Realistic Threat Models in Satellite-Based QKD

M Ghalaii[1,2], S Bahrani[3], Carlo Liorni[4], Federico Grasselli[4], Hermann Kampermann[4], Lewis Wooltorton[2,3], Rupesh Kumar[2], Stefano Pirandola[2], Timothy P. Spiller[2], Alexander Ling[5], Bruno Huttner[6], and Mohsen Razavi[1]

[1] University of Leeds
[2] University of York
[3] University of Bristol
[4] University of Dusseldorf
[5] National University of Singapore
[6] ID Quantique

Available at:
arXiv:2212.04807

Quantum Key Distribution (QKD)

key

1001100
0101011
0100010
110 …

……. …….

key

1001100
0101011
0100010
110 …

Alice
Eve
Bob

- <span>Challenge:</span> our existing techniques for sharing a secret key, based on public key cryptography, can be broken by quantum computers. How shall we distribute a key securely in the quantum era?
- Solution: Instead of computational complexity, let us rely on the laws of physics as we understand them by Quantum Mechanics!

Quantum Key Distribution (QKD)

key

1001100
0101011
0100010
110 …

……. …….

key

1001100
0101011
0100010
110 …

Alice

Eve

Bob

- Challenge: our existing techniques for sharing a secret key, based on public key cryptography, can be broken by quantum computers. How shall we distribute a key securely in the quantum era?

- Solution: Instead of computational complexity, let us rely on the laws of physics as we understand them by Quantum Mechanics!

- Key Feature: Any eavesdropping attempt can be detected and its impact quantified.

QKD: Security Assumptions

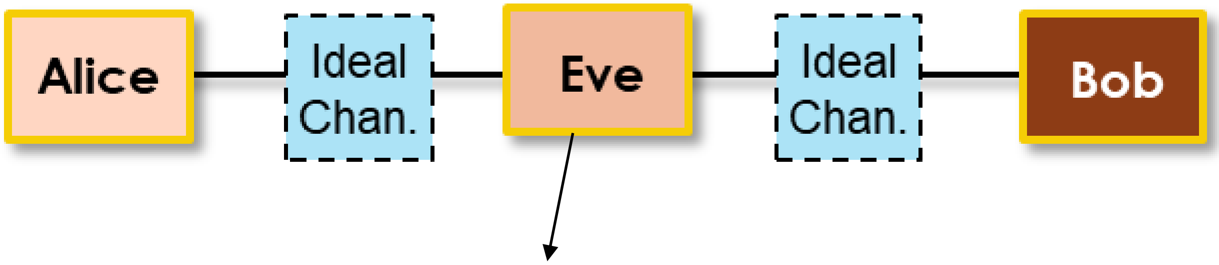
- QKD security proofs are based on the assumption that

Eve has full access to the channel

1- She can collect Alice’s signal in full and send whatever she wants to Bob

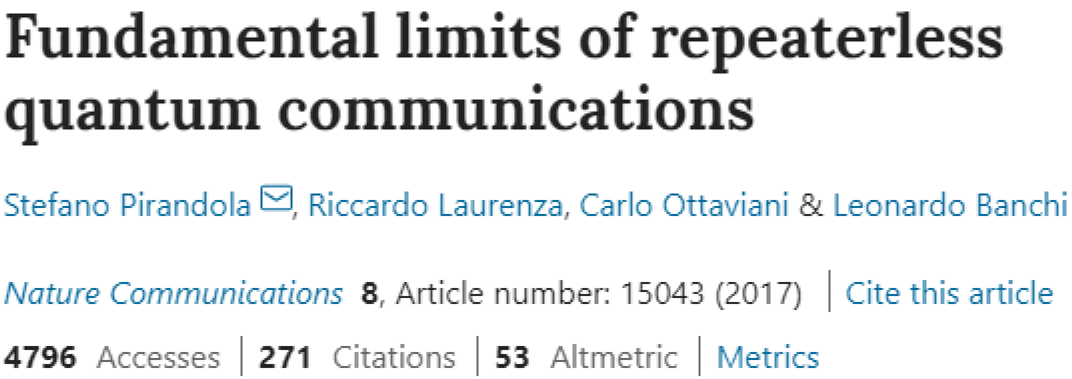
2- Alice and Bob make no assumption on the channel; they just rely on their measurement results to bound the leaked information to Eve

Unrestricted Eavesdropping



Bound by Qu. Mech.

How far you can go without a repeater?



Fundamental limits of repeaterless quantum communications

Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani & Leonardo Banchi

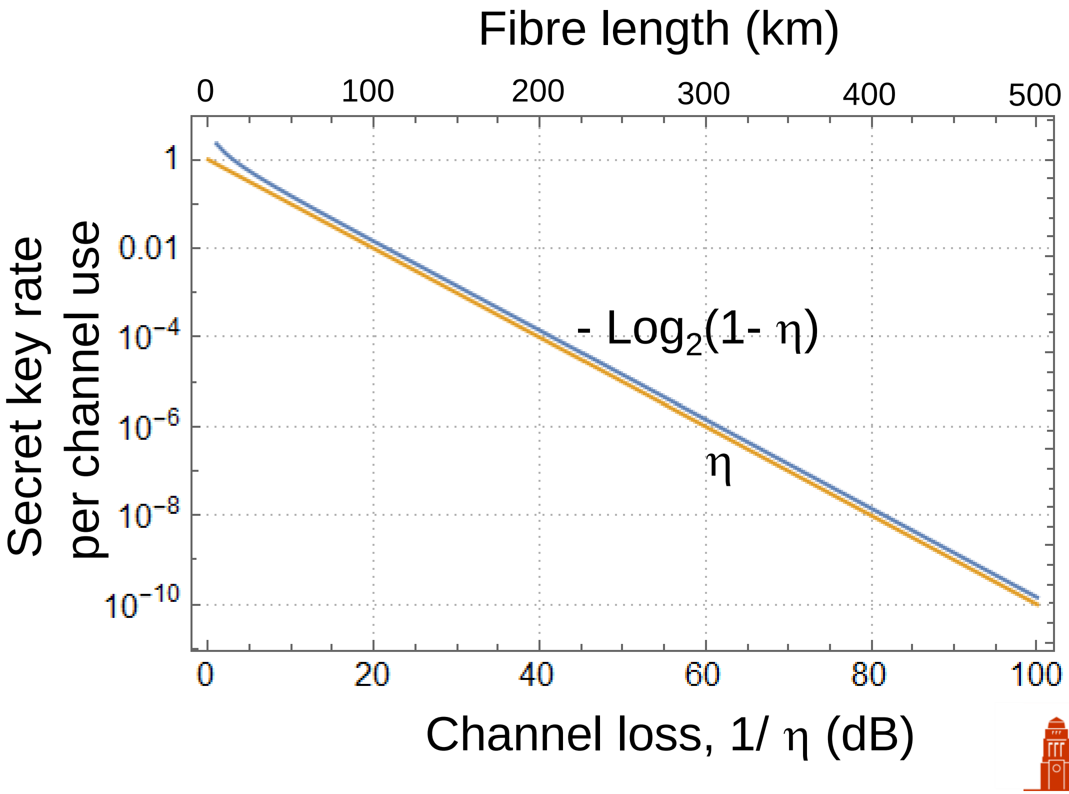
Nature Communications **8**, Article number: 15043 (2017) | Cite this article

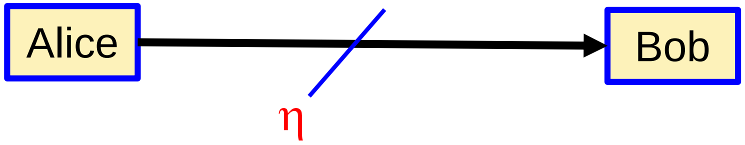
4796 Accesses | **271** Citations | **53** Altmetric | Metrics

QKD as a benchmarking tool

PLOB Bound:
The secret key rate in a repeaterless lossy channel with transmissivity η is bounded by

$-\mathrm{Log}_2(1-\eta)$

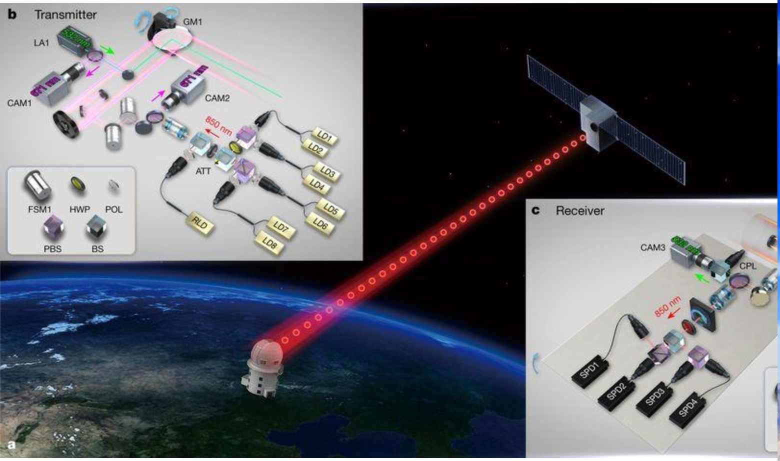




Satellite-based QKD

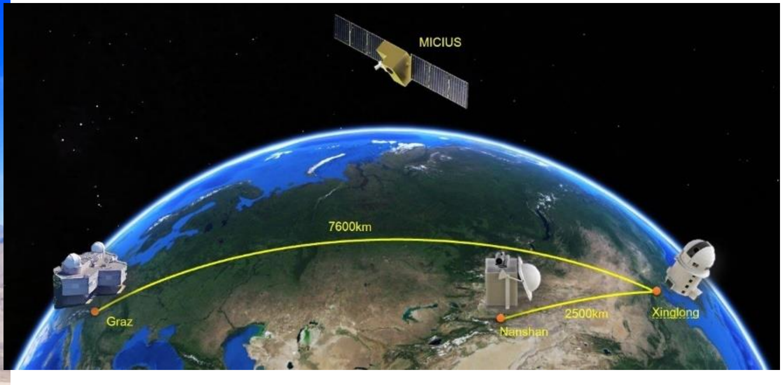
- First QKD satellite, Micius, in orbit!
- 3 breakthrough experiments:
  - QKD between satellite and ground station
  - Teleportation
  - QKD between two cities 7600 km apart

[Nature **549,** 43 (2017)]



[Nature **549,** 70 (2017)]

[PRL **120,** 030501 (2018)]



Satellite-based QKD: Challenges

- First QKD satellite, Micius, in orbit!
- 3 breakthrough experiments:
  - QKD between satellite and ground station
  - Teleportation
  - QKD between two cities 7600 km apart
- Not without limitations
  - Right now, definitely expensive
  - For LEO satellites, you have about 5 minutes to exchange keys → you need a constellation → even more ambitious
  - Day light could kill you; so far only night operation
  - Weather dependent
  - Not everyone has a large telescope; but such ground stations can be part of the trusted node network
  - The satellite would remain a trusted node in most practical cases

- Can we do anything to better capitalize on the investment will make in the space?

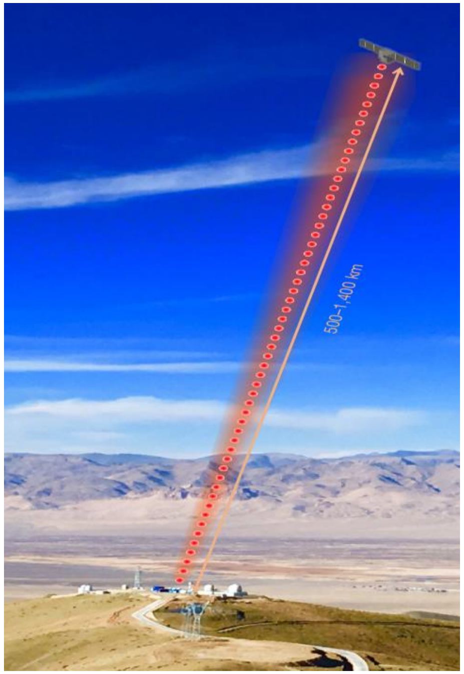
QKD: Strict vs Restricted Security Assumptions

- Strict assumptions in QKD (generous for Eve!)
  - Eve has full access to the channel:

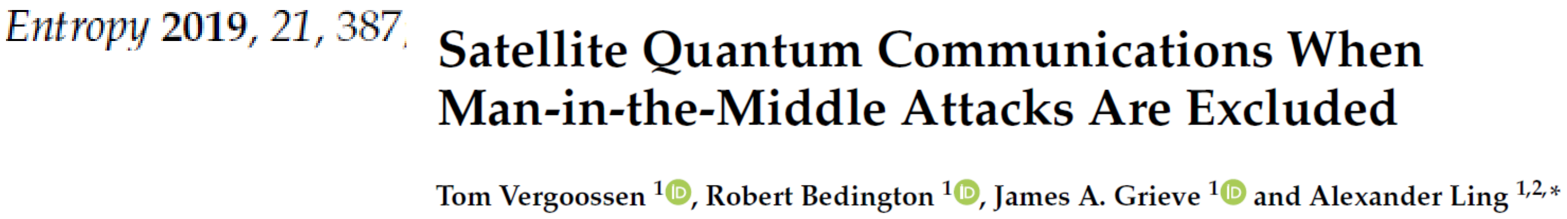
    1- She can collect Alice’s signal in full and send whatever she wants to Bob

    2- Alice and Bob make no assumption on the channel; they just rely on their measurement results to bound the leaked information to Eve

- But, can we relax some of these assumptions for line-of-sight satellite links?



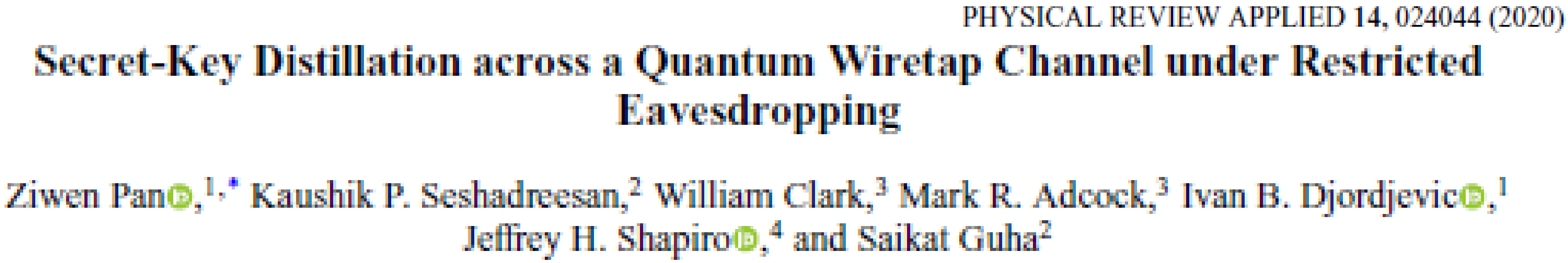
QKD over a Wiretap Channel



Entropy **2019**, *21*, 387

Satellite Quantum Communications When Man-in-the-Middle Attacks Are Excluded

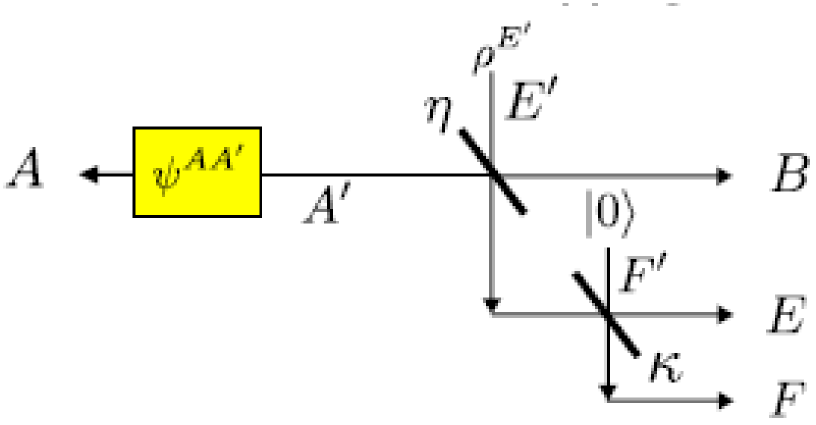
Tom Vergoossen [1], Robert Bedington [1], James A. Grieve [1] and Alexander Ling [1,2,*]

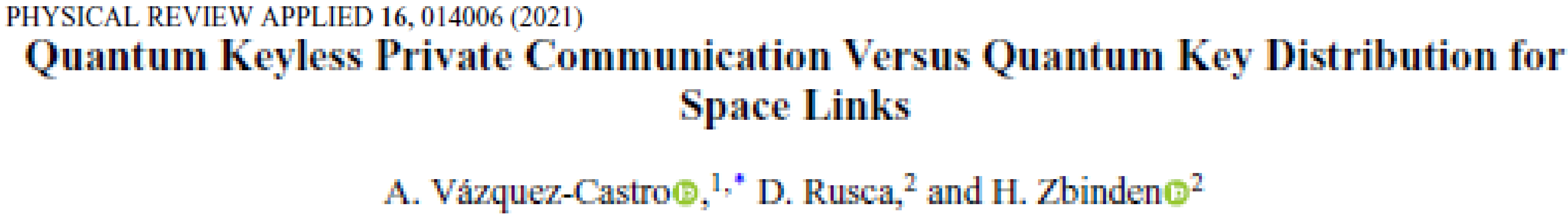


PHYSICAL REVIEW APPLIED **14**, 024044 (2020)

Secret-Key Distillation across a Quantum Wiretap Channel under Restricted Eavesdropping

Ziwen Pan,[1,*] Kaushik P. Seshadreesan,[2] William Clark,[3] Mark R. Adcock,[3] Ivan B. Djordjevic,[1] Jeffrey H. Shapiro,[4] and Saikat Guha[2]





PHYSICAL REVIEW APPLIED **16**, 014006 (2021)

Quantum Keyless Private Communication Versus Quantum Key Distribution for Space Links

A. Vázquez-Castro,[1,*] D. Rusca,[2] and H. Zbinden[2]

QKD: Strict vs Restricted Security Assumptions

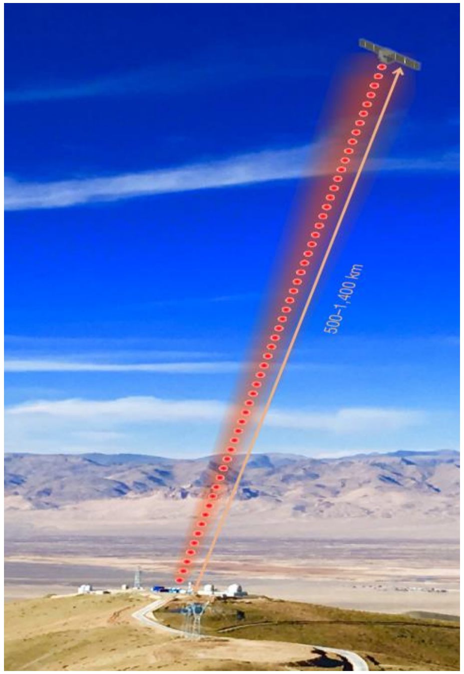
- Strict assumptions in QKD
  - Eve has full access to the channel:

    1- She can collect Alice's signal in full and send whatever she wants to Bob

    2- Alice and Bob make no assumption on the channel; they just rely on their measurement results to bound the leaked information to Eve

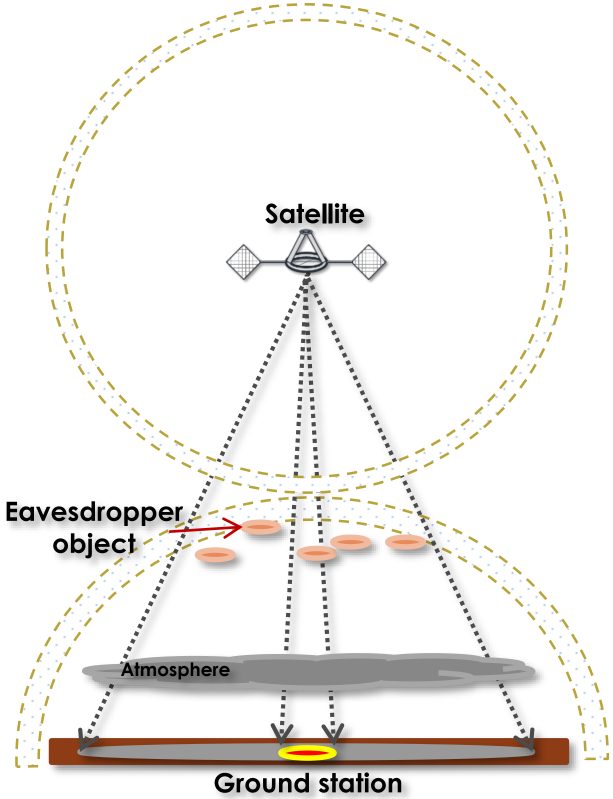
- But, can we relax some of these assumptions for line-of-sight satellite links?

- What if we have a monitoring system that could alert us to eavesdropping objects?

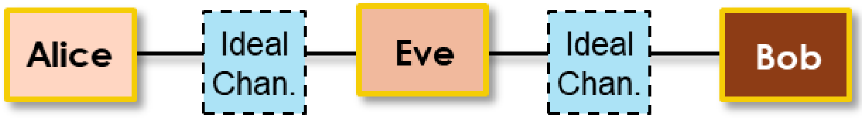


Satellite QKD with Restricted Eve

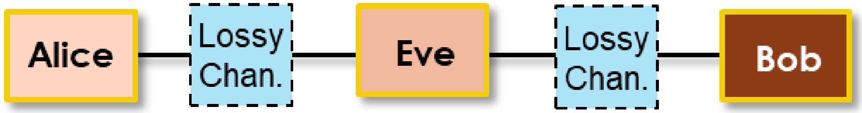
- **Monitoring assumptions:** With detection systems, such as Lidar or certain imaging systems, Alice and Bob can possibly rule out the presence of eavesdropping objects of a certain size within a distance
- This could limit the size of Eve’s collection antennas and/or her resend capability for active eavesdropping



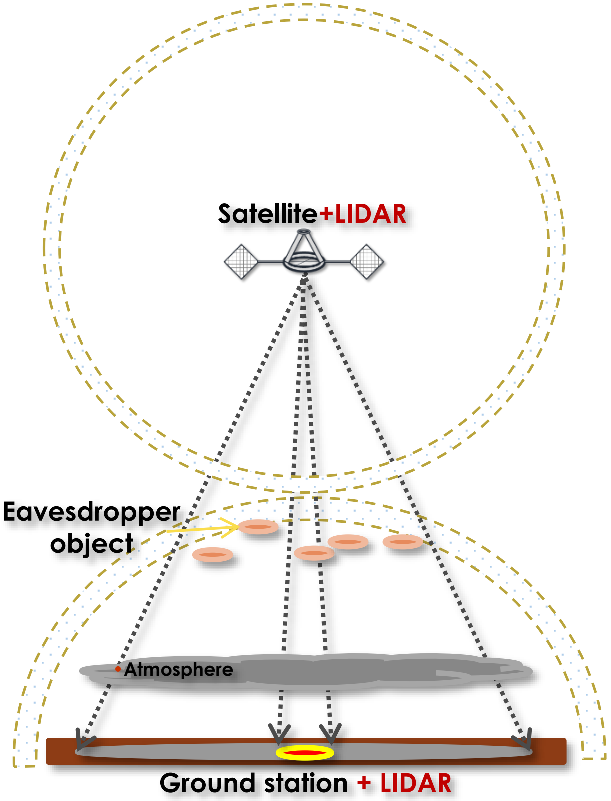
- **Unrestricted Eavesdropping**



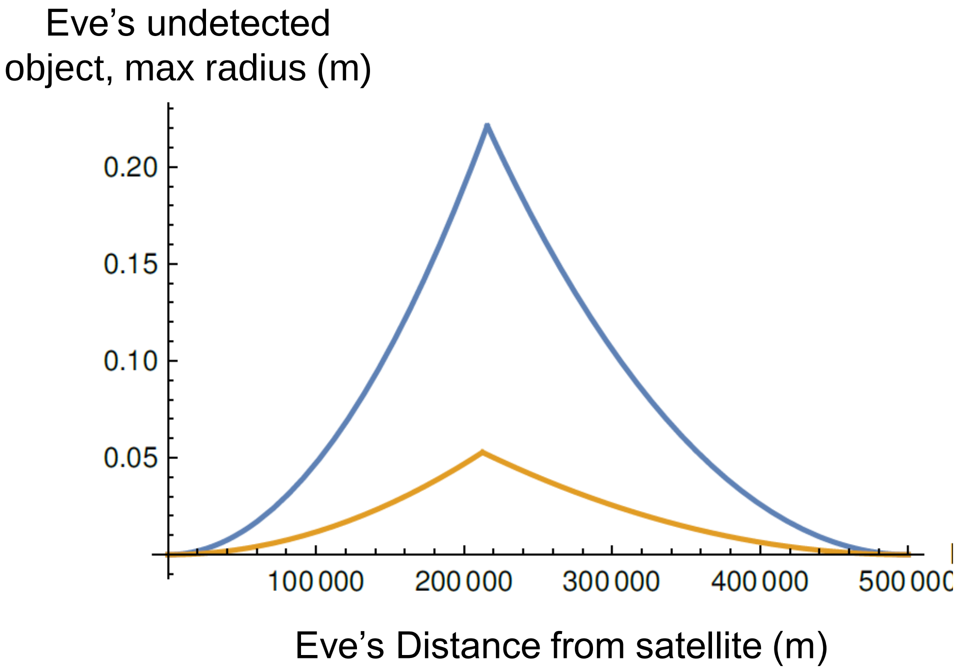
- **Restricted Eavesdropping**



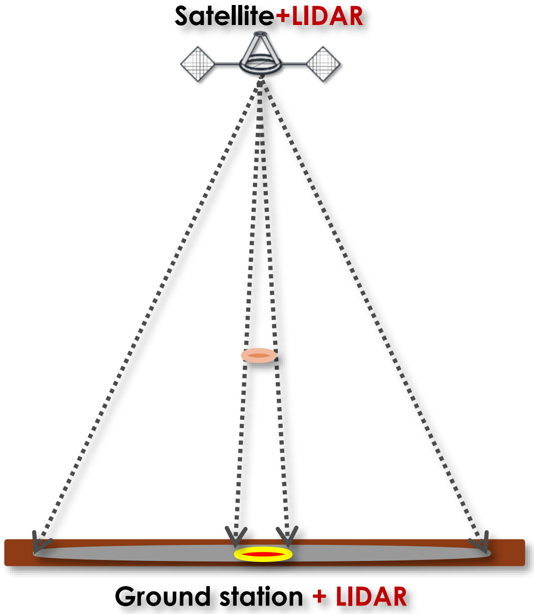
Eve’s Detection by LIDAR

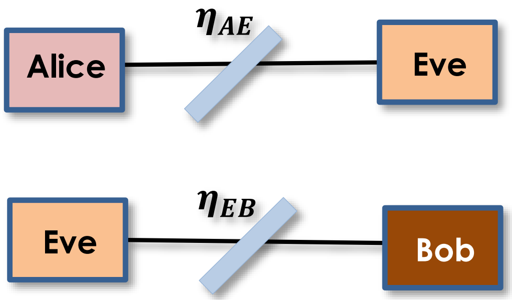


LIDAR with 1W TX power; satellite telescope diam: 30 cm; ground station diam: 1m; Sensitivity tuned to night-time background noise; Eve’s reflectivity (isotropic) = 0.1

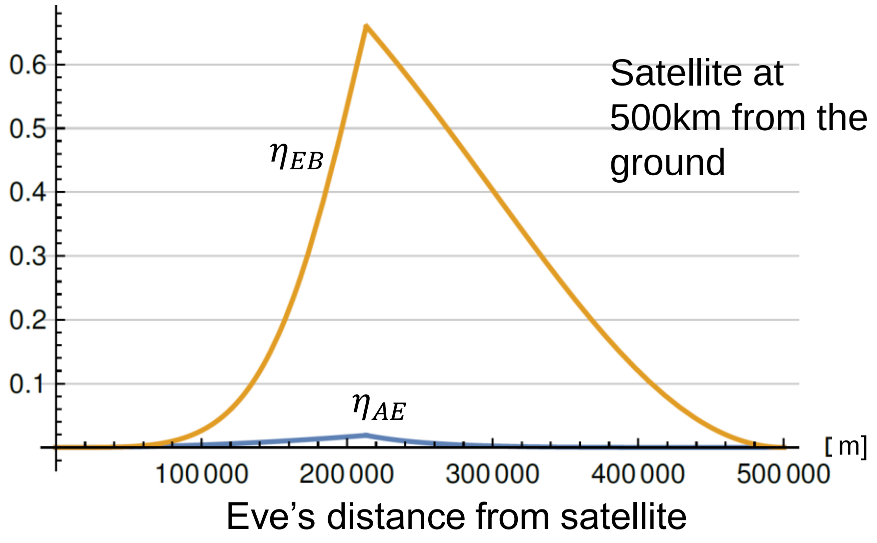


Eve’s Detection by LIDAR

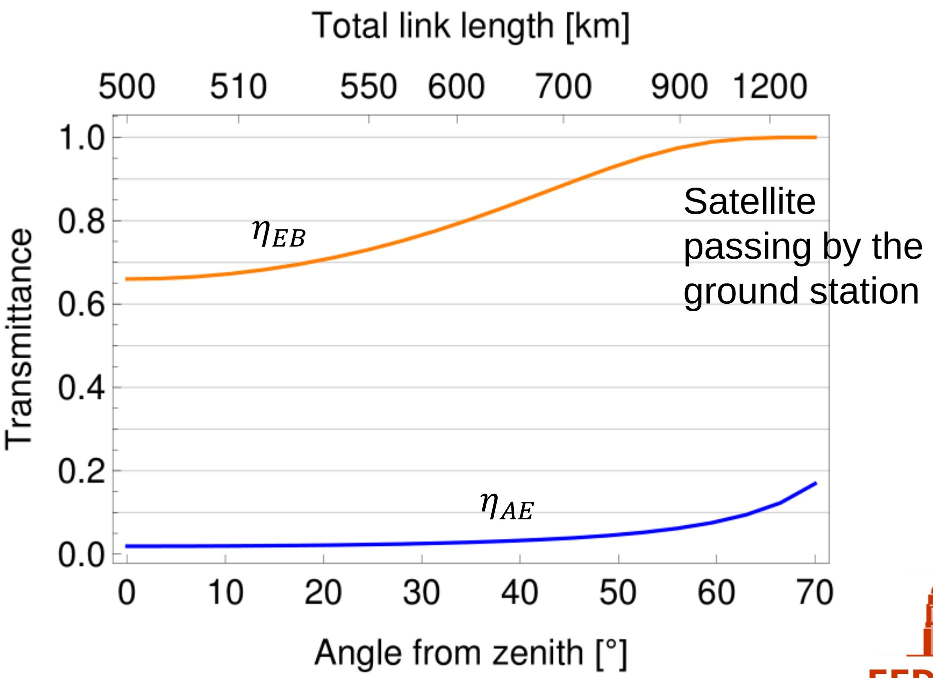




LIDAR with 4W TX power; satellite telescope diam: 30cm; ground station diam: 1m; Sensitivity tuned to night-time background noise; Eve’s reflectivity (isotropic) = 0.1



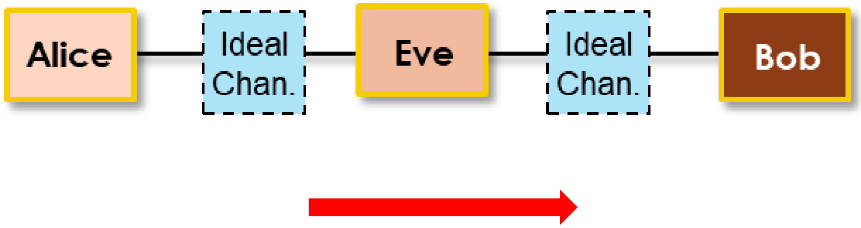
Satellite at 500km from the ground



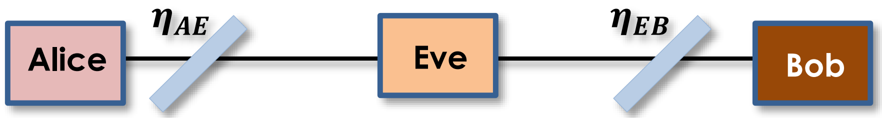
Satellite passing by the ground station

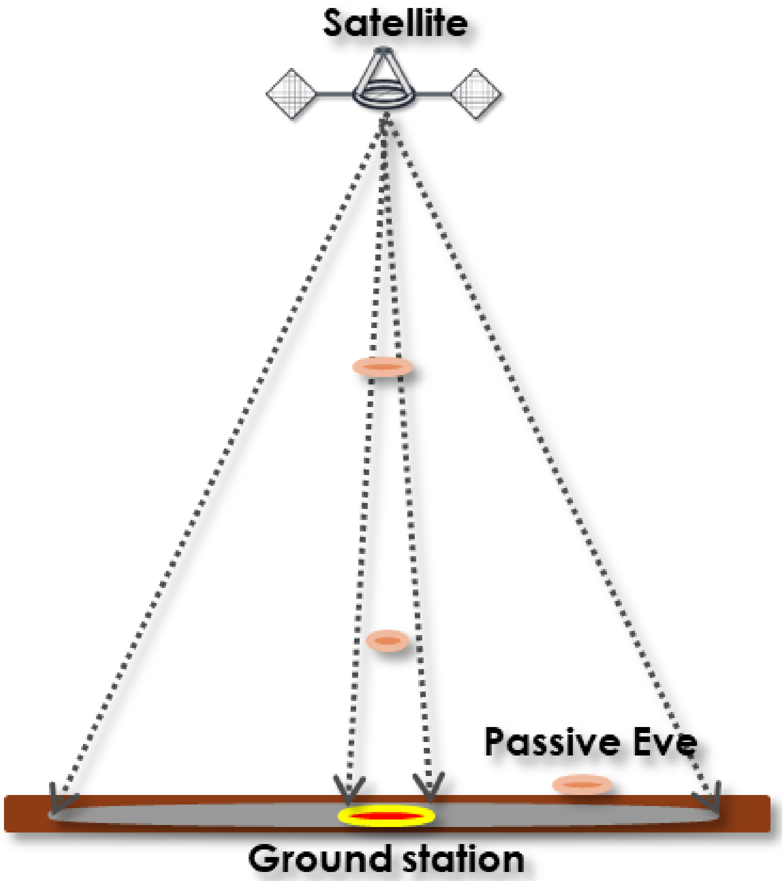
Satellite QKD w/ restricted Eve

- Unrestricted Eavesdropping



- Restricted Eavesdropping

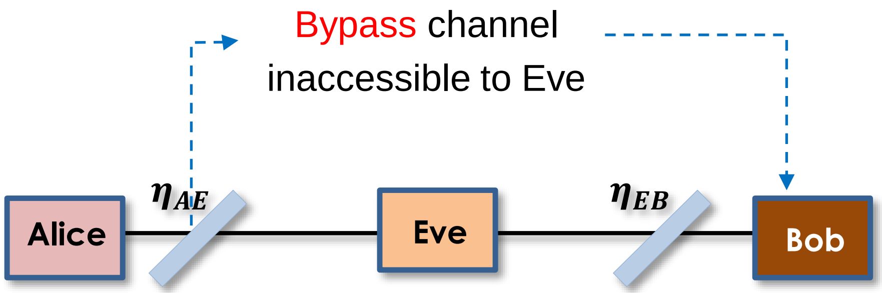




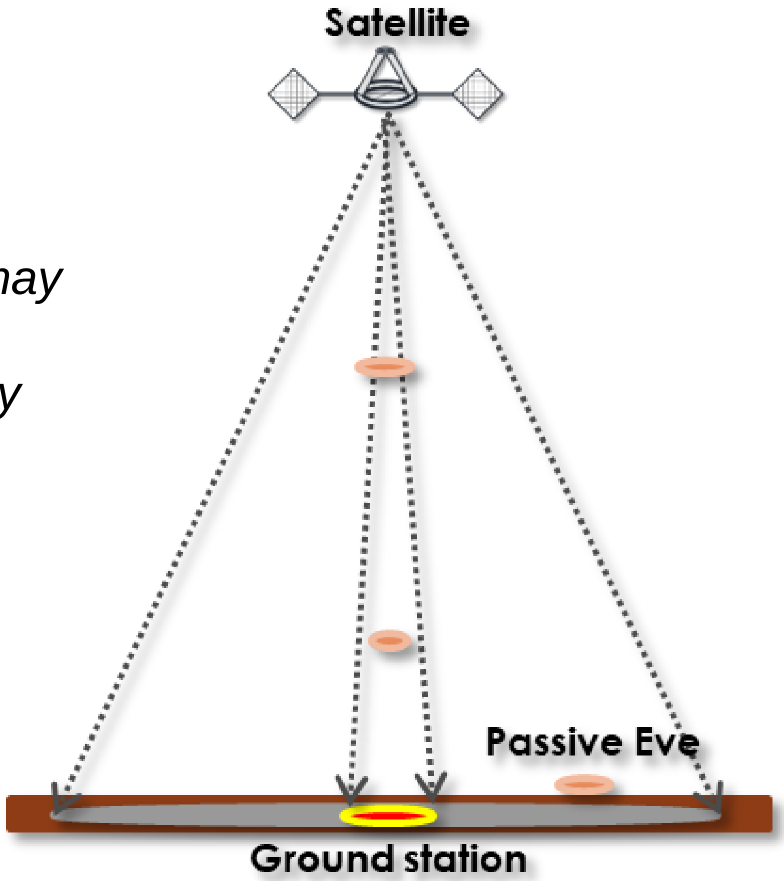
But, what happens to the signal that does not reach Eve? Can it still find its way to get to Bob?

Satellite QKD w/ restricted Eve: Bypass Channel

- **Restricted Eavesdropping: Scenario (a)**

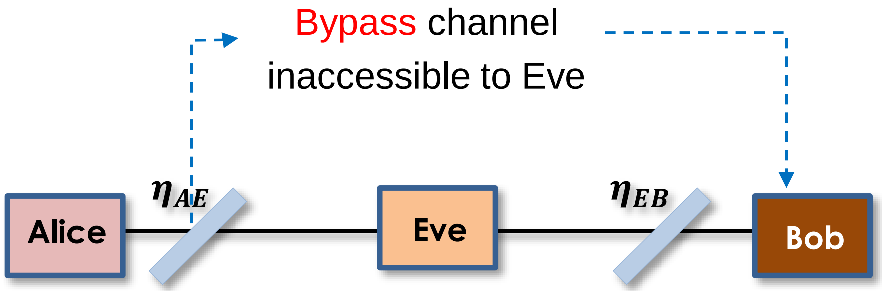


In general, some signals that reach Bob may bypass Eve; such a bypass channel is inaccessible to Eve, but A&B cannot fully characterise it either.



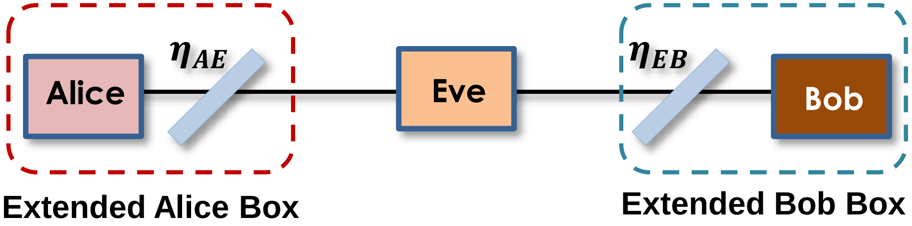
Satellite QKD w/ restricted Eve: Different scenarios

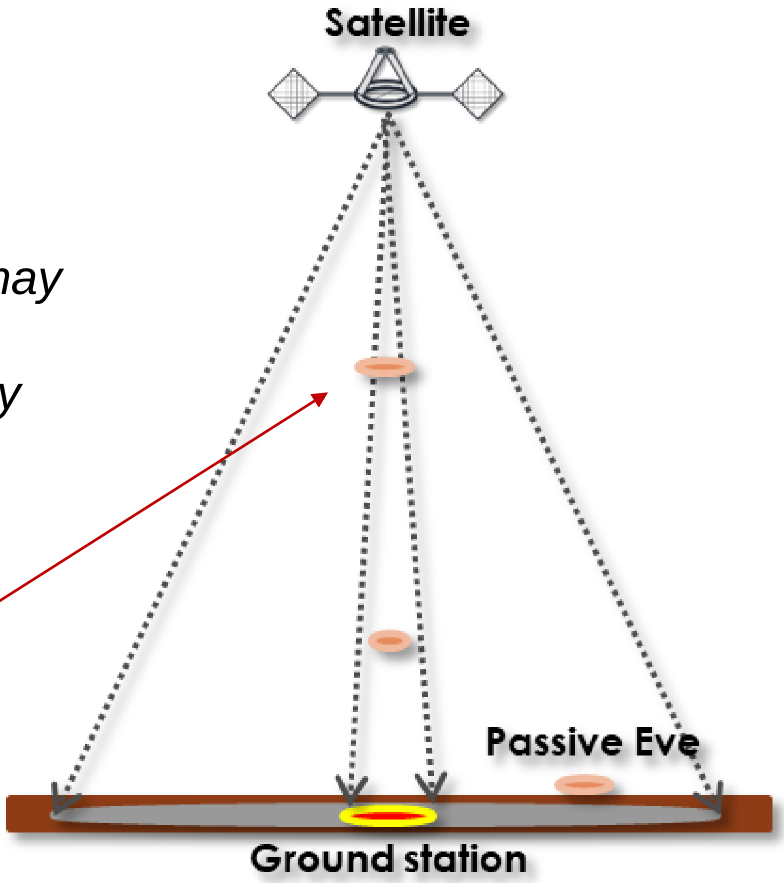
- **Restricted Eavesdropping: Scenario (a)**



In general, some signals that reach Bob may bypass Eve; such a bypass channel is inaccessible to Eve, but A&B cannot fully characterise it either.

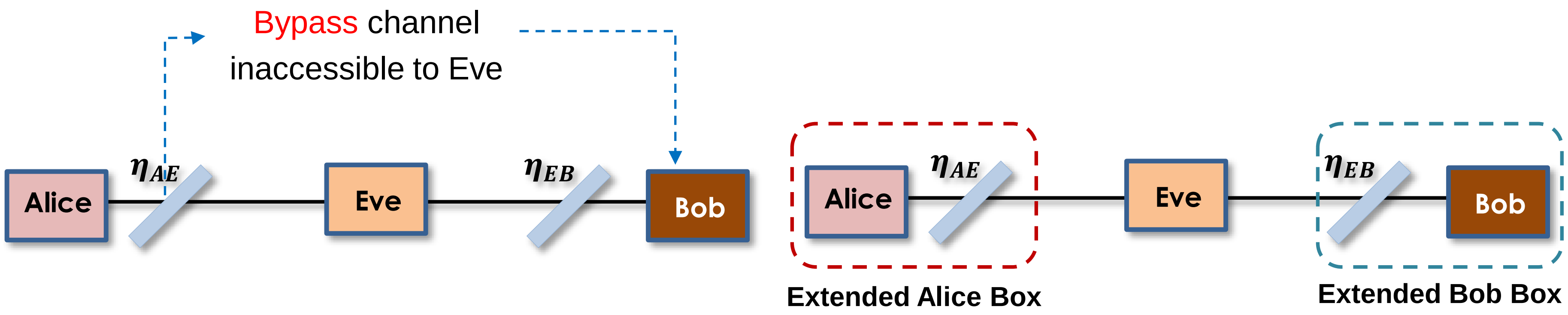
- **Restricted Eavesdropping: Scenario (b)**





Everything that reaches Bob would go through Eve; this is a special case of (a), with bypass channel output being a vacuum state.

QKD with an uncharacterised bypass channel



(a) Restricted Eavesdropping with bypass

(b) Restricted Eavesdropping without bypass

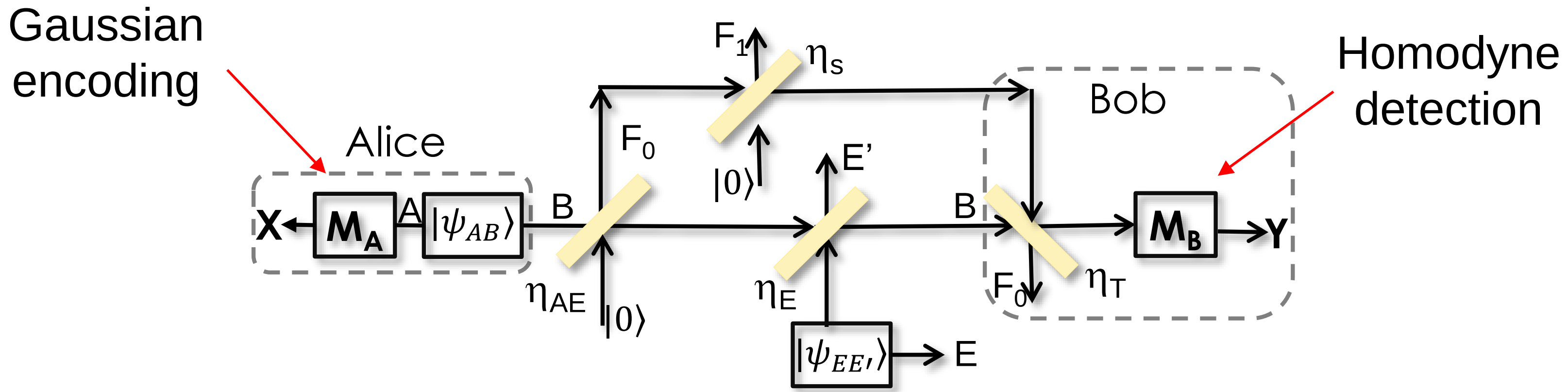
arXiv:2212.04807

Key Result: For the same observable data points,

Theorem 1: Secret key rate of (a) ≤ Secret key rate of (b)

Key argument: the space over which Alice and Bob have to minimise the key rate in (b) is a subset of that of (a)

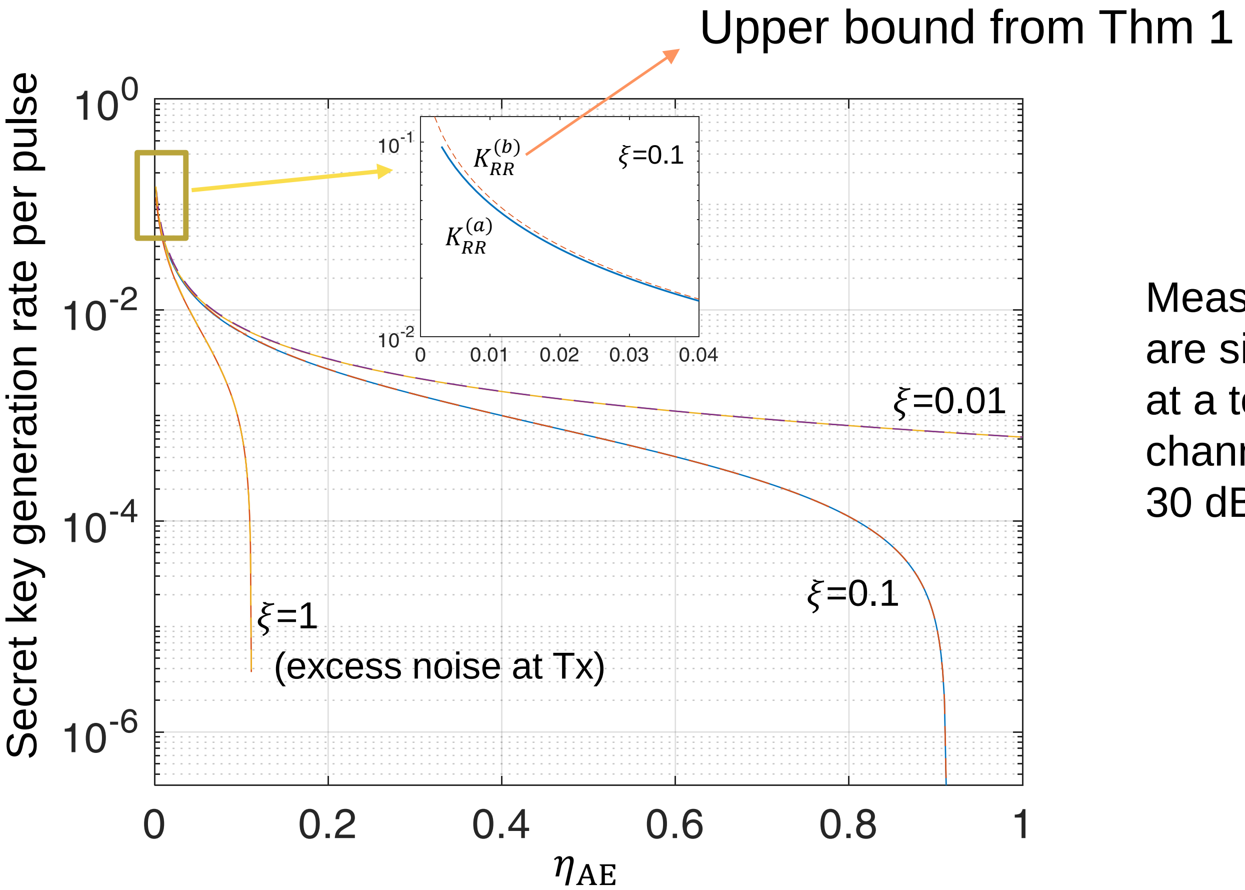
Implications of Thm 1 on CV QKD


Gaussian encoding

Homodyne detection

- We work out the key rate for a Gaussian encoded CV QKD system with homodyne detection for a special lossy bypass channel under an entangling cloner attack
- Telescope action is modelled by a beam splitter
- We minimise the key rate over a feasible set of parameters (i.e. when valid values can be assigned to all parameters on the graph)

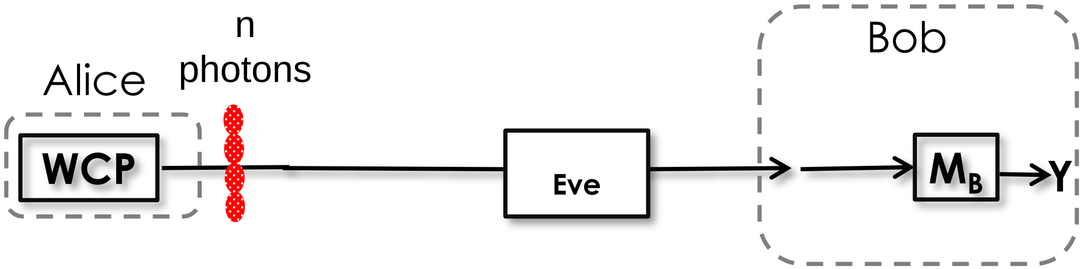
Implications of Thm 1 on CV QKD



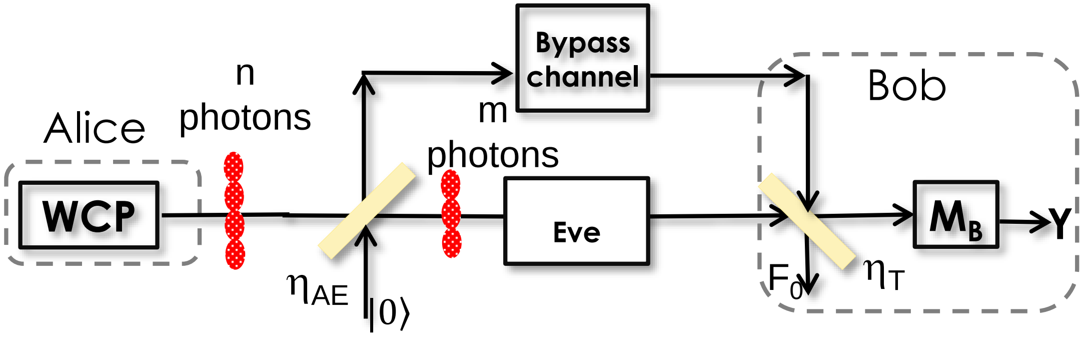
Measured data are simulated at a total channel loss of 30 dB; $\eta_{\mathrm{EB}} = 1$

- For reverse reconciliation: the lower bound on the key rate is numerically very close to the upper bound from Thm 1, and is achieved when bypass channel is loss and noise free.
- For direct reconciliation: advantage only at very low η_{AE}

Implications of Thm 1 on BB84 with WCP

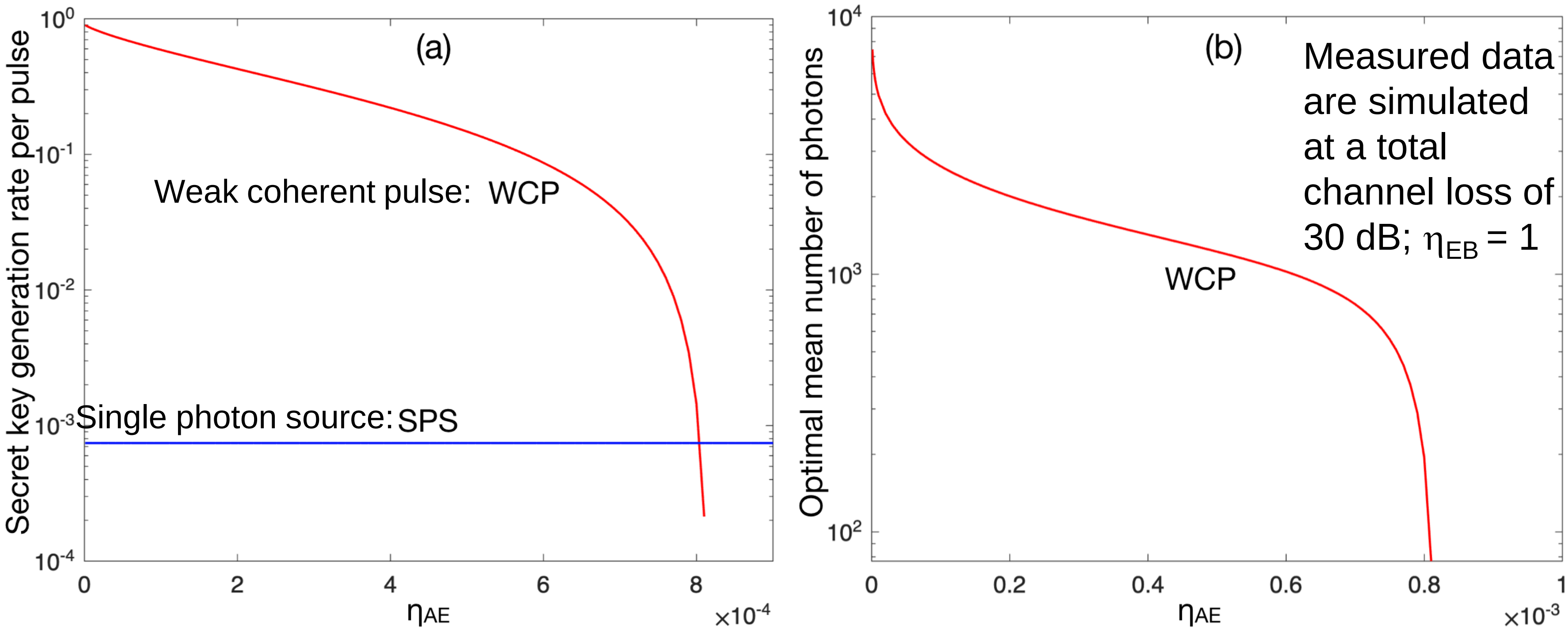


- Simplest BB84 protocol is the one that uses weak coherent pulses (WPC) at a fixed intensity (no decoy, or single-photon sources)
- For phase-randomised sources, this implies a photon-number channel. Secure key bits are those obtained when Alice sends exactly one photon.



- When there is a bypass channel, it is also possible that we get a detection at Bob while no photon has gone through Eve.

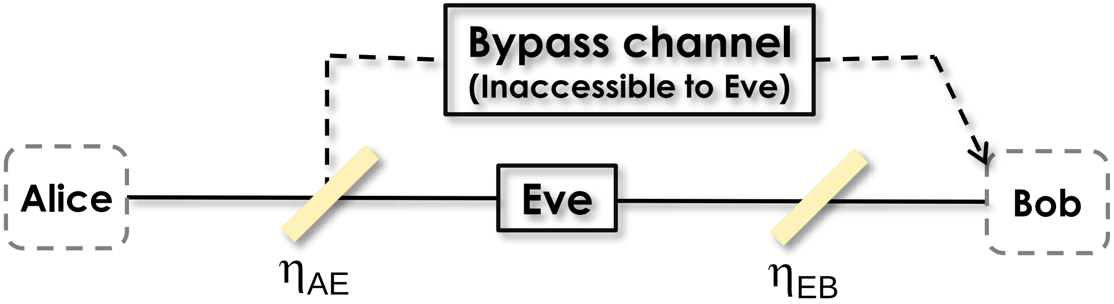
Implications of Thm 1 on BB84 with WCP



Measured data are simulated at a total channel loss of 30 dB; $\eta_{EB} = 1$

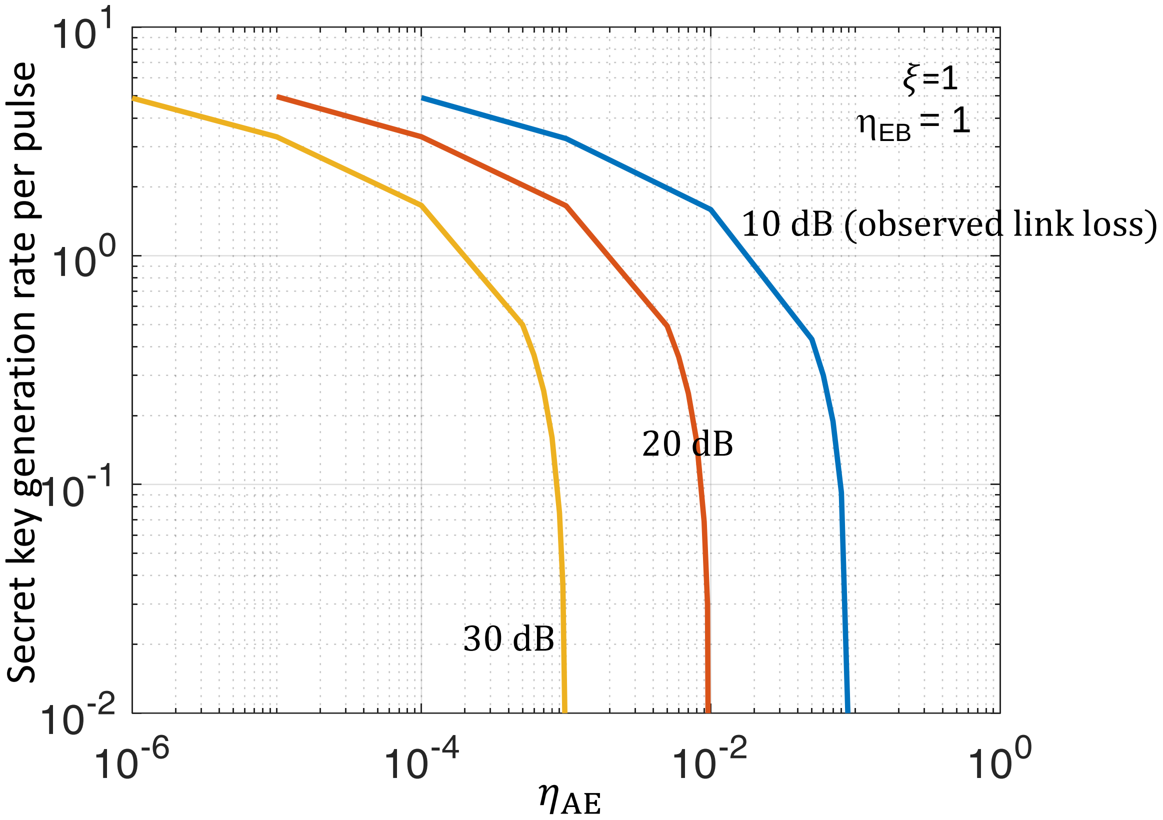
- Phase randomised WCP offers advantage over SPS only at very low η_{AE}
- We can capitalise on cases where no photon has gone through Eve
- Some ideas to obtain tighter bounds: in progress

Summary: Realistic Threat Models for Satellite QKD



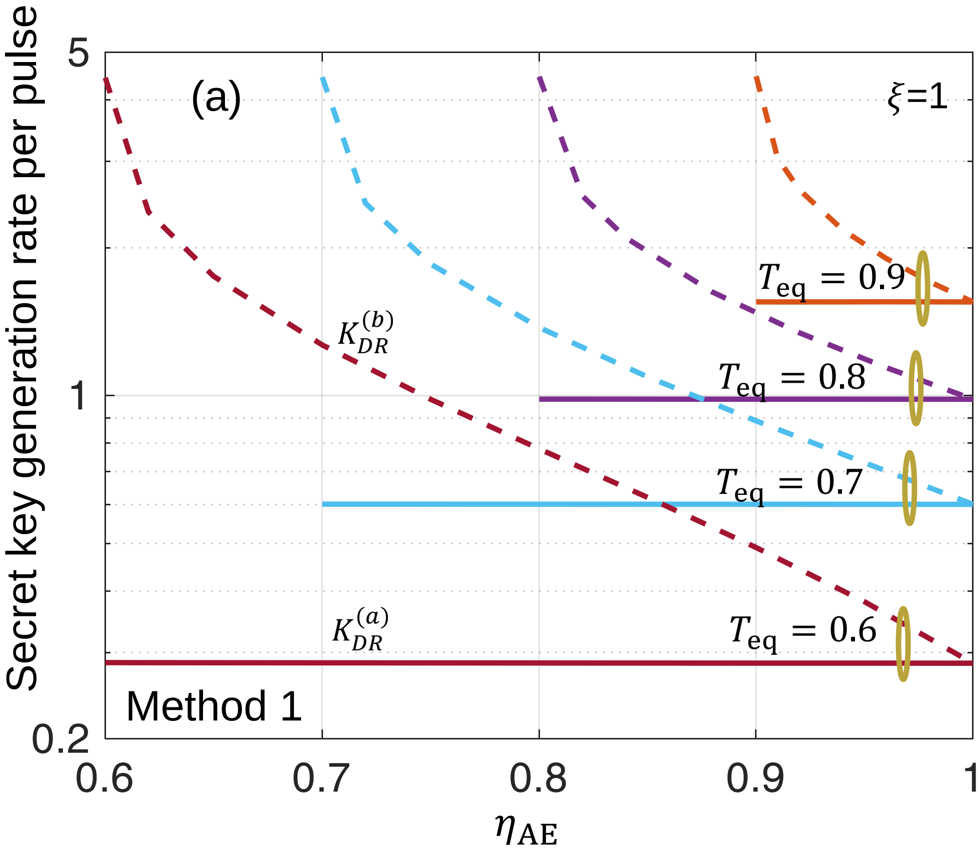
- We considered prepare-and-measure QKD under some nominal restrictions on Eve in terms of accessing Alice’s signal or reaching Bob’s telescope; this could be relevant to satellite-based QKD
- This resulted in a new QKD setting with an uncharacterised *bypass* channel inaccessible to Eve
- We found a generic upper bound for P&M QKD with a bypass channel, which is easy to calculate
- Under certain realistic assumptions on the bypass channel, we found that the numerically obtained lower bound for CV QKD is very close to the above upper bound if we use reverse reconciliation
- For DV-QKD, WCP sources can offer advantage if $\eta_{AE} << 1$.

Implications of Thm 1 on CV QKD



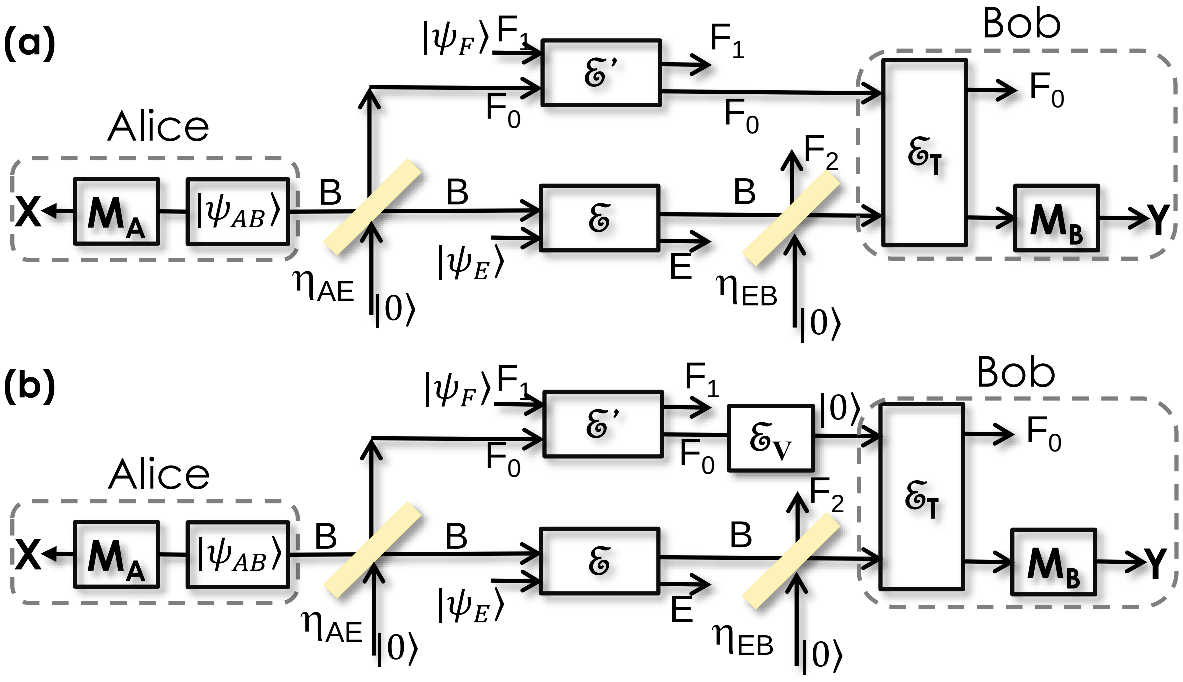
- For direct reconciliation: advantage only at very low η_{AE}

Implications of Thm 1 on CV QKD



- For direct reconciliation: advantage only at very low η_{AE}

QKD with an uncharacterised bypass channel



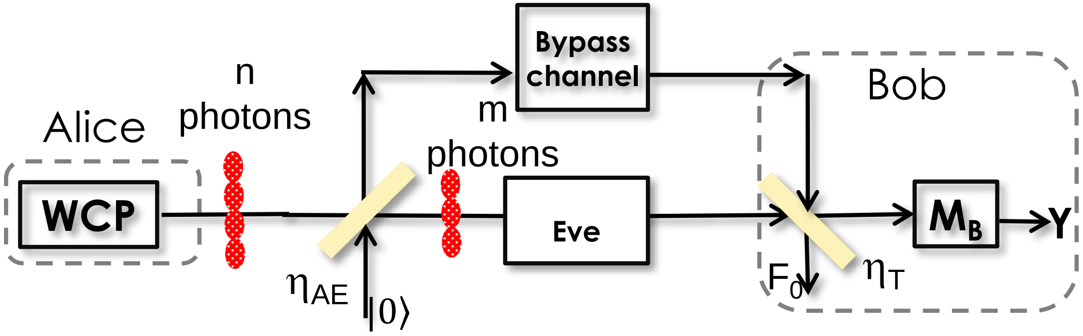
arXiv:2212.04807

Key Result: For the same observable data points,

Theorem 1: Secret key rate of (a) ≤ Secret key rate of (b)

Key argument: the space over which Alice and Bob have to minimise the key rate in (b) is a subset of that of (a)

Implications of Thm 1 on BB84 with WCP



- Simplest BB84 protocol is the one that uses weak coherent pulses (WPC) at a fixed intensity (no decoy, or single-photon sources)
- For phase-randomised sources, this implies a photon-number channel. Upon Bob’s detection, the amount of information leaked to Eve can be bounded by:

$$I_{\mathrm{E}} = \begin{cases} 0 & m = 0, n \geq 0 \\ 1 & m > 1, n \geq m \\ h(\varepsilon_{11}) & m = 1, n = 1 \\ 1 & m = 1, n > 1 \end{cases}$$