Satellite-based quantum key distribution in the presence of bypass channels

QCrypt 2023

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

August 2023

[1]*University of Leeds, UK*, [2]*University of York, UK*, [3]*University of Bristol, UK*, [4]*University of Düsseldorf, Germany*, [5]*National University of Singapore*, [6]*ID Quantique, Switzerland*

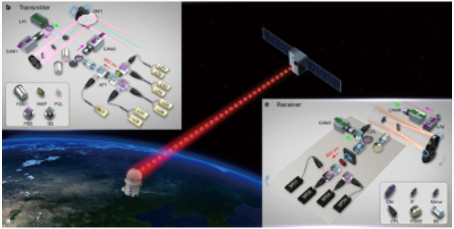
arXiv:2212.04807

Background and motivation

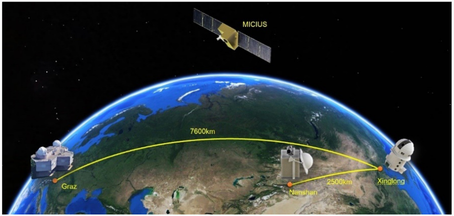
Satellite based QKD

As a solution to achieve very long distance QKD, and overcome fundamental bounds without repeaters, significant effort has been devoted to satellite QKD:

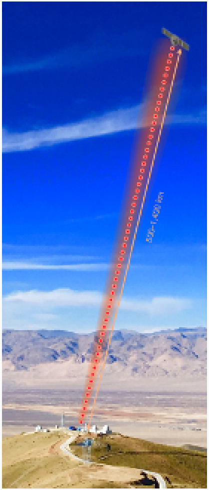
[Nature **549**, 43 (2017)]



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



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



Getting the most out of Sat-QKD

But significant challenges remain:

Getting the most out of Sat-QKD

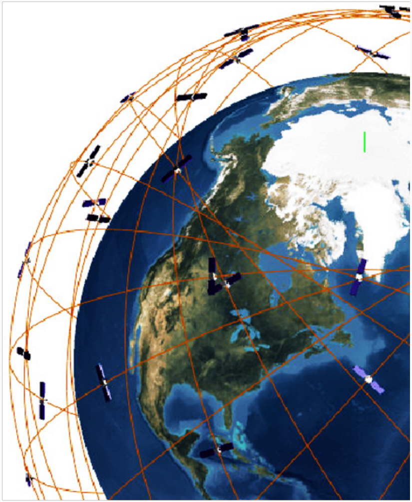
But significant challenges remain:

- Very expensive
- Limited availability (For LEO satellites roughly 5mins to exchange keys)
- Only night operation
- Highly weather dependent
- Requirement of large ground station telescopes (order of 1m diameter)

Getting the most out of Sat-QKD

But significant challenges remain:

- Very expensive
- Limited availability (For LEO satellites roughly 5mins to exchange keys)
- Only night operation
- Highly weather dependent
- Requirement of large ground station telescopes (order of 1m diameter)



What can we do?

With such challenges, how can we hope to do any better in space? Lets consider relevant eavesdropping models...

Goal of QKD

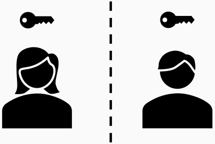
We are looking for **shared, private randomness**:

Goal of QKD

We are looking for **shared, private randomness**:

Shared

Alice and Bob hold the same key

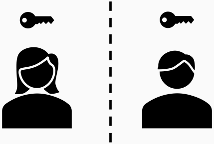


Goal of QKD

We are looking for **shared, private randomness**:

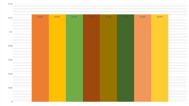
Shared

Alice and Bob hold the same key



Private randomness

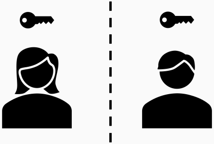
The key is unpredictable to any third party/eavesdropper



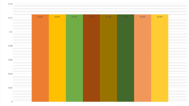
Goal of QKD

We are looking for **shared, private randomness**:

Shared
Alice and Bob hold the same key



Private randomness
The key is unpredictable to any third party/eavesdropper



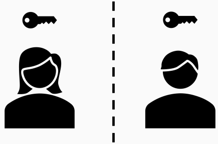
Goal:
Given some basic and necessary assumptions on Eve, and experimental observations, prove the above properties

Goal of QKD

We are looking for **shared, private randomness**:

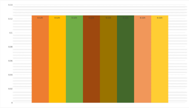
Shared

Alice and Bob hold the same key



Private randomness

The key is unpredictable to any third party/eavesdropper



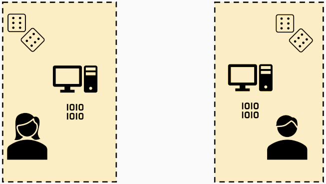
Goal:

Given some basic and necessary assumptions on Eve, and experimental observations, prove the above properties

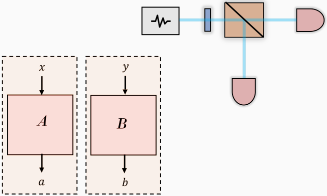
Let us examine the different eavesdropping assumptions and restrictions commonly encountered in QKD...

Common eavesdropping assumptions in QKD

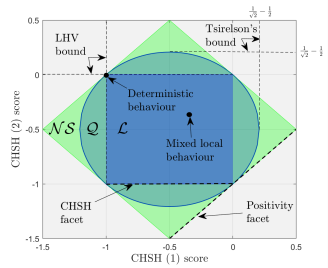
Secure lab and user assumptions



Eve's control over the devices

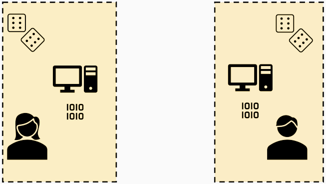


Fundamental physics governing an all powerful Eve

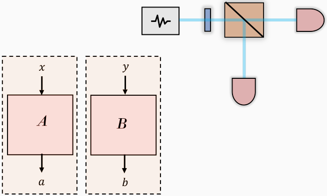


Common eavesdropping assumptions in QKD

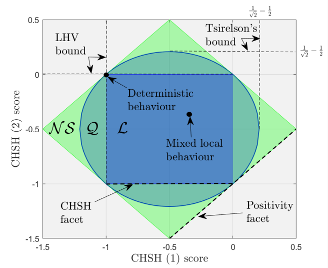
Secure lab and user assumptions



Eve's control over the devices



Fundamental physics governing an all powerful Eve

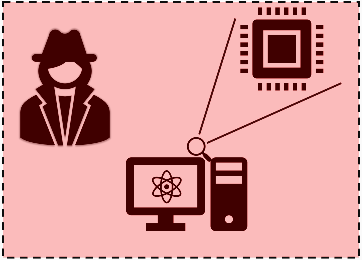


Underlying assumption:
Eve still has access to the **entire channel**, and **unlimited computational resources**. Is this always realistic?

Additional eavesdropping restrictions in QKD

Current literature has explored making QKD more practical by imposing well justified *restrictions* on Eve:

Computational assumptions on Eve

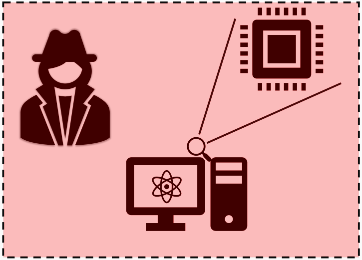


(and others...)

Additional eavesdropping restrictions in QKD

Current literature has explored making QKD more practical by imposing well justified *restrictions* on Eve:

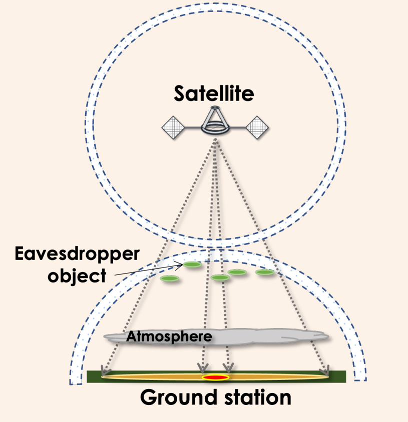
Computational assumptions on Eve



(and others...)

This work:

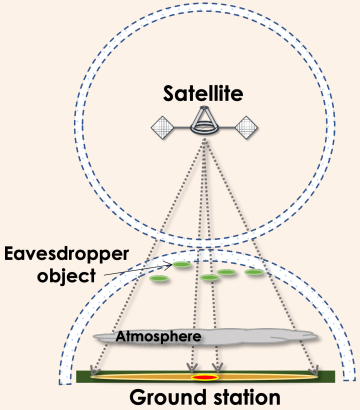
Restrictions on Eve in satellite QKD



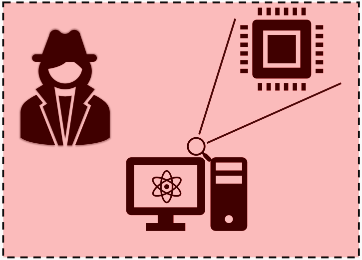
Additional eavesdropping restrictions in QKD

Current literature has explored making QKD more practical by imposing well justified *restrictions* on Eve:

This work:
Restrictions on Eve in satellite QKD



Computational assumptions on Eve



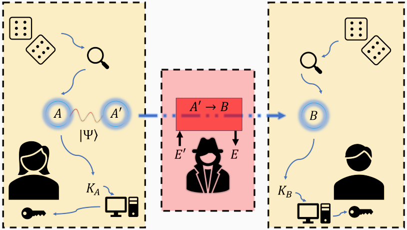
(and others...)

Depart from an all powerful Eve

Satellite QKD with restricted eavesdropping: this work

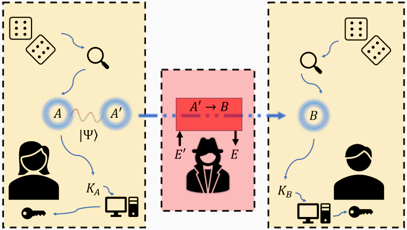
Restricted versus unrestricted eavesdropping

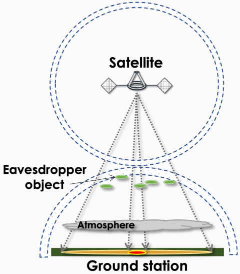
Unrestricted eavesdropping:
Eve has complete access to the channel



Restricted versus unrestricted eavesdropping

Unrestricted eavesdropping:
Eve has complete access to the channel

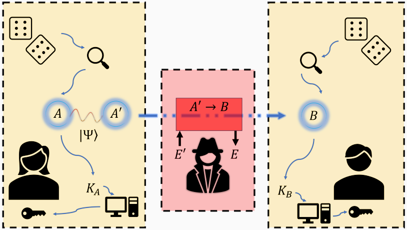


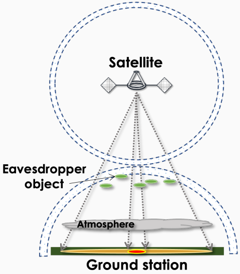


Restricted versus unrestricted eavesdropping

Unrestricted eavesdropping:

Eve has complete access to the channel



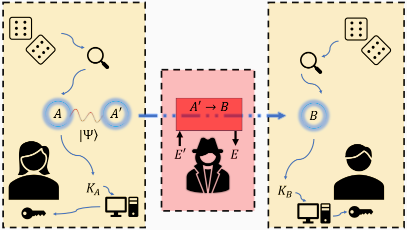


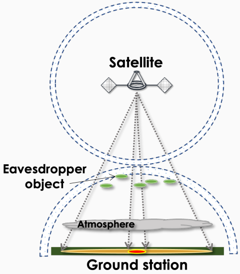
Implications for satellite QKD:

- Eve can collect Alice's signal in full, and send anything to Bob
- No channel assumptions are made

Restricted versus unrestricted eavesdropping

Unrestricted eavesdropping:
Eve has complete access to the channel



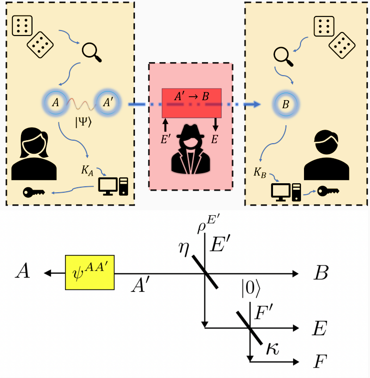


Implications for satellite QKD:

- Eve can collect Alice's signal in full, and send anything to Bob
- No channel assumptions are made

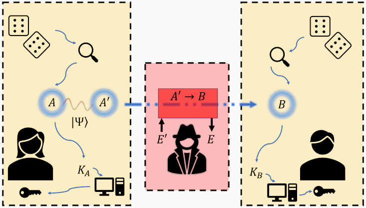
Can we relax this for line of sight satellite links? Could we monitor the link, alerting us to eavesdropping objects?

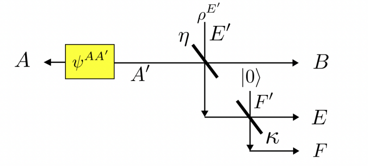
Existing Satellite QKD Eavesdropping model: wiretap channel

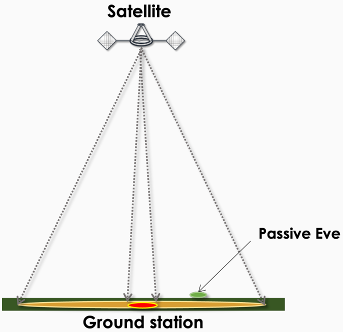


[Phys. Rev. Applied **14** 024044 2020], [Entropy **21** 397 2019], [Phys. Rev. Applied **16** 2021]

Existing Satellite QKD Eavesdropping model: wiretap channel



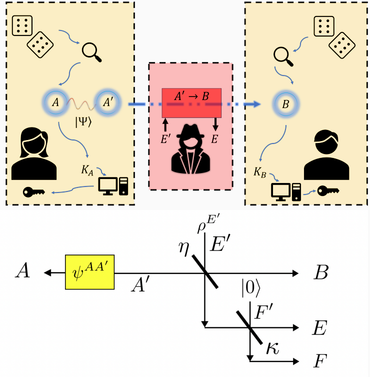


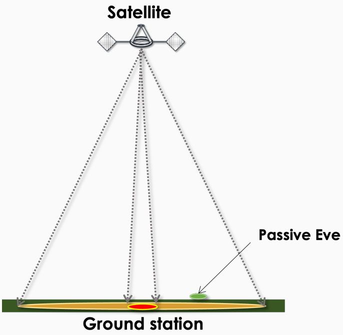


[Phys. Rev. Applied **14** 024044 2020], [Entropy **21** 397 2019], [Phys. Rev. Applied **16** 2021]

Difficult for Eve to be in space$\rightarrow$ one might assume a *wiretap channel*

Existing Satellite QKD Eavesdropping model: wiretap channel



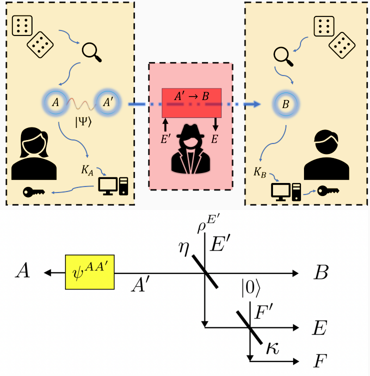


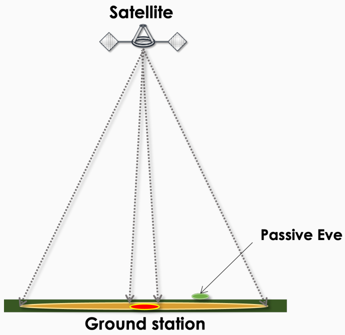
[Phys. Rev. Applied **14** 024044 2020], [Entropy **21** 397 2019], [Phys. Rev. Applied **16** 2021]

Difficult for Eve to be in space$\rightarrow$ one might assume a *wiretap channel*

However it is difficult to verify this through experimental observations

Existing Satellite QKD Eavesdropping model: wiretap channel





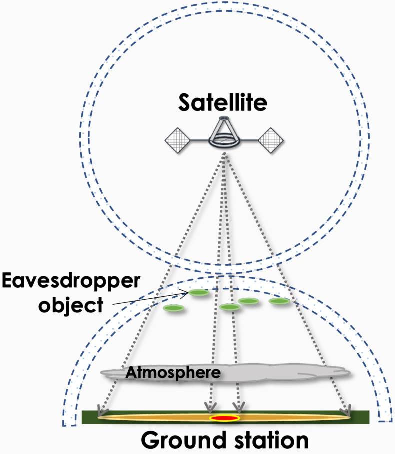
[Phys. Rev. Applied **14** 024044 2020], [Entropy **21** 397 2019], [Phys. Rev. Applied **16** 2021]

Difficult for Eve to be in space$\rightarrow$ one might assume a *wiretap channel*

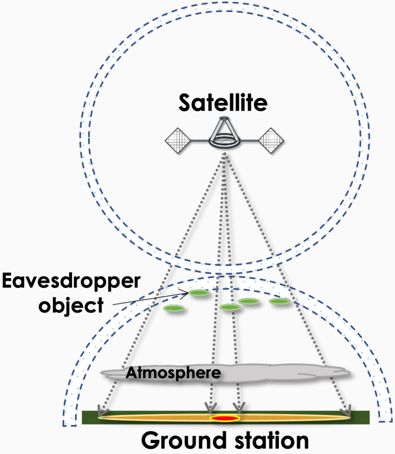
However it is difficult to verify this through experimental observations

Key goal:
To provide a **generic framework** for restricted Eavesdropping with **verifiable assumptions**

Restricted versus unrestricted eavesdropping



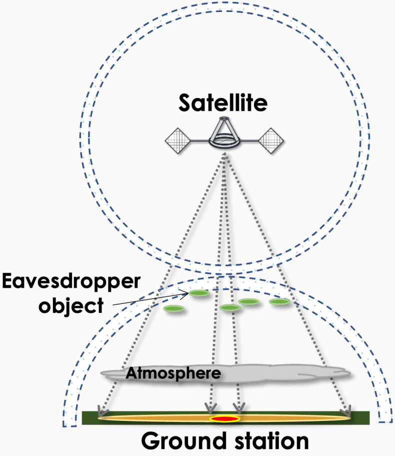
Restricted versus unrestricted eavesdropping



Monitoring possibilities:

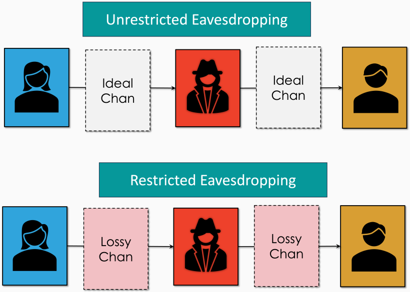
With detection systems, such as LIDAR, Alice and Bob can possibly rule out the presence of eavesdropping objects of a certain size

Restricted versus unrestricted eavesdropping



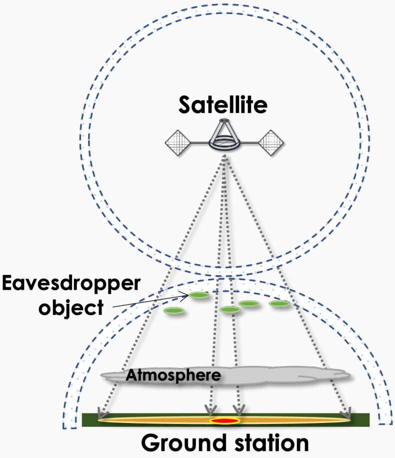
Monitoring possibilities:

With detection systems, such as LIDAR, Alice and Bob can possibly rule out the presence of eavesdropping objects of a certain size



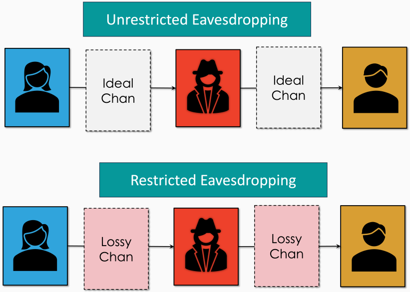
Implication:

Restricted versus unrestricted eavesdropping



Monitoring possibilities:

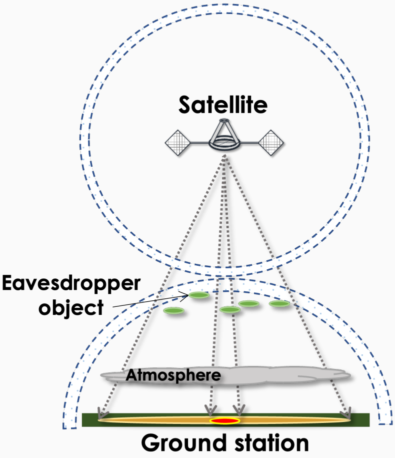
With detection systems, such as LIDAR, Alice and Bob can possibly rule out the presence of eavesdropping objects of a certain size



Implication:

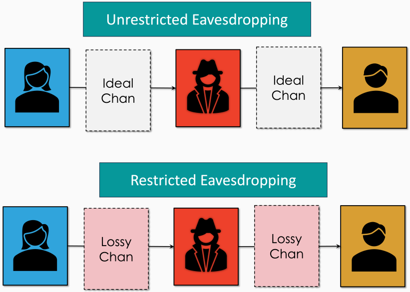
→Limit size of Eve's object

Restricted versus unrestricted eavesdropping



Monitoring possibilities:

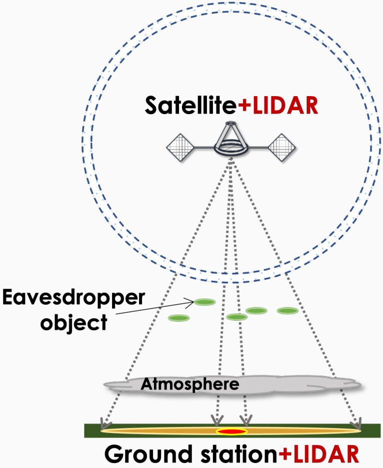
With detection systems, such as LIDAR, Alice and Bob can possibly rule out the presence of eavesdropping objects of a certain size

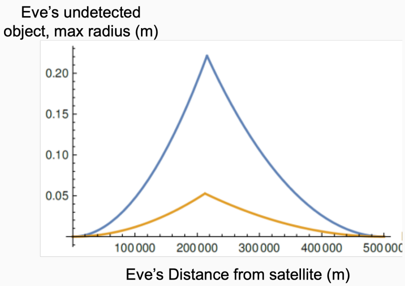


Implication:

$\rightarrow$Limit size of Eve's object$\rightarrow$ limit Eve's collection and resend efficiency, i.e. *ideal channels are replaced with lossy channels*

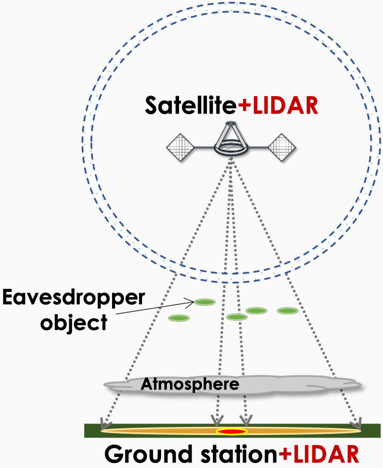
Monitoring example using LIDAR

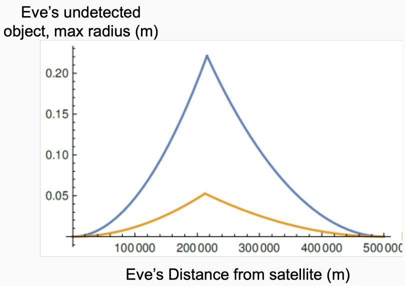




LIDAR with 1W, 4W, Tx power and telescope diameter 30cm, 100cm, for Alice (satellite) and Bob (ground station) resp. LEO satellite altitude 500km.

Monitoring example using LIDAR

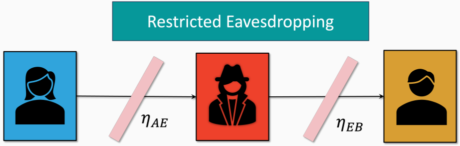


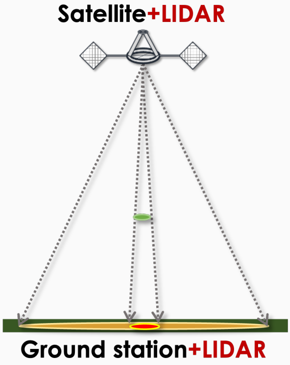


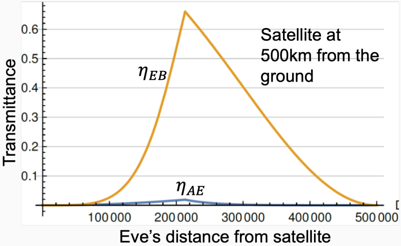
LIDAR with 1W, 4W, Tx power and telescope diameter 30cm, 100cm, for Alice (satellite) and Bob (ground station) resp. LEO satellite altitude 500km. Max object size ≈ 20cm → definitely limits her capabilities...

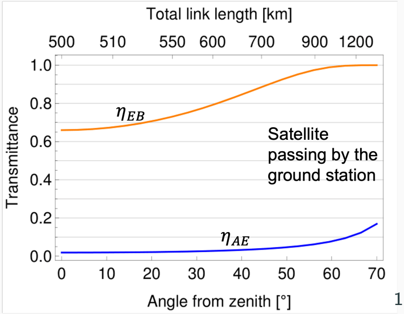
Eve’s collection and resend capabilities

Continuing the LIDAR example, preliminary calculations suggest:



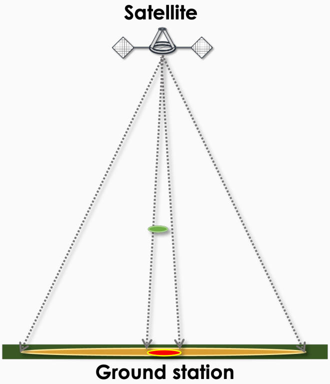






A new QKD scenario

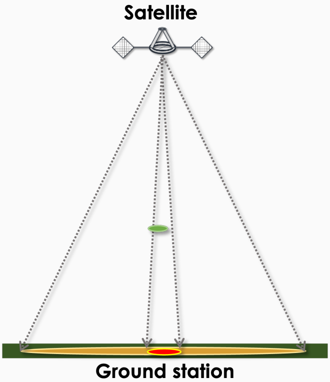
What about signal that does not reach Eve, but might still find its way to Bob?



A general model

A new QKD scenario

What about signal that does not reach Eve, but might still find its way to Bob?



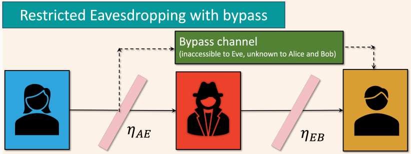
Regardless of the monitoring technique, bounds on η_{AE}, η_{EB} result in a new QKD model which is interesting in its own right...

Satellite QKD with bypass channels

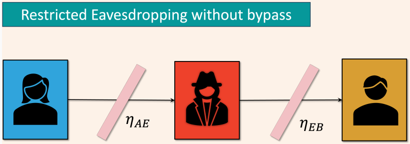
Different models

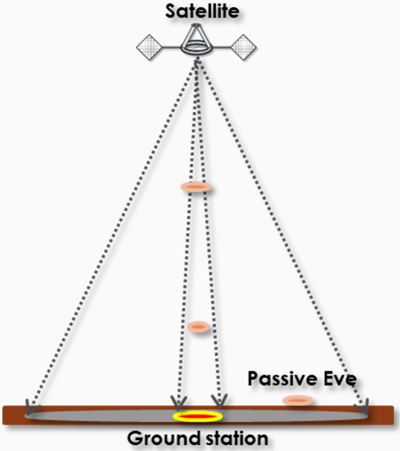
In principle, some signals that reach Bob may **bypass** Eve, but Alice and Bob are unable to fully characterise it either. Assume Alice and Bob have characterised η_{AE}, η_{EB} by some means; we are then left with two case:

Scenario (a):



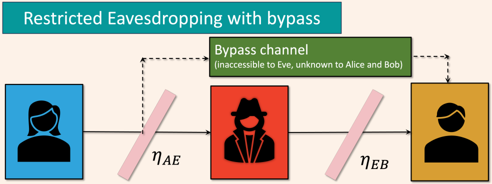
Scenario (b):



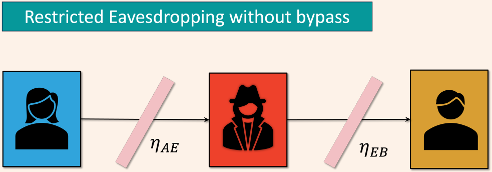


Different models: key rate comparison

Scenario (a):

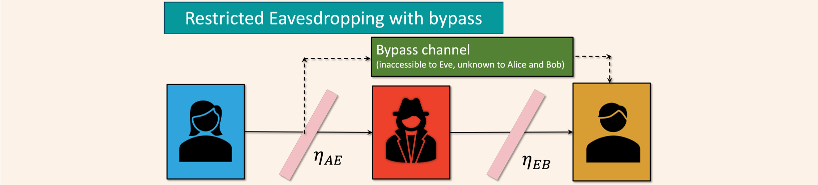


Scenario (b):

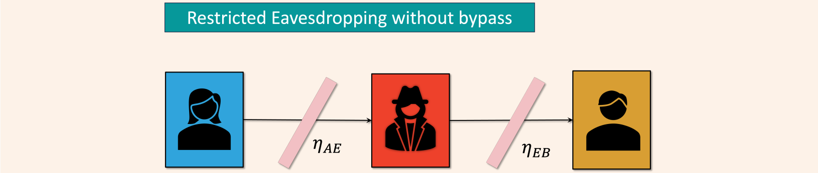


Different models: key rate comparison

Scenario (a):



Scenario (b):



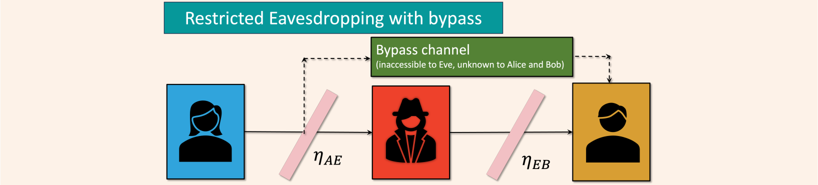
Theorem 1

For a fixed set of observables, secret key rate (b) $\geq$ secret key rate (a).

Why? Attacks in (b) can be viewed as a subset of those in (a).

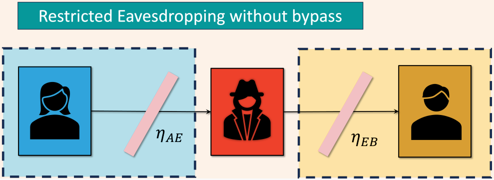
Different models: key rate comparison

Scenario (a):



Scenario (b):

Extended Alice and Bob box: easy to compute upper bound



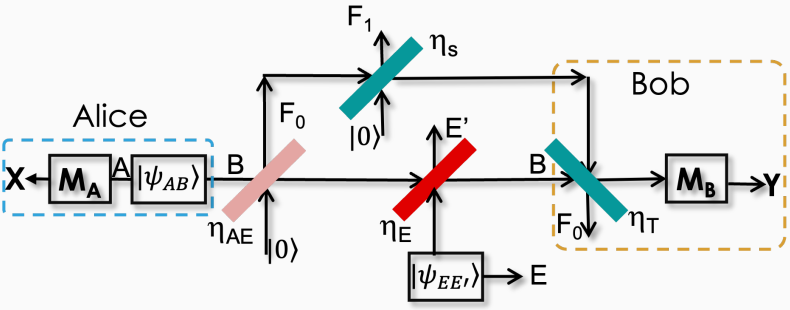
Theorem 1

For a fixed set of observables, secret key rate (b) $\geq$ secret key rate (a).

Why? Attacks in (b) can be viewed as a subset of those in (a).

Implications on key rates

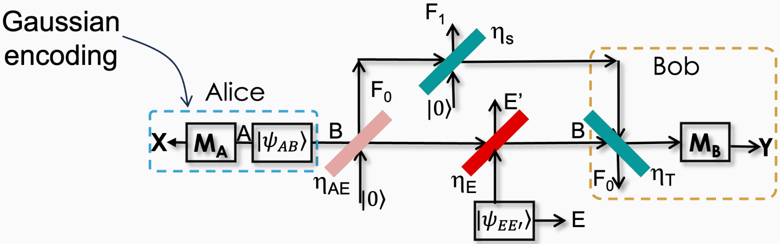
CV-QKD setup



We work out the key rate for a CV-QKD system with:

- Lossy bypass channel, $\eta_{EB} = 1$

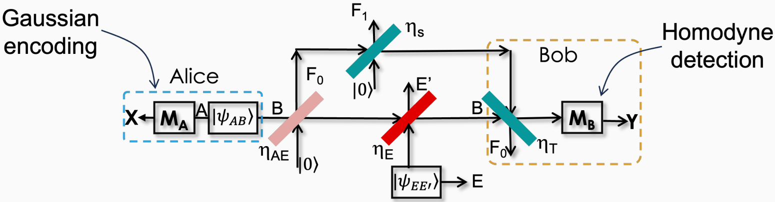
CV-QKD setup



We work out the key rate for a CV-QKD system with:

- Lossy bypass channel $\eta_{EB} = 1$
- Gaussian encoding

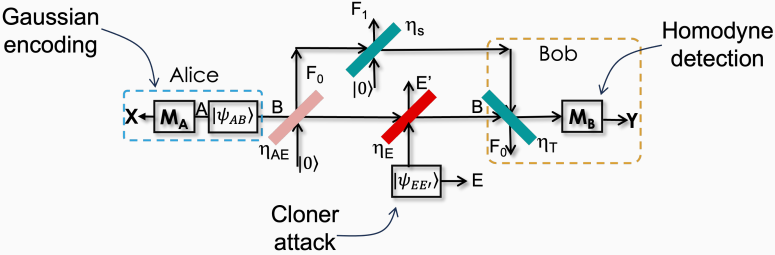
CV-QKD setup



We work out the key rate for a CV-QKD system with:

- Lossy bypass channel $\eta_{EB} = 1$
- Gaussian encoding
- Homodyne detection

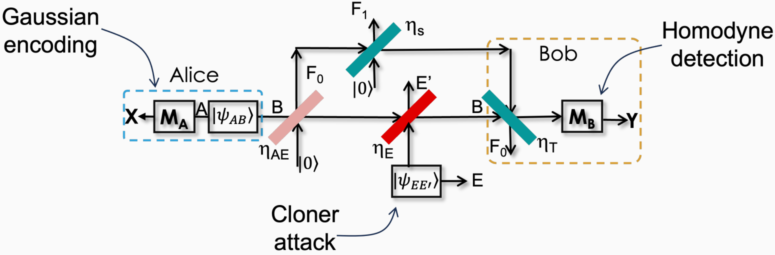
CV-QKD setup



We work out the key rate for a CV-QKD system with:

- Lossy bypass channel $\eta_{EB} = 1$
- Gaussian encoding
- Homodyne detection
- Entangling cloner attack

CV-QKD setup

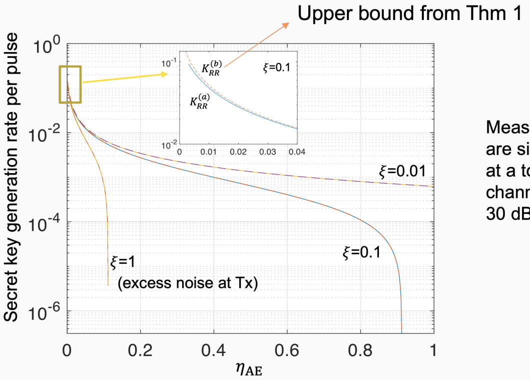


We work out the key rate for a CV-QKD system with:

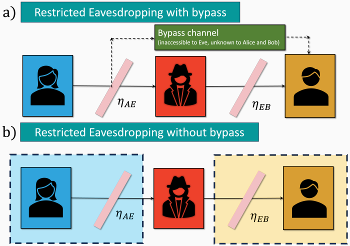
- Lossy bypass channel $\eta_{EB} = 1$
- Gaussian encoding
- Homodyne detection
- Entangling cloner attack

Recall: bypass is uncharacterised $\rightarrow$ minimise key rate over feasible set

Generic upper bound:
scenario (b)

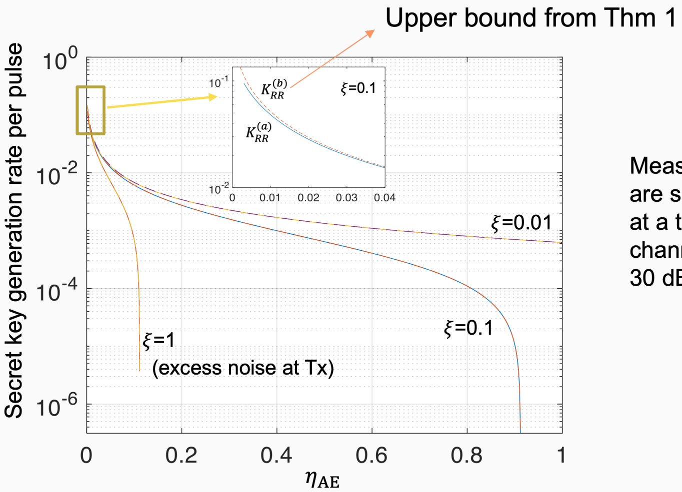


Measured data are simulated at a total channel loss of 30 dB; $\eta_{EB} = 1$



Lower bound from the bypass model:
scenario (a)

CV-QKD results

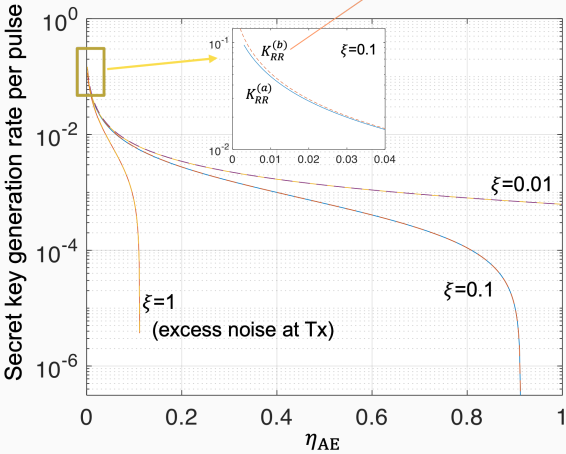


Measured data are simulated at a total channel loss of 30 dB; $\eta_{EB} = 1$

- **Reverse reconciliation:** Lower bound is very close to upper bound; optimum is achieved when bypass is lossless and noiseless

CV-QKD results

Upper bound from Thm 1



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

- **Reverse reconciliation:** Lower bound is very close to upper bound; optimum is achieved when bypass is lossless and noiseless
- **Direct reconciliation:** advantage only at very lower η_{AE}

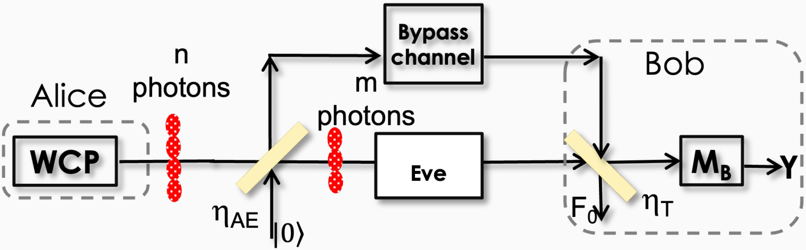
DV-QKD setup

We also consider BB84 with single photons and phase-randomnised weak coherent pulses

DV-QKD setup

We also consider BB84 with single photons and phase-randomnised weak coherent pulses

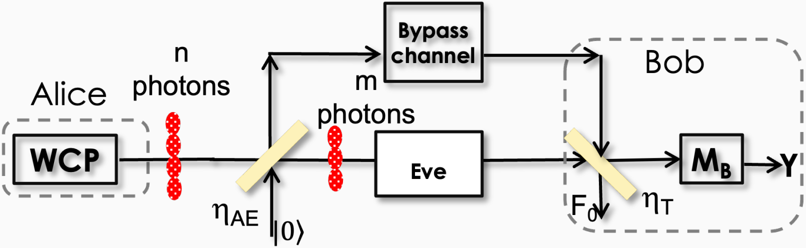
→ *photon number channel*



DV-QKD setup

We also consider BB84 with single photons and phase-randomnised weak coherent pulses

$\rightarrow$ *photon number channel*

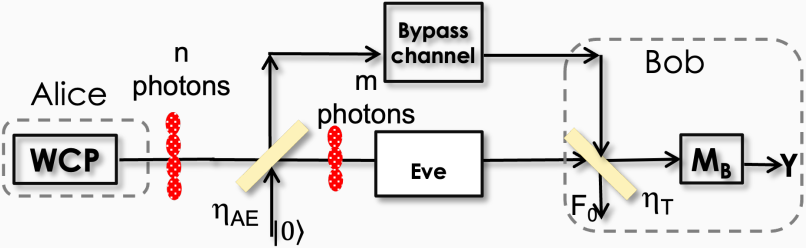


- Secret key bits are obtained when Alice sends exactly one photon

DV-QKD setup

We also consider BB84 with single photons and phase-randomnised weak coherent pulses

→ *photon number channel*

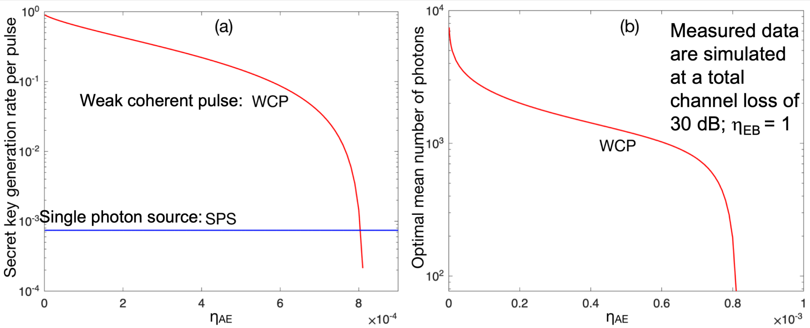


- Secret key bits are obtained when Alice sends exactly one photon
- With a bypass channel we can get detection at Bob with no photon going through Eve

DV-QKD results

Phase randomised WCP offers advantage at lower η_{AE}

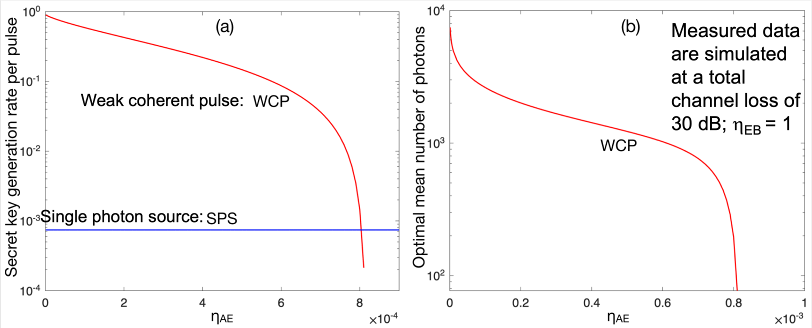
We can capitalise on cases where no photon has gone through Eve



DV-QKD results

Phase randomised WCP offers advantage at lower η_{AE}

We can capitalise on cases where no photon has gone through Eve

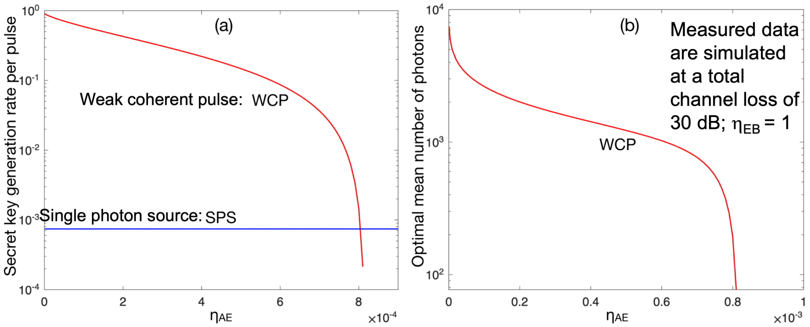


- Single photon BB84 *is not* optimal in the bypass model $\rightarrow$ eavesdropping restrictions influence best choice of protocol

DV-QKD results

Phase randomised WCP offers advantage at lower η_{AE}

We can capitalise on cases where no photon has gone through Eve



- Single photon BB84 *is not* optimal in the bypass model $\rightarrow$ eavesdropping restrictions influence best choice of protocol
- Behaviour we would expect to see in wiretap channel

DV-QKD numerical approach

Ongoing investigation$\rightarrow$ application of numerical security proofs (Winick *et al.*, [Quantum **2**, 77 (2018)]) to this problem.

DV-QKD numerical approach

Ongoing investigation $\rightarrow$ application of numerical security proofs (Winick *et al.*, [Quantum **2**, 77 (2018)]) to this problem.

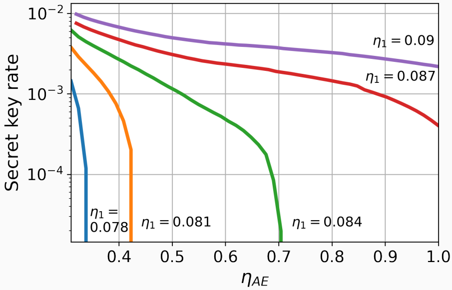
We can modify this technique to the bypass setting
Potential to improve **versatility**, **practicality** and **tighten bounds**

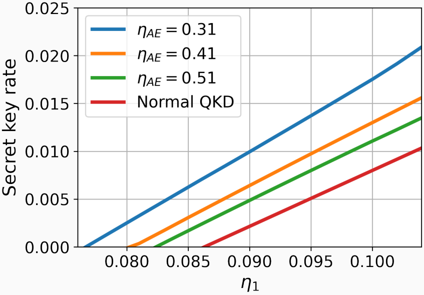
DV-QKD numerical approach

Ongoing investigation→ application of numerical security proofs (Winick *et al.*, [Quantum **2**, 77 (2018)]) to this problem.

We can modify this technique to the bypass setting
Potential to improve **versatility**, **practicality** and **tighten bounds**

As an example for SPS: bypass channels can improve robustness to a detector efficiency mismatch at the receiver





η_1 = Bob's detector efficiency mismatch, $\eta_T \approx \eta_{AE}$, $\eta_S = 1$.

Summary

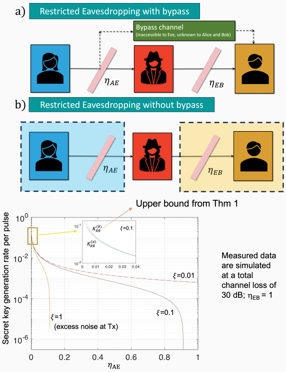
Take home message

We introduce and study a new setting: QKD with bypass channels, which implies improvements for satellite QKD implementations

Summary

Take home message

We introduce and study a new setting: QKD with bypass channels, which implies improvements for satellite QKD implementations

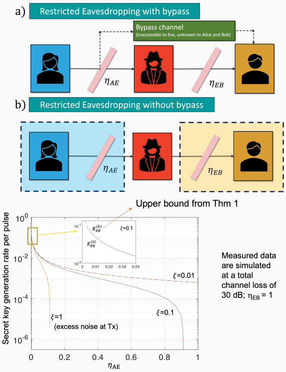


Measured data are simulated at a total channel loss of 30 dB; $\eta_{EB} = 1$

Summary

Take home message

We introduce and study a new setting: QKD with bypass channels, which implies improvements for satellite QKD implementations

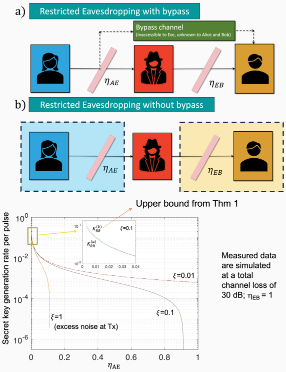


- We found a generic (easy to calculate) upper bound

Summary

Take home message

We introduce and study a new setting: QKD with bypass channels, which implies improvements for satellite QKD implementations

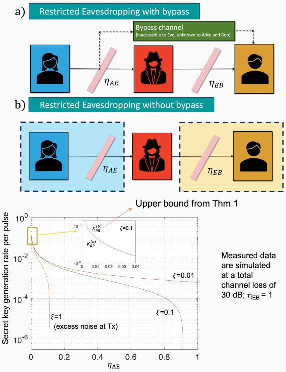


- We found a generic (easy to calculate) upper bound
- A lower bound for CV-QKD with RR is very close to this upper bound

Summary

Take home message

We introduce and study a new setting: QKD with bypass channels, which implies improvements for satellite QKD implementations

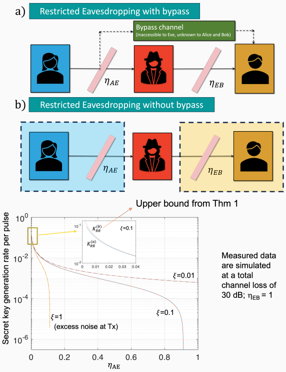


- We found a generic (easy to calculate) upper bound
- A lower bound for CV-QKD with RR is very close to this upper bound
- Bypass models can achieve non-zero rates when it would vanishes under normal QKD

Summary

Take home message

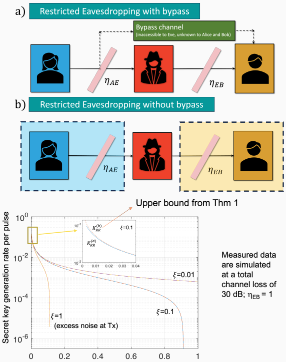
We introduce and study a new setting: QKD with bypass channels, which implies improvements for satellite QKD implementations



- We found a generic (easy to calculate) upper bound
- A lower bound for CV-QKD with RR is very close to this upper bound
- Bypass models can achieve non-zero rates when it would vanishes under normal QKD
- Similar results for DV QKD

Take home message

We introduce and study a new setting: QKD with bypass channels, which implies improvements for satellite QKD implementations



- We found a generic (easy to calculate) upper bound
- A lower bound for CV-QKD with RR is very close to this upper bound
- Bypass models can achieve non-zero rates when it would vanishes under normal QKD
- Similar results for DV QKD

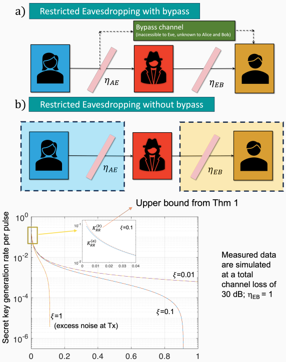
Future work:

Numerical approach for better rates, finite statistics, DV-QKD with RR, non-P&M QKD, wider work on unconventional security

Summary

Take home message

We introduce and study a new setting: QKD with bypass channels, which implies improvements for satellite QKD implementations



- We found a generic (easy to calculate) upper bound
- A lower bound for CV-QKD with RR is very close to this upper bound
- Bypass models can achieve non-zero rates when it would vanishes under normal QKD
- Similar results for DV QKD

Future work:

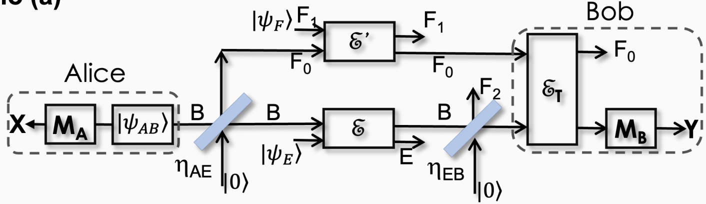
Numerical approach for better rates, finite statistics, DV-QKD with RR, non-P&M QKD, wider work on unconventional security

Thank you for your attention! arXiv:2212.04807

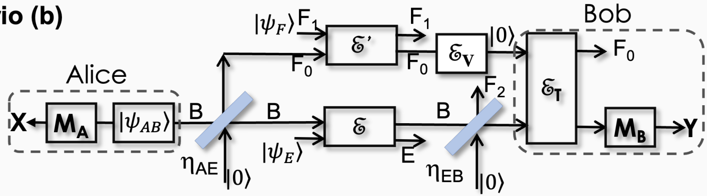
Bonus slides

Generic model for QKD with bypass

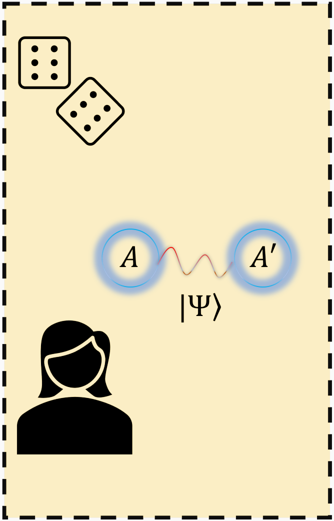
Scenario (a)



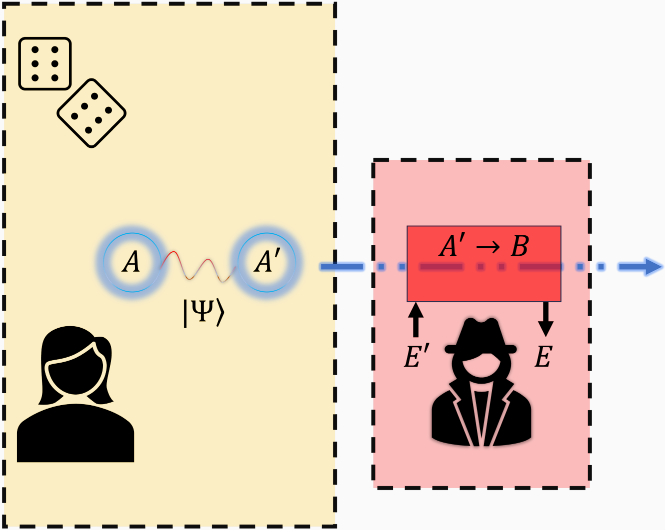
Scenario (b)



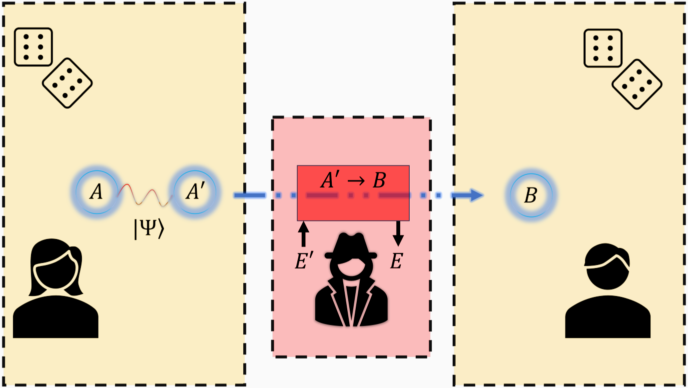
Standard QKD scenario



Standard QKD scenario



Standard QKD scenario



Standard QKD scenario