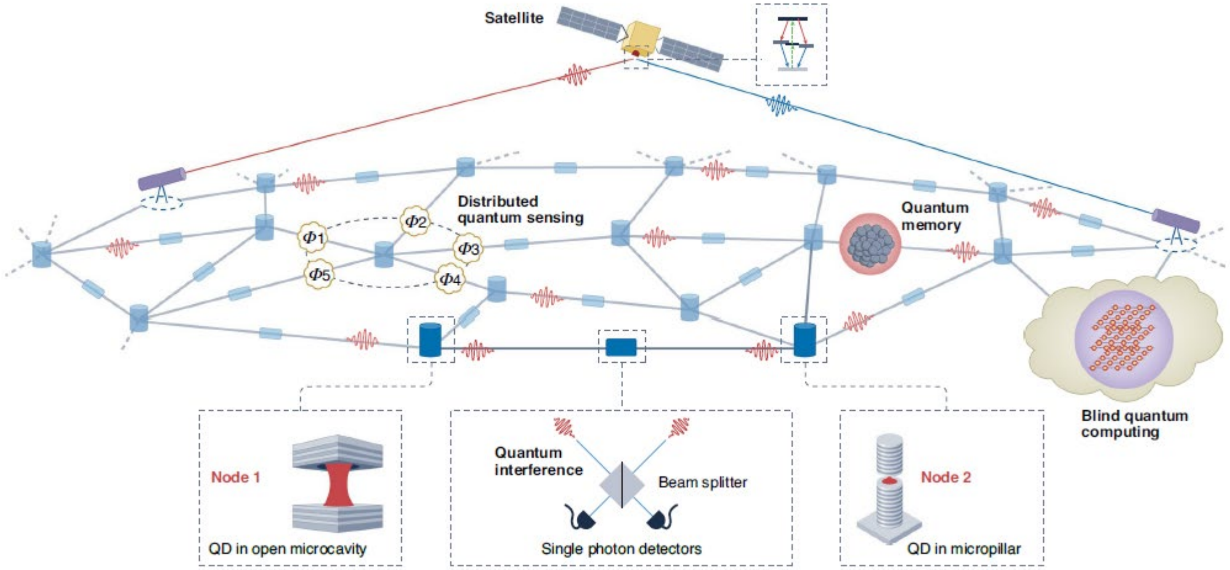
Long Distance Quantum Key Distribution Gets Simpler

Lai Zhou
Beijing Academy of Quantum Information Sciences
2023-08-16

Secure Communication and Quantum Network



Distributed quantum network:
Quantum sensing, distributed quantum computing,
Quantum key distribution (QKD)

Main Components:
- Single photon source
- quantum memory
- Single photon detector
- Fiber, free space channel
- Control system, e.g.,

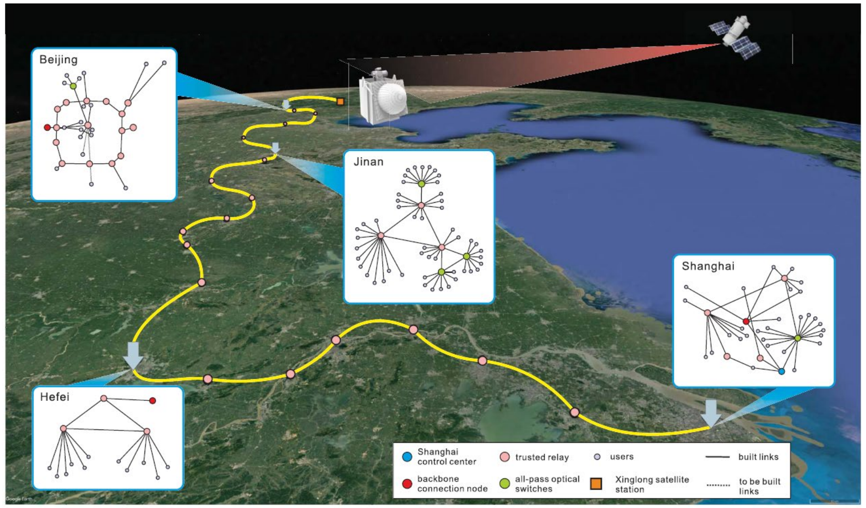
phase, polarization, synchronization, beam tracking

Practical quantum network:
Trusted QKD network

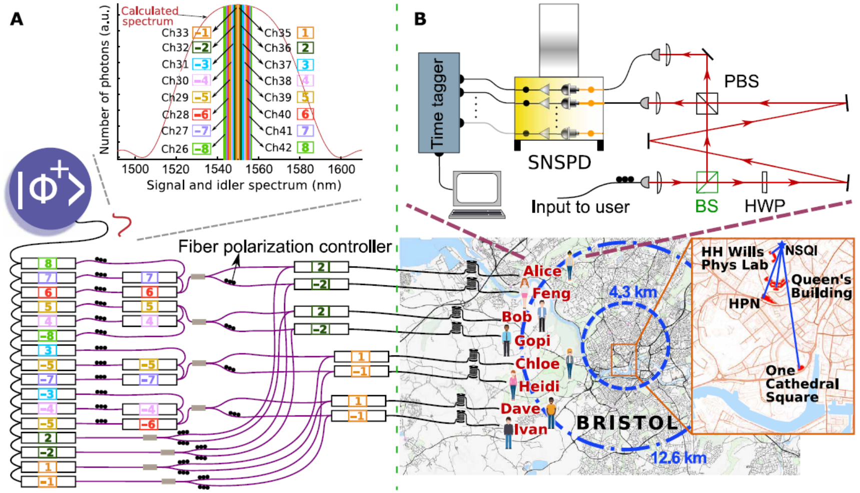
The next stage:
Untrusted QKD network, entanglement QKD network
Quantum repeaters

C. Lu et al., Nature Nanotechnology 16.12 (2021)
S. Wehner et al., Science, 362.6412 (2018)

Secure Communication and Quantum Network



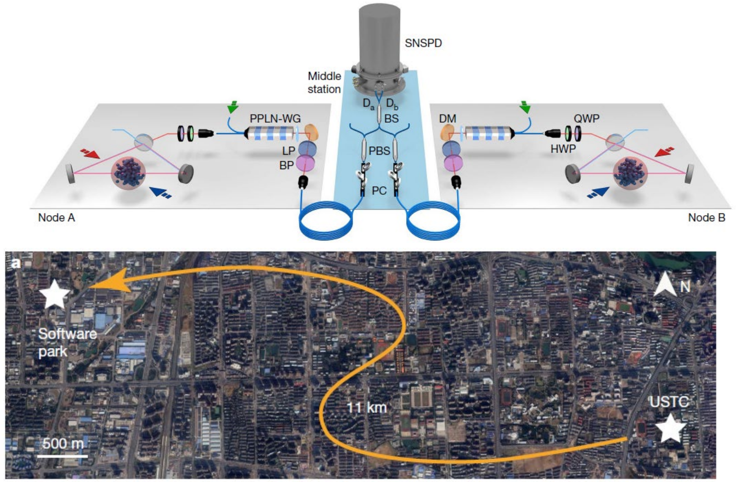
T. Chen et al., Nature 589.214(2021) (China)



S. Joshi et al., Science advance 6.36 (2020) (Bristol, UK)

Security

Distance



Y. Yong et al., Nature 578.7794(2020) (China)

2G

⇧

1G

Network performance update

1) Higher security, untrusted node
2) Longer distance, 300-600km intercity
3) Higher rate, 10Mbps@10km
4) Miniaturization, photonic chip

Application

Practical Candidate:
Twin field QKD

Secure Communication and Quantum Network

BB84

Bennett

IBM, USA

Decoy state attack in source

- Decoy state idea -Hwang
- Decoy state (2005)

-H. K. Lo, X. F. Ma, Toronto

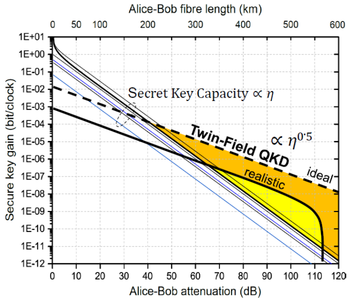
-X. B. Wang, Tsinghua

MDI-QKD attack in detector

H. K. Lo, X. F. Ma

Toronto, Canada

TF-QKD



Toshiba, Cambridge, UK

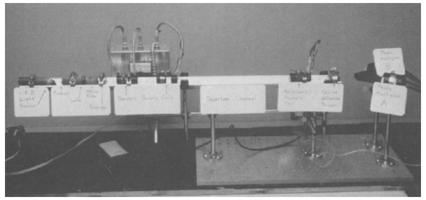
1984 1992 2003 2005 2012 2017 2018 2019

First QKD experiment

- Free space 32 cm

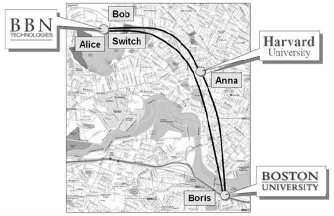
  - Bennett, IBM, USA
- Fiber1 km (1993)

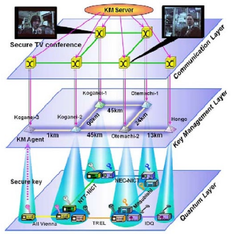
  - Gisin Geneva, Switzerland



Field trial QKD network

- DARPA-QKD, USA
- SECOQC-QKD, Europe (2008)
- Tokyo-QKD, Japan (2010)





Space-QKD：Mozi QKD network：Beijing-Shanghai

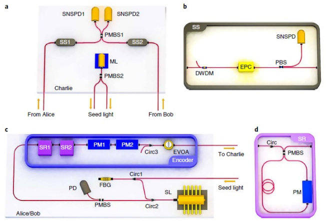
J. W. Pan, USTC

TF-QKD in fiber

- 300 km (2019)

  - Z. F. Han, USTC
- 502 km (2020)

  - J. W. Pan, USTC

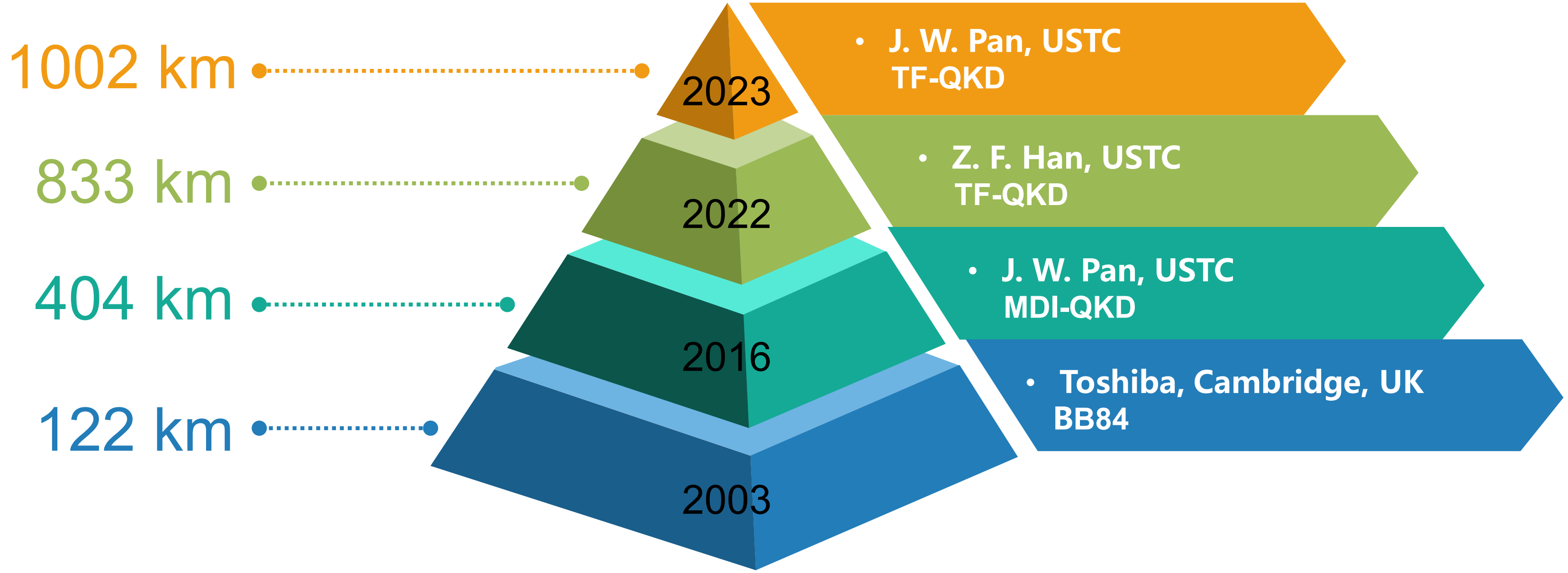


F. H. Xu et al., Reviews of Modern Physics 92 (2), 025002 (2020)

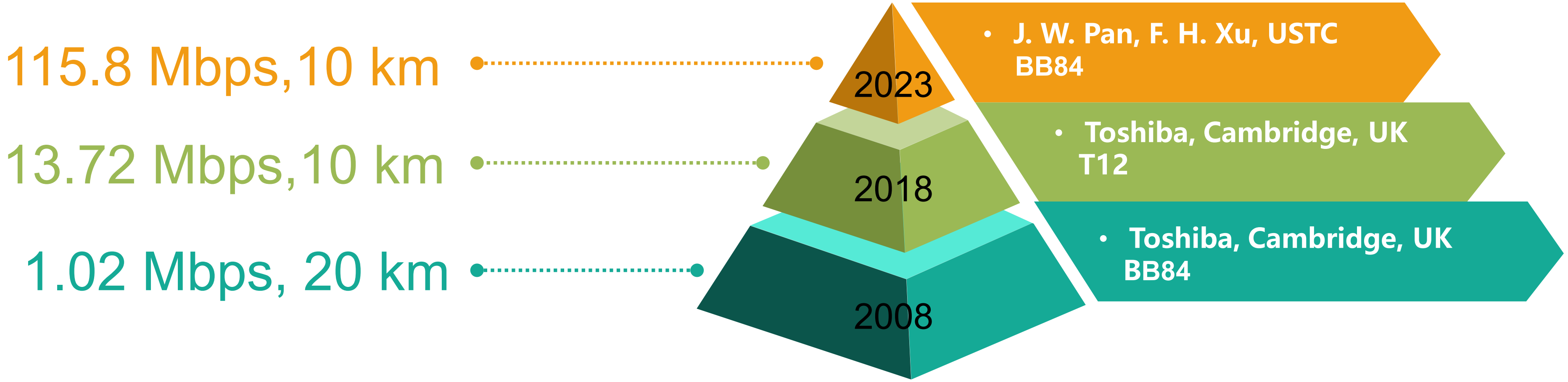
Long Distance Quantum Key Distribution Gets Simpler

Secure Communication and Quantum Network

Distance in fiber



Secure key rate



Long Distance Quantum Key Distribution Gets Simpler

Simpler System with good performance

- Open Twin Field QKD assisted by the coherence frequency comb
- Measurement device independent QKD with post-measurement pairing technique

Physics ABOUT BROWSE PRESS COLLECTIONS Search articles

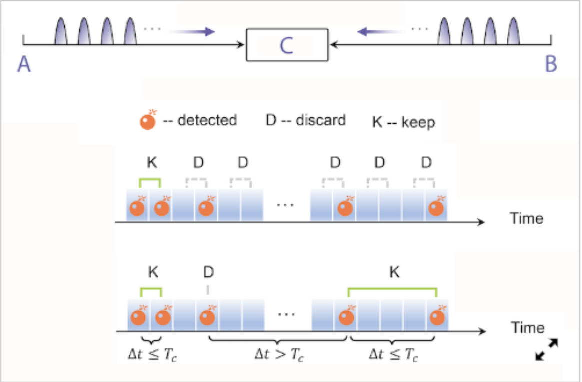
VIEWPOINT

Long-Range Quantum Cryptography Gets Simpler

Marco Avesani
Department of Information Engineering, University of Padua, Padua, Italy

June 20, 2023 • *Physics* 16, 104

A series of demonstrations considerably ease the requirements for implementing quantum cryptography protocols over large distances.



L. Zhou *et al.* [1]

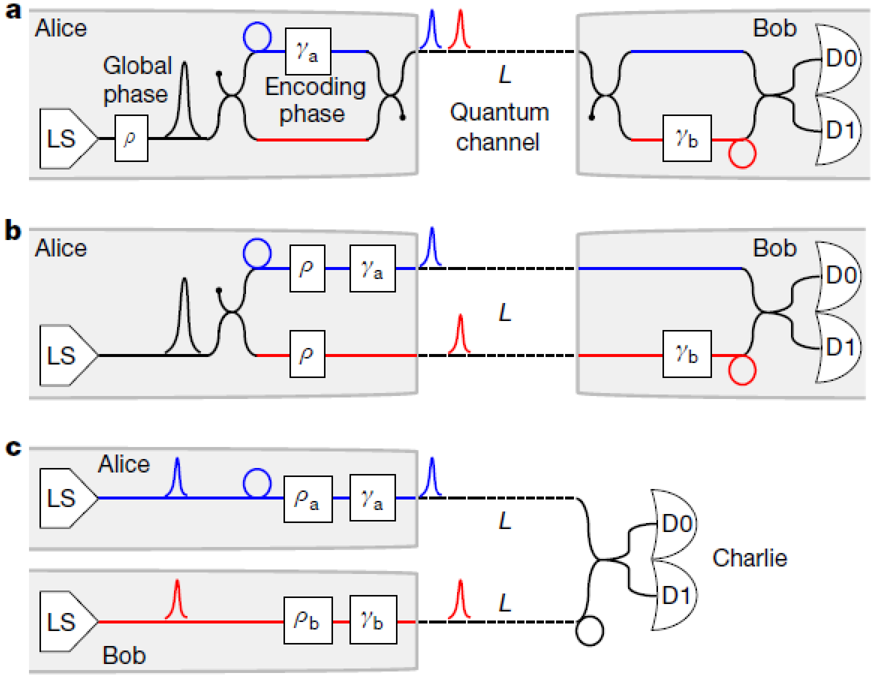
10. L. Zhou *et al.*, "Twin-field quantum key distribution without optical frequency dissemination," **Nat. Commun. 14, 928** (2023).

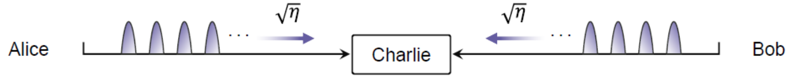
Experimental Quantum Communication Overcomes the Rate-Loss Limit without Global Phase Tracking
Lai Zhou, Jinping Lin, Yuan-Mei Xie, Yu-Shuo Lu, Yumang Jing, Hua-Lei Yin, and Zhiliang Yuan
Phys. Rev. Lett. 130, 250801 (2023)
Published June 20, 2023
Read PDF

Experimental Mode-Pairing Measurement-Device-Independent Quantum Key Distribution without Global Phase Locking
Hao-Tao Zhu, Yizhi Huang, Hui Liu, Pei Zeng, Mi Zou, Yunqi Dai, Shibiao Tang, Hao Li, Lixing You, Zhen Wang, Yu-Ao Chen, Xiongfeng Ma, Teng-Yun Chen, and Jian-Wei Pan
Phys. Rev. Lett. 130, 030801 (2023)
Published January 17, 2023
Read PDF

Twin-Field Quantum Key Distribution without Phase Locking
Wei Li, Likang Zhang, Yichen Lu, Zheng-Ping Li, Cong Jiang, Yang Liu, Jia Huang, Hao Li, Zhen Wang, Xiang-Bin Wang, Qiang Zhang, Lixing You, Feihu Xu, and Jian-Wei Pan
Phys. Rev. Lett. 130, 250802 (2023)
Published June 20, 2023
Read PDF

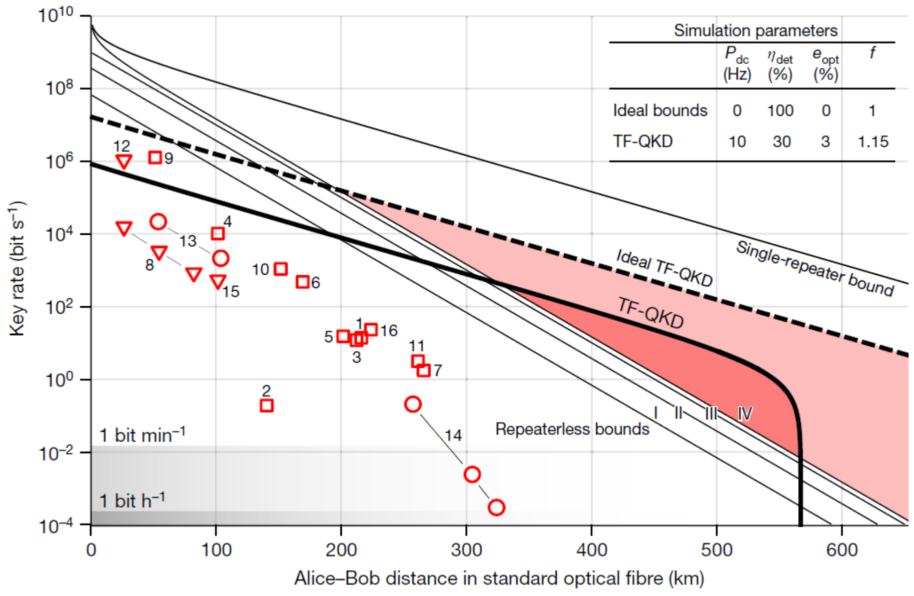
1）Twin Field QKD

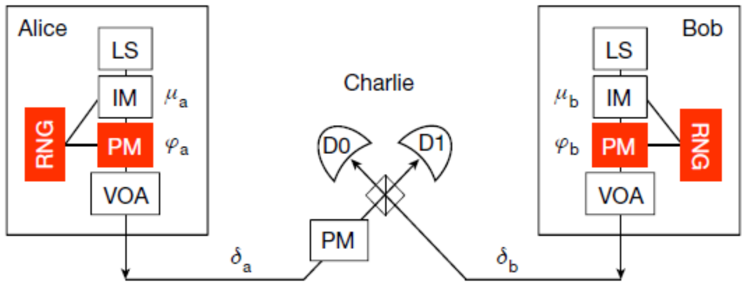


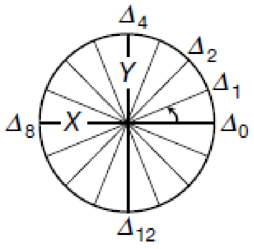


$$SKC = -log_2(1-\sqrt{\eta}) \propto \sqrt{\eta}$$

Overcome the linear rate-transmittance bound





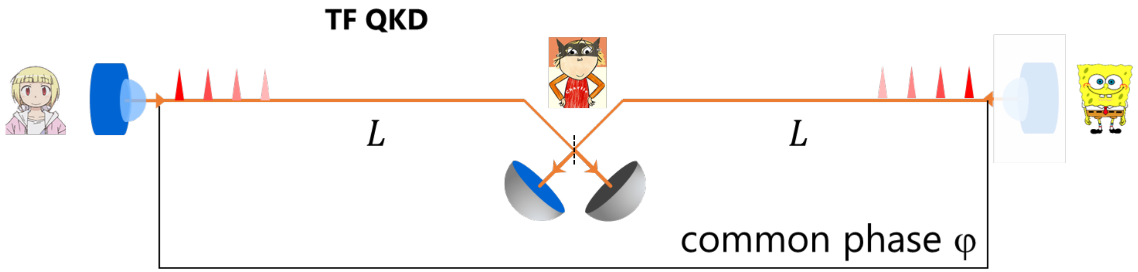


Phase slices

M. Lucamarini et al., Nature 557.7705, (2018).
S. Pirandola et al., Nature Communication 8,15043 (2017).

Long Distance Quantum Key Distribution Gets Simpler

1）Twin Field QKD

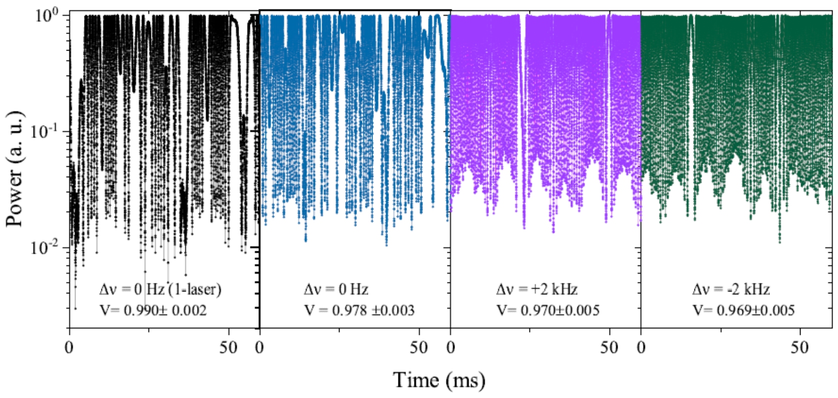


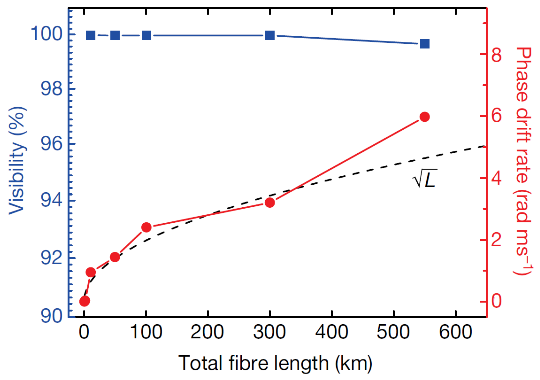
Single photon interference (phase stabilization)

$$\frac{\mathrm{d}\phi}{\mathrm{d}t} = 2\pi\left(\Delta\nu + \frac{\nu}{c}\frac{\mathrm{d}\Delta(nL)}{\mathrm{d}t}\right)$$

Frequency difference between the users' lasers

Fast phase evolution in long fibers



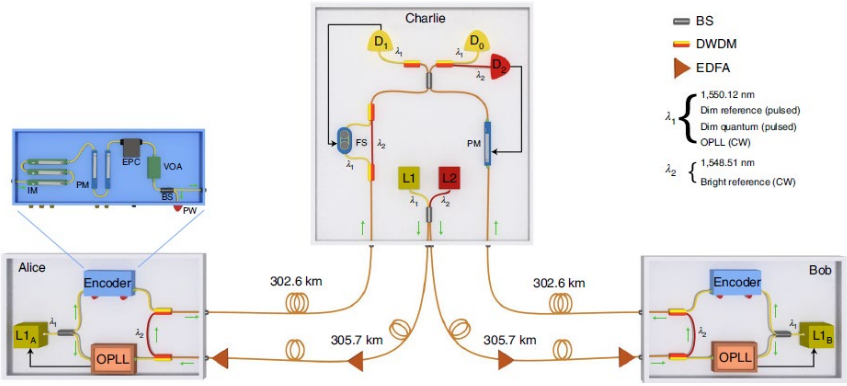


Distance record in recent years:

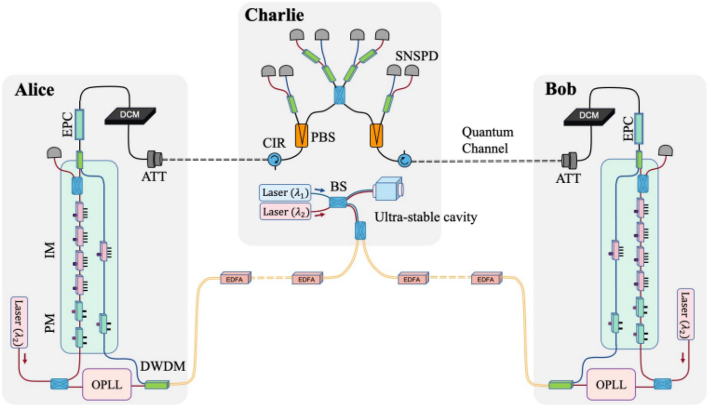
509 km, Phys. Rev. Lett. 124, 070501 (2020).
605 km, Nat. Photonics 15, 530 (2021).
658 km, Phys. Rev. Lett. 128,180502 (2022).
833 km, Nat. Photonics 16, 154 (2022)
1002 km, Phys. Rev. Lett. 130, 210801 (2023)

M. Lucamarini et al., Nature 557.7705, (2018).
S. Pirandola et al., Nature Communication 8,15043 (2017).

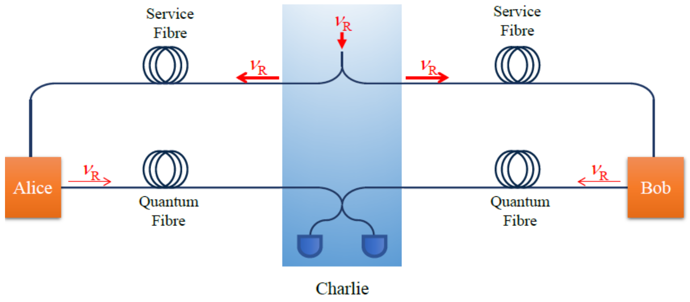
Closed configuration: Twin Field QKD

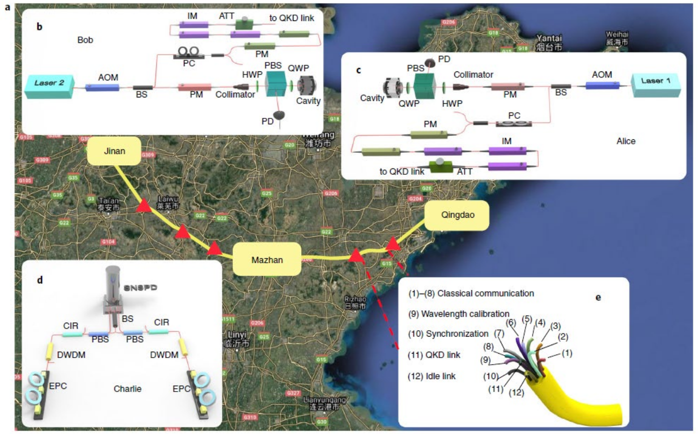


M. Pittaluga et al., Nat. Photonics 15, 530 (2021) (Toshiba, UK)

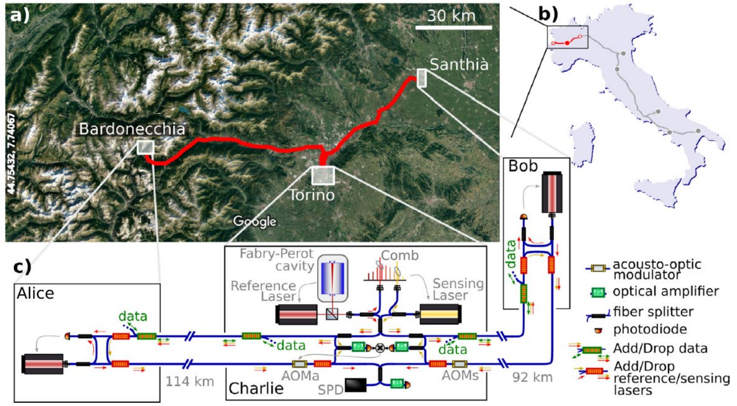


Y. Liu et al., Phys. Rev. Lett. 130, 210801 (2023) (USTC, China)





J. Chen et al., Nat. Photonics 13, 570 (2021) (USTC,China)

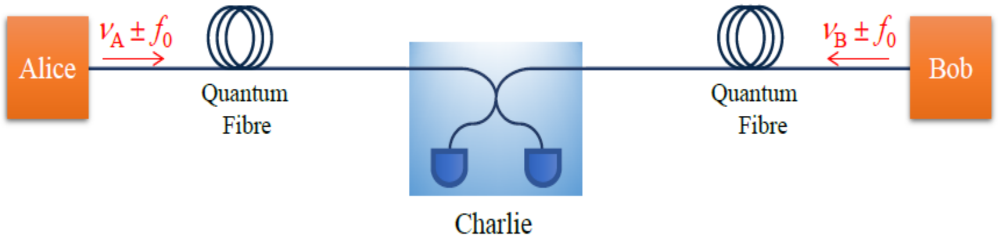


C. Clivati et al., Nat. Communications 13, 157 (2022) (INRIM, Italy)

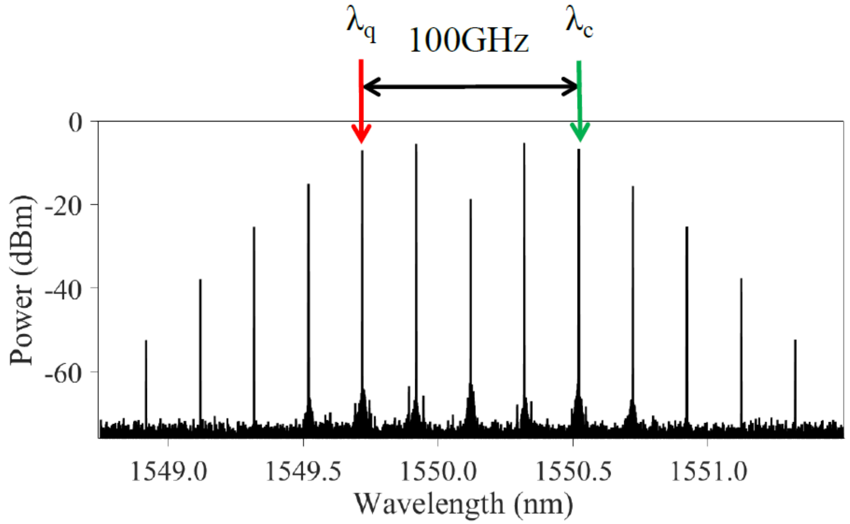
Frequency dissemination with service fiber

- Injection locking / OPLL module
- EDFA
- Fiber resource
- Scalability into a larger network?

Open TF-QKD

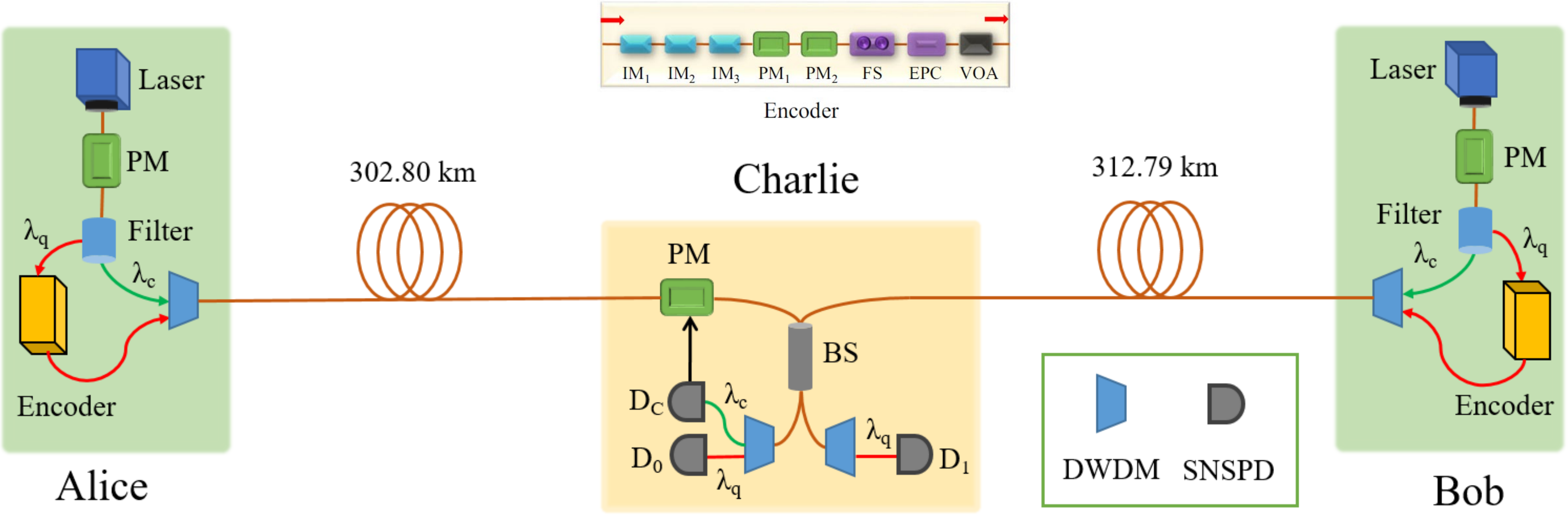


Open channel setup



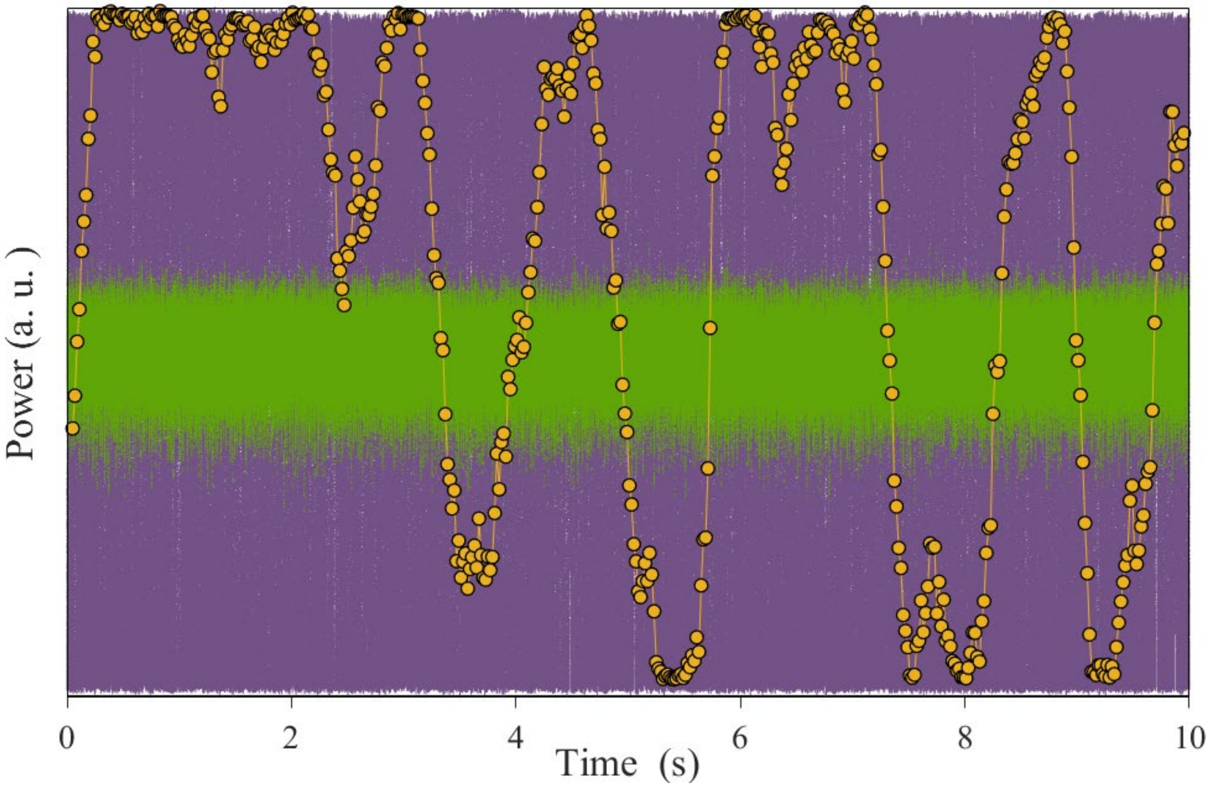
Coherent frequency comb

- λc, channel reference light (1550.52 nm)
- λq, quantum signal light (1549.72 nm)



- Ultra stable laser source (1550.12nm, ~1 Hz linewidth)
- Independent lasers (97.8% visibility)
- SNSPD (~2 Hz DCR, 60% eff)
- System repetition rate @ 1 GHz
- SNS-TF-QKD @ 500 MHz rate

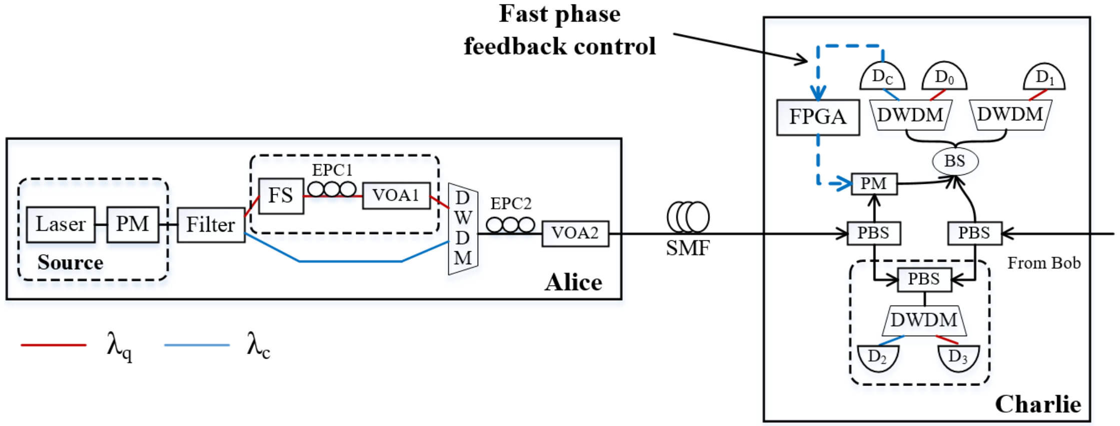
Dual-band phase stabilization



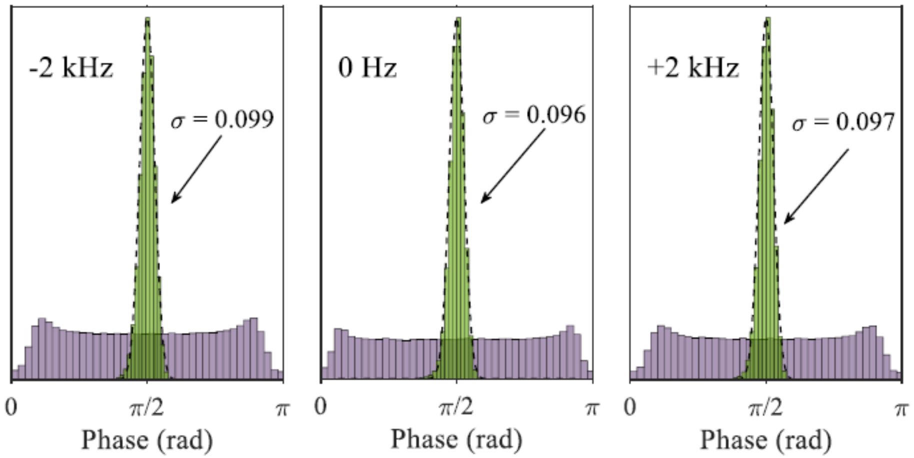
Dual-band high speed phase compensation

- Unstabilized λc (purple), 1.07 kHz drift rate $\frac{|\lambda_q - \lambda_c|}{\lambda_q}$
- Stabilized λc (blue)
- Stablized λq (yellow), 96.8% visibility, 0.72 Hz drift rate

Channel isolation is more than 65 dB

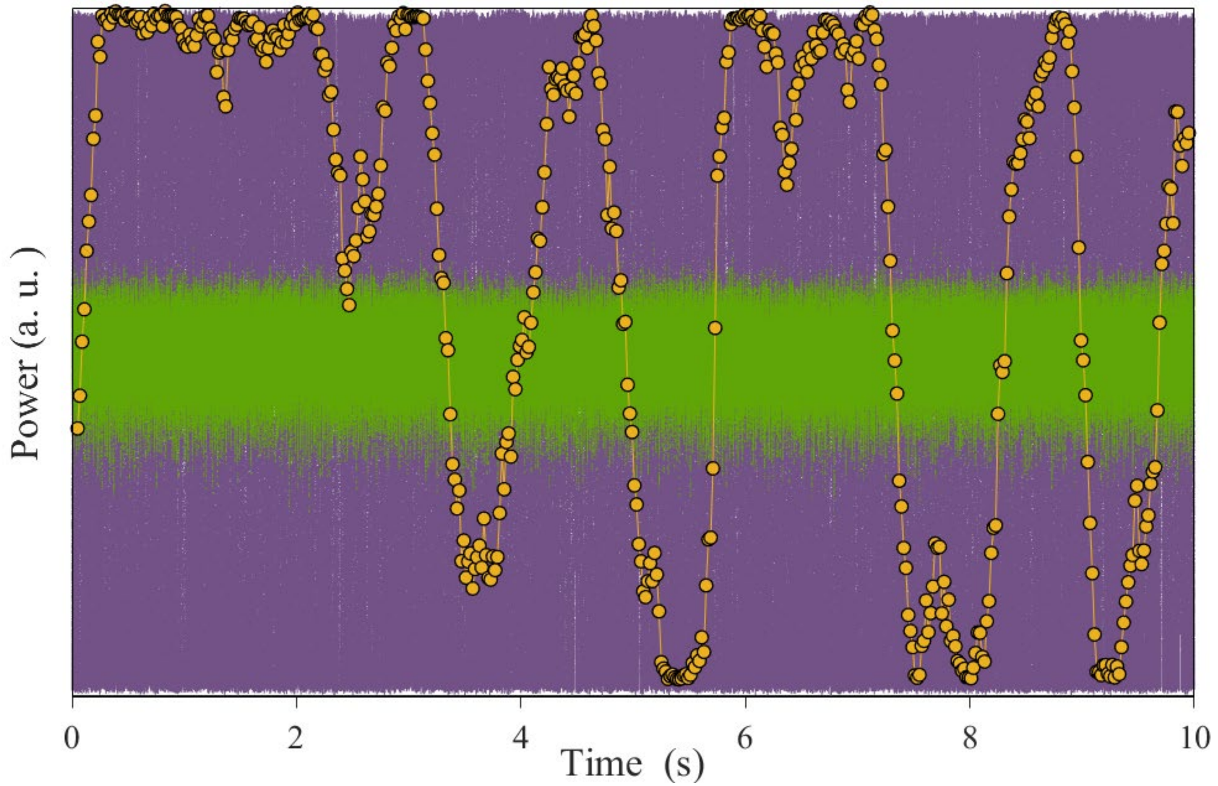


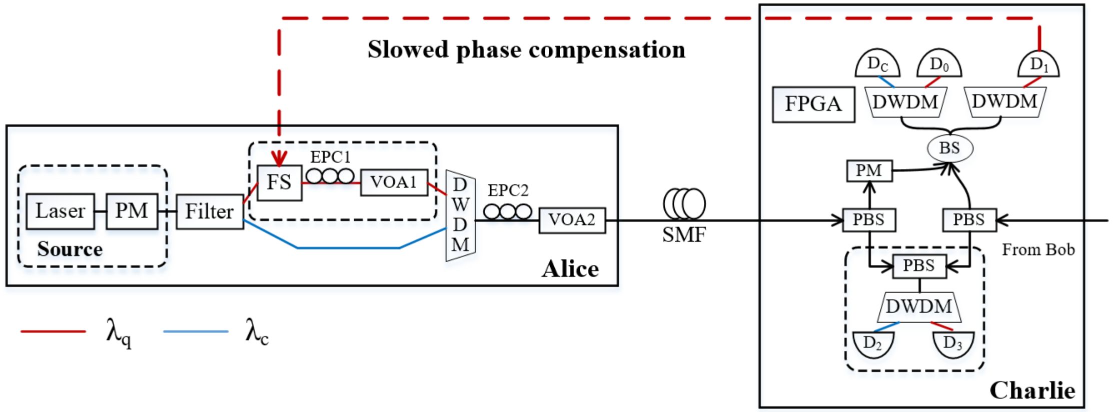
Dc, 13 MHz counts rate, 200 kHz PID feedback rate



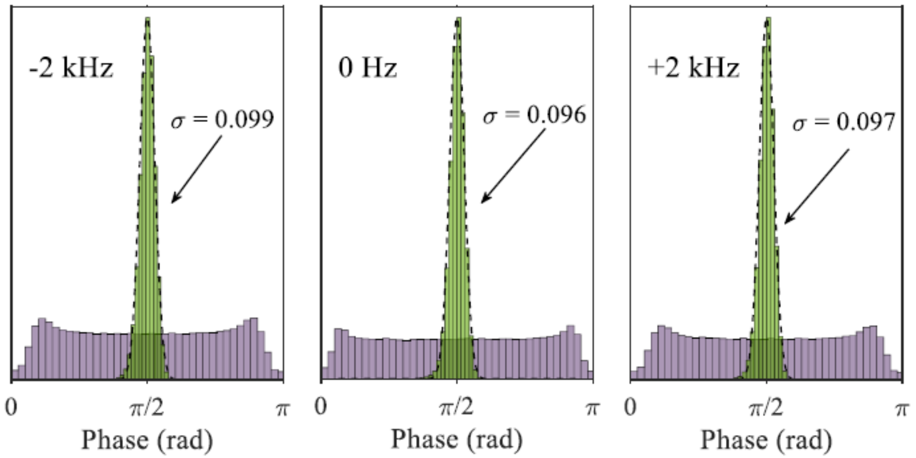
Good stabilized result, <0.1 rad std.

Dual-band phase stabilization





10-20 kHz count rate, 50-100 Hz feedback rate



Dual-band high speed phase compensation

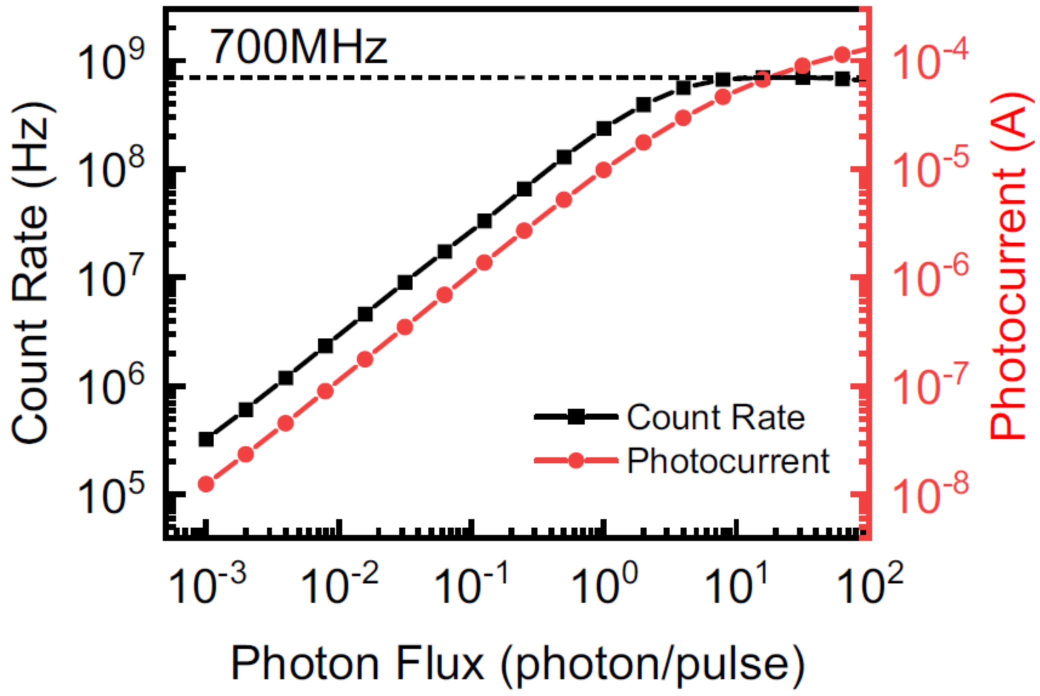
$$\frac{|\lambda_q - \lambda_c|}{\lambda_q}$$

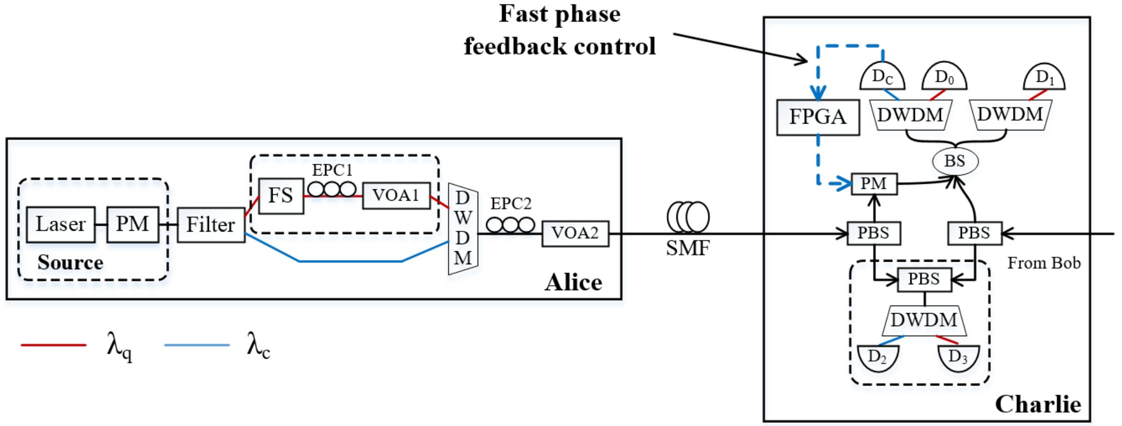
- Unstabilized λc (purple), 1.07 kHz drift rate
- Stabilized λc (blue)
- Stablized λq (yellow), 96.8% visibility, 0.72 Hz drift rate

Good stabilized result, <0.1 rad std.

Channel isolation is more than 65 dB

Dual-band phase stabilization



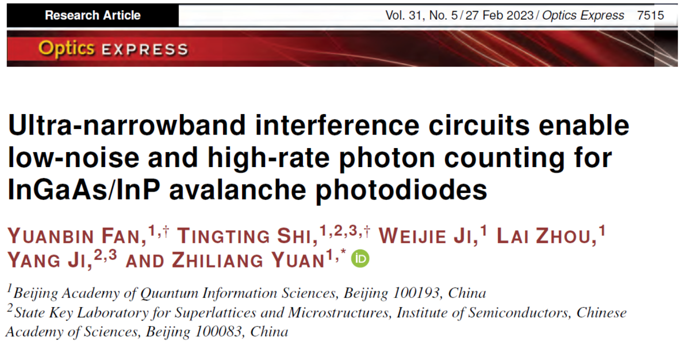


One application: More counts rate, faster feedback rate

Low-noise and high-rate APD

- 1.25 GHz gating rate
- 700MC/s, 0.5% afterpulsing, 25.3% detection efficiency
- 5.4e-7/gate, 1.0% afterpulsing, 21.2% detection efficiency

Fabricated APD in BAQIS


Research Article Vol. 31, No. 5 / 27 Feb 2023 / Optics Express 7515

Optics EXPRESS

Ultra-narrowband interference circuits enable low-noise and high-rate photon counting for InGaAs/InP avalanche photodiodes

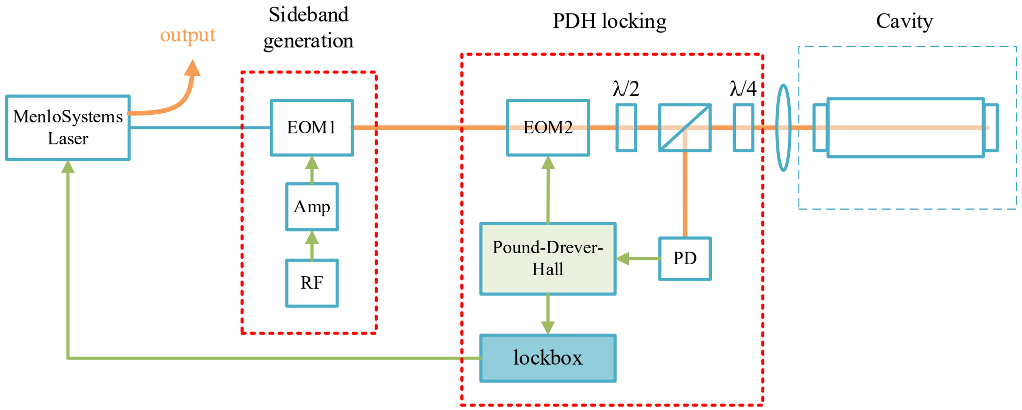
YUANBIN FAN,[1,†] TINGTING SHI,[1,2,3,†] WEIJIE JI,[1] LAI ZHOU,[1] YANG JI,[2,3] AND ZHILIANG YUAN[1,*]

[1] *Beijing Academy of Quantum Information Sciences, Beijing 100193, China*
[2] *State Key Laboratory for Superlattices and Microstructures, Institute of Semiconductors, Chinese Academy of Sciences, Beijing 100083, China*

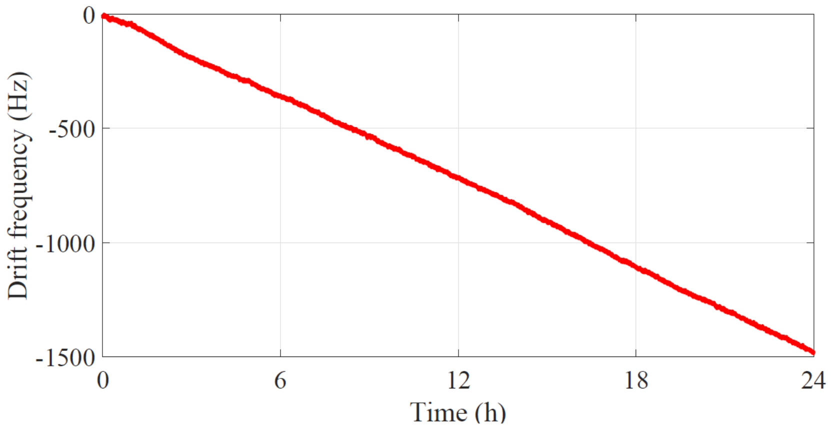
ultra-narrowband interference circuit (new patent filing)

Y. Fan et al., Optics Express 31,5 (2023)

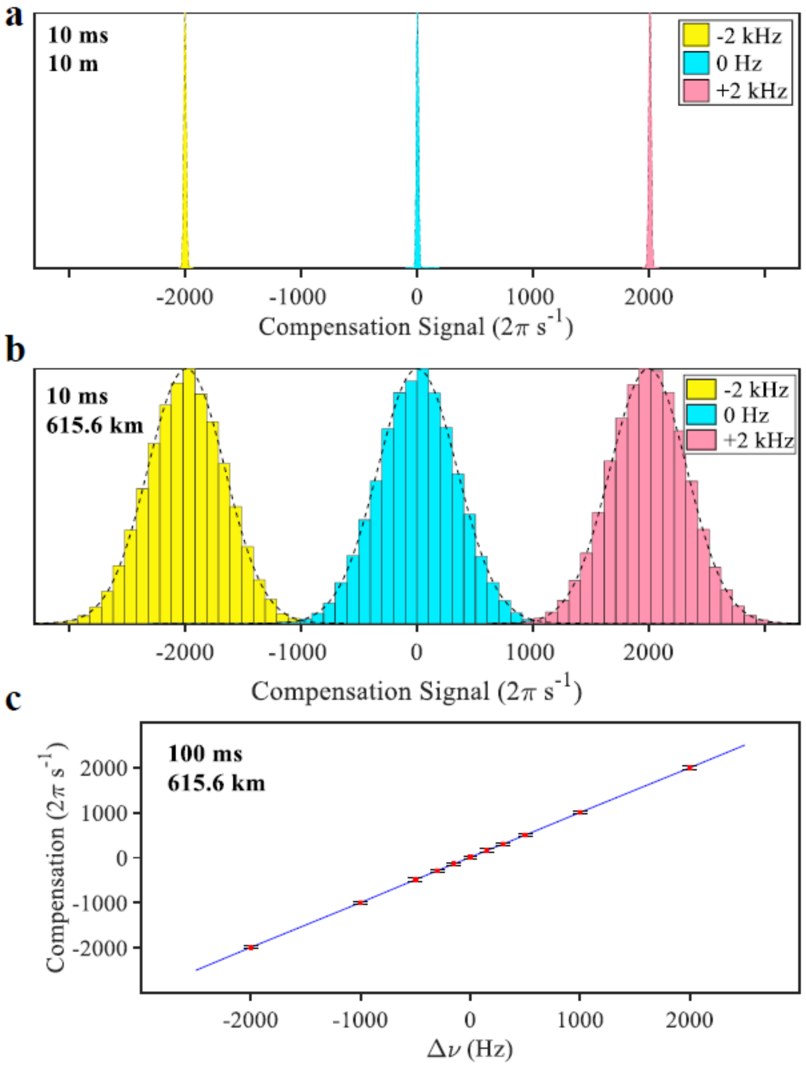
Frequency drift and compensation



Sideband generation to calibration Δν (1.5 GHz range)



Frequency drift
(110 mHz/s@Alice, 93 mHz/s@Bob)

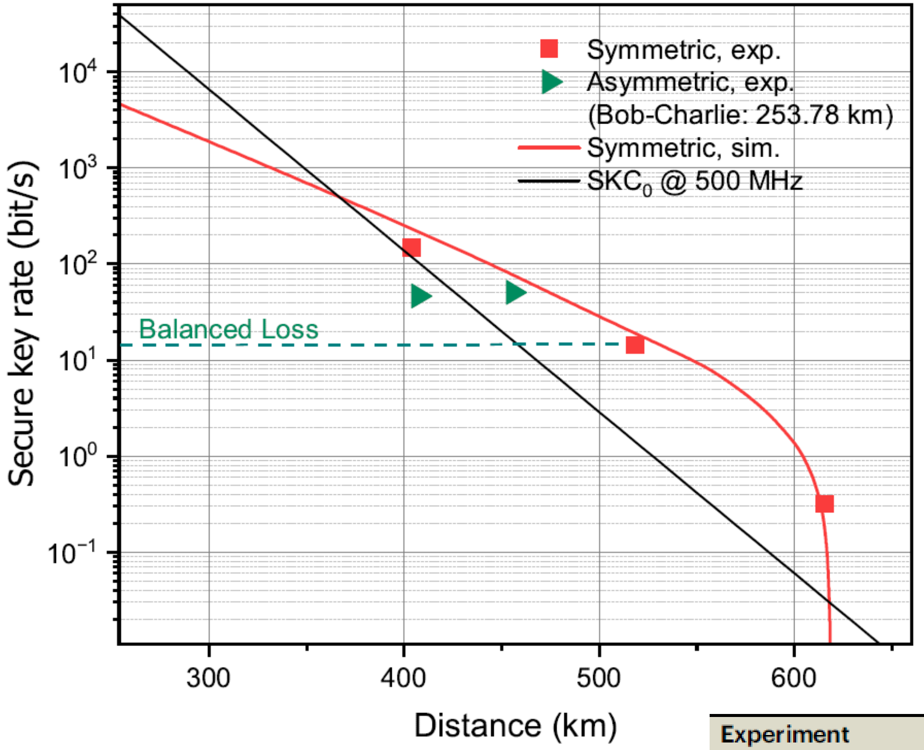


Short fibre (10 m)
Tracking the laser frequency difference (Δν)

Long fibre (615.6 km)
Broadened drift rate but still tracking Δν

Long fibre (615.6 km)
Compensate the drifted Δν in real time

Secure key rate



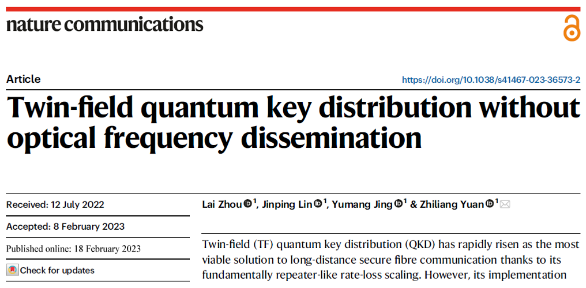
AOPP-SNS-TF QKD protocol in finite size

Symmetric case:

- 146.7 bit/s@403.7 km
- 14.4 bit/s@518.2 km (SKR/SKC_0 = 10.1)
- 0.32 bit/s @615.6 km (SKR/SKC_0 = 9.7)

Asymmetric case:

- 46.3 bit/s@407.2 km
- 153.5 km + 253.8 km (longest asymmetric distance)



nature communications

Article https://doi.org/10.1038/s41467-023-36573-2

Twin-field quantum key distribution without optical frequency dissemination

Received: 12 July 2022
Accepted: 8 February 2023
Published online: 18 February 2023
Check for updates

Lai Zhou[1], Jinping Lin[1], Yumang Jing[1] & Zhiliang Yuan[1]

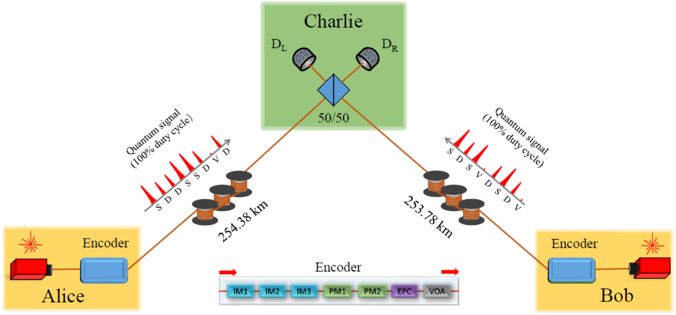
Twin-field (TF) quantum key distribution (QKD) has rapidly risen as the most viable solution to long-distance secure fibre communication thanks to its fundamentally repeater-like rate-loss scaling. However, its implementation

Experiment	Quantum/ service fibre	Frequency dissemi- nation	Phase compen- sation	Number of wave-lengths	Inter- wavelength Coherence	Check- basis QBER	Bit-flip QBER
Wang et al.[32], 2022	833.8 km/833.8 km	Homodyne OPLL	Active	1	n/a	n/a	3.79%
Clivati et al.[31], 2022	206 km/206 km	Heterodyne OPLL	Active, partial	2	Yes	n/a	n/a
Chen et al.[33], 2022	658.7 km/500 km	Time-freq. metrology	Post- selection	1	n/a	~5.0%	2.12%
Pittaluga et al.[28], 2021	605.2 km/611.4 km	Heterodyne OPLL	Active	2	No	5.41%	3.65%
This work	615.6 km/ not needed	Not needed	Active	2	Yes	4.75%	1.97%

L. Zhou et al., Nature Communications 14,928 (2023)

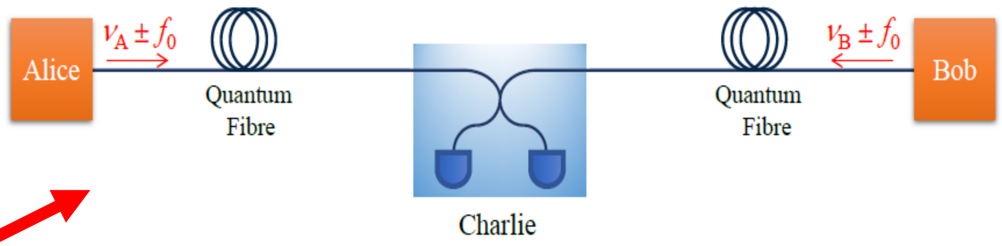
2) Open TF QKD → Simpler System

Practical Candidate:
New protocol, post-measurement-pairing QKD

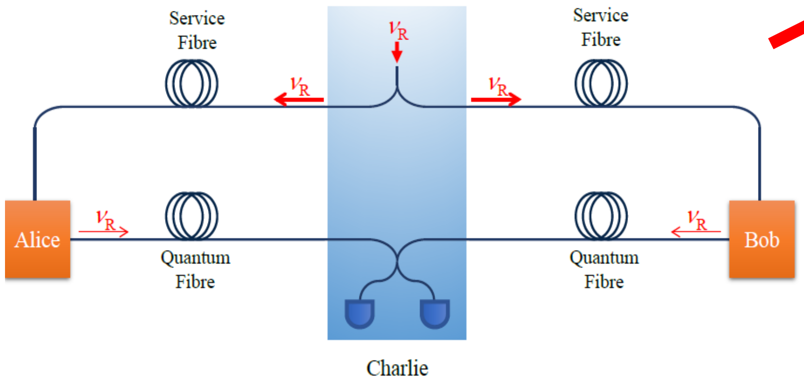


Removing the phase tracking module?

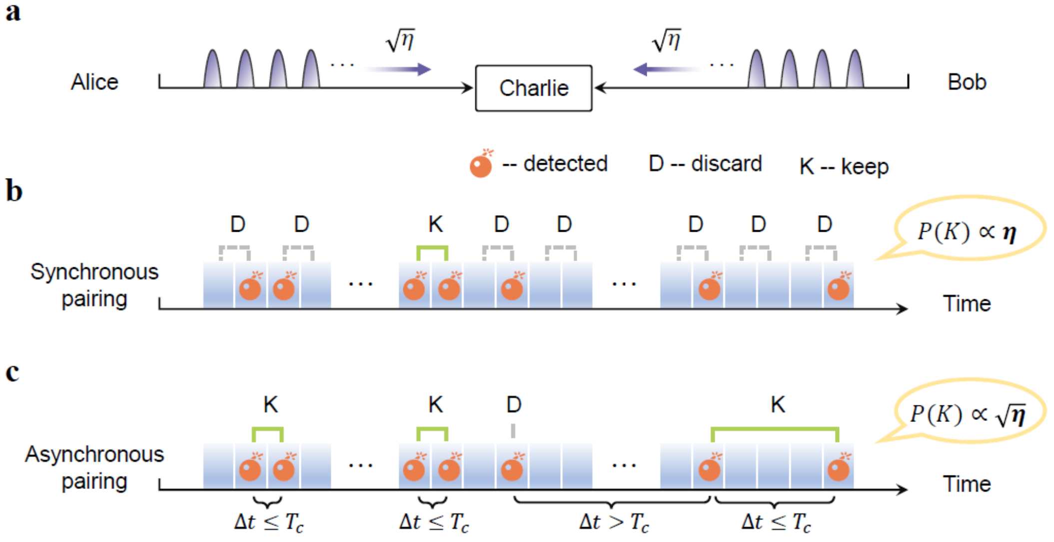
Open TF QKD



TF QKD with closed configuration



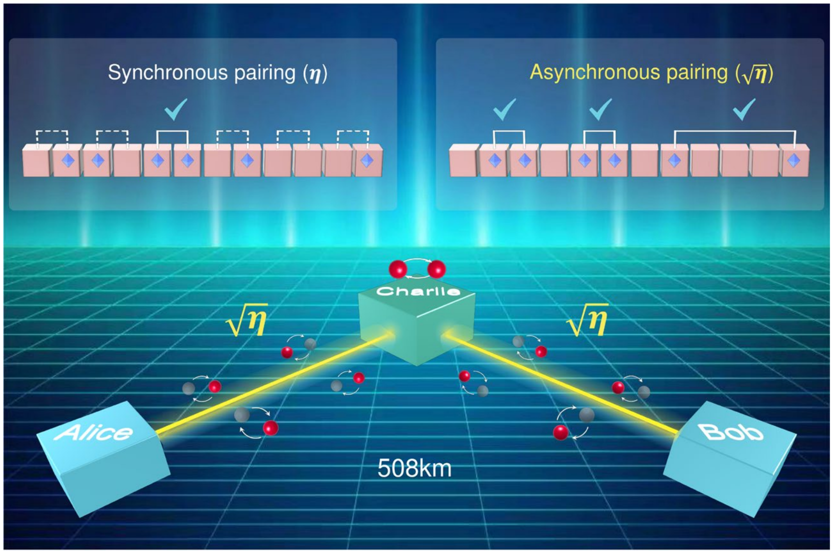
Post-measurement-pairing scheme



→ Generic MDI-QKD

→ Synchronous coincidence paring

→ Asynchronous coincidence paring



	No phase tracking module	Open architecture	Beat SKC0
Open TF-QKD	X	√	√
MDI-QKD	√	√	X
AMDI/MP-QKD	√	√	√

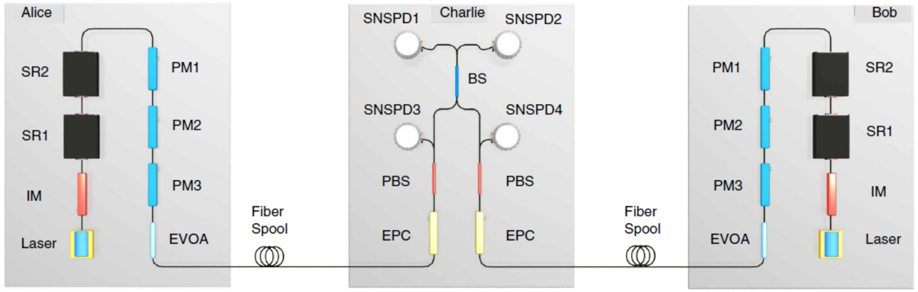
PRX Quantum 3, 020315 (2022)
Nat. Commun. 13, 3903 (2022)

Simpler System with different schemes

Practical Candidate:

New protocol, post-measurement-pairing QKD

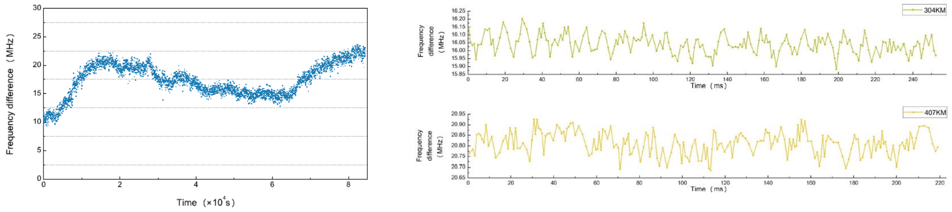
New scheme, estimation of frequency and phase via data post-processing

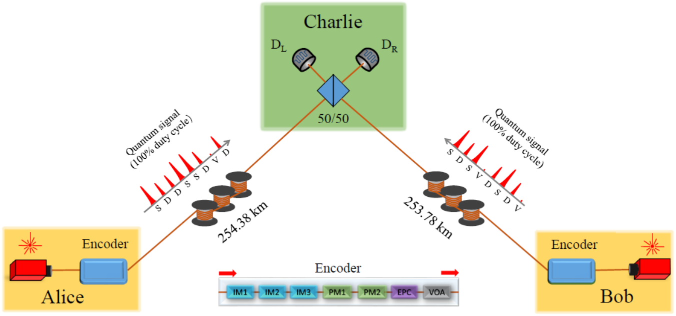


H. Tao et al., Physical Review Letter 130,030801 (2023)

Frequency difference estimation (maximum likelihood)

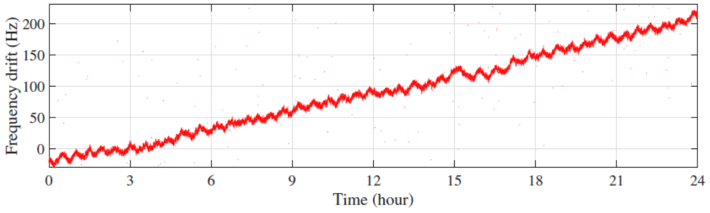
$$f(\Delta\omega) = \sum_{(i,j)} \ln \left\{ \frac{1}{2} + (-1)^{D_i - D_j} \frac{\cos[\Delta\omega\tau(j-i)]}{4} \right\}$$

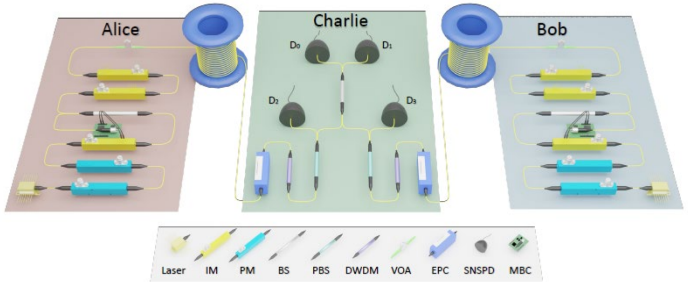




L. Zhou et al., Phys. Rev. Lett. 130, 250801 (2023)

Frequency difference calibration with two independent ultra stable lasers

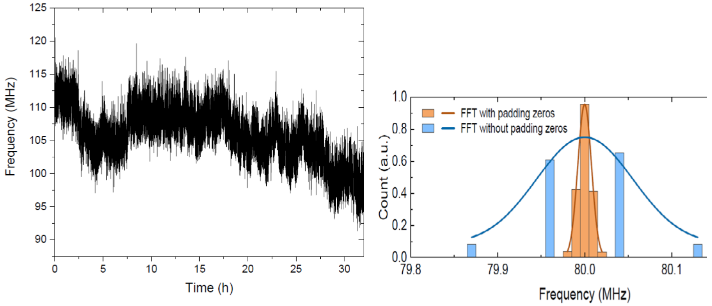




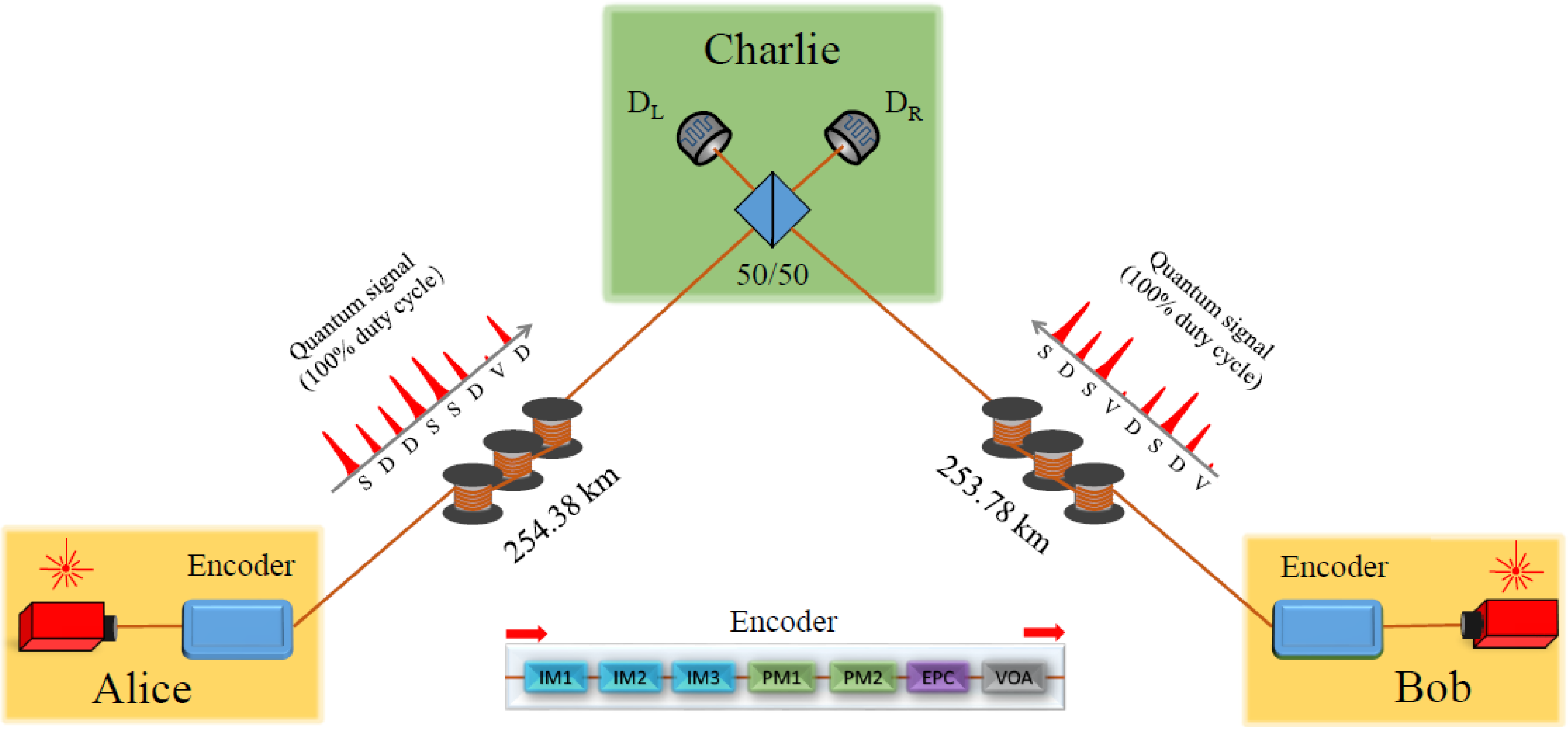
W. Li et al., Phys. Rev. Lett. 130, 250802 (2023)

FFT based algorithm (power spectrum density)

$$\left|\cos\left(2\pi\hat{\nu}t + \hat{\phi}_0 + (\phi_a - \phi_b)\right)\right| \geq \cos(\pi/16),$$



Asynchronous MDI QKD system



Laser
- Ultra stable laser source (1550.12nm, ~1 Hz linewidth)
- Able to control lasers' mutual frequency offset

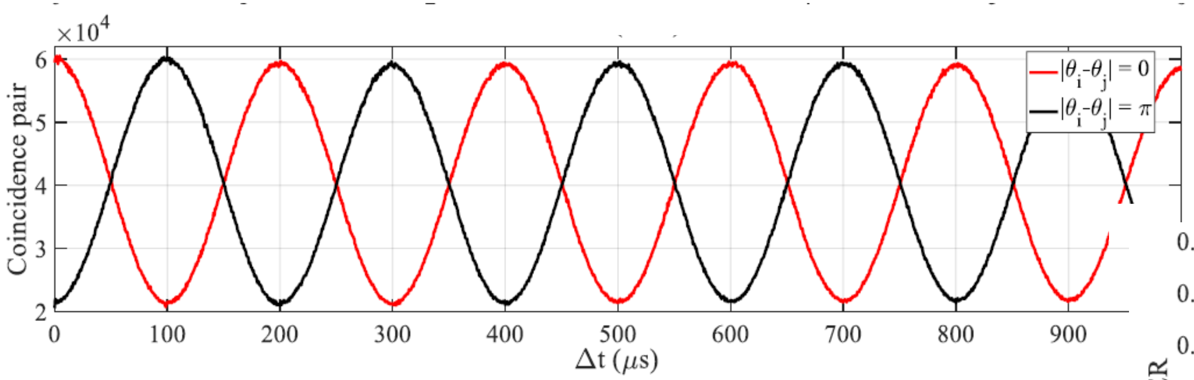
Encoder
- 1GHz repetition rate (100% duty cycle)
- No need for phase tracking

Detector
- SNSPD (78.1% and 77% eff)
- DCR 10.1 Hz and 12.7 Hz

北京量子信息科学研究院

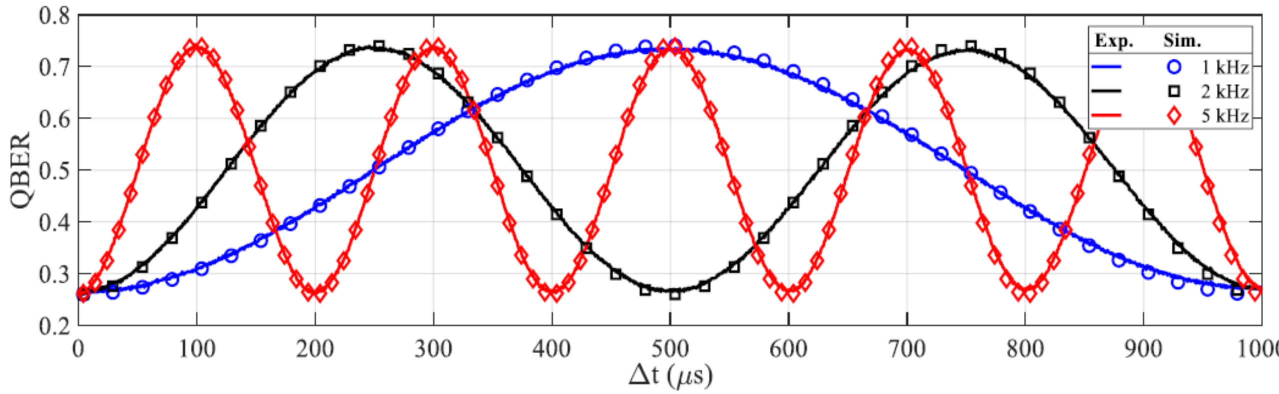
南京大學 NANJING UNIVERSITY

Asynchronous two photons interference



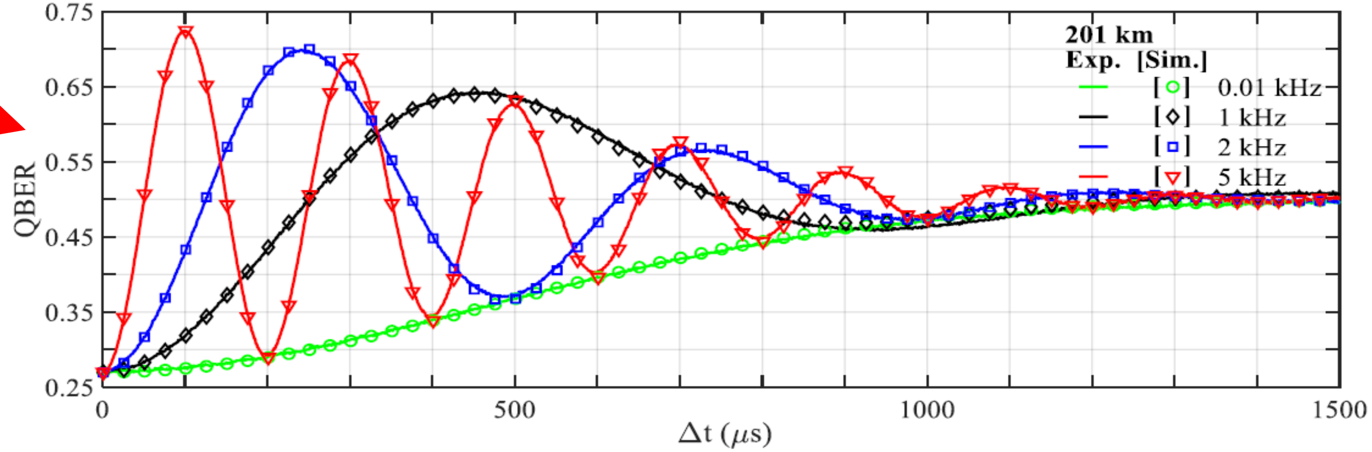
Coincidence pairing
1) Frequency difference, 5 kHz
2) 0/pi modulation
3) Short fibre

$$E_x = \frac{1}{2} - \frac{V_2}{2}\cos(2\pi\Delta f\Delta t)$$

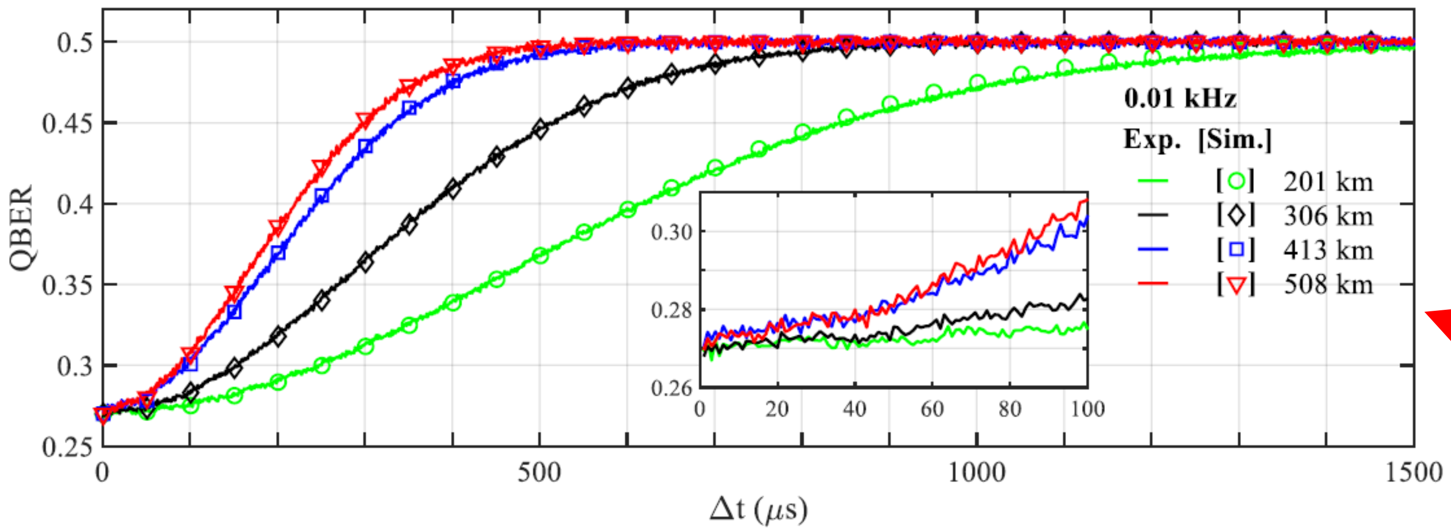


$$E_x = \frac{1-V_2}{2} + \frac{V_2}{2}\left[1 - e^{-\sigma^2\Delta t^2/2}\cos(2\pi\Delta f\Delta t)\right]$$

X basis QBER in the experiment
1) 201 km fibre
2) Different frequency differences
3) Phase randomization & decoy state



Asynchronous MDI / MP QKD



X basis QBER in the experiment
1) 201/306/413/508 km fibre
2) Small frequency difference
3) Phase randomization & decoy state

$$E_x = \frac{1}{2} - \frac{V_2}{2} e^{-\sigma^2 \Delta t^2 / 2}$$

TABLE S2. The average paring interval at various quantum link fiber lengths.

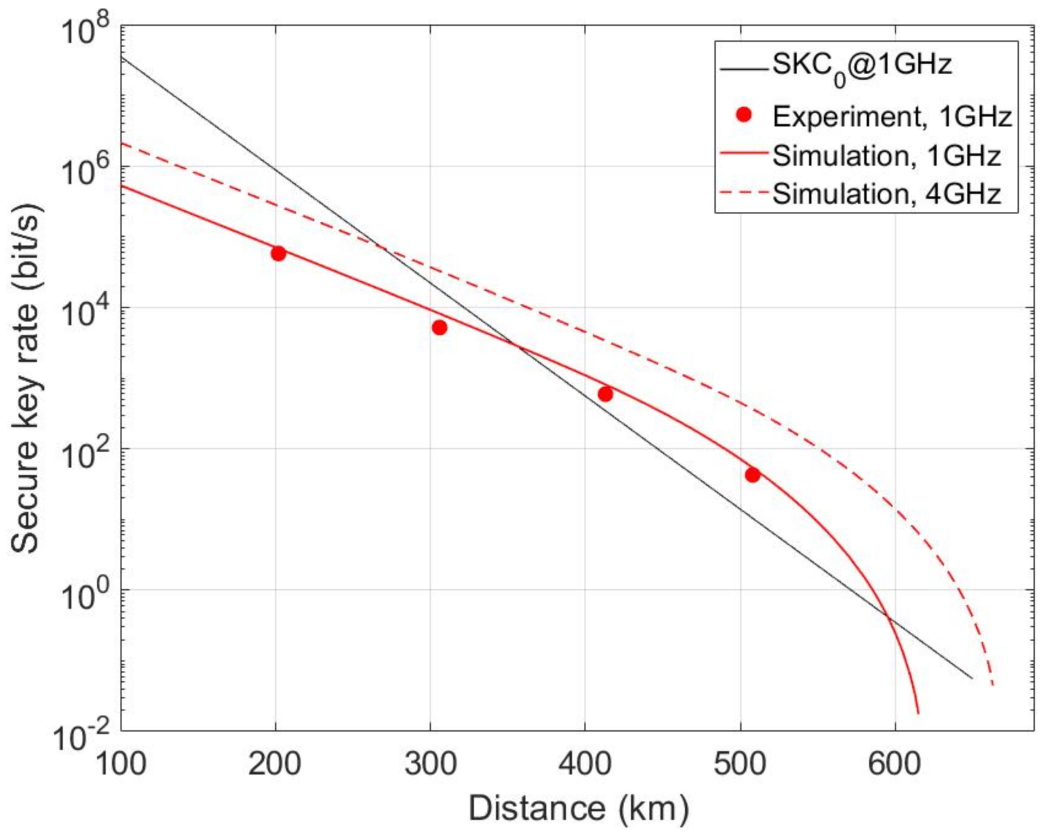
Total length (km)	201.86	306.31	413.73	508.16
F (Hz)	10^9	10^9	10^9	10^9
T_c (μs)	5	20	60	200
Simulation T_{mean} (μs)	0.41	3.52	19.73	70.06
Experiment T_{mean} of $\mathcal{S}_{[\mu,\mu]}$ (μs)	0.44	3.79	19.82	70.96
Experiment T_{mean} of $\mathcal{S}_{[2\mu,2\mu]}$ (μs)	0.43	3.79	19.81	70.96
Experiment T_{mean} of $\mathcal{S}_{[2\nu,2\nu]}$ (μs)	0.43	3.79	19.83	70.89

TABLE S3. Experimental parameters and results at various quantum link fiber lengths.

Total length (km)	201.86	306.31	413.73	508.16
E_z	0.00066	0.00060	0.00111	0.00204
E_x	0.2694	0.2734	0.2772	0.2931
$\underline{s}_{11}^{z}$	460369142	159161908	39264580	14357572
$\underline{s}_{11}^{x}$	18739	31965	47132	24307
$\overline{\phi}_{z}^{11}$	0.0916	0.1212	0.1150	0.1960

Shorter paring intervals lead to lower QBER in X basis

Asynchronous MDI / MP QKD



- 57.63Kbit/s@201km
- 5.18Kbit/s@306km
- 42bit/s@508km(SKR/SKC0=4.1)

TABLE S3. Experimental parameters and results at various quantum link fiber lengths.

Total length (km)	201.86	306.31	413.73	508.16
SKR (bit/s)	5.7631×10^4	5.1821×10^3	5.9061×10^2	42.6351
SKR (bit/clock)	5.7631×10^{-5}	5.1821×10^{-6}	5.9061×10^{-7}	4.2635×10^{-8}
SKC_0 (bit/clock)	8.5961×10^{-4}	1.5459×10^{-5}	3.2898×10^{-7}	1.0451×10^{-8}
Ratio SKR over SKC_0	0.0670	0.3352	1.7953	4.0795

PHYSICAL REVIEW LETTERS **130,** 250801 (2023)

Editors' Suggestion Featured in Physics

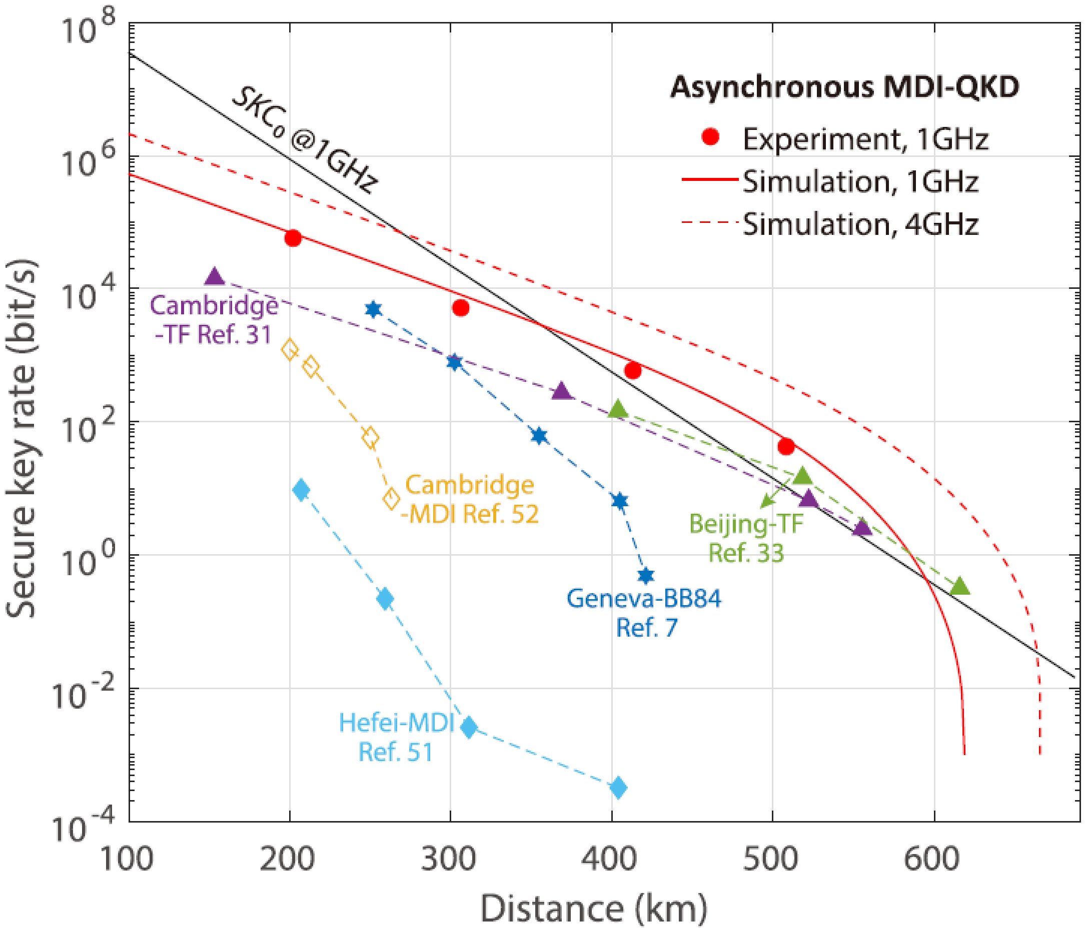
Experimental Quantum Communication Overcomes the Rate-Loss Limit without Global Phase Tracking

Lai Zhou,[1] Jinping Lin,[1] Yuan-Mei Xie,[2] Yu-Shuo Lu,[2] Yumang Jing,[1] Hua-Lei Yin,[2,1,*] and Zhiliang Yuan[1,†]

[1]*Beijing Academy of Quantum Information Sciences, Beijing 100193, China*
[2]*National Laboratory of Solid State Microstructures and School of Physics, Collaborative Innovation Center of Advanced Microstructures, Nanjing University, Nanjing 210093, China*

Long Distance Quantum Key Distribution Gets Simpler

Asynchronous MDI / MP QKD



- 57.63Kbit/s@201km
- 5.18Kbit/s@306km
- 42bit/s@508km(SKR/SKC_0=4.1)

TABLE S3. Experimental parameters and results at various quantum link fiber lengths.

Total length (km)	201.86	306.31	413.73	508.16
SKR (bit/s)	5.7631×10^4	5.1821×10^3	5.9061×10^2	42.6351
SKR (bit/clock)	5.7631×10^{-5}	5.1821×10^{-6}	5.9061×10^{-7}	4.2635×10^{-8}
SKC_0 (bit/clock)	8.5961×10^{-4}	1.5459×10^{-5}	3.2898×10^{-7}	1.0451×10^{-8}
Ratio SKR over SKC_0	0.0670	0.3352	1.7953	4.0795

PHYSICAL REVIEW LETTERS **130,** 250801 (2023)

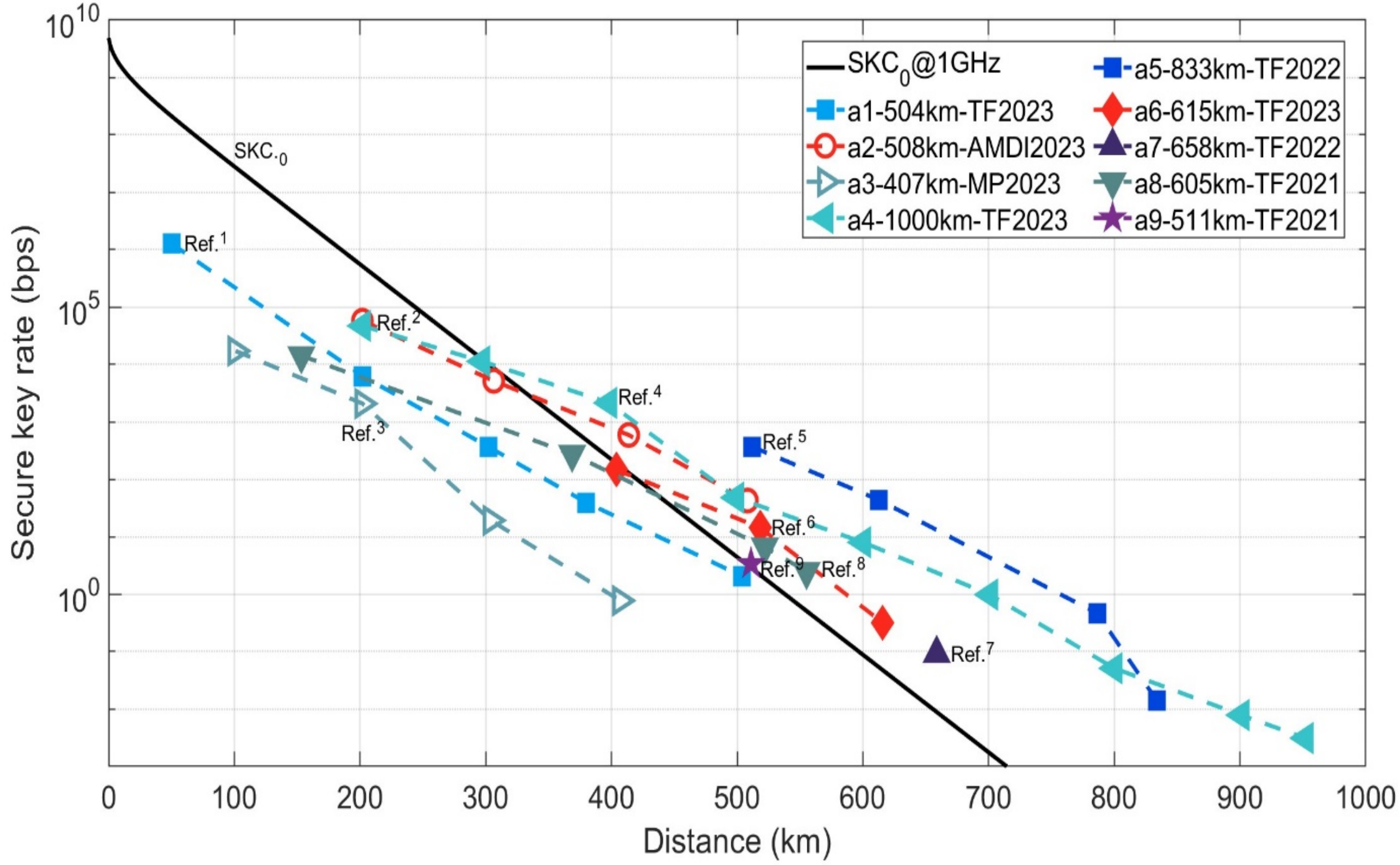
Editors' Suggestion | Featured in Physics

Experimental Quantum Communication Overcomes the Rate-Loss Limit without Global Phase Tracking

Lai Zhou,[1] Jinping Lin,[1] Yuan-Mei Xie,[2] Yu-Shuo Lu,[2] Yumang Jing,[1] Hua-Lei Yin,[2,1,*] and Zhiliang Yuan[1,†]

[1]*Beijing Academy of Quantum Information Sciences, Beijing 100193, China*
[2]*National Laboratory of Solid State Microstructures and School of Physics, Collaborative Innovation Center of Advanced Microstructures, Nanjing University, Nanjing 210093, China*

Key Rate Comparison



- The key rate of Asynchronous MDI / MP QKD is comparable with TF QKD
- L < 200km, Decoy BB84
- 200km < L < 500km, Asynchronous MDI / MP QKD
- L > 500km, TF QKD

Summary and discussion

- Develop a first open TF-QKD setup and confirm the repeater-like behavior at a distance of 615 km
- Open-channel stabilization technique with coherence frequency comb

- Implement a simple MDI-QKD that exploits post-measurement pairing technique
- Demonstrate the capability of asynchronous MDI-QKD (also named mode-pairing QKD) overcoming the SKC0 without global phase tracking
- Improve the clock rate and also use less-demanding lasers for practicality enhancement

- Develop a high count rate of up to 700 MC/s and a low afterpulsing of 0.5 % at a detection efficiency of 25.3 % for 1.25 GHz gated InGaAs/InP APDs

DLCZ scheme with single photon interference Y. Yong et al., Nature 578.7794(2020)

Sensing the vibration with interference result G. Marra et al., Science 376.6595(2022)

北京量子信息科学研究院
Beijing Academy of Quantum Information Sciences

The team behind this work:


Jinping Lin

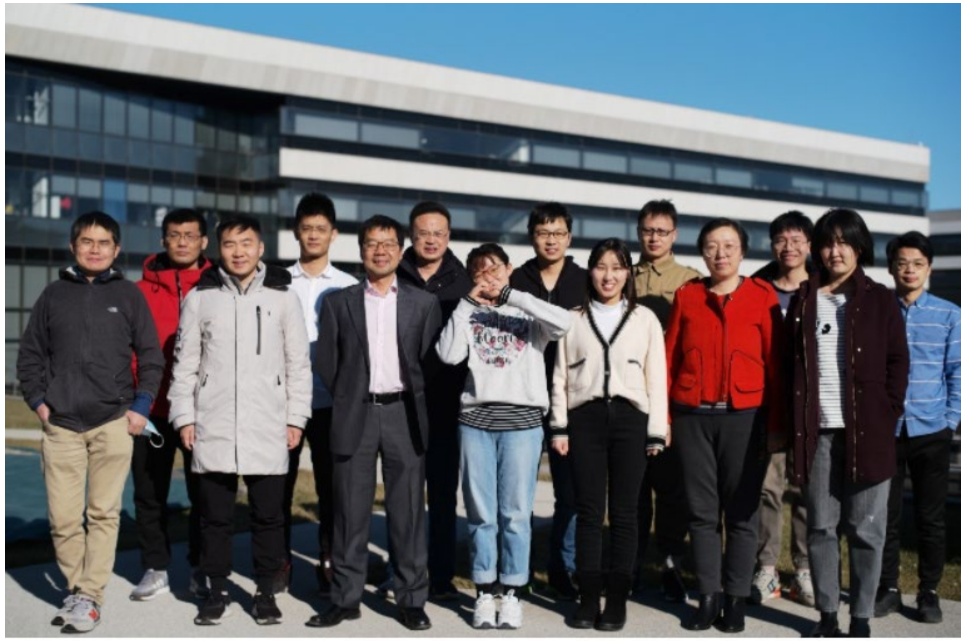

Yumang Jing


Yuanbin Fan


Zhiliang Yuan


Hualei Yin (Nanjing University)

Tingting Shi (Institute of Semiconductors)
Yuanmei Xie (Nanjing University)
Yushuo Lu (Nanjing University)


Our group in the BAQIS, Zhiliang Yuan (group leader)
http://en.baqis.ac.cn/research/groups/?cid=816

Thank you !