QCRYPT2021

Practical long distance twin-field quantum key distribution through sending-or-not-sending

Xiang-Bin Wang

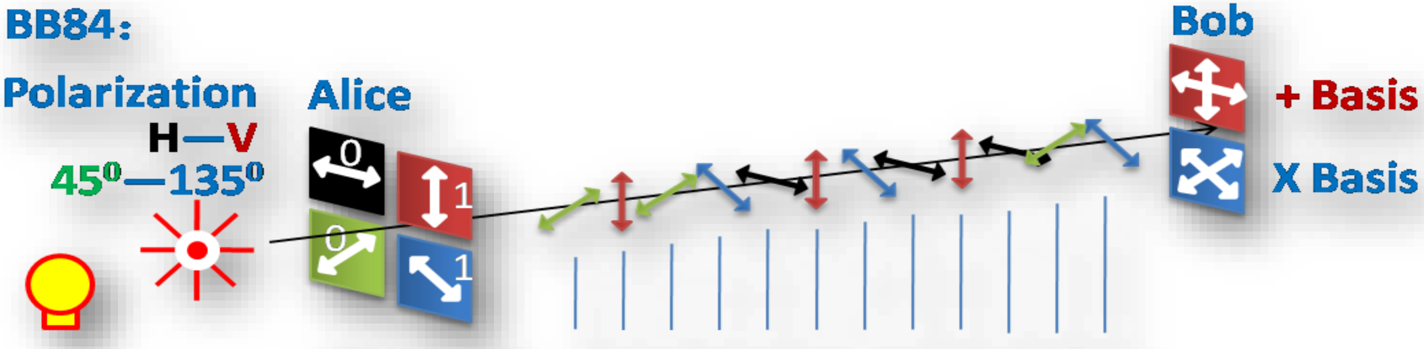
Tsinghua university

Email: xbwang@mail.Tsinghua.edu.cn

Outline of this talk

- Decoy-state method
- Measurement-device-independent (MDI) QKD
- Twin-Field (TF) QKD through sending-or-not-sending
- Side-channel-free (SCF) protocol

The BB84 protocol



Alice's Bit	0	1	0	1	0	1	1	0	1	0	0	1
Bob's Bases	+	+	X	X	+	X	+	X	X	+	+	X
Bob's Results	1	1	0	1	0	1	0	1	0	0	0	1
Raw Key	-	1	0	1	0	-	-	-	-	0	-	1

C. H. Bennett and G. Brassard, in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing (IEEE, Piscataway, NJ, 1984) pp. 175–179.

Major methods in practical QKD

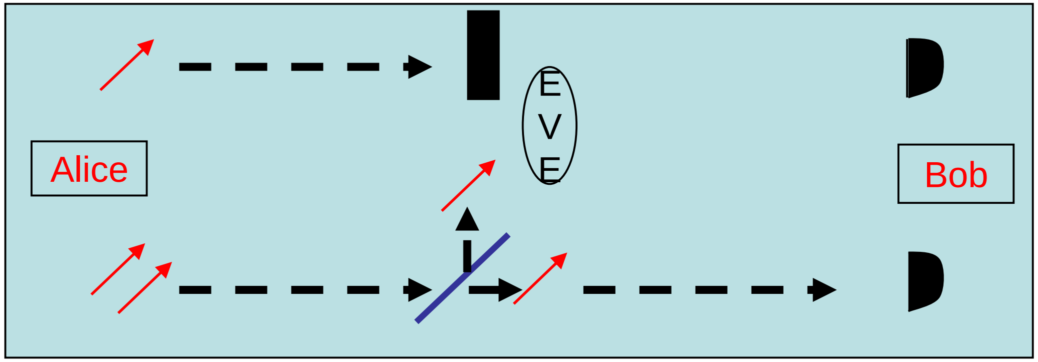
- **Decoy-state method**
- W.-Y. Hwang, Phys. Rev. Lett. 91, 057901 (2003).
- X.-B. Wang, Phys. Rev. Lett. 94, 230503 (2005).
- H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. 94, 230504 (2005).
- **Measurement-device-independent (MDI) QKD**
- H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. 108, 130503 (2012).
- S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. 108, 130502 (2012).
- Y.-H. Zhou, Z.-W. Yu, X.-B. Wang, Phys. Rev. A 93, 042324 (2016).
- **Twin-Field (TF) QKD**
- M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Nature (London) 557, 400 (2018).
- X.-B. Wang, Z.-W. Yu, X.-L. Hu, Phys. Rev. A 98, 062323 (2018)
- M. Curty, K. Azuma, and H. K. Lo, npj Quantum Inf. 5, 64 (2019).
- **Side-channel-free (SCF) protocol**
- X.-B. Wang, X.-L. Hu, Z.-W. Yu， Physical Review Applied 12, 054034 (2019).

Let us start with the decoy-state method.

Decoy-state method and its application

In practice, we don't have perfect single-photon source. If we simply go ahead to take the BB84 protocol with the imperfect source such as the coherent states, the security is threatened by the photon number splitting attack. Under Eve's attack, In this way, the key rate is in the scale of eta square, square of channel transmittance. Surely, this severely limits the practical application of QKD.

Photon number splitting (PNS) attack



Key rate:

$R \sim \eta^2$

$R \sim \eta$

Decoy-state method

B. Huttner et al, Phys. Rev. A51, 1863(1985)
G. Brassard et al, Phys. Rev. Lett., 85, 1330(2000)

Decoy-state method and its application

➢Decoy-state method to beat the PNS attack

- W.-Y. Hwang, Phys. Rev. Lett. 91, 057901 (2003).
- X.-B. Wang, Phys. Rev. Lett. 94, 230503 (2005).
- H.-K. Lo et al Phys. Rev. Lett. 94, 230504 (2005).

Key rate:

$$\begin{tikzcd} R\sim\eta^2 \arrow[d, bend left, "\text{Decoy-state method}"] \\ R\sim\eta \end{tikzcd}$$

Luckily, with the decoy-state method, one can go ahead to use the imperfect single photon source in practical QKD, with the key rate in linear scale of eta, the channel transmittance. The implementation is very simple: just switching the intensities of source light among a few values. The net result is equivalent to the case that we have only used the single-photon pulses in QKD.

The decoy-state method has been extensively applied in long distance QKD in practice.

The decoy state BB84 protocol:
Satellite-to-ground quantum key distribution

The decoy state method is successfully applied in satellite-based QKD with the final key rate around **1 kbps then. The most recent result is larger than this by one magnitude order.**

[1] *X.-B. Wang, Phys. Rev. Lett. 94, 230503 (2005).*

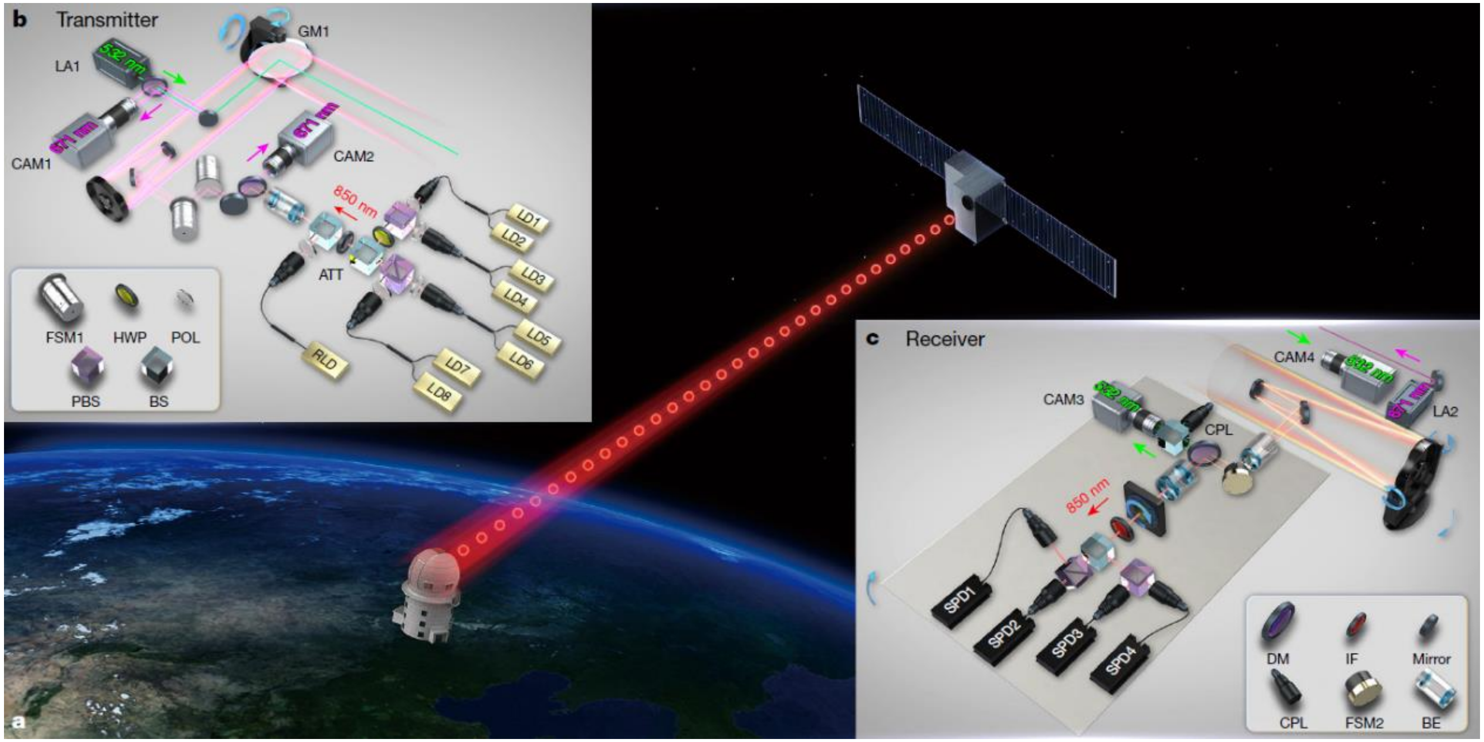
[2] *H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. 94, 230504 (2005).*

Here the **intensity fluctuation** has been considered, which improves the practical security level. The result is secure Even though there are small errors in the intensity controll in decoy-state method.

[3] *X.-B. Wang et al. Physical Review A, 2008, 77(4): 042311; New Journal of Physics, 2009, 11: 075006.*

Liao S K, Cai W Q, Liu W Y, et al. Nature, 2017, 549(7670):43.

The decoy state BB84 protocol:
Satellite-to-ground quantum key distribution

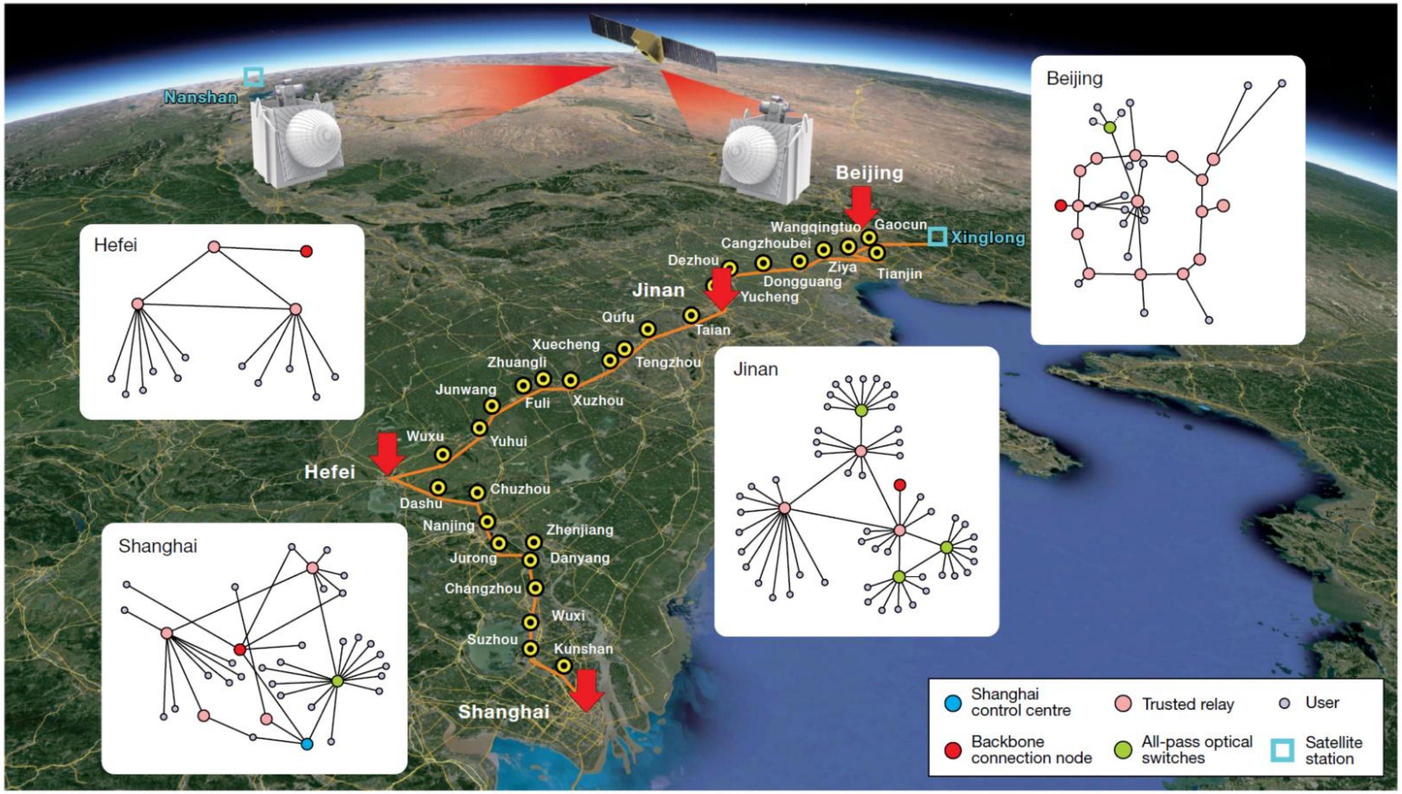


Satellite-based QKD

Liao S K, Cai W Q, Liu W Y, et al. Nature, 2017, 549(7670):43.

The decoy state BB84 protocol : Space-to-ground quantum communication network over 4,600 km

Very recently, an experiment was done on the integrated system of space-to-ground communication



Chen Y A, et al. Nature, 2021, 589(7841): 214.

The decoy state BB84 protocol :Other applications

There are many other applications. The decoy-state method has been extensively applied on earth, in more than 100 QKD experiments. For example:

- **The 421 km experiment**

Zbinden group, Boaron, A., Boso, G., Rusca, D., Vulliez, C., Autebert, C., Caloz, M., ... & Zbinden, H. Physical review letters, 121(19), 190502 (2018).

- **The QKD networks,**

[1]European team, Peev, M. et al, A. New Journal of Physics, 11(7), 075001 (2009)
[2]USTC team, Chen, T. Y. et al, Optics express, 18(26), 27217-27225 (2010)
[3] Japan & Europe, Sasaki, M. et al, Optics express, 19(11), 10387-10409 (2011)
[4] Toshiba/Cambridge, Dynes et al, NPJ Quantum Information 5, 101(2019).

The early experiments:

[1] NIST & Los Alamos Lab., D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S.W. Nam, and J. E. Nordholt, Phys. Rev. Lett. 98, 010503 (2007)
[2] U. Viena, T. Schmitt-Manderbach et al, Phys. Rev. Lett. 98, 010504 (2007)
[3] USTC & Tsinghua, C.-Z. Peng, J. Zhang, D. Yang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, Phys. Rev. Lett. 98, 010505 (2007)
[4] Toshiba, Z. Yuan, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. 90, 011118 (2007).

MDI-QKD

Besides source imperfection, there are also security loopholes in the limited detection efficiency. This problem has been thoroughly solved by the MDIQKD.

- **Measurement-device-independent (MDI) QKD**
- **H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. 108, 130503 (2012).**
- **S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. 108, 130502 (2012).**

MDIQKD is secure under whatever attack to measurement device, including the case Eve fully controls the detectors. It is secure under all types of attacks to detectors, such as the one by L. Lydersen et al, Nature Photonics, 4, 686(2010).

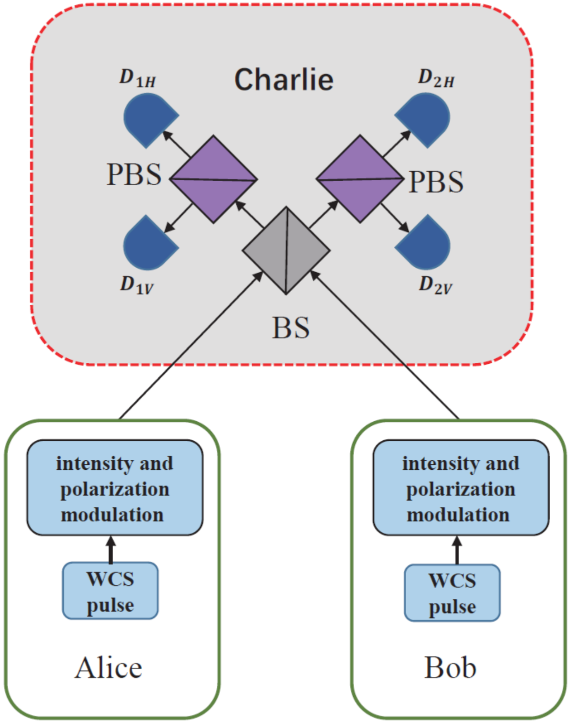
$R \sim \eta$

Combining the decoy-state method, secure MDIQKD can be made with imperfect single-photon source.

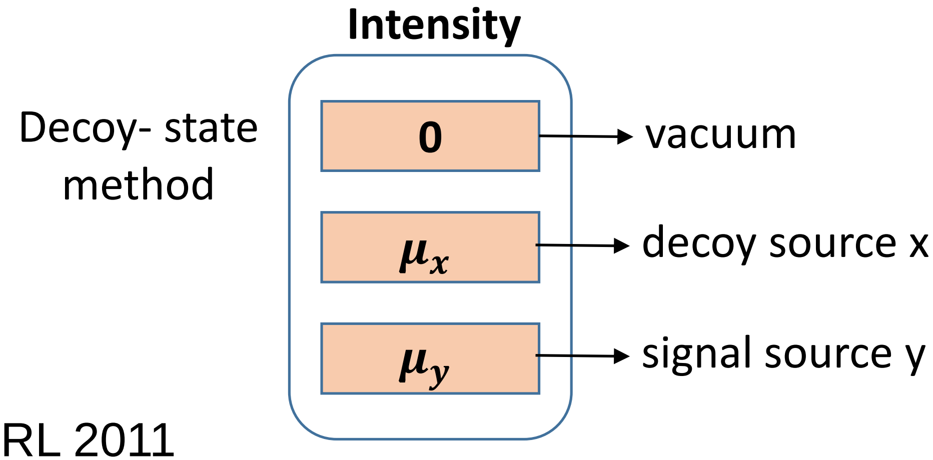
The **most efficient** protocol in practice: 4-intensity protocol with full optimization:

Y.-H. Zhou, Z.-W. Yu, X.-B. Wang, Phys. Rev. A 93, 042324 (2016)

Three-intensity decoy-state MDI QKD protocol


D_{1H}
Charlie
D_{2H}
PBS
PBS
D_{1V}
D_{2V}
BS
intensity and polarization modulation
WCS pulse
Alice
intensity and polarization modulation
WCS pulse
Bob

We presented the first analytical formula for the decoy-state analysis with only a few decoy states. X.-B. Wang, Phys. Rev. A 87, 012320 (2013). [arXiv:1207.0392]



Intensity

Decoy- state method

0 → vacuum

μ_x → decoy source x

μ_y → signal source y

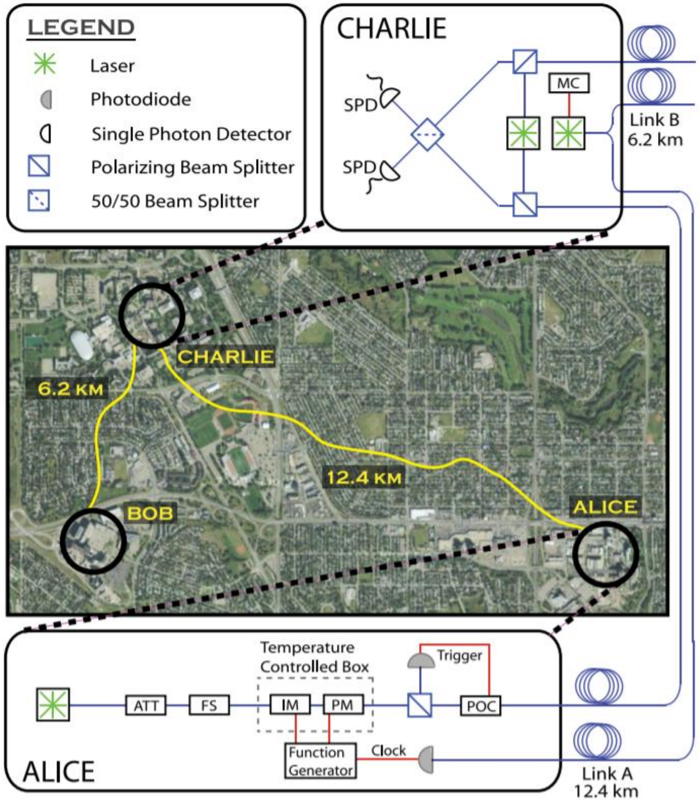
H.K. Lo et al, PRL 2011
S.L. Braunstein and S. Pirandola PRL 2011

X.-B. Wang, Phys. Rev. A 87, 012320 (2013). [arXiv:1207.0392]

Three-intensity decoy-state MDI QKD protocol

Three-intensity protocol presents the first analytical formula for decoy-state MDI QKD with only a few intensities. X.-B. Wang, Phys. Rev. A 87, 012320 (2013) [arXiv:1207.0392]

It has been applied successfully by Calgary group, Canada, in the early demonstration of MDI QKD in Phys. Rev. Lett. 111, 130501 (2013), which made "QKD secure again" as commented by *Science*. (Another MDIQKD experiment done by USTC group was published in the same issue in PRL.111, 130502)



X.-B. Wang, Phys. Rev. A 87, 012320 (2013) [arXiv:1207.0392]

Major Problems for MDIQKD in Practical application

- Low key rate
- Finite key effects

The finite key effects can be taken by the entropy analysis :

M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Nat.Commun 3, 634 (2012);

For MDIQKD, theoretical result for finite-key effects is presented by:

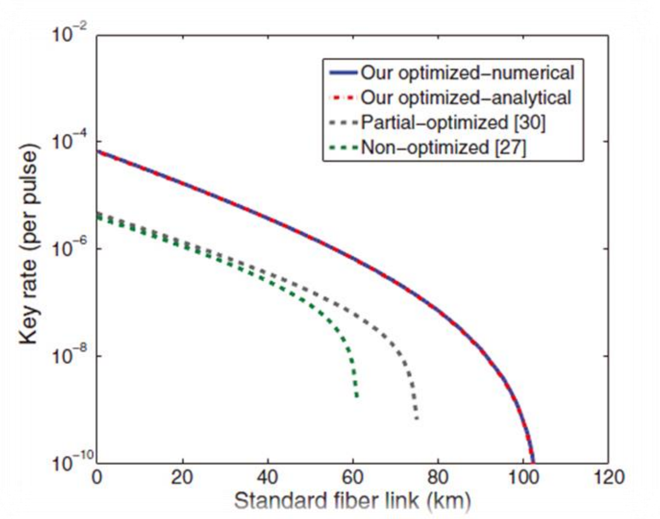
M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Nat. Commun. 5, 3732 (2014).

But due to the high error rate in the X basis (as high as 25%), the key rate is pretty low.

Solutions to major Problem for Practical application

- Global optimization in parameter choosing
- Joint constraint
- Four-intensity protocol using biased basis with full optimization

Improve the key rate of MDI QKD: choosing parameter values globally



F. Xu et al, PRA 2014

Further optimization:
vary the steps in the gradient-descent algorithm.

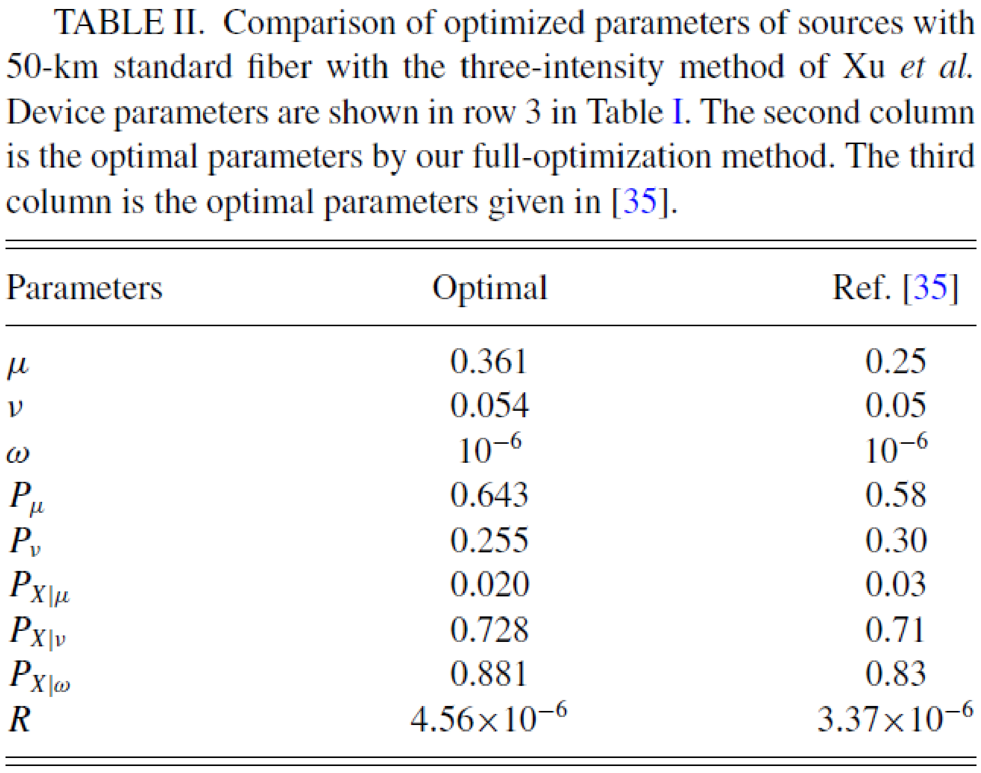
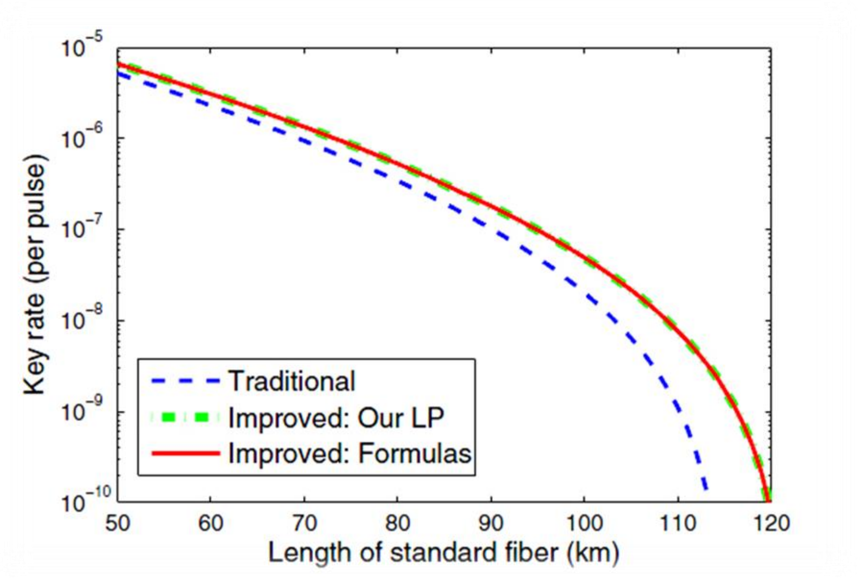


TABLE II. Comparison of optimized parameters of sources with 50-km standard fiber with the three-intensity method of Xu *et al.* Device parameters are shown in row 3 in Table I. The second column is the optimal parameters by our full-optimization method. The third column is the optimal parameters given in [35].

Parameters	Optimal	Ref. [35]
μ	0.361	0.25
ν	0.054	0.05
ω	10^{-6}	10^{-6}
P_μ	0.643	0.58
P_ν	0.255	0.30
$P_{X\|\mu}$	0.020	0.03
$P_{X\|\nu}$	0.728	0.71
$P_{X\|\omega}$	0.881	0.83
R	4.56×10^{-6}	3.37×10^{-6}

Improve the key rate of MDI QKD : joint constraints

- We can consider the data from different sources as one set and consider the statistical fluctuation for the data in the set. This adds many new constraints and makes the estimation tighter. This improves the key rate can be improved by 2 times
- Here we also choose parameter values globally

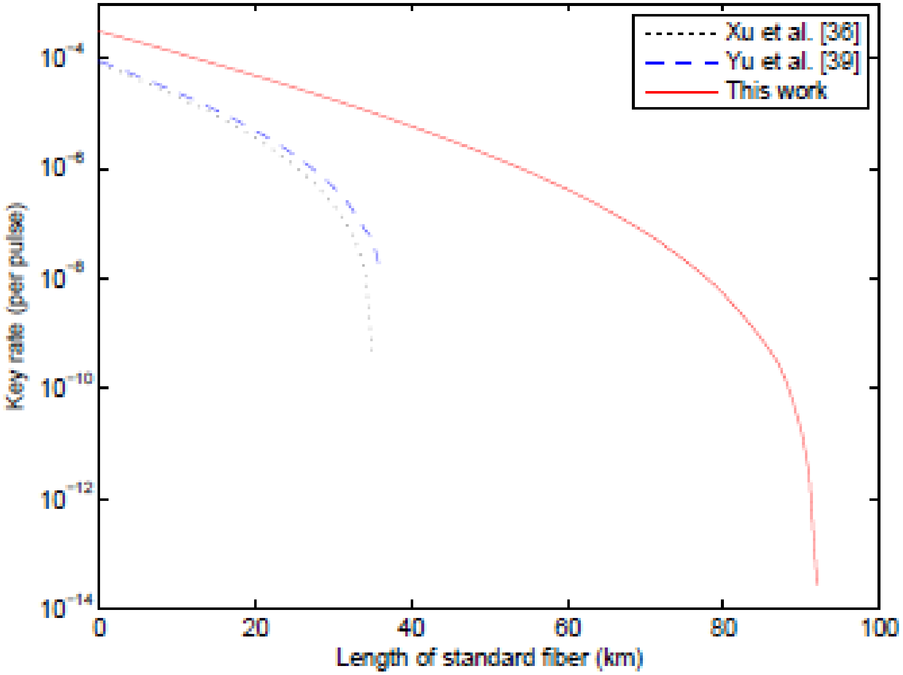


Traditional: F. Xu et al, PRA 2014
Improved: Z.-W. Yu et al, , PRA91, 032318 (2015)

Z.-W. Yu, Y.-H. Zhou, X.-B. Wang, Phys. Rev. A 91, 032318 (2015)

Most efficient protocol for practical MDIQKD: four-intensity protocol with full optimization

- Each of Alice and Bob use 4 intensities, one intensity in Z basis, three intensities in X basis including one vacuum, and two non-zero intensities in X basis. Using bits from Z basis to distill the final key
- Take global search for parameter values
- Take constraints of from finite-key effects jointly.
- Take one parameter scan for the worst-case result directly pointing to the final key rather than worst-case in each steps.



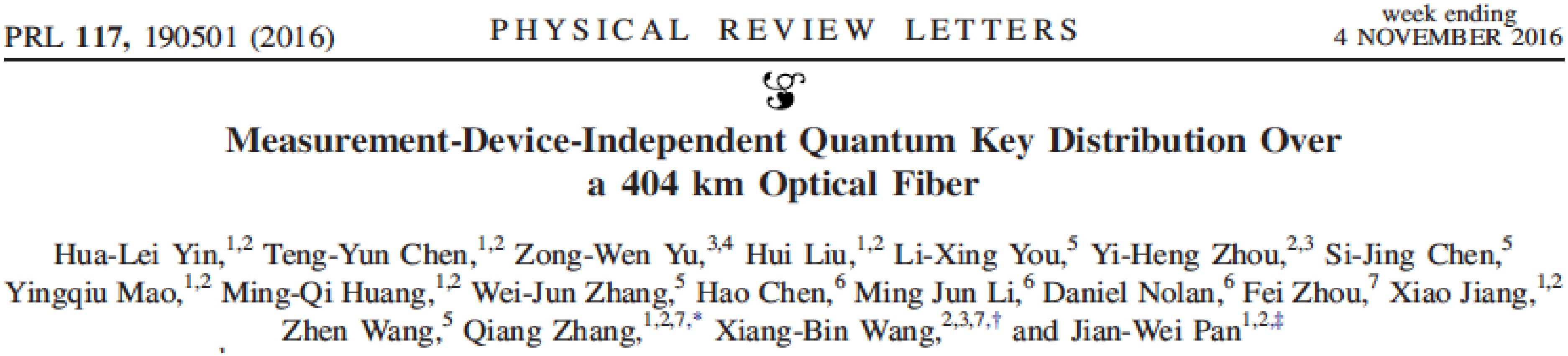
The key rate is improved greatly, by 50 to hundreds of times

Y.-H. Zhou, Z.-W. Yu, X.-B. Wang, Phys. Rev. A 93, 042324 (2016)

Improve the key rate of MDIQKD:

The four-intensity MDIQKD protocol: Y.-H. Zhou, Z.-W. Yu, X.-B. Wang, Phys. Rev. A 93, 042324 (2016) has been widely applied in the experiments:

1. High-speed MDI QKD experiment, Toshiba Cambridge Lab., Nature Photonics 10, 312 (2016).
2. 404km MDI QKD experiment, USTC, Physical Review Letters 117, 190501 (2016).
3. Rotation reference-frame-independent MDI QKD experiment, USTC, Optica 4, 1016 (2017).
4. MDI QKD digital signatures, Toshiba, Nature communications 8, 1 (2017).
5. First free-space MDI QKD experiment, USTC, Physical Review Letters 125, 260503 (2020).
6. On-chip MDI QKD experiment, University of Bristol, Optica 7, 238 (2020).
7. On-chip MDI QKD experiment, USTC, Physical Review X 10, 031030 (2020).
8. On-chip MDI QKD experiment, NTU Singapore, Physical Review Applied 14, 011001 (2020).
9. GHz MDI-QKD experiment, Toshiba Cambridge Lab., NPJ QI, 2021, 7(1): 1-6.
10. MDIQKD with malicious device, USTC, Physical Review Applied 15, 034081(2021).



PRL 117, 190501 (2016) PHYSICAL REVIEW LETTERS week ending 4 NOVEMBER 2016

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

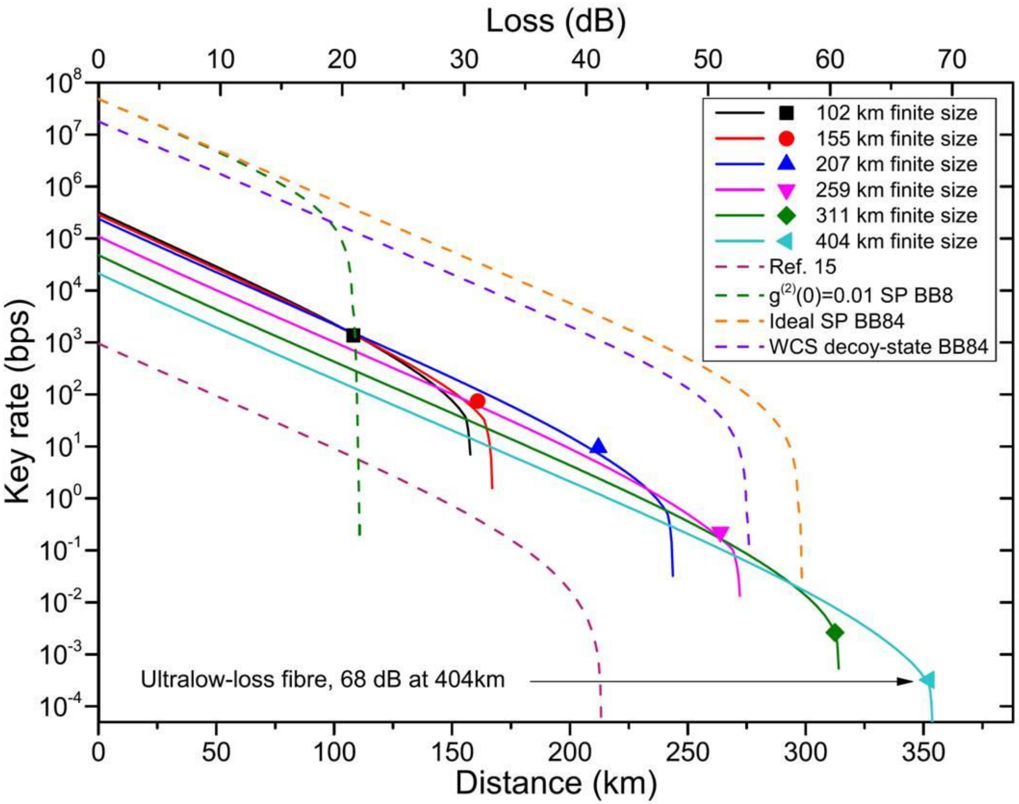
Hua-Lei Yin,[1,2] Teng-Yun Chen,[1,2] Zong-Wen Yu,[3,4] Hui Liu,[1,2] Li-Xing You,[5] Yi-Heng Zhou,[2,3] Si-Jing Chen,[5] Yingqiu Mao,[1,2] Ming-Qi Huang,[1,2] Wei-Jun Zhang,[5] Hao Chen,[6] Ming Jun Li,[6] Daniel Nolan,[6] Fei Zhou,[7] Xiao Jiang,[1,2] Zhen Wang,[5] Qiang Zhang,[1,2,7,*] Xiang-Bin Wang,[2,3,7,†]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

1) **404 km, Ultralow-loss fiber**

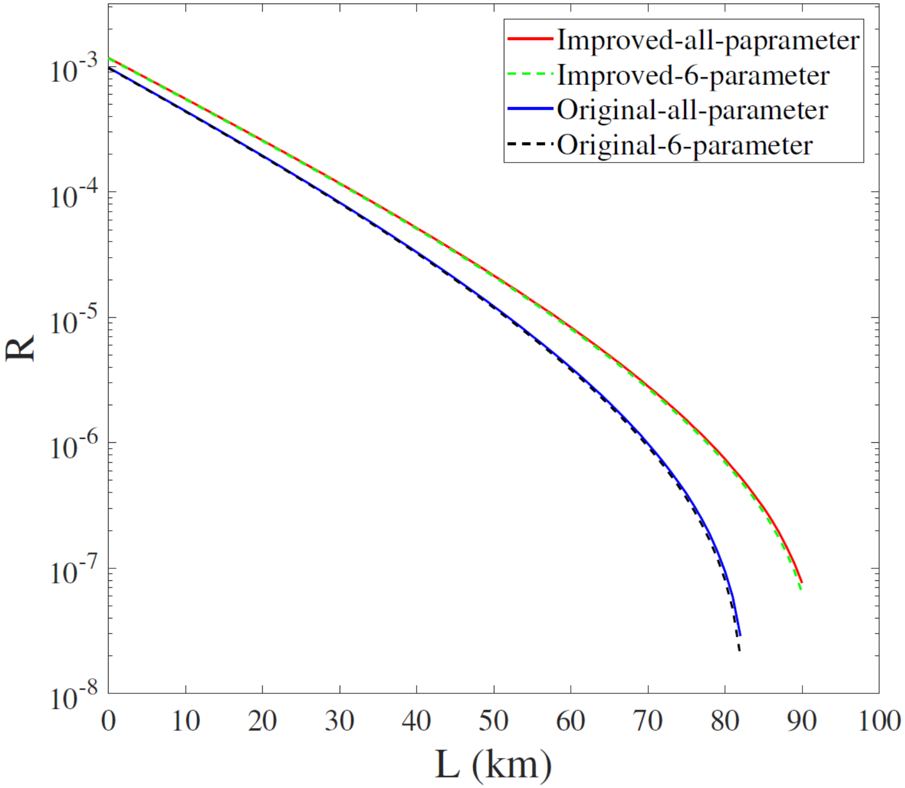
2) **311km, ordinary fiber**

3) **207km, 500 times**

4) **Break the distance limit of BB84 with perfect single-photon source**



Further improve the key rate with double-scanning method



The comparison between original and improved four-intensity protocol under the symmetric condition with 10^{11} pulses.

C. Jiang, Z.-W. Yu, X.-L. Hu, and X.-B. Wang, Physical Review A, 103, 012402 (2021).

Twin-Field (TF) QKD

The TF-QKD:

[1] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Nature (London) 557, 400 (2018) improves the key rate from $R \sim \eta$ to $R \sim \sqrt{\eta}$; breaking the PLOB bound, upper bound for repeater less QKD

The following two important variants of TF-QKD:

[2] Sending-or-not-sending (SNS) protocol: X.-B. Wang, Z.-W. Yu, X.-L. Hu, Phys. Rev. A 98, 062323 (2018)

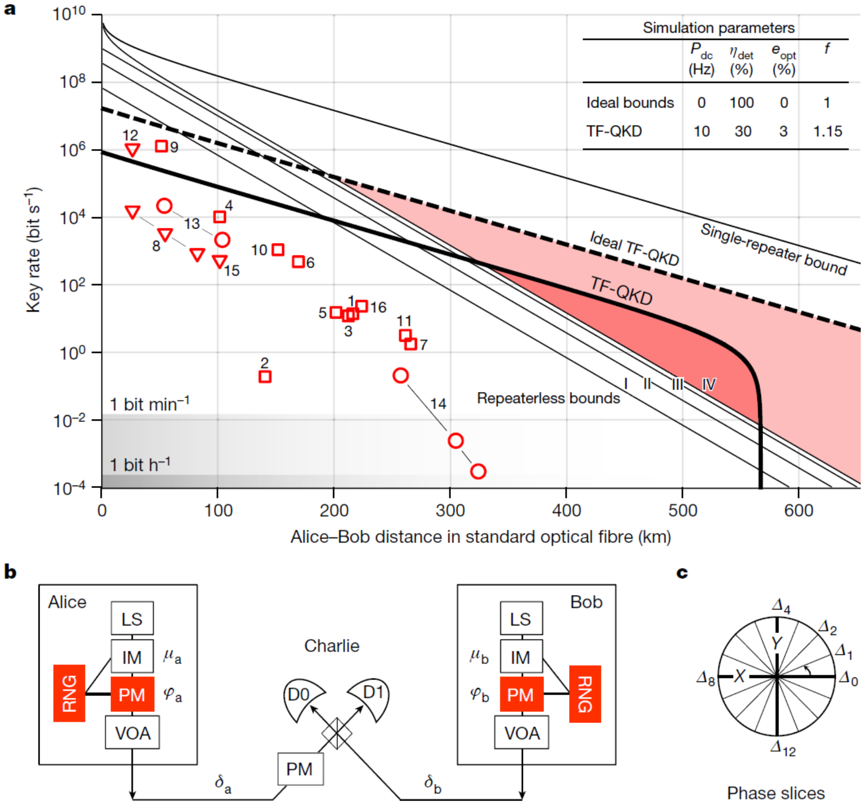
[3] CAL protocol: M. Curty, K. Azuma, and H. K. Lo, npj Quantum Inf. 5, 64 (2019)

are secure against general attacks and robust to channel noise and finite-key effects.

SNS, CAL, NPP, TF*,PM

Key rate: $R \sim \eta^2 \xrightarrow[\text{Decoy-state method}]{} R \sim \eta \xrightarrow[\text{TF protocol}]{} R \sim \sqrt{\eta}$

Twin-Field (TF) QKD



Simulation parameters

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

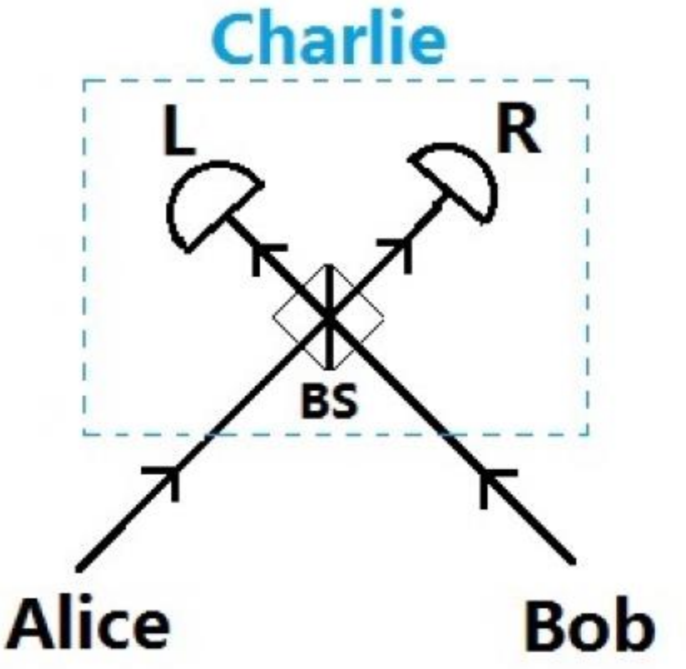
main idea: quantum relay with single-photon interference in the measurement station

Alice and Bob only need to send coherent states to Charlie.

Two properties: : improve the key rate from $R \sim \eta$ to $R \sim \sqrt{\eta}$; breaking the PLOB bound, upper bound for repeater less QKD

M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Nature (London) 557, 400 (2018).

TF-QKD through sending or not sending (SNS) protocol



Schematic picture of TF-QKD

M. Lucamarini et al, Nature 2018

Decoy state method:

Z window: Alice (Bob) decides to send out coherent state $|\alpha_Z\rangle$ to Charlie by probability p_z and decides not to send it out by probability $1 - p_z$.

X window: Alice (Bob) sends out coherent state $|\alpha_i\rangle$ by probability p_i , $i = 1,2, \ldots$, and decides not to send it out (i.e., sends out vacuum) by probability1-$\sum_i p_i$.

Encoding state :

Z window: $|01\rangle, |10\rangle$

X window: $(|01\rangle + |10\rangle)/\sqrt{2}$

$(|01\rangle - |10\rangle)/\sqrt{2}$

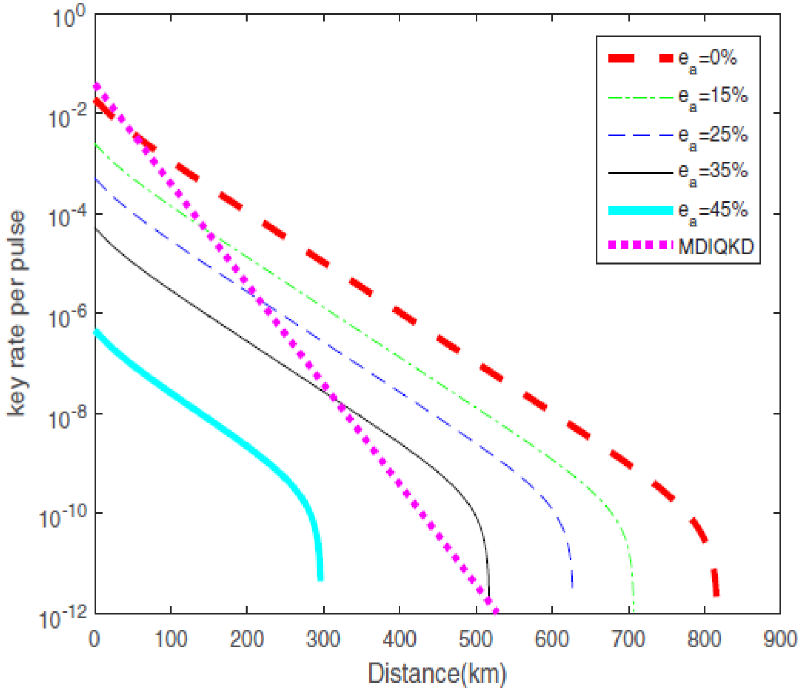
X.-B. Wang, Z.-W. Yu, X.-L. Hu, Phys. Rev. A 98, 062323 (2018)

TF-QKD: sending or not sending protocol

1) SNS protocol uses single photons in the coherent states to encode bits; The traditional GLLP model directly applies for decoy-state analysis

2) Strong fault tolerance (No interference in Z basis);

3) The secure key rate and distance is greatly increased compared with MDI protocol, the key rate at 404 km is increased by 5-6 orders of magnitude



X.-B. Wang, Z.-W. Yu, X.-L. Hu, Phys. Rev. A 98, 062323 (2018)

TF-QKD: sending or not sending protocol

The error rate can be reduced by error rejection (ER) with two-way classical communication, thus we can improve the probability of sending and hence further raise the final key rate and also the distance.

[H. Xu, Z.-W. Yu, C. Jiang, X.-L. Hu, and X.-B. Wang, Phys. Rev. A 101, 042330 (2020)]:

SNS with standard ER: Improve the key rate at longer distance regime, and improve the distance by 50 kms.

SNS with odd-parity ER (OPER): Improve the key rate in the whole distance regime by about 40%, and improve the distance by 50 kms.

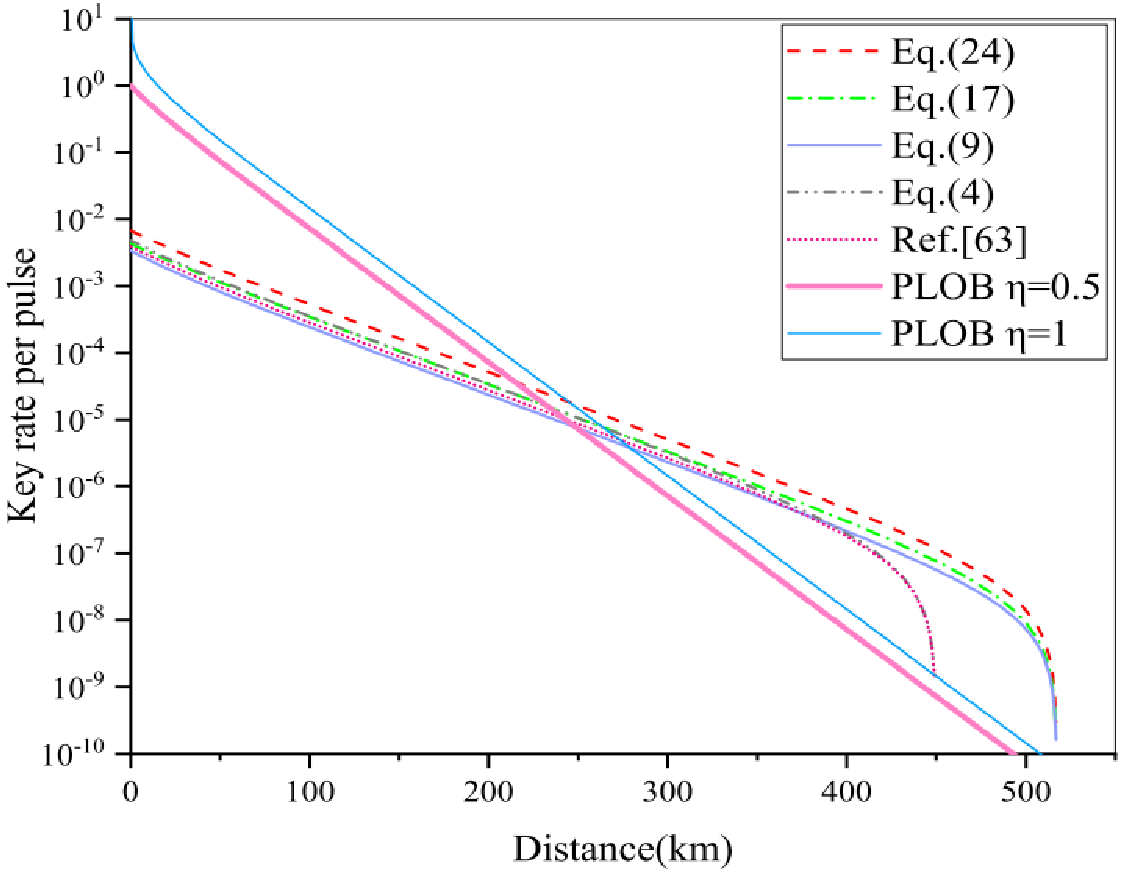
SNS actively odd parity pairing: Improve the key rate in the whole distance regime by about 80%, and improve the distance by 50 kms.

H. Xu, Z.-W. Yu, C. Jiang, X.-L. Hu, and X.-B. Wang,
Phys. Rev. A 101, 042330 (2020)

The SNS protocol also applies for the asymmetric source parameters:
X.-L. Hu, C. Jiang, Z.-W. Yu, and X.-B. Wang, **Phys. Rev. A 100, 062337 (2019)**

TF-QKD: sending or not sending protocol

[H Xu, Z.-W. Yu, C. Jiang, X.-L. Hu, and X.-B. Wang Phys. Rev. A 101, 042330 (2020)]:



Eq.(24): active odd-parity pairing (AOPP)
Eq.(17): random pairing with odd-parity sifting
Eq.(9): random pairing
Eq.(4): refined structure
Ref. (63): the original SNS protocol

TF-QKD: finite-key effects

1, For SNS protocol with original post data processing, the finite key effects are studied in

C. Jiang, Z.-W. Yu, X.-L. Hu, and X.-B. Wang, **Phys. Rev. Applied, 12**, 024061 (2019).

And also:

Z.-W. Yu, X.-L. Hu, C. Jiang, H. Xu, and X.-B. Wang, **Sci. Rep. 9**, 3080 (2019).

2, For SNS protocol with error rejection in post data processing, the finite-key effects are studied in:

C. Jiang, X.-L. Hu, H. Xu, Z.-W. Yu, and X.-B. Wang, **New J. Phs, 22**, 053048 (2020).

C. Jiang, X.-L. Hu, Z.-W. Yu, and X.-B. Wang**, New J. Phys, 23**, 063038 (2021).

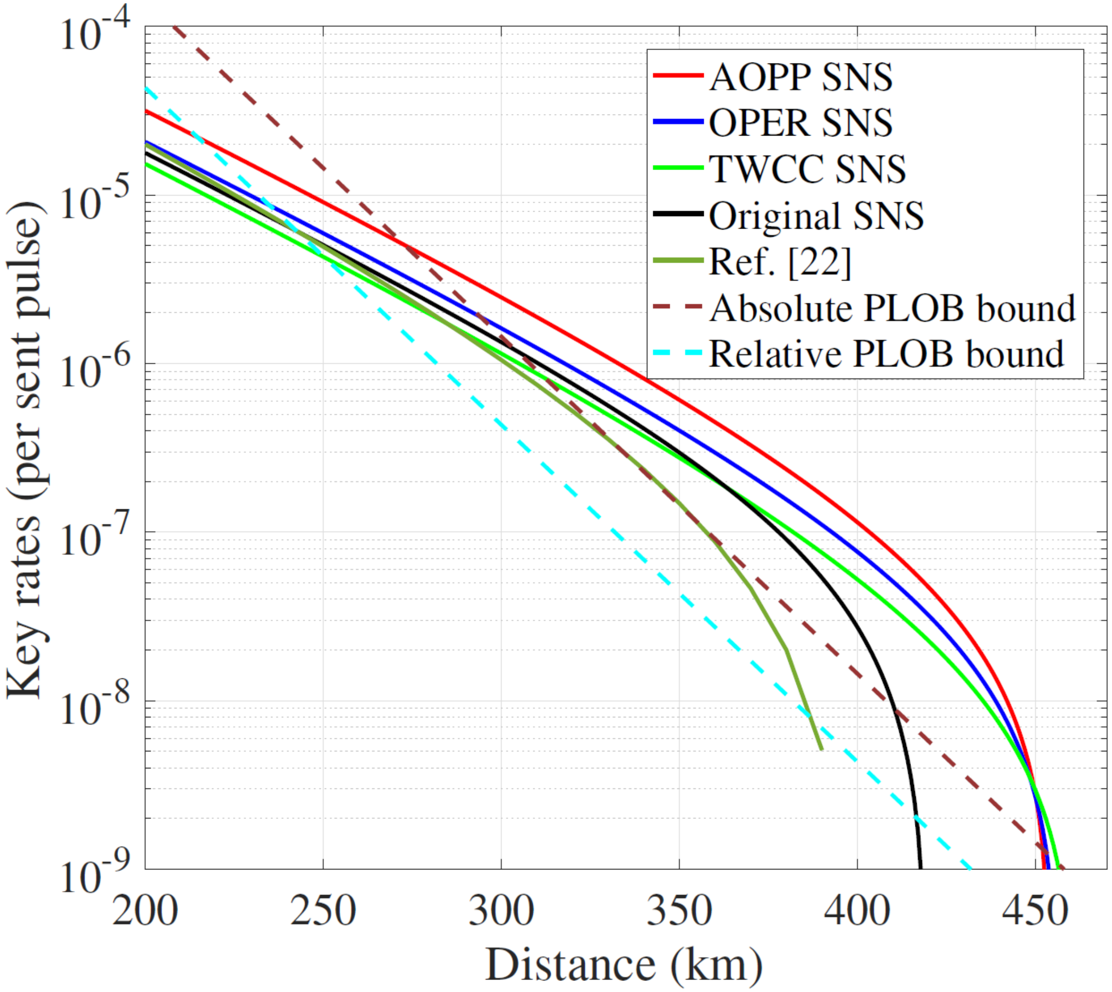
3, MSK result:

K. Maeda, T. Sasaki, and M. Koashi, Nature Communications 10, 3140 (2019).

4, For CAL protocol, the finite key effects in

Currás-Lorenzo, G., Navarrete, Á., Azuma, K., Kato, G., Curty, M., & Razavi, M.
NPJ Quantum Information, 7(1), 1-9 (2021).

TF-QKD: finite-key effects



The key rates of SNS protocol and its variants.

Ref.[22]:K. Maeda, T. Sasaki, and M. Koashi, Nature Communications 10, 3140 (2019).

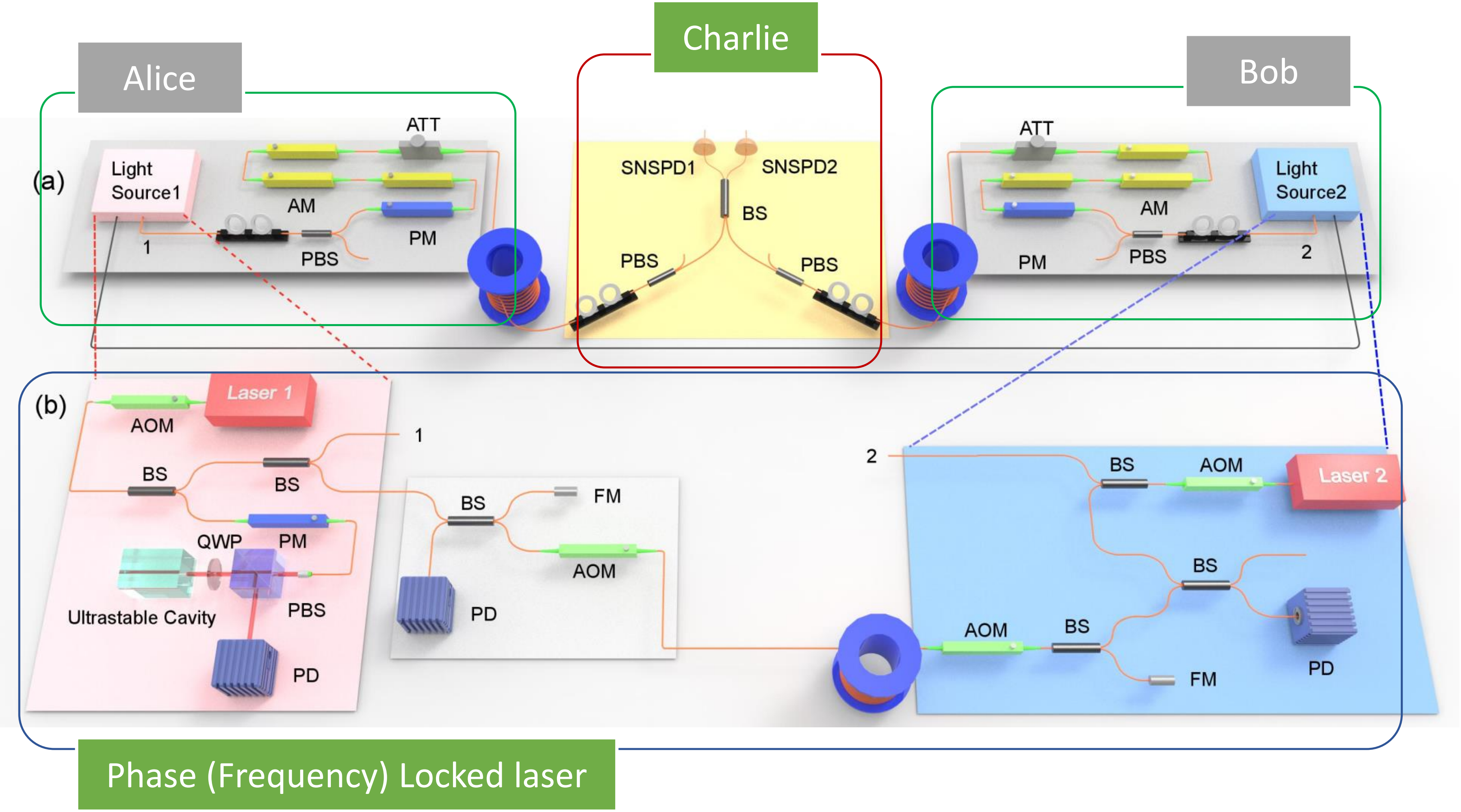
TF-QKD through sending or not sending (SNS)： Experiments

The SNS protocol for TFQKD has been implemented successfully in many experiments, including 4 of them exceeding 500 km distance, one of them exceeding 600km distance, 2 field tests through commercial optical fiber between metropolitans JINAN and QINGDAO in Shandong province, China. The 2 field tests by SNS protocol are the only field tests of TFQKD so far.

JNAN:
Population： 8.9million
Area:10244 km square
Research Institute there: JIQT
(Jinan Institute of Quantum Technology)

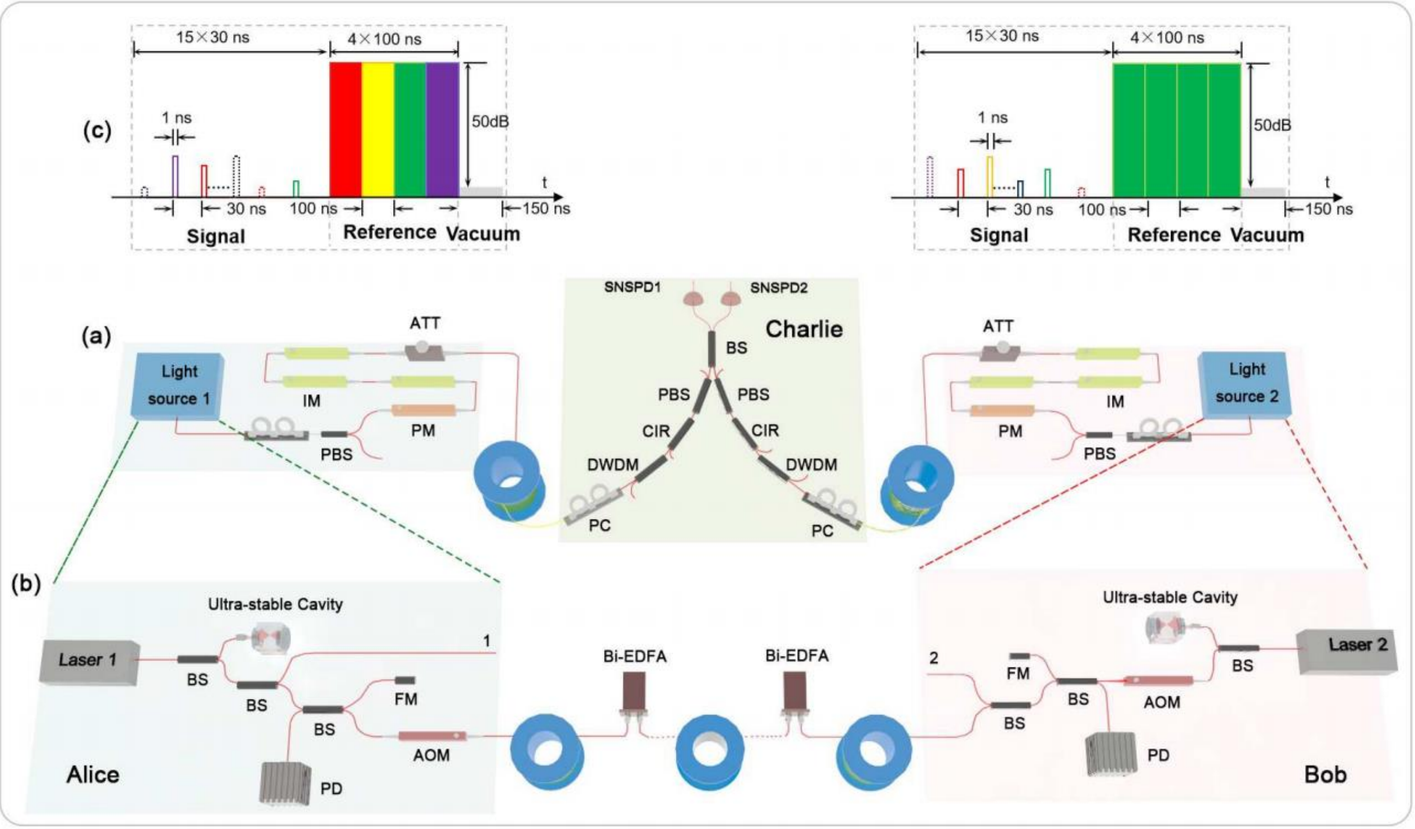
Qingdao:
Population: 7.40million
Area:11282 km square

TF-QKD experiments through sending-or-not-sending (SNS): Experiment 1: the first real-system TFQKD



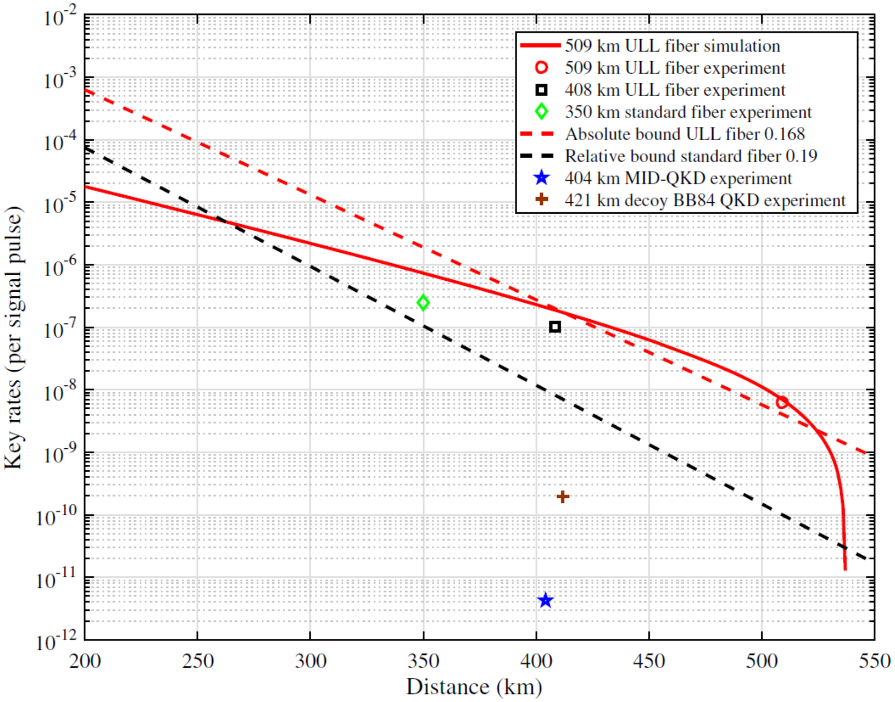
USTC group: Y Liu et al, Physical Review Letters, 123, 100505 (2019)

TF-QKD experiments through sending-or-not -ending (SNS)：
Experiment 2: long-distance experiment （509 km）



USTC， J.P. Chen et al, Physical Review Letters, 124, 070501 (2020).

TF-QKD experiments through sending-or-not -ending (SNS)：
Experiment 2: long-distance experiment （509 km）



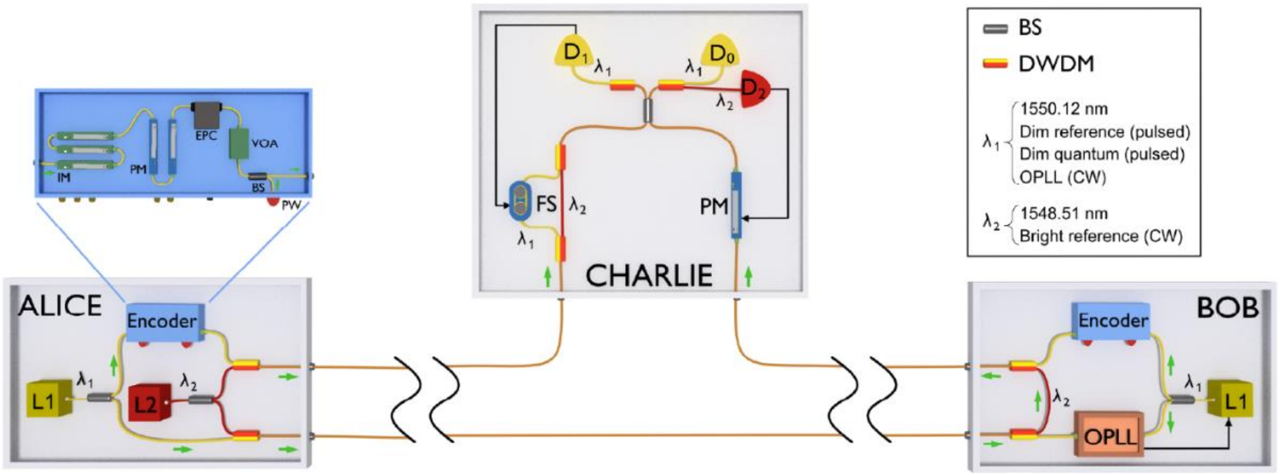
Key rates with standard TWCC

Distance	Key rate	Absolute PLOB bound
350 km	6.12×10^{-7}	3.23×10^{-7}
408 km	3.07×10^{-7}	2.02×10^{-7}
509 km	1.54×10^{-8}	4.05×10^{-9}

Key rates with OPER

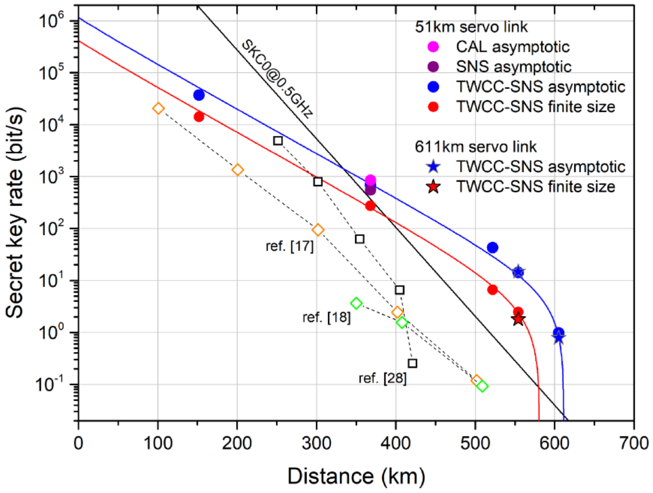
Remark: In this experiment, we have also done TF-QKD experiment over 408 km by SNS protocol, we obtain a key rate 4-magnitude-order higher than that our MDIQKD experiment taken in 2016.

TF-QKD experiments through sending-or-not-sending (SNS): Experiment 3 and 4: (550km and 600km)

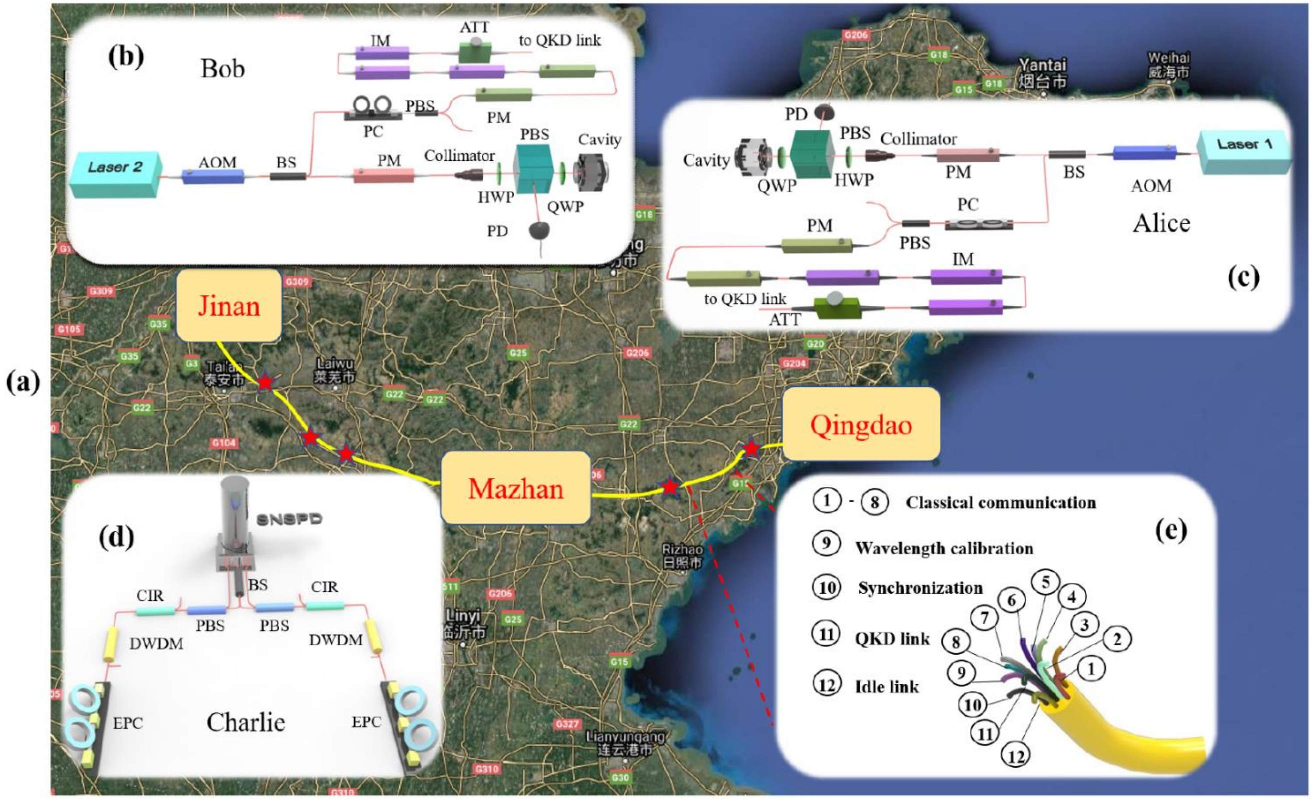


Adopting the SNS protocol, Toshiba Cambridge Laboratory has successfully implemented the 550 km TF-QKD and 600km TF-QKD in laboratory.

M. Pittaluga et al, Nat. Photon. 15, 530(2021)



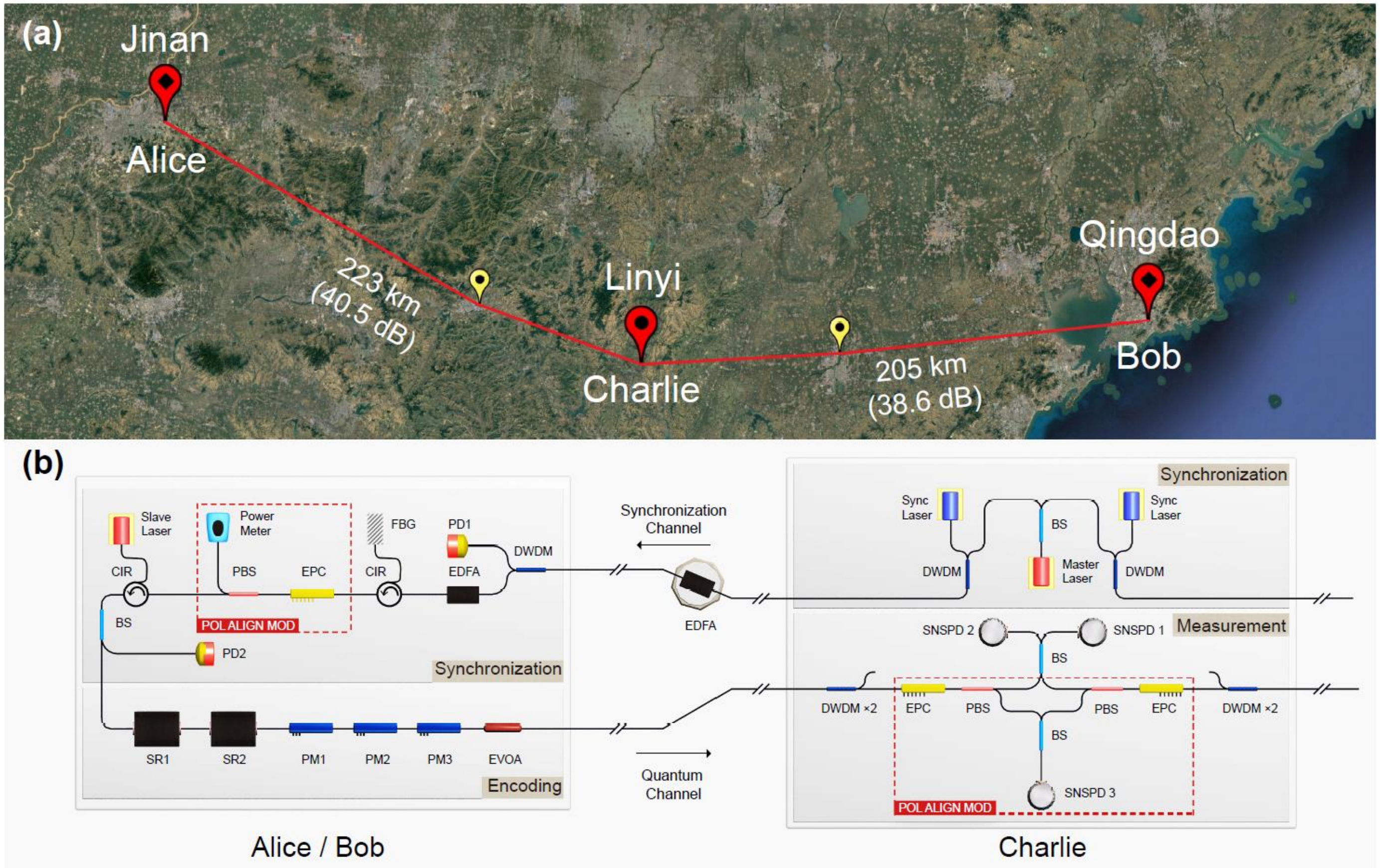
TF-QKD experiments through sending-or-not-sending (SNS)： Experiment 5: 511 km field test between Jinan and Qingdao



Adopting the SNS protocol, USTC team has successfully implemented the 511 km field test（Nat. Photon. 15, 570–575 (2021)）.

TF-QKD experiments through sending or not sending (SNS)：

Experiment 6: 428 km field test between Jinan and Qingdao



Adopting the SNS protocol, USTC team has successfully implemented the 428 km field test（Phys. Rev. Lett., 126, 250502 (2021)）.

TF-QKD experiments through sending-or-not-sending (SNS)：Field test between Metripolitans Jinan and Qindao

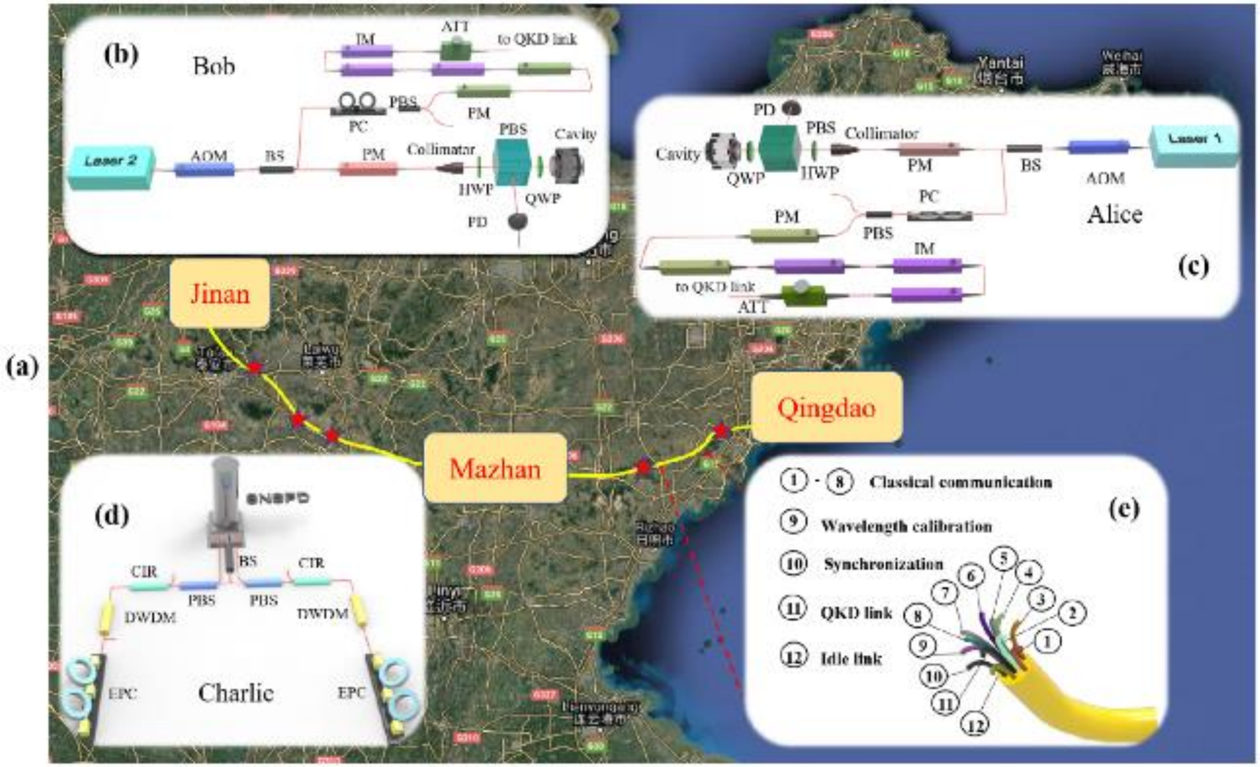
济南量子技术研究院

JIQT

Jinan Institute of Quantum Technology

JNAN:
Provincial capital of Shandon Province
Population： 8.9million
Area:10244 km square
Research Institute there: JIQT
(Jinan Institute of Quantum Technology)

Qingdao:
Population:
7.40million
Area:
11282 km square



Summary of Recent TF-QKD experiments （1）
Long-distance experiments

Protocol	SNS	SNS	SNS	SNS	PM	SNS
Distance	605	550	511	509	502	428
Consider the finite key effect ?	No	Yes	Yes	Yes	Yes	Yes
Exceed the PLOB bound ?	Yes	Yes	Yes	Yes	No	Yes
Group/year	Toshiba /2021	Toshiba/ 2021	USTC/ 2021	USTC/ 2020	USTC/ 2020	USTC/ 2021

Note: So far, there are five on-earth QKD experiments exceeding the distance of 500 kms. Four of them are done by SNS protocol. They are the four longest-distance experiments.

1. **SNS**: sending-or-not-sending protocol of TFQKD [X.-B. Wang, Z.-W. Yu, X.-L. Hu, Phys. Rev. A 98, 062323 (2018)]

2. **PLOB bound**: Theoretical limit for key rate of repeaterless QKD [S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nature Communications 8, 15043 (2017).] There exists other key rate bounds such as the TGW bound.

3. Prior to these, the longest distance on earth was 421km for QKD, by **H. Zbinden** group, in PRL 121(19), 190502 (2018); 404km for **MDIQKD** by **J.W. Pan** group, in PRL 117, 190501 (2016).

4. The USTC experiments of 511km and 428km by SNS protocol are **field test** QKD between metropolitans Jinan to Qingdao.

Summary of Recent TF-QKD experiments （2）

Protocol	SNS & CAL	SNS	NPP	CAL	SNS	CAL
Distance	Proof-of-principle	300	300	Proof-of-principle	408	Proof-of-principle
Consider the finite key effect ?	No	Yes	No	No	Yes	Yes
Exceed the PLOB bound ?	Yes	Yes	Yes	Yes	Yes	Yes
Group/year	Toshiba/ 2019	USTC/ 2019	USTC/ 2019	Torento/ 2019	USTC/ 2020	Torento/ 2021

Note

1. **SNS**: sending-or-not-sending protocol of TFQKD by X.-B. Wang, Z.-W. Yu, X.-L. Hu, Phys. Rev. A 98, 062323 (2018)

2. **CAL**: TFQKD protocol by M. Curty, K. Azuma, and H. K. Lo, npj Quantum Inf. 5, 64 (2019);
   NPP: TFQKD protocol by C.H. Cui, ZQ Yin et al, Phys. Rev. Appl. 11, 034053 (2019).

Summary of recent TFQKD experiments 3: **Field test of TF-QKD experiments**

Protocol	SNS	SNS
Distance	511	428
Consider the finite key effect	Yes	Yes
Exceed the PLOB bound	Yes	Yes
Group/year	**USTC/2021**	**USTC/2021**

Both experiments are implemented by our SNS protocol. So far they are the only field test experiments for TFQKD. The field test results conclude that TFQKD is feasible for practical application.

Side-channel-free quantum key distribution

An important application of the idea of sending-or-not-sending

Side Channel Space:

The subspace except the encoding space, such as the frequency spectrum, the emission time, the spatial anhular momentum, wave shape of pulses and so on. The security in the operational space does not guarantee the security in the whole space.

Side-channel is inevitable given realistic sources.

By sending or not sending a coherent state, we can construct a side channel free (SCF) protocol where we don't have to worry about any imperfection of the source state in the side channel space, we only need a correct state in the operational space (photon number space).

The key idea of SCF protocol： Assume there is an ideal (virtual) source P and a realistic source S. If states of source P can be mapped into that of S by a quantum process M, then the protocol with real source is secure provided that it is secure with the virtual source.

X.-B. Wang, X.-L. Hu, Z.-W. Yu, Physical Review Applied, 12, 054034 (2019)

Side Channel Free (SCF) QKD through SNS protocol

The SCF QKD can be made by the idea of sending-or-nit sending.

If in the protocol Alice and Bob only decide sending or not-sending a coherent states, there exists a unitary transformation to map ideal source states the real source states in the whole space, provided that the two source states have the same probability distribution in photon number space (the operational space).

$$|0\rangle \rightarrow |0\rangle$$
$$|\alpha_A\rangle \rightarrow e^{-\mu/2}|0\rangle + \sqrt{1-e^{-\mu}}|\psi_A(\tilde{\alpha}_A)\rangle$$
$$|\alpha_B\rangle \rightarrow e^{-\mu/2}|0\rangle + \sqrt{1-e^{-\mu}}|\psi_B(\tilde{\alpha}_B)\rangle$$

where $|\alpha_k\rangle = e^{-\mu/2}|0\rangle + \sqrt{1-e^{-\mu}}|\tilde{\alpha}_k\rangle, k = A, B$, and $|\psi_A(\tilde{\alpha}_A)\rangle$ and $|\psi_B(\tilde{\alpha}_B)\rangle$ are states in the whole space, containing the side-channel information.

This means that the protocol with real source states must be secure if it is secure with virtual idea source. Because Eve can also take the unitary transformation by pretending channel property even in the case we use the virtual ideal source.

Side Channel Free (SCF) QKD through SNS protocol

Since the security of real states is equivalent to the security of perfect states, we now only need to consider the source states in operational space $\{|0,\alpha_B\rangle, \ |\alpha_A,0\rangle, \ |0{,}0\rangle, \ |\alpha_A,\alpha_B\rangle\}$

Such states contain (virtual) sub-source states

$\{|0,\alpha_B\rangle, \ |\alpha_A,0\rangle, \ \ |\chi^+\rangle = (|0,\alpha_B\rangle + \ |\alpha_A,0\rangle) \ /\mathrm{N}_+\}$

And the security with these states can be proven strictly.

The phase error rate in the real protocol can be estimated by worst-case study.

Side Channel Free (SCF) QKD through SNS protocol

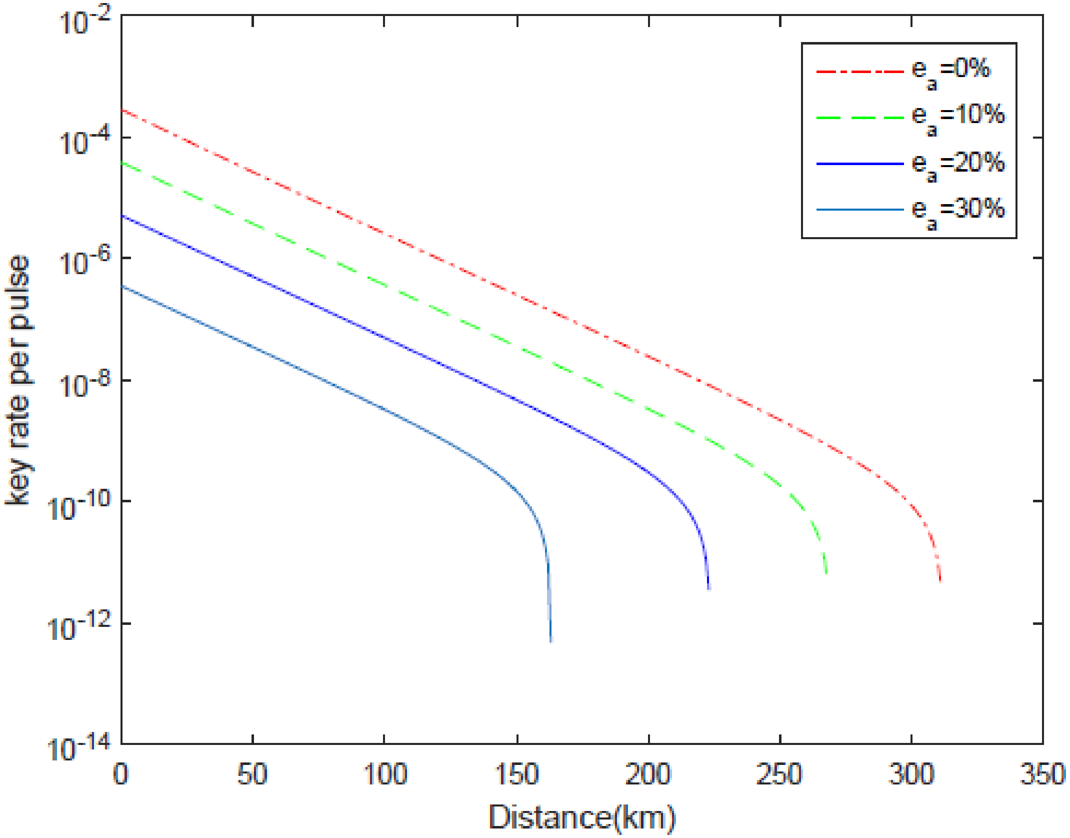
Conclusion: the protocol is secure if we can prepare exact vacuum in the operational space for those time windows of not-sending and Eve cannot attack inside Alice and Bob's labs.

Security level comparison:

Compared with the DIQKD, our SCF protocol is stronger in the measurement part: it is MDI security, say, it is secure even though Eve controls the detectors. However SCF is not source device independent though it is source side channel free. The secure distance can reach more than 100 kms by existing technology.

Our SCF QKD protocol has been experimentally implemented over a distance of 50 kms by USTC group.

TF QKD protocol—SCF protocol



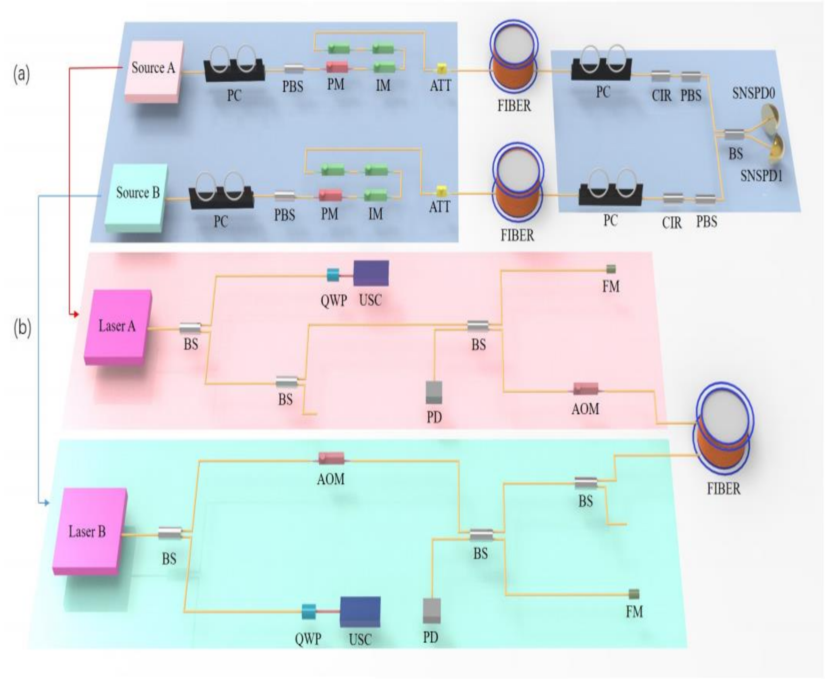
X.-B. Wang, X.-L. Hu, Z.-W. Yu, Physical Review Applied, 12, 054034 (2019)

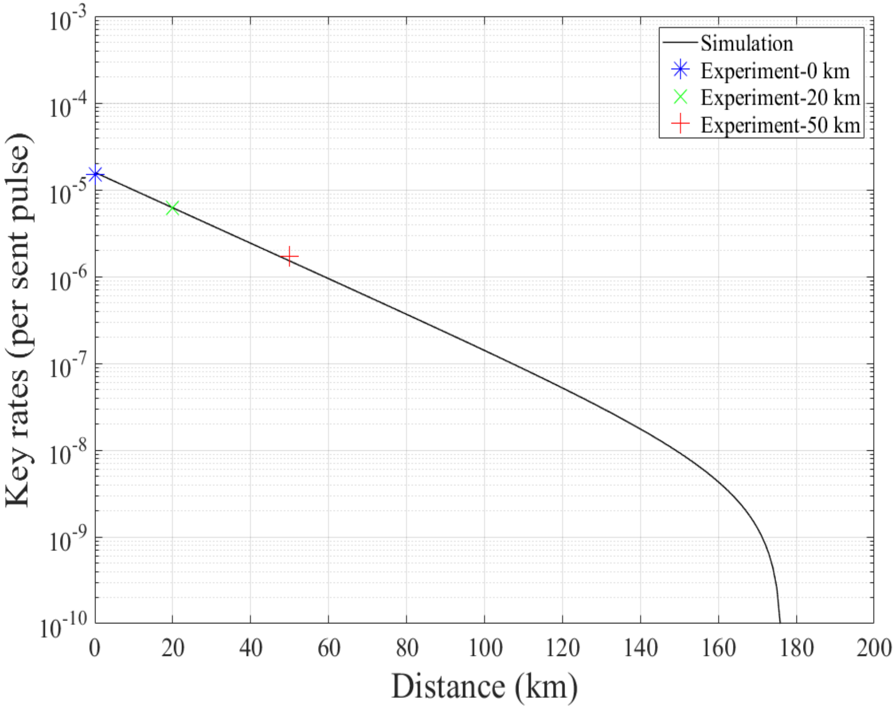
The comparison of different QKD protocols

Protocol	MDI-QKD	TF QKD	SCF QKD	DI QKD
Measurement device independent	Yes	Yes	Yes	No
Source independent	No	No	No	Yes
Source side channel free	No	No	Yes	Yes
Achievable Distance	400 km	>600 km	>200 km	<10 km

X.-B. Wang, X.-L. Hu, Z.-W. Yu, Physical Review Applied, 12, 054034 (2019)

The experiment of SCF protocol





Zhang C, Hu X L, Chen J P, et al. arXiv preprint arXiv:2103.06058, 2021.

THANK YOU!