Finite key effects

— in satellite quantum key distribution —

Jasminder Sidhu

QCrypt 2021

University of Strathclyde

QUANTUM COMMUNICATIONS HUB

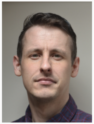
EPSRC Engineering and Physical Sciences Research Council

UK Research and Innovation

Retrowave Neon 80's Background

Outline

1. Introduction & overview
2. Modelling satellite QKD
    - operation description
    - finite block sizes
    - SatQuMA: optimised finite key length software
3. Applications
    - system performance
    - expected annual SKL
    - protocol performance
4. Summary of work

J. Sidhu, T. Brougham, D. McArthur, R. Pousa, D. Oi, arXiv:2012.07829.

Introduction & Overview

Barrier to global networking

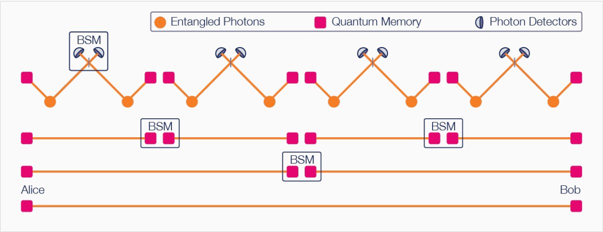
Max secret bits distributed over lossy channel: $< -\log_2(1-\eta) \sim 1.44\eta$.

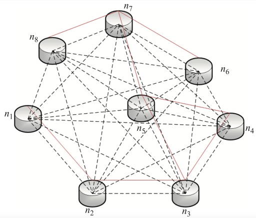
Barrier to global networking

Max secret bits distributed over lossy channel: $< -\log_2(1-\eta) \sim 1.44\eta$.

Can overcome limitation through:

- quantum repeaters
- multi-hop quantum networks





[1] *Front. Phys. 13(5), 130314 (2018).*

Barrier to global networking

Max secret bits distributed over lossy channel: $< -\log_2(1-\eta) \sim 1.44\eta$.

Can overcome limitation through:

- quantum repeaters
- multi-hop quantum networks

However, quantum repeaters have limitations

Barrier to global networking

Max secret bits distributed over lossy channel: $< -\log_2(1-\eta) \sim 1.44\eta$.

Can overcome limitation through:

- quantum repeaters
- multi-hop quantum networks

} repeater links with transmissivities η_i

$-\log_2(1 - \min_i \eta_i)$

However, quantum repeaters have limitations

- not experimentally feasible

Barrier to global networking

Max secret bits distributed over lossy channel: $< -\log_2(1-\eta) \sim 1.44\eta$.

Can overcome limitation through:

- quantum repeaters
- multi-hop quantum networks

} repeater links with transmissivities η_i

$-\log_2(1 - \min_i \eta_i)$

However, quantum repeaters have limitations

- not experimentally feasible
- some regions inaccessible - free space links required

Satellite quantum communications

Why satellites?

Satellite quantum communications

Why satellites?

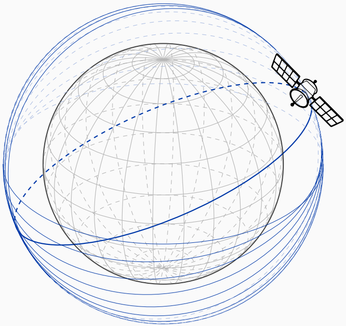
1. Overcome direct transmission limits

Satellite quantum communications

Why satellites?

1. Overcome direct transmission limits

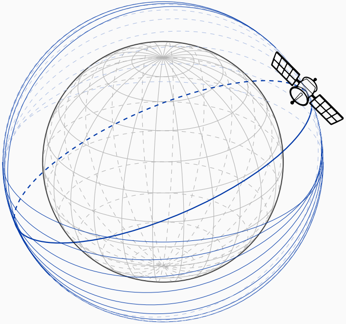
    - reduce demand on quantum repeaters

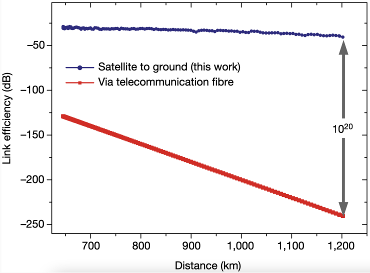


Satellite quantum communications

Why satellites?

1. Overcome direct transmission limits
    - reduce demand on quantum repeaters
    - less noise than ground links





[2] *Satellite-to-ground QKD, Nature* **549** *43 (2017).*
[3] *Network over 4,600 km, Nature* **589** *214 (2021).*

Satellite quantum communications

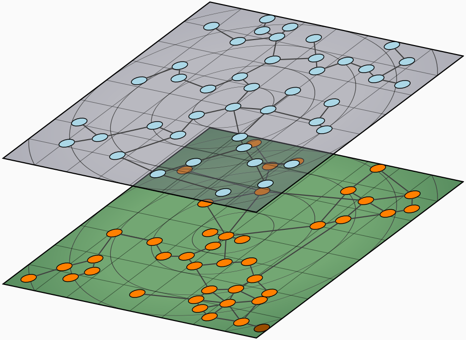
Why satellites?

1. Overcome direct transmission limits
    - reduce demand on quantum repeaters
    - less noise than ground links
2. Extend quantum networks

Satellite quantum communications

Why satellites?

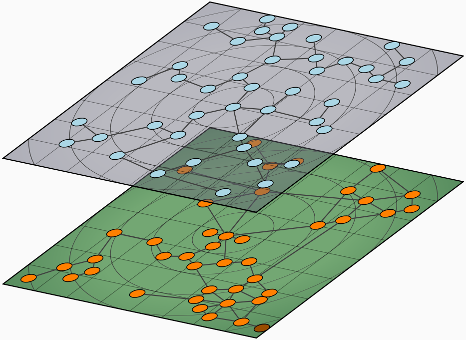
1. Overcome direct transmission limits
    - reduce demand on quantum repeaters
    - less noise than ground links
2. Extend quantum networks
    - uplink/downlink



Satellite quantum communications

Why satellites?

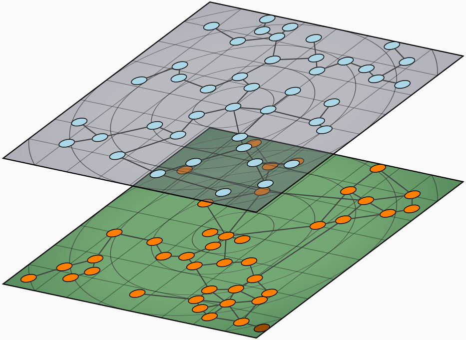
1. Overcome direct transmission limits
    - reduce demand on quantum repeaters
    - less noise than ground links
2. Extend quantum networks
    - uplink/downlink
    - inter-satellite links



Satellite quantum communications

Why satellites?

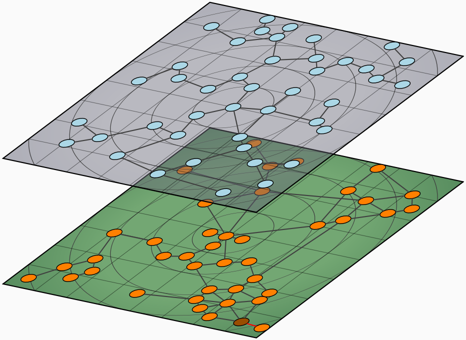
1. Overcome direct transmission limits
    - reduce demand on quantum repeaters
    - less noise than ground links
2. Extend quantum networks
    - uplink/downlink
    - inter-satellite links
    - efficient entanglement routing



Satellite quantum communications

Why satellites?

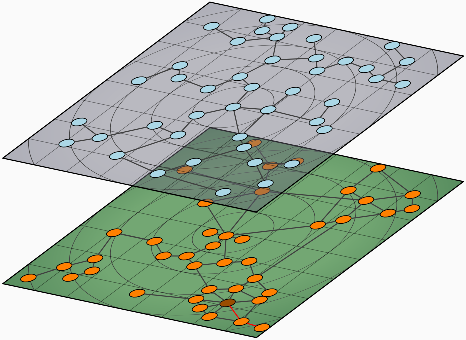
1. Overcome direct transmission limits
   - reduce demand on quantum repeaters
   - less noise than ground links
2. Extend quantum networks
   - uplink/downlink
   - inter-satellite links
   - efficient entanglement routing



Satellite quantum communications

Why satellites?

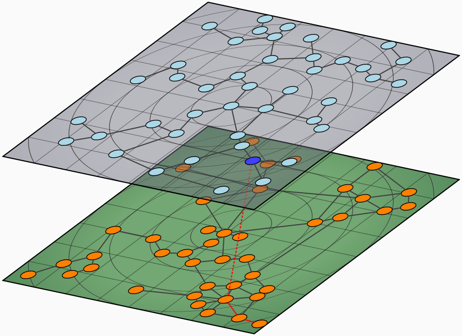
1. Overcome direct transmission limits
   - reduce demand on quantum repeaters
   - less noise than ground links
2. Extend quantum networks
   - uplink/downlink
   - inter-satellite links
   - efficient entanglement routing



Satellite quantum communications

Why satellites?

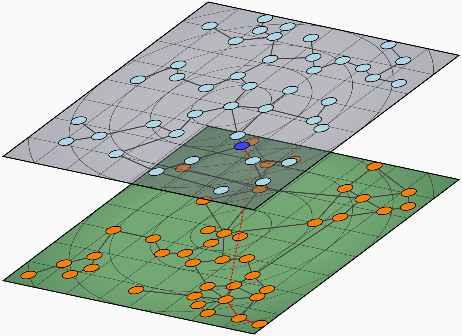
1. Overcome direct transmission limits
   - reduce demand on quantum repeaters
   - less noise than ground links
2. Extend quantum networks
   - uplink/downlink
   - inter-satellite links
   - efficient entanglement routing



Satellite quantum communications

Why satellites?

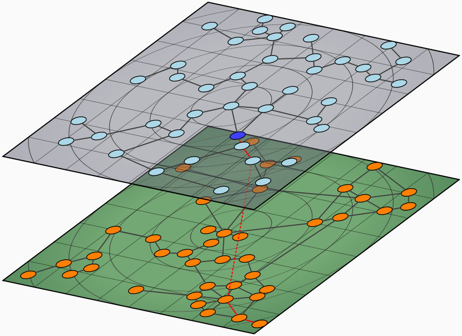
1. Overcome direct transmission limits
   - reduce demand on quantum repeaters
   - less noise than ground links
2. Extend quantum networks
   - uplink/downlink
   - inter-satellite links
   - efficient entanglement routing



Satellite quantum communications

Why satellites?

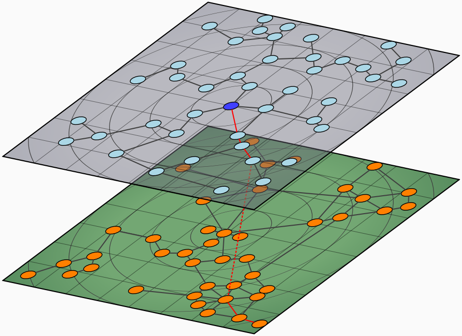
1. Overcome direct transmission limits
    - reduce demand on quantum repeaters
    - less noise than ground links
2. Extend quantum networks
    - uplink/downlink
    - inter-satellite links
    - efficient entanglement routing



Satellite quantum communications

Why satellites?

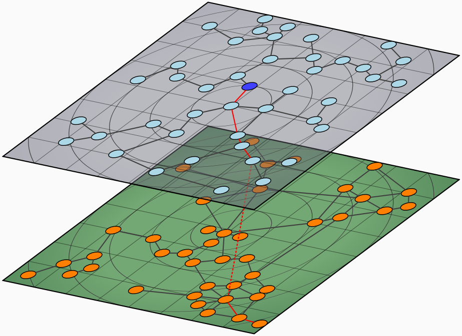
1. Overcome direct transmission limits
    - reduce demand on quantum repeaters
    - less noise than ground links
2. Extend quantum networks
    - uplink/downlink
    - inter-satellite links
    - efficient entanglement routing



Satellite quantum communications

Why satellites?

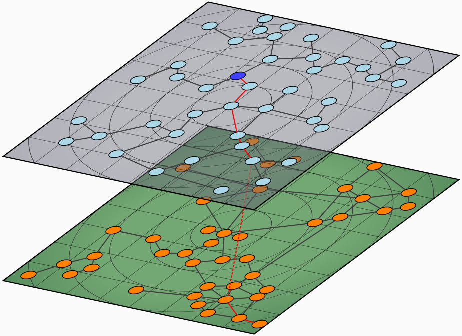
1. Overcome direct transmission limits
   - reduce demand on quantum repeaters
   - less noise than ground links
2. Extend quantum networks
   - uplink/downlink
   - inter-satellite links
   - efficient entanglement routing



Satellite quantum communications

Why satellites?

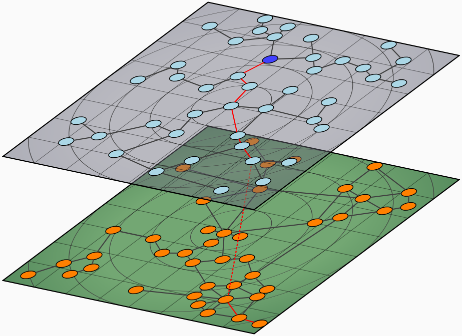
1. Overcome direct transmission limits
    - reduce demand on quantum repeaters
    - less noise than ground links
2. Extend quantum networks
    - uplink/downlink
    - inter-satellite links
    - efficient entanglement routing



Satellite quantum communications

Why satellites?

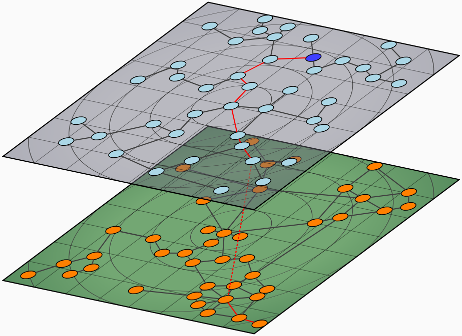
1. Overcome direct transmission limits
   - reduce demand on quantum repeaters
   - less noise than ground links
2. Extend quantum networks
   - uplink/downlink
   - inter-satellite links
   - efficient entanglement routing.



Satellite quantum communications

Why satellites?

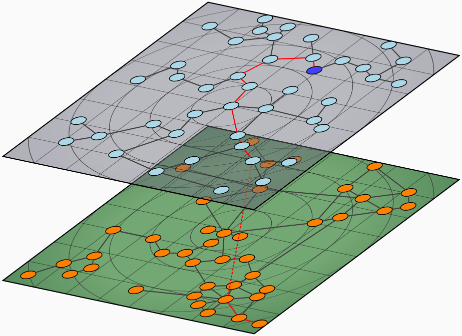
1. Overcome direct transmission limits
   - reduce demand on quantum repeaters
   - less noise than ground links
2. Extend quantum networks
   - uplink/downlink
   - inter-satellite links
   - efficient entanglement routing



Satellite quantum communications

Why satellites?

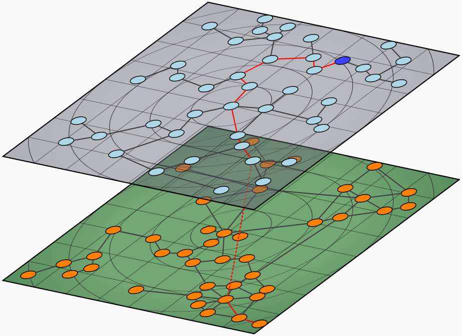
1. Overcome direct transmission limits
    - reduce demand on quantum repeaters
    - less noise than ground links
2. Extend quantum networks
    - uplink/downlink
    - inter-satellite links
    - efficient entanglement routing



Satellite quantum communications

Why satellites?

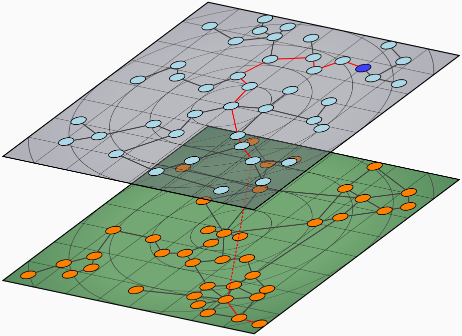
1. Overcome direct transmission limits
   - reduce demand on quantum repeaters
   - less noise than ground links
2. Extend quantum networks
   - uplink/downlink
   - inter-satellite links
   - efficient entanglement routing



Satellite quantum communications

Why satellites?

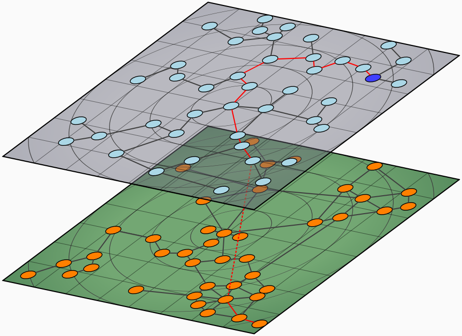
1. Overcome direct transmission limits
   - reduce demand on quantum repeaters
   - less noise than ground links
2. Extend quantum networks
   - uplink/downlink
   - inter-satellite links
   - efficient entanglement routing



Satellite quantum communications

Why satellites?

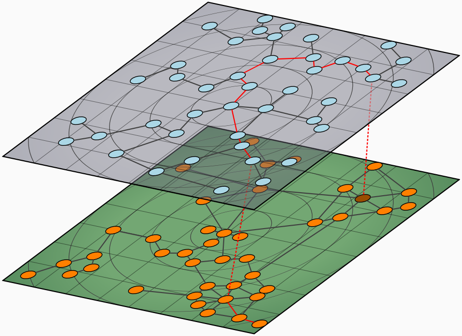
1. Overcome direct transmission limits
    - reduce demand on quantum repeaters
    - less noise than ground links
2. Extend quantum networks
    - uplink/downlink
    - inter-satellite links
    - efficient entanglement routing



Satellite quantum communications

Why satellites?

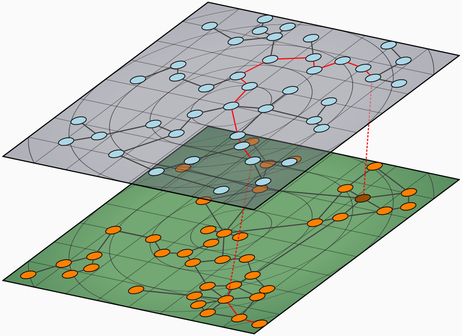
1. Overcome direct transmission limits
   - reduce demand on quantum repeaters
   - less noise than ground links
2. Extend quantum networks
   - uplink/downlink
   - inter-satellite links
   - efficient entanglement routing



Satellite quantum communications

Why satellites?

1. Overcome direct transmission limits
   - reduce demand on quantum repeaters
   - less noise than ground links
2. Extend quantum networks
   - uplink/downlink
   - inter-satellite links
   - efficient entanglement routing



Distributed quantum technologies.

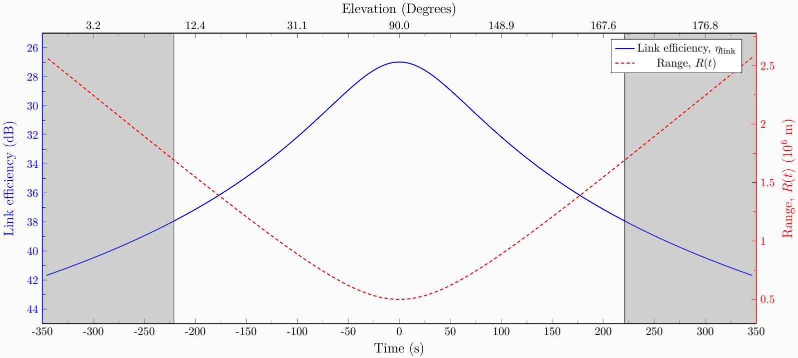
Modelling satellite QKD

SatQKD operation (I)

System link efficiency $\eta_{\text{link}}^{\text{sys}}$ characterises performance of SatQKD: satellite-OGS link efficiency at zenith.

SatQKD operation (I)

System link efficiency $\eta_{\text{link}}^{\text{sys}}$ characterises performance of SatQKD: satellite-OGS link efficiency at zenith.

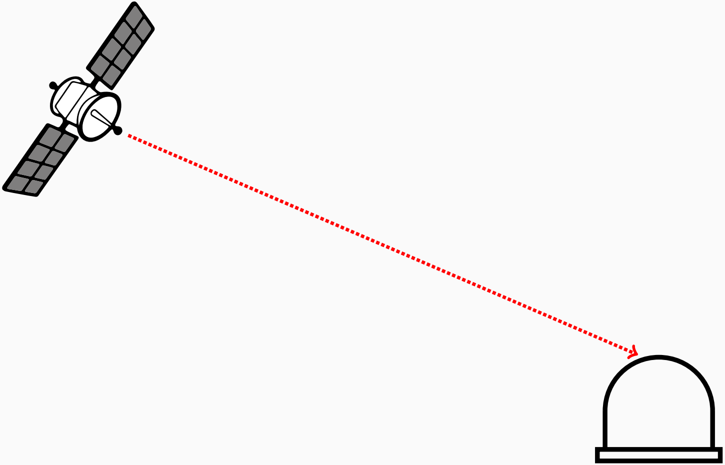


A baseline of $\eta_{\text{link}}^{\text{sys}} = 27$ dB is considered - empirical data from Micius.

4 *Entanglement-based secure quantum cryptography over 1,120 kilometres, Nature* **582***, 501 (2020).*

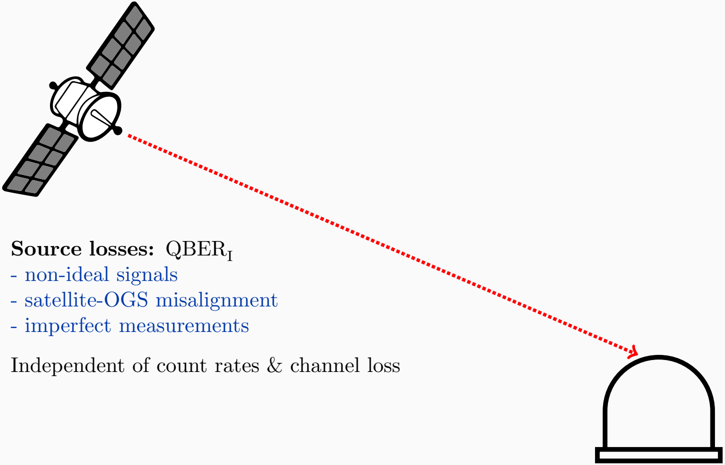
SatQKD operation (I)

System link efficiency $\eta_{\text{link}}^{\text{sys}}$ characterises performance of SatQKD: satellite-OGS link efficiency at zenith.



SatQKD operation (I)

System link efficiency $\eta_{\text{link}}^{\text{sys}}$ characterises performance of SatQKD: satellite-OGS link efficiency at zenith.



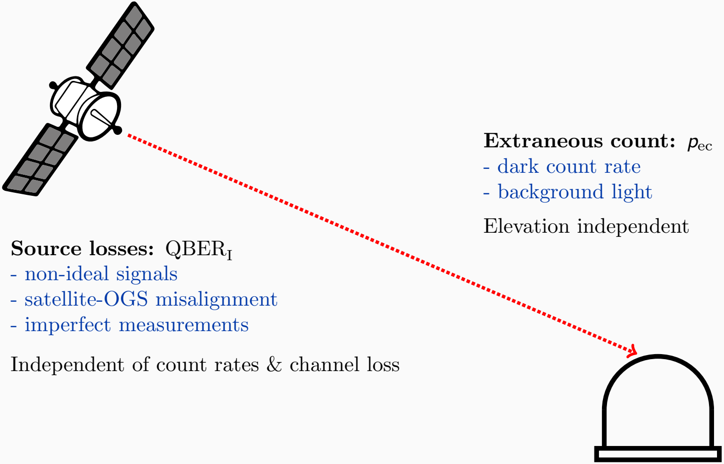
Source losses: QBER_{I}

- non-ideal signals
- satellite-OGS misalignment
- imperfect measurements

Independent of count rates & channel loss

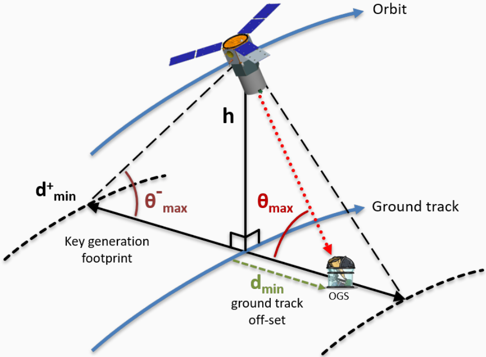
SatQKD operation (I)

System link efficiency $\eta_{\text{link}}^{\text{sys}}$ characterises performance of SatQKD: satellite-OGS link efficiency at zenith.



SatQKD operation (II)

General satellite overpass geometry for circular orbit of altitude h:



Single block:
$$\mathsf{SKL}_{\mathsf{finite}} = \mathsf{SKL}\left(\{n_k^\mu, m_k^\mu\}\right),$$

where $\{n_k^\mu, m_k^\mu\}$ = agglomerated counts without partitioning into sub-segments.

Finite key two-decoy state BB84

Three intensities μ_j with probabilities p_j, such that $\mu_1 > \mu_2 > \mu_3 = 0$:

Finite block secret key length (SKL)

$$\ell = s_{X,0} + s_{X,1}(1 - h(\phi_X)) - \lambda_{EC} - 6\log_2 \frac{21}{\epsilon_s} - \log_2 \frac{2}{\epsilon_c}$$

[4] *Concise security bounds for practical decoy-state quantum key distribution, Phys. Rev. A* **89***, 022307 (2014).*

Finite key two-decoy state BB84

Three intensities μ_j with probabilities p_j, such that $\mu_1 > \mu_2 > \mu_3 = 0$:

Finite block secret key length (SKL)

$$\ell = s_{X,0} + s_{X,1}(1 - h(\phi_X)) - \lambda_{EC} - 6\log_2 \frac{21}{\epsilon_s} - \log_2 \frac{2}{\epsilon_c}$$

Finite SKL determined from finite sample data block sizes

Finite key two-decoy state BB84

Three intensities μ_j with probabilities p_j, such that $\mu_1 > \mu_2 > \mu_3 = 0$:

Finite block secret key length (SKL)

$$\ell = s_{\mathrm{X},0} + s_{\mathrm{X},1}(1 - h(\phi_{\mathrm{X}})) - \lambda_{\mathrm{EC}} - 6\log_2 \frac{21}{\epsilon_{\mathrm{s}}} - \log_2 \frac{2}{\epsilon_{\mathrm{c}}}$$

Finite SKL determined from finite sample data block sizes

$$n^{\pm}_{\mathrm{X(Z)},k} = \frac{e^k}{p_k}\left[n_{\mathrm{X(Z)},k} \pm \delta^{\pm}_{n_{\mathrm{X(Z)},k}}\right],$$

Correction terms: $\delta^{+}_{Y} = \beta + \sqrt{2\beta y + \beta^2}, \quad \delta^{-}_{Y} = \frac{\beta}{2} + \sqrt{2\beta y + \frac{\beta^2}{4}}$

derived from inverse multiplicative Chernoff bounds with $\beta = \ln(1/\varepsilon)$.

[5] *Tight security bounds for decoy-state quantum key distribution, Sci. Rep.* **10**, *14312 (2020).*

Finite key two-decoy state BB84

Three intensities μ_j with probabilities p_j, such that $\mu_1 > \mu_2 > \mu_3 = 0$:

Finite block secret key length (SKL)

$$\ell = s_{X,0} + s_{X,1}(1 - h(\phi_X)) - \lambda_{EC} - 6\log_2 \frac{21}{\epsilon_s} - \log_2 \frac{2}{\epsilon_c}$$

Finite SKL determined from finite sample data block sizes

Photon yield

$s_{X,1}$

Photon event LB

Lim et al.

Finite key two-decoy state BB84

Three intensities μ_j with probabilities p_j, such that $\mu_1 > \mu_2 > \mu_3 = 0$:

Finite block secret key length (SKL)

$$\ell = s_{X,0} + s_{X,1}(1 - h(\phi_X)) - \lambda_{EC} - 6 \log_2 \frac{21}{\epsilon_s} - \log_2 \frac{2}{\epsilon_c}$$

Finite SKL determined from finite sample data block sizes

Photon yield

$s_{X,1}$

Photon event LB

Lim et al.

Vacuum yield

$s_{X,0}$

Vacuum events

Lim et al.

Finite key two-decoy state BB84

Three intensities μ_j with probabilities p_j, such that $\mu_1 > \mu_2 > \mu_3 = 0$:

Finite block secret key length (SKL)

$$\ell = s_{X,0} + s_{X,1}(1 - h(\phi_X)) - \lambda_{EC} - 6\log_2 \frac{21}{\epsilon_s} - \log_2 \frac{2}{\epsilon_c}$$

Finite SKL determined from finite sample data block sizes

Photon yield

$s_{X,1}$

Photon event LB

Lim et al.

Vacuum yield

$s_{X,0}$

Vacuum events

Lim et al.

Error correction

$\lambda_{EC} < \log|\mathcal{M}|$

Post-processing

Tomamichel et al.

Finite key two-decoy state BB84

Three intensities μ_j with probabilities p_j, such that $\mu_1 > \mu_2 > \mu_3 = 0$:

Finite block secret key length (SKL)

$$\ell = s_{X,0} + s_{X,1}(1 - h(\phi_X)) - \lambda_{EC} - 6 \log_2 \frac{21}{\epsilon_s} - \log_2 \frac{2}{\epsilon_c}$$

Finite SKL determined from finite sample data block sizes

Photon yield	Vacuum yield	Error correction

$$s_{X,1} = \frac{\tau_1 \mu_1 \left[n^-_{X,2} - n^+_{X,3} - \frac{\mu_2^2 - \mu_3^2}{\mu_1^2} \left(n^+_{X,1} - \frac{s_{X,0}}{\tau_0} \right) \right]}{\mu_1(\mu_2 - \mu_3) - \mu_2^2 + \mu_3^2}$$

Finite key two-decoy state BB84

Three intensities μ_j with probabilities p_j, such that $\mu_1 > \mu_2 > \mu_3 = 0$:

Finite block secret key length (SKL)

$$\ell = s_{\mathrm{X},0} + s_{\mathrm{X},1}(1 - h(\phi_{\mathrm{X}})) - \lambda_{\mathrm{EC}} - 6\log_2 \frac{21}{\epsilon_{\mathrm{s}}} - \log_2 \frac{2}{\epsilon_{\mathrm{c}}}$$

Finite SKL determined from finite sample data block sizes

Photon yield | Vacuum yield | Error correction

$$s_{\mathrm{X},0} \geq \tau_0 \frac{\mu_2 n^{-}_{\mathrm{X},\mu_3} - \mu_3 n^{+}_{\mathrm{X},\mu_2}}{\mu_2 - \mu_3}$$

Lower bound is tight when $\mu_3 \to 0$.

Finite key two-decoy state BB84

Three intensities μ_j with probabilities p_j, such that $\mu_1 > \mu_2 > \mu_3 = 0$:

Finite block secret key length (SKL)

$$\ell = s_{X,0} + s_{X,1}(1 - h(\phi_X)) - \lambda_{EC} - 6\log_2 \frac{21}{\epsilon_s} - \log_2 \frac{2}{\epsilon_c}$$

Finite SKL determined from finite sample data block sizes

Photon yield | Vacuum yield | Error correction

$$\begin{aligned}\lambda_{EC} =& n_X h(Q) + n_X(1-Q)\log\left[\frac{(1-Q)}{Q}\right] \\ & - \left(F^{-1}(\epsilon_c; n_X, 1-Q,) - 1\right)\log\left[\frac{(1-Q)}{Q}\right] - \frac{1}{2}\log(n_X) - \log(1/\epsilon_c)\end{aligned}$$

[6] *Fundamental finite key limits for one-way information reconciliation in quantum key distribution, Quant. Inf. Proc.,* **16** *280 (2017).*

Transmission time optimisation

Overpass transmission time optimisation is important

Transmission time optimisation

Overpass transmission time optimisation is important

1. highly variable channel loss

Transmission time optimisation

Overpass transmission time optimisation is important

1. highly variable channel loss
    - expected observed statistics vary

Transmission time optimisation

Overpass transmission time optimisation is important

1. highly variable channel loss
   - expected observed statistics vary
   - data from low elevations has small count rate and high QBER.

Transmission time optimisation

Overpass transmission time optimisation is important

1. highly variable channel loss
   - expected observed statistics vary
   - data from low elevations has small count rate and high QBER.

2. optimise SKL by truncating poorer quality data

Transmission time optimisation

Overpass transmission time optimisation is important

1. highly variable channel loss
    - expected observed statistics vary
    - data from low elevations has small count rate and high QBER.
2. optimise SKL by truncating poorer quality data
    - trade-off block size with data quality.

Transmission time optimisation

Overpass transmission time optimisation is important

Transmission time optimisation

Overpass transmission time optimisation is important

Transmission time optimisation

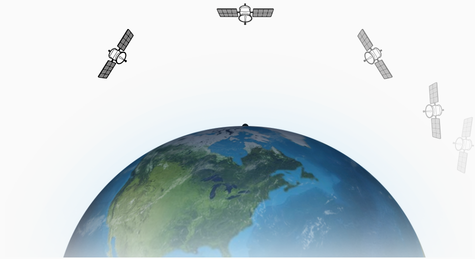
Overpass transmission time optimisation is important

Transmission time optimisation

Overpass transmission time optimisation is important

Transmission time optimisation

Overpass transmission time optimisation is important



Transmission time optimisation

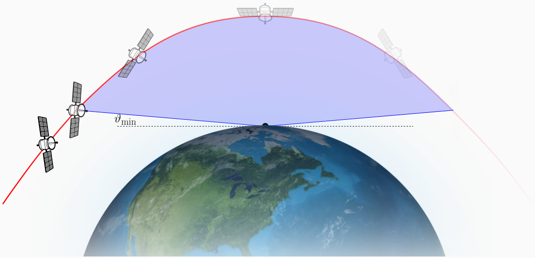
Overpass transmission time optimisation is important

Transmission time optimisation

Overpass transmission time optimisation is important

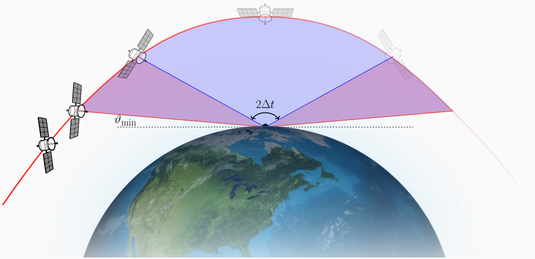
Transmission time optimisation

Overpass transmission time optimisation is important



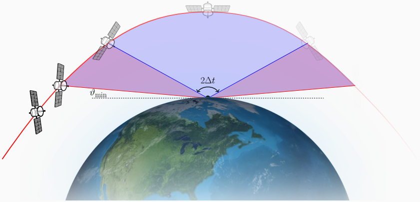
Transmission time optimisation

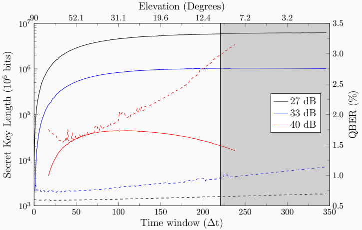
Overpass transmission time optimisation is important



Transmission time optimisation

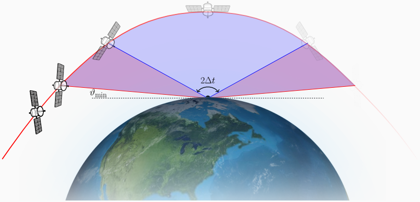
Overpass transmission time optimisation is important

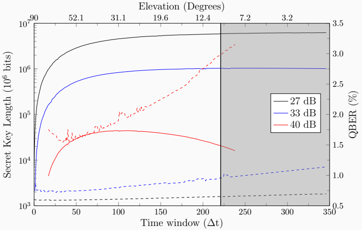




Transmission time optimisation

Overpass transmission time optimisation is important

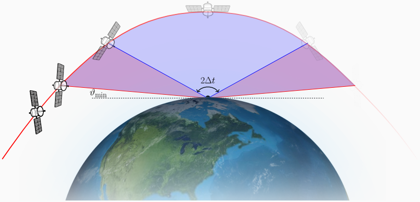


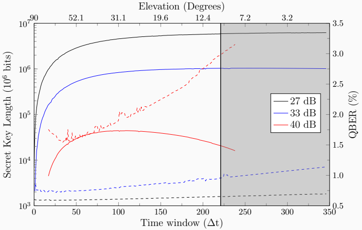


Low $\eta_{\text{link}}^{\text{sys}}$: construct keys using greatest amount of data (max Δt).

Transmission time optimisation

Overpass transmission time optimisation is important



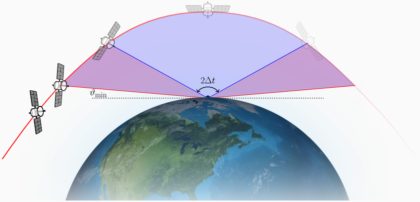


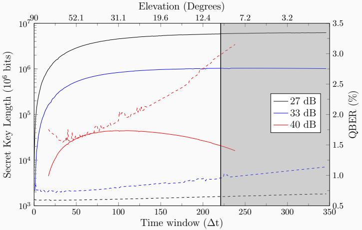
Low $\eta_{\text{link}}^{\text{sys}}$: construct keys using greatest amount of data (max Δt).

High $\eta_{\text{link}}^{\text{sys}}$: use only data around zenith

Transmission time optimisation

Overpass transmission time optimisation is important





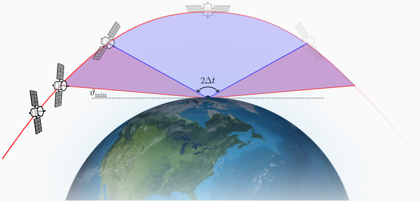
Low $\eta_{\text{link}}^{\text{sys}}$: construct keys using greatest amount of data (max Δt).

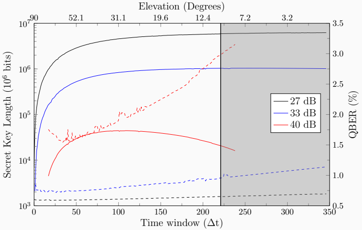
High $\eta_{\text{link}}^{\text{sys}}$: use only data around zenith

- better average QBER

Transmission time optimisation

Overpass transmission time optimisation is important





Low $\eta_{\text{link}}^{\text{sys}}$: construct keys using greatest amount of data (max Δt).

High $\eta_{\text{link}}^{\text{sys}}$: use only data around zenith

- better average QBER
- counters smaller raw key length and larger statistical uncertainties.

Optimised finite key length

Maximise SKL over parameter space:

https://github.com/cnqo-qcomms/SatQuMA.

Optimised finite key length

Maximise SKL over parameter space:

Optimised finite key length, ℓ

$$\begin{aligned} \underset{p_X, \mu_1, \mu_2, p_1, p_2, \Delta t}{\text{maximize}} \quad & s_{X,0} + s_{X,1}(1 - h(\phi_X)) - \lambda_{EC} - 6 \log_2 \frac{21}{\epsilon_s} - \log_2 \frac{2}{\epsilon_c} \\ \text{subject to} \quad & 0 < \{p_X, p_j\} < 1, \\ & 0 < \{\mu_1, \mu_2\} < 1, \\ & \mu_1 > \mu_2 > \mu_3, \\ & 0 < \Delta t \leq t(10^\circ) \end{aligned}$$

https://github.com/cnqo-qcomms/SatQuMA.

Optimised finite key length

Maximise SKL over parameter space:

Finite key effects in satellite quantum key distribution

Jasminder S. Sidhu,* Thomas Brougham,† Duncan McArthur,‡ Roberto G. Pousa,§ and Daniel K. L. Oi¶
SUPA Department of Physics, University of Strathclyde, Glasgow, G4 0NG, United Kingdom
(Dated: 26th April 2021)

Global quantum communications will enable long-distance secure data transfer, networked distributed quantum information processing, and other entanglement-enabled technologies. Satellite quantum communication overcomes optical fibre range limitations, with the first realisations of satellite quantum key distribution (SatQKD) being rapidly developed. However, limited transmission times between satellite and ground station severely constrains the amount of secret key due to finite-block size effects. Here, we analyse these effects and the implications for system design and operation, utilising published results from the Micius satellite to construct an empirically-derived channel and system model for a trusted-node downlink employing efficient BB84 weak coherent pulse decoy states with optimised parameters. We quantify practical SatQKD performance limits and examine the effects of link efficiency, background light, source quality, and overpass geometries to estimate long-term key generation capacity. Our results may guide design and analysis of future missions, and establish performance benchmarks for both sources and detectors.

https://github.com/cnqo-qcomms/SatQuMA.

Optimised finite key length

Maximise SKL over parameter space:

https://github.com/cnqo-qcomms/SatQuMA.

Optimised finite key length

Maximise SKL over parameter space:

Satellite Quantum Modelling & Analysis Software

https://github.com/cnqo-qcomms/SatQuMA.

Optimised finite key length

Maximise SKL over parameter space:

SatQuMA

Satellite Quantum Modelling & Analysis Software

- toolkit to model satellite QKD

https://github.com/cnqo-qcomms/SatQuMA.

Optimised finite key length

Maximise SKL over parameter space:

Satellite Quantum Modelling & Analysis Software

- toolkit to model satellite QKD
- available to download on GitHub

https://github.com/cnqo-qcomms/SatQuMA.

Applications

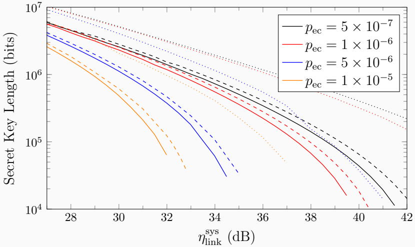
Relative system performance

Variation in SKL with p_{ec} and QBER_I:

Relative system performance

Variation in SKL with p_{ec} and QBER_I:

Extraneous count probability

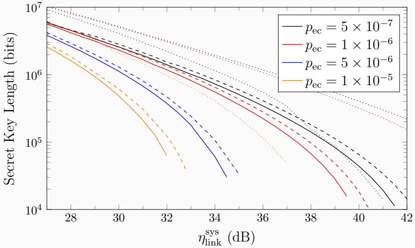


- p_{ec} changes vacuum yield $s_{\text{X},0}$
- worse phase error/error correction
- p_{ec} at high $\eta_{\text{link}}^{\text{sys}}$ gives zero SKL due to excessive QBER.

Relative system performance

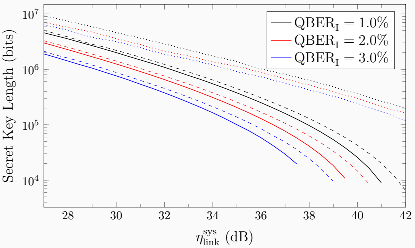
Variation in SKL with p_{ec} and QBER_I:

Extraneous count probability



- p_{ec} changes vacuum yield $s_{X,0}$
- worse phase error/error correction
- p_{ec} at high $\eta_{\mathrm{link}}^{\mathrm{sys}}$ gives zero SKL due to excessive QBER.

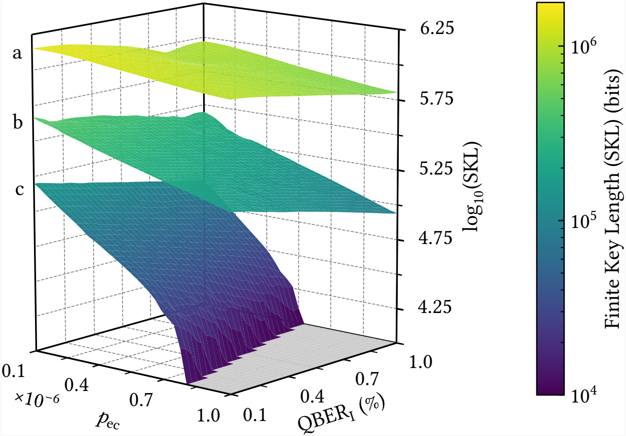
Intrinsic QBER



- affects observed count rates
- SKL more robust to changes in $\mathrm{QBER_I}$
- Focus on decreasing p_{ec}.

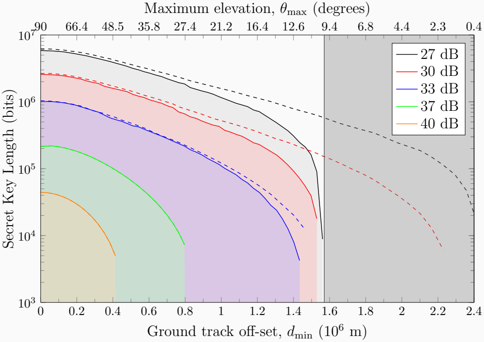
Relative system performance

Variation in SKL with p_{ec} and $QBER_I$:

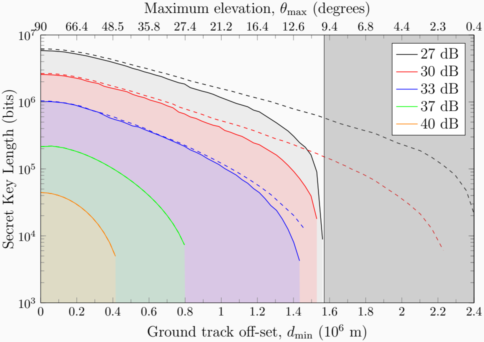


Improve background light suppression and detector dark counts over source fidelities and satellite alignment.

Expected annual finite key



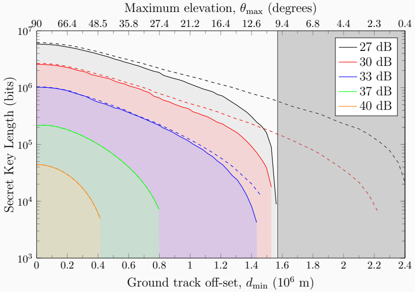
Expected annual finite key



Annual key: $$\overline{\mathsf{SKL}}_{\text{year}} = N_{\text{orbits}}^{\text{year}} \frac{\mathsf{SKL}_{\text{int}}}{L_{\text{lat}}},$$

where $N_{\text{orbits}}^{\text{year}}$ is the number of orbits per year, and L_{lat} is the longitudinal circumference along the line of latitude at the OGS location.

Expected annual finite key



$\eta_{\text{link}}^{\text{sys}}$	SKL_{int}	$\overline{\text{SKL}}_{\text{year}}^{55.9^\circ\text{N}}$
27 dB	3.74×10^{12} bm	0.9131 Gb
30 dB	1.52×10^{12} bm	0.3720 Gb
33 dB	5.40×10^{11} bm	0.1318 Gb
37 dB	8.75×10^{10} bm	0.0214 Gb
40 dB	1.13×10^{10} bm	0.0028 Gb

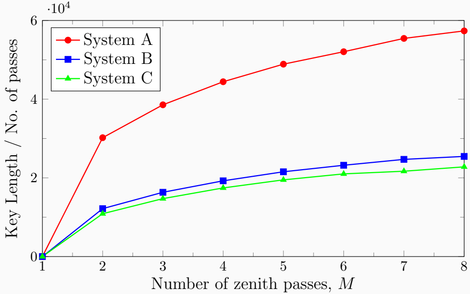
Annual key:

$$\overline{\text{SKL}}_{\text{year}} = N_{\text{orbits}}^{\text{year}} \frac{\text{SKL}_{\text{int}}}{L_{\text{lat}}},$$

where $N_{\text{orbits}}^{\text{year}}$ is the number of orbits per year, and L_{lat} is the longitudinal circumference along the line of latitude at the OGS location.

Multiple satellite passes

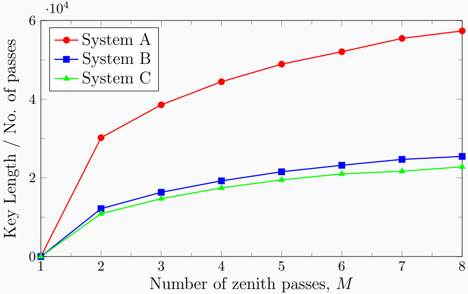
Data from several overpasses can be combined to improve SKL generation



System	$\eta_{\text{link}}^{\text{sys}}$	p_{ec}	QBER_{I}
A	45.7 dB	10^{-7}	0.5%
B	44.8 dB	10^{-7}	0.5%
C	40.5 dB	5×10^{-7}	1%

Multiple satellite passes

Data from several overpasses can be combined to improve SKL generation



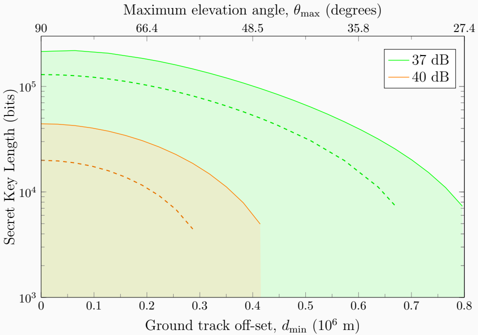
System	$\eta_{\text{link}}^{\text{sys}}$	p_{ec}	QBER_{I}
A	45.7 dB	10^{-7}	0.5%
B	44.8 dB	10^{-7}	0.5%
C	40.5 dB	5×10^{-7}	1%

Systems with zero single-overpass SKL can generate key from M overpasses:

- $\ell_M \geq M\ell_1$ with diminishing improvement $\ell_{M+1} - \ell_M$ with increasing M
- smaller estimation uncertainties from increased sample size
- greater latency leads to potential security vulnerabilities.

Protocol performance

Efficient BB84 performs better than standard BB84 in asymptotic regime.



Asymmetric BB84 delivers more finite key than symmetric BB84

- Improvement of 3 dB gives 7.6 times more annual key volume
- better sifting ratio and longer raw key length
- better handling of parameter estimation.

Summary of work

In summary ...

1. Numerical toolkit to benchmark system performance for SatQKD
2. SatQKD systems should prioritise background light suppression over higher intrinsic quantum signal visibilities or extending transmission
3. Efficient BB84 provides larger operation footprint than conventional BB84
4. secret key extraction efficiency enhanced by combining data blocks from several passes.

J. Sidhu, T. Brougham, D. McArthur, R. Pousa, D. Oi, arXiv:2012.07829.

In summary ...

1. Numerical toolkit to benchmark system performance for SatQKD
2. SatQKD systems should prioritise background light suppression over higher intrinsic quantum signal visibilities or extending transmission
3. Efficient BB84 provides larger operation footprint than conventional BB84
4. secret key extraction efficiency enhanced by combining data blocks from several passes.

Future work:

1. More comprehensive constraints to reflect additional restrictions on system operations and deployment
2. Incorporate orbital modelling of constellations with cost/performance trade-off studies.

J. Sidhu, T. Brougham, D. McArthur, R. Pousa, D. Oi, arXiv:2012.07829.

Thank you for your attention!