Enhancing the performance of quantum key distribution

based on New J. Phys. 21 113052 (2019); Phys. Rev. A 101, 012325 (2020) and arXiv:2006.16891 (2020)

Róbert Trényi
Supervisor: Prof. Marcos Curty

Escuela de Ingeniería de Telecomunicación, Department of Signal Theory and Communications, Universidade de Vigo

November 24, 2020

UNIVERSIDADE DE VIGO

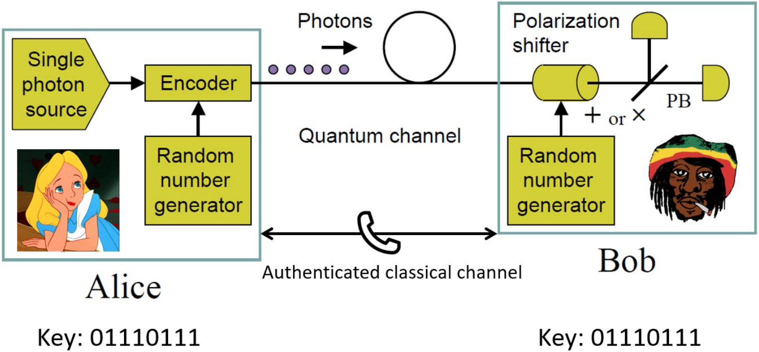
This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 675662

Outline

1. Introduction
2. Source imperfections
   - Photon number splitting attack
   - Techniques against the photon number splitting attack
3. Fundamental limitations
   - Repeaterless bound
   - Overcoming the repeaterless bound
4. Conclusions

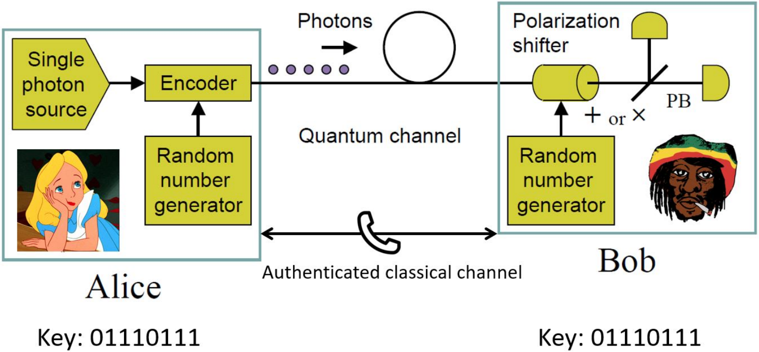
Basic setting for quantum key distribution

Task: obtain information-theoretically secure secret keys (in contrast to computational security)



Basic setting for quantum key distribution

Task: obtain information-theoretically secure secret keys (in contrast to computational security)



- Security is guaranteed by quantum physics
- The key is not perfect $\rightarrow$ error-correction and privacy amplification
- Figure of merits: secret key rate and distance

Milestones of quantum key distribution

- First idea: S. Wiesner in the 70s
- BB84 protocol [Bennett and Brassard, 1984] $\rightarrow$ polarization encoding in the X, Z-basis
- Entanglement-based schemes [Ekert, 1991] [Bennett, Brassard, and Mermin, 1992]

Milestones of quantum key distribution

- First idea: S. Wiesner in the 70s
- BB84 protocol [Bennett and Brassard, 1984] $\rightarrow$ polarization encoding in the X, Z-basis
- Entanglement-based schemes [Ekert, 1991] [Bennett, Brassard, and Mermin, 1992]
- First rigorous security proofs [Mayers, 1996], [Shor and Preskill, 2000]
- Detector side-channels [Makarov, 2009] $\rightarrow$ measurement-device independent QKD [Lo, Curty, and Qi, 2012]

Milestones of quantum key distribution

- First idea: S. Wiesner in the 70s
- BB84 protocol [Bennett and Brassard, 1984] $\rightarrow$ polarization encoding in the X, Z-basis
- Entanglement-based schemes [Ekert, 1991] [Bennett, Brassard, and Mermin, 1992]
- First rigorous security proofs [Mayers, 1996], [Shor and Preskill, 2000]
- Detector side-channels [Makarov, 2009] $\rightarrow$ measurement-device independent QKD [Lo, Curty, and Qi, 2012]
- Optical fiber-based setups: [Boaron et al., 2018] $\rightarrow$ 421 km, 6.5 bps [J.-P. Chen et al., 2020] $\rightarrow$ 509 km, 0.269 bps
- Satellite-based setups: [Liao et al., 2018] 7600 km on Earth
- Ultimate goal: improve the rate and the distance

Outline

1. Introduction
2. Source imperfections
   - Photon number splitting attack
   - Techniques against the photon number splitting attack
3. Fundamental limitations
   - Repeaterless bound
   - Overcoming the repeaterless bound
4. Conclusions

Source imperfections

High-quality and high-performance single photon sources $\rightarrow$ challenging

Instead:

- Weak coherent pulses (WCP)

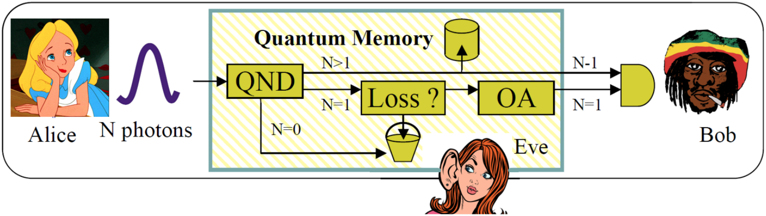
$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \xrightarrow[\text{randomization}]{\text{phase}} \rho = \sum_{n=0}^{\infty} \frac{e^{-\mu}\mu^n}{n!} |n\rangle\langle n|$$

with $\mu = |\alpha|^2$ average photon number

Practical sources have $2, 3 \cdots$-photon components

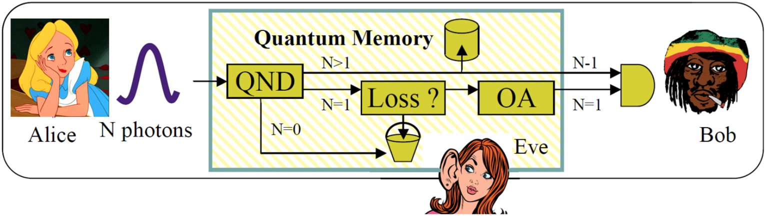
Photon number splitting (PNS) attack

- PNS attack [Lütkenhaus, 2000] $\rightarrow$ single photon sources are preferred



Photon number splitting (PNS) attack

- PNS attack [Lütkenhaus, 2000] $\rightarrow$ single photon sources are preferred

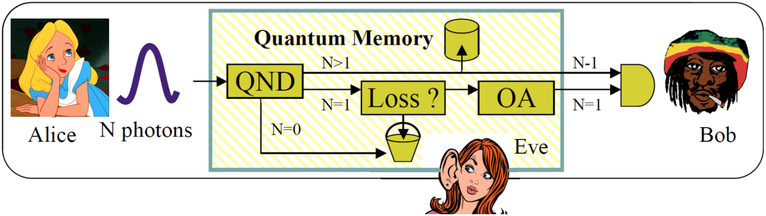


- Example: BB84 with WCPs have a key rate $\mathcal{O}(\eta^2)$ [Inamori, Lütkenhaus, and Mayers, 2007]

$$\eta = 10^{-\alpha l/10}$$

Photon number splitting (PNS) attack

- PNS attack [Lütkenhaus, 2000] → single photon sources are preferred



- Example: BB84 with WCPs have a key rate $\mathcal{O}(\eta^2)$ [Inamori, Lütkenhaus, and Mayers, 2007]

$$\eta = 10^{-\alpha l/10}$$

- Special techniques are required to avoid the PNS attack

Outline

1 Introduction

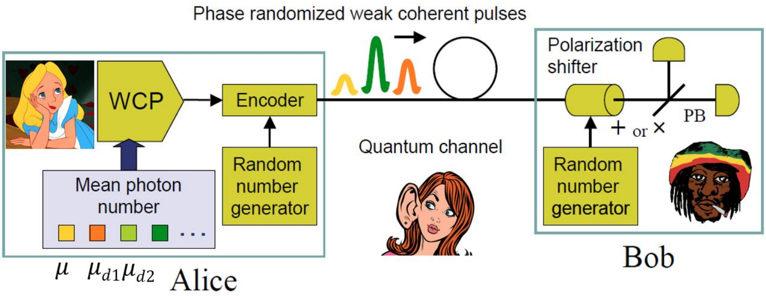
2 Source imperfections
- Photon number splitting attack
- Techniques against the photon number splitting attack

3 Fundamental limitations
- Repeaterless bound
- Overcoming the repeaterless bound

4 Conclusions

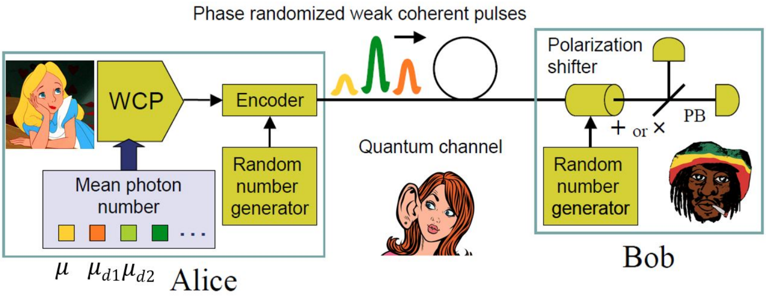
Decoy state QKD

[Hwang, 2003] $\rightarrow$ security proof [Lo, Ma, and K. Chen, 2005]



Decoy state QKD

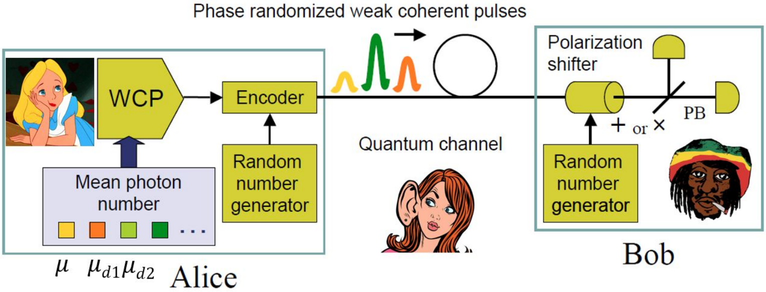
[Hwang, 2003] → security proof [Lo, Ma, and K. Chen, 2005]



- Alice uses phase-randomized WCPs with more intensities → $\mu, \mu_{d1}, \ldots$ to estimate the behavior of the channel better
- Field QKD networks: Vienna [Peev et al., 2009], Tokyo [Sasaki et al., 2011] and China [T.-Y. Chen et al., 2009]

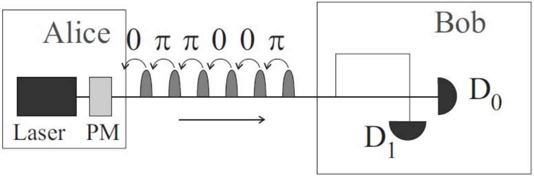
Decoy state QKD

[Hwang, 2003] → security proof [Lo, Ma, and K. Chen, 2005]



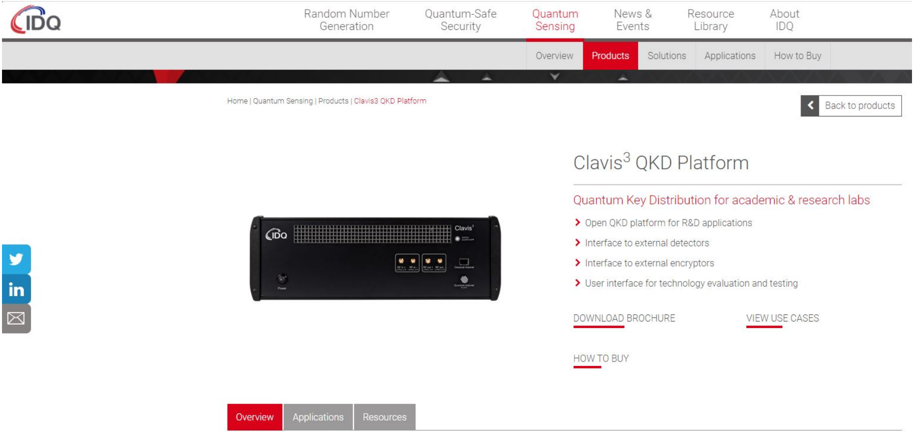
- Alice uses phase-randomized WCPs with more intensities → $\mu, \mu_{d1}, \ldots$ to estimate the behavior of the channel better
- Field QKD networks: Vienna [Peev et al., 2009], Tokyo [Sasaki et al., 2011] and China [T.-Y. Chen et al., 2009]
- There are simpler/more convenient approaches

Differential-phase-shift (DPS) QKD

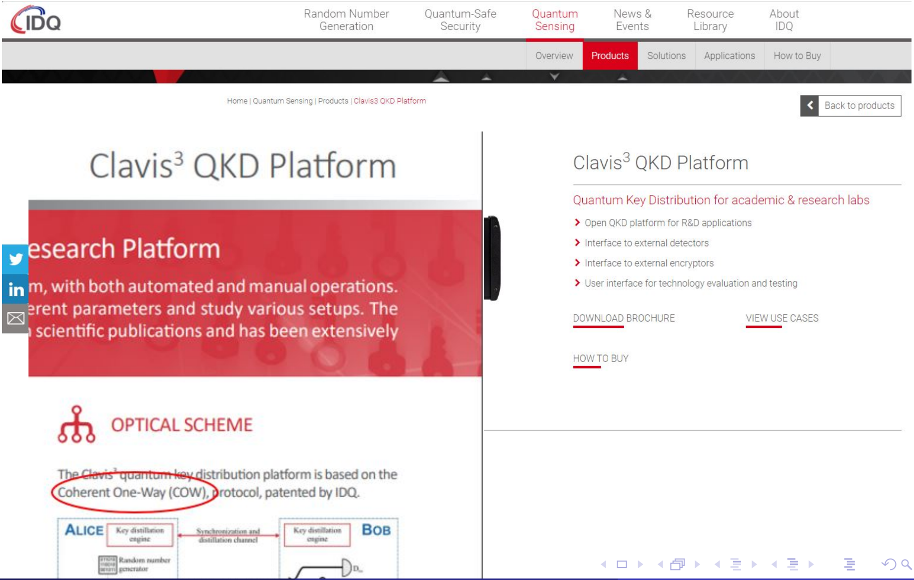


(figure from [Inoue, Waks, and Yamamoto, 2002])

The promising coherent-one-way (COW) protocol



The promising coherent-one-way (COW) protocol



The promising coherent-one-way (COW) protocol

Published: 09 February 2015

Provably secure and practical quantum key distribution over 307 km of optical fibre

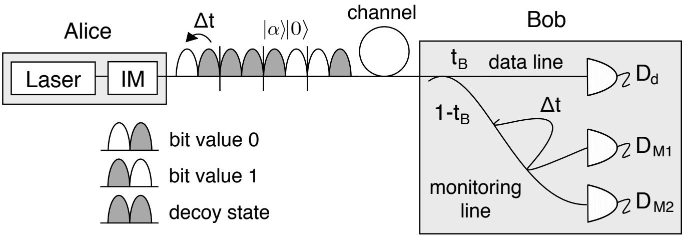
Boris Korzh, Charles Ci Wen Lim, Raphael Houlmann, Nicolas Gisin, Ming Jun Li, Daniel Nolan, Bruno Sanguinetti, Rob Thew & Hugo Zbinden

Nature Photonics **9**, 163–168(2015) | Cite this article

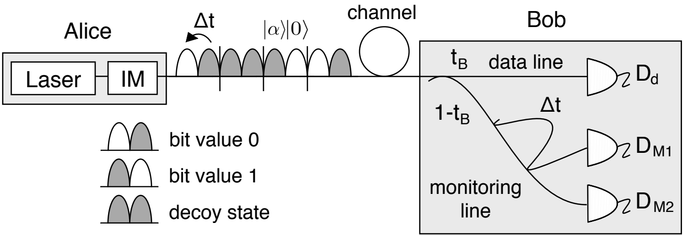
Abstract

Proposed in 1984, quantum key distribution (QKD) allows two users to exchange provably secure keys via a potentially insecure quantum channel[1]. Since then, QKD has attracted much attention and significant progress has been made both in theory and practice[2,3]. On

Layout of the COW protocol

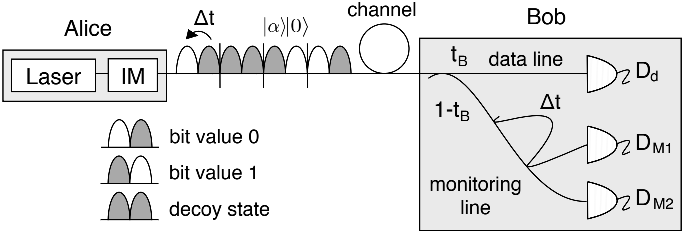


Layout of the COW protocol



- Monitored quantities:
  - Quantum bit error rate (QBER)
  - Visibilities $V_s = \frac{p(\mathrm{DM1}|s)-p(\mathrm{DM2}|s)}{p(\mathrm{DM1}|s)+p(\mathrm{DM2}|s)}$ with $s \in \{d, 01, 0d, 1d, dd\}$
  - as a function of the Gain (probability that Bob observes a detection event per signal)

Layout of the COW protocol



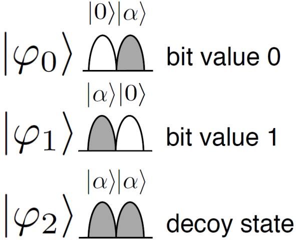
- Monitored quantities:
  - Quantum bit error rate (QBER)
  - Visibilities $V_s = \frac{p(\mathrm{DM1}|s)-p(\mathrm{DM2}|s)}{p(\mathrm{DM1}|s)+p(\mathrm{DM2}|s)}$ with $s \in \{d, 01, 0d, 1d, dd\}$
  - as a function of the Gain (probability that Bob observes a detection event per signal)
- Performance was not yet established
  - upper bound $\mathcal{O}(\eta)$
  - lower bound $\mathcal{O}(\eta^2)$

Failure of the COW protocol

We introduced an *intercept-resend* type of attack [González-Payo et al., 2020] (submitted to PRL) $\rightarrow$ entanglement breaking channel $\rightarrow$ no secret key can be generated [Curty, Lewenstein, and Lütkenhaus, 2004] $\rightarrow$ can the attack be detected?

Failure of the COW protocol

We introduced an *intercept-resend* type of attack [González-Payo et al., 2020] (submitted to PRL) $\rightarrow$ entanglement breaking channel $\rightarrow$ no secret key can be generated [Curty, Lewenstein, and Lütkenhaus, 2004] $\rightarrow$ can the attack be detected?

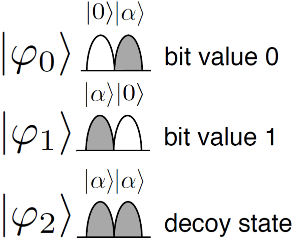


Unambiguous state discrimination (USD)

- $|\langle\varphi_0|\varphi_1\rangle| = e^{-|\alpha|^2}$
- $|\langle\varphi_0|\varphi_2\rangle| = e^{-|\alpha|^2/2}$
- inconclusive result $q_{\rm inc}$ $\rightarrow$ vacuum is resent

Failure of the COW protocol

We introduced an *intercept-resend* type of attack [González-Payo et al., 2020] (submitted to PRL) $\rightarrow$ entanglement breaking channel $\rightarrow$ no secret key can be generated [Curty, Lewenstein, and Lütkenhaus, 2004] $\rightarrow$ can the attack be detected?



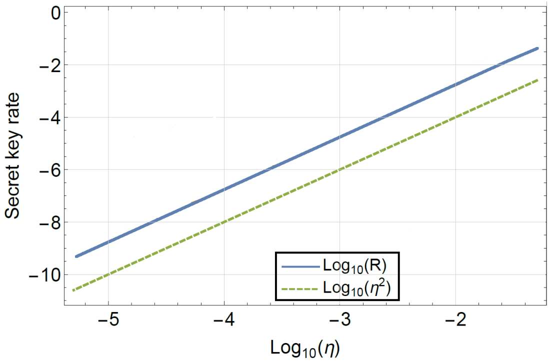
Unambiguous state discrimination (USD)

- $|\langle\varphi_0|\varphi_1\rangle| = e^{-|\alpha|^2}$
- $|\langle\varphi_0|\varphi_2\rangle| = e^{-|\alpha|^2/2}$
- inconclusive result $q_{\text{inc}} \rightarrow$ vacuum is resent

Eve only resends blocks of type "0...1" and USD $\rightarrow$ no errors (QBER=0), not breaking coherence (visibility 1) $\rightarrow$ the protocol is insecure

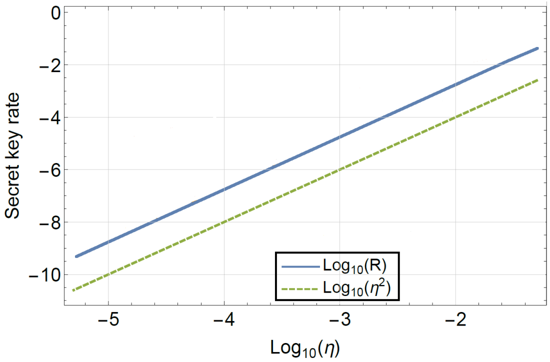
Upper bound for the secret key rate

- Given $\eta \to \exists\, \alpha_{\max}$ s.t. Eve cannot achieve QBER=0 and visibilities 1 at the gain Bob expects
- Trivial upper bound for the key rate $\eta|\alpha_{\max}(\eta)|^2$



Upper bound for the secret key rate

- Given $\eta \to \exists\, \alpha_{\max}$ s.t. Eve cannot achieve QBER=0 and visibilities 1 at the gain Bob expects
- Trivial upper bound for the key rate $\eta|\alpha_{\max}(\eta)|^2$



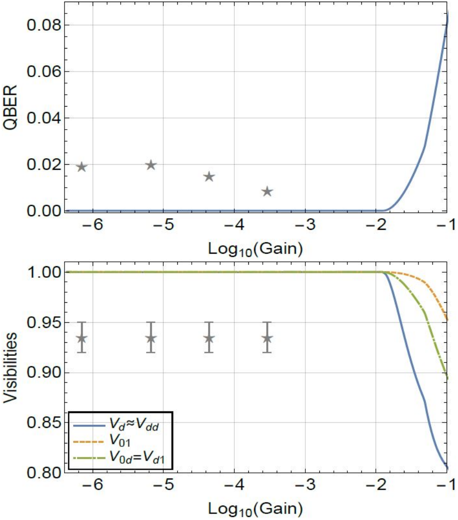
Upper bound for the secret key rate scales $\mathcal{O}(\eta^2) \to$ not suitable for long-distance $(\eta = 10^{-\alpha l/10}$ is the channel loss)

COW experiments are insecure

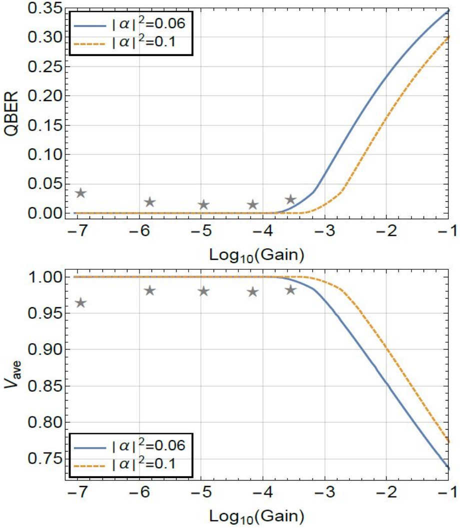
All experiments in scientific literature are insecure [Gisin et al., 2004], [Stucki, Brunner, et al., 2005], [Stucki, Walenta, et al., 2009] [Korzh et al., 2014]

COW experiments are insecure

[Stucki, Walenta, et al., 2009]

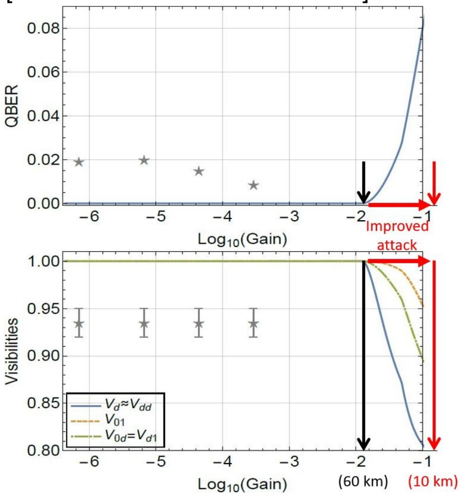


[Korzh et al., 2014]

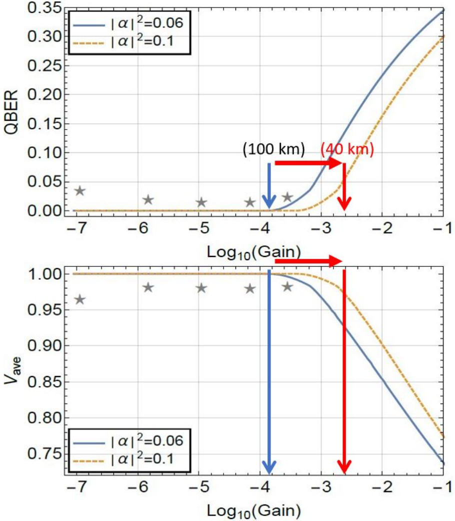


Performance of our improved attack

[Stucki, Walenta, et al., 2009]



[Korzh et al., 2014]



Outline

1. Introduction

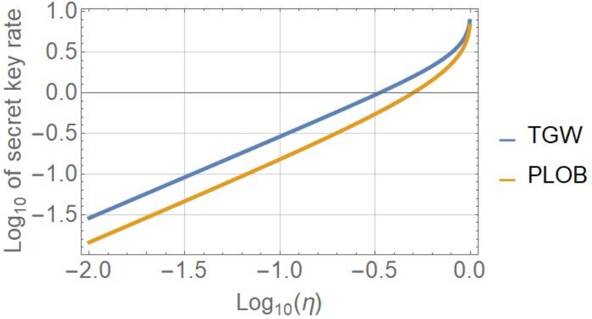
2. Source imperfections
   - Photon number splitting attack
   - Techniques against the photon number splitting attack

3. Fundamental limitations
   - Repeaterless bound
   - Overcoming the repeaterless bound

4. Conclusions

Repeaterless bounds

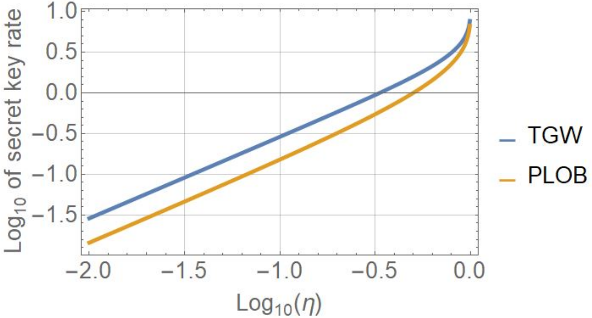
The secret key rate of *point-to-point* QKD protocols is *fundamentally* limited:



- $\log_2[(1+\eta)/(1-\eta)]$ [Takeoka, Guha, and Wilde, 2014] (TGW)
- $-\log_2(1-\eta)$ [Pirandola et al., 2017] (PLOB)

Repeaterless bounds

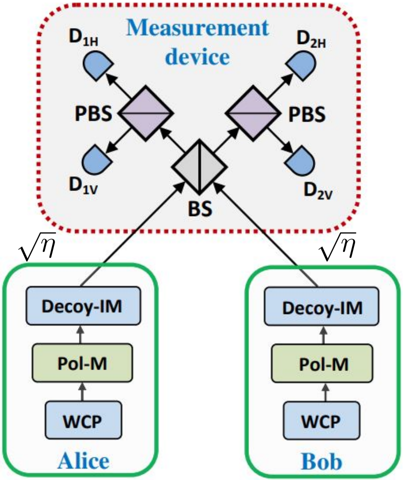
The secret key rate of *point-to-point* QKD protocols is *fundamentally* limited:



- $\log_2[(1+\eta)/(1-\eta)]$ [Takeoka, Guha, and Wilde, 2014] (TGW)
- $-\log_2(1-\eta)$ [Pirandola et al., 2017] (PLOB)
- $\mathcal{O}(\eta)$ for long distances $\rightarrow$ η decays exponentially with distance for optical fibers $\rightarrow$ intermediate nodes (and special techniques) are necessary to overcome

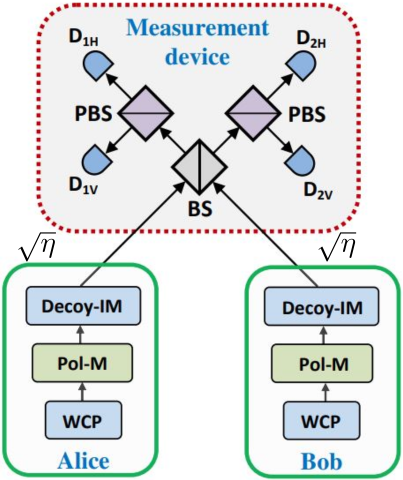
Example: measurement-device-independent (MDI) QKD

(figure from [Lo, Curty, and Qi, 2012])



Example: measurement-device-independent (MDI) QKD

(figure from [Lo, Curty, and Qi, 2012])



- key rate scales with $\mathcal{O}(\eta)$
- just the intermediate node itself is not enough to overcome the repeaterless bound

Outline

1 Introduction

2 Source imperfections
- Photon number splitting attack
- Techniques against the photon number splitting attack

3 Fundamental limitations
- Repeaterless bound
- Overcoming the repeaterless bound

4 Conclusions

Techniques to overcome the repeaterless bound

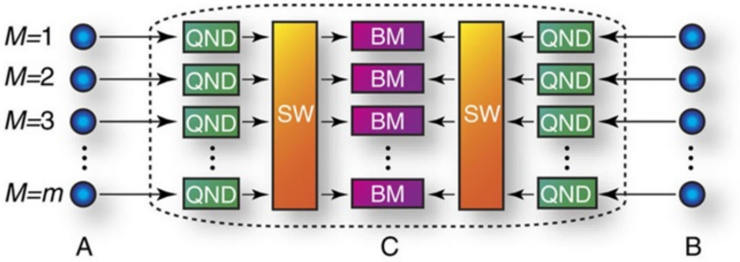
- $\eta^{1/n}$ (containing more intermediate nodes)
  - Full-scale quantum repeaters (e.g. based on entanglement swapping) $\rightarrow$ challenging experimentally

Techniques to overcome the repeaterless bound

- $\eta^{1/n}$ (containing more intermediate nodes)
  - Full-scale quantum repeaters (e.g. based on entanglement swapping) $\rightarrow$ challenging experimentally
- $\sqrt{\eta}$ improvement (one intermediate node)
  - Adaptive MDI-QKD approach [Azuma, Tamaki, and Munro, 2015]
  - Quantum memory based approach [Panayi et al., 2014]
  - Twin-field QKD [Lucamarini et al., 2018]

Adaptive MDI-QKD

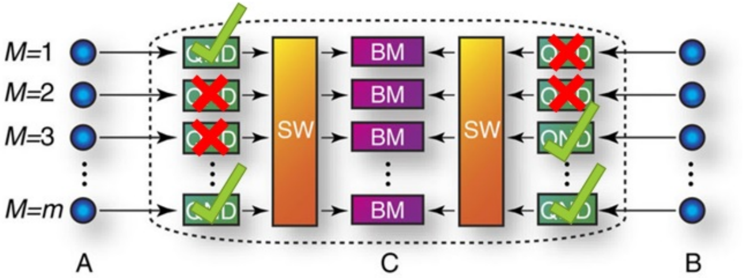
(figure from [Azuma, Tamaki, and Munro, 2015])



- parallelized version of MDI-QKD using a multiplexing technique and QND measurements
- single-photon sources are assumed
- key generation: enough for a photon to travel half the distance $\rightarrow \sqrt{\eta}$

Adaptive MDI-QKD

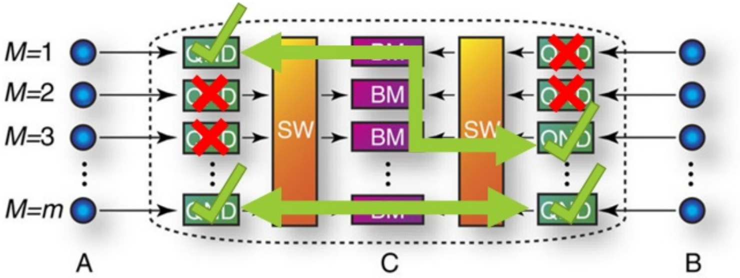
(figure from [Azuma, Tamaki, and Munro, 2015])



- parallelized version of MDI-QKD using a multiplexing technique and QND measurements
- single-photon sources are assumed
- key generation: enough for a photon to travel half the distance $\rightarrow \sqrt{\eta}$

Adaptive MDI-QKD

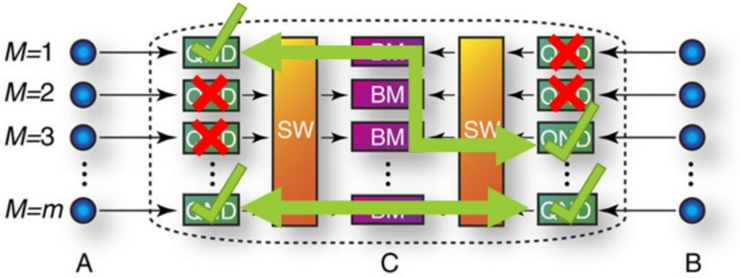
(figure from [Azuma, Tamaki, and Munro, 2015])



- parallelized version of MDI-QKD using a multiplexing technique and QND measurements
- single-photon sources are assumed
- key generation: enough for a photon to travel half the distance $\rightarrow \sqrt{\eta}$

Adaptive MDI-QKD

(figure from [Azuma, Tamaki, and Munro, 2015])



- parallelized version of MDI-QKD using a multiplexing technique and QND measurements
- single-photon sources are assumed
- key generation: enough for a photon to travel half the distance $\rightarrow \sqrt{\eta}$

$\mathcal{O}(\sqrt{\eta})$ but single photon sources are assumed

Adaptive MDI-QKD with realistic devices

[Trényi, Azuma, and Curty, 2019]

- single-photon sources $\to$ heralded PDC sources $\sum_{n=0}^{\infty} \sqrt{p_n} \, |\phi_n\rangle$
- perfect EPR sources in the QND $\to$ PDC sources $\sum_{m=0}^{\infty} \sqrt{q_m} \, |\phi_m\rangle$

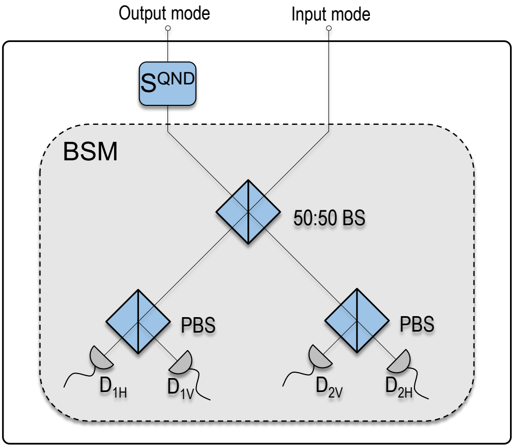
Adaptive MDI-QKD with realistic devices

[Trényi, Azuma, and Curty, 2019]

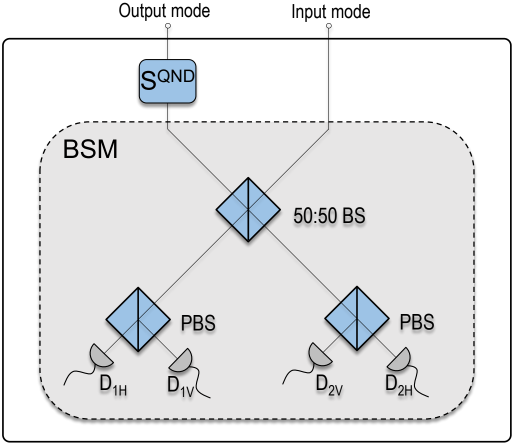
- single-photon sources $\rightarrow$ heralded PDC sources $\sum_{n=0}^{\infty} \sqrt{p_n} \, |\phi_n\rangle$
- perfect EPR sources in the QND $\rightarrow$ PDC sources $\sum_{m=0}^{\infty} \sqrt{q_m} \, |\phi_m\rangle$

$$p_n = \frac{(n+1)(\lambda')^n}{(1+\lambda')^{n+2}} \text{ and } q_m = \frac{(m+1)\lambda^m}{(1+\lambda)^{m+2}} \text{ with}$$
$$|\phi_n\rangle = \frac{1}{\sqrt{n+1}} \sum_{m=0}^{n} (-1)^m \, |n-m, m\rangle_a \, |m, n-m\rangle_b$$

The QND measurement



The QND measurement



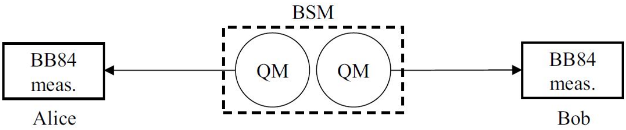
- Impossible to beat the repeaterless bound with PDC sources
- Characterized allowable q_2/q_1 and p_2/p_1 to overcome the bound

A quantum memory based approach

[Luong et al., 2016]

- perfect Bell-states are emitted by the QMs → first towards Alice → then towards Bob → once both QMs are loaded, a BSM is performed

(figure from [Luong et al., 2016])

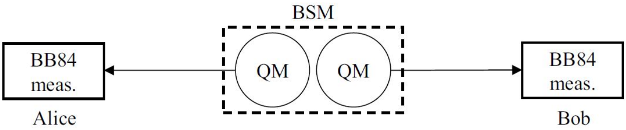


A quantum memory based approach

[Luong et al., 2016]

- perfect Bell-states are emitted by the QMs → first towards Alice → then towards Bob → once both QMs are loaded, a BSM is performed

(figure from [Luong et al., 2016])



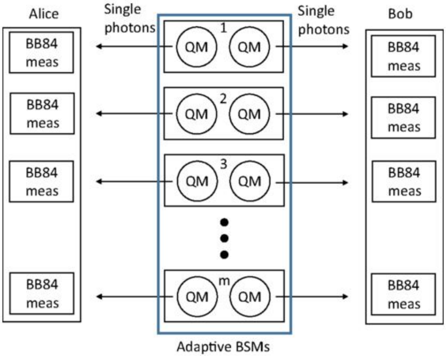
Parameters

- T_2: dephasing-time constant of the QMs
- η_{total}: total efficiency, $\eta_{\text{total}} = \eta_{\text{c}}\eta_{\text{p}}\eta_{\text{d}}$
    - η_{p}: preparation efficiency
    - η_{c}: photon-fiber coupling efficiency, wavelength conversion
    - η_{d}: detection efficiency

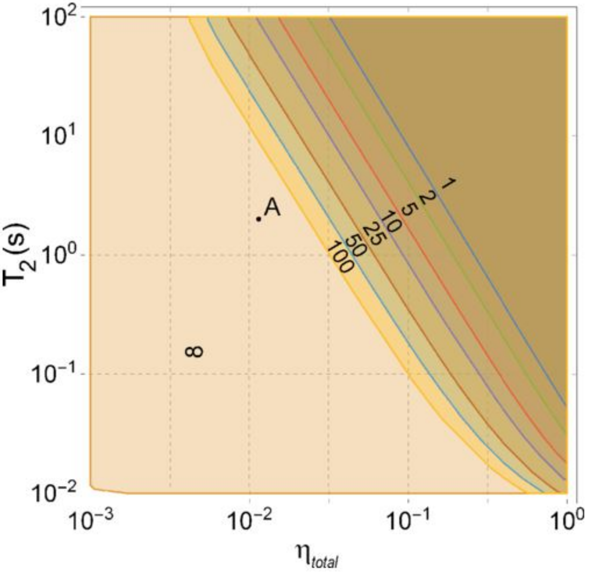
Improving the previous QM based approach

[Trényi and Lütkenhaus, 2020]

- multiplexing to relax the conditions on T_2
- multiple QMs working in parallel $\rightarrow$ a loaded QM has to wait less $\rightarrow$ for a pair $\rightarrow$ improved key rate



Improving the previous QM based approach



Conclusions

- COW protocol is not appropriate for long-distance QKD

Conclusions

- COW protocol is not appropriate for long-distance QKD
- Adaptive MDI-QKD cannot beat the repeaterless bound with PDC sources

Conclusions

- COW protocol is not appropriate for long-distance QKD
- Adaptive MDI-QKD cannot beat the repeaterless bound with PDC sources
- Extension of a QM-based QKD protocol

Conclusions

- COW protocol is not appropriate for long-distance QKD
- Adaptive MDI-QKD cannot beat the repeaterless bound with PDC sources
- Extension of a QM-based QKD protocol

Thank you very much for your attention!

Conclusions

- COW protocol is not appropriate for long-distance QKD
- Adaptive MDI-QKD cannot beat the repeaterless bound with PDC sources
- Extension of a QM-based QKD protocol

Thank you very much for your attention!

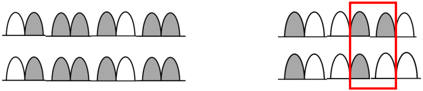
Questions?

Why the "0...1" blocks?

Alice sends:	0	1	1	0	d	1	d	d	0	1	0	1	0
Eve gets:	inc	1	1	0	d	1	d	inc	0	1	0	inc	0

Alice sends:

Eve gets:



How do we improve?

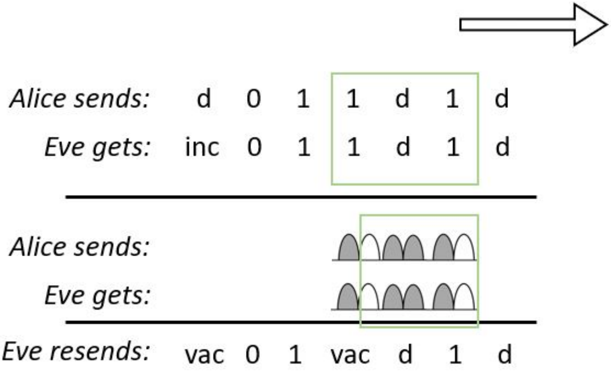
Emitting probability		Eve's POVM elements			
	Alice's signal	E_0	E_1	E_2	E_3
$(1-f)/2$	$\lvert\varphi_0\rangle$	q_{s}	q_{f}	q_{f}	q_{inc}
$(1-f)/2$	$\lvert\varphi_1\rangle$	q_{f}	q_{s}	q_{f}	q_{inc}
f	$\lvert\varphi_2\rangle$	q_{f}	q_{f}	q_{s}	q_{inc}

$$\Downarrow$$

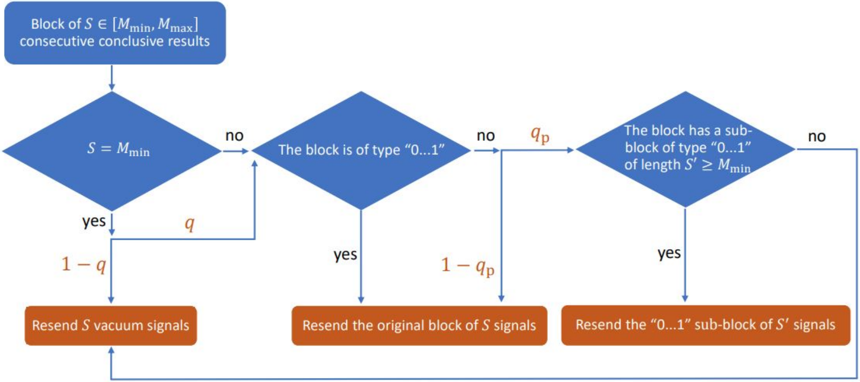
Emitting probability		Eve's POVM elements			
	Alice's signal	E_0	E_1	E_2	E_3
$(1-f)/2$	$\lvert\varphi_0\rangle$	$q_{\mathrm{s}}^{\mathrm{s}}$	$q_{\mathrm{f}}^{\mathrm{s}}$	$q_{\mathrm{f}}^{\mathrm{s}}$	$q_{\mathrm{inc}}^{\mathrm{s}}$
$(1-f)/2$	$\lvert\varphi_1\rangle$	$q_{\mathrm{f}}^{\mathrm{s}}$	$q_{\mathrm{s}}^{\mathrm{s}}$	$q_{\mathrm{f}}^{\mathrm{s}}$	$q_{\mathrm{inc}}^{\mathrm{s}}$
f	$\lvert\varphi_2\rangle$	$q_{\mathrm{f}}^{\mathrm{d}}$	$q_{\mathrm{f}}^{\mathrm{d}}$	$q_{\mathrm{s}}^{\mathrm{d}}$	$q_{\mathrm{inc}}^{\mathrm{d}}$

How do we improve?

- When Eve can perform USD $\rightarrow$ she does not just send “0...1” but also sends all the blocks that are bordered by vacuum pulses $\rightarrow$ still not breaking coherence



Full attack



Block of $S \in [M_{\mathrm{min}}, M_{\mathrm{max}}]$ consecutive conclusive results
$S = M_{\mathrm{min}}$
no
The block is of type "0...1"
no
q_{p}
The block has a sub-block of type "0...1" of length $S' \geq M_{\mathrm{min}}$
no
yes
q
$1 - q$
yes
$1 - q_{\mathrm{p}}$
yes
Resend S vacuum signals
Resend the original block of S signals
Resend the "0...1" sub-block of S' signals

Twin-field (TF) QKD

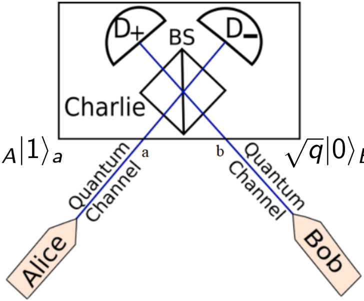
- First introduced in [Lucamarini et al., 2018] $\rightarrow$ based on single-photon interference $\rightarrow \mathcal{O}(\sqrt{\eta})$ but security proof only against some special type of attacks and challenging experimentally
- Simplifications [Curty, Azuma, and Lo, 2019] and experiments [Zhong et al., 2019] [J.-P. Chen et al., 2020]

Twin-field (TF) QKD

- First introduced in [Lucamarini et al., 2018] $\rightarrow$ based on single-photon interference $\rightarrow \mathcal{O}(\sqrt{\eta})$ but security proof only against some special type of attacks and challenging experimentally
- Simplifications [Curty, Azuma, and Lo, 2019] and experiments [Zhong et al., 2019] [J.-P. Chen et al., 2020]

(figure from [Jie Lin and Lütkenhaus, 2018])

$\sqrt{q}|0\rangle_A|0\rangle_a + \sqrt{1-q}|1\rangle_A|1\rangle_a$



$\sqrt{q}|0\rangle_B|0\rangle_b + \sqrt{1-q}|1\rangle_B|1\rangle_b$