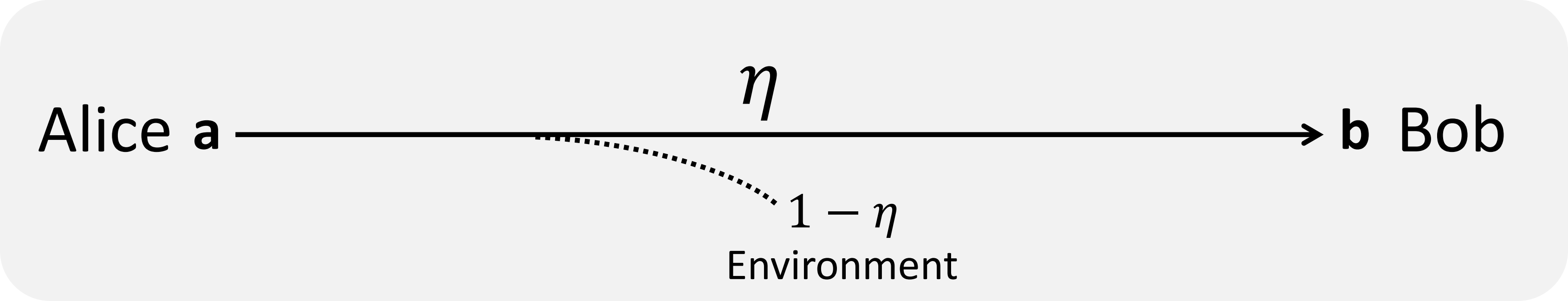
- *transmitting qubits*
- *sharing entanglement bits (ebits)*
- *generating secret key bits (QKD)*

What are the maximum rates achievable over the channel?

(qubits/ebits/secret bits per channel use)

Fundamental limits of quantum communications

Consider a lossy communication channel with transmissivity η



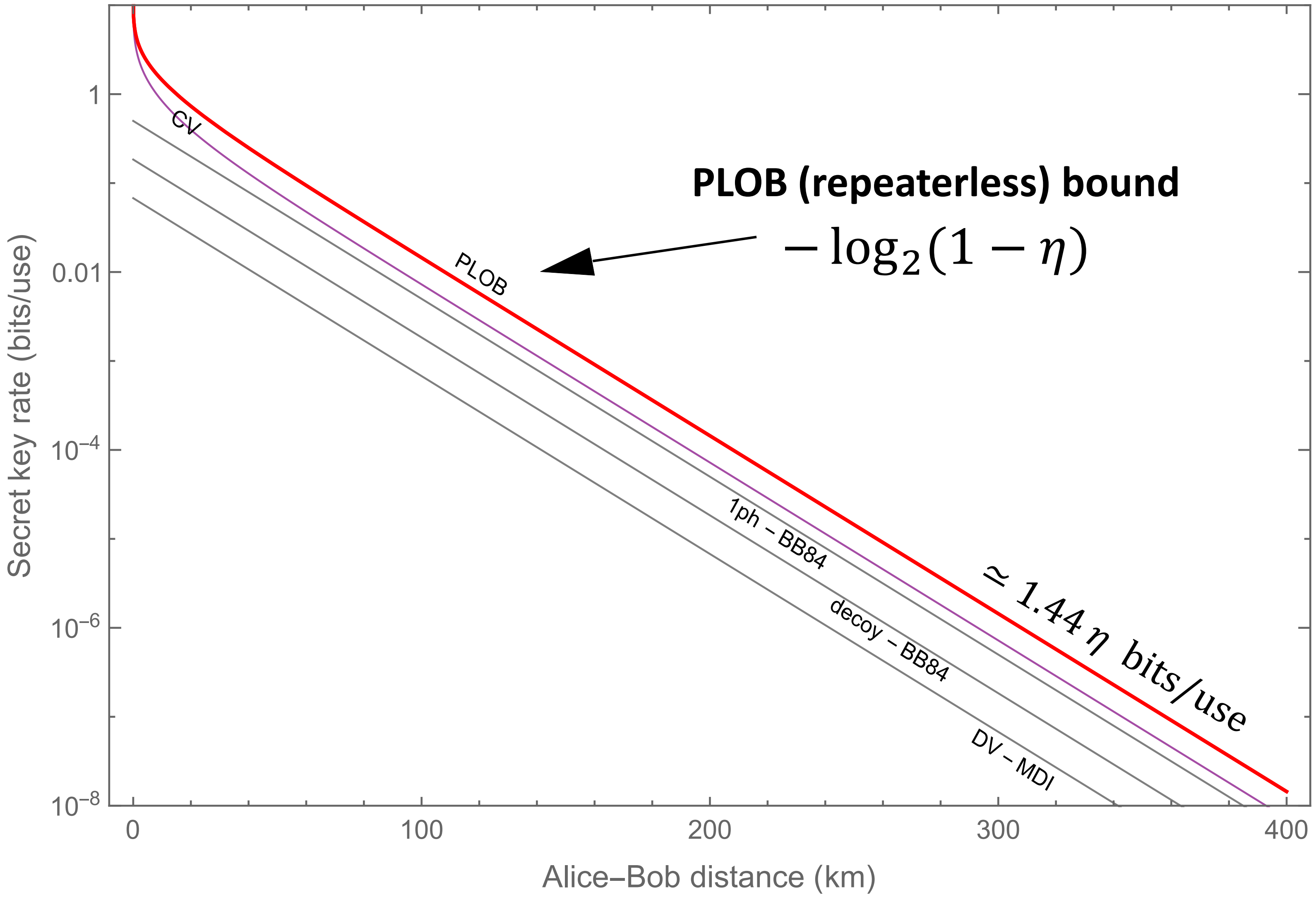
$$\boxed{K = -\log_2(1-\eta)}$$

[Pirandola, Laurenza, Ottaviani, Banchi, Nature Comm 8, 15043 (2017)]

PLOB bound is the fundamental benchmark for quantum communications:

- Provides the ultimate performance of quantum communication protocols over a quantum channel, in the absence of repeaters (repeaterless bound)
- Establishes if a quantum repeater effectively *repeats*

QKD limits before PLOB



PLOB (repeaterless) bound

$$-\log_2(1-\eta)$$

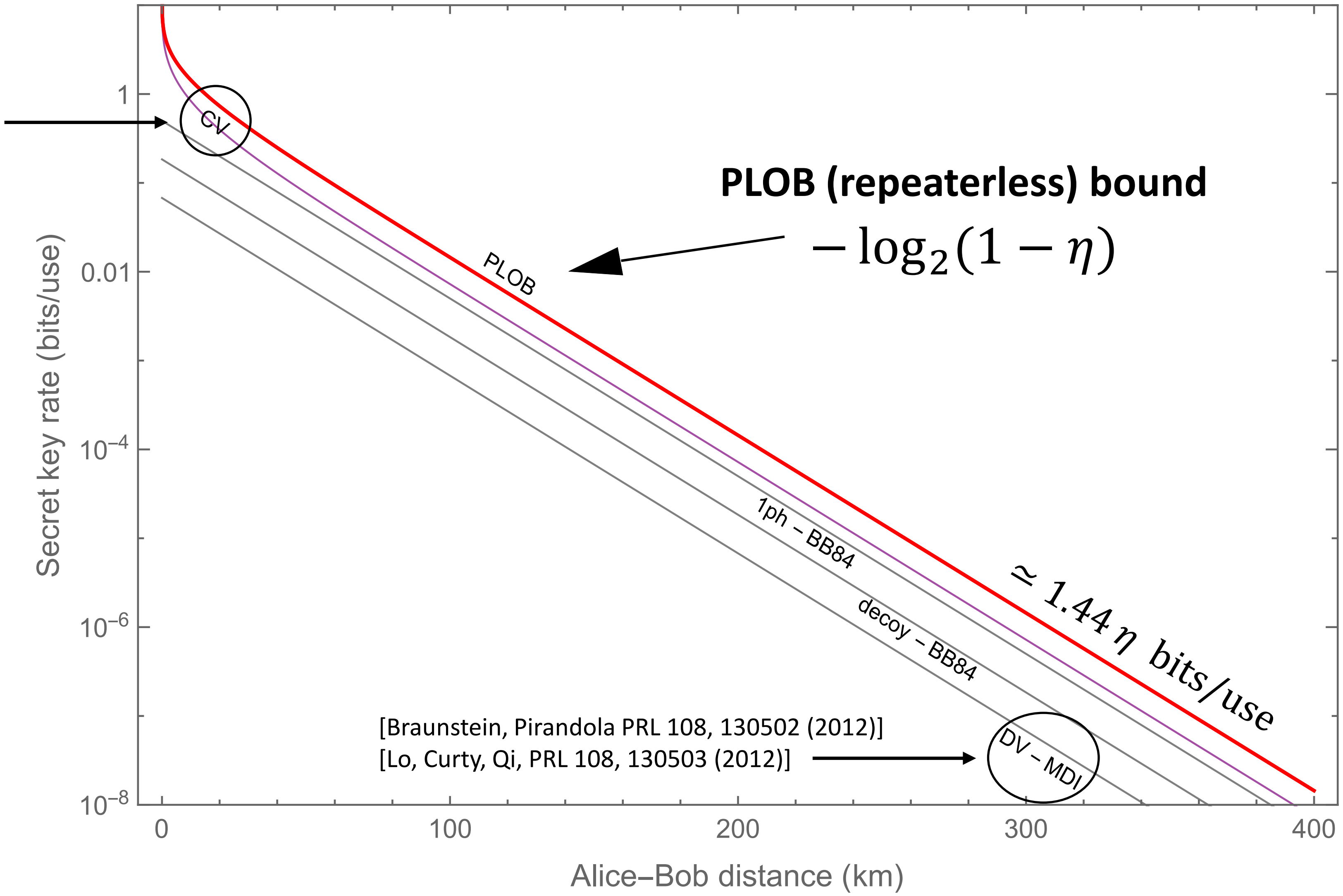
$$\simeq 1.44\,\eta \text{ bits/use}$$

[Pirandola et al., *Advances in Quantum Cryptography*, AOP 12, 1012-1236 (2020)]

QKD limits before PLOB

- GG02
- Het protocol,
- CV-MDI-QKD

[Pirandola et al, Nature Photonics 9, 397 (2015)]

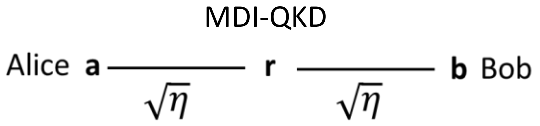


PLOB (repeaterless) bound

$$-\log_2(1-\eta)$$

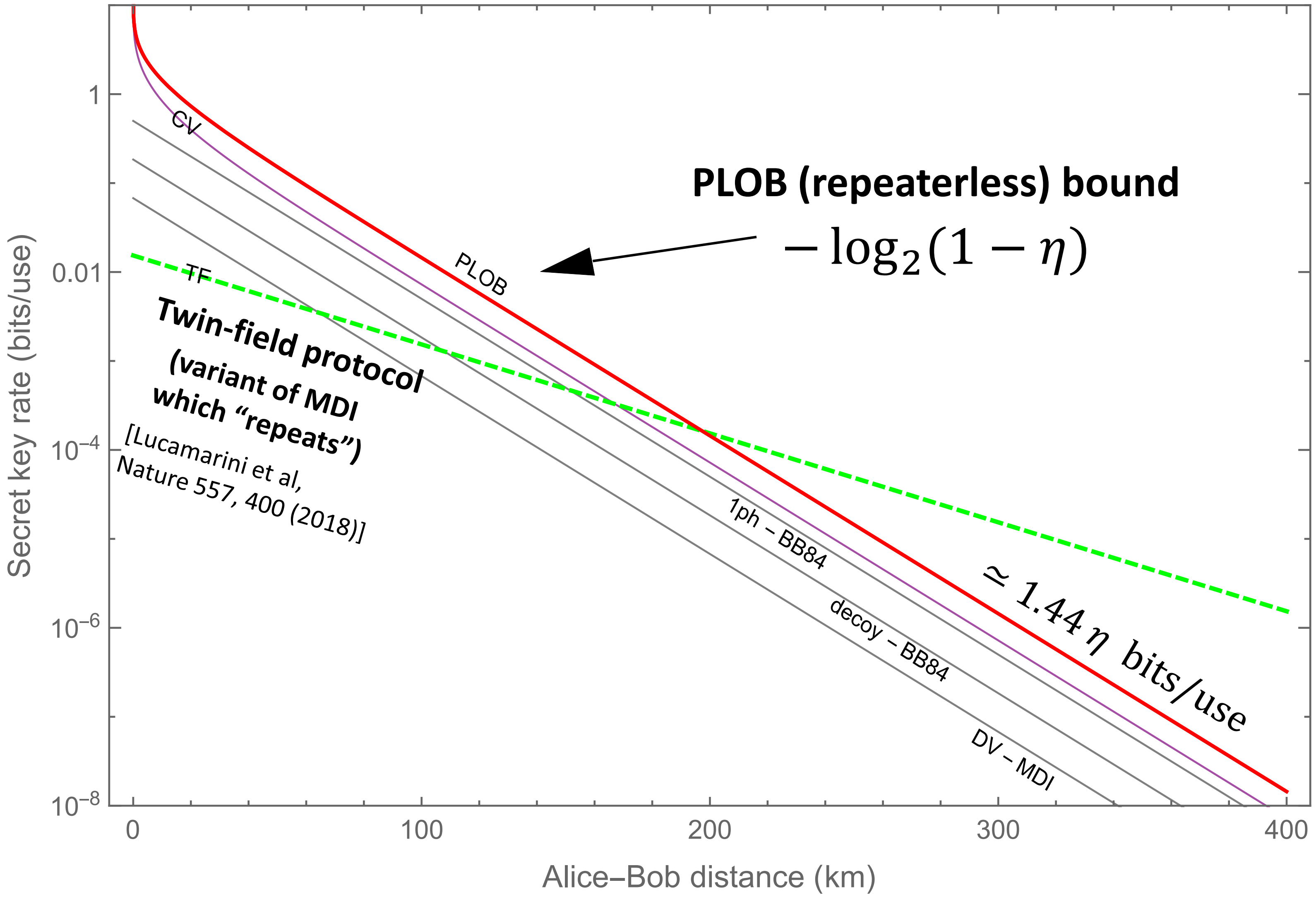
$\simeq 1.44\,\eta$ bits/use

[Braunstein, Pirandola PRL 108, 130502 (2012)]
[Lo, Curty, Qi, PRL 108, 130503 (2012)]



[Pirandola et al., *Advances in Quantum Cryptography*, AOP 12, 1012-1236 (2020)]

Repeater-assisted protocols introduced after PLOB



PLOB (repeaterless) bound

$$-\log_2(1-\eta)$$

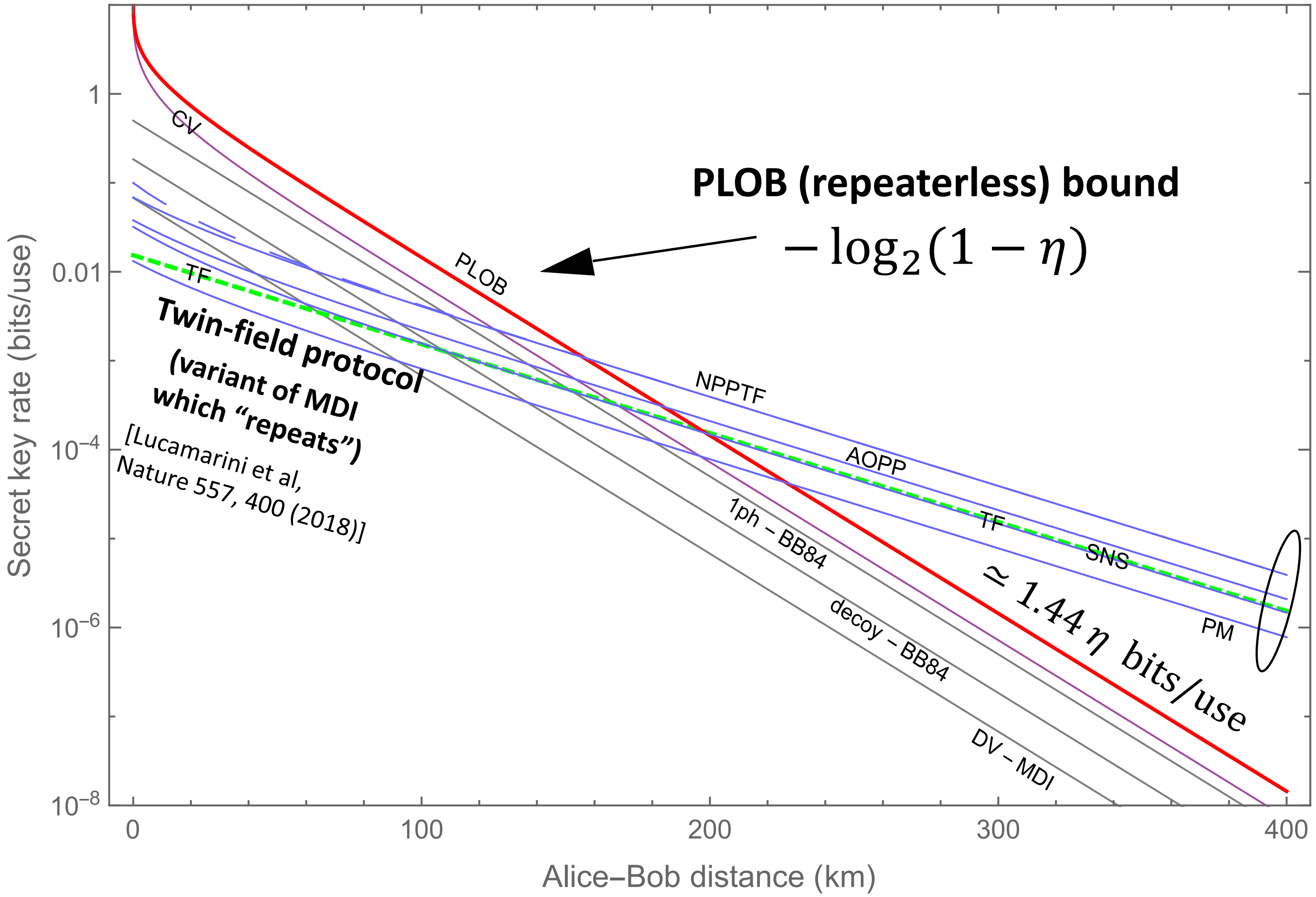
Twin-field protocol (variant of MDI which “repeats”)

[Lucamarini et al, Nature 557, 400 (2018)]

$\simeq 1.44\,\eta$ bits/use

[Pirandola et al., *Advances in Quantum Cryptography*, AOP 12, 1012-1236 (2020)]

Repeater-assisted protocols introduced after PLOB



PLOB (repeaterless) bound

$-\log_2(1-\eta)$

Twin-field protocol (variant of MDI which "repeats")

[Lucamarini et al, Nature 557, 400 (2018)]

$\simeq 1.44\,\eta$ bits/use

Other repeater-assisted protocols

- ☐ Sending or not sending (SNS)
  Wang et al, PRA 98, 062323 (2018)
  Jiang et al, PRApp 12, 024061 (2019)
- ☐ Active odd-parity pair (AOPP)
  Xu et al., PRA 101, 042330 (2020)
- ☐ No-phase-postselected (NPPTF)
  Cui et al., PRApp 11, 034053 (2019)
  Grasselli, NJP 21, 073001 (2019)
- ☐ Phase-matching (PM)
  PRX 8, 031043 (2018)

[Pirandola et al., *Advances in Quantum Cryptography*, AOP 12, 1012-1236 (2020)]

Limits of repeater-assisted quantum communications

Optical link with transmissivity η

Alice **a** $\longrightarrow$ **b** Bob

PLOB bound $K = -\log_2(1-\eta)$

only beaten by effective repeaters

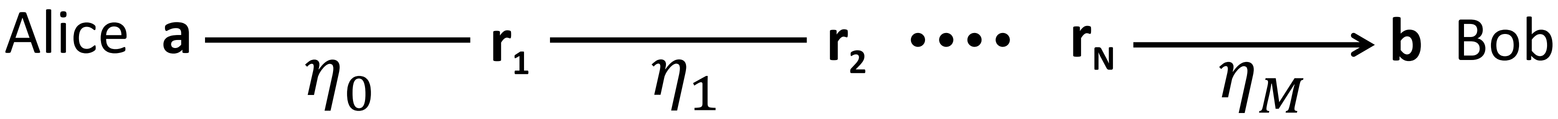
Next question: what are the optimal rates achievable by repeater-assisted protocols?

Limits of repeater-assisted quantum communications

PLOB bound $K = -\log_2(1-\eta)$

only beaten by effective repeaters

Consider a chain of M ideal repeaters between Alice and Bob



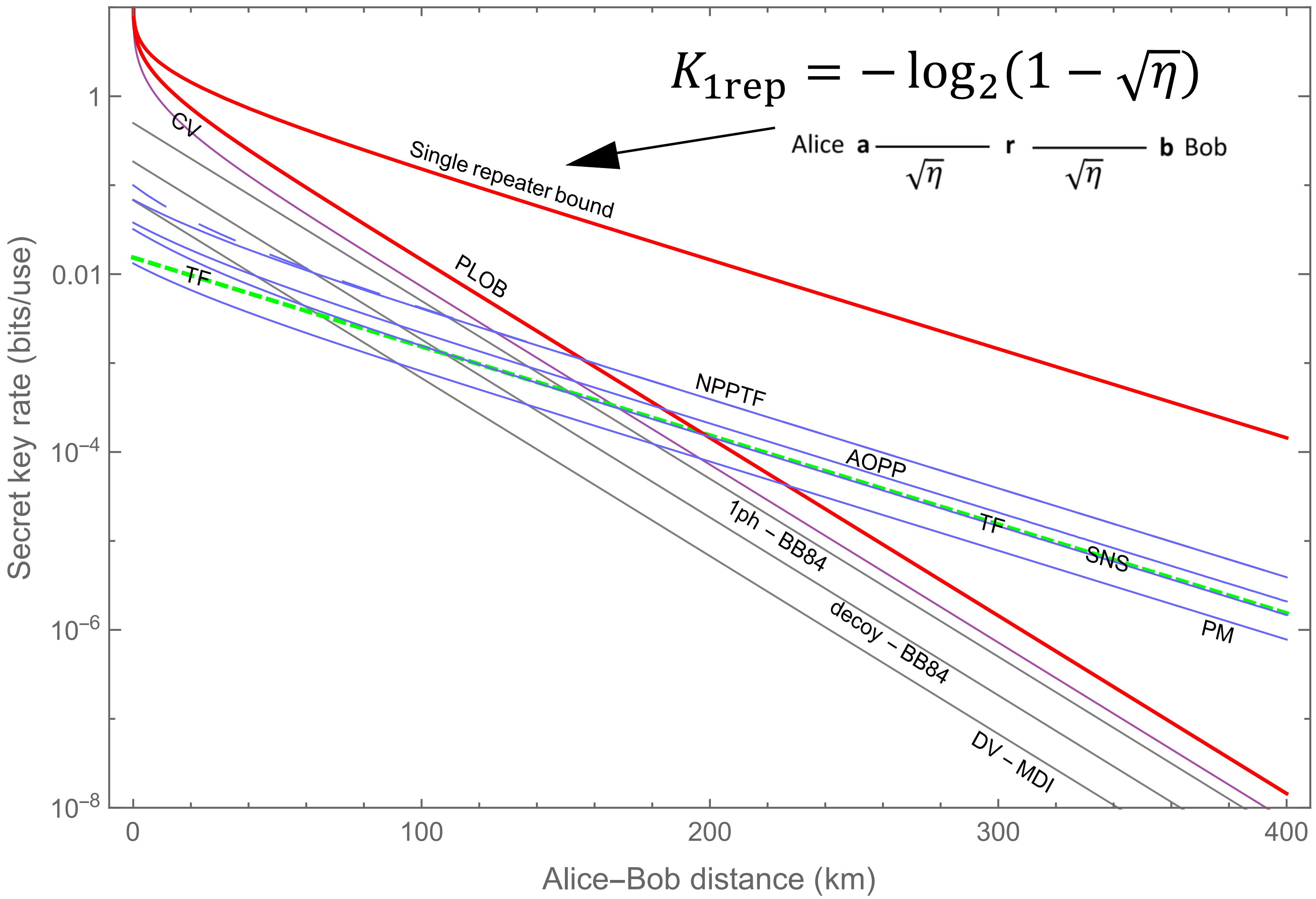
The capacity of the chain is given by the min transmissivity

$$K = -\log_2(1 - \min_i\{\eta_i\})$$

Techniques:
-Lower bound (simple, by composition)
-Upper bound (difficult, via REE and teleportation simulation)

[Pirandola, *End-to-end capacities of a quantum communication network*, Communications Physics 2, 51 (2019)]

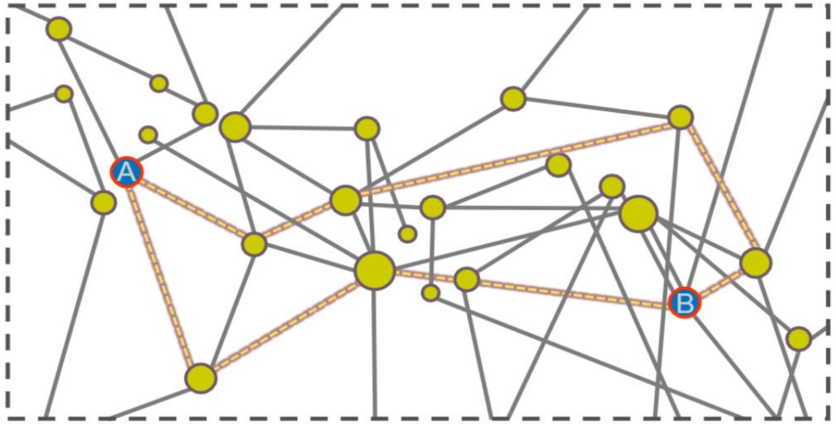
Limits of repeater-assisted quantum communications



$$K_{1\mathrm{rep}} = -\log_2(1-\sqrt{\eta})$$

[Pirandola et al., *Advances in Quantum Cryptography*, AOP 12, 1012-1236 (2020)]

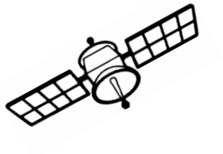
Quantum network architecture



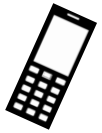
Theory well developed for wired connections (optical fibres)

Need to integrate free-space links

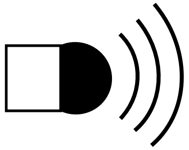
- Satellite links (global quantum network)

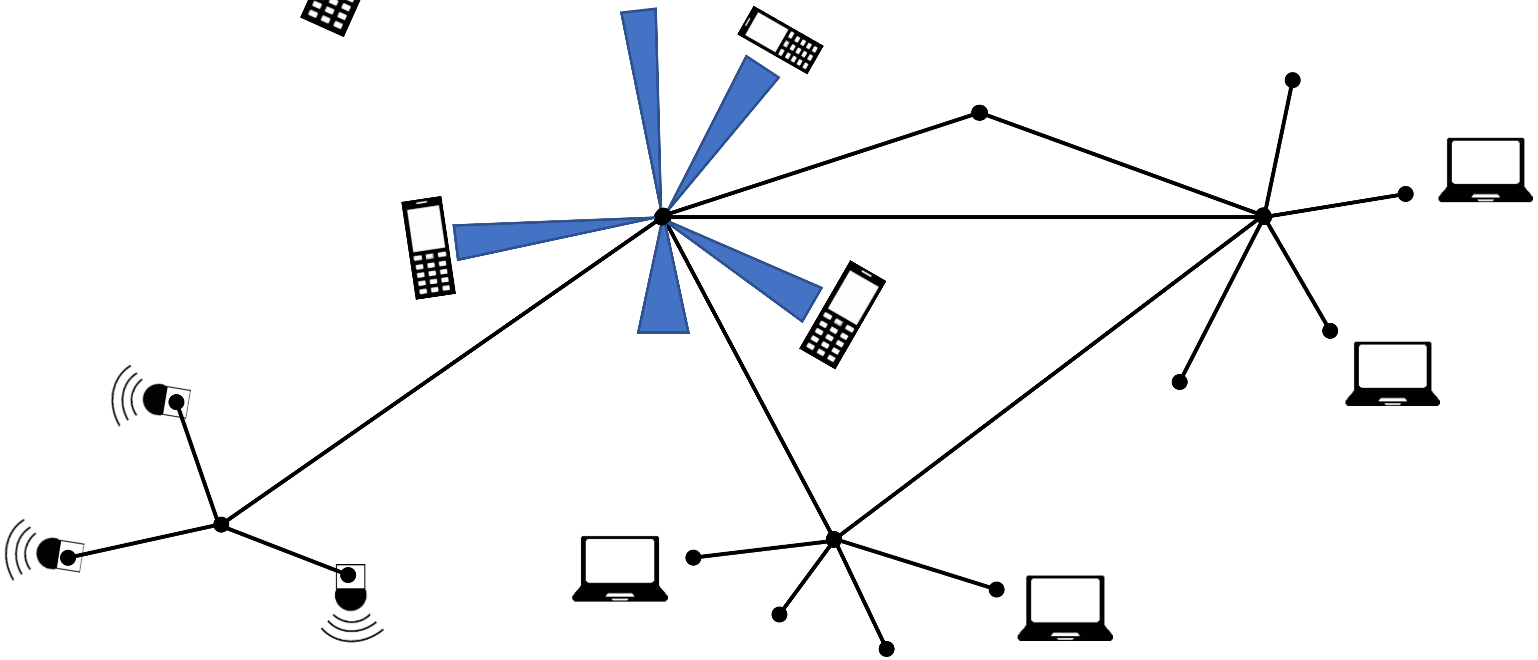


- Local wireless sub-networks with mobile devices

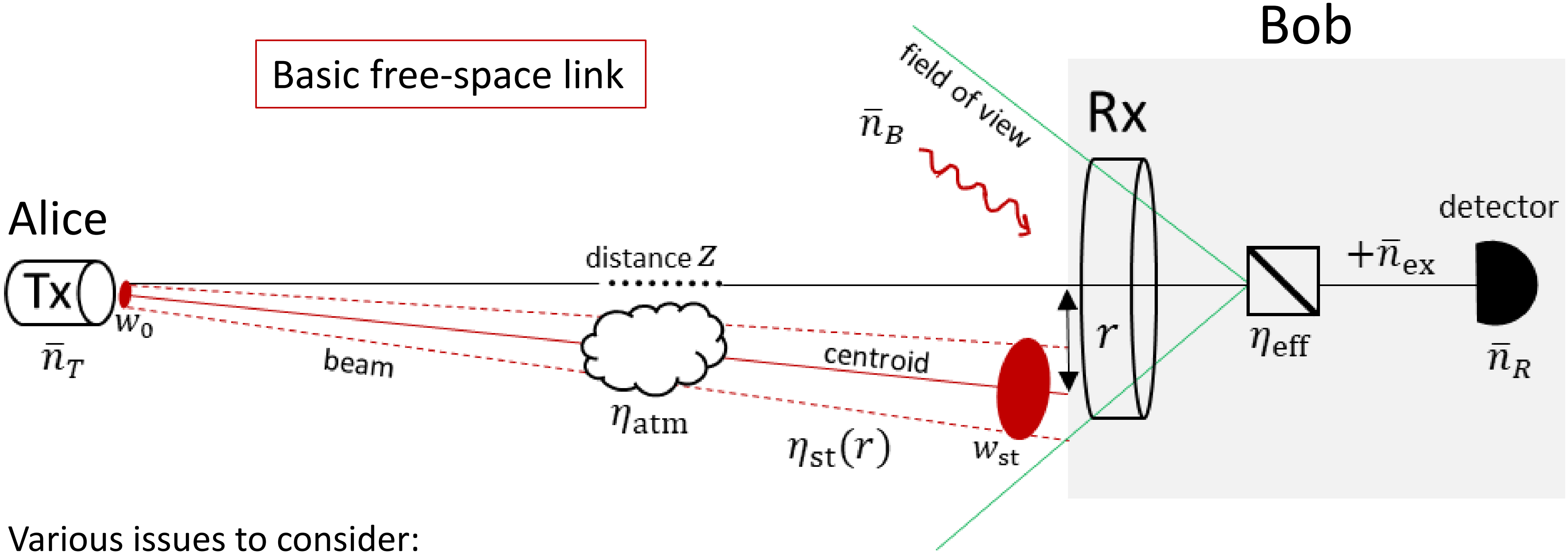


- Sensors (IoT)





Limits and security of free-space quantum communications



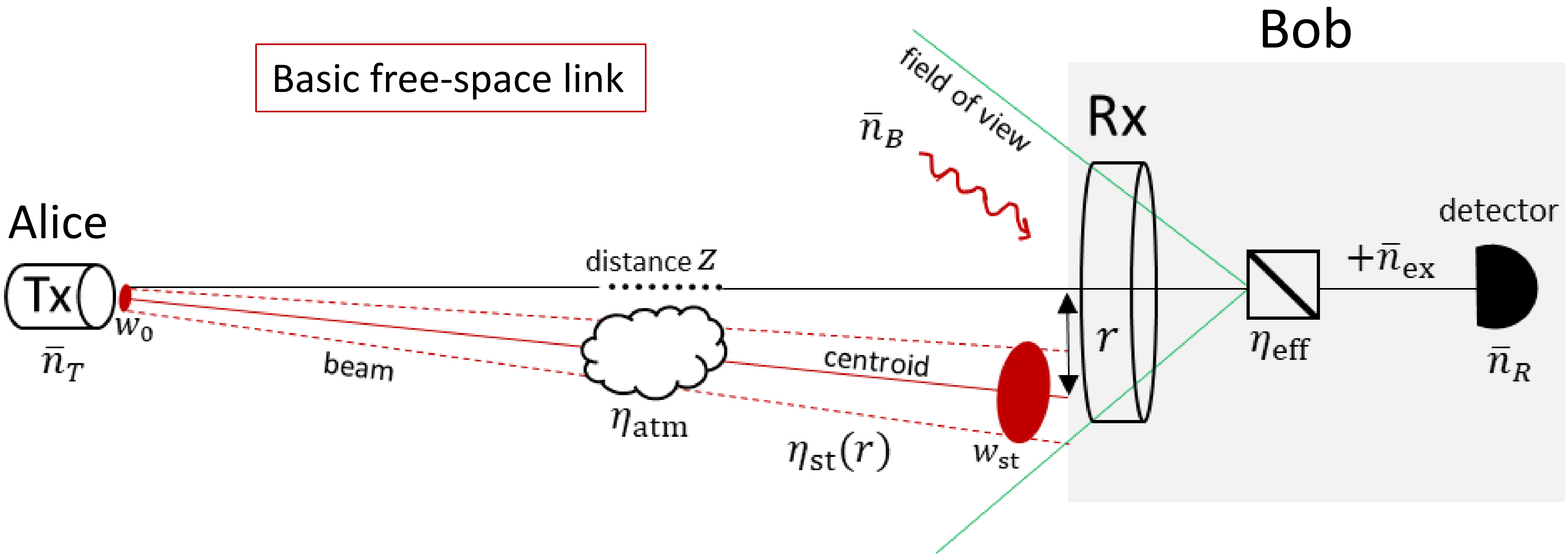
Various issues to consider:

- Free-space diffraction
- Atmospheric extinction (Beer-Lambert model)
- Beam deflection and pointing errors
- Weak turbulence (beam spreading and wandering; H-V model)
- Background thermal noise (sky brightness)
- Setup imperfections (<1 efficiency, electronic noise etc.)

[Pirandola, *Limits and security of free-space quantum communications*, Physical Review Research 3, 013279 (2021)]

Limits and security of free-space quantum communications

Basic free-space link



η max transmissivity

σ^2 variance due to fading

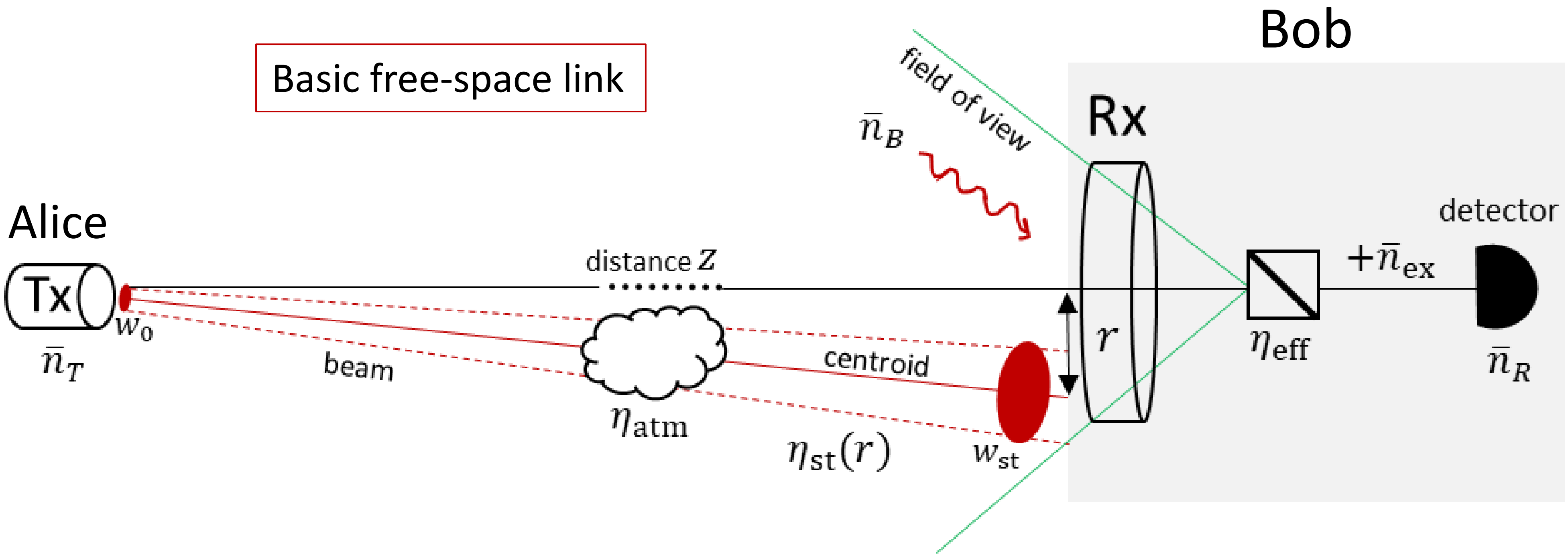
$\bar{n}$ total noise

Free-space limit for q. comms

$$\boxed{K_{\text{free}} \leq -\underbrace{\Delta(\eta, \sigma)}_{\text{fading correction}} \log_2(1-\eta)}$$

[Pirandola, *Limits and security of free-space quantum communications*, Physical Review Research 3, 013279 (2021)]

Limits and security of free-space quantum communications



η	max transmissivity
σ^2	variance due to fading
$\bar{n}$	total noise

Free-space limit for q. comms

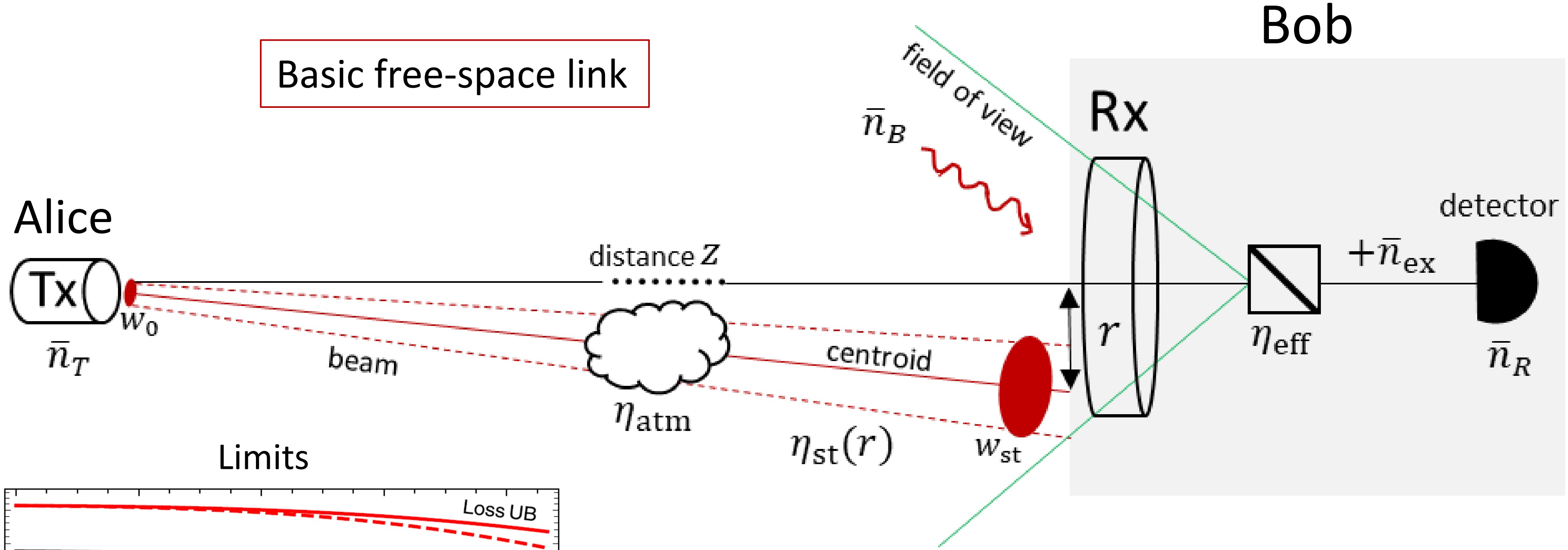
$$\boxed{K_{\mathrm{free}} \leq -\Delta(\eta, \sigma) \log_2(1-\eta)}$$

$$\boxed{K_{\mathrm{free}} \leq -\Delta(\eta, \sigma) \log_2(1-\eta) - \underbrace{\mathcal{T}(\bar{n}, \eta, \sigma)}_{\text{thermal correction}}}$$

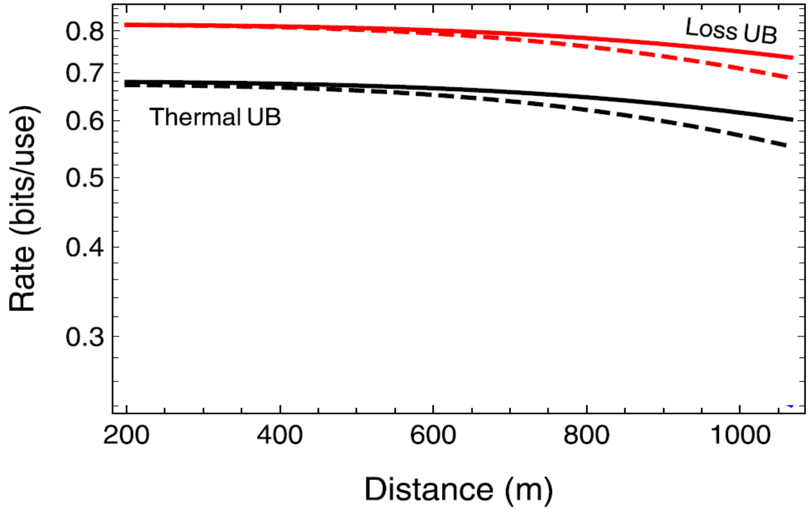
[Pirandola, *Limits and security of free-space quantum communications*, Physical Review Research 3, 013279 (2021)]

Limits and security of free-space quantum communications

Basic free-space link



Limits



Free-space limit for q. comms

$$\boxed{K_{\text{free}} \leq -\Delta(\eta,\sigma)\log_2(1-\eta)}$$

$$\boxed{K_{\text{free}} \leq -\Delta(\eta,\sigma)\log_2(1-\eta) - \underbrace{\mathcal{T}(\bar{n},\eta,\sigma)}_{\text{thermal correction}}}$$

[Pirandola, *Limits and security of free-space quantum communications*, Physical Review Research 3, 013279 (2021)]

Limits and security of free-space quantum communications

Remarkably, practical rates for CV-QKD are not far from the free-space limit

- We derive a general formula for the secret key rate accounting for:
  - Finite-size effects (finite number of uses, parameter estimation, finite digitalization)
  - Composable security (error correction, privacy amplification etc.. each associated with an epsilon error)
  - Free space fading (data undergoes suitable de-fading procedure by using pilots and post-selection)

$$R \geqslant r\left(R_{\mathrm{pe}} - \frac{\Delta_{\mathrm{aep}}}{\sqrt{n}} + \frac{\Theta}{n}\right)$$

[Pirandola, *Limits and security of free-space quantum communications*, Physical Review Research 3, 013279 (2021)]

Limits and security of free-space quantum communications

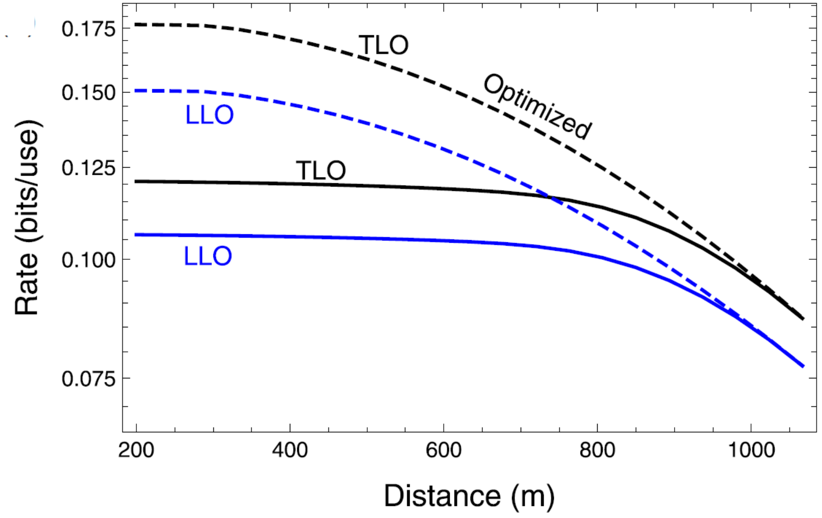
Remarkably, practical rates for CV-QKD are not far from the free-space limit

- We derive a general formula for the secret key rate accounting for:
  - Finite-size effects (finite number of uses, parameter estimation, finite digitalization)
  - Composable security (error correction, privacy amplification etc.. each associated with an epsilon error)
  - Free space fading (data undergoes suitable de-fading procedure by using pilots and post-selection)

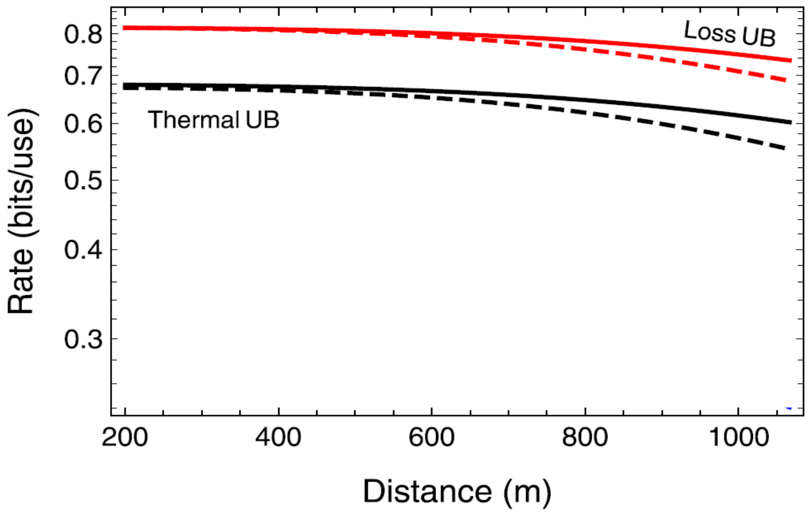
$$R \geqslant r\left(R_{\mathrm{pe}} - \frac{\Delta_{\mathrm{aep}}}{\sqrt{n}} + \frac{\Theta}{n}\right)$$

- We compare the practical CV-QKD performance with the ultimate limits:
  High-rate free-space CV-QKD is feasible with current tech!

Practical rates



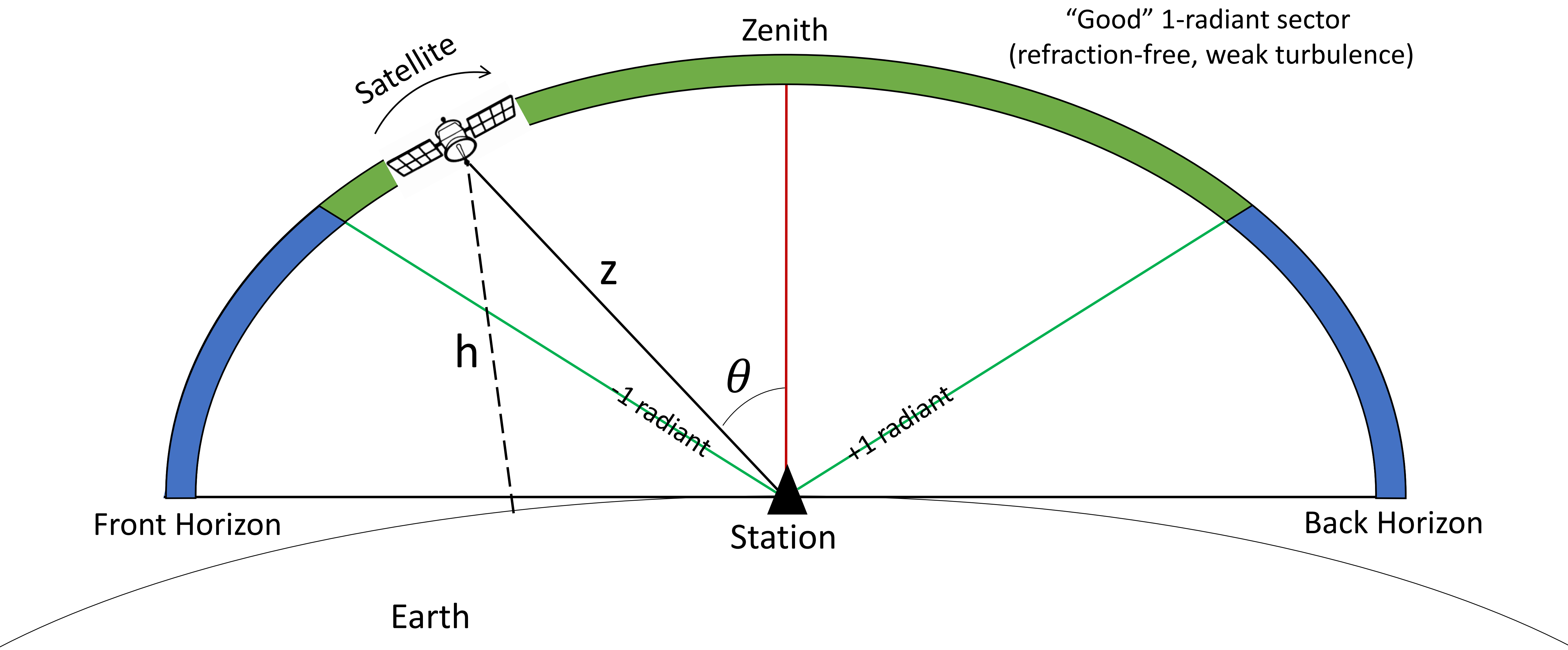
Limits



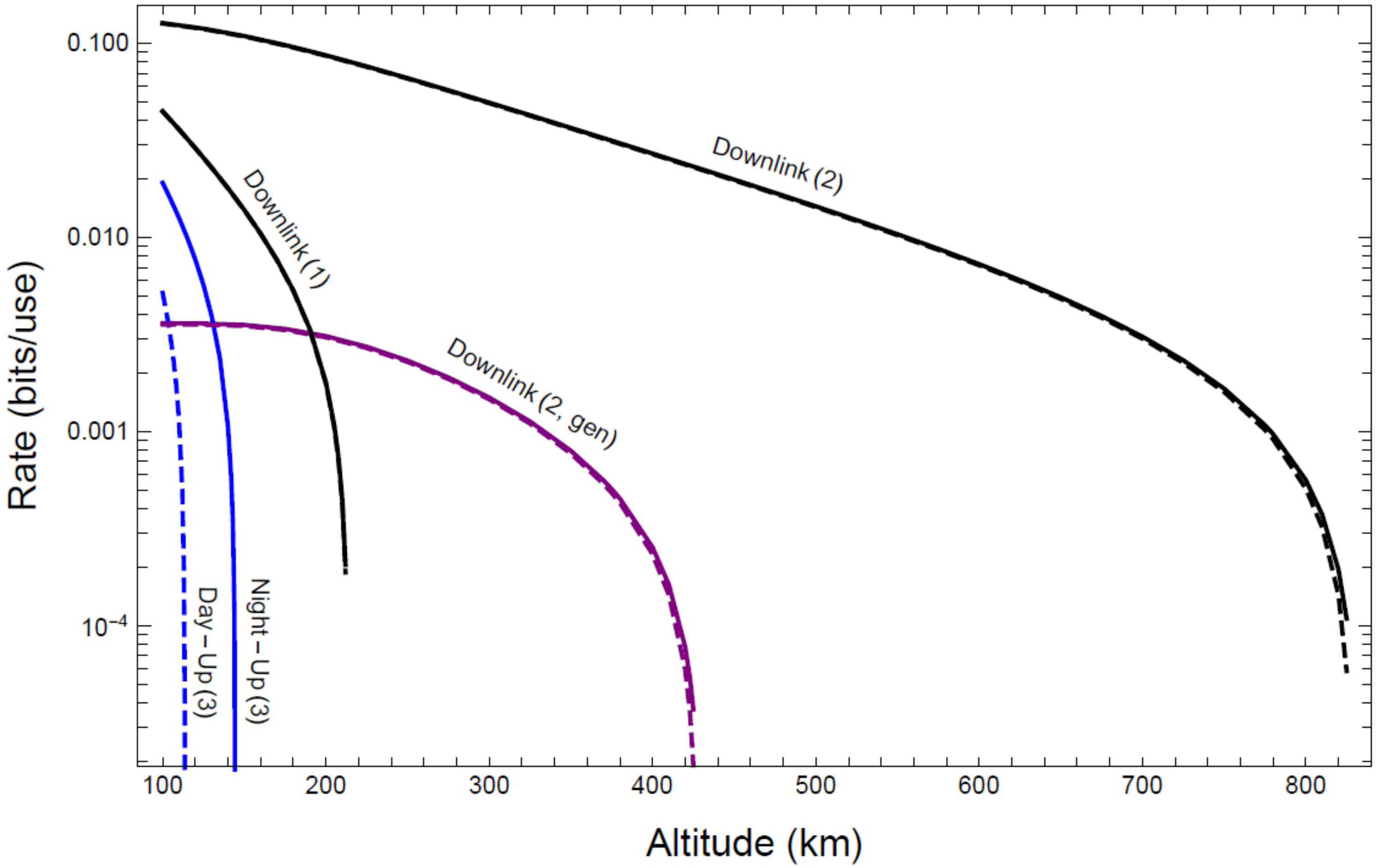
[Pirandola, *Limits and security of free-space quantum communications*, Physical Review Research 3, 013279 (2021)]

Satellite quantum communications with CVs

Results can be extended to satellite quantum communications



Satellite quantum communications with CVs



Practical CV-QKD rates

Solid = night
Dashed = day

High-rate CV-QKD with satellite feasible for all configurations in the LEO/sub-LEO region (but with different requirements)

[Pirandola, *Satellite Quantum Communications: Fundamental Bounds and Practical Security*, Phys. Rev. Res. 3, 023130 (2021)]

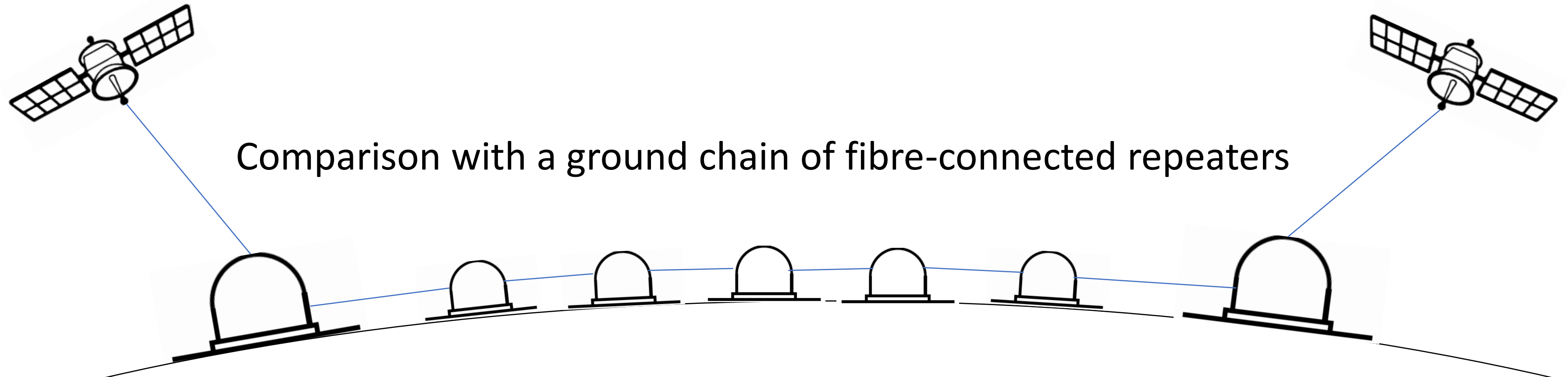
Satellite versus repeater chains

Consider a sun-synchronous satellite (almost circular orbit) which crosses the zenith points of two remote ground stations

Daily rate of secret bits that the satellite can distribute between the two stations

	Night	Day
Downlink (530 km)	$\approx 6.13 \times 10^7$	$\approx 6.08 \times 10^7$
Uplink (103 km)	$\approx 1.69 \times 10^7$	$\approx 1.09 \times 10^7$

*Clock 10 MHz

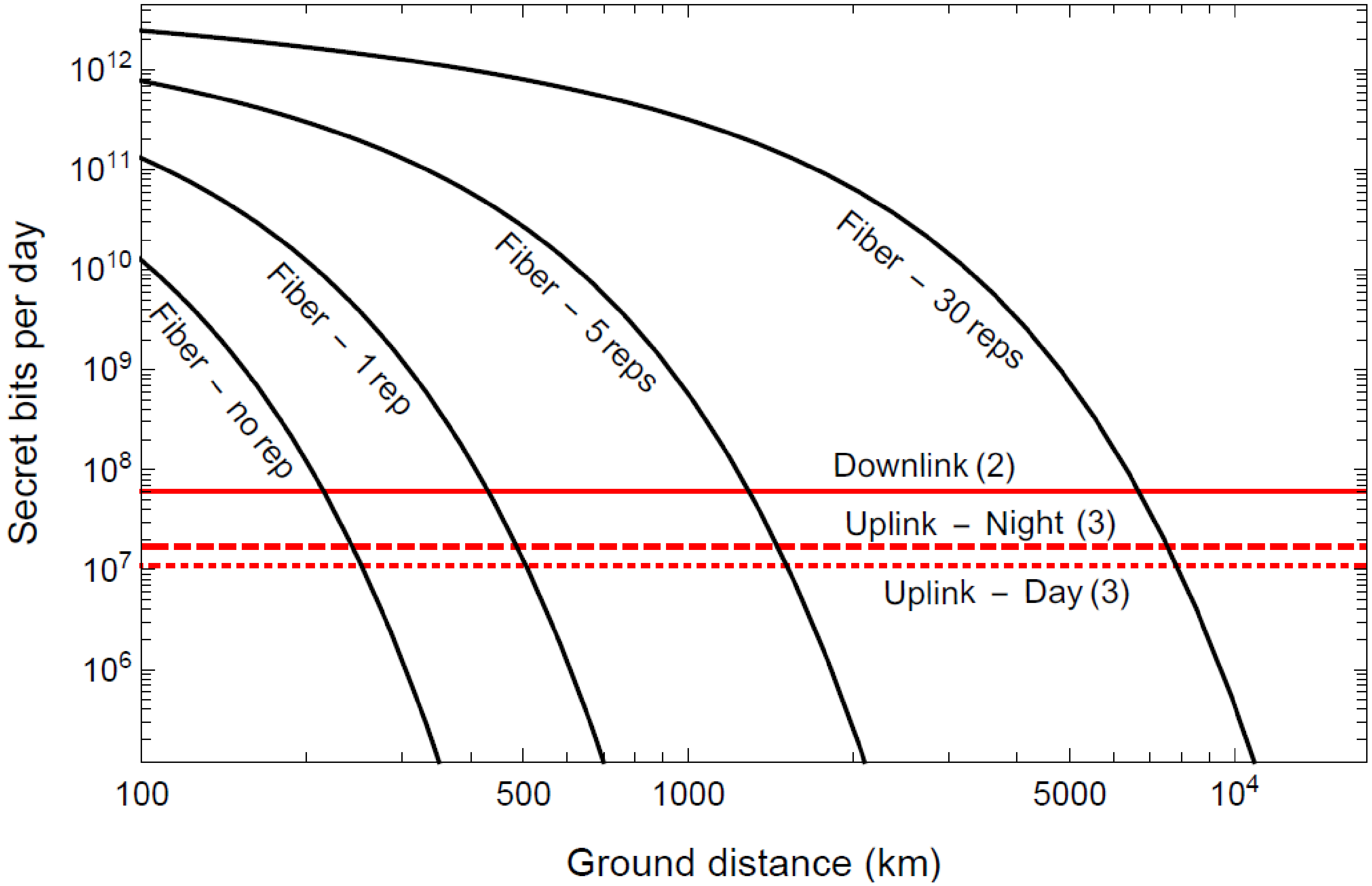


Comparison with a ground chain of fibre-connected repeaters

[Pirandola, *Satellite Quantum Communications: Fundamental Bounds and Practical Security*, Phys. Rev. Res. 3, 023130 (2021)]

Satellite versus repeater chains

Consider a sun-synchronous satellite (almost circular orbit) which crosses the zenith points of two remote ground stations



[Pirandola, *Satellite Quantum Communications: Fundamental Bounds and Practical Security*, Phys. Rev. Res. 3, 023130 (2021)]

[Harney and Pirandola, *Analytical Methods for High-Rate Global Quantum Networks*, PRX Quantum 3, 010349 (2022)]

Take-home messages for sat quantum comms

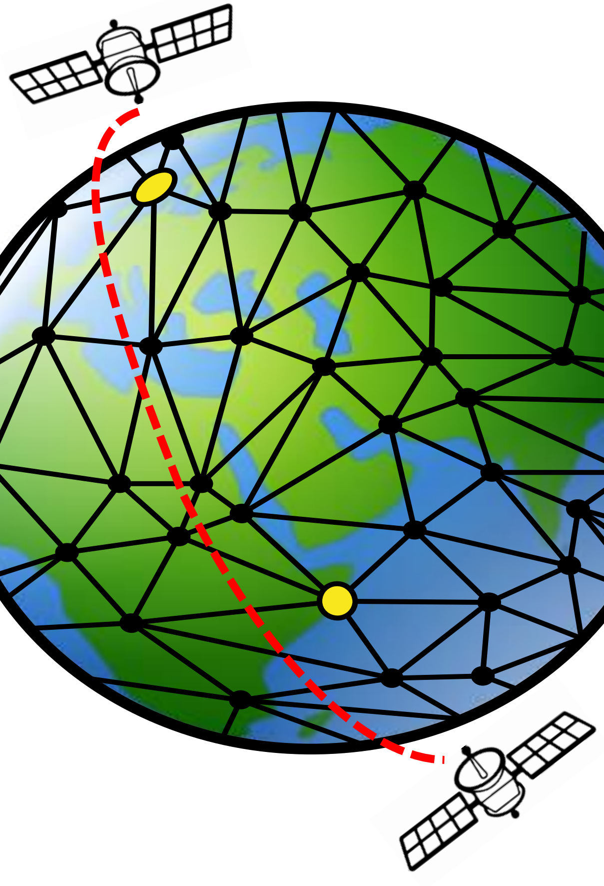
❑ High rates can be achieved with CV-QKD technology (cheaper than DV)

❑ Best case is downlink from LEO (day or night)

❑ Sat-based QKD can be more viable than fibre-connected repeater chains

❑ Important bottleneck for sats: QKD data processing not so fast for orbital dynamics

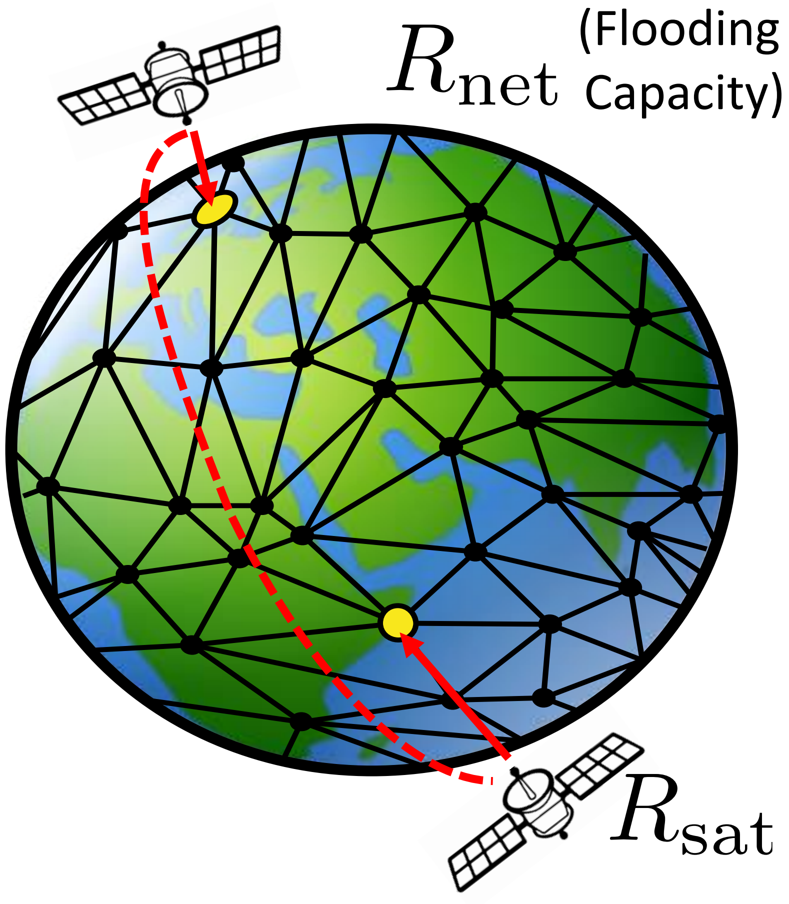
❑ Good news: QKD data processing is now fast for both DVs and CVs (nodeQ's software)



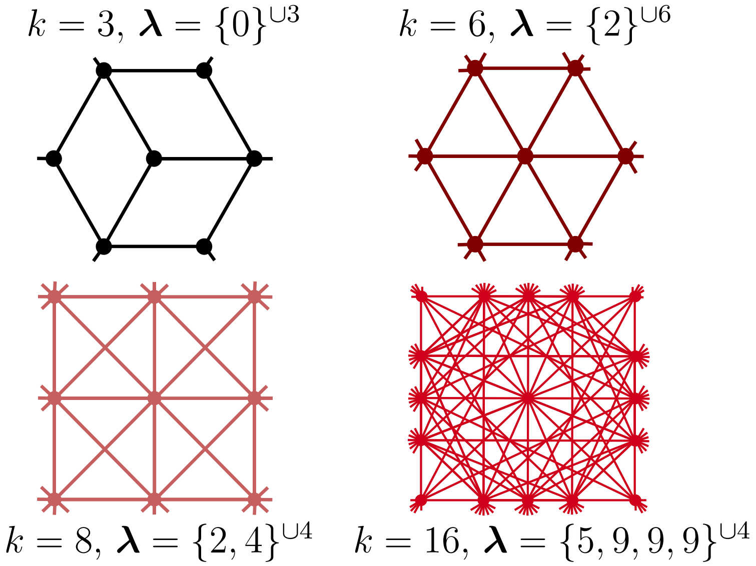
Thanks for your attention!

Additional Slides

Satellite versus ground network



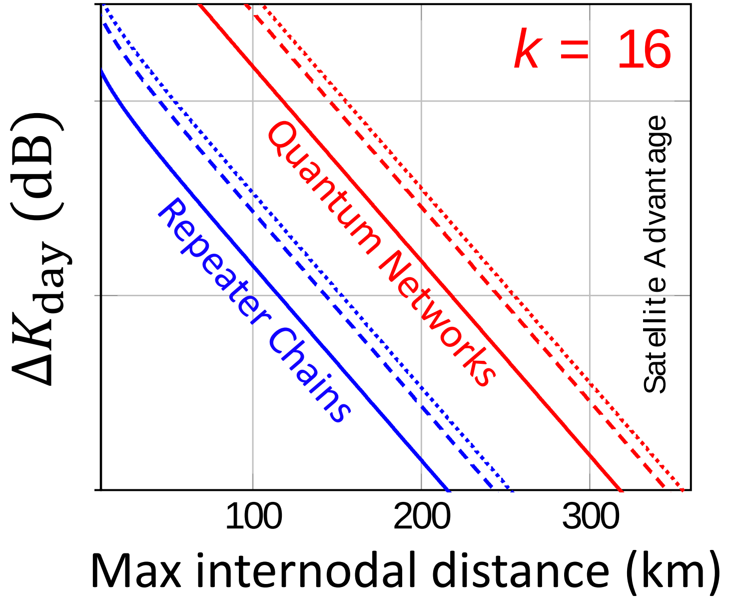
Network topologies



Satellite advantage for negative decibels

$$\boxed{\Delta K_{\text{day}} = 10\log_{10}\left(\frac{R_{\text{net}}}{R_{\text{sat}}}\right)}$$

$$d_{\mathcal{N}}^{\text{crit}} \sim 317\text{km}$$



[Harney and Pirandola, *Analytical Methods for High-Rate Global Quantum Networks*, PRX Quantum 3, 010349 (2022)]

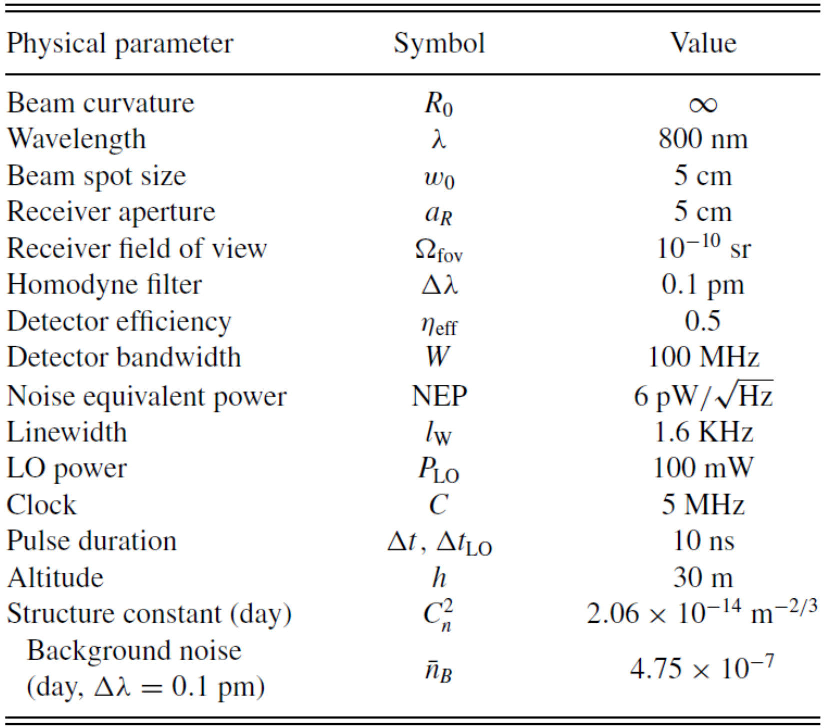
Limits and security of free-space quantum communications

Remarkably, practical rates for CV-QKD are not far from the free-space limit

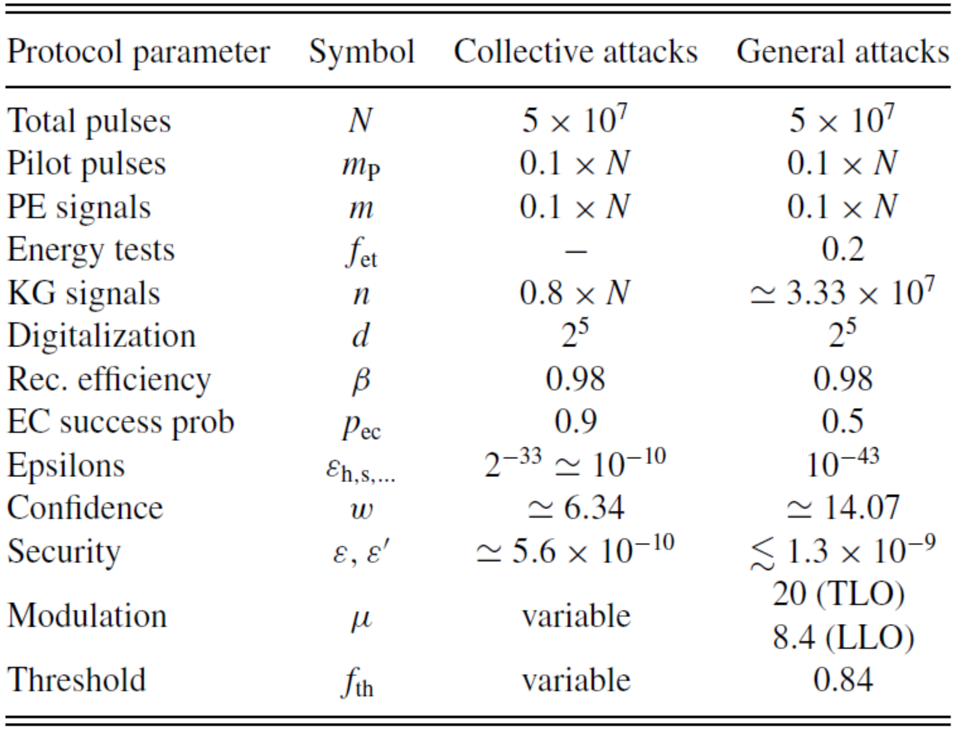
- We derive a general formula for the secret key rate accounting for:
  - Finite-size effects (finite number of uses, parameter estimation, finite digitalization)
  - Composable security (error correction, privacy amplification etc.. each associated with an epsilon error)
  - Free space fading (data undergoes suitable de-fading procedure by using pilots and post-selection)

$$R \geqslant r\left(R_{\mathrm{pe}} - \frac{\Delta_{\mathrm{aep}}}{\sqrt{n}} + \frac{\Theta}{n}\right)$$

- We consider practical parameters and physical conditions:



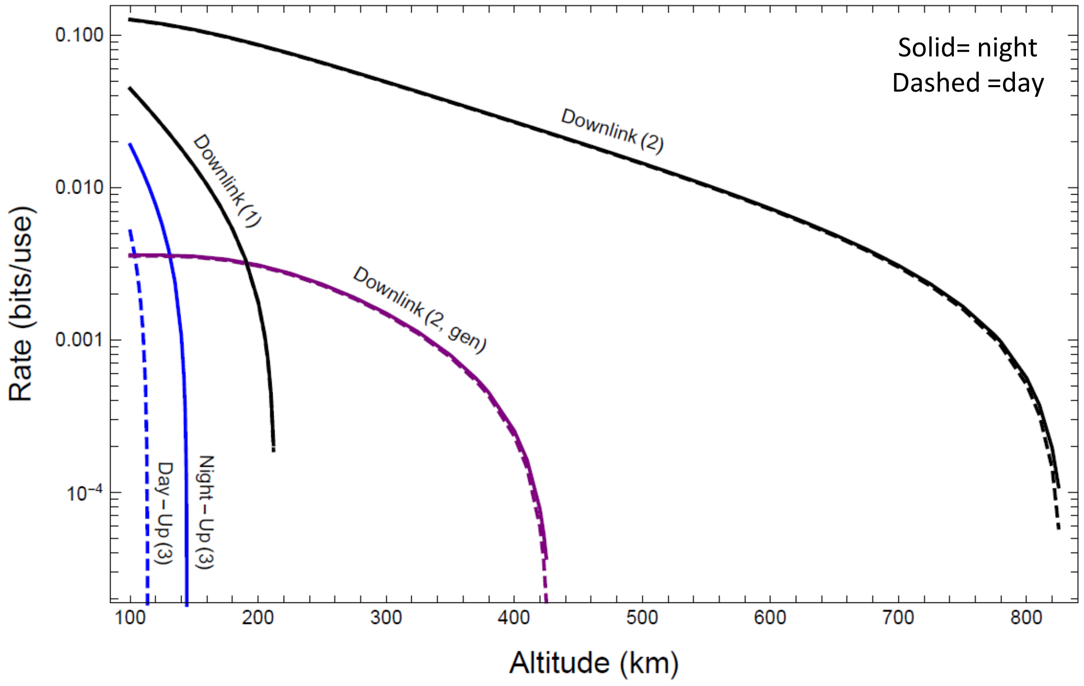
Physical parameter	Symbol	Value
Beam curvature	R_0	∞
Wavelength	λ	800 nm
Beam spot size	w_0	5 cm
Receiver aperture	a_R	5 cm
Receiver field of view	Ω_{fov}	10^{-10} sr
Homodyne filter	$\Delta\lambda$	0.1 pm
Detector efficiency	η_{eff}	0.5
Detector bandwidth	W	100 MHz
Noise equivalent power	NEP	$6\ \mathrm{pW}/\sqrt{\mathrm{Hz}}$
Linewidth	l_{W}	1.6 KHz
LO power	P_{LO}	100 mW
Clock	C	5 MHz
Pulse duration	Δt, Δt_{LO}	10 ns
Altitude	h	30 m
Structure constant (day)	C_n^2	$2.06 \times 10^{-14}\ \mathrm{m}^{-2/3}$
Background noise (day, $\Delta\lambda = 0.1$ pm)	$\bar{n}_B$	4.75×10^{-7}



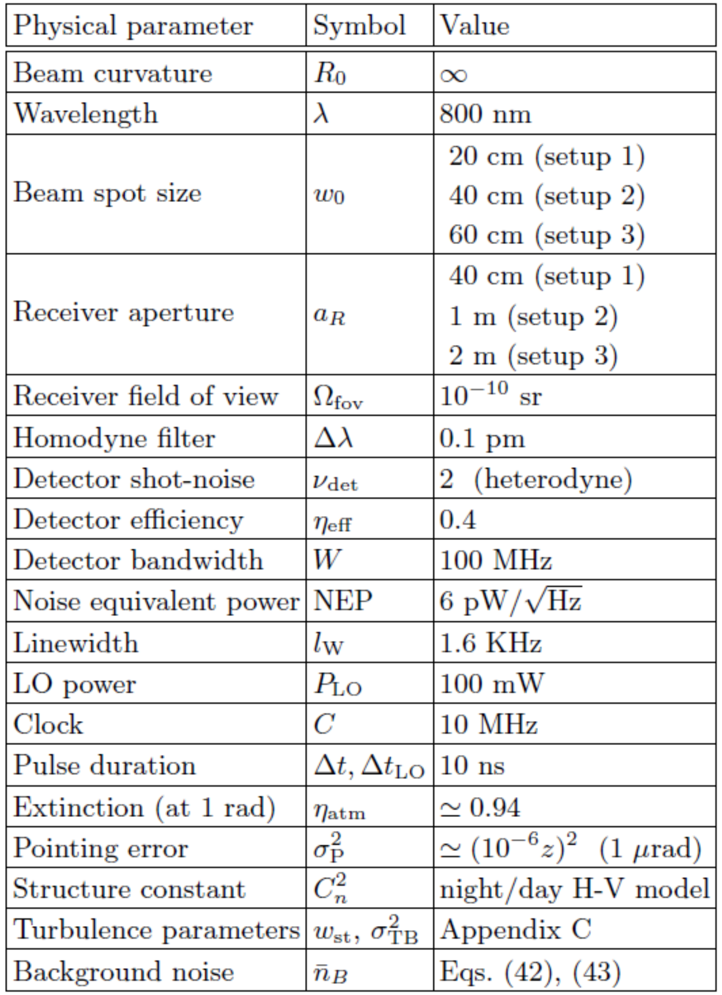
Protocol parameter	Symbol	Collective attacks	General attacks
Total pulses	N	5×10^7	5×10^7
Pilot pulses	m_{P}	$0.1 \times N$	$0.1 \times N$
PE signals	m	$0.1 \times N$	$0.1 \times N$
Energy tests	f_{et}	–	0.2
KG signals	n	$0.8 \times N$	$\simeq 3.33 \times 10^7$
Digitalization	d	2^5	2^5
Rec. efficiency	β	0.98	0.98
EC success prob	p_{ec}	0.9	0.5
Epsilons	$\varepsilon_{\mathrm{h,s,\ldots}}$	$2^{-33} \simeq 10^{-10}$	10^{-43}
Confidence	w	$\simeq 6.34$	$\simeq 14.07$
Security	ε, ε'	$\simeq 5.6 \times 10^{-10}$	$\lesssim 1.3 \times 10^{-9}$
Modulation	μ	variable	20 (TLO) 8.4 (LLO)
Threshold	f_{th}	variable	0.84

Satellite quantum communications with CVs

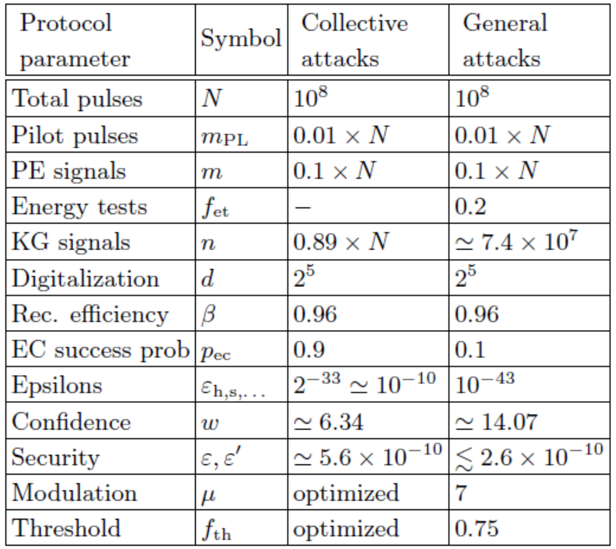
Practical CV-QKD rates



High-rate CV-QKD with satellite feasible for all configurations in the LEO/sub-LEO region (but with different requirements)



Physical parameter	Symbol	Value
Beam curvature	R_0	∞
Wavelength	λ	800 nm
Beam spot size	w_0	20 cm (setup 1) 40 cm (setup 2) 60 cm (setup 3)
Receiver aperture	a_R	40 cm (setup 1) 1 m (setup 2) 2 m (setup 3)
Receiver field of view	Ω_{fov}	10^{-10} sr
Homodyne filter	$\Delta\lambda$	0.1 pm
Detector shot-noise	ν_{det}	2 (heterodyne)
Detector efficiency	η_{eff}	0.4
Detector bandwidth	W	100 MHz
Noise equivalent power	NEP	$6\ \text{pW}/\sqrt{\text{Hz}}$
Linewidth	l_{W}	1.6 KHz
LO power	P_{LO}	100 mW
Clock	C	10 MHz
Pulse duration	Δt, Δt_{LO}	10 ns
Extinction (at 1 rad)	η_{atm}	$\simeq 0.94$
Pointing error	σ_{P}^2	$\simeq (10^{-6}z)^2$ (1 μrad)
Structure constant	C_n^2	night/day H-V model
Turbulence parameters	w_{st}, σ_{TB}^2	Appendix C
Background noise	$\bar{n}_B$	Eqs. (42), (43)



Protocol parameter	Symbol	Collective attacks	General attacks
Total pulses	N	10^8	10^8
Pilot pulses	m_{PL}	$0.01 \times N$	$0.01 \times N$
PE signals	m	$0.1 \times N$	$0.1 \times N$
Energy tests	f_{et}	–	0.2
KG signals	n	$0.89 \times N$	$\simeq 7.4 \times 10^7$
Digitalization	d	2^5	2^5
Rec. efficiency	β	0.96	0.96
EC success prob	p_{ec}	0.9	0.1
Epsilons	$\varepsilon_{\text{h,s,...}}$	$2^{-33} \simeq 10^{-10}$	10^{-43}
Confidence	w	$\simeq 6.34$	$\simeq 14.07$
Security	$\varepsilon, \varepsilon'$	$\simeq 5.6 \times 10^{-10}$	$\lesssim 2.6 \times 10^{-10}$
Modulation	μ	optimized	7
Threshold	f_{th}	optimized	0.75

[Pirandola, *Satellite Quantum Communications: Fundamental Bounds and Practical Security*, Phys. Rev. Res. 3, 023130 (2021)]