JIQT

Experimental Twin-Field Quantum Key Distribution Through Sending-or-Not-Sending

Yang Liu

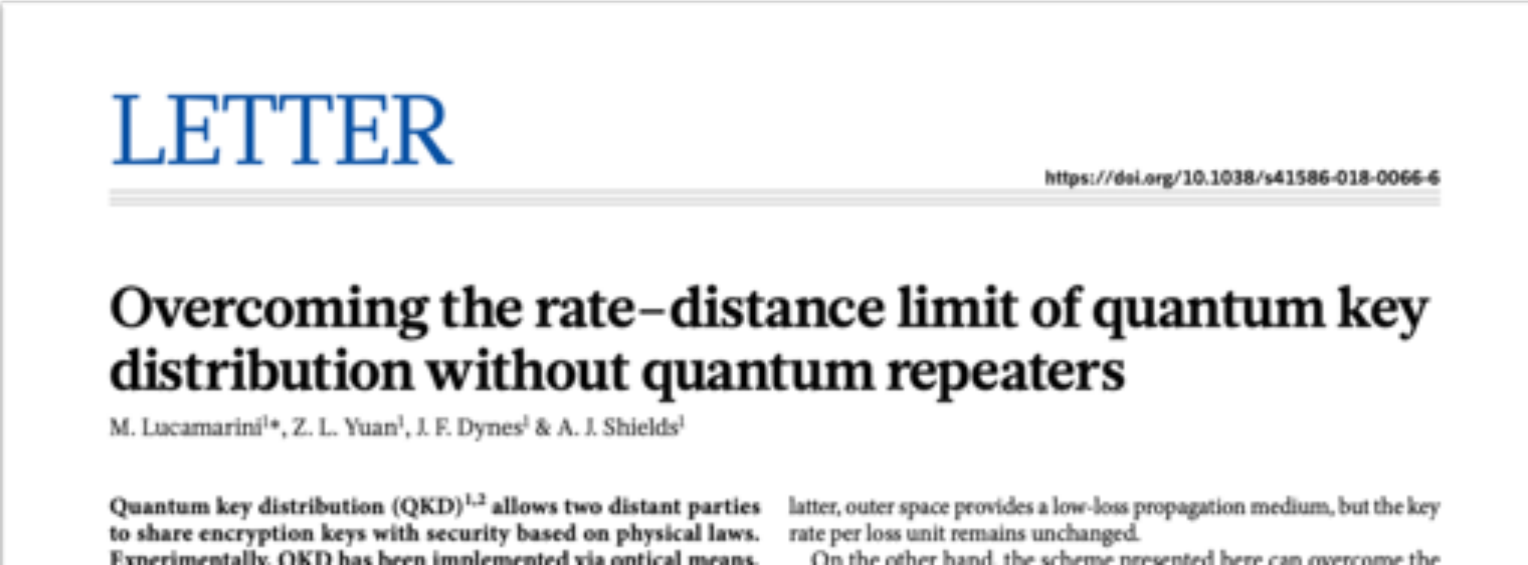
Jinan Institute of Quantum Technology (JIQT)
University of Science and Technology of China (USTC)

QCRYPT 2020

Twin-Field QKD (TF-QKD)

Proposed in 2018, which “greatly extending the range of secure quantum communications”, and “feasible with current technology”.

Lucamarini, M., et.al., *Nature* **557**, 400–403 (2018).



LETTER

https://doi.org/10.1038/s41586-018-0066-6

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

M. Lucamarini[1]*, Z. L. Yuan[1], J. F. Dynes[1] & A. J. Shields[1]

Quantum key distribution (QKD)[1,2] allows two distant parties to share encryption keys with security based on physical laws. Experimentally, QKD has been implemented via optical means.

latter, outer space provides a low-loss propagation medium, but the key rate per loss unit remains unchanged.

On the other hand, the scheme presented here can overcome the

Recent Progress

Theories

Nature **557**, 400 (2018).
Phys Rev Appl **12**, 054034 (2018).
Phys Rev Appl **11**, 034053 (2018).
Phys Rev X **8**, 031043 (2018).
Phys Rev A **98**, 042332 (2018).
Npj QI **5**, 64 (2019).
Phys Rev A **98**, 062323 (2018).
New J Phys **21**, 073001 (2019).
New J Phys **21**, 113032 (2019).
New J Phys **22**, 013020 (2019).
PR Applied **11**, 034053 (2019).
Phys Rev A **100**, 062337 (2019).
Phys Rev Appl **12**, 024061 (2019).
Phys Rev A **100**, 022306 (2019).
Sci Report **9**, 14918 (2019).
New J Phys **21**, 123030 (2019).
Npj QI **5**, 64 (2019).
Phys Rev A **99**, 062316 (2019).
Opt Lett **44**, 1468 (2019).
Phys Rev A **101**, 042330 (2020).
New J Phys **22**, 053048 (2020).
Opt Express **28**, 22594 (2020).

Experiments

Experimental quantum key distribution beyond the repeaterless secret key capacity, *Nature Photonics* **13**, 334 (2019).

Beating the Fundamental Rate-Distance Limit in a Proof-of-Principle Quantum Key Distribution System, *Physical Review X* **9**, 021046 (2019).

Experimental Twin-Field Quantum Key Distribution Through Sending-or-Not-Sending, *Physical Review Letters* **123**, 100505 (2019).

Proof-of-Principle Experimental Demonstration of Twin-Field Type Quantum Key Distribution, *Physical review letters* **123**, 100506 (2019).

Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution Over 509 km, *Physical Review Letters* **124**, 070501 (2019).

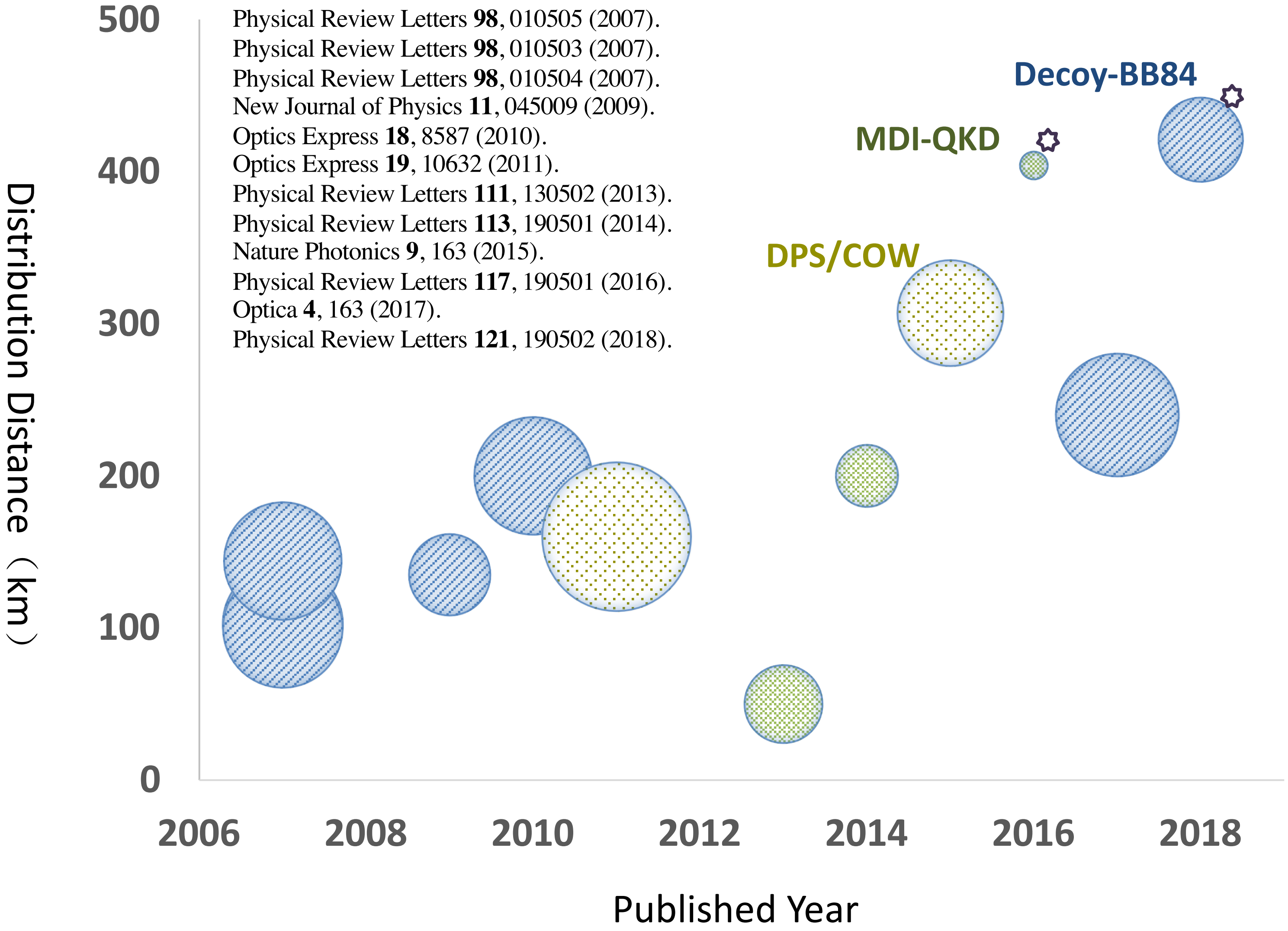
Implementation of quantum key distribution surpassing the linear rate-transmittance bound, *Nat Photonics* **14**, 422–425 (2020).

(and many more works…)

Previous QKD performances

Status of QKD (before TF-QKD) Systems

Limited distribution distance in QKD systems

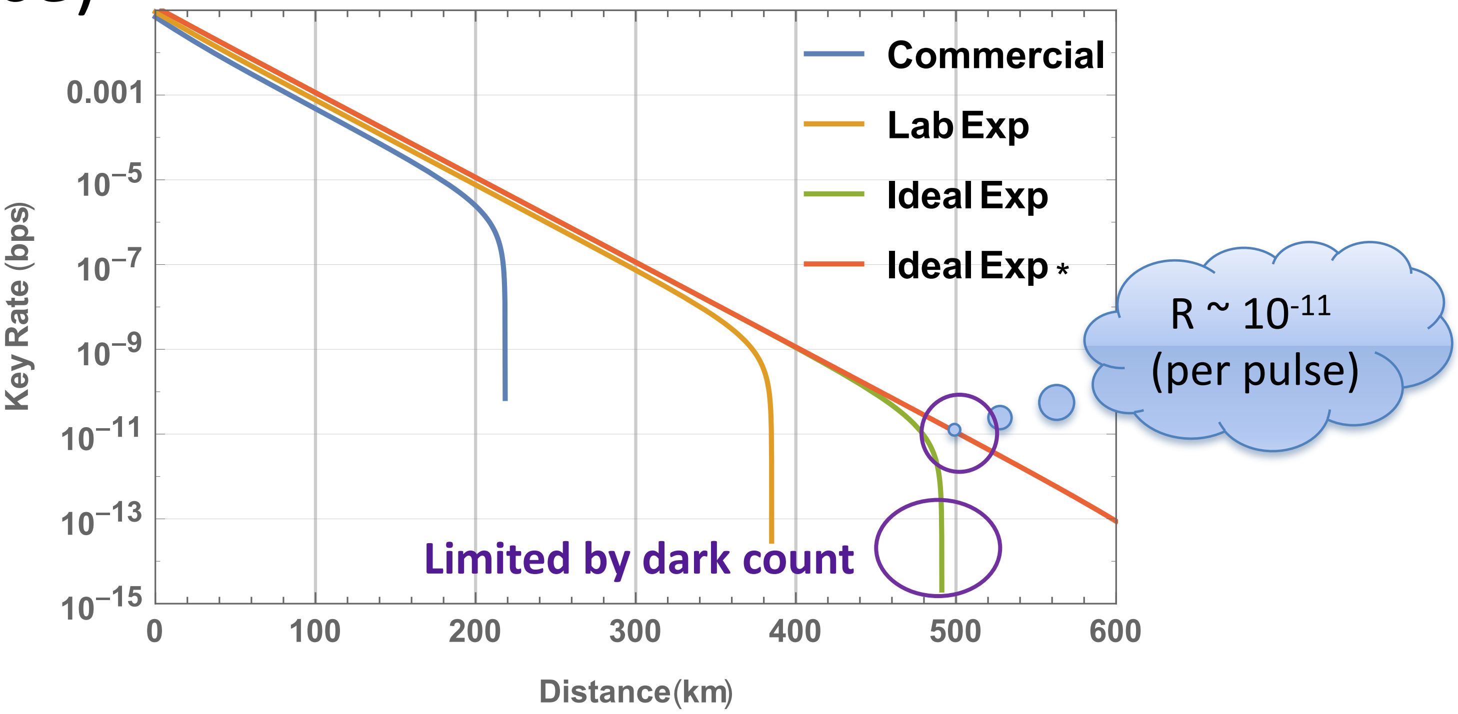

Physical Review Letters **98**, 010505 (2007).
Physical Review Letters **98**, 010503 (2007).
Physical Review Letters **98**, 010504 (2007).
New Journal of Physics **11**, 045009 (2009).
Optics Express **18**, 8587 (2010).
Optics Express **19**, 10632 (2011).
Physical Review Letters **111**, 130502 (2013).
Physical Review Letters **113**, 190501 (2014).
Nature Photonics **9**, 163 (2015).
Physical Review Letters **117**, 190501 (2016).
Optica **4**, 163 (2017).
Physical Review Letters **121**, 190502 (2018).

✡ Using Low Loss Fiber

Example: Decoy based BB84 QKD

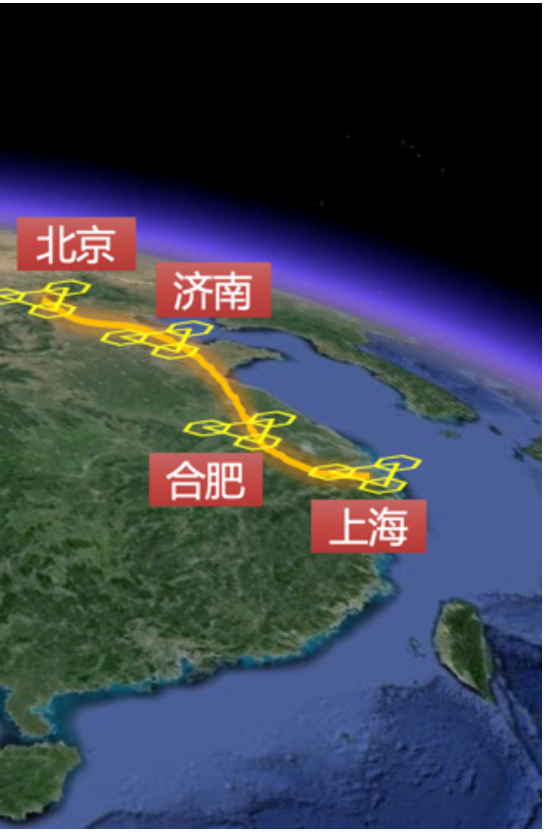
System	Exp. Time	System Freq.	Det. Efficiency	QBER	Dark count
Commercial	5 mins	100 MHz	30%	2%	10000
Lab Exp.	1 Month	1 GHz	90%	1%	10
Ideal Exp.	>1 Month	10 GHz	100%	0%	0.1
Ideal Exp. *	>1 Month	10 GHz	100%	0%	0

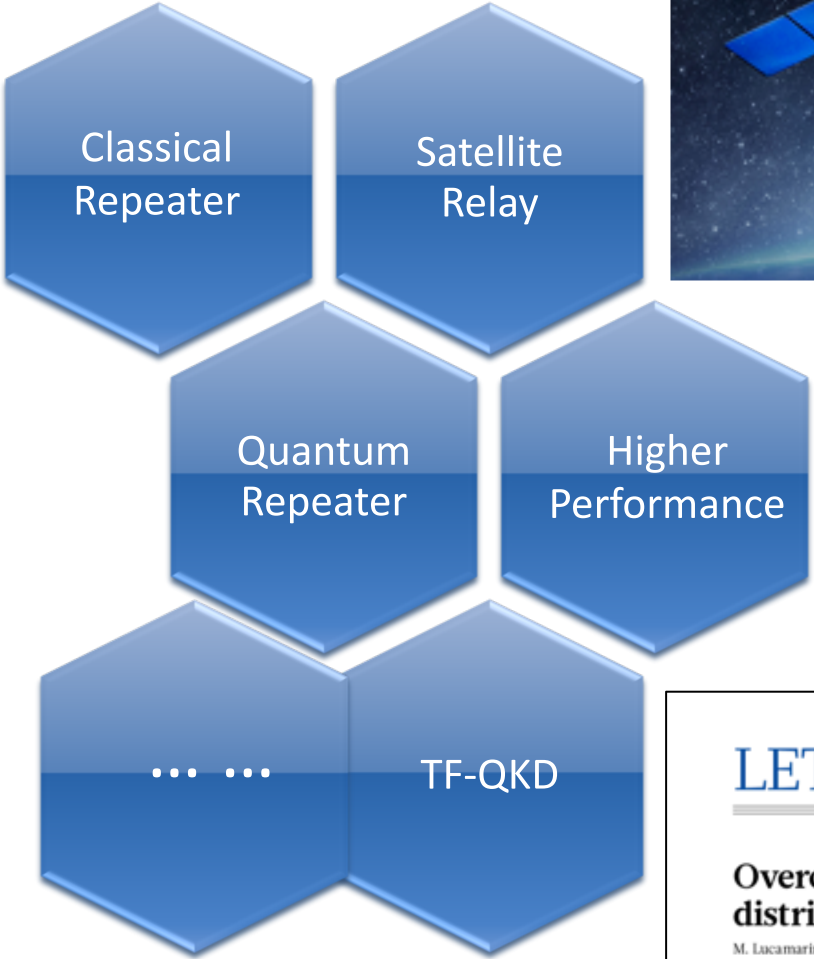
(In Practice)



To improve the performance…

Further enhancing the distribution distance




Classical Repeater

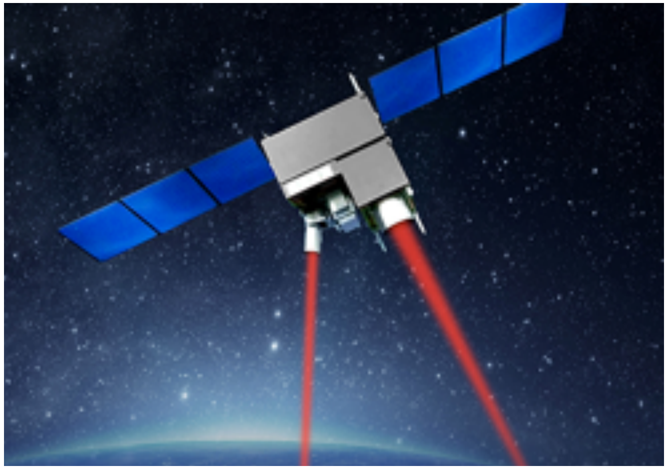
Satellite Relay

Quantum Repeater

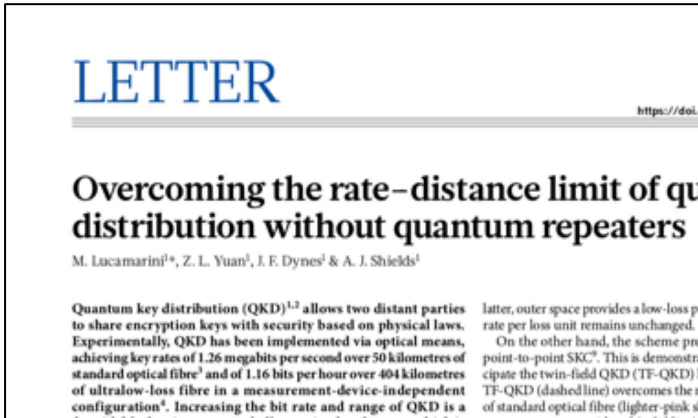
Higher Performance

… …

TF-QKD



Nature **557**, 400 (2018)


LETTER

https://doi.

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

M. Lucamarini[1]*, Z. L. Yuan[1], J. F. Dynes[1] & A. J. Shields[1]

Quantum key distribution (QKD)[1,2] allows two distant parties to share encryption keys with security based on physical laws. Experimentally, QKD has been implemented via optical means, achieving key rates of 1.26 megabits per second over 50 kilometres of standard optical fibre[3] and of 1.16 bits per hour over 404 kilometres of ultralow-loss fibre in a measurement-device-independent configuration[4]. Increasing the bit rate and range of QKD is a

latter, outer space provides a low-loss p rate per loss unit remains unchanged.

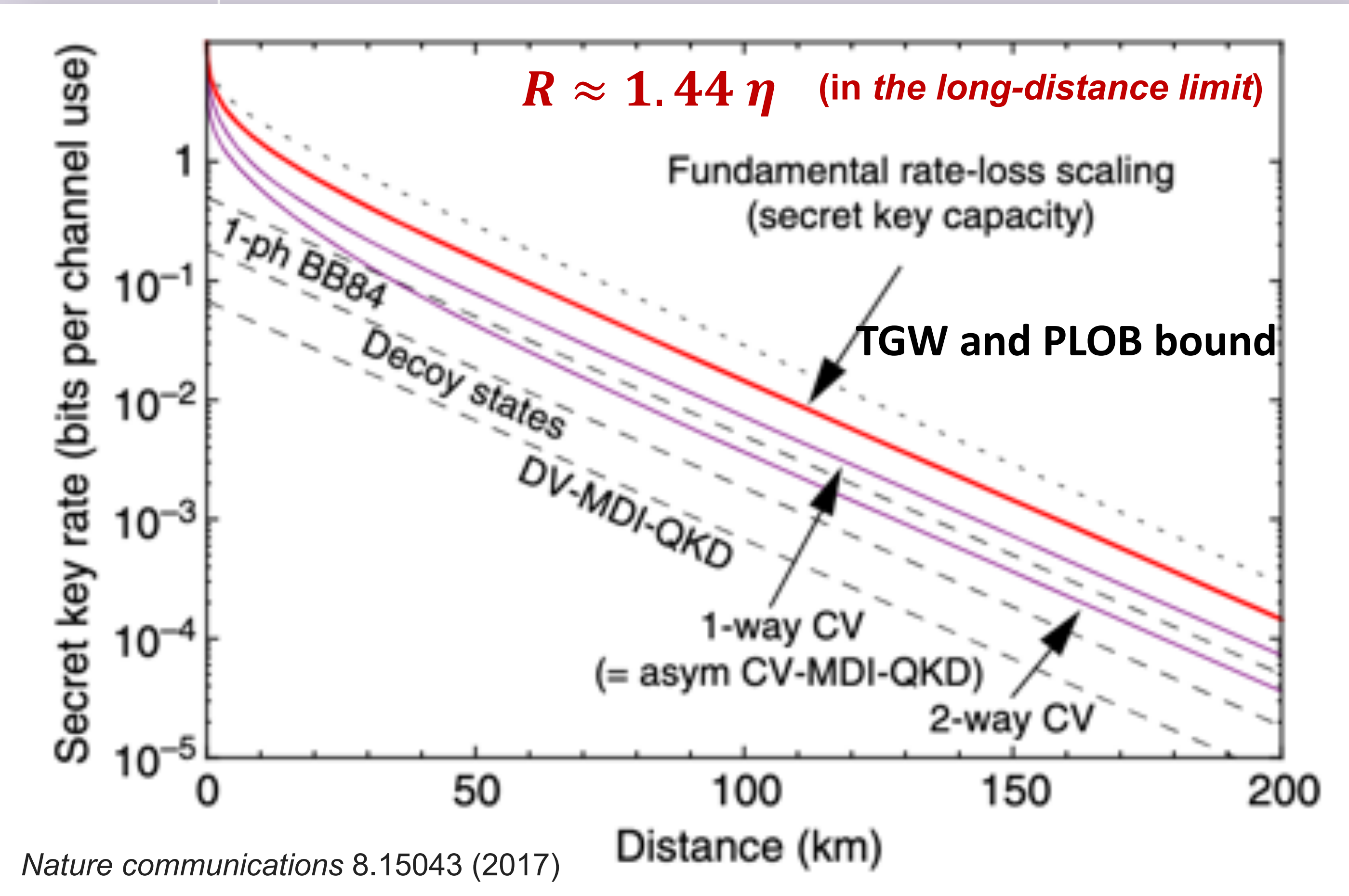
On the other hand, the scheme pr point-to-point SKC[9]. This is demonstr cipate the twin-field QKD (TF-QKD) TF-QKD (dashed line) overcomes the of standard optical fibre (lighter-pink s

Key rate v.s. Channel loss

Protocol	Key rate
BB84 (Single Photon)	$R = \eta[1 - H_2(\delta) - H_2(\delta_p)]$ $R \propto \eta$
BB84 (Coherent light)	$R = \frac{1}{2} p_D \times R' \approx \eta^2 \Delta \times R'$ $R' = [(1-\Delta) - H_2(\delta) - (1-\Delta) H_2\left(\frac{\delta_p}{1-\Delta}\right)]$ (if Δ fixed as η gets small) $R \propto \eta^2$ Gottesman, Daniel, et al. *ISIT 2004.*
BB84 (Decoy)	$R = q\{Q_1[1 - H_2(e_1)] - Q_\mu H_2(E_\mu)\}$ $Q_\mu = Y_0 + 1 - e^{-\eta\mu} \approx \eta\mu$ $Q_1 = \eta\mu e^{-\mu}$ $R \propto \eta$ PRL 94.230503 (2005) PRL 94.230504 (2005).
MDI-QKD	$R = P_z^{11} Y_z^{11}[1 - H_2(e_x^{1,1})] - Q_z f(E_z) \mathrm{H}_2(\mathrm{E}_z)$ $R \propto \eta$

Key rate v.s. Channel loss

Protocol	Key rate
(Sing	$R \propto \eta$
(Coh	d as η gets small) $R \propto \eta^2$ el, et al. *ISIT 2004.*
BB8	$R \propto \eta$ 2005) 2005).
M	$R \propto \eta$



$R \approx 1.44\,\eta$ (in *the long-distance limit*)

TGW and PLOB bound

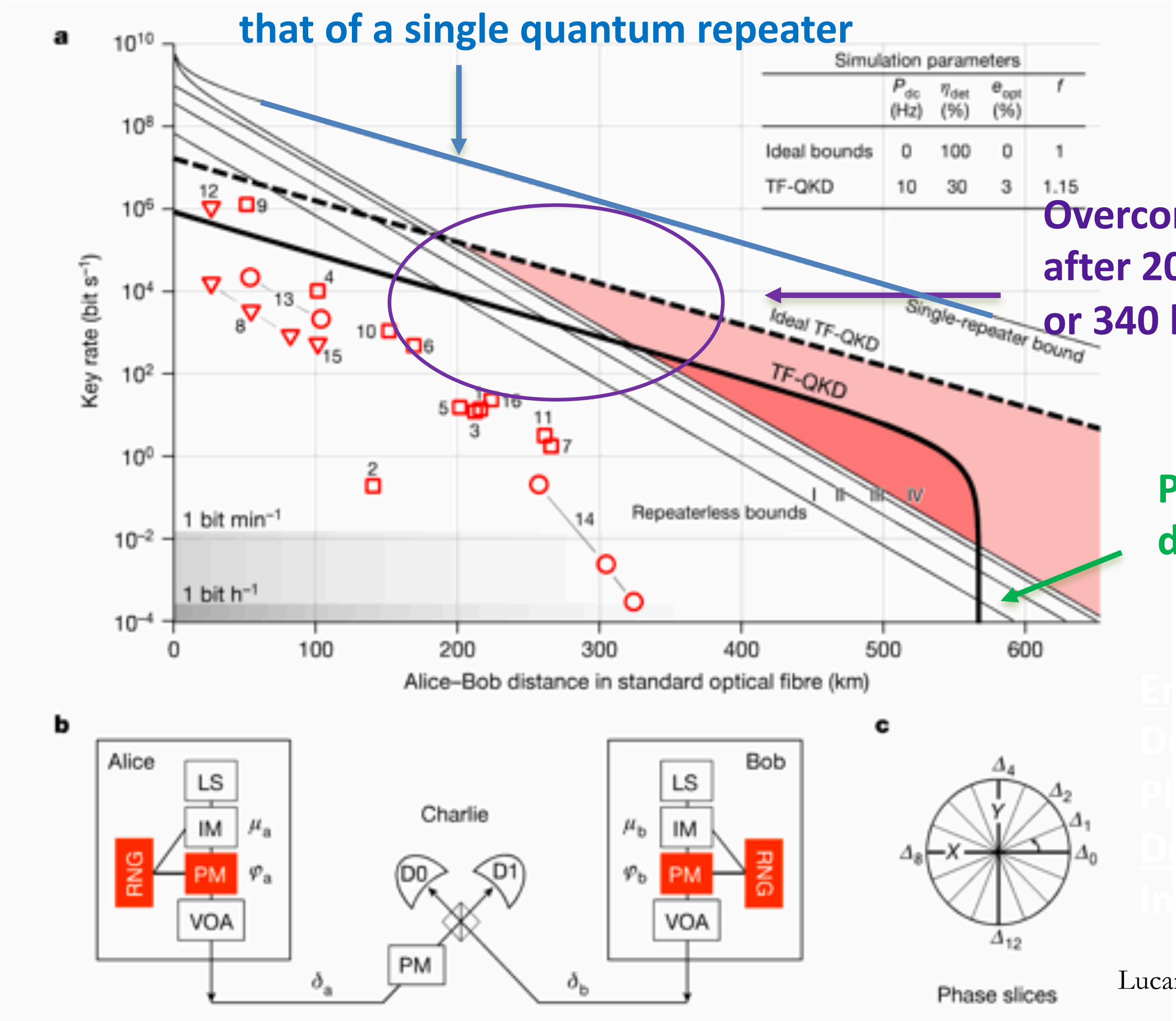
Nature communications 8.15043 (2017)

Key rate v.s. Channel loss

Protocol	**Key rate**
BB84 (Single Photon)	$R = \eta[1 - H_2(\delta) - H_2(\delta_p)]$ $R \propto \eta$
BB84 (Coherent light)	$R = \frac{1}{2} p_D \times R' \approx \eta^2 \Delta \times R'$ $R' = [(1-\Delta) - H_2(\delta) - (1-\Delta) H_2\left(\frac{\delta_p}{1-\Delta}\right)]$ (if Δ fixed as η gets small) $R \propto \eta^2$ Gottesman, Daniel, et al. *ISIT 2004.*
BB84 (Decoy)	$R = q\{Q_1[1 - H_2(e_1)] - Q_\mu H_2(E_\mu)\}$ $Q_\mu = Y_0 + 1 - e^{-\eta\mu} \approx \eta\mu$ $\qquad Q_1 = \eta\mu \mathrm{e}^{-\mu}$ $R \propto \eta$ PRL 94.230503 (2005) PRL 94.230504 (2005).
MDI-QKD	$R = P_z^{11} Y_z^{11}[1 - H_2(e_x^{1,1})] - Q_z f(E_z) \mathrm{H}_2(\mathrm{E}_z)$ $R \propto \eta$
TF-QKD	$R = Q_{\mu,L}^1[1 - H_2(e_{\mu,L}^1)] - Q_{\mu,L} f(E_z) \mathrm{H}_2(\mathrm{E}_{\mu,L})$ $R \propto \sqrt{\eta}$

Twin-Field QKD (TF-QKD)

Key rate resembles
that of a single quantum repeater



Simulation parameters

	P_{dc} (Hz)	η_{det} (%)	e_{opt} (%)	f
Ideal bounds	0	100	0	1
TF-QKD	10	30	3	1.15

$$R \propto \sqrt{\eta}$$

Overcomes the repeaterless bounds
after 200 km (ideal)
or 340 km (practical)

Promises 500 km long
distance distribution

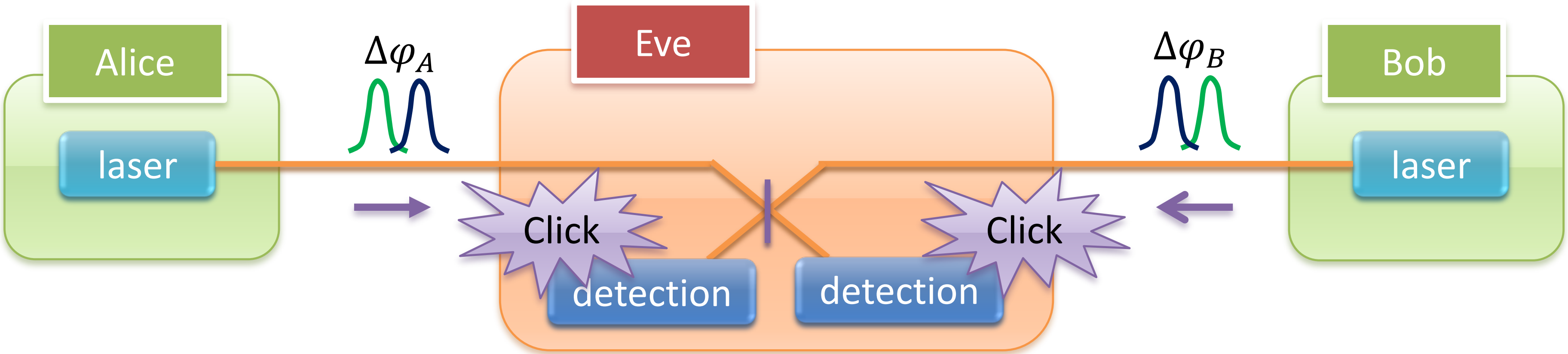
Lucamarini, et.al., *Nature* **557,** 400–403 (2018).

TF-QKD Protocol

To be more specific…

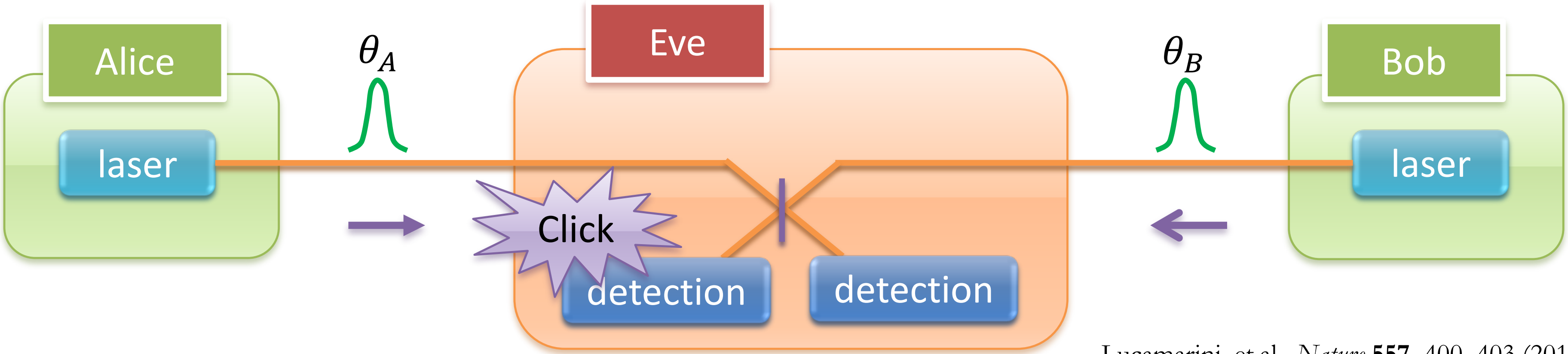
1) General "Sending−Receiving " QKD (e.g., BB84)

2) Measurement device independent (MDI−QKD)



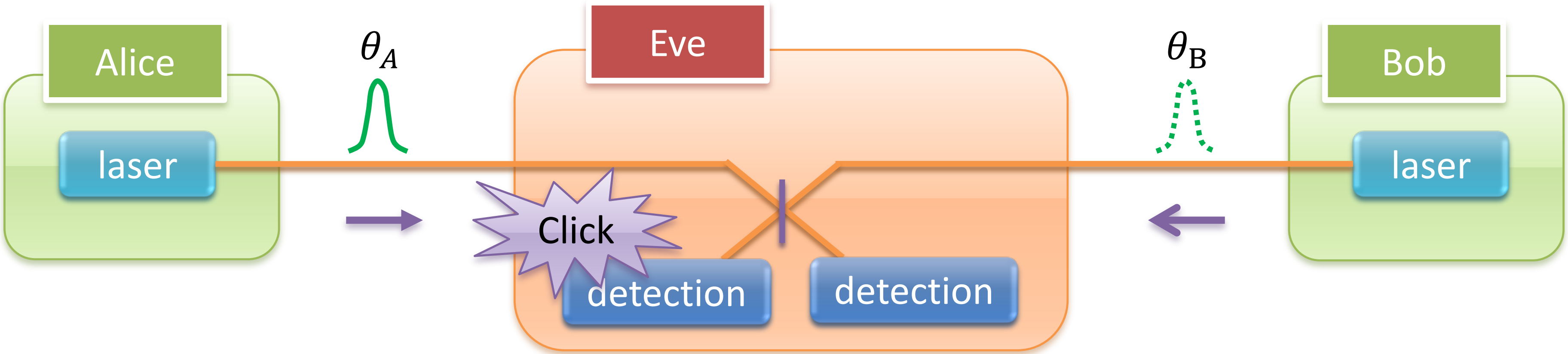
TF-QKD Schemes

3) Twin−Field QKD (QKD)



Lucamarini, et.al., *Nature* **557,** 400–403 (2018).

4) Sending−or−Not−Sending (SNS−TF−QKD)



Wang, X.-B., et.al., *Physical Review A* **98,** 062323 (2018).

SNS-TF-QKD Introduction: Encoding

Alice/Bob Encoding (Example)

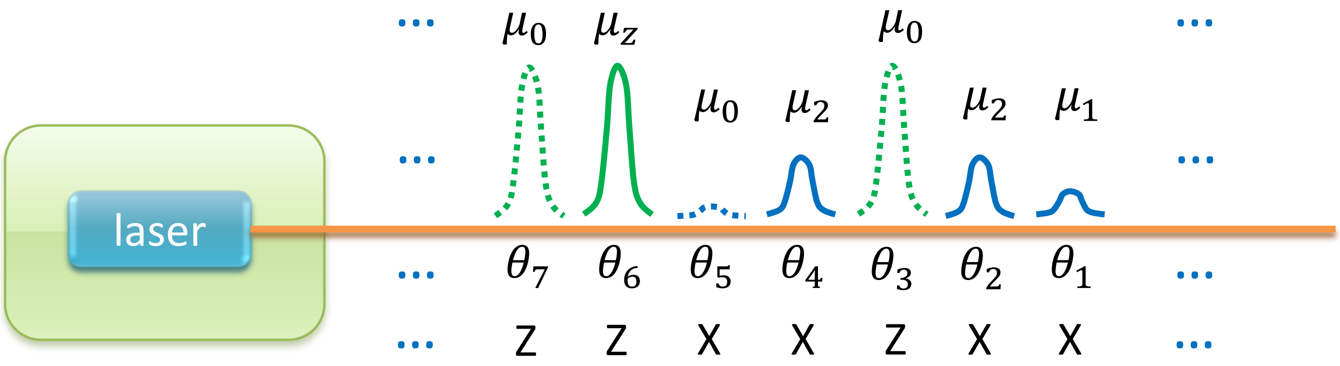
Basis	**Phase (Alice / Bob)**	**Intensity**	**S/NS**	**Probability**
Z	θ_A / θ_B	μ_z	Not Sending	$p_z * (1 - p_a)$
Z	θ_A / θ_B	μ_z	Sending	$p_z * p_a$
X	θ_A / θ_B	$\mu_0 = 0$	Sending	$p_X * p_0$
X	θ_A / θ_B	μ_1	Sending	$p_X * p_1$
X	θ_A / θ_B	μ_2	Sending	$p_X * p_2$

Wang, X.-B., et.al., *Physical Review A* **98,** 062323 (2018).

Z basis: encoding 0/1 with “Send”/”Not Sending”

X basis: encoding with 16 different phases θ_A/θ_B

e.g., $\left|\sqrt{\mu_z}\, e^{i\theta_A}\right\rangle \left|\sqrt{\mu_z}\, e^{i\theta_B}\right\rangle$

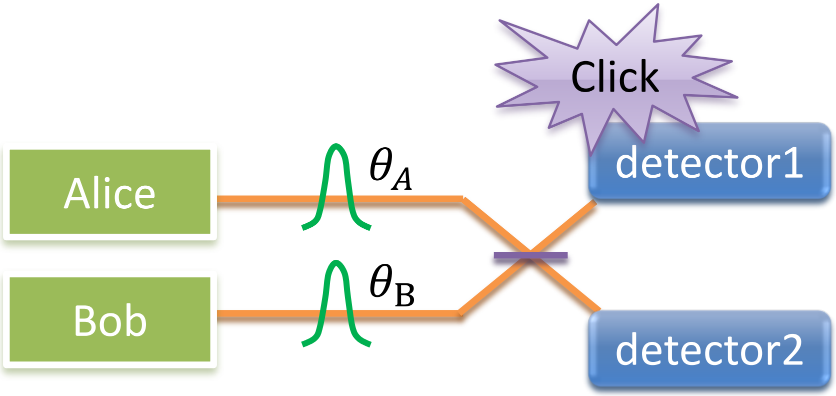


SNS-TF-QKD Introduction: Decoding

Charlie measures all interference, and announces effect event with:
One detector counting if A/B both determined signal/decoy window

Z-Window (A/B choose Z basis)

	Alice	Bob
Correct	S	N
	N	S
Error	S	S
	N	N



X-Window (A/B choose X basis)

Only keep the events satisfy:

$$|\theta_A - \theta_B + \Delta\varphi_T| \le Ds$$

$$|\theta_A - \theta_B + \Delta\varphi_T| \le Ds + \pi$$

where $\Delta\varphi_T$ is the path phase,
Ds is the allowed deviation.

Range	Ds	$Ds + \pi$
Correct	Det 1	Det 2
Error	Det 2	Det 1

The phase and bit information are not announced. Detections for different bases are record for analysis.

ZZ00, ZZ03, ZZ30, ZZ33, ZX00, ZX01, ZX02, ZX30, XZ00, XZ10, XZ20, XZ03, XX00, XX01, XX02, XX20, XX11, XX22

SNS-TF-QKD Introduction: Security

Estimate flipping rate in X1-window $e_1^{\mathcal{X}_1} \leqslant \bar{e}_1^{\mathcal{X}_1} = \frac{S_\mu E_\mu^X - e^{-2\mu} s_0/2}{2\mu e^{-2\mu} s_1}$

Asymptotically: $e_1^{ph} = e_1^{\chi_1}$

Final secure key rate: $\boxed{N_f = n_1 - n_1 H\left(e_1^{ph}\right) - n_t f H(E^Z)}$

Security is proofed with Virtual protocols and reduction:

Consider virtual ancillary state $\mathcal{A}n$, phase randomized coherent state, extended state is

$\Omega = \sum_r q_r \Omega_r$,with

(for 1-photon/vac/multi-photon)

$$\Omega_1 = (1/2)(|01\rangle\langle 01| \otimes |01\rangle\langle 01| + |10\rangle\langle 10| \otimes |10\rangle\langle 10|),$$

$$\Omega_2 = (1/2)[(|0\rangle\langle 0|\tilde{\otimes}\bar{\rho}) \otimes |01\rangle\langle 01| + (\bar{\rho}\tilde{\otimes}|0\rangle\langle 0|) \otimes |10\rangle\langle 10|],$$

$$\Omega_3 = |00\rangle\langle 00| \otimes |00\rangle\langle 00|,$$

$$\Omega_4 = (\rho_{\mu'}\tilde{\otimes}\rho_{\mu'}) \otimes |11\rangle\langle 11|.$$

Consider 1-photon component,

$$\Omega_{0i} = |\Psi_{1i}\rangle\langle\Psi_{1i}|,$$

$$|\Psi_{1i}\rangle = \frac{1}{\sqrt{2}}(e^{i\gamma_{B_i}}|01\rangle \otimes |01\rangle + e^{i\gamma_{A_i}}|10\rangle \otimes |10\rangle)$$

After Charlie's measuring, and purification ancillary state becomes $|\Phi^0\rangle = |01\rangle + |10\rangle$,

or $|\Phi^1\rangle = |01\rangle - |10\rangle$

A/B measure locally to obtain final key k_f

SNS-TF-QKD Introduction: Conclusion

- TF-QKD
  - MDI- type QKD protocol
  - Key rate scales with square root of loss: $R \propto \sqrt{\eta}$
    - Longer distribution distance and higher key rate
- SNS-TF-QKD
  - Does not announce phase information
    - So decoy state method can apply
  - Phase interference only in X basis
    - QBER in Z basis can be negligibly small
    - Allow high (e.g., 20%) X basis QBER due to interference
    - Still possible to achieve long distribution distance

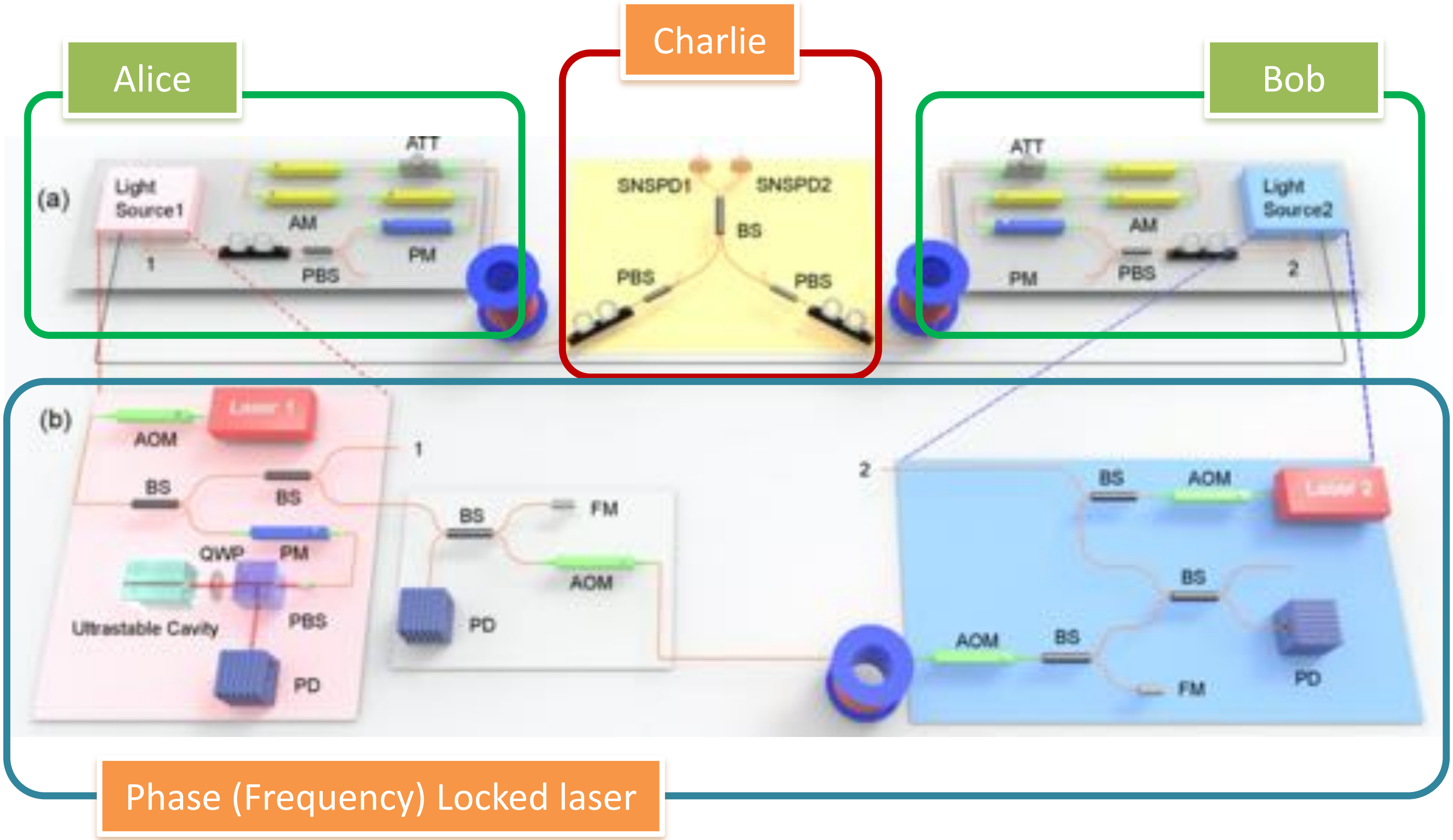
Challenges in TF-QKD experiment

Experimental TF-QKD is not easy

- ❖Single photon interference
  - ◉Requires same wavelength independent laser
  - ◉Requires ultra narrow laser bandwidth (10 kHz)
  - ◉Requires precise fiber phase stabilization
- ❖Low dark count noise
  - ◉SNS-TF-QKD requires ultra-low dark count in SPD
  - ◉Understanding and controlling fiber noise
- ❖Phase stabilization
  - ◉Reference pulses requires deep modulation
  - ◉Stabilizing/recover phase in short time

SNS-TF-QKD experimental setup

SNS-TF-QKD Setup



Alice

Charlie

Bob

Phase (Frequency) Locked laser

SNS-TF-QKD: Phase Stabilization

- Phase interference with Independent lasers

$$\delta_{\text{ba}} = \frac{2\pi}{s}(\Delta\nu L + \nu\Delta L)$$

Wavelength difference (A/B)

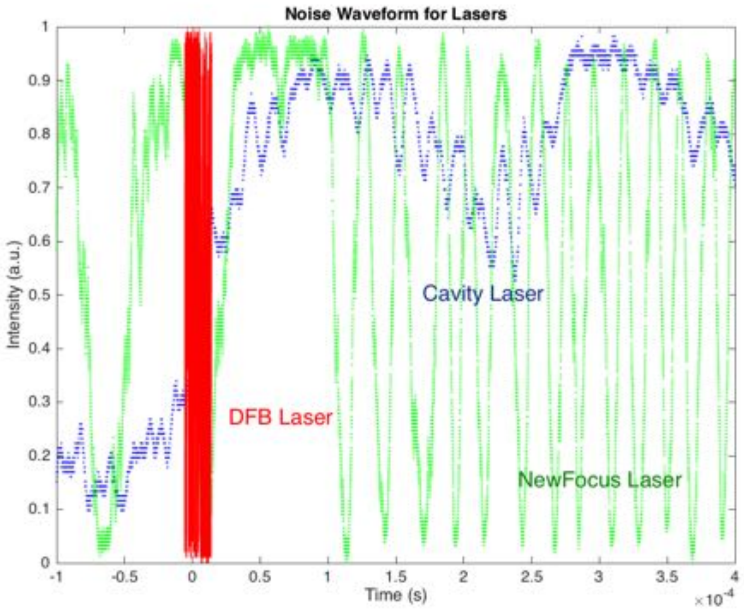
Fiber length difference (A/B)

MDI-QKD (as comparison) Two photon interference, do not require phase interference, only requires time coincidence and wavelengths from the sources are the same.

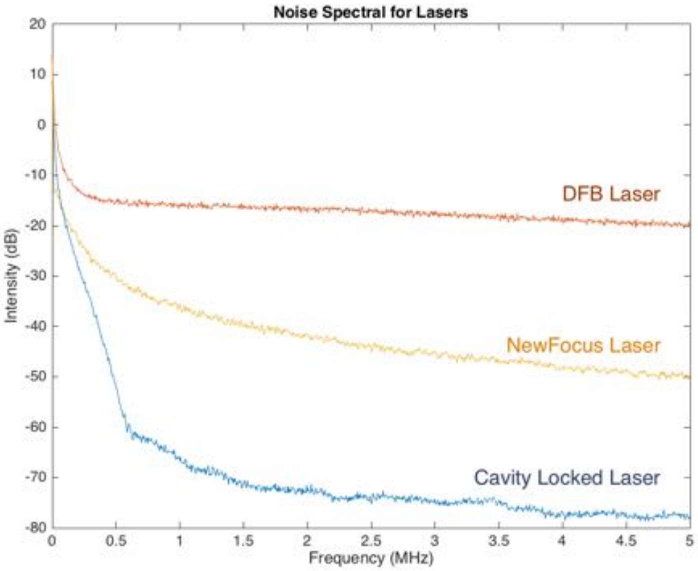
  - Stabilizing source wavelength
    - A/B uses narrow bandwidth lasers (<kHz)
    - A/B locks the laser wavelength with each other
  - Stabilizing fiber phase fluctuation
    - A/B Stabilize the phase within the statistical period

Laser source stability

- The interference result of single laser source
  - The wavelength stability compared with different lasers
    - With one single source passes a 20 km arm unbalanced interferometer
  - Limits the time period phase is stable



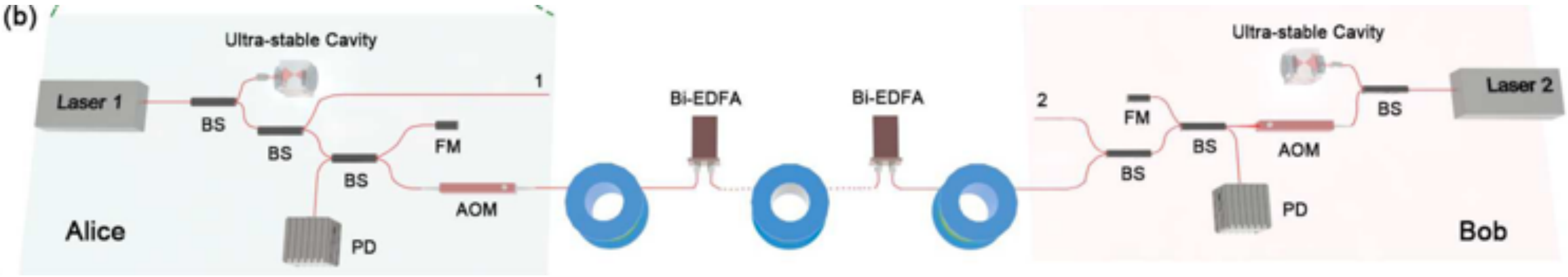
Interference result



Noise spectrom

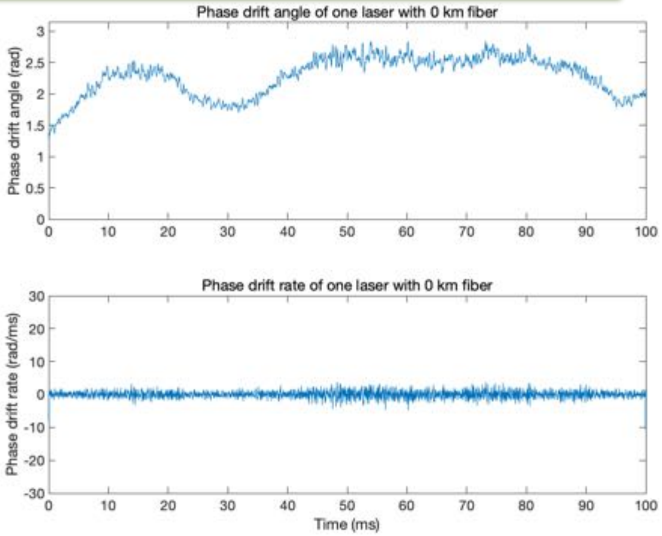
Laser sources

- Continuous wave laser sources (< 1 Hz linewidth)
  - Alice internally locks to her cavity at 1550.0465 nm
  - Bob locks to his cavity at 1550.0474 nm with PDH
  - Relative frequency drift ~0.1 Hz/s (freq. diff. ~112 MHz)
- Wavelength locking through 500 km fiber (9 EDFAs)
  - B compensate source phase difference with AOM (~100 Hz)
  - A compensate fiber phase fluctuation with AOM (~50 Hz)
  - Bi-EDFA gain is set to ~11 dB to control the signal intensity below the threshold for Stimulated Brillouin Scattering (SBS)

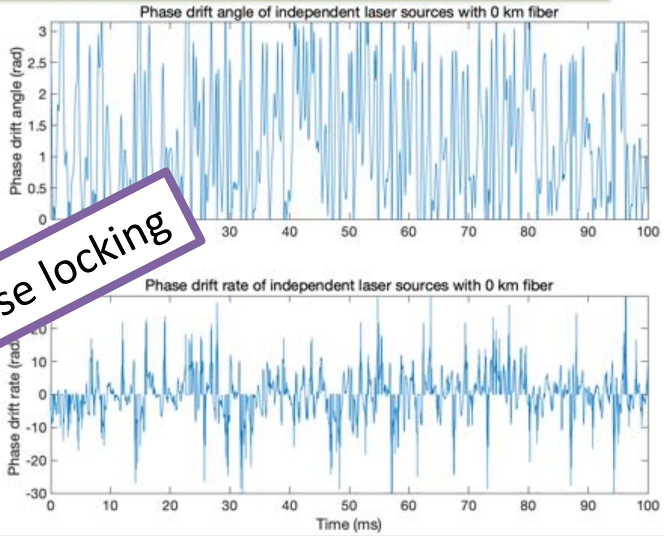


Phase fluctuation by fiber fluctuation

Single source, 0 km: 1.0 rad/ms

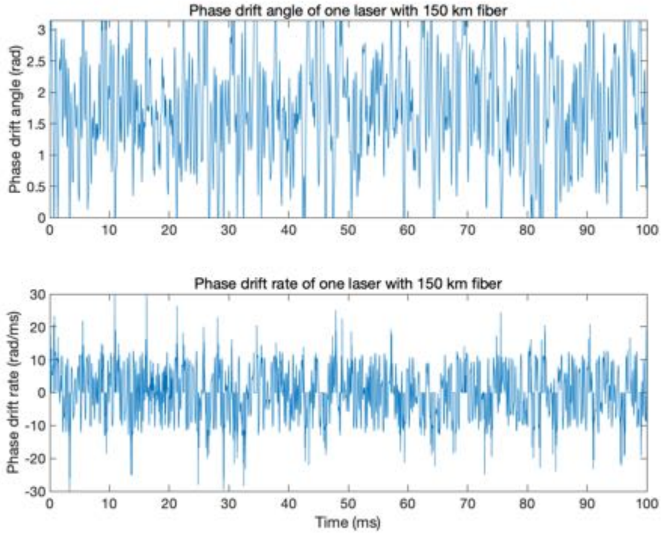


Two sources, 0 km: 5.8 rad/ms

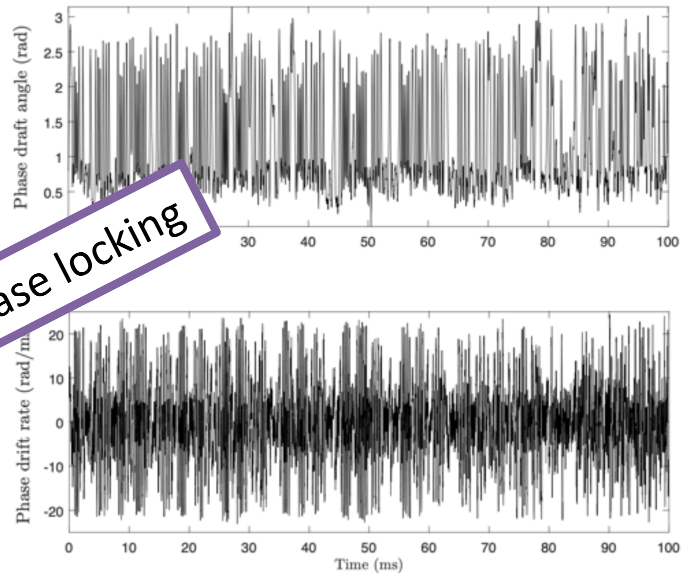


phase locking

Single source, 75 km x 2: 7.1 rad/ms



Independent lasers, 509 km: 9.6 rad/ms



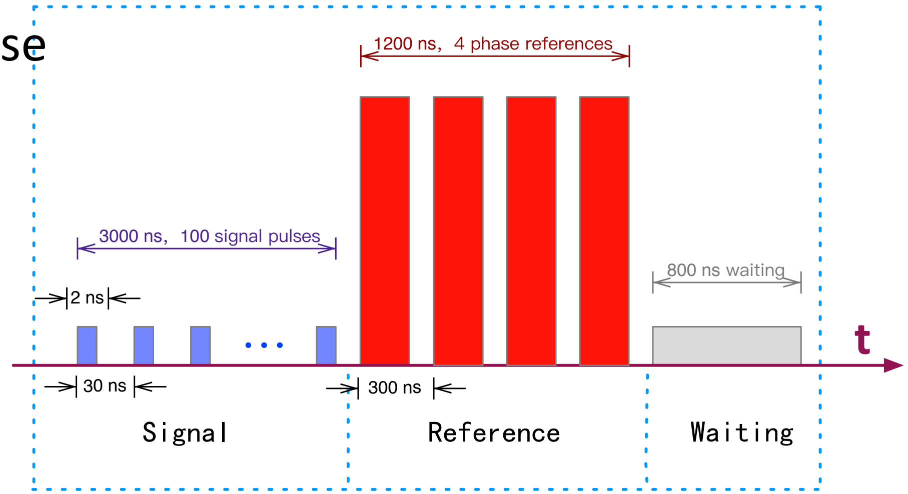
phase locking

Compensating fiber phase drift

Estimate fiber phase with reference pulse

Assume phase is stable within 10 μs

(Based on measure rate 7.5 rad/ms)



- Interference relates to phase difference:

$$\mathrm{I}(\phi) = 4\cos^2(\phi/2)$$

- By sending phase sequences in ref:

$$\theta_A - \theta_B = \{0, \pi/2, \pi, 3\pi/2\}$$

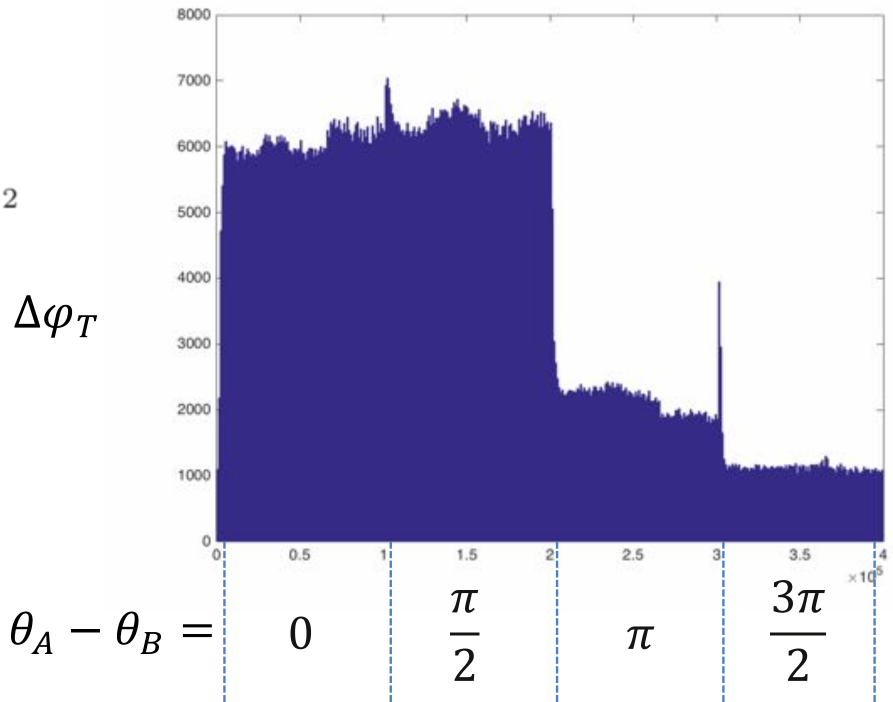
- Consider the relative phase in fiber:

$$\phi = \theta_A - \theta_B + \Delta\varphi_T$$

- We establish error model:

$$Err(\Delta\varphi_T) = \sum_i [p_i - p_{Ti}(\Delta\varphi_T)]^2$$

- Minimizing error to get relative phase $\Delta\varphi_T$



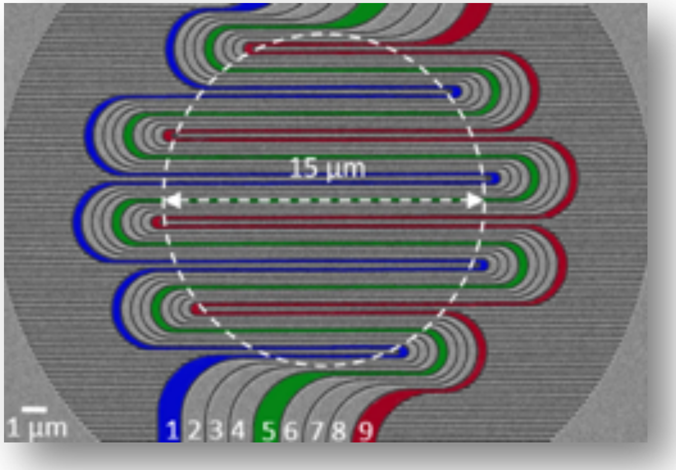
Requirements of Reference Pulse

1. Wavelength: $\lambda_{Ref} = \lambda_{Sig}$
2. Reference travel the same path as signal
3. Reference intensity should be high (~2MHz detection) for quick estimation

superconducting nanowire SPD (SNSPD)

- Higher Counting rate
  - For fast phase compensation with reference pulses
  - Parallel configuration → reduces kinetic inductance → reduce recovery time
  - 50 Ohm shunt resistor → prevent the detector latching at high count rates
  - Achieves 10 Mhz with continuous light test (>3MHz that is required)

- Lower Dark count for Signal
  - For long distance distribution. QBER-Z is ultra-sensitive to noise.
  - Integrating a filter onto the end face of the coupling fiber → reduce dark count and the insertion loss
  - active area of 16 µm in diameter
  - System efficiency 56% and 58%
  - Dark count ~3.5 Hz



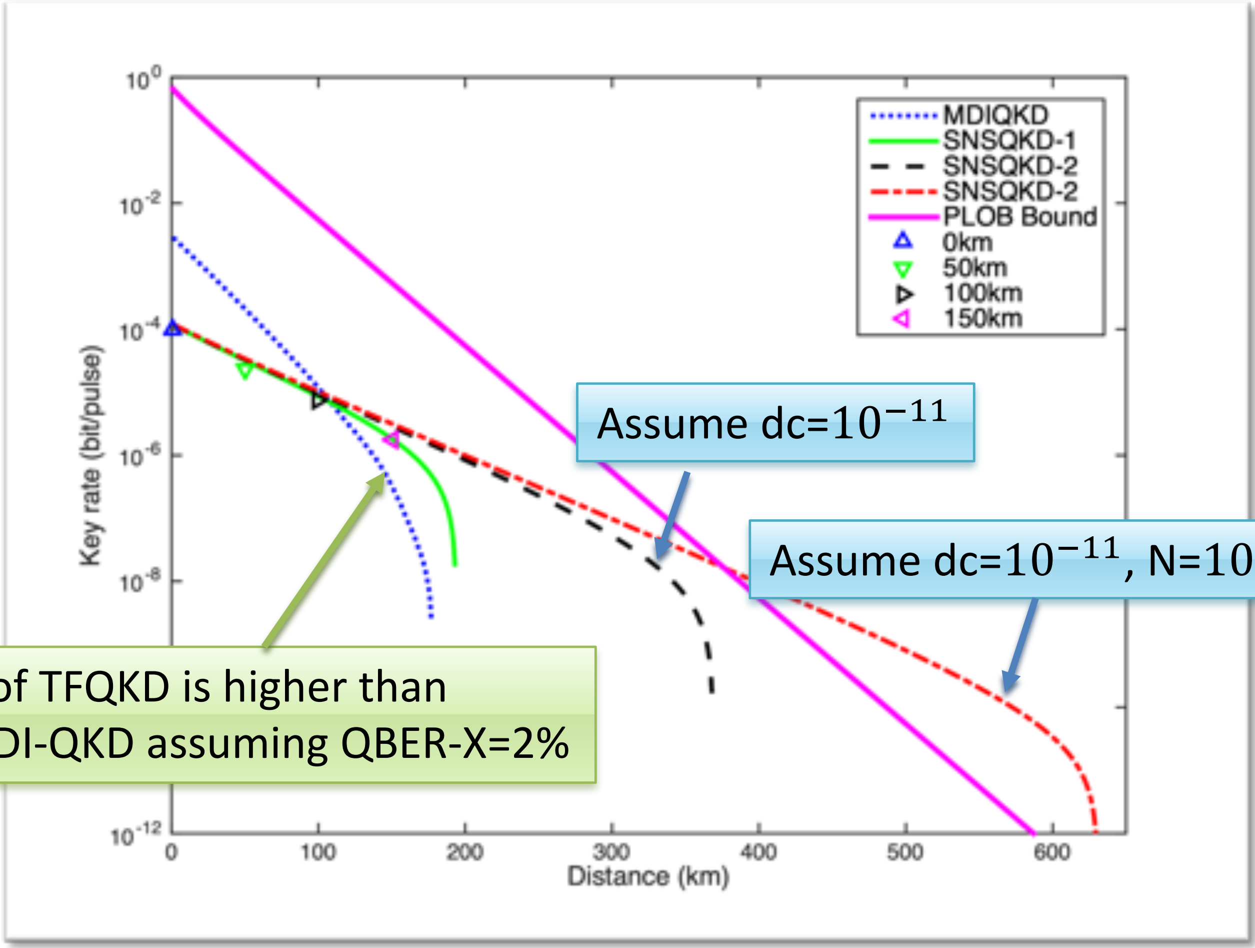
SNS-TF-QKD experimental results

Parameters (that in common)

Fiber (Signal)	Fiber spools without stabilization
Fiber (locking)	Same or longer than signal fiber
System frequency	30 ns signal interval 3 µs for signal, 2 µs for phase estimation
Phase estimation	Collect phase estimation data in 10 µs
Fiber drift	<10 rad/ms (up to 509 km)
Failure probability	$\epsilon = 10^{-10}$ (considering finite size effect and statistical fluctuation)

Experiment I: proof of principle

- SNSPD efficiency: 75.3%/76.6%, dark count: ~1000 Hz (10^{-6} per ns)
- Total pulses sent = 7.2×10^{11} (about 10 hours)
- Valid detections are:
  $0\ km{:}\ \ 6.5\times10^{9}, 50\ km{:}\, 2.3\times10^{9}, 100\ km{:}\ \ 7.6\times10^{8}, 150\ km{:}\ \ 2.5\times10^{8}$



Assume dc=10^{-11}

Assume dc=10^{-11}, N=10^{14}

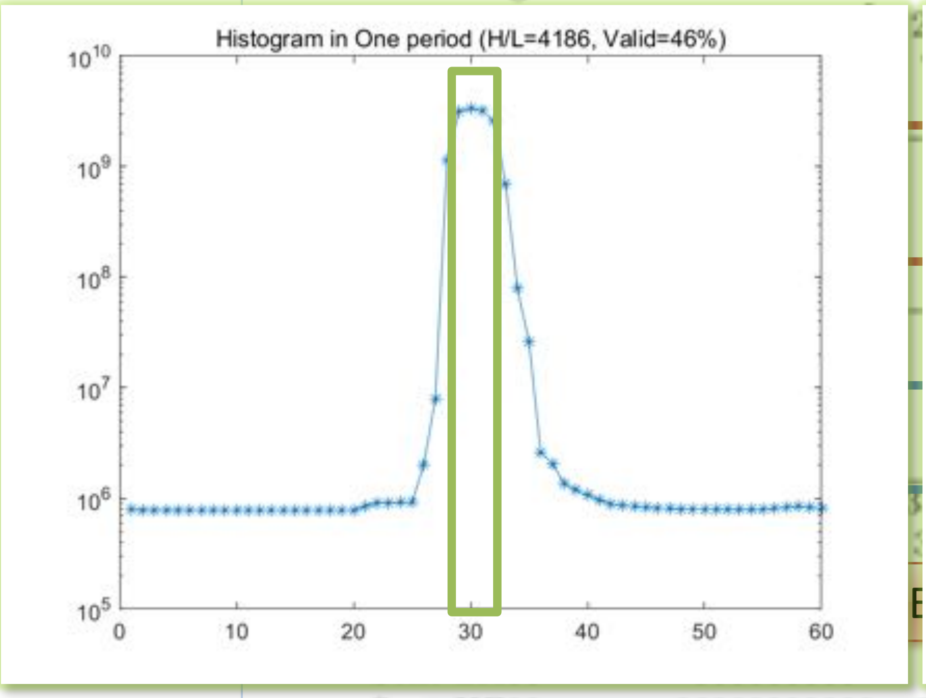
R of TFQKD is higher than MDI-QKD assuming QBER-X=2%

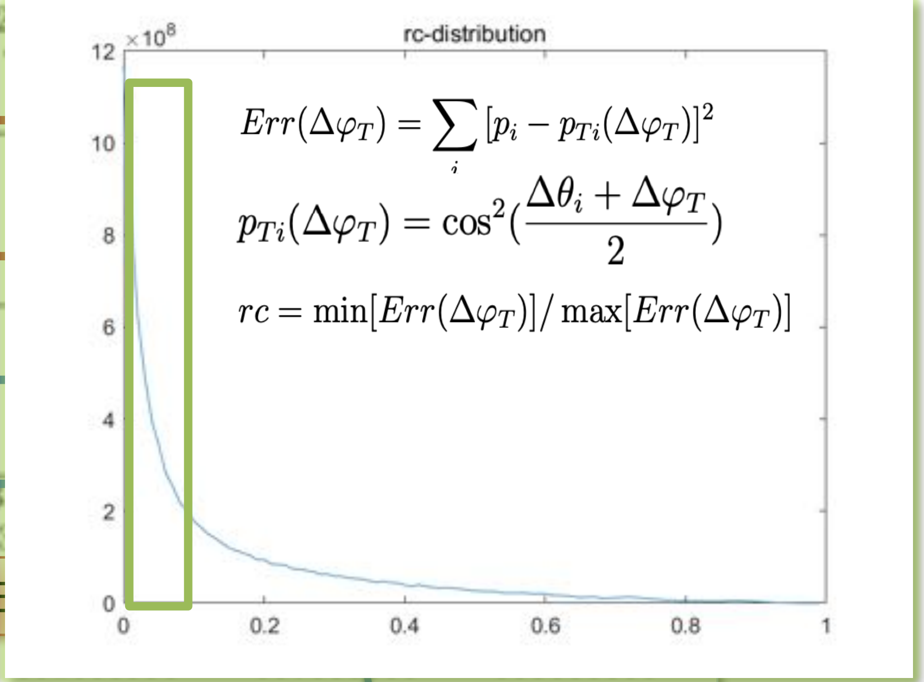
Physical Review Letters **123**, 100505 (2019).

Experiment I: proof of principle

- SNSPD efficiency: 75.3%/76.6%, dark count: ~1000 Hz (10^{-6} per ns)
- Total pulses sent = 7.2×10^{11} (about 10 hours)
- Valid detections are:
  $0\ km$: 6.5×10^{9}, $50\ km$: 2.3×10^{9}, $100\ km$: 7.6×10^{8}, $150\ km$: 2.5×10^{8}

Fiber Length	0 km	50 km	100 km	150 km
Sen				74400000
Sen				15200000
Sent-XZ20	369252000000	369586000000	369860000000	369988000000
Sent-XZ03	826800000	833000000	864200000	838800000
Sent-XX00	40342000000	40598000000	40068000000	40030000000
Sent-XX01	8159800000	8127400000	8009600000	8139000000





$$Err(\Delta\varphi_T) = \sum_i [p_i - p_{Ti}(\Delta\varphi_T)]^2$$

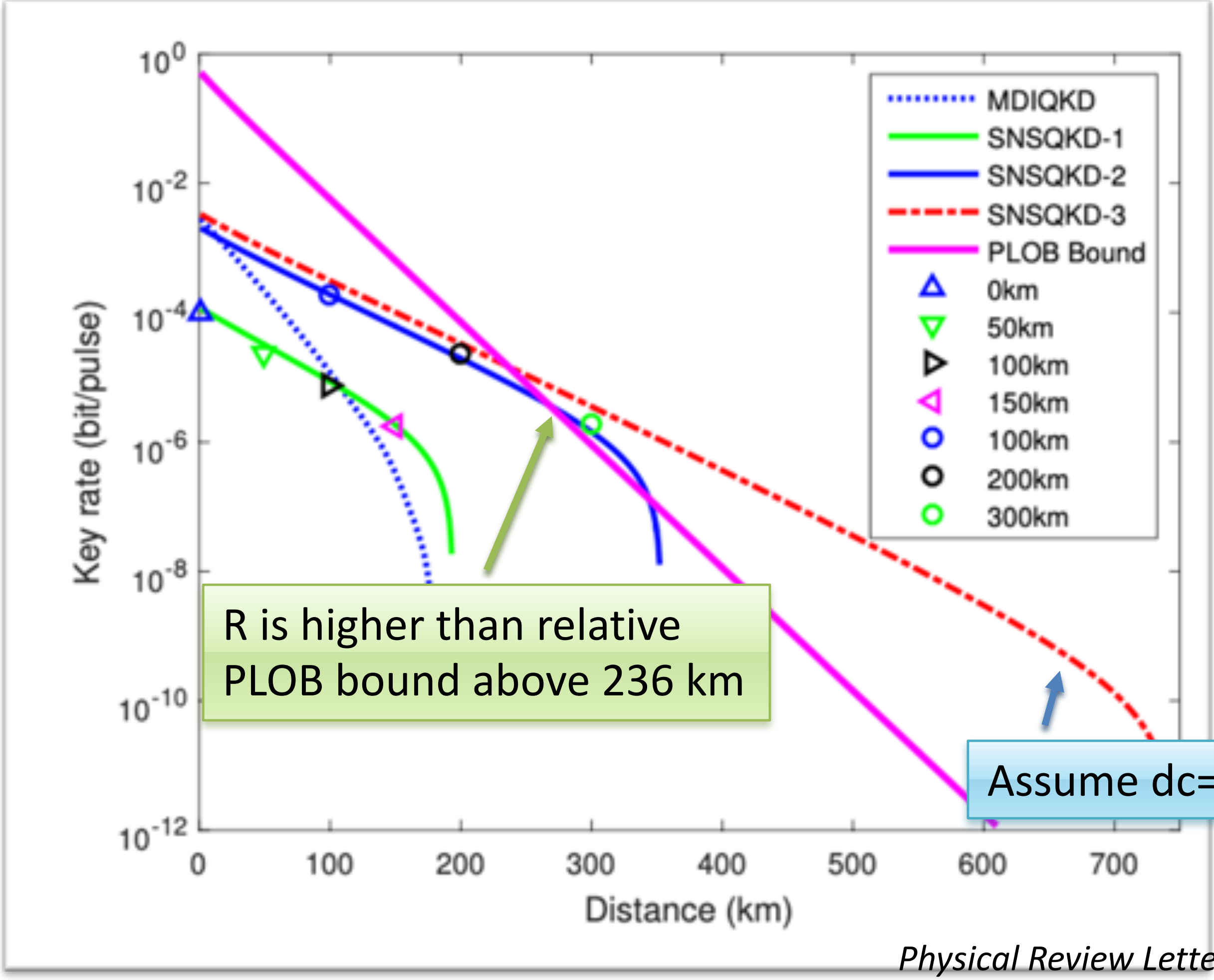
$$p_{Ti}(\Delta\varphi_T) = \cos^2(\frac{\Delta\theta_i + \Delta\varphi_T}{2})$$

$$rc = \min[Err(\Delta\varphi_T)]/\max[Err(\Delta\varphi_T)]$$

Filtering pulses and phase help to decrease errors.

Experiment II: higher than relative PLOB

- SNSPD efficiency: 58%/38%, dark count: ~100 Hz (10^{-7} per ns)
- Total pulses sent = 7.2×10^{11} (about 10 hours)
- Valid detections $100\ km$: 1.7×10^{9}, $200\ km$: 1.9×10^{8}, $300\ km$: 2.4×10^{7}
- Decreasing QBER-X with the updated system



R is higher than relative PLOB bound above 236 km

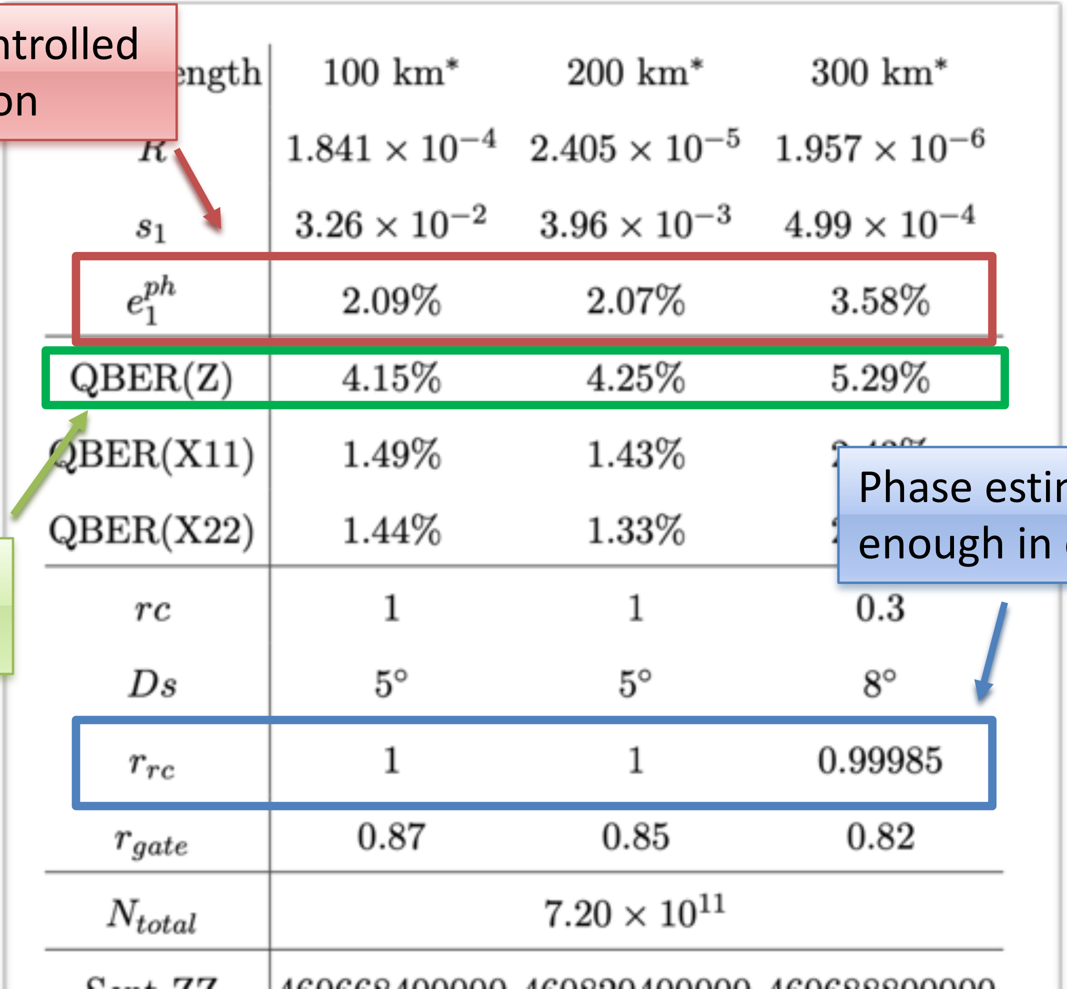
Assume dc=10^{-11}, N=10^{14}

Physical Review Letters **123**, 100505 (2019).

Experiment II: higher than relative PLOB

- SNSPD efficiency: 58%/38%, dark count: ~100 Hz (10^{-7} per ns)
- Total pulses sent = 7.2×10^{11} (about 10 hours)
- Valid detections $100\ km\colon\ 1.7\times10^{9}, 200\ km\colon\ 1.9\times10^{8}, 300\ km\colon\ 2.4\times10^{7}$
- Decreasing QBER-X with the updated system

Phase error can be controlled under realistic condition



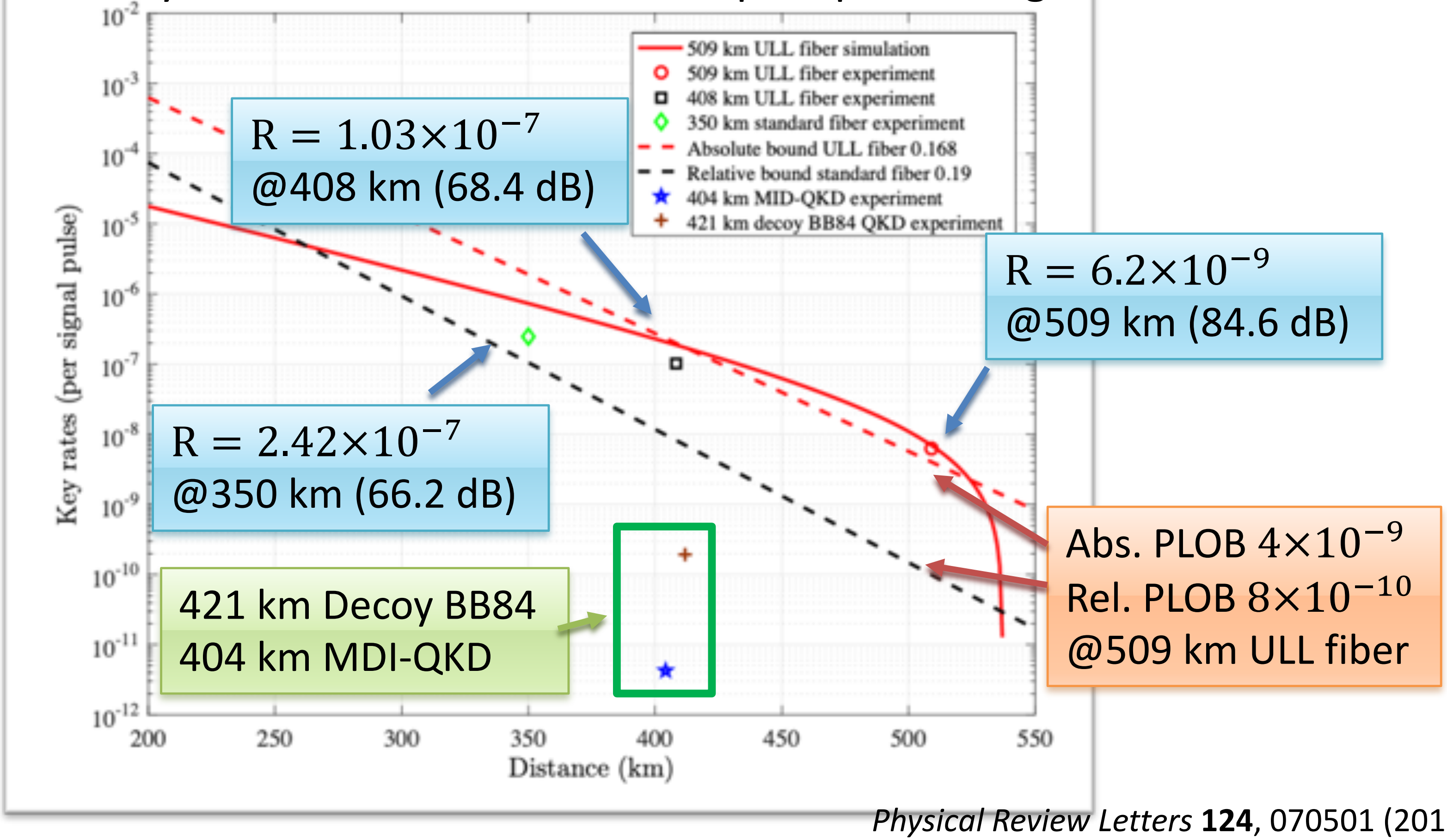
ength	100 km*	200 km*	300 km*
R	1.841×10^{-4}	2.405×10^{-5}	1.957×10^{-6}
s_1	3.26×10^{-2}	3.96×10^{-3}	4.99×10^{-4}
e_1^{ph}	2.09%	2.07%	3.58%
QBER(Z)	4.15%	4.25%	5.29%
QBER(X11)	1.49%	1.43%	[illegible]
QBER(X22)	1.44%	1.33%	[illegible]
rc	1	1	0.3
Ds	5°	5°	8°
r_{rc}	1	1	0.99985
r_{gate}	0.87	0.85	0.82
N_{total}	7.20×10^{11}		
Sent ZZ	460668400000	460820400000	460688800000

QBER-Z is optimized
QBER v.s. detections

Phase estimation is good enough in experiment

Experiment III: higher than absolute PLOB

- SNSPD efficiency: 58%/56%, dark count: ~3.5 Hz (3.5×10^{-9} per ns)
- Total pulses sent 350 km: 2.1×10^{11}, 408 km: 3.5×10^{11}, 509 km: 1.1×10^{12}
- Valid detections 350 km: 2.0×10^{6}, 408 km: 2.6×10^{6}, 509 km: 9.0×10^{5}
- Using Ultra-Low-Loss fiber in 509 km (84.6 dB) experiment
- Using two-way classical communication in post processing



$R = 1.03\times10^{-7}$
@408 km (68.4 dB)

$R = 6.2\times10^{-9}$
@509 km (84.6 dB)

$R = 2.42\times10^{-7}$
@350 km (66.2 dB)

421 km Decoy BB84
404 km MDI-QKD

Abs. PLOB 4×10^{-9}
Rel. PLOB 8×10^{-10}
@509 km ULL fiber

Physical Review Letters **124**, 070501 (2019).

Re-Rayleigh Scattering Noise in Fiber

When reference appears

- Rayleigh scattering (elastic scattering) in fiber
  - The intensity is proportional to the input power $P_L = P_0 e^{-\alpha L}$

$$dP_B = dP_{B'} e^{-\alpha L} = P_L S e^{-\alpha L} dL = P_0 S e^{-2\alpha L} dL$$

  - Total reflected power $P_B = \int_0^L dP_B = \frac{P_0 S}{2\alpha}(1 - e^{-2\alpha L})$

In all time period

- Back Scattered light is again back scattered (Re-Rayleigh Scattering)

$$dP_{Sl} = P_0 S^2 e^{-\alpha L} e^{-\alpha(L-L')} e^{-\alpha(l-L')} dL dL'$$

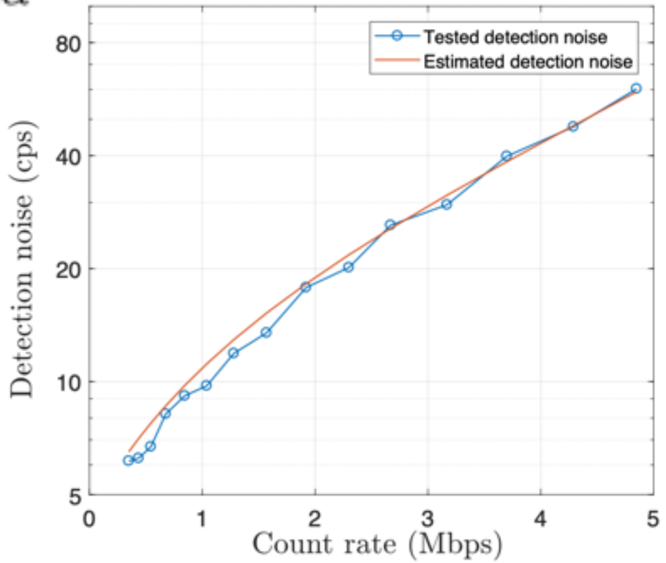
  - With random polarization, the total power is

$$P_{srs} = \frac{1}{2} P_{Sl} = \frac{P_0 S^2}{4\alpha} e^{-\alpha l}[l + \frac{e^{-2\alpha l}}{2\alpha} - \frac{1}{2\alpha}]$$

α = −0.168dB/km
S = 3.919×10^{-5}
Ref = 2MHz (12.65 nW)
Noise ≈ 8.6cps (@500km)

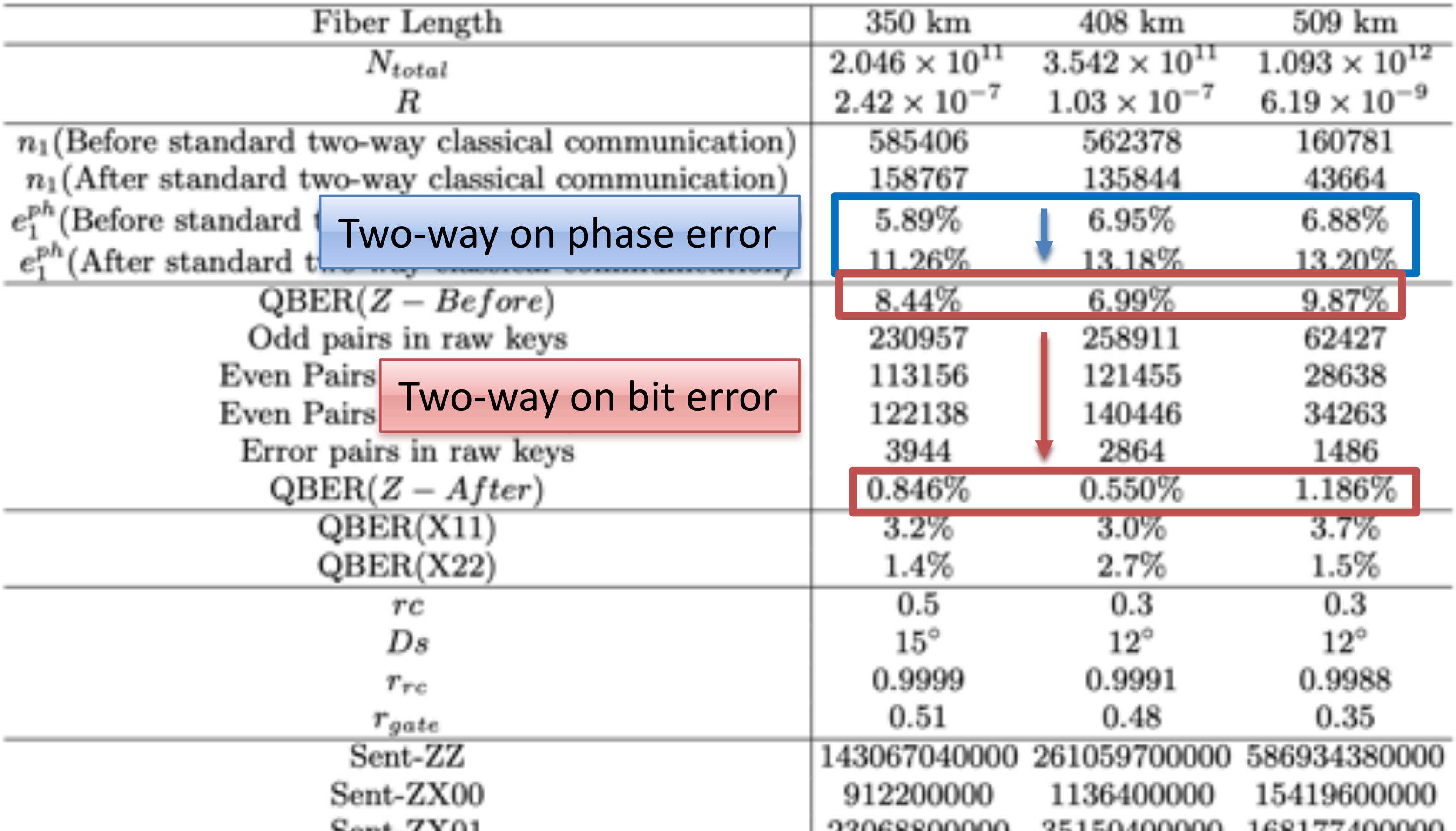
(a) Rayleigh scattering in optical fiber

(b) Re-Rayleigh scattering in optical fiber



Experiment III: higher than absolute PLOB

- SNSPD efficiency: 58%/56%, dark count: ~3.5 Hz (3.5×10^{-9} per ns)
- Total pulses sent 350 km: 2.1×10^{11}, 408 km: 3.5×10^{11}, 509 km: 1.1×10^{12}
- Valid detections 350 km: 2.0×10^{6}, 408 km: 2.6×10^{6}, 509 km: 9.0×10^{5}
- Using Ultra-Low-Loss fiber in 509 km (84.6 dB) experiment
- Using two-way classical communication in post processing



Fiber Length	350 km	408 km	509 km
N_{total}	2.046×10^{11}	3.542×10^{11}	1.093×10^{12}
R	2.42×10^{-7}	1.03×10^{-7}	6.19×10^{-9}
n_1(Before standard two-way classical communication)	585406	562378	160781
n_1(After standard two-way classical communication)	158767	135844	43664
e_1^{ph}(Before standard	5.89%	6.95%	6.88%
e_1^{ph}(After standard t	11.26%	13.18%	13.20%
QBER($Z-Before$)	8.44%	6.99%	9.87%
Odd pairs in raw keys	230957	258911	62427
Even Pairs	113156	121455	28638
Even Pairs	122138	140446	34263
Error pairs in raw keys	3944	2864	1486
QBER($Z-After$)	0.846%	0.550%	1.186%
QBER(X11)	3.2%	3.0%	3.7%
QBER(X22)	1.4%	2.7%	1.5%
rc	0.5	0.3	0.3
Ds	15°	12°	12°
r_{rc}	0.9999	0.9991	0.9988
r_{gate}	0.51	0.48	0.35
Sent-ZZ	143067040000	261059700000	586934380000
Sent-ZX00	912200000	1136400000	15419600000
Sent-ZX01	[illegible]	[illegible]	[illegible]

Two-way on phase error

Two-way on bit error

Two-way communication

Type	C0	C1	D	V
Alice	0	1	1	0
Bob	1	0	1	0

e.g. 2 bits	VV	C0C1	C1D	DV	…
Alice	00	01	11	10	…
Bob	00	10	01	10	…

PRA 66, 060302 (2002).
arXiv:1904.06331 (2019).
PRA 101, 042330 (2020).

Type	CC	VV	DD	~~CV~~	~~VC~~	~~CD~~	~~DC~~	VD	DV
Parity A	0	0	0	0	0	1	1	1	1
Parity B	0	0	0	1	1	0	0	1	1

Assume C=C0, parity checking (A=B?) is the same for other C

Type	C0C0	C0C1	C1C0	C1C1	VV	DD	VD	DV
Parity B	0	1	1	0	0	0	1	1
Correct	○	○	○	○	✕	✕	✕	✕

bit-flip error rate reduced dramatically after BFER

Standard two-way classical communication (for phase error) $\tilde{e}_1^{ph} = 2e_1^{ph}(1\text{-}\ e_1^{ph})$

$$N_f = \tilde{n}_1[1-H(\tilde{e}_1^{\mathrm{ph}})]-f[n_{t1}H(E_1)+n_{t2}H(E_2)+n_{t3}H(E_3)].$$

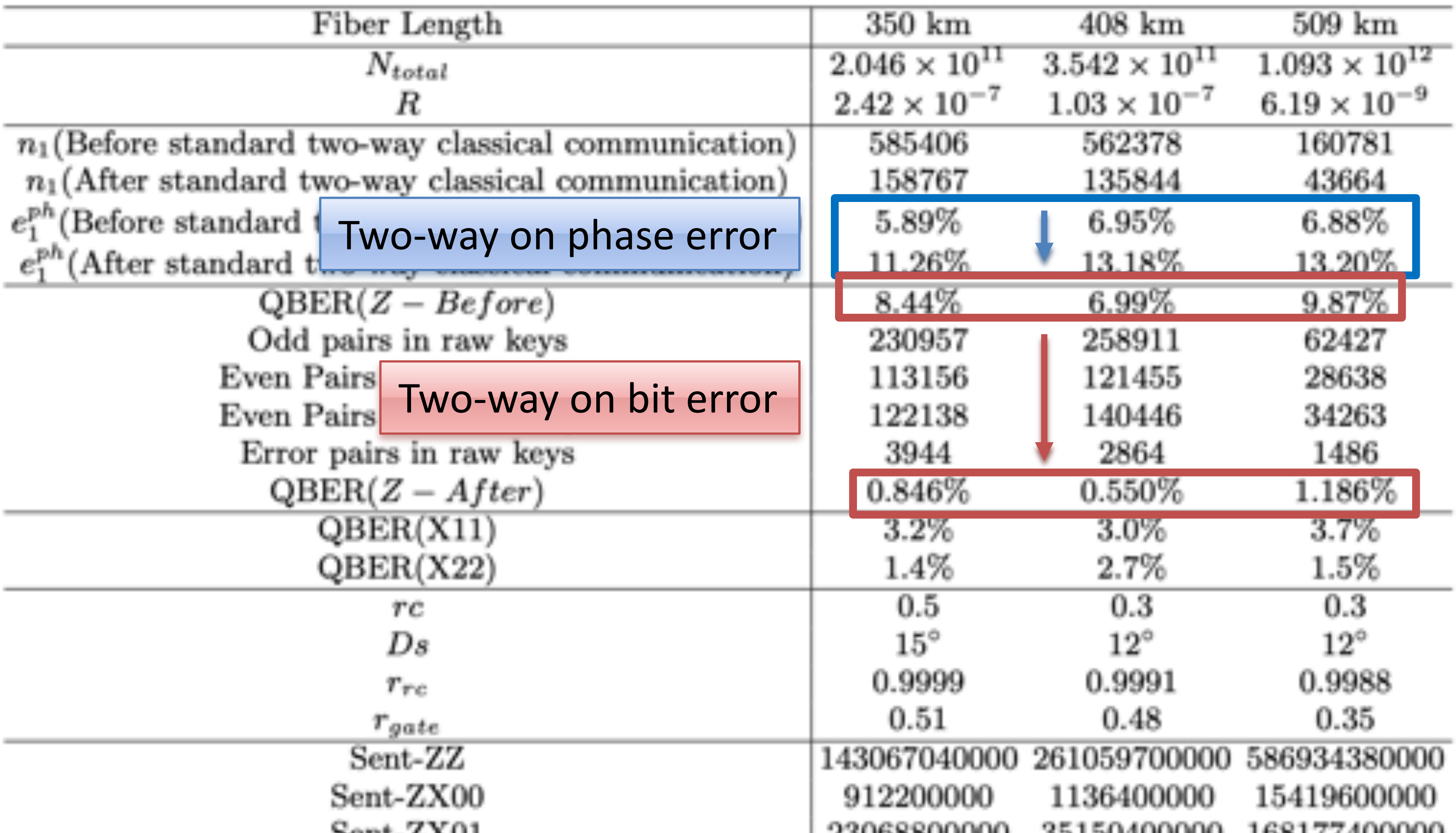
Odd Parity Sifting

Actively Odd Parity Sifting (AOPP)

Bit-flip error is concentrated on even-parity pairs: Sifting or actively make odd parity pairing in groups, will further reduce the bit flip error.

Experiment III: higher than absolute PLOB

- SNSPD efficiency: 58%/56%, dark count: ~3.5 Hz (3.5×10^{-9} per ns)
- Total pulses sent 350 km: 2.1×10^{11}, 408 km: 3.5×10^{11}, 509 km: 1.1×10^{12}
- Valid detections 350 km: 2.0×10^{6}, 408 km: 2.6×10^{6}, 509 km: 9.0×10^{5}
- Using Ultra-Low-Loss fiber in 509 km (84.6 dB) experiment
- Using two-way classical communication in post processing



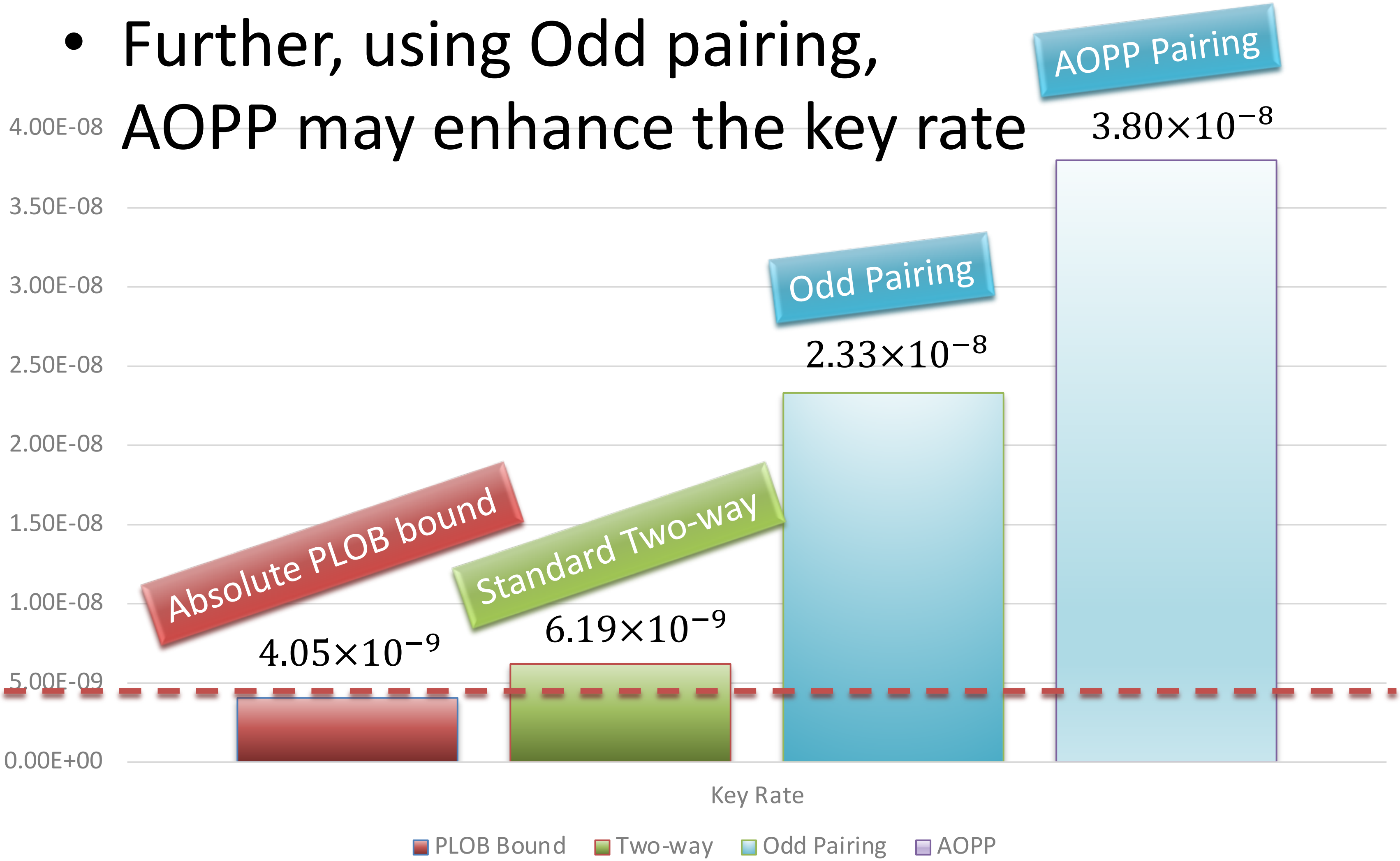
Fiber Length	350 km	408 km	509 km
N_{total}	2.046×10^{11}	3.542×10^{11}	1.093×10^{12}
R	2.42×10^{-7}	1.03×10^{-7}	6.19×10^{-9}
n_1(Before standard two-way classical communication)	585406	562378	160781
n_1(After standard two-way classical communication)	158767	135844	43664
e_1^{ph}(Before standard	5.89%	6.95%	6.88%
e_1^{ph}(After standard t	11.26%	13.18%	13.20%
QBER($Z - Before$)	8.44%	6.99%	9.87%
Odd pairs in raw keys	230957	258911	62427
Even Pairs	113156	121455	28638
Even Pairs	122138	140446	34263
Error pairs in raw keys	3944	2864	1486
QBER($Z - After$)	0.846%	0.550%	1.186%
QBER(X11)	3.2%	3.0%	3.7%
QBER(X22)	1.4%	2.7%	1.5%
rc	0.5	0.3	0.3
Ds	15°	12°	12°
r_{rc}	0.9999	0.9991	0.9988
r_{gate}	0.51	0.48	0.35
Sent-ZZ	143067040000	261059700000	586934380000
Sent-ZX00	912200000	1136400000	15419600000
Sent-ZX01	[illegible]	[illegible]	[illegible]

Two-way on phase error

Two-way on bit error

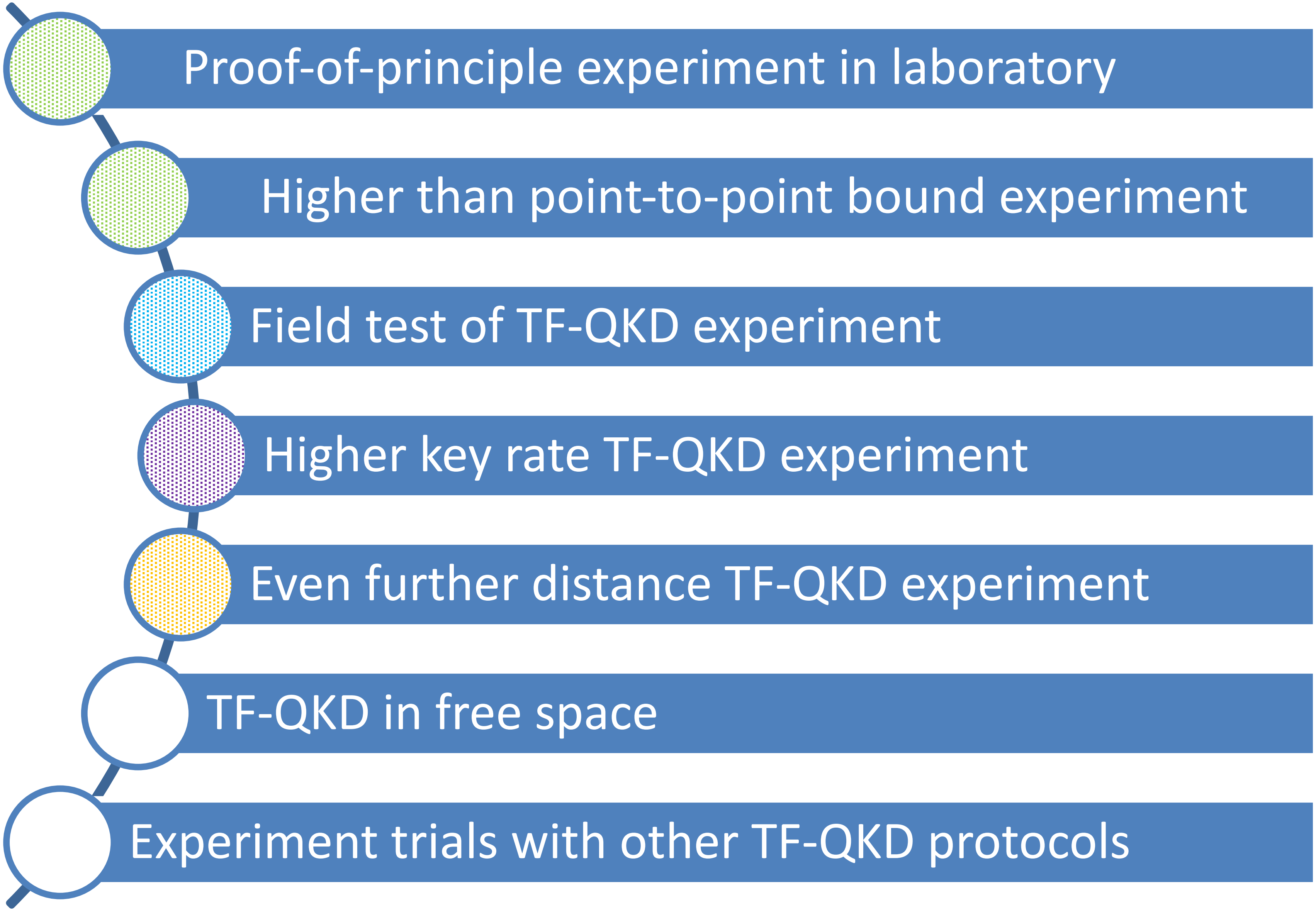
Experiment III: higher than absolute PLOB

- Further, using Odd pairing, AOPP may enhance the key rate



That is what we have for now, and next…

Outlook



- Proof-of-principle experiment in laboratory
- Higher than point-to-point bound experiment
- Field test of TF-QKD experiment
- Higher key rate TF-QKD experiment
- Even further distance TF-QKD experiment
- TF-QKD in free space
- Experiment trials with other TF-QKD protocols

University of Science and Technology of China:
Yang Liu, Jiu-Peng Chen, Chi Zhang, Jian-Yu Guan,
Jin Lin, **Qiang Zhang, Jian-Wei Pan**

Tsinghua University:
Cong Jiang, Xiao-Long Hu, Zong-Wen Yu, Xiang-Bin Wang

Shanghai Institute of Microsystem and Information Technology:
Weijun Zhang, Hai Xu, Hao Li, Lixing You, Zhen Wang

Corning Inc.
Ming-Jun Li, Hao Chen

CHINESE ACADEMY OF SCIENCES

NSFC

National Key R&D Program of China

Anhui Initiative in Quantum Information Technologies

Thank you for listening!