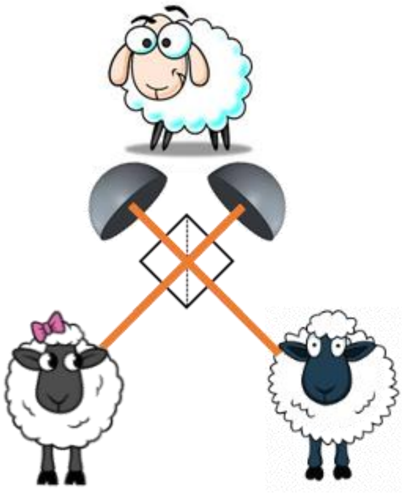
TOSHIBA
Leading Innovation >>>

QCrypt 2018
Shanghai, China
27-31 August 2018

Recent progress on Measurement-Device-Independent (MDI) Quantum Key Distribution (QKD)



Marco Lucamarini

Quantum Information Group
Cambridge Research Laboratory
Toshiba Research Europe Ltd

Copyright 2018, Toshiba Corporation

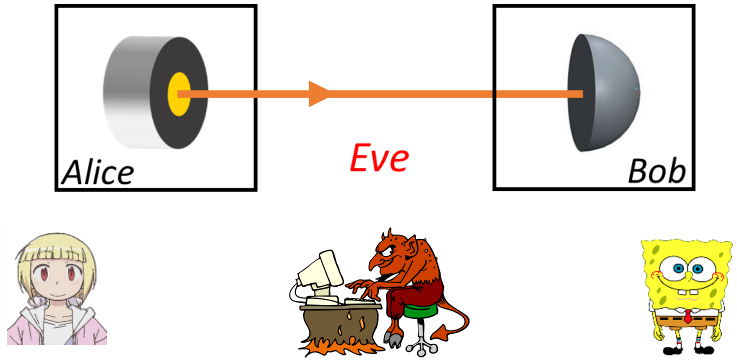
A couple of useful links

Joshua Slater's tutorial on MDI-QKD
QCrypt 2014 (Paris, France)
https://youtu.be/WL7OPSO0s_s

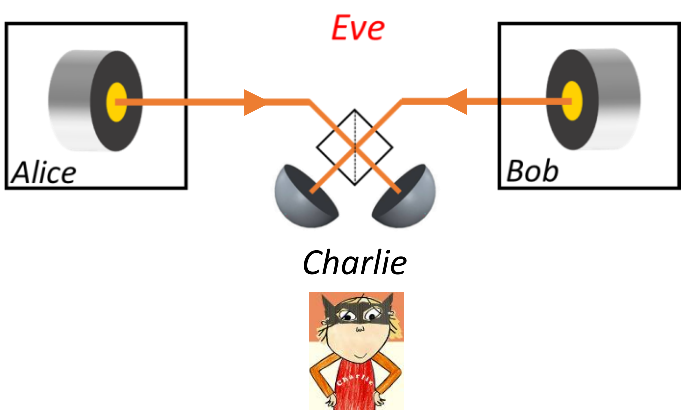
ML's video lecture on MDI-QKD
1st QCall school (2018, Baiona, Spain)
http://tv.uvigo.es/matterhorn/36609

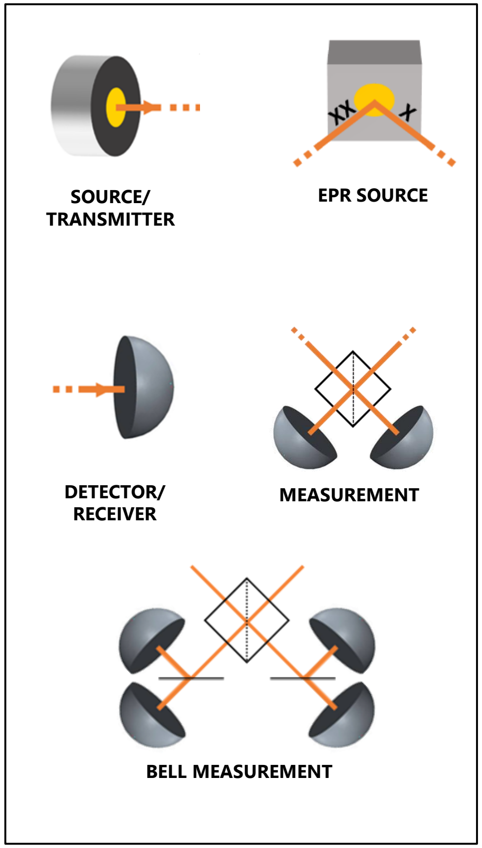
MDI QKD - Notation

QKD



MDI-QKD





Outline of this tutorial

1. Motivation and Introduction of MDI-QKD
    - Detector vulnerabilities and trusted networks
    - Basic features of MDI-QKD
2. MDI-QKD origin and working mechanism
    - Optical Interference
    - Entanglement swapping
3. Experiments
4. Variants
    - Twin-Field QKD

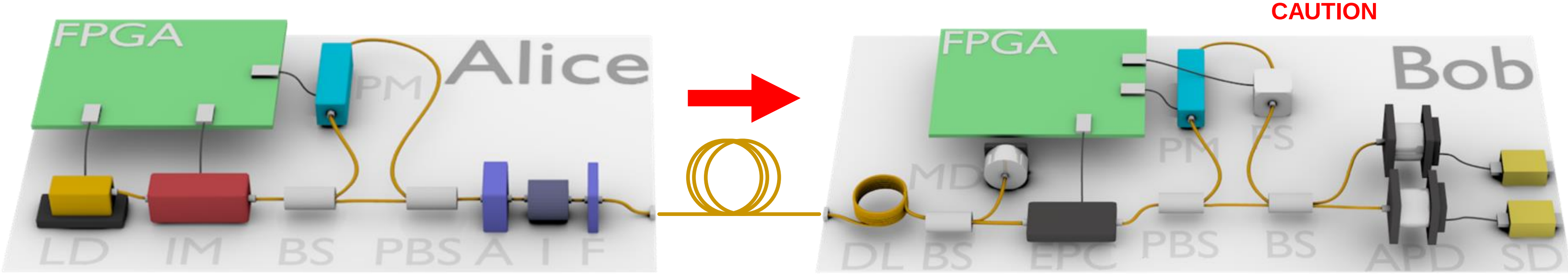
Outline of this tutorial

1. Motivation and Introduction of MDI-QKD
   - Detector vulnerabilities and trusted networks
   - Basic features of MDI-QKD
2. MDI-QKD origin and working mechanism
   - Optical Interference
   - Entanglement swapping
3. Experiments
4. Variants
   - Twin-Field QKD

Motivation 1: Implementation Security

Motivation 1: Implementation Security

Typical fibre-based one-way QKD setup



Laser Diode: 1GHz rep rate, characterised to have phase randomised pulses.	Intensity Modulator: BB84 with 3 decoy states, + stronger stabilisation pulses.	AMZI: Information encoded on phase. Polarisation used to increase efficiency.	Attenuator: Feedback controlled to 0.5 photons per pulse. Increases loss for Trojan horse.	Isolator: Increases loss for incoming Trojan horse light.	Band Pass Filter: Limits Trojan horse to 1550nm

Delay Line: Trojan horse security.	Monitor Diode: Monitors input power for basic check against APD blinding attacks.	Polarisation Control: Automatic stabilisation to correct for polarisation drift in fibre.	Interferometer Control: Automatic stabilisation to match Alice and Bob interferometer path lengths.	Detector gate: Automatic stabilisation to match gate with photon arrival.	APDs: Self-differenced for GHz gating. Temperature monitored for basic APD blinding attack prevention.

Most targeted components

Secure quantum key distribution

Hoi-Kwong Lo[1†], Marcos Curty[2†] and Kiyoshi Tamaki[3†]

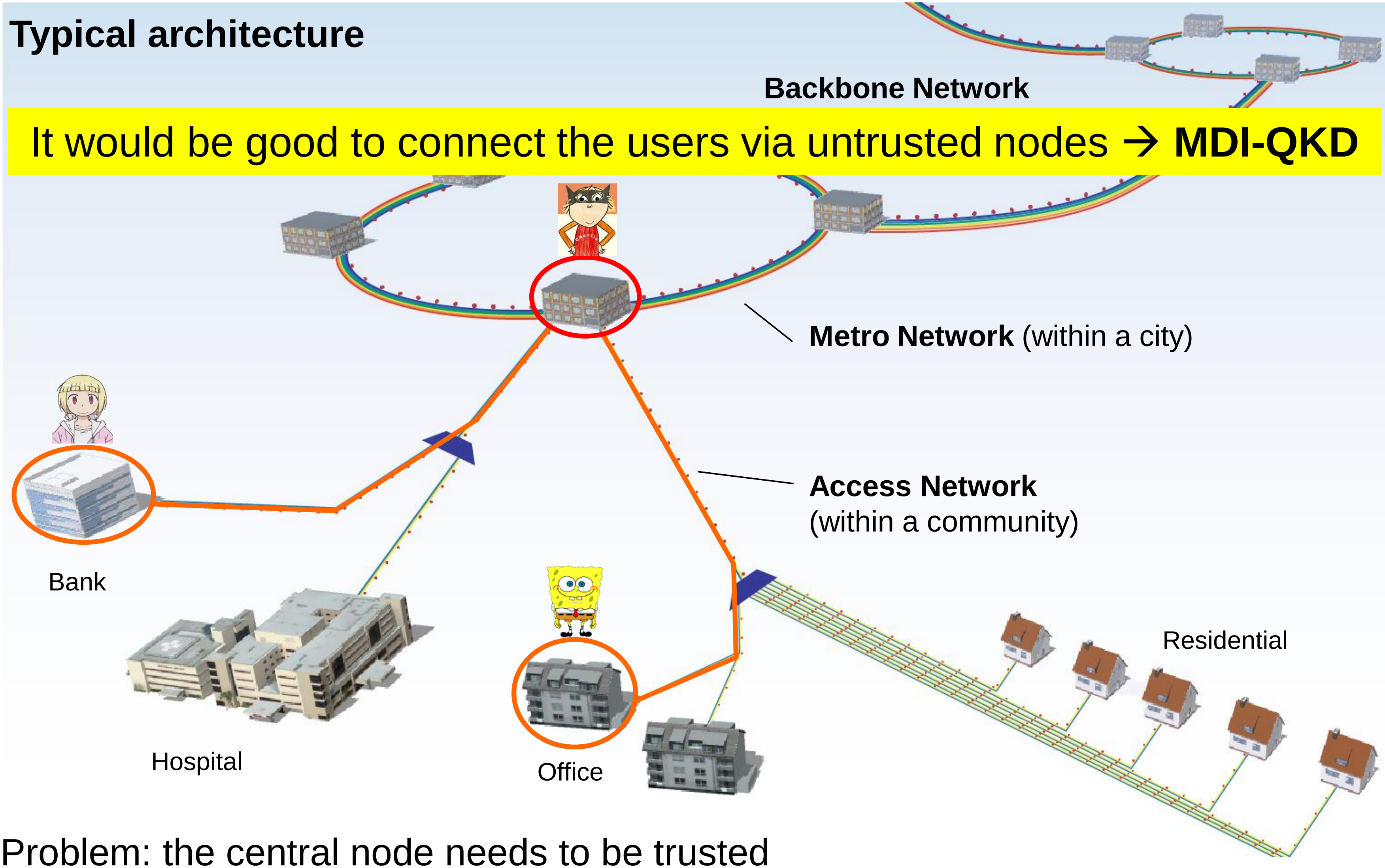
ArXiv:1505.05303.
Nature Photonics **8**, 595-604 (2014).

Attack	*Target component*	*Tested system*
Time-shift [76–79]	Detector	Commercial system
Time-information [80]	Detector	Research system
Detector-control [81–83]	Detector	Commercial system
Detector-control [84]	Detector	Research system
Detector dead-time [85]	Detector	Research system
Channel calibration [86]	Detector	Commercial system
Faraday-mirror [88]	Faraday mirror	Theory
Wavelength [89]	Beam-splitter	Theory
Phase information [90]	Source	Research system
Device calibration [91]	Local oscillator	Research system

It would be good to remove assumptions from detectors in QKD → **MDI-QKD**

Motivation 2: Trusted-node Networks

Typical architecture



Problem: the central node needs to be trusted

Measurement-Device-Independent Quantum Key Distribution over Untrustful Metropolitan Network

Yan-Lin Tang,[1,2] Hua-Lei Yin,[1,2] Qi Zhao,[3] Hui Liu,[1,2] Xiang-Xiang Sun,[1,2] Ming-Qi Huang,[1,2] Wei-Jun Zhang,[4] Si-Jing Chen,[4] Lu Zhang,[4] Li-Xing You,[4] Zhen Wang,[4] Yang Liu,[1,2] Chao-Yang Lu,[1,2] Xiao Jiang,[1,2,*] Xiongfeng Ma,[3,†] Qiang Zhang,[1,2,‡] Teng-Yun Chen,[1,2,§] and Jian-Wei Pan[1,2,∥]

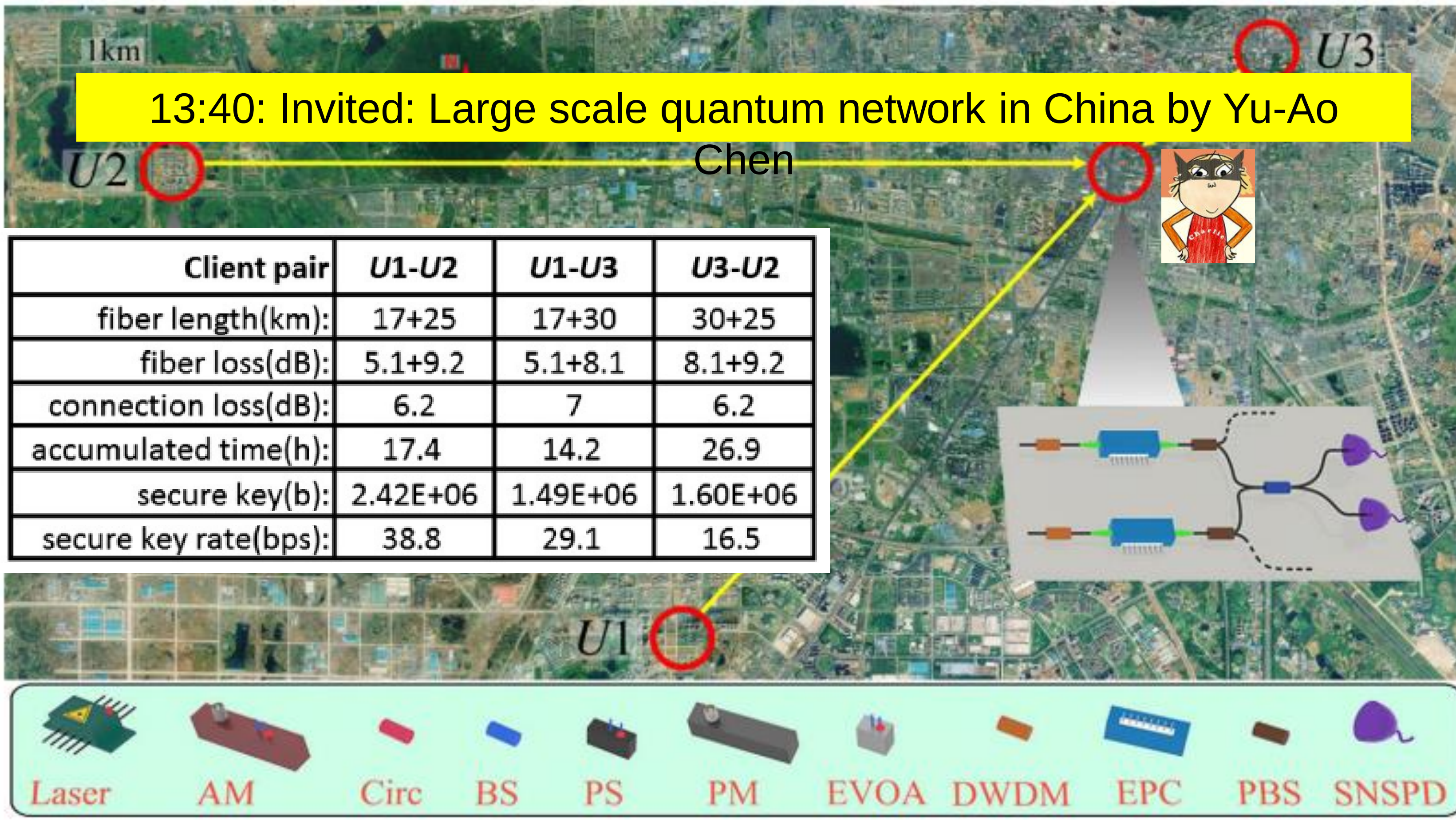
Phys. Rev. X **6**, 011024 (2016)

Measurement-Device-Independent Quantum Key Distribution over Untrustful Metropolitan Network

Yan-Lin Tang,[1,2] Hua-Lei Yin,[1,2] Qi Zhao,[3] Hui Liu,[1,2] Xiang-Xiang Sun,[1,2] Ming-Qi Huang,[1,2] Wei-Jun Zhang,[4] Si-Jing Chen,[4] Lu Zhang,[4] Li-Xing You,[4] Zhen Wang,[4] Yang Liu,[1,2] Chao-Yang Lu,[1,2] Xiao Jiang,[1,2,*] Xiongfeng Ma,[3,†] Qiang Zhang,[1,2,‡] Teng-Yun Chen,[1,2,§] and Jian-Wei Pan[1,2,‖]

Phys. Rev. X **6**, 011024 (2016)

13:40: Invited: Large scale quantum network in China by Yu-Ao Chen



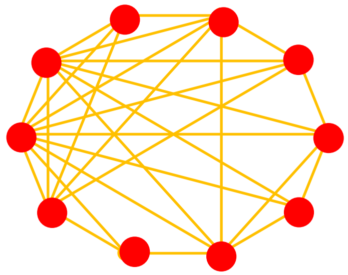
Client pair	*U1-U2*	*U1-U3*	*U3-U2*
fiber length(km):	17+25	17+30	30+25
fiber loss(dB):	5.1+9.2	5.1+8.1	8.1+9.2
connection loss(dB):	6.2	7	6.2
accumulated time(h):	17.4	14.2	26.9
secure key(b):	2.42E+06	1.49E+06	1.60E+06
secure key rate(bps):	38.8	29.1	16.5

- 8-by-4 mechanical optical switch to route the three users to the relay
- randomly switch any two users to the relay every two hours

MDI/QKD Reconfigurable Network

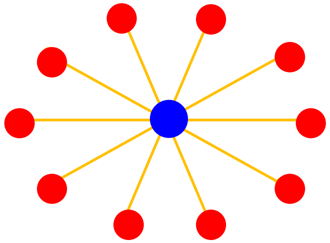
- MDI-QKD well matches star networks: it connects all the nodes with a minimum amount of optical links

Fully connected network with N+1 nodes



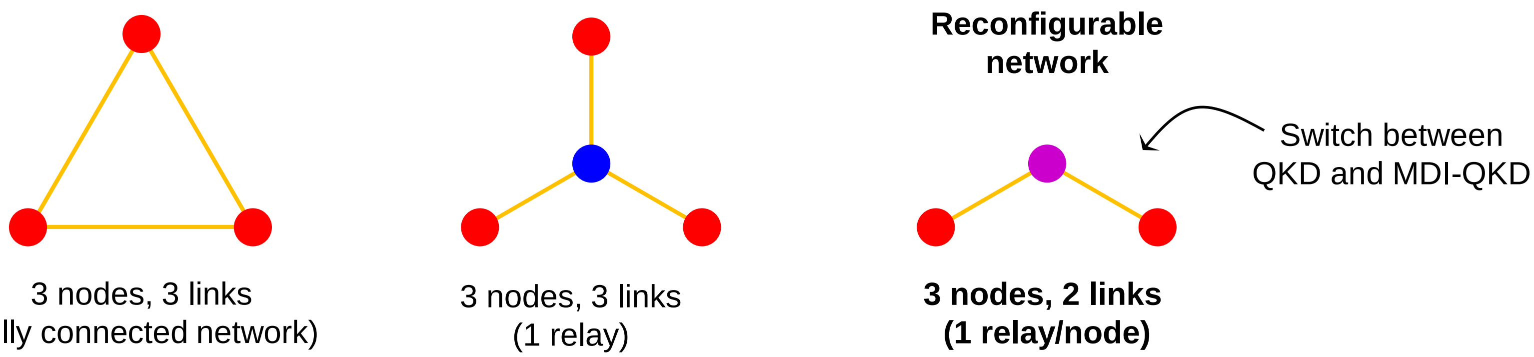
N(N+1)/2 physical links

Fully connected MDI-QKD network with N+1 nodes

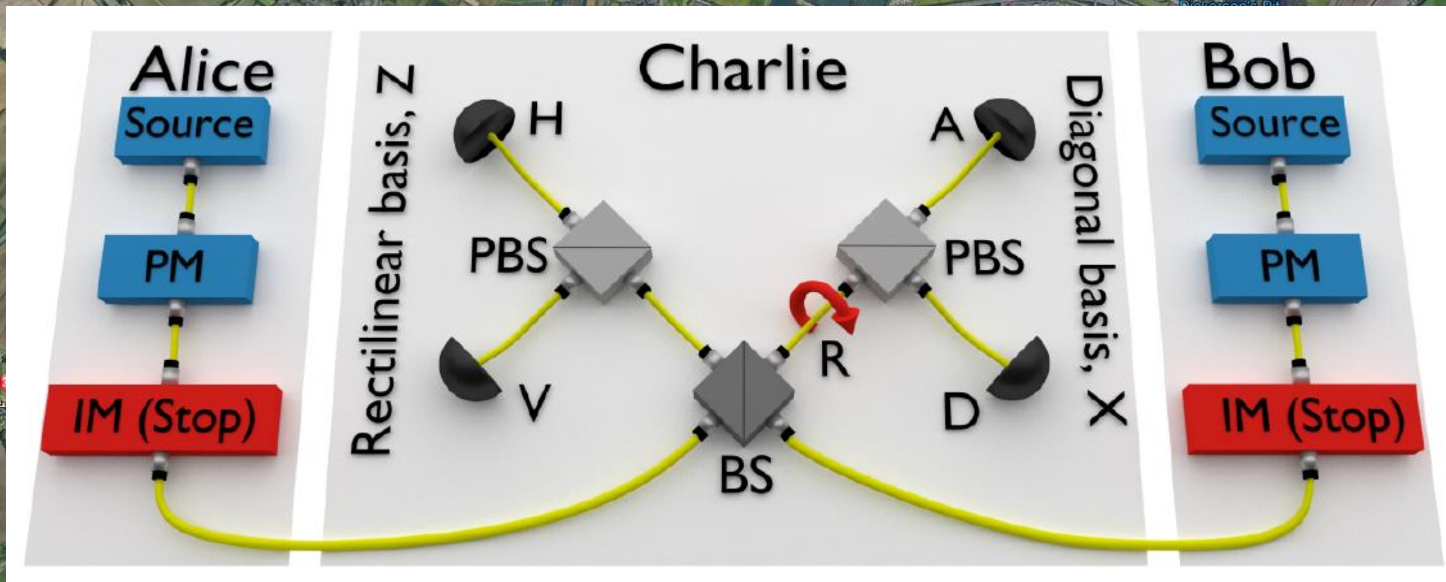


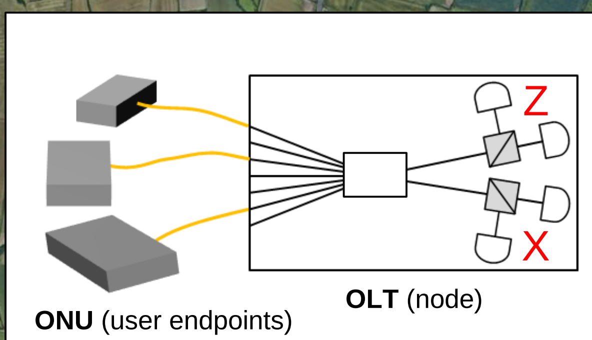
N physical links

- See also the 11:25 am talk by Mike Wang
  "*Enabling a scalable high-rate MDI-QKD network: theory and experiment*".

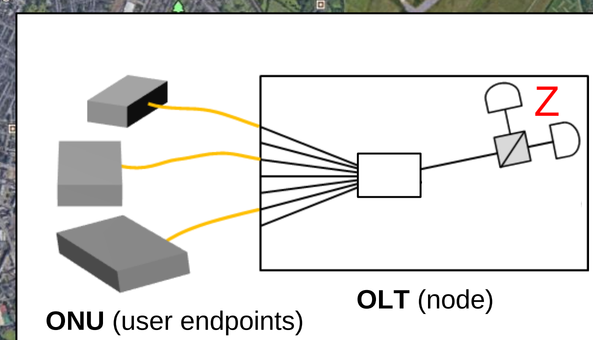


MDI/QKD Reconfigurable Network





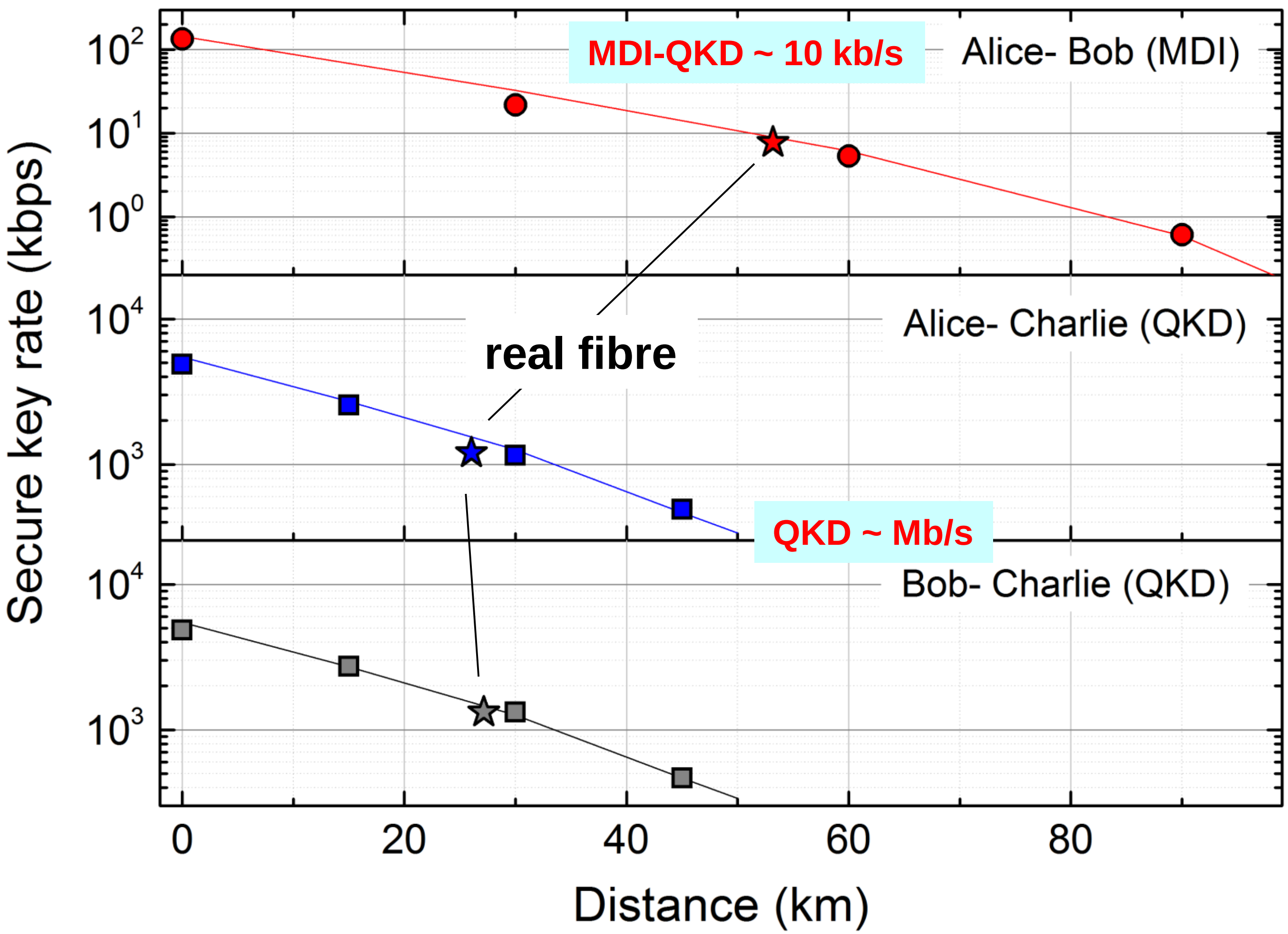
QKD/Trusted node

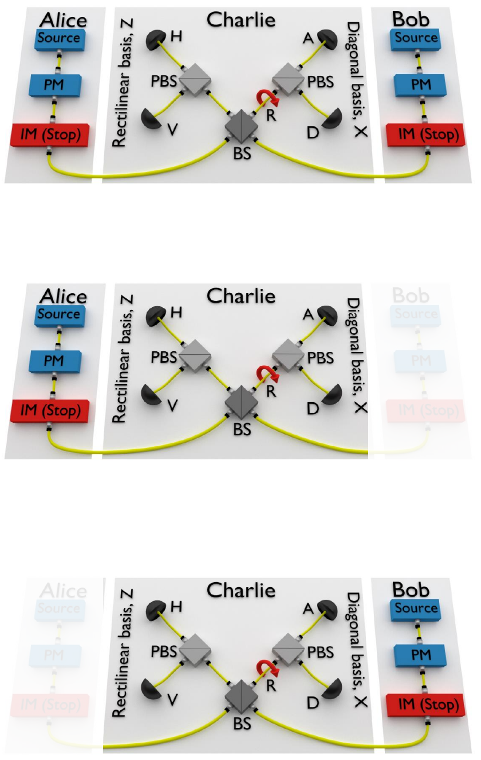


MDI-QKD/Untrusted node

G. L. Roberts *et al.*, Nature Communications **8**, 1098 (2017).

MDI/QKD Reconfigurable Network

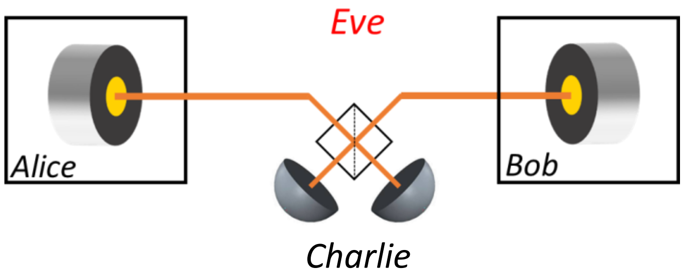




G. L. Roberts *et al.*, Nature Communications **8**, 1098 (2017).

Measurement-device-independent (MDI) QKD

MDI-QKD

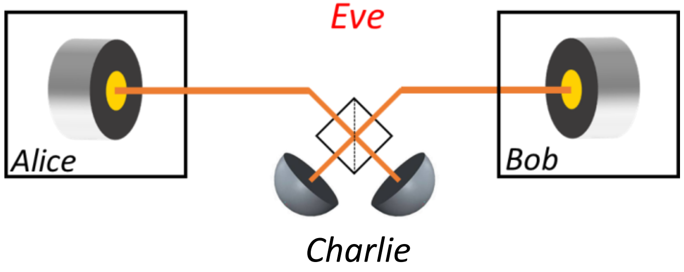


Pros & Cons

- *Any* detector vulnerability is removed
- Users are linked by an untrusted relay
- Operational range is longer than QKD
- The key rate is smaller than QKD

Measurement-device-independent (MDI) QKD

MDI-QKD



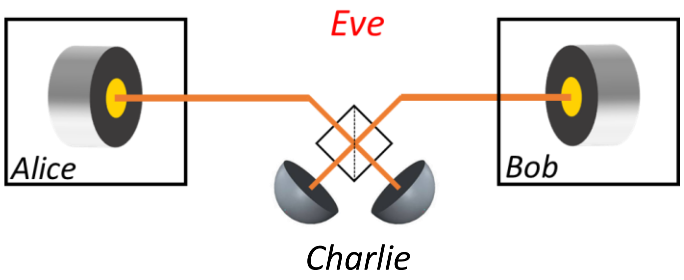
Pros & Cons

- *Any* detector vulnerability is removed
- Users are linked by an untrusted relay
- Operational range is longer than QKD
- The key rate is smaller than QKD

If we consider the progress in the last 4 months we have to revise the last statement

Measurement-device-independent (MDI) QKD

MDI-QKD



Pros & Cons

- *Any* detector vulnerability is removed
- Users are linked by an untrusted relay
- Operational range is longer than QKD
- The key rate is smaller than QKD for standard MDI-QKD, not for *Twin-Field QKD*

If we consider the progress in the last 4 months we have to revise the last statement

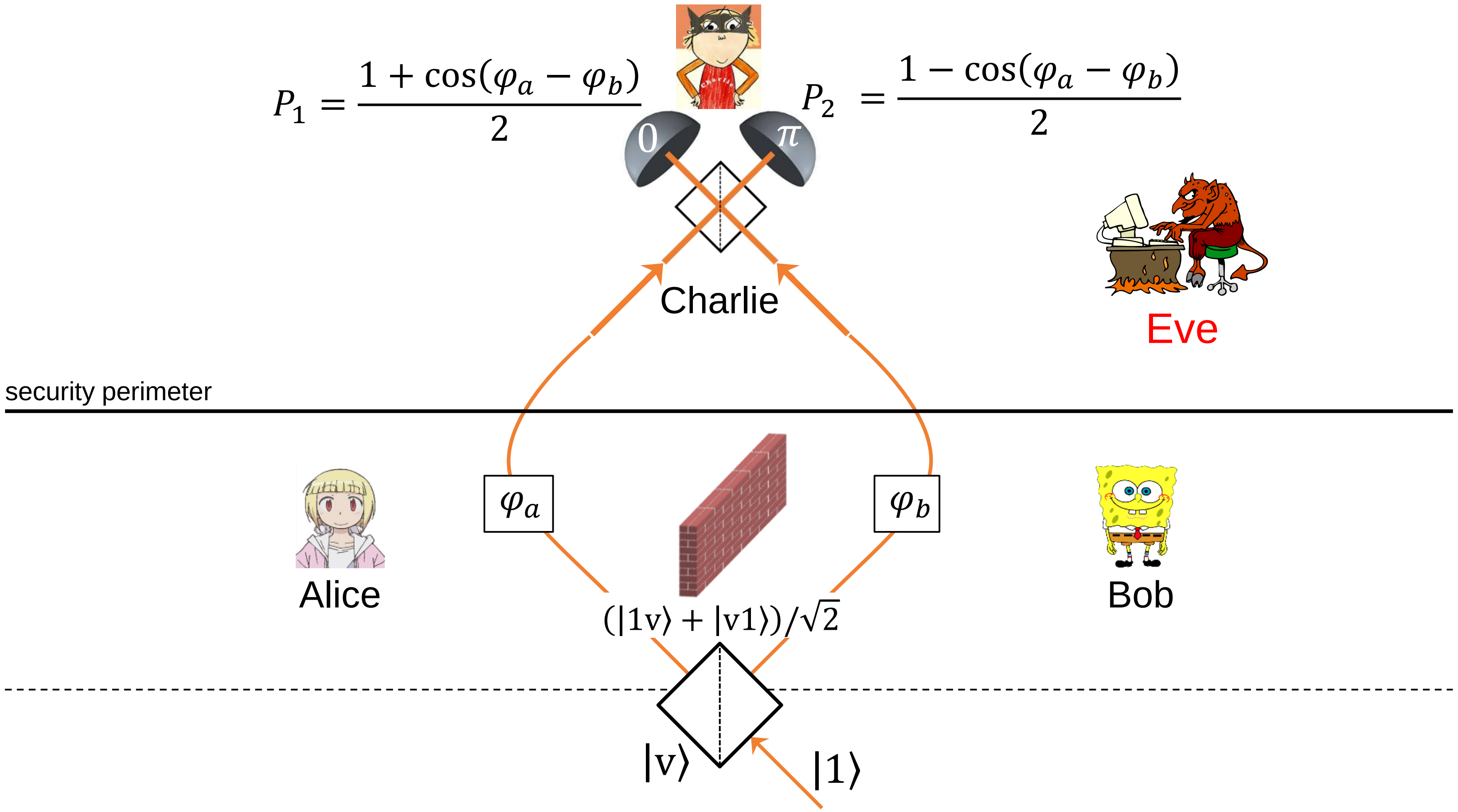
Outline of this tutorial

1. Motivation and Introduction of MDI-QKD
   - Detector vulnerabilities and trusted networks
   - Basic features of MDI-QKD
2. MDI-QKD origin and working mechanism
   - Optical Interference
   - Entanglement swapping
3. Experiments
4. Variants
   - Twin-Field QKD

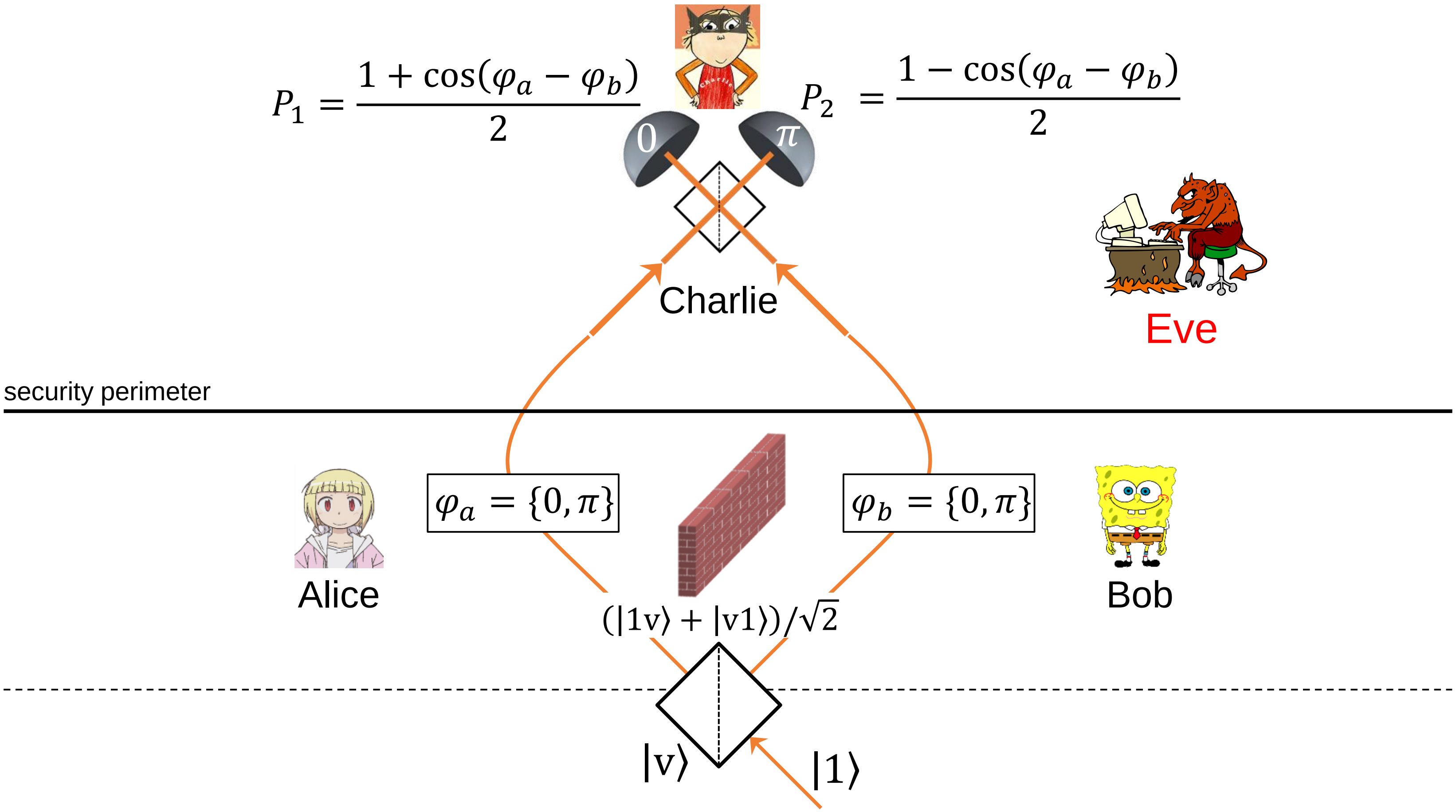
Outline of this tutorial

1. Motivation and Introduction of MDI-QKD
    - Detector vulnerabilities and trusted networks
    - Basic features of MDI-QKD
2. MDI-QKD origin and working mechanism
    - Optical Interference
    - Entanglement swapping
3. Experiments
4. Variants
    - Twin-Field QKD

Simple interferometric MDI-QKD scheme



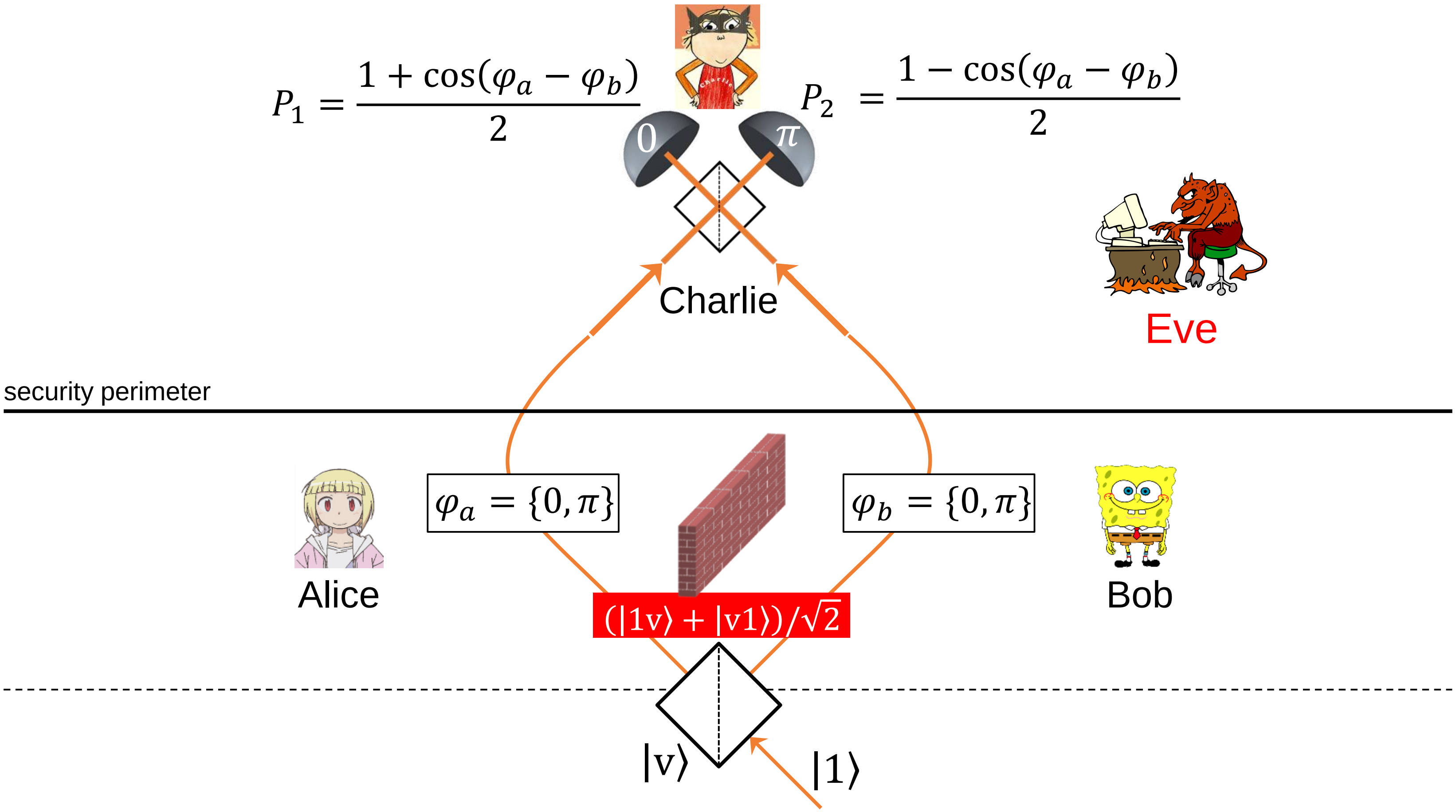
Simple interferometric MDI-QKD scheme



With this scheme we achieve the MDI goals:

1) Detectors are outside the security perimeter
2) The relay is untrusted

Simple interferometric MDI-QKD scheme



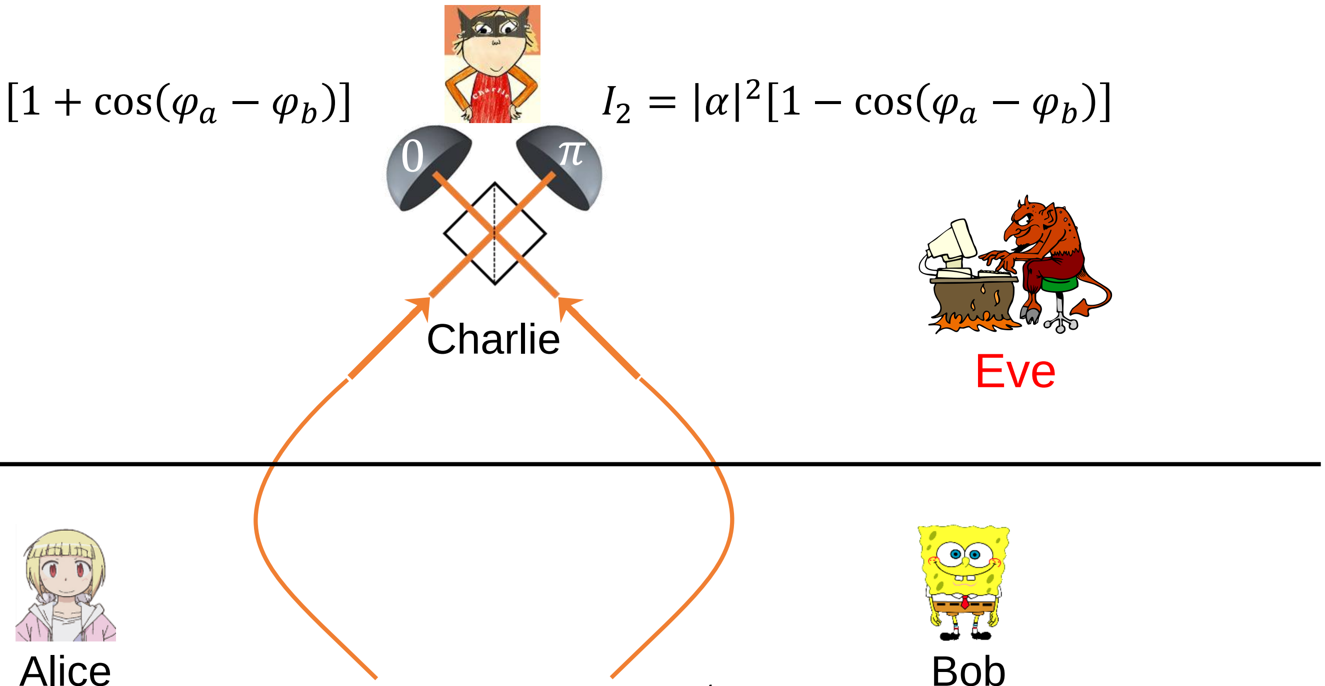
However, how do we distribute the entangled state to distant parties?

We start from separable states and then use entanglement swapping.

Phase-encoding MDI-QKD

$I_1 = |\alpha|^2[1 + \cos(\varphi_a - \varphi_b)]$

$I_2 = |\alpha|^2[1 - \cos(\varphi_a - \varphi_b)]$



$\left|\alpha e^{i\varphi_a}\right\rangle$ $\left|\alpha e^{i\varphi_b}\right\rangle$

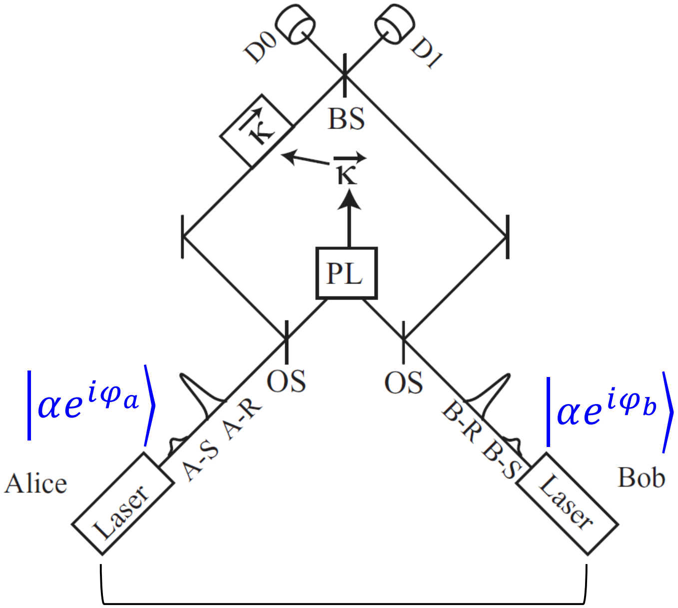
$$|\alpha\rangle \approx e^{-\frac{|\alpha|^2}{2}}(|\mathrm{v}\rangle + \alpha|1\rangle)$$ for $\alpha \ll 1$

$$|\alpha\rangle|\beta\rangle \approx e^{-\frac{|\alpha|^2+|\beta|^2}{2}}(|\mathrm{v}\rangle|\mathrm{v}\rangle + \boxed{\alpha|1\rangle|\mathrm{v}\rangle + \beta|\mathrm{v}\rangle|1\rangle} + \alpha\beta|1\rangle|1\rangle)$$

Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw

Kiyoshi Tamaki,[1,2] Hoi-Kwong Lo,[3] Chi-Hang Fred Fung,[4] and Bing Qi[3]

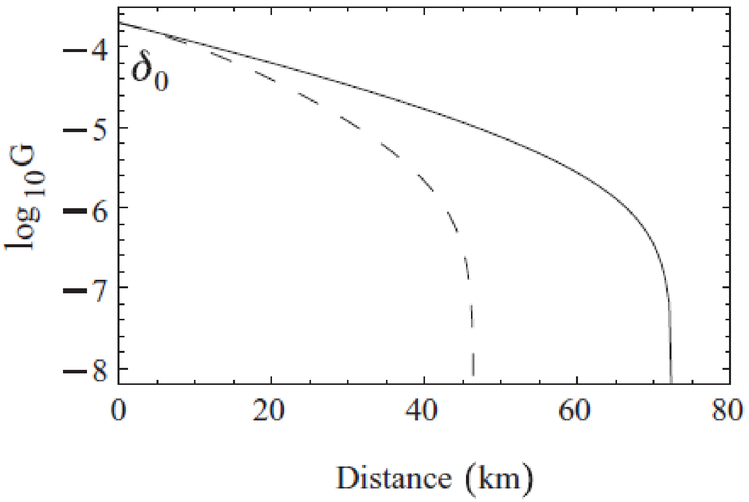
ArXiv:1111.3413. Also @ Phys. Rev. A **85**, 042307 (2012).



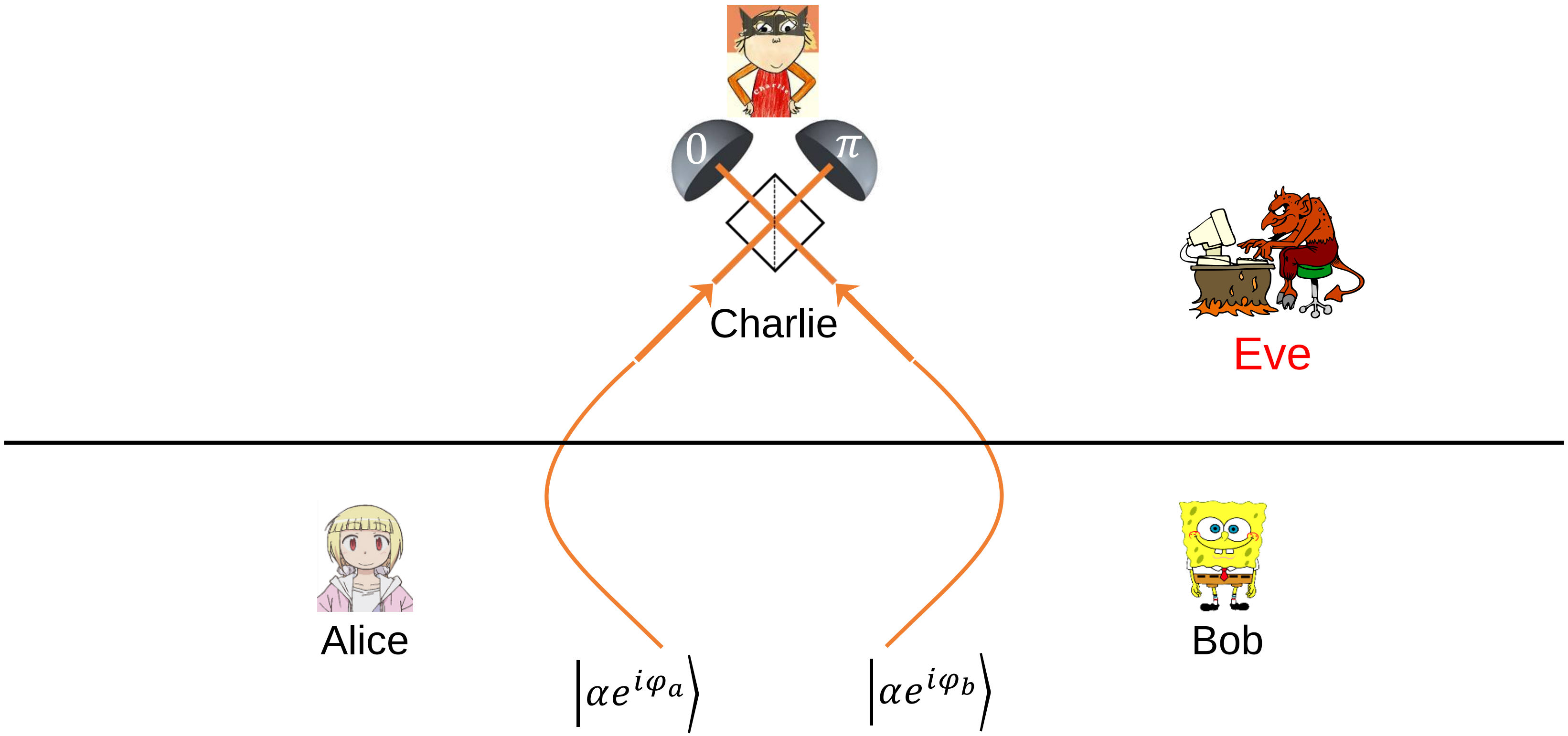
phase locked!

Limitations:

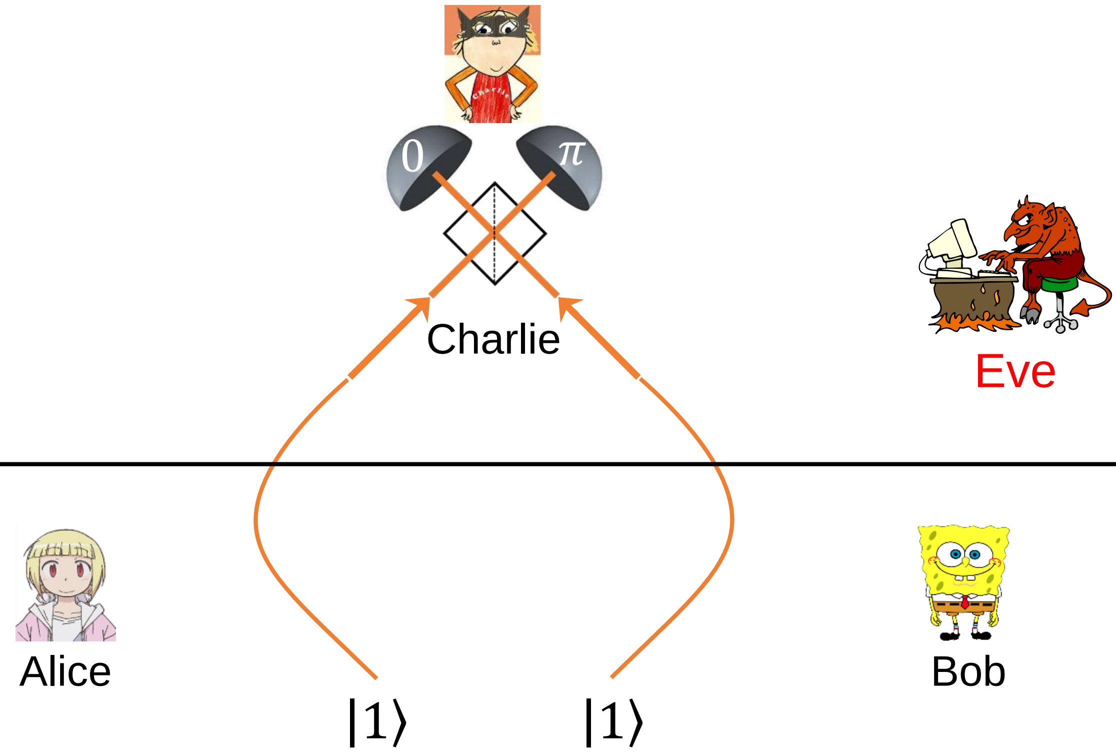
1) needs phase stabilization
2) limited distance



Phase-encoding MDI-QKD

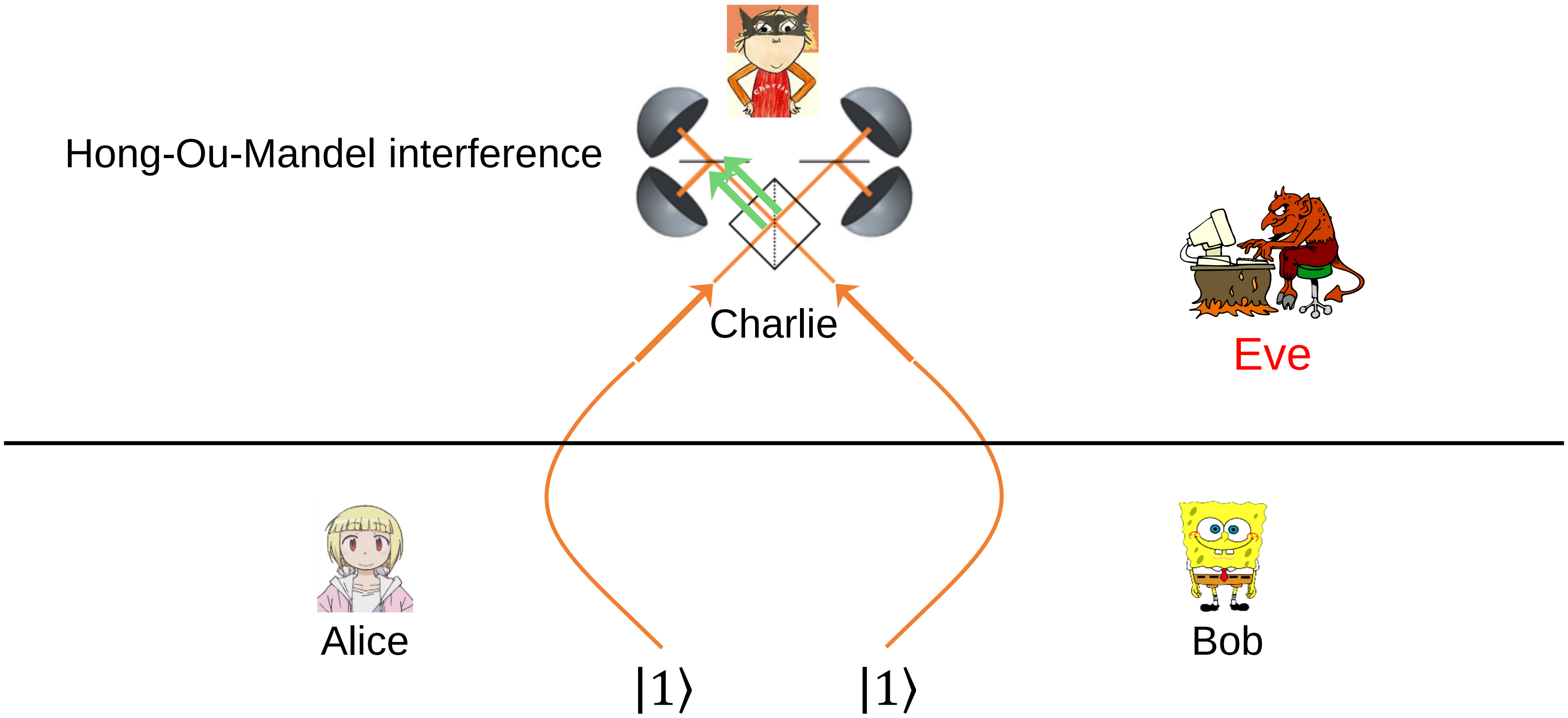


Phase-encoding MDI-QKD



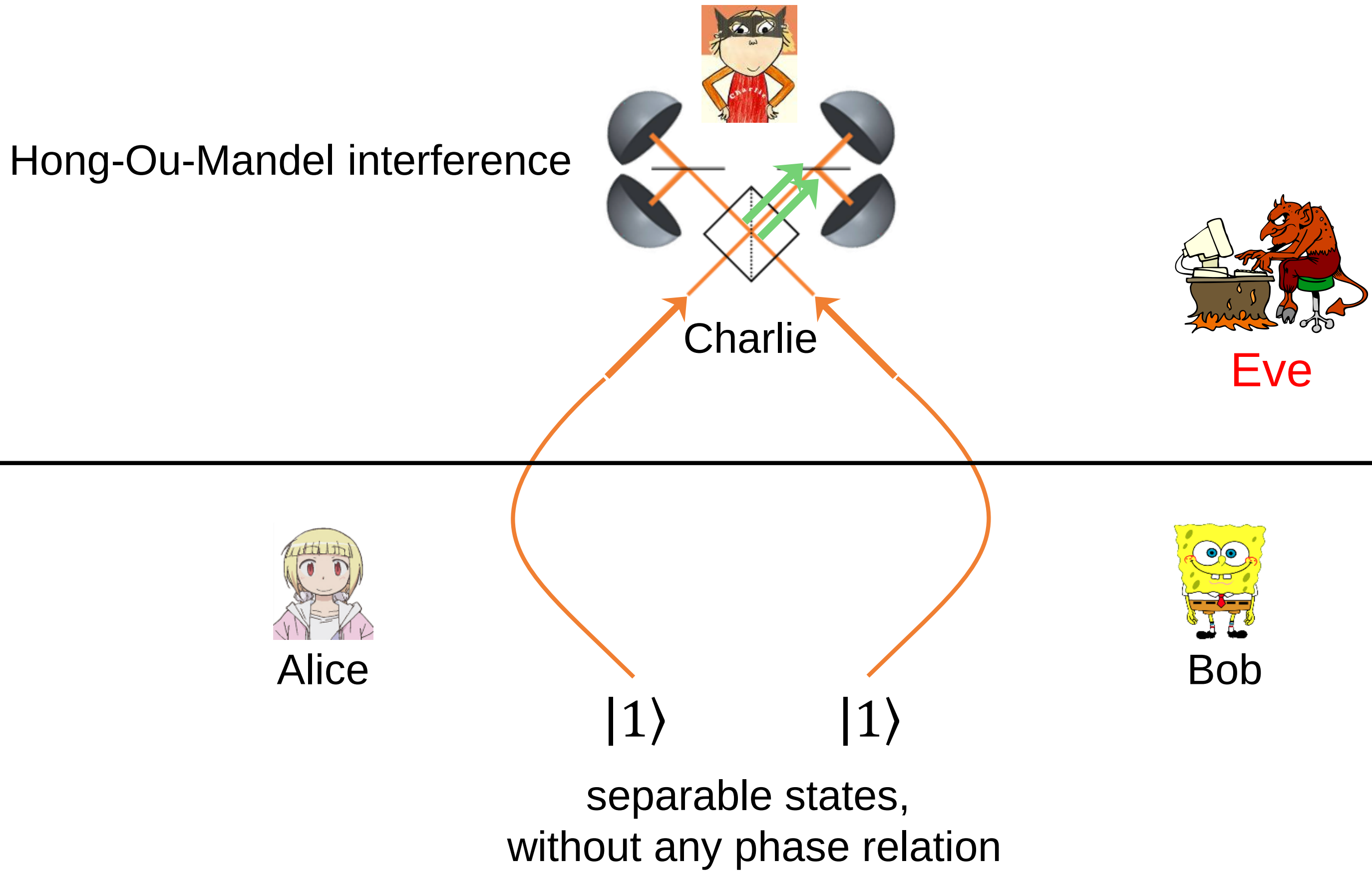
separable states,
without any phase relation

Phase-encoding MDI-QKD



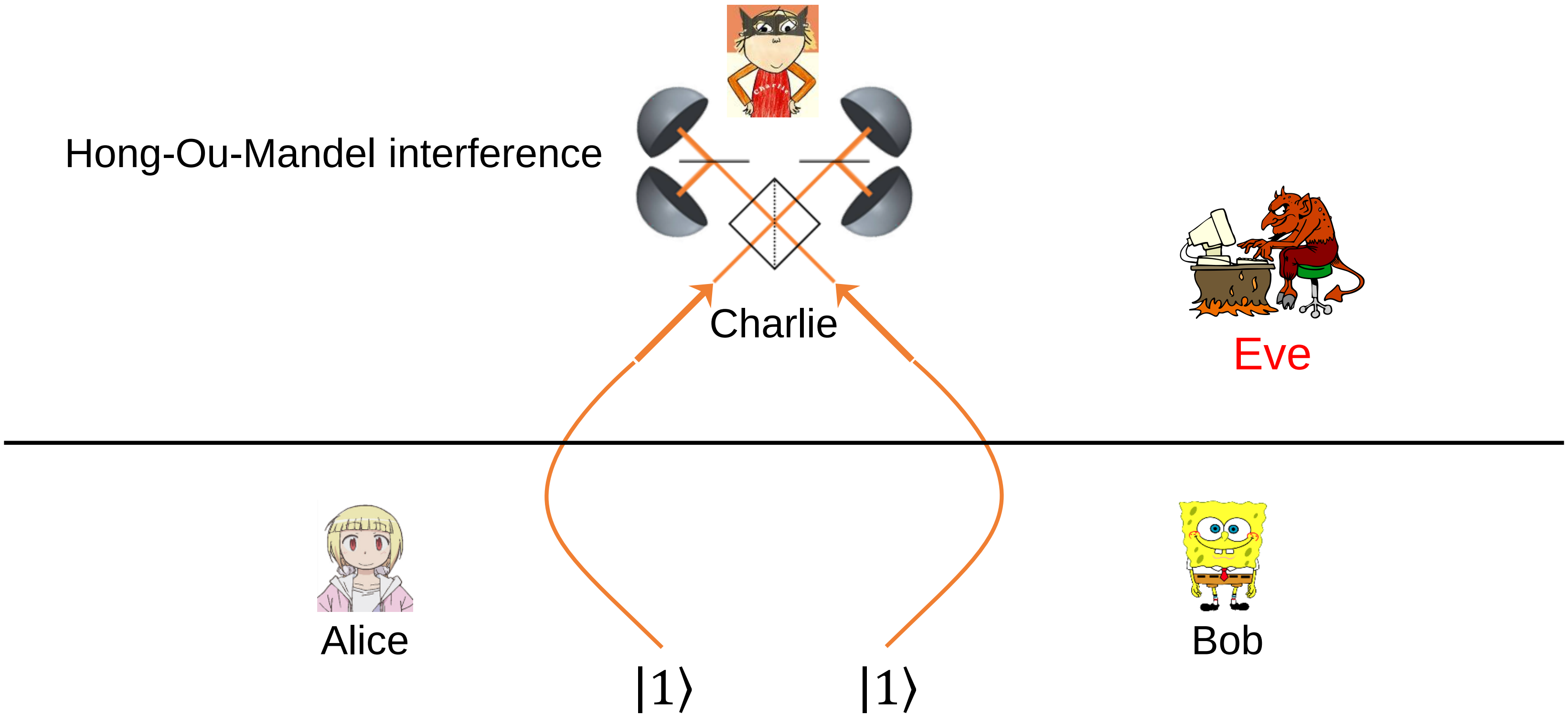
separable states,
without any phase relation

Phase-encoding MDI-QKD



Phase-encoding MDI-QKD

Hong-Ou-Mandel interference



It is not easy to perfectly generate the states $|1\rangle$, but we have approximations:

1. Heralding single-photon sources
2. Coherent states and decoy-state technique

Schemes with heralding single photons

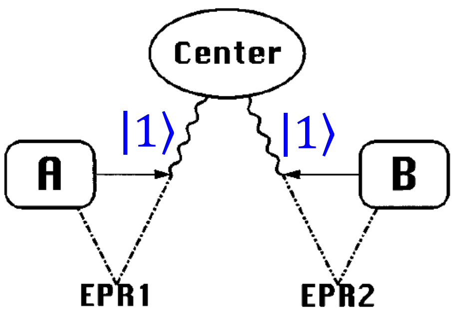
Quantum cryptographic network based on quantum memories

Eli Biham
Computer Science Department, Technion, Haifa 32000, Israel

Bruno Huttner
Group of Applied Physics, University of Geneva, CH-1211, Geneva 4, Switzerland

Tal Mor
Department of Physics, Technion, Haifa 32000, Israel

ArXiv:quant-ph/9604021. Also @ Phys. Rev. A **54**, 2651 (1996).



Security of Practical Time-Reversed EPR Quantum Key Distribution[1]

Hitoshi Inamori[2]
[2] Centre for Quantum Computation, Oxford University, Oxford, England.

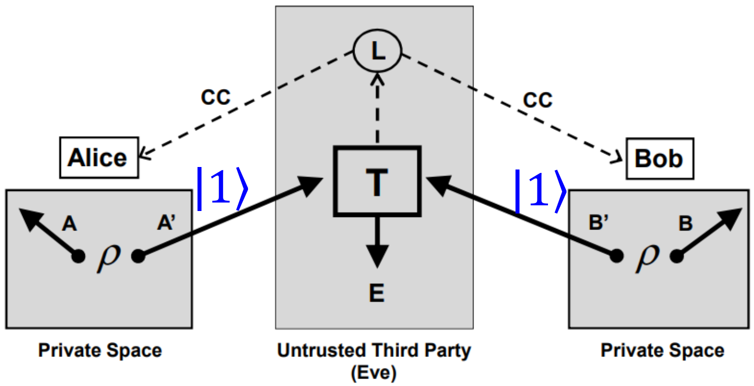
Algorithmica **34**, 340 (2002)

Side-Channel-Free Quantum Key Distribution

Samuel L. Braunstein and Stefano Pirandola
Computer Science, University of York, York YO10 5GH, United Kingdom

ArXiv:1109.2330. Also @ Phys. Rev. Lett. **108**, 130502 (2012).

Private spaces



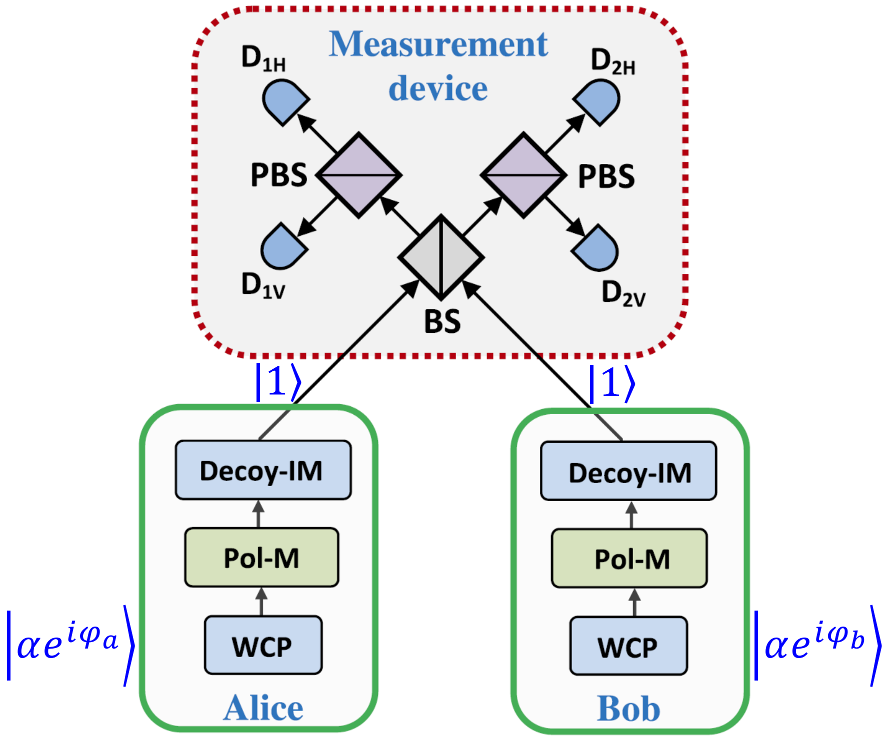
- S. Pirandola et al., Nature Photon. **9**, 397 (2015)
- F. Xu et al., Nature Photon. **9**, 772 (2015)
- S. Pirandola et al., Nature Photon. **9**, 773 (2015)

Scheme using coherent decoy states

Measurement-Device-Independent Quantum Key Distribution

Hoi-Kwong Lo,[1] Marcos Curty,[2] and Bing Qi[1]

ArXiv:1109.1473. Also @ Phys. Rev. Lett. **108**, 130503 (2012).



Phase randomization + Decoy states

$$\int_0^{2\pi} \frac{d\varphi}{2\pi} |\alpha e^{i\varphi}\rangle\langle\alpha e^{i\varphi}| = \sum_n p_n |n\rangle\langle n|$$

Privacy amplification to "postselect" $|1\rangle\langle 1|$

intensity $|\alpha|^2$ is varied for decoy states

encoding is done using polarization

φ_a and φ_b are random variables

First MDI-QKD key rate

$$R \geqslant P_Z^{1,1} Y_Z^{1,1}[1 - H_2(e_X^{1,1})] - Q_Z f_e(E_Z) H_2(E_Z)$$

Decoy states ⟶

$$\underbrace{Q_Z^{q_a q_b}}_{\text{measured}} = \underbrace{\sum_{n,m=0} e^{-(q_a+q_b)} \frac{q_a^n}{n!} \frac{q_b^m}{m!}}_{\text{known}} \underbrace{Y_Z^{n,m}}_{\text{unknown}}$$

First MDI-QKD key rate, finite size effects

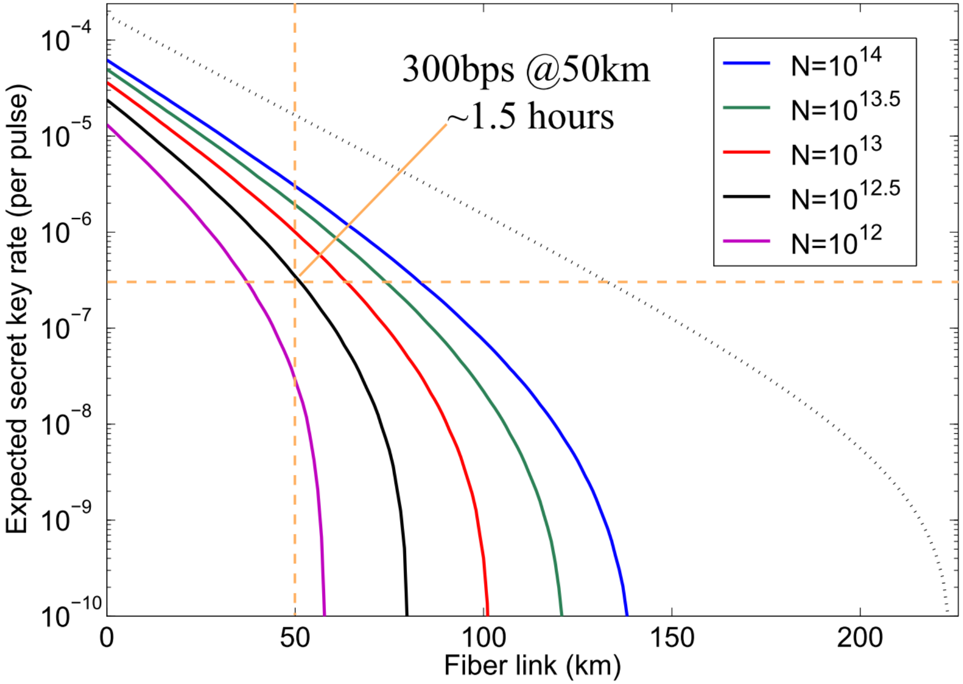
$$R \geqslant P_Z^{1,1} Y_Z^{1,1}[1 - H_2(e_X^{1,1})] - Q_Z f_e(E_Z) H_2(E_Z)$$

Decoy states ⟶

$$\underbrace{Q_Z^{q_a q_b}}_{\text{measured}} = \underbrace{\sum_{n,m=0} e^{-(q_a+q_b)} \frac{q_a^n}{n!} \frac{q_b^m}{m!}}_{\text{known}} \underbrace{Y_Z^{n,m}}_{\text{unknown}}$$

M. Curty *et al.*,
Nature Commun. **5**, 3732 (2014)

Finite-size ⟶



Decoy states and finite size effect

Making the decoy-state measurement-device-independent quantum key distribution practically useful

Yi-Heng Zhou,[1,2] Zong-Wen Yu,[1,3] and Xiang-Bin Wang[1,2,4,*]
[1] *State Key Laboratory of Low Dimensional Quantum Physics, Department of Physics, Tsinghua University, Beijing 100084, People's Republic of China*

4-intensity protocol

ArXiv:1502.01262.
Also @ Phys. Rev. A **93**, 042324 (2016).

The original decoy-state MDI-QKD adopts 2 bases (X, Z) and 3 independent intensities (u, v, w) → 36 combinations

		Z			**X**		
		u	***v***	***w***	***u***	***v***	***w***
Z	***u***	p_{ZZ}^{uu}	p_{ZZ}^{uv}	p_{ZZ}^{uw}	p_{ZX}^{uu}	p_{ZX}^{uv}	p_{ZX}^{uw}
	v	p_{ZZ}^{vu}	p_{ZZ}^{vv}	p_{ZZ}^{vw}	p_{ZX}^{vu}	p_{ZX}^{vv}	p_{ZX}^{vw}
	w	p_{ZZ}^{wu}	p_{ZZ}^{wv}	p_{ZZ}^{ww}	p_{ZX}^{wu}	p_{ZX}^{wv}	p_{ZX}^{ww}
X	***u***	p_{XZ}^{uu}	p_{XZ}^{vu}	p_{XZ}^{wu}	p_{XX}^{uu}	p_{XX}^{uv}	p_{XX}^{uw}
	v	p_{XZ}^{uv}	p_{XZ}^{vv}	p_{XZ}^{wv}	p_{XX}^{vu}	p_{XX}^{vv}	p_{XX}^{vw}
	w	p_{XZ}^{uw}	p_{XZ}^{vw}	p_{XZ}^{ww}	p_{XX}^{wu}	p_{XX}^{wv}	p_{XX}^{ww}

Data used in the decoy-state parameter estimation, relevant for finite-size effects

Decoy states and finite size effect

Making the decoy-state measurement-device-independent quantum key distribution practically useful

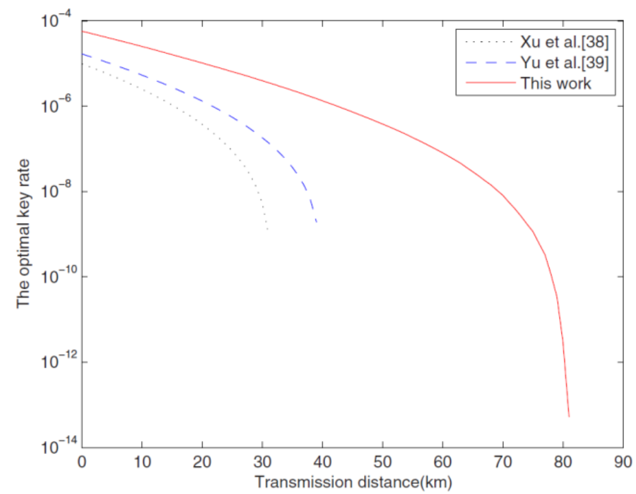
Yi-Heng Zhou,[1,2] Zong-Wen Yu,[1,3] and Xiang-Bin Wang[1,2,4,*]
[1] *State Key Laboratory of Low Dimensional Quantum Physics, Department of Physics, Tsinghua University, Beijing 100084, People's Republic of China*

4-intensity protocol

ArXiv:1502.01262.
Also @ Phys. Rev. A **93**, 042324 (2016).

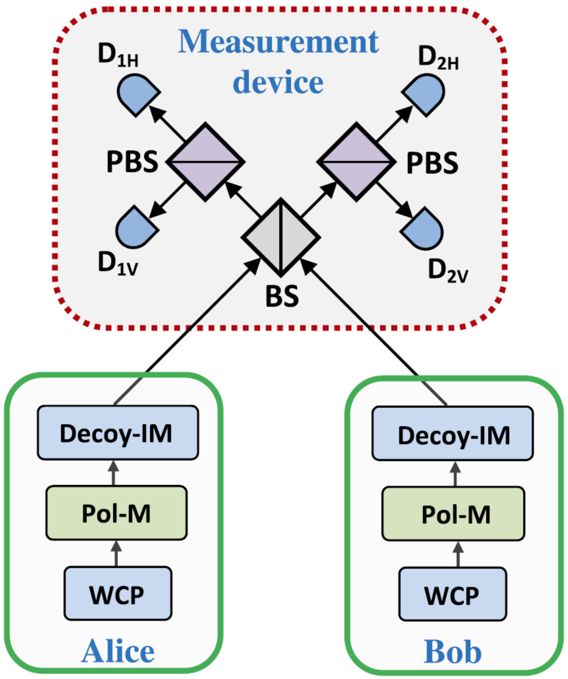
The new protocol(*) adopts 2 bases (X, Z) and 4 coupled intensities $(s; u, v, w)$ → 16 combinations

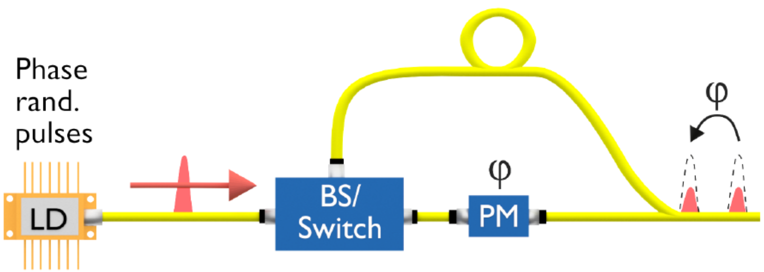
		Z	X		
		s	u	v	w
Z	s	p_{ZZ}^{ss}	p_{ZX}^{su}	p_{ZX}^{sv}	p_{ZX}^{sw}
X	u	p_{XZ}^{us}	p_{XX}^{uu}	p_{XX}^{uv}	p_{XX}^{uw}
	v	p_{XZ}^{vs}	p_{XX}^{vu}	p_{XX}^{vv}	p_{XX}^{vw}
	w	p_{XZ}^{ws}	p_{XX}^{wu}	p_{XX}^{wv}	p_{XX}^{ww}



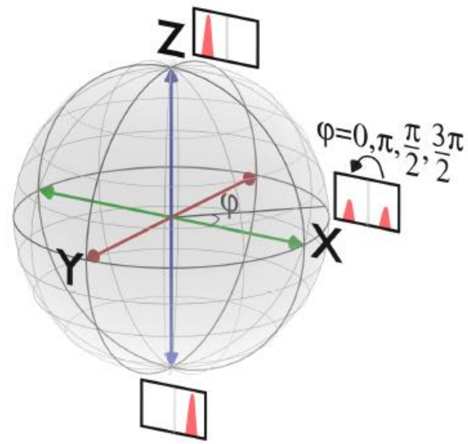
- This protocol was first implemented in *Comandar et al., Nature Photon.* ***10****, 312 (2016)*, where its composable security is proven and the highest MDI-QKD key rate is achieved.
- Then it was implemented in *Yin et al., Phys. Rev. Lett.* ***117,*** *190501 (2016)*, to achieve the longest fibre-based MDI-QKD transmission.

Equivalent description with Time Bins

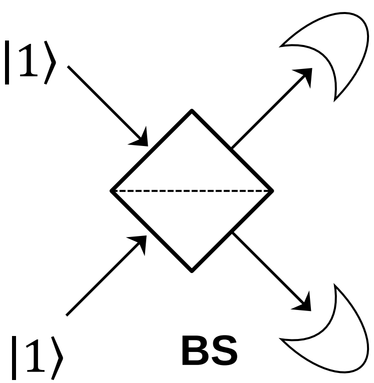


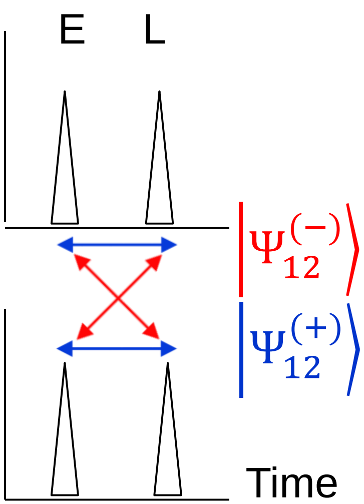


Polarization



Time bin





TOSHIBA
Leading Innovation >>>

Outline of this tutorial

1. Motivation and Introduction of MDI-QKD
   - Detector vulnerabilities and trusted networks
   - Basic features of MDI-QKD
2. MDI-QKD origin and working mechanism
   - Optical Interference
   - Entanglement swapping
3. Experiments
4. Variants
   - Twin-Field QKD

Outline of this tutorial

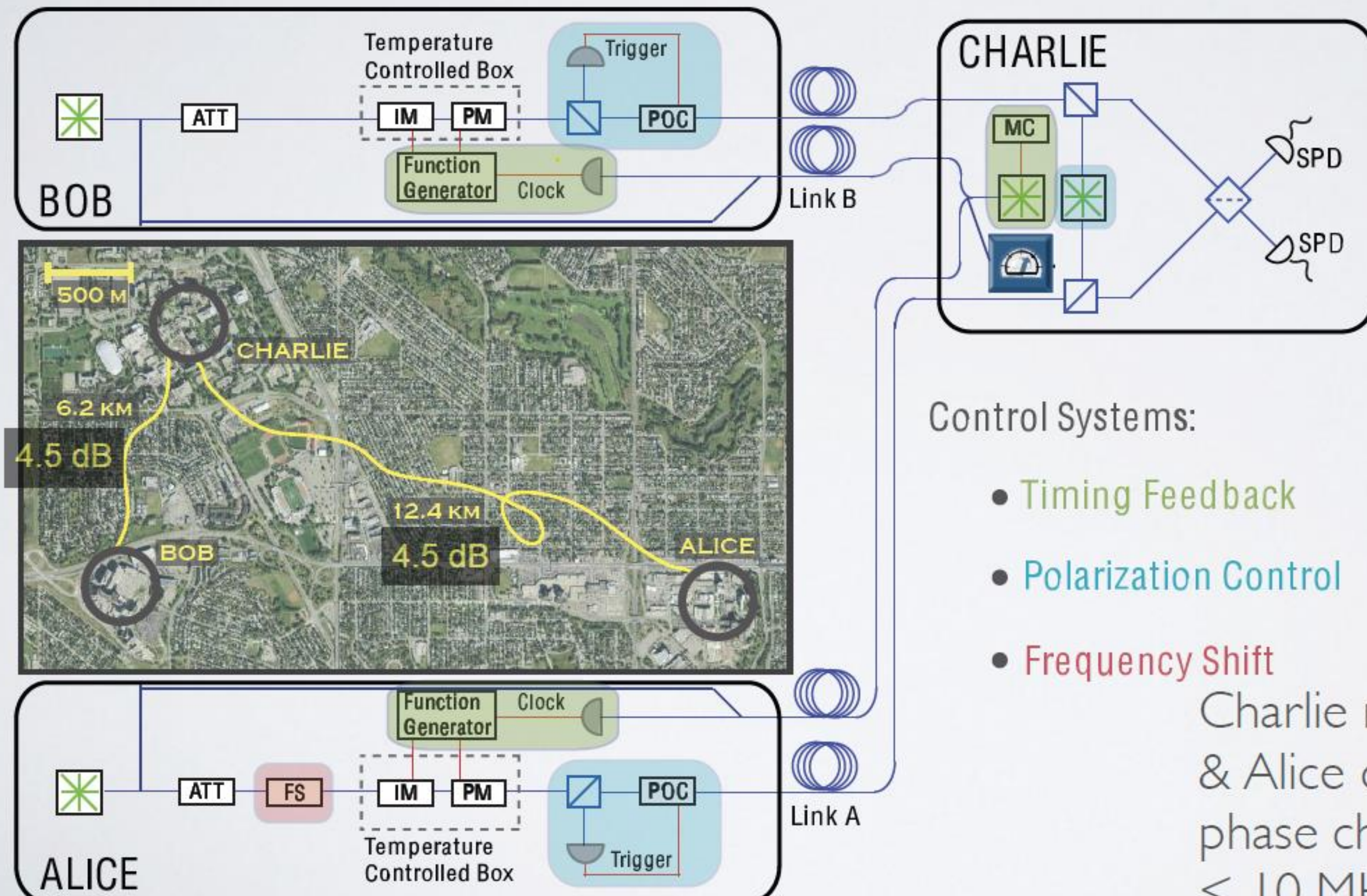
1. Motivation and Introduction of MDI-QKD
    - Detector vulnerabilities and trusted networks
    - Basic features of MDI-QKD
2. MDI-QKD origin and working mechanism
    - Optical Interference
    - Entanglement swapping
3. Experiments
4. Variants
    - Twin-Field QKD

Watch Joshua Slater’s talk @ QCrypt 2014 website

https://youtu.be/WL7OPSO0s_s

EXPERIMENTS

Calgary, Canada (A. Rubenok, JAS, et al. PRL 111, 130501 (2013))



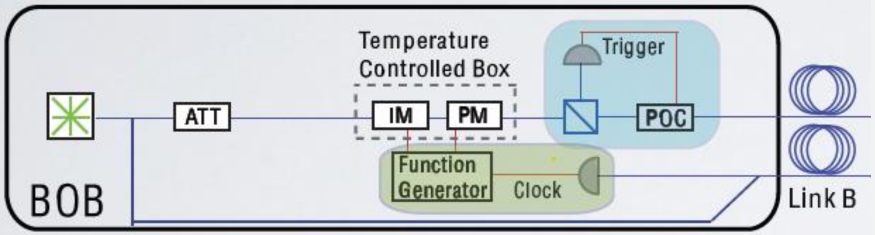
Control Systems:

- Timing Feedback
- Polarization Control
- Frequency Shift

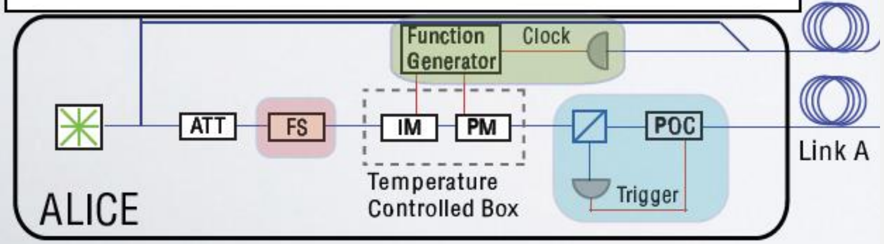
Charlie measured
& Alice corrected with linear phase chirp
< 10 MHz difference

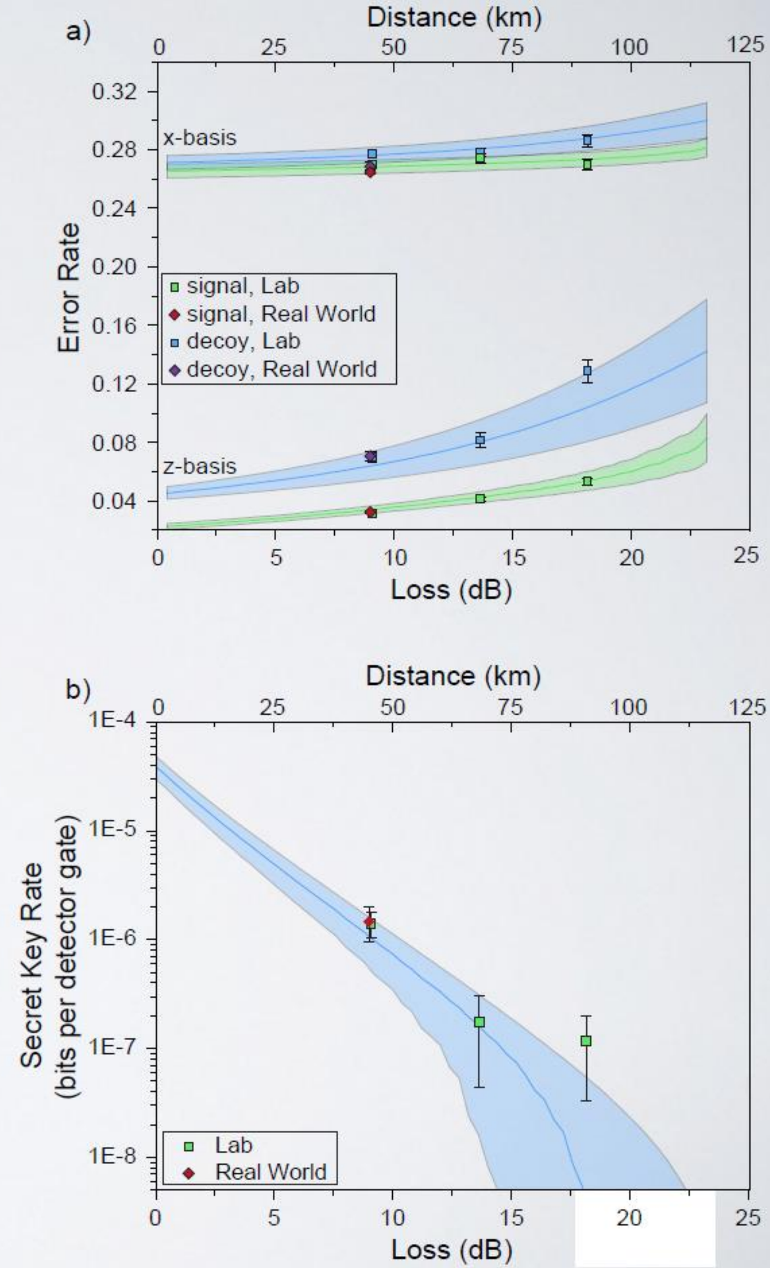
EXPERIMENTS

Calgary, Canada (A. Rubenok, JAS, et al. P



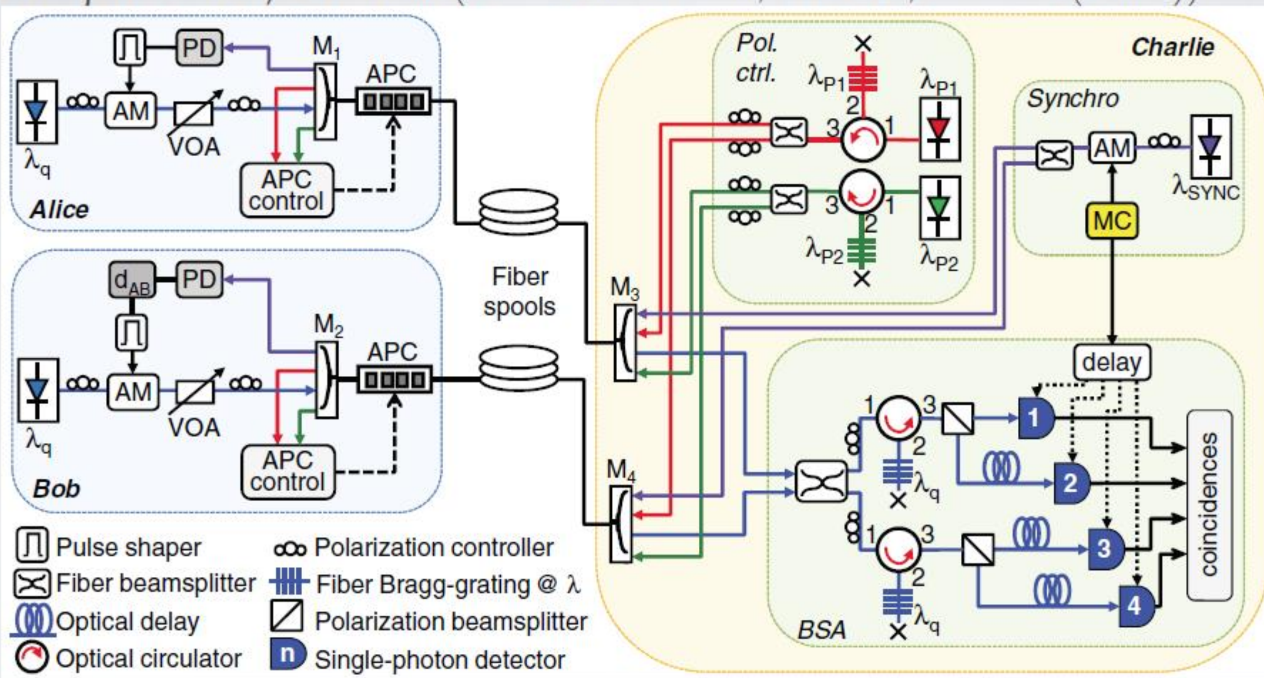
Specifications
CW Laser, 1553nm
2 MHz rep rate
500 ps / 2 GHz
1.4 ns time-bin qubits
Decoy-States (0.5*, 0.05, 0)





EXPERIMENTS

Rio de Janeiro, Brazil (T. F. da Silva et al., PRA 88, 052303 (2013))



Extracted data

$$Q_r^{11} = 6.88\times10^{-6}$$
$$E_d^{11} = 0.018$$
$$Q_{\text{rect}} = 1.36\times10^{-5}$$
$$E_{\text{rect}} = 0.057$$
$$\text{R} = 1.04\times10^{-6}$$

Specifications

cw laser, 1546 nm

1.5 ns / 650 MHz

Polarization qubits

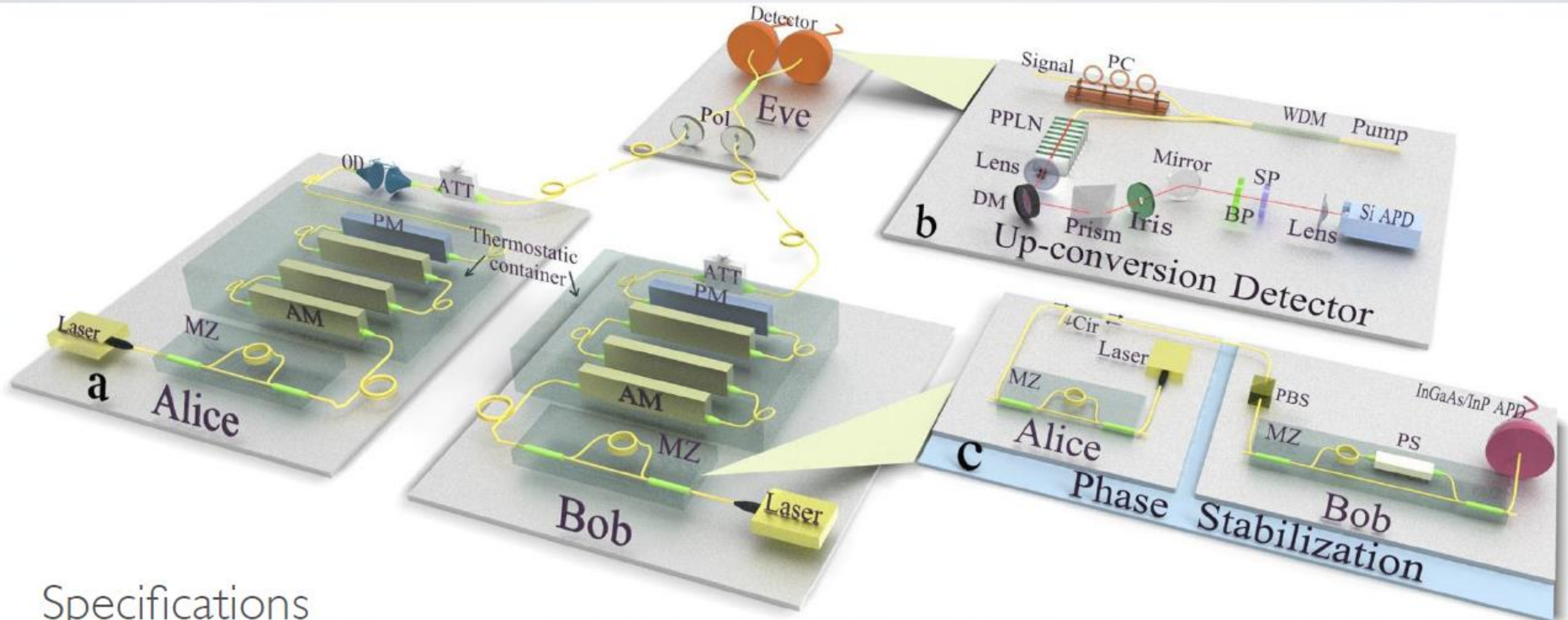
Decoy-States (0.5, 0.1,0)

Rep 1 MHz

Multiplexed - time / polarization sync

EXPERIMENTS

Hefei, China (Y. Liu, et al. PRL 111, 130502 (2013))



Specifications

Pulsed, 1550 nm

2 ns / 10 pm

85 ns time-bin qubits

Decoy-States (0.5, 0.2, 0.1,0)

0.1 pm frequency precision

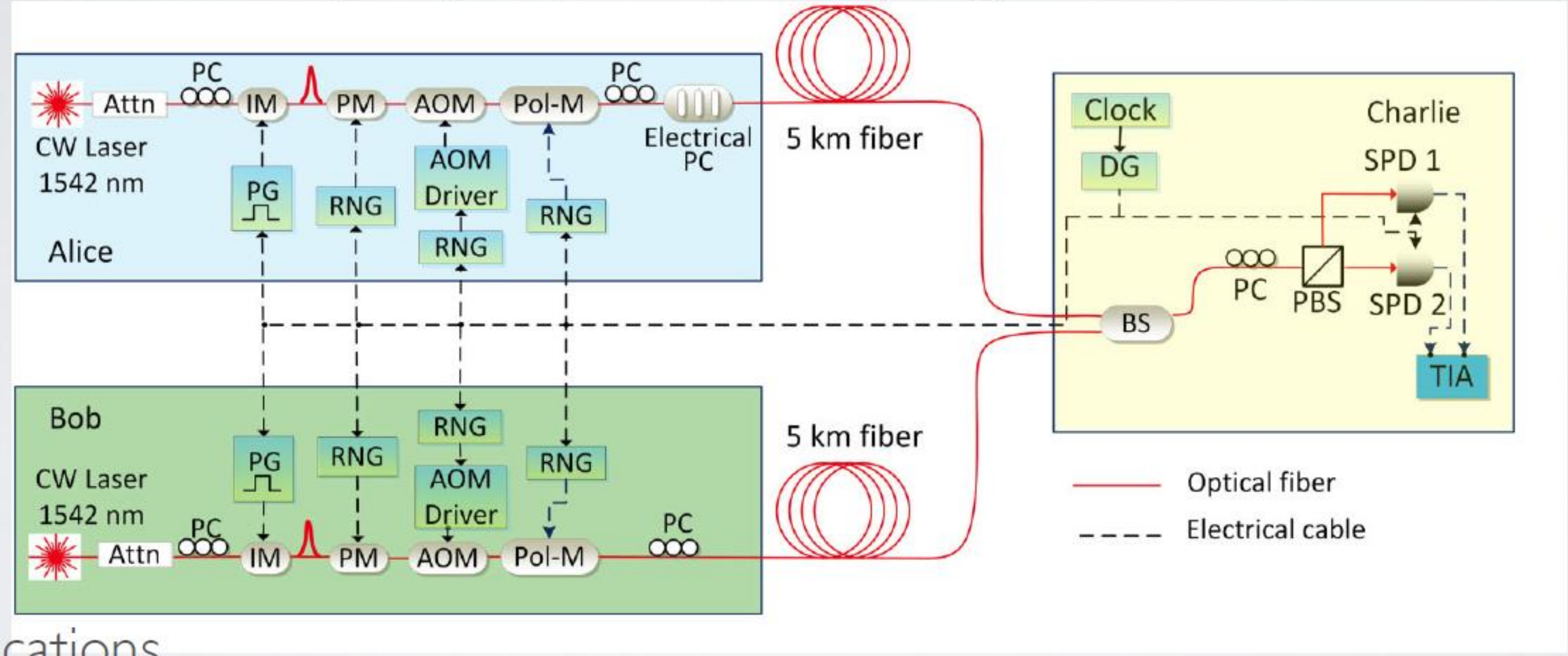
10 ps time precision

Random modulations

Phase-stabilized interferometers

EXPERIMENTS

Toronto, Canada (Z.Tang et al., PRL 112, 190503 (2014))



Specifications
cw laser, 1542 nm
Phase randomized states
1.5 ns / 650 MHz
Polarization qubits
Decoy-States (0.3, 0.1,0.01)

$$e^X = 26.2\%$$

$$e^Z = 1.8\ \%$$

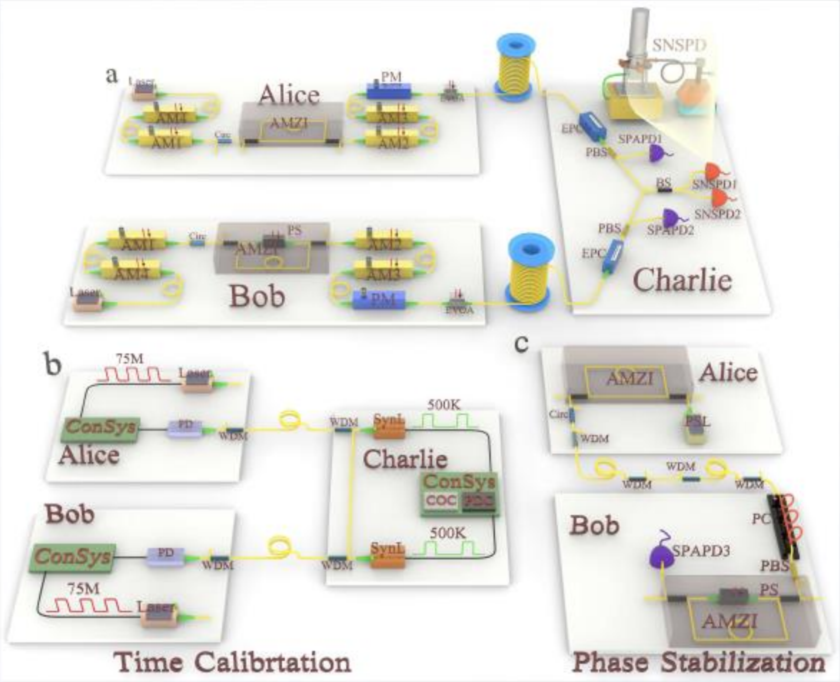
$$S = 1e^{-8}$$

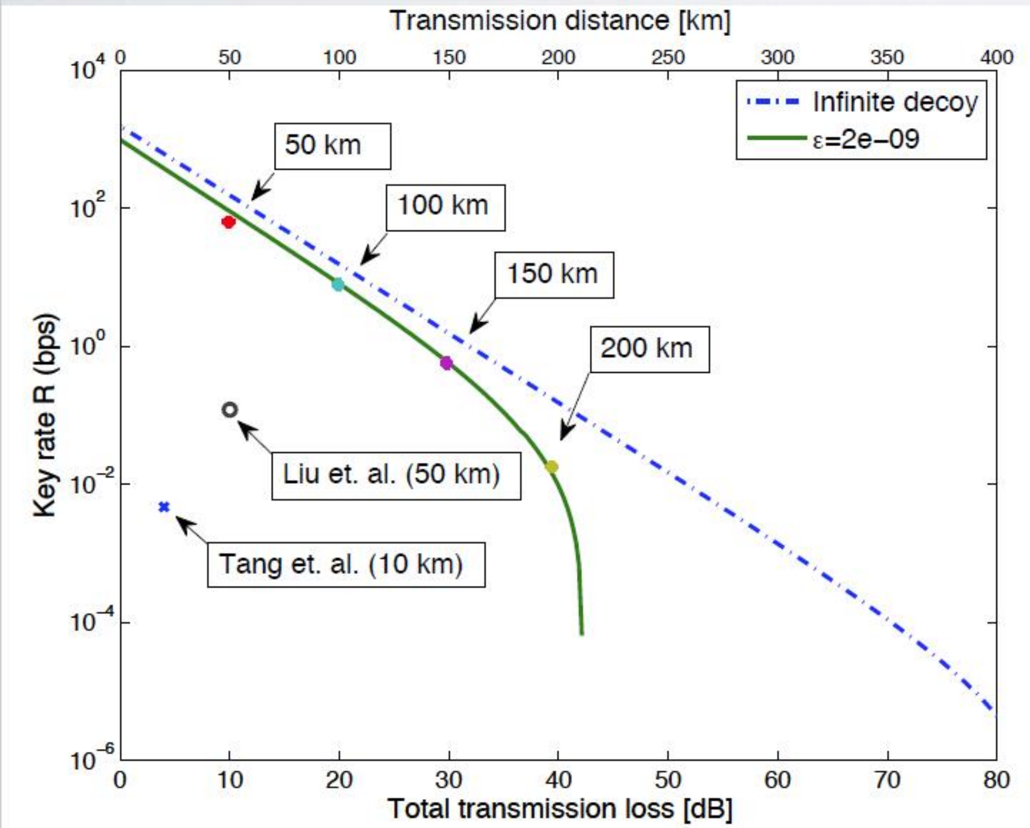
THE CUTTING-EDGE OF MDI-QKD

Long Distance / High Loss
Hefei, China

(Y.-L. Tang et al., arxiv:1407.8012)

Also @ Phys. Rev. Lett. **113**, 190501 (2014)





75 MHz Rep-Rate

@ 200 km, 0.009 b/sec

@ 100 km, 3 kbps

Key rate performance gap of MDI-QKD

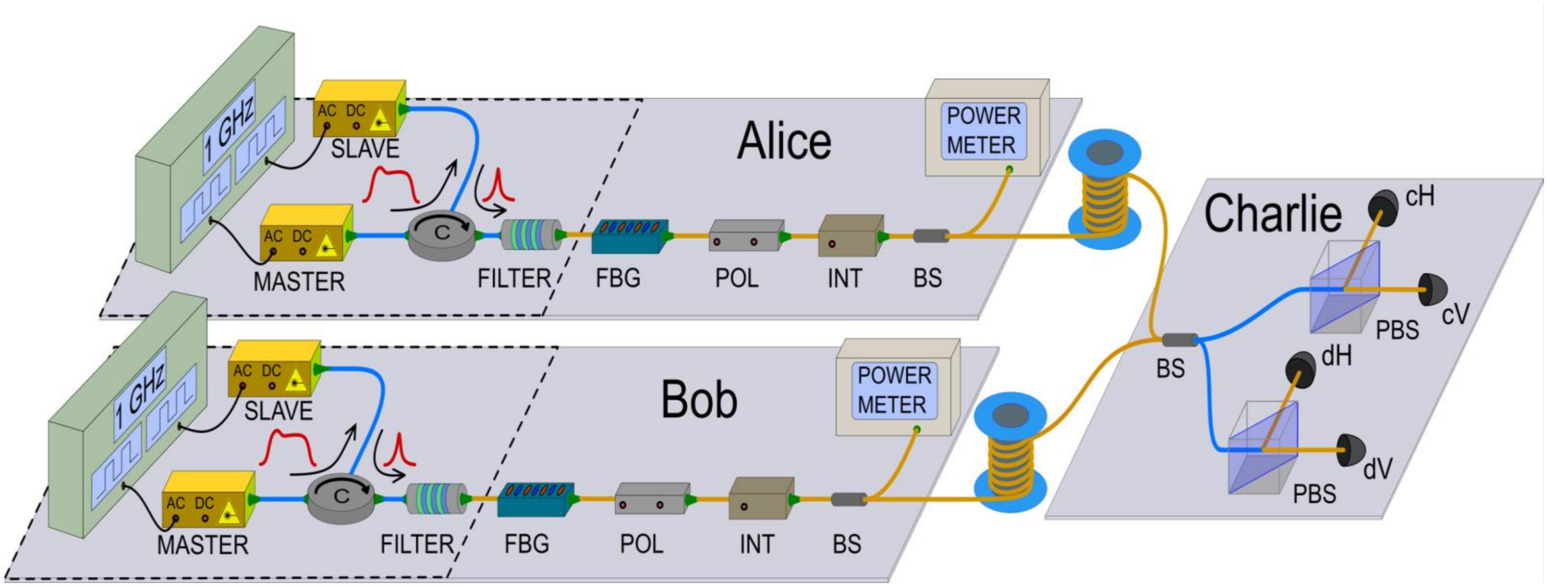
State of the art up to 2015

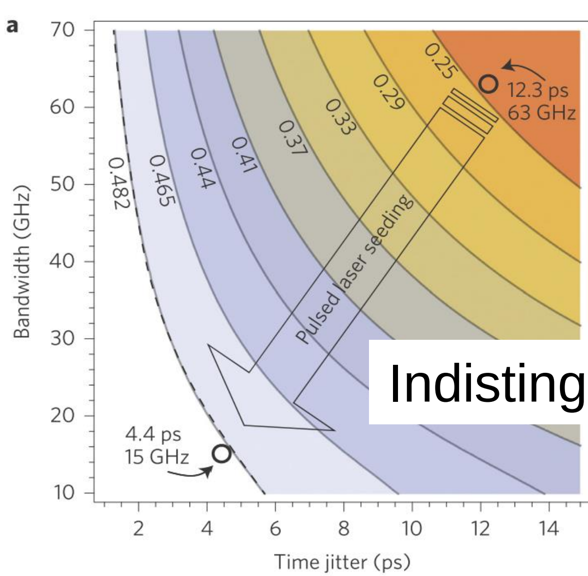
	Clock (MHz)	Pulse width (ps)	Eq. distance (km)	Max key rate (bit/s)
Ref. [18]	75	2500	50	6.7×10^1
Ref. [19]	2	250	45	3.4×10^0
	20	290	80	6.2×10^2
Ref. [14]	2	500	45	3×10^0
Ref. [16]	1	1500	17	1×10^0

- In May 2016 the key rate was improved
- In June 2016 the distance was extended

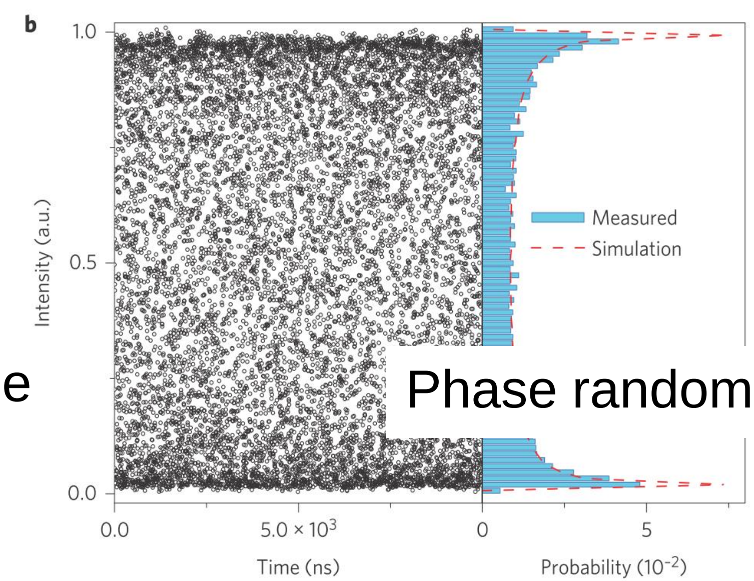
[18] Y-L Tang *et al*, Phys. Rev. Lett. 2014. [19] R Valivarthi *et al*, J. Mod. Opt. 2015.
[14] A Rubenok *et al*, Phys. Rev. Lett. 2013. [16] T Ferreira da Silva et al, Phys. Rev. A 2013.

Experimental setup and novel light source





Indistinguishable



Phase randomised

TOSHIBA
Leading Innovation >>>

(*) L. Comandar *et al.*, Nature Photon. **10**, 312 (2016)

Going high-rate

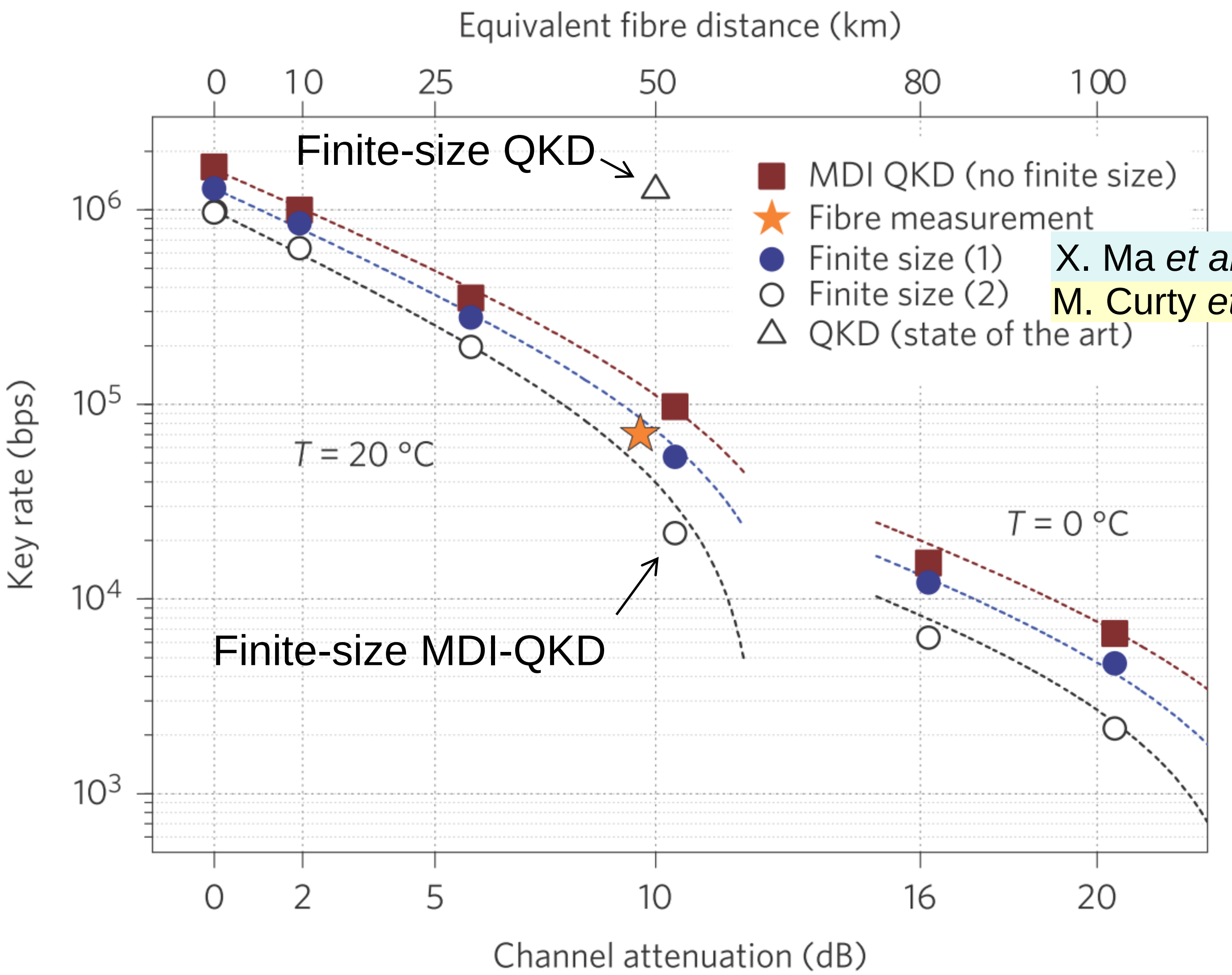
Increased key rate in 2016

	Clock (MHz)	Pulse width (ps)	Eq. distance (km)	Max key rate (bit/s)
Ref. [18]	75	2500	50	6.7×10^1
Ref. [19]	2	250	45	3.4×10^0
	20	290	80	6.2×10^2
Ref. [14]	2	500	45	3×10^0
Ref. [16]	1	1500	17	1×10^0
This work (*)	1000	35	0	1.660×10^6
				1.286×10^6
			52	9.7×10^4
			80	1.6×10^4

[18] Y-L Tang *et al*, Phys. Rev. Lett. 2014. [19] R Valivarthi *et al*, J. Mod. Opt. 2015.
[14] A Rubenok *et al*, Phys. Rev. Lett. 2013. [16] T Ferreira da Silva et al, Phys. Rev. A 2013.

(*) L. Comandar *et al.*, Nature Photon. **10**, 312 (2016)

MDI-QKD: Finite sample size included



X. Ma *et al*, Phys. Rev A 2012

M. Curty *et al*, Nat. Comm. 2014

4-intensity protocol in Y.-H. Zhou et al., Phys. Rev. A **93**, 042324 (2016) refined and used

TOSHIBA Leading Innovation

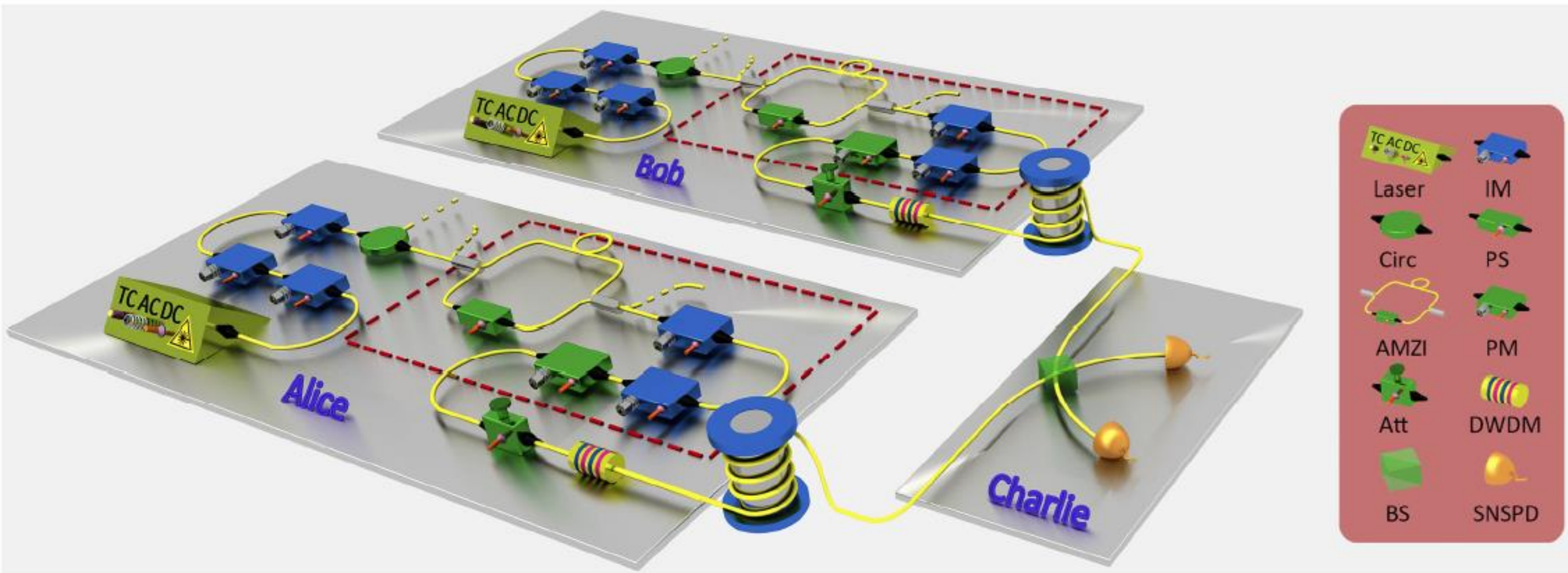
(*) L. Comandar et al., Nature Photon. **10**, 312 (2016)

Going long distance

Measurement-Device-Independent Quantum Key Distribution Over a 404 km Optical Fiber

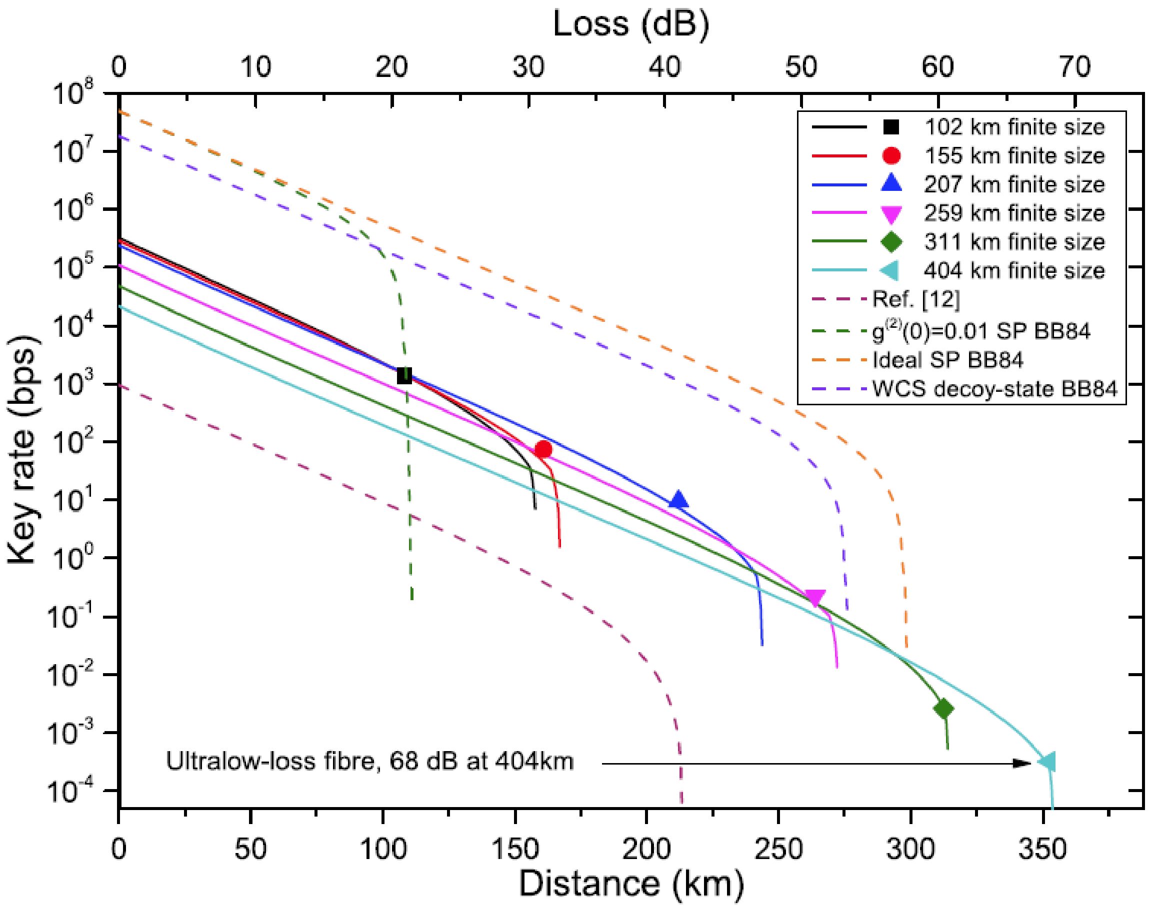
Hua-Lei Yin,[1,2] Teng-Yun Chen,[1,2] Zong-Wen Yu,[3,4] Hui Liu,[1,2] Li-Xing You,[5] Yi-Heng Zhou,[2,3] Si-Jing Chen,[5] Yingqiu Mao,[1,2] Ming-Qi Huang,[1,2] Wei-Jun Zhang,[5] Hao Chen,[6] Ming Jun Li,[6] Daniel Nolan,[6] Fei Zhou,[7] Xiao Jiang,[1,2] Zhen Wang,[5] Qiang Zhang,[1,2,7,*] Xiang-Bin Wang,[2,3,7,†] and Jian-Wei Pan[1,2,‡]

ArXiv:1606.06821.
Phys. Rev. Lett. **117**, 190501 (2016).



- Phase randomised WCP
- Time bin encoding and 4 intensities for decoy states
- 5 IMs in each user! 1 pulse shaping, 2 decoys, 2 time-bin encoding (ToA)
- 3 months: 2584 bits (0.00034 bits/s), no EC, no PA
- Detectors: SNSP efficiency 65%, dark counts 30 Hz

Going long distance



Longest fibre-based secure quantum communication until recently

Still the longest distance for experimental fibre-based MDI-QKD

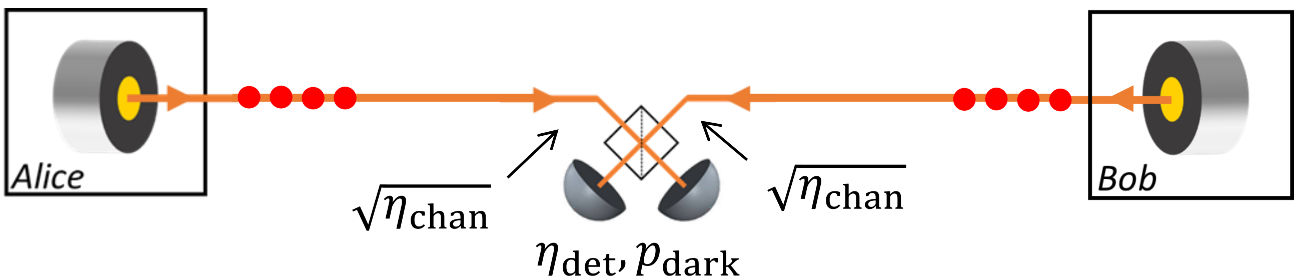
(*) H.-L. Yin et al., arXiv:1606.06821. Also @ Phys. Rev. Lett. **117**, 190501 (2016).

Long distance performance of MDI QKD

QKD

$$\frac{N}{S} \approx \frac{p_{\text{dark}}}{\eta_{\text{chan}}\eta_{\text{det}}}$$

MDI QKD



$$\frac{N}{S} \approx \frac{2p_{\text{dark}}}{\sqrt{\eta_{\text{chan}}}\eta_{\text{det}}}$$

How far can we go with a decent key rate?

see N. Gisin *et al.*, Rev. Mod. Phys. **74**, 145 (2002)

Outline of this tutorial

1. Motivation and Introduction of MDI-QKD
   - Detector vulnerabilities and trusted networks
   - Basic features of MDI-QKD
2. MDI-QKD origin and working mechanism
   - Optical Interference
   - Entanglement swapping
3. Experiments
4. Variants
   - Twin-Field QKD

Outline of this tutorial

1. Motivation and Introduction of MDI-QKD
   - Detector vulnerabilities and trusted networks
   - Basic features of MDI-QKD
2. MDI-QKD origin and working mechanism
   - Optical Interference
   - Entanglement swapping
3. Experiments
4. Variants
   - Twin-Field QKD

Fundamental limit of QKD

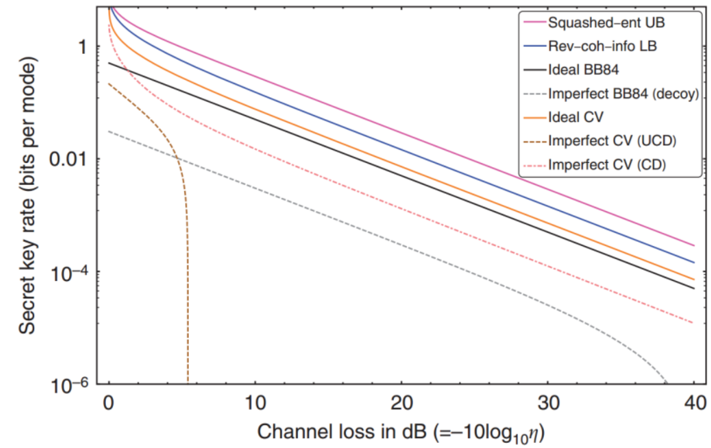
Received 15 Apr 2014 | Accepted 11 Sep 2014 | Published 24 Oct 2014 DOI: 10.1038/ncomms6235

Fundamental rate-loss tradeoff for optical quantum key distribution

Masahiro Takeoka[1,2], Saikat Guha[2] & Mark M. Wilde[3]

"TGW" bound for the secret key capacity (SKC)

$$SKC(\eta) \leq \log_2\left(\frac{1+\eta}{1-\eta}\right)$$



In a point-to-point configuration it is *impossible* to overcome the SKC bounds

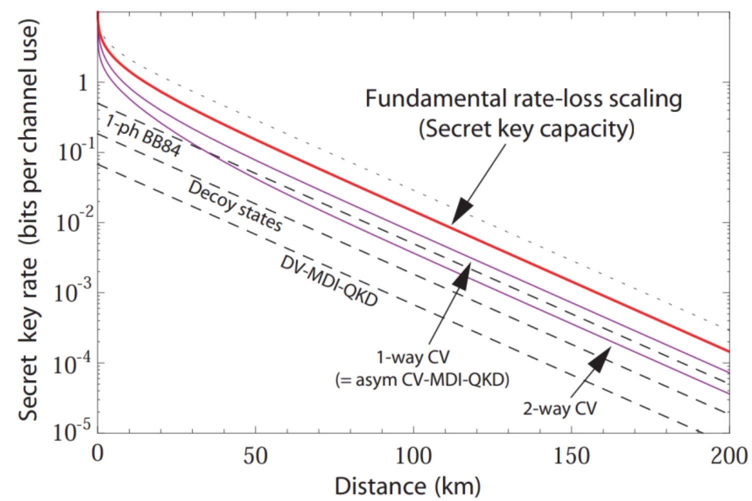
Received 15 Mar 2016 | Accepted 23 Feb 2017 | Published 26 Apr 2017 DOI: 10.1038/ncomms15043 OPEN

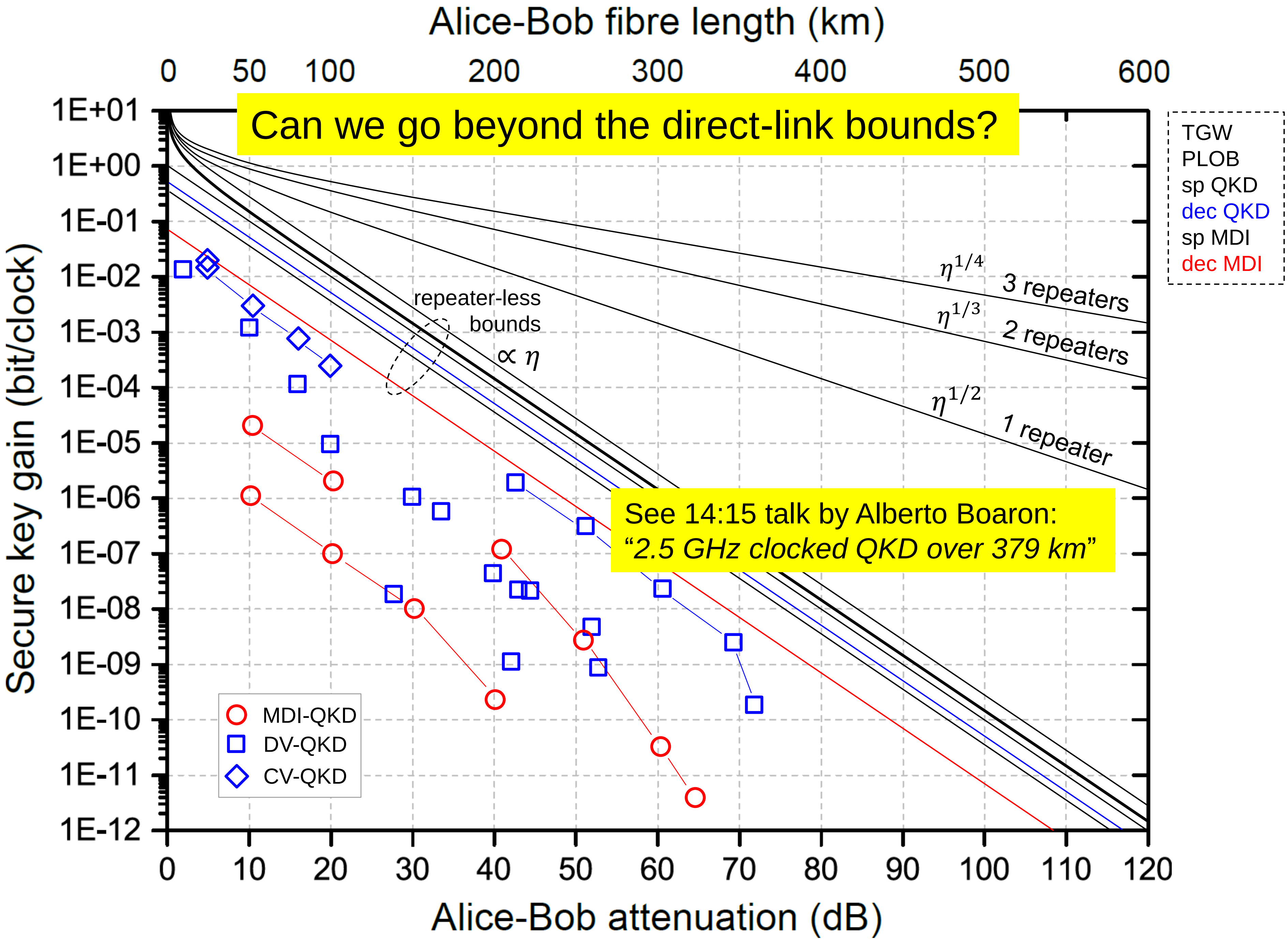
Fundamental limits of repeaterless quantum communications

Stefano Pirandola[1], Riccardo Laurenza[1], Carlo Ottaviani[1] & Leonardo Banchi[2]

"PLOB" bound

$$SKC(\eta) = \log_2\left(\frac{1}{1-\eta}\right)$$



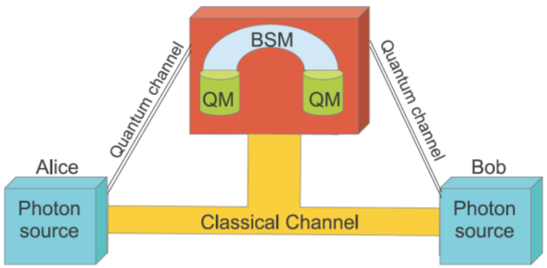

Alice-Bob fibre length (km)
0
50
100
200
300
400
500
600
Can we go beyond the direct-link bounds?
TGW
PLOB
sp QKD
dec QKD
sp MDI
dec MDI
1E+01
1E+00
1E-01
1E-02
1E-03
1E-04
1E-05
1E-06
1E-07
1E-08
1E-09
1E-10
1E-11
1E-12
Secure key gain (bit/clock)
$\eta^{1/4}$
3 repeaters
$\eta^{1/3}$
2 repeaters
$\eta^{1/2}$
1 repeater
repeater-less bounds
$\propto \eta$
See 14:15 talk by Alberto Boaron:
"*2.5 GHz clocked QKD over 379 km*"
MDI-QKD
DV-QKD
CV-QKD
0
10
20
30
40
50
60
70
80
90
100
110
120
Alice-Bob attenuation (dB)

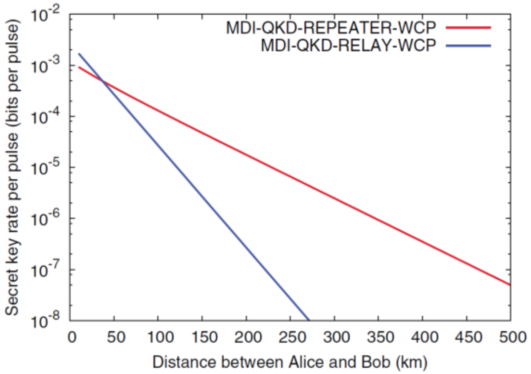
Other solutions

Measurement-device-independent quantum key distribution with quantum memories

Silvestre Abruzzo, Hermann Kampermann, and Dagmar Bruß

ArXiv:1306.3095. Also @
Phys. Rev. A **89**, 012301 (2014)

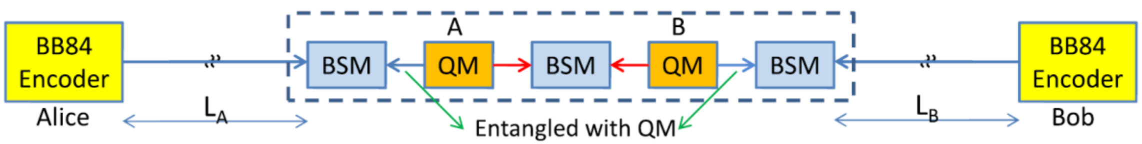


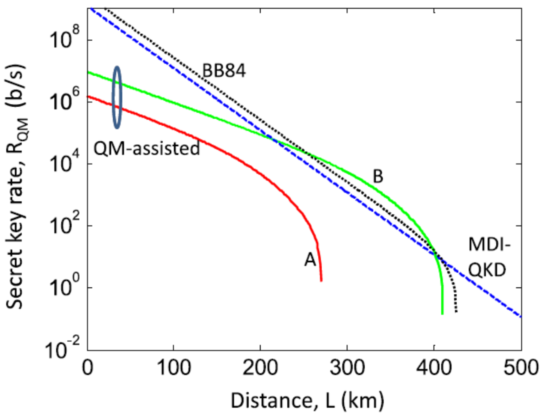


Memory-assisted measurement-device-independent quantum key distribution

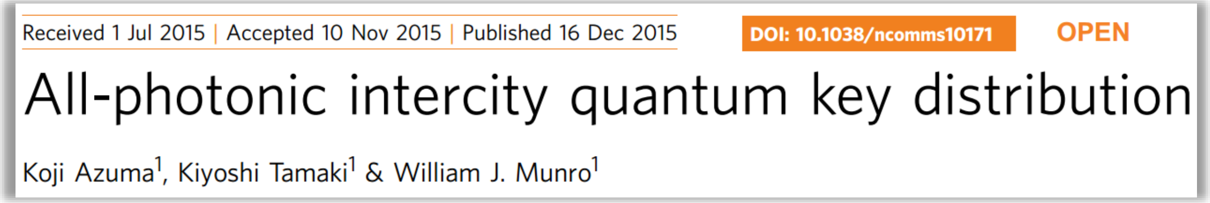
C. Panayi, M. Razavi, X. Ma, N. Lütkenhaus

New Journal of Physics **16** (2014) 043005



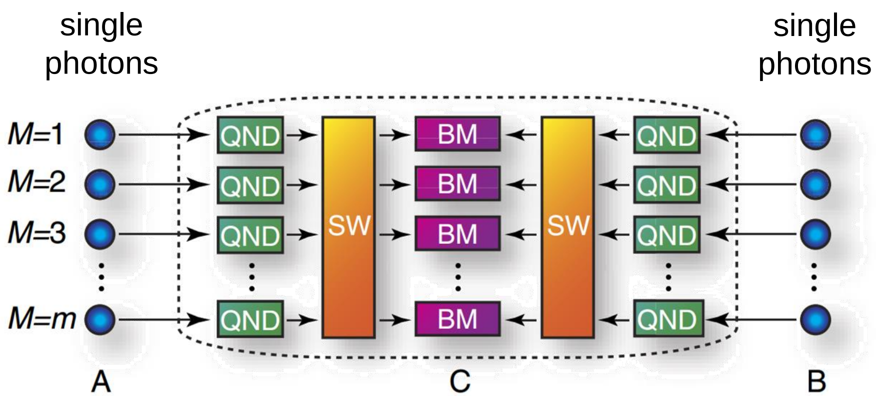


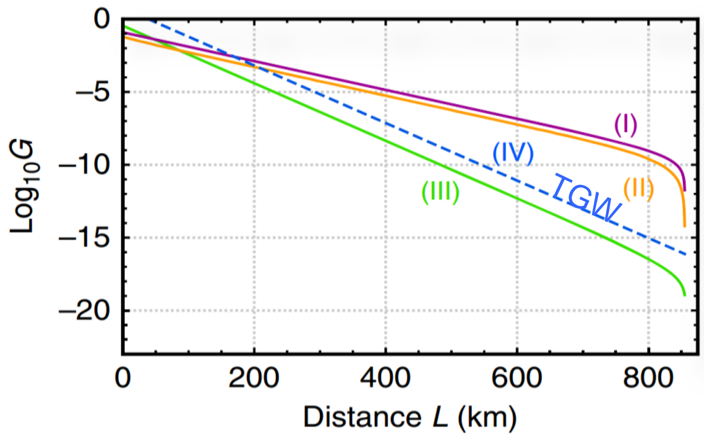
Other solutions


Received 1 Jul 2015 | Accepted 10 Nov 2015 | Published 16 Dec 2015 DOI: 10.1038/ncomms10171 OPEN

All-photonic intercity quantum key distribution

Koji Azuma[1], Kiyoshi Tamaki[1] & William J. Munro[1]





The implementation of these schemes is still challenging!

It turns out that we can overcome the direct-link bounds with a scheme nearly as simple as MDI-QKD

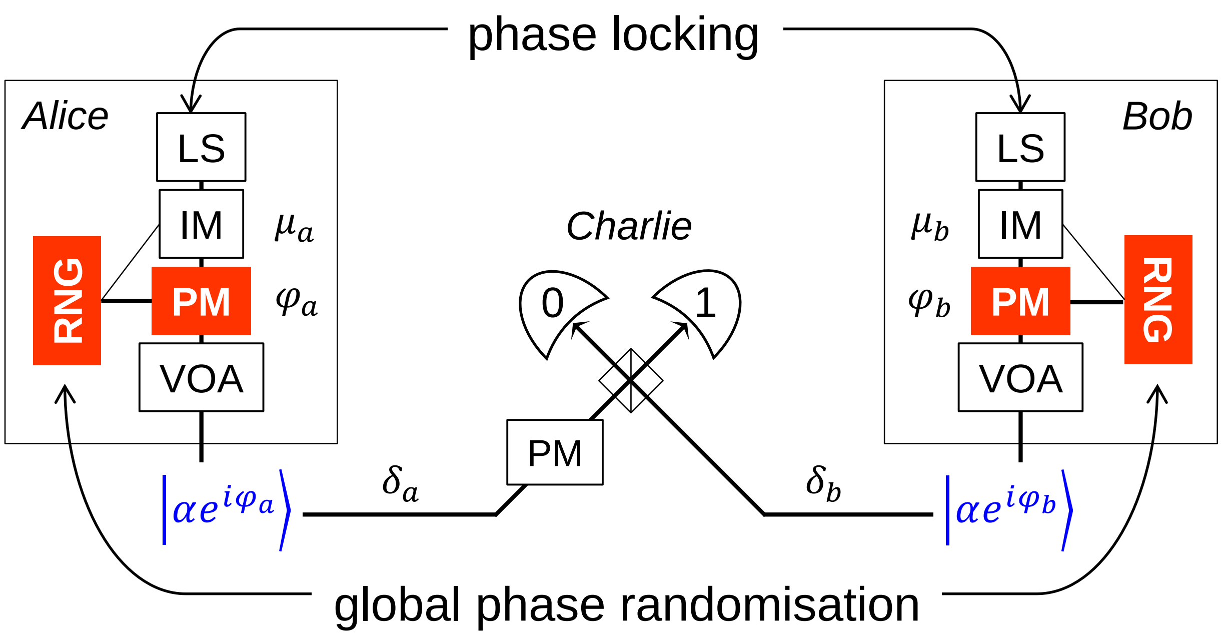
Twin-Field QKD

Overcoming the rate–distance limit of quantum key distribution without quantum repeaters

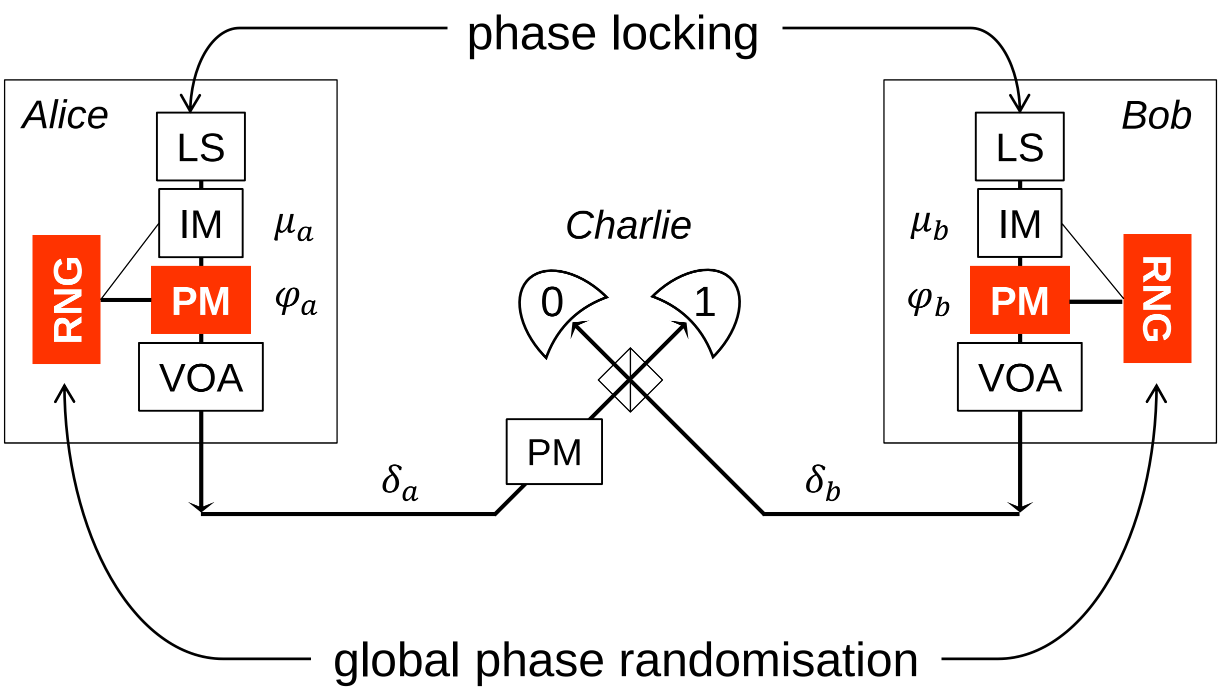
M. Lucamarini ✉, Z. L. Yuan, J. F. Dynes & A. J. Shields

Nature **557**, 400–403 (2018)
doi:10.1038/s41586-018-0066-6
Download Citation

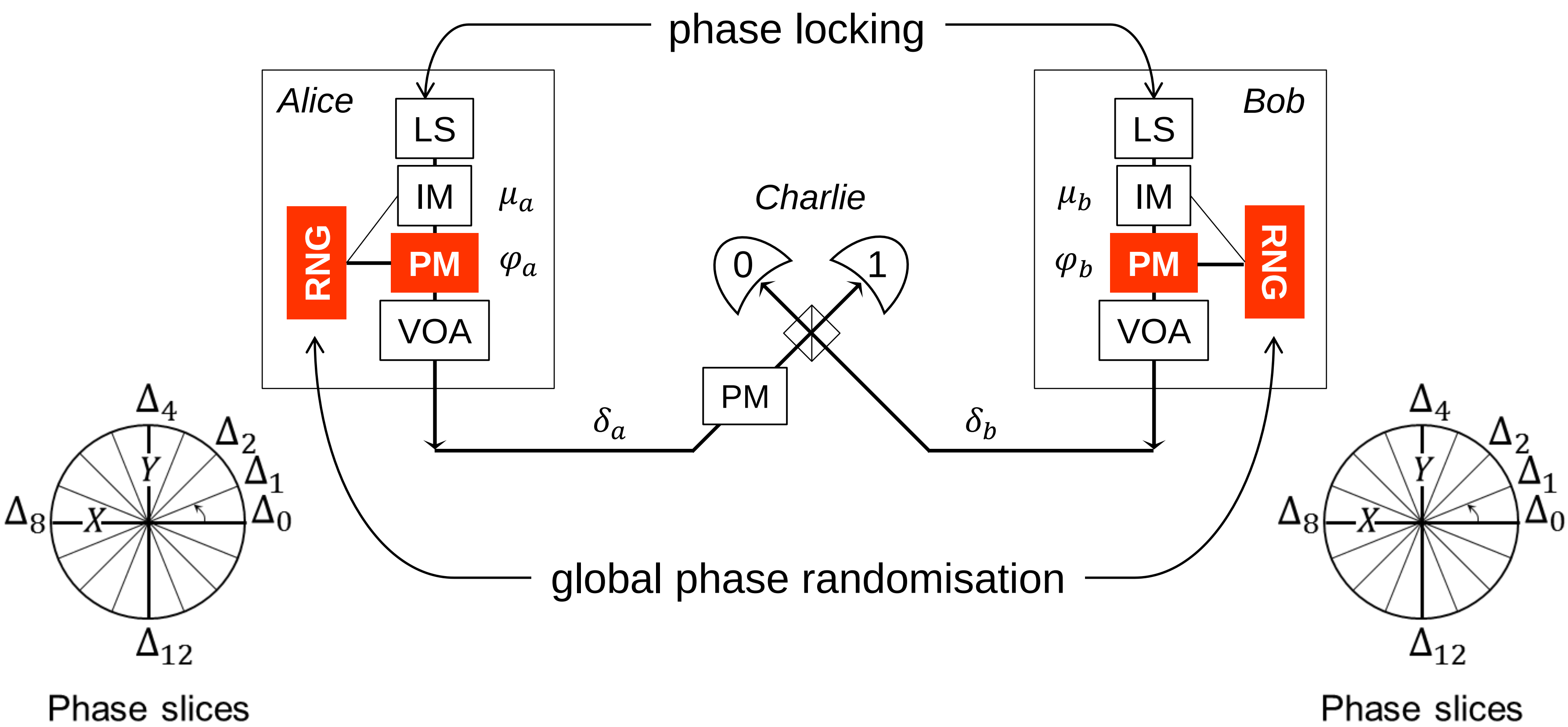
Received: 27 April 2017
Accepted: 05 February 2018
Published: 02 May 2018



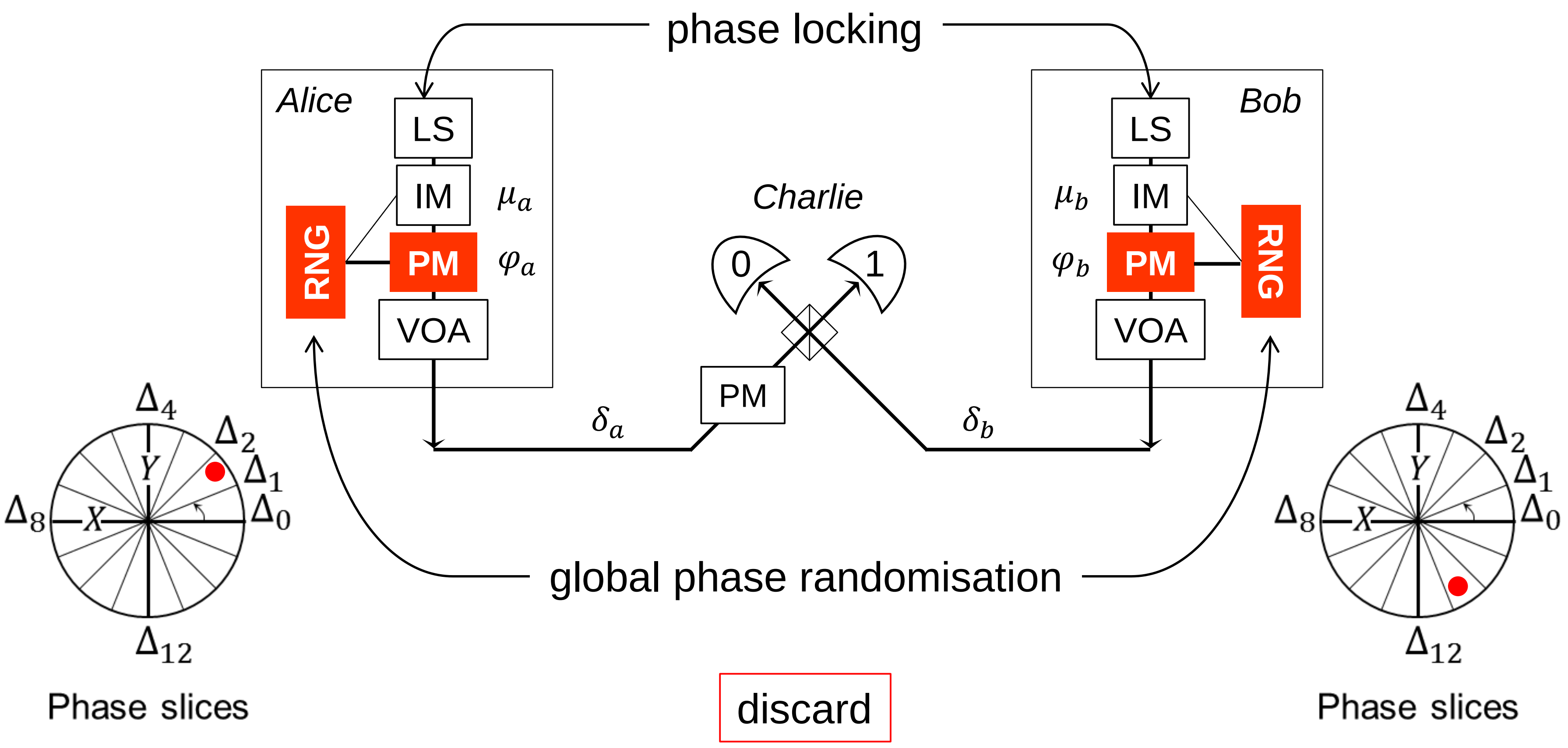
Twin-Field QKD



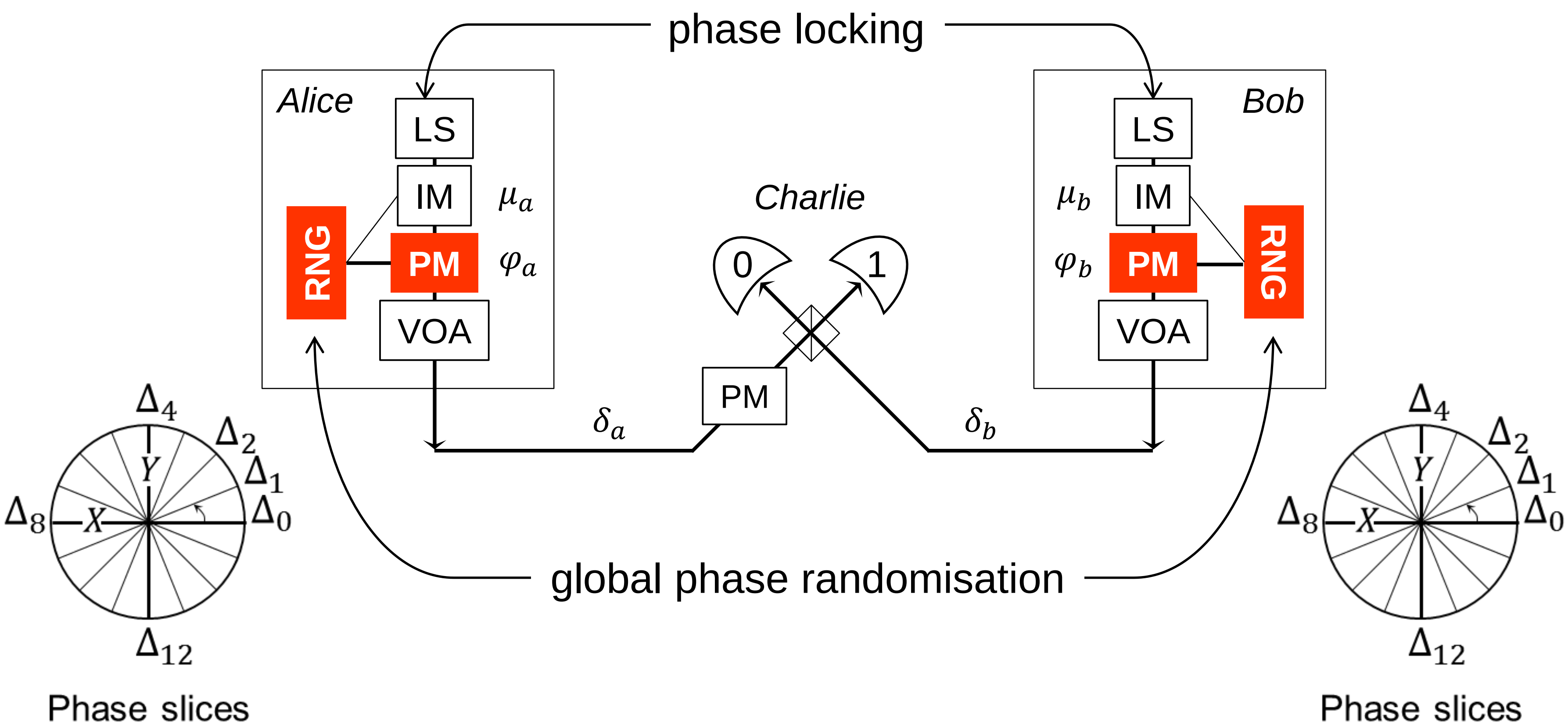
Twin-Field QKD



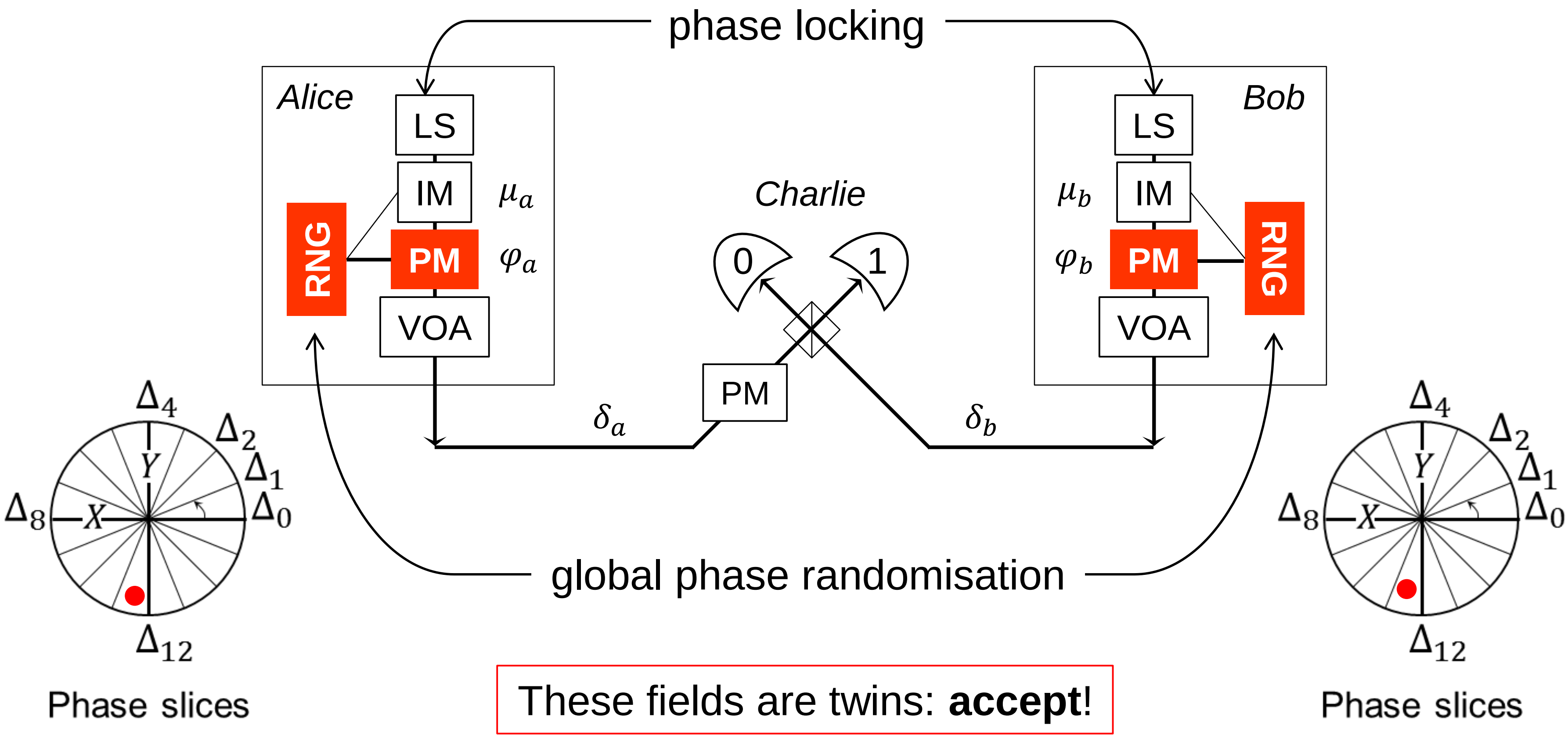
Twin-Field QKD



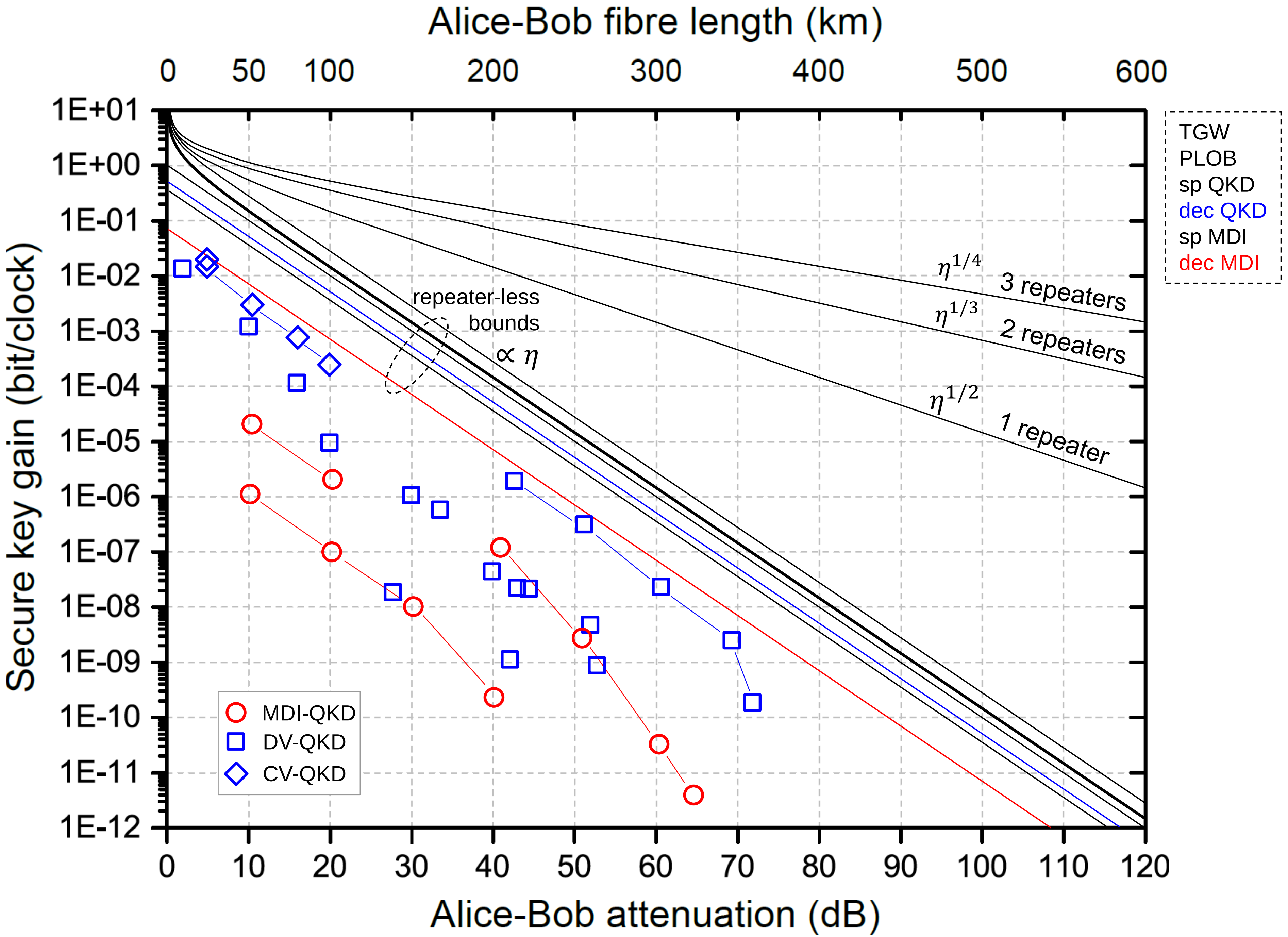
Twin-Field QKD



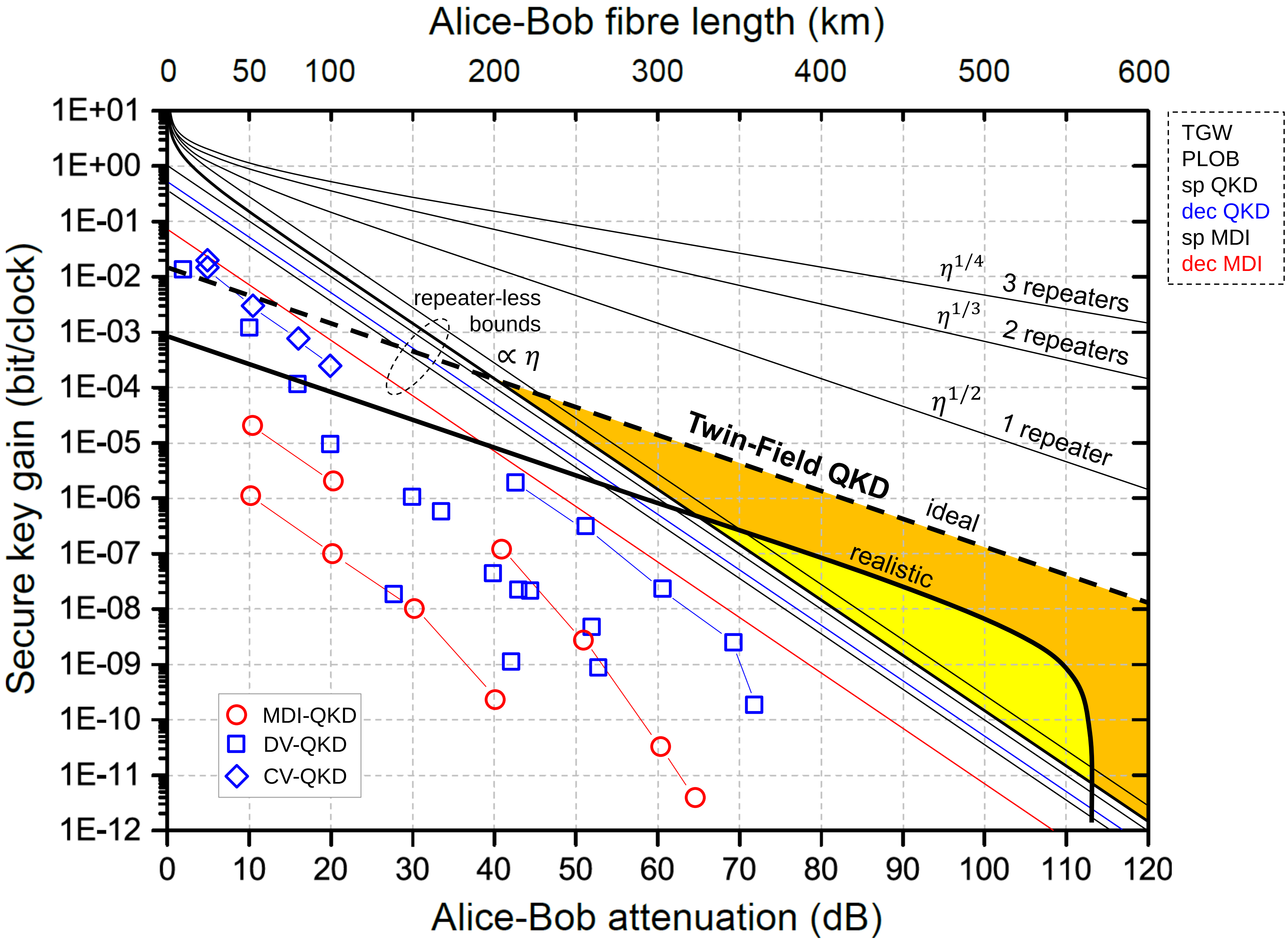
Twin-Field QKD



The users end up in a situation similar to decoy-state QKD, but with a twice-as-long fibre in between



Alice-Bob fibre length (km)
0
50
100
200
300
400
500
600
Secure key gain (bit/clock)
1E+01
1E+00
1E-01
1E-02
1E-03
1E-04
1E-05
1E-06
1E-07
1E-08
1E-09
1E-10
1E-11
1E-12
Alice-Bob attenuation (dB)
0
10
20
30
40
50
60
70
80
90
100
110
120
TGW
PLOB
sp QKD
dec QKD
sp MDI
dec MDI
repeater-less bounds
$\propto \eta$
$\eta^{1/4}$ 3 repeaters
$\eta^{1/3}$ 2 repeaters
$\eta^{1/2}$ 1 repeater
MDI-QKD
DV-QKD
CV-QKD

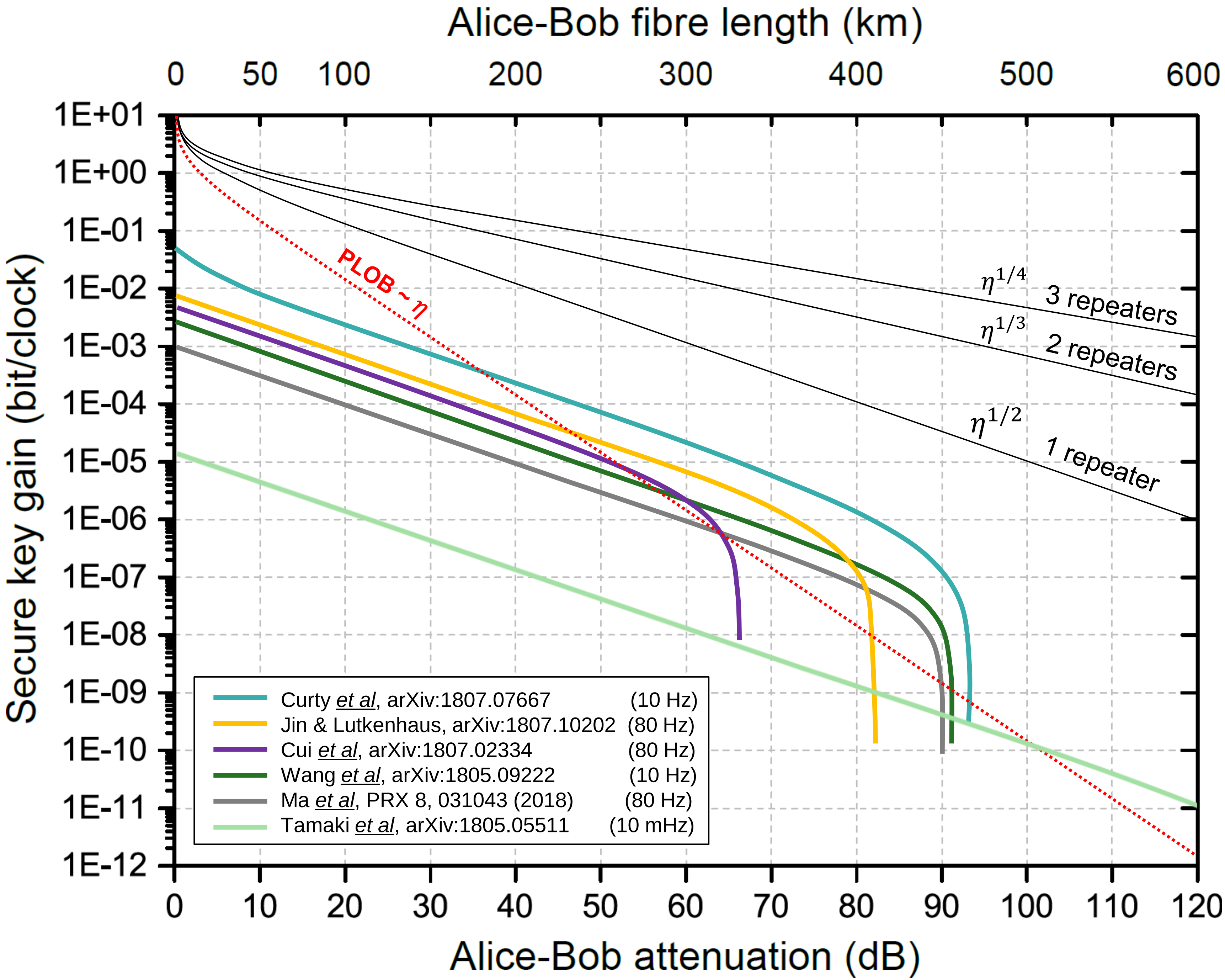


Alice-Bob fibre length (km)
0
50
100
200
300
400
500
600
Secure key gain (bit/clock)
1E+01
1E+00
1E-01
1E-02
1E-03
1E-04
1E-05
1E-06
1E-07
1E-08
1E-09
1E-10
1E-11
1E-12
Alice-Bob attenuation (dB)
0
10
20
30
40
50
60
70
80
90
100
110
120
TGW
PLOB
sp QKD
dec QKD
sp MDI
dec MDI
$\eta^{1/4}$
3 repeaters
$\eta^{1/3}$
2 repeaters
$\eta^{1/2}$
1 repeater
repeater-less
bounds
$\propto \eta$
Twin-Field QKD
ideal
realistic
MDI-QKD
DV-QKD
CV-QKD

Very recent (and very promising) progress

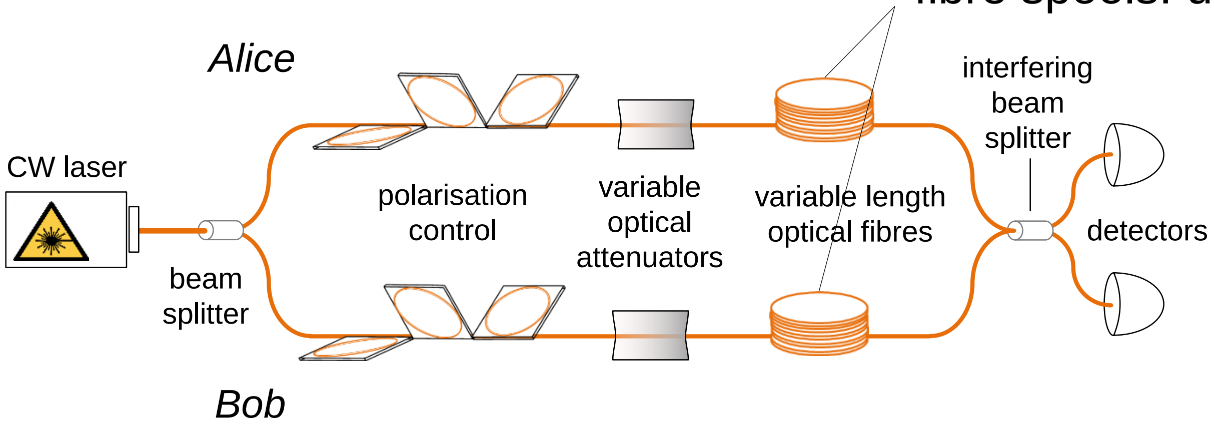
See next talk (10:50 am) by Pei Zeng: "*Global Phase Encoding QKD*"

- *15 May* X. Ma, P. Zeng & H. Zhou, "Phase-matching QKD", arXiv:1805.05538. Also @ Phys. Rev. X **8**, 031043 (2018).
- *15 May* K. Tamaki, H.-K. Lo, W. Wang & ML, "IT security of QKD overcoming the repeaterless secret key capacity bound", arXiv:1805.05511.
- *28 May* X.-B. Wang, Z.-W. Yu & X.-L. Hu, "Sending or not sending: Twin-Field QKD with large misalignment error", arXiv:1805.09222.
- *6 July* C. Cui, Z.-Q. Yin, R. Wang, W. Chen, S. Wang, G.-C. Guo & Z.-F. Han, "Phase-matching QKD without phase post-selection", arXiv:1807.02334.
- *19 July* M. Curty, K. Azuma & H.-K. Lo, "Simple security proof of Twin-Field type QKD protocol", 1807.07667. See Poster 14
- *26 July* J. Lin & N. Lütkenhaus, "A simple security analysis of phase-matching MDI-QKD", 1807.10202. See Poster 99

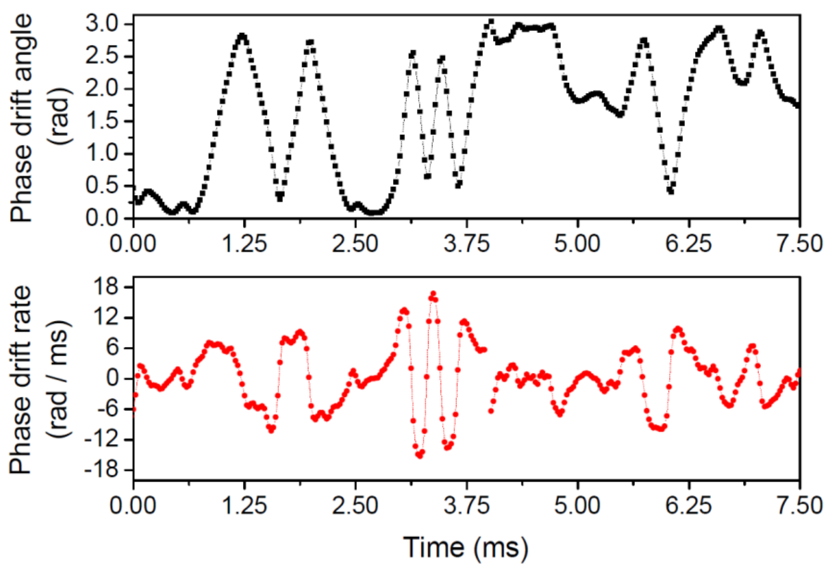

Alice-Bob fibre length (km)
0
50
100
200
300
400
500
600
Secure key gain (bit/clock)
1E+01
1E+00
1E-01
1E-02
1E-03
1E-04
1E-05
1E-06
1E-07
1E-08
1E-09
1E-10
1E-11
1E-12
PLOB ~ η
$\eta^{1/4}$ 3 repeaters
$\eta^{1/3}$ 2 repeaters
$\eta^{1/2}$ 1 repeater
Curty et al, arXiv:1807.07667 (10 Hz)
Jin & Lutkenhaus, arXiv:1807.10202 (80 Hz)
Cui et al, arXiv:1807.02334 (80 Hz)
Wang et al, arXiv:1805.09222 (10 Hz)
Ma et al, PRX 8, 031043 (2018) (80 Hz)
Tamaki et al, arXiv:1805.05511 (10 mHz)
0
10
20
30
40
50
60
70
80
90
100
110
120
Alice-Bob attenuation (dB)

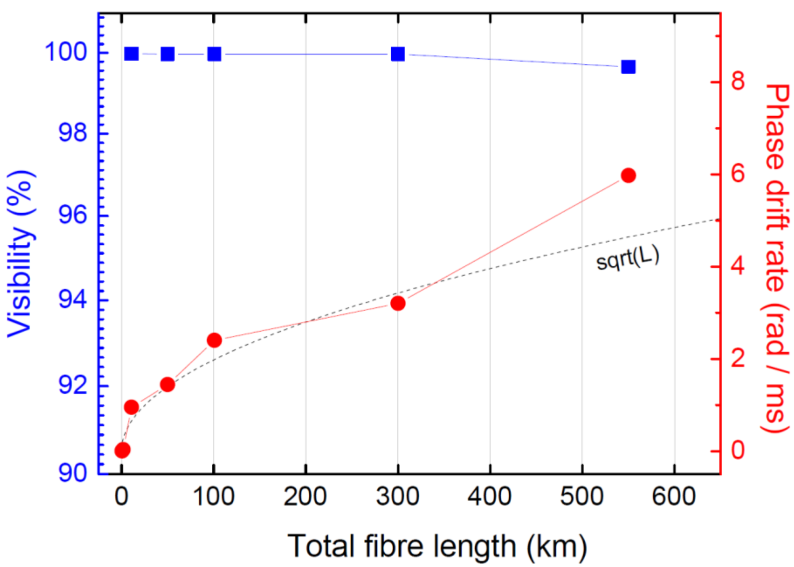
Twin-Field QKD Feasibility

Phase drift: $\delta_b - \delta_a = \frac{2\pi}{s}(\Delta v\ L + v\ \Delta L)$



With 6 rad/ms, a feedback every ~50 µs is necessary to make the optical error rate lower than 3%





Conclusions

- MDI-QKD is only 6 year-old, but we already have impressive results in terms of performance (key rate, distance) and functionalities (untrusted-node networks). This means the community is strong and responsive to innovations.
- The research on MDI-QKD has led to developments like
  - all-optical quantum repeaters
  - coherent-state HOM interference
  - optically-injected laser sources for quantum communications
  - refined control techniques for the in-field implementations.
- The (MDI) Twin-Field QKD allows us to overcome a bound considered unsurmountable without quantum repeaters. New techniques for quantum communications are likely to be imported from other fields.

The path to MDI Quantum Information has just started and we can expect many more surprising and exciting results along the way!

Thanks to…

MDI-QKD team at TREL


Mariella Minder


Mirko Pittaluga


George Roberts


Zhiliang Yuan


Andrew Shields


James Dynes

…and to you for your attention!