Quantum
Physics & Quantum Information

JIQT

Recent Progress of Quantum Communication in China

Qiang Zhang

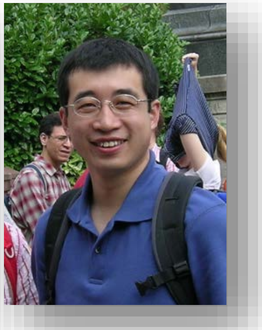
University of Science and Technology of China

Quantum Physics & Quantum Information Devision

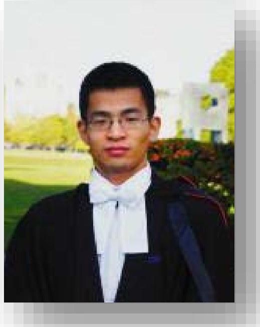
Jianwei Pan

Zengbing Chen

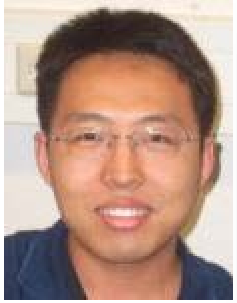
Kai Chen


Shuai Chen

Yuao Chen


Chaoyang Lu

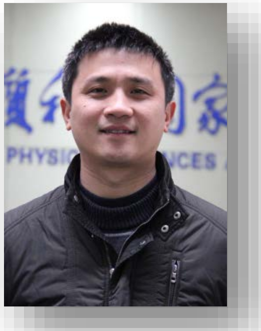
Youjin Deng

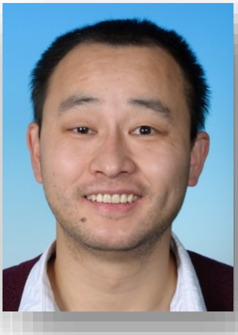

Xiaohui Bao

Qiang Zhang

Zhensheng Yuan

Jun Zhang


Chengzhi Peng


Bo Zhao

Tengyun Chen

Content

- Research in the Lab
- Field test & Practical quantum network
- Future: Quantum Backbone and Satellite

Quantum Key Distribution

Classical Encryption

Nowadays secure key → Based on computational complexity → Computational Complexity security

“One-time pad” key → Algorithm independent → distribution may not secure

→ Cannot decode

BB84: C.H. Bennett and G. Brassard, “Quantum cryptography: public key distribution and coin tossing”

Quantum Key Distribution

x Mission Impossible

Without destroy initial state

Unknown quantum state

Copy to another quantum system

→

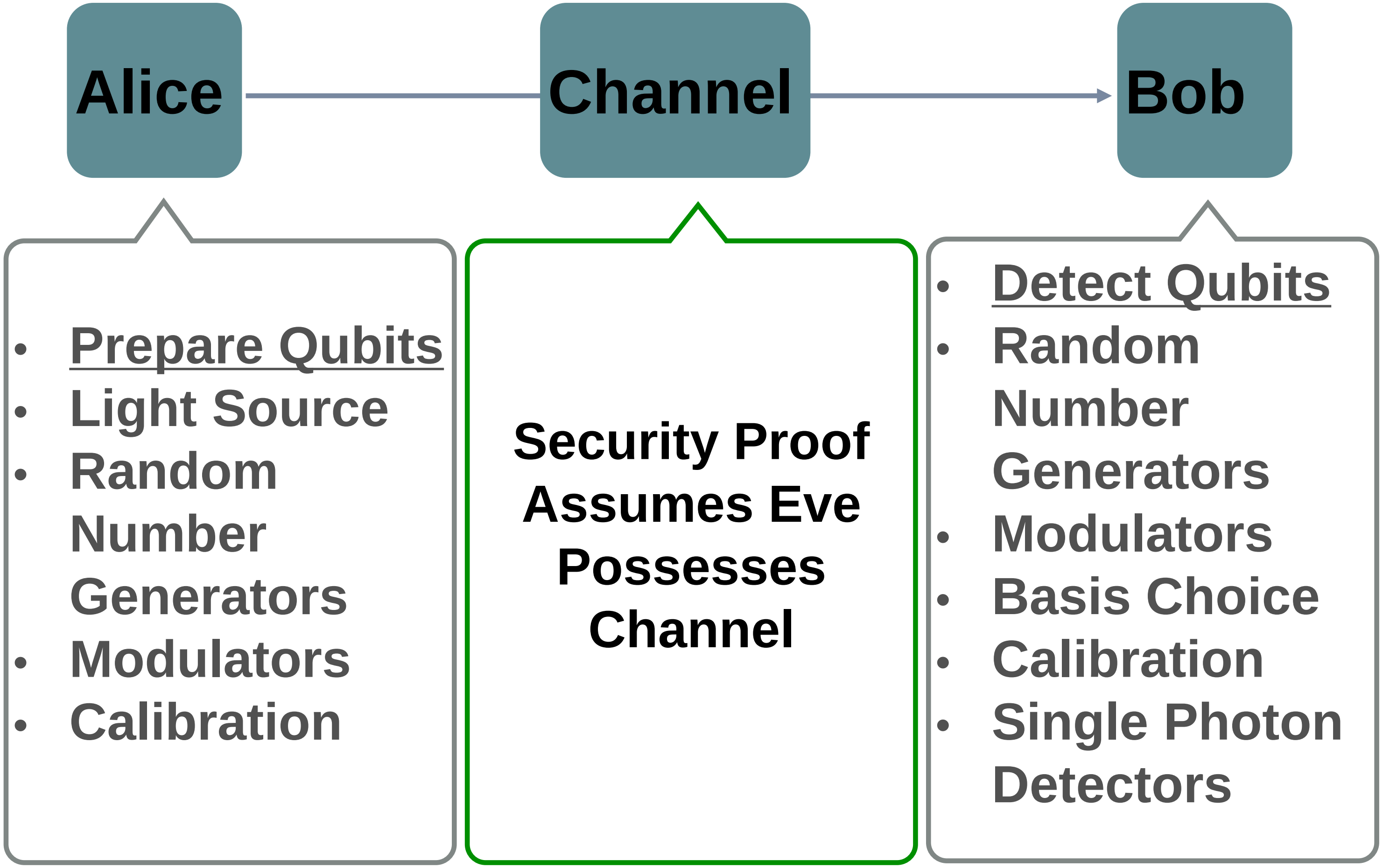
Information theoretical security

E91: A.K.Ekert, “Quantum cryptography based on Bell’ s theorem”

Single photon can NOT be cloned

can NOT be separated !

System with realistic devices



Alice

Channel

Bob

- Prepare Qubits
- Light Source
- Random Number Generators
- Modulators
- Calibration

Security Proof Assumes Eve Possesses Channel

- Detect Qubits
- Random Number Generators
- Modulators
- Basis Choice
- Calibration
- Single Photon Detectors

Source

Alice → Channel → Bob

- Prepare Qubits
- Light Source
- Random Number Generators
- Modulators
- Calibration

Decoy State ✓

Weak Coherent Source

USD ⚠

Unambitious State Measurement

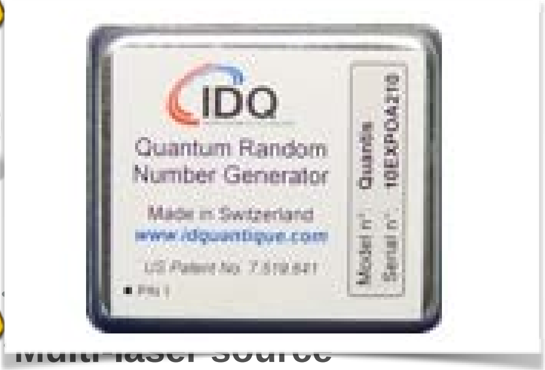
QRNG ✓

State Prepare ⚠

Multi-laser source

Imperfect modulation

Side channel

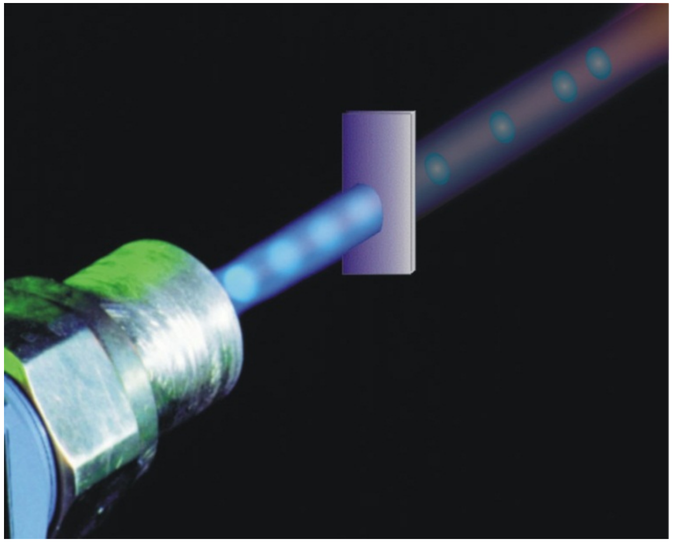


Weak Coherent State and Decoy State Method

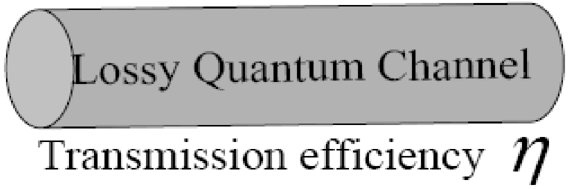
Weak coherence pulse

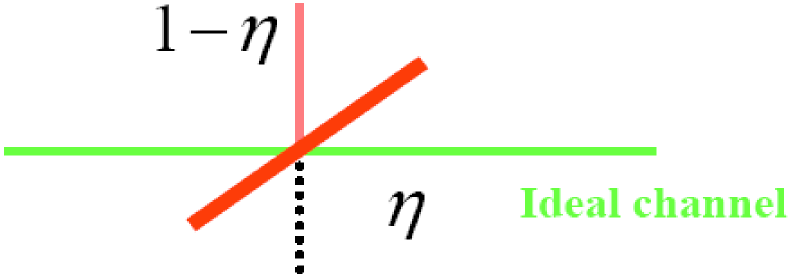
$$|\psi\rangle \sim \sum_{n=0}^{\infty} \frac{p^n}{\sqrt{n!}}|n\rangle \xrightarrow{p\ll 1} |0\rangle + p|1\rangle$$

Two identical photons per pulse with probability *P*^{2}/2



Photon number splitting attack (PNS)



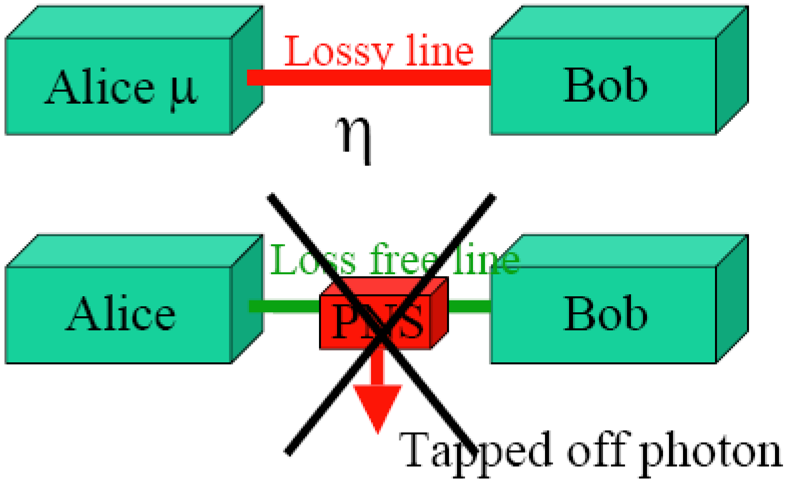


Weak Coherent State and Decoy State Method

Faking correct photon number statistics requires knowledge of μ!

choose:
$\mu_1, \mu_2, \mu_3, \ldots$

rule out
PNS via
statistics



- **Theory**

  Hwang, PRL 91, 057901 (2003)

  Wang, PRL 94, 230503 (2005)

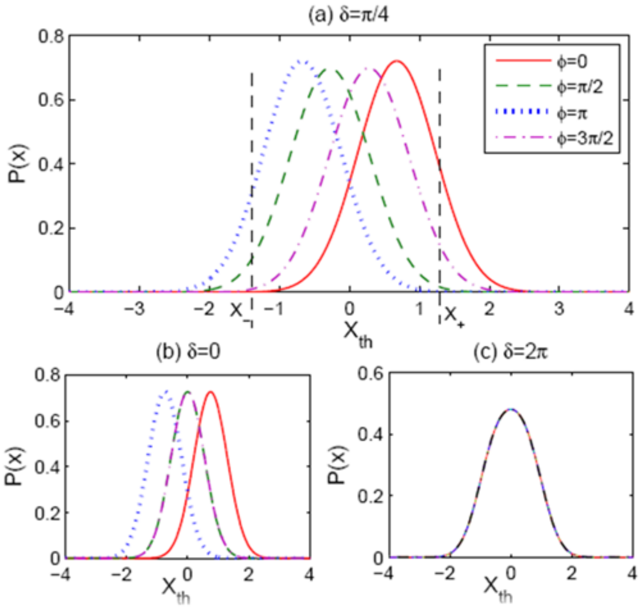
  Lo *et al.*, PRL 94, 230504 (2005)

- **Experiment**

  200km:

  Liu *et al.*, Optics Express 18, 8587 (2010)

Modulators and Passive Decoy



Frequency shift due to intensity modulation

Side channel exists!

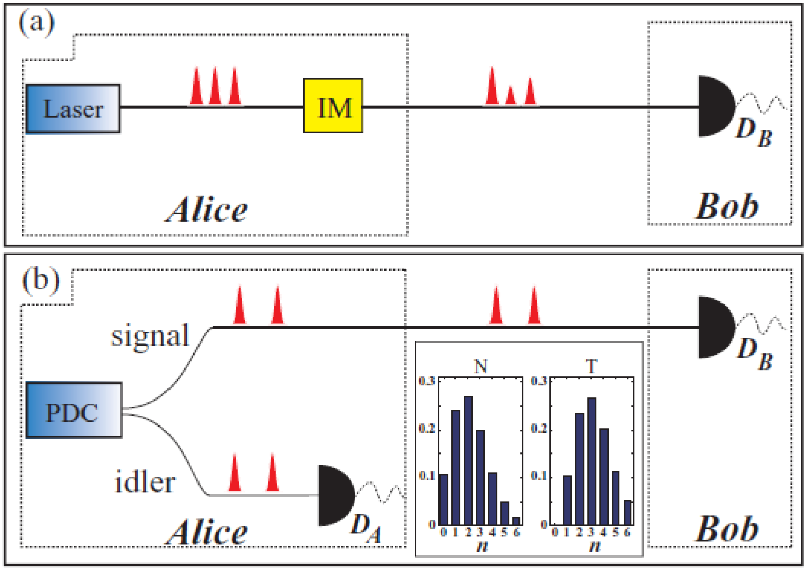
- **Theory**

  Mauerer & Silberhorn, PRA 75, 050305(R) (2007).

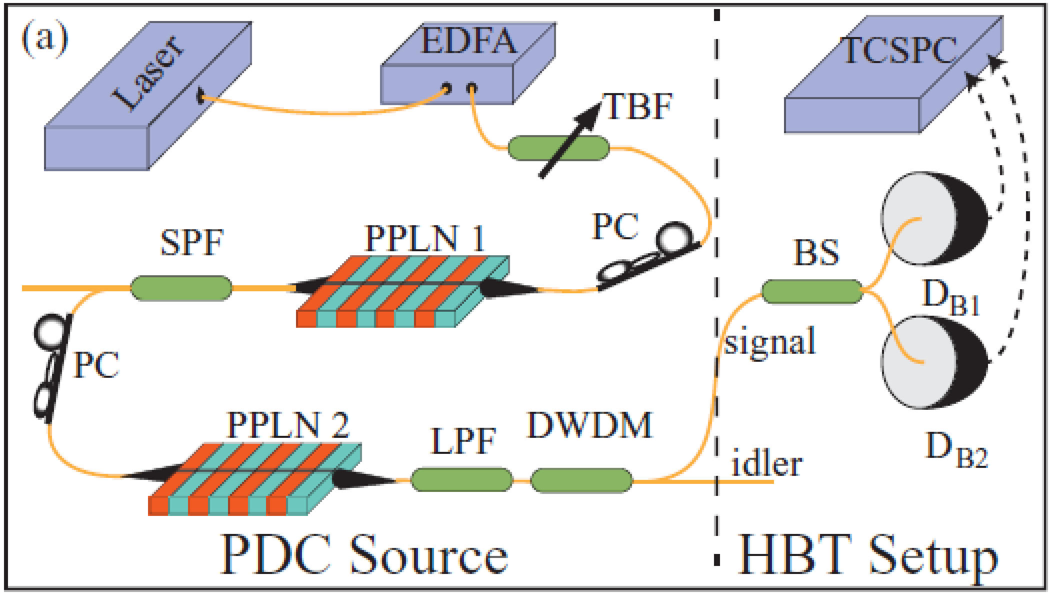
  Adachi et al., PRL 99, 180503 (2007).

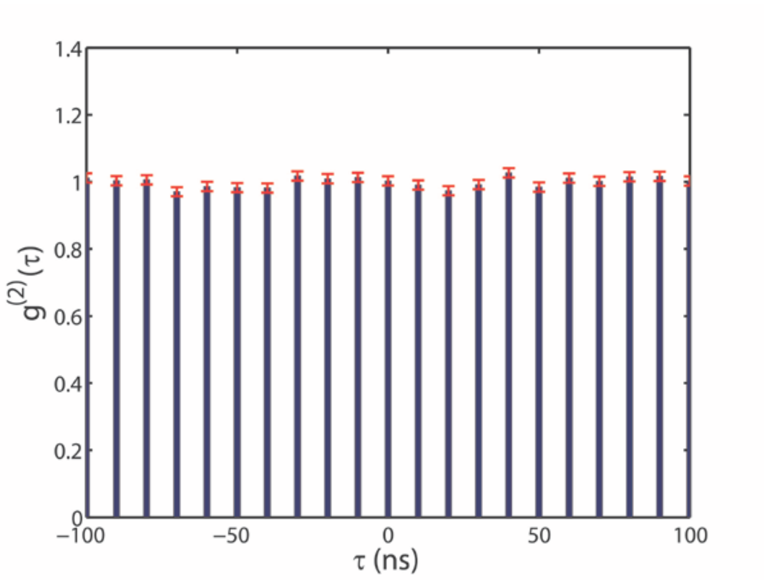
- **Experiment**

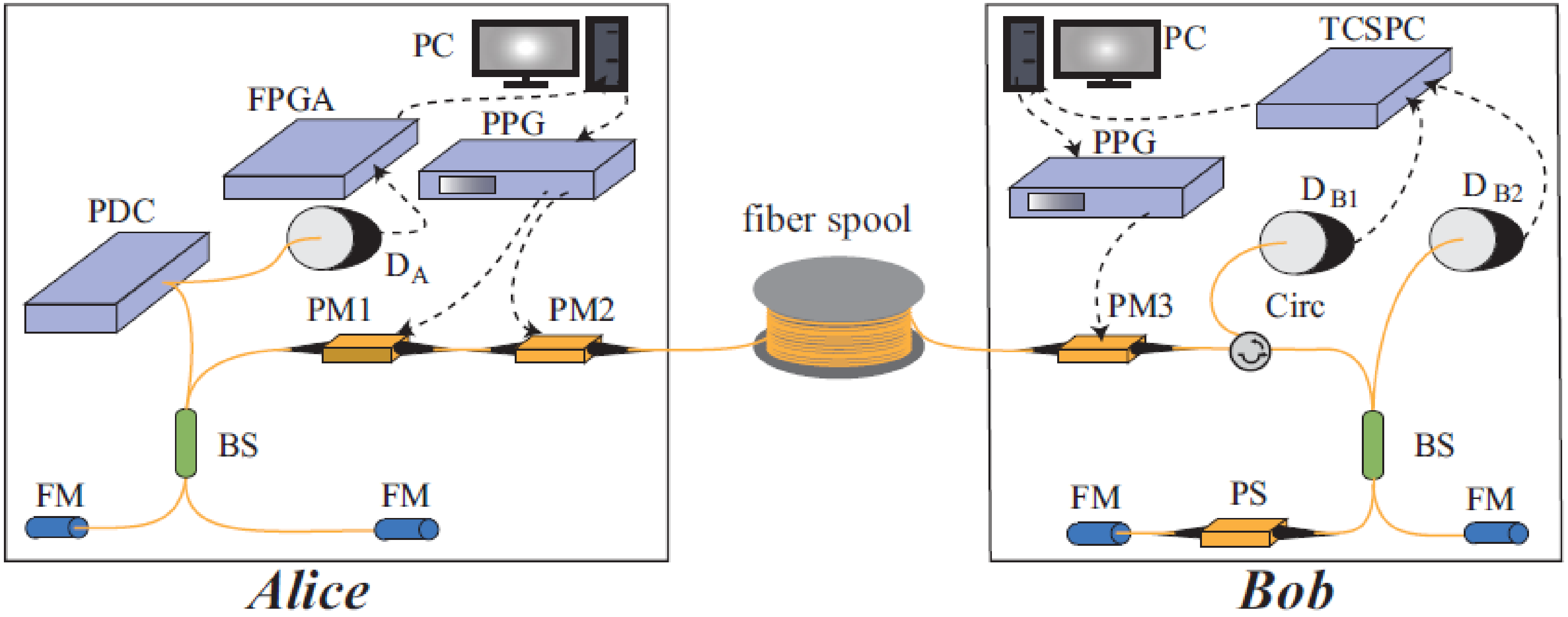
  ?



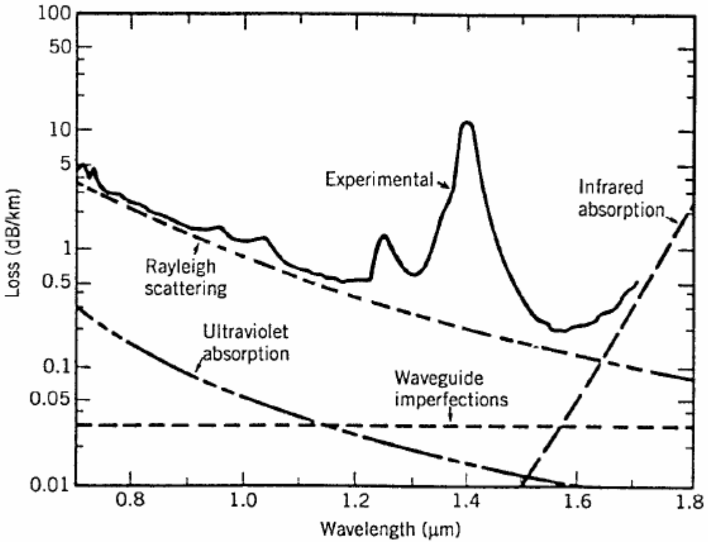
Passive Decoy QKD Experiment

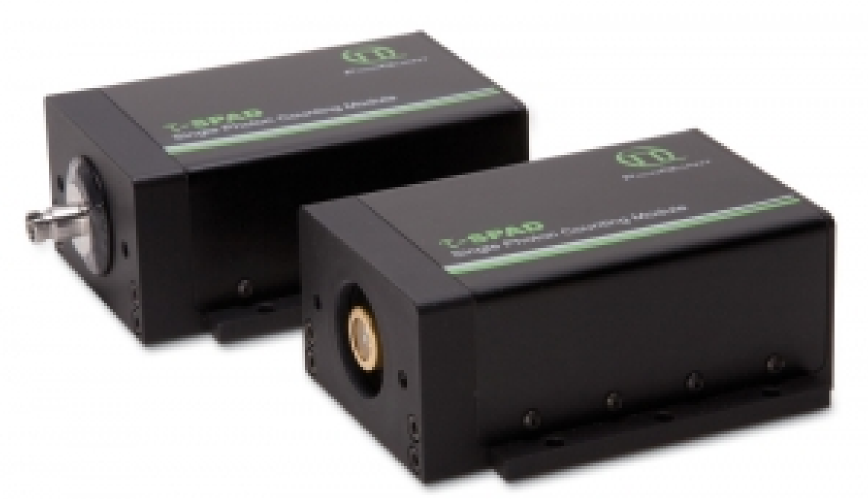


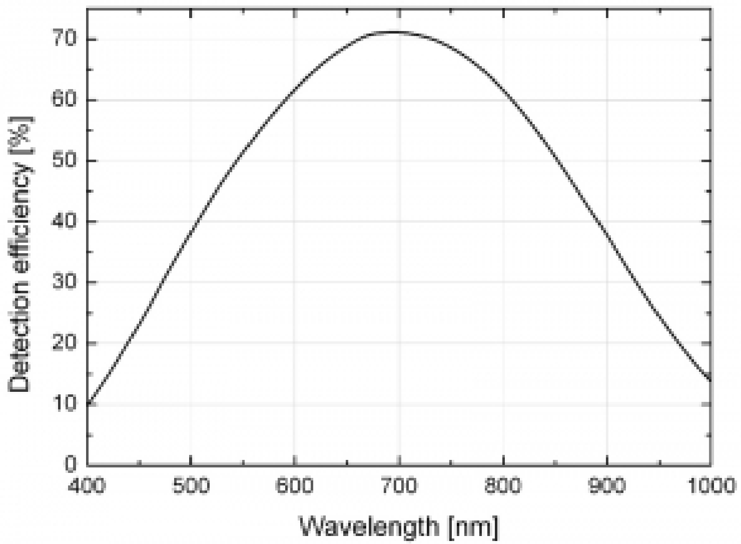


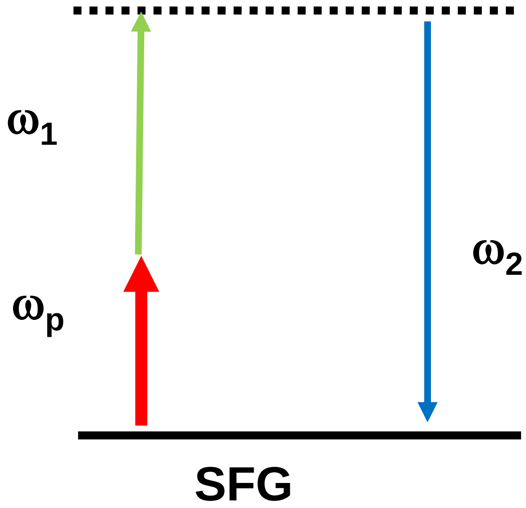


Telecomband single photon detection









ω_1

ω_p

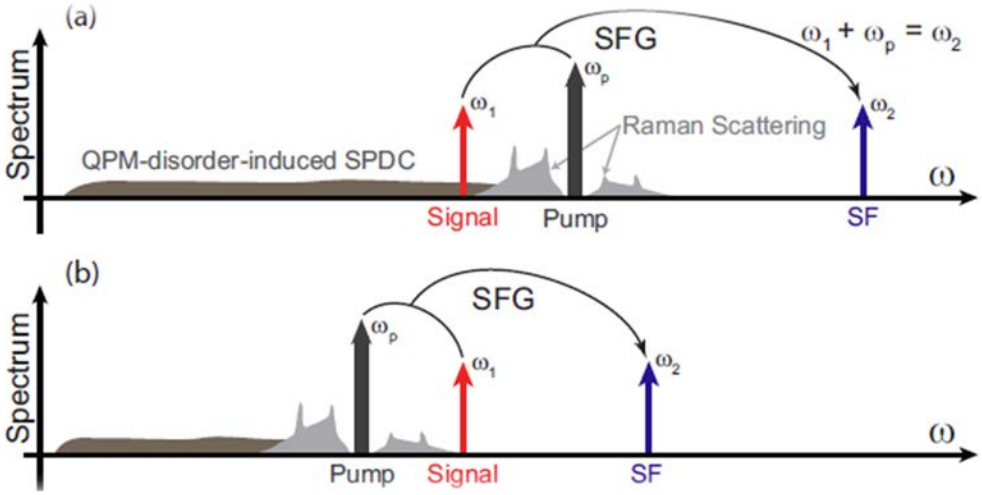
ω_2

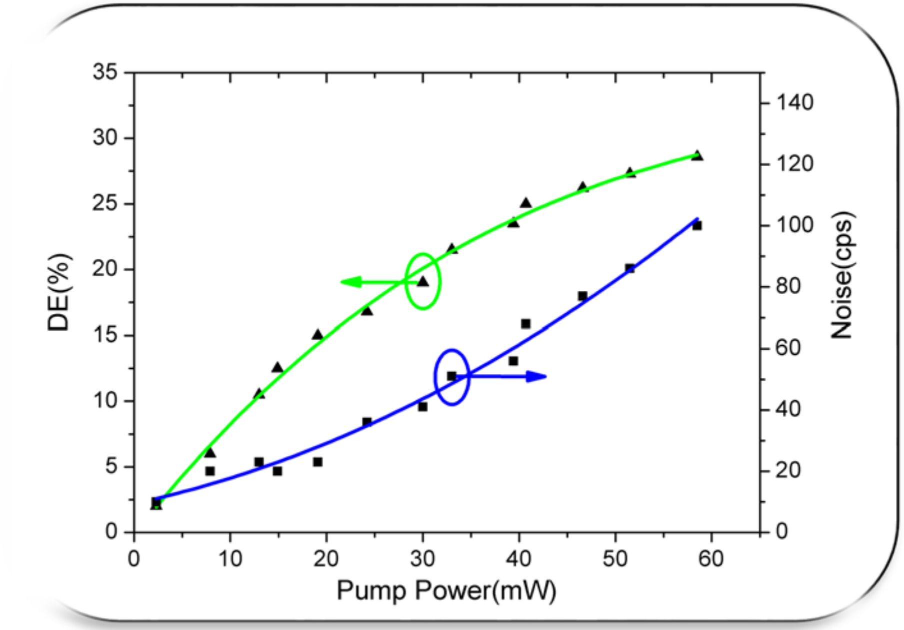
SFG

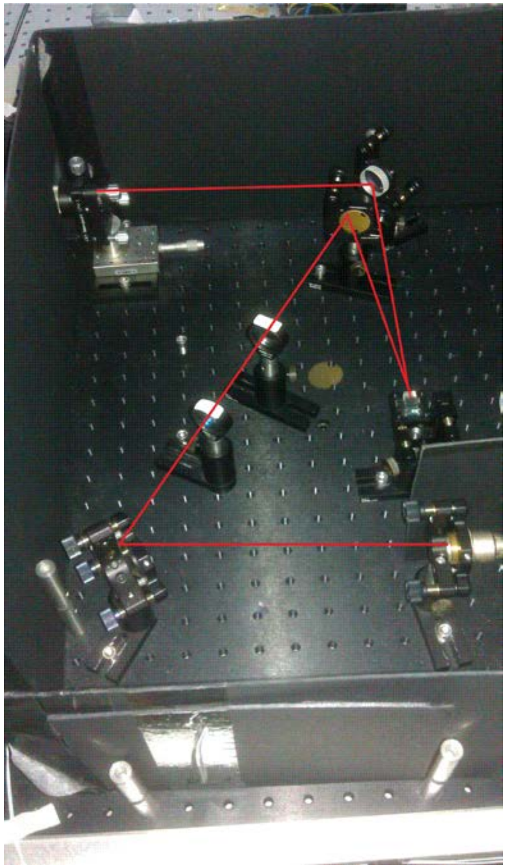
τ-SPAD by PicoQuant

[Kumar, OL. 15, 1476 (1990)]

Upconversion single photon detector





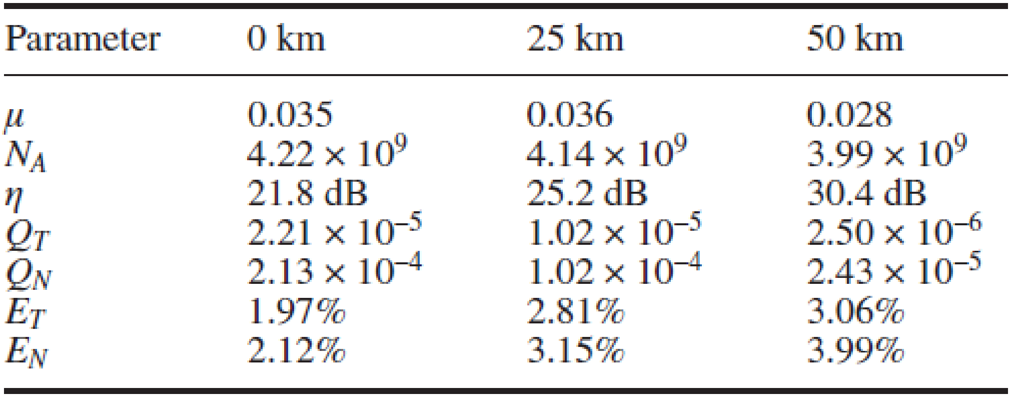


Shentu et al., OE 2013

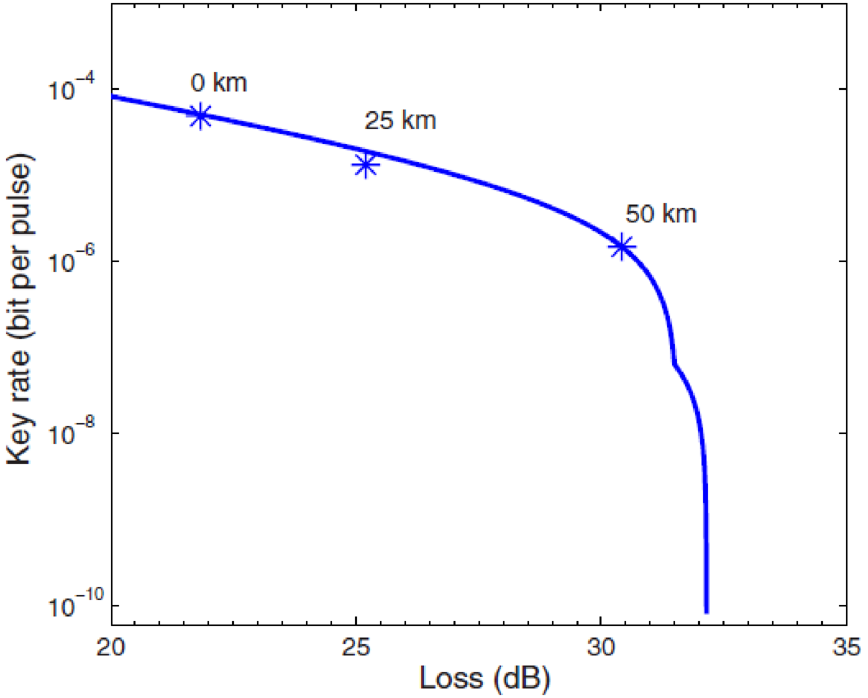
Passive Decoy Result

$$R = R_N + R_T$$

$$R_j \geq q\left\{-fQ_jH(E_j) + Q_{j,1}[1 - H(e_1)] + Q_{j,0}\right\}$$

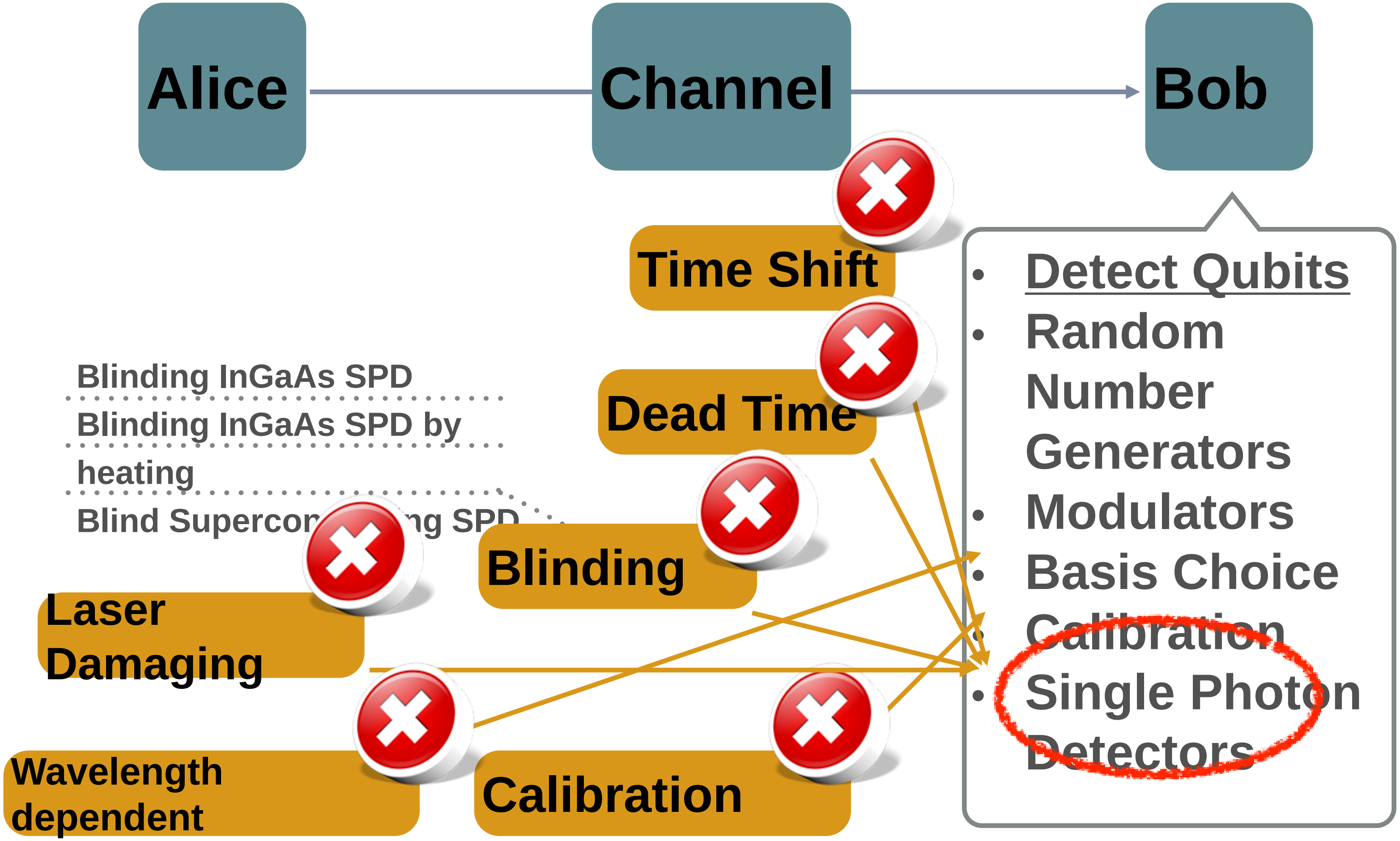


Parameter	0 km	25 km	50 km
μ	0.035	0.036	0.028
N_A	4.22×10^9	4.14×10^9	3.99×10^9
η	21.8 dB	25.2 dB	30.4 dB
Q_T	2.21×10^{-5}	1.02×10^{-5}	2.50×10^{-6}
Q_N	2.13×10^{-4}	1.02×10^{-4}	2.43×10^{-5}
E_T	1.97%	2.81%	3.06%
E_N	2.12%	3.15%	3.99%



Sun *et al.*, Laser Phys. Lett. 11, 085202 (2014)

Detector



Alice

Channel

Bob

- Detect Qubits
- Random Number Generators
- Modulators
- Basis Choice
- Calibration
- Single Photon Detectors

Time Shift

Dead Time

Blinding

Laser Damaging

Wavelength dependent

Calibration

Blinding InGaAs SPD

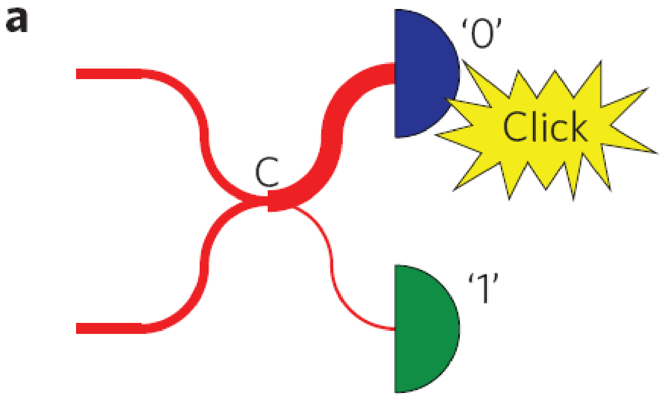
Blinding InGaAs SPD by heating

Blind Superconducting SPD

Attacks against detectors

☒ **Blinding attack: can fully control detectors by specially tailored bright illumination**

Lydersen *et al.*, Nature Photonics 4, 686 (2010)



- **When detector is blinded, it can only respond for intensity larger than *I***
- **If Eve set input intensity between *I* to *2I*, the detector can only click when Bob's choice of bases is as same as Eve**

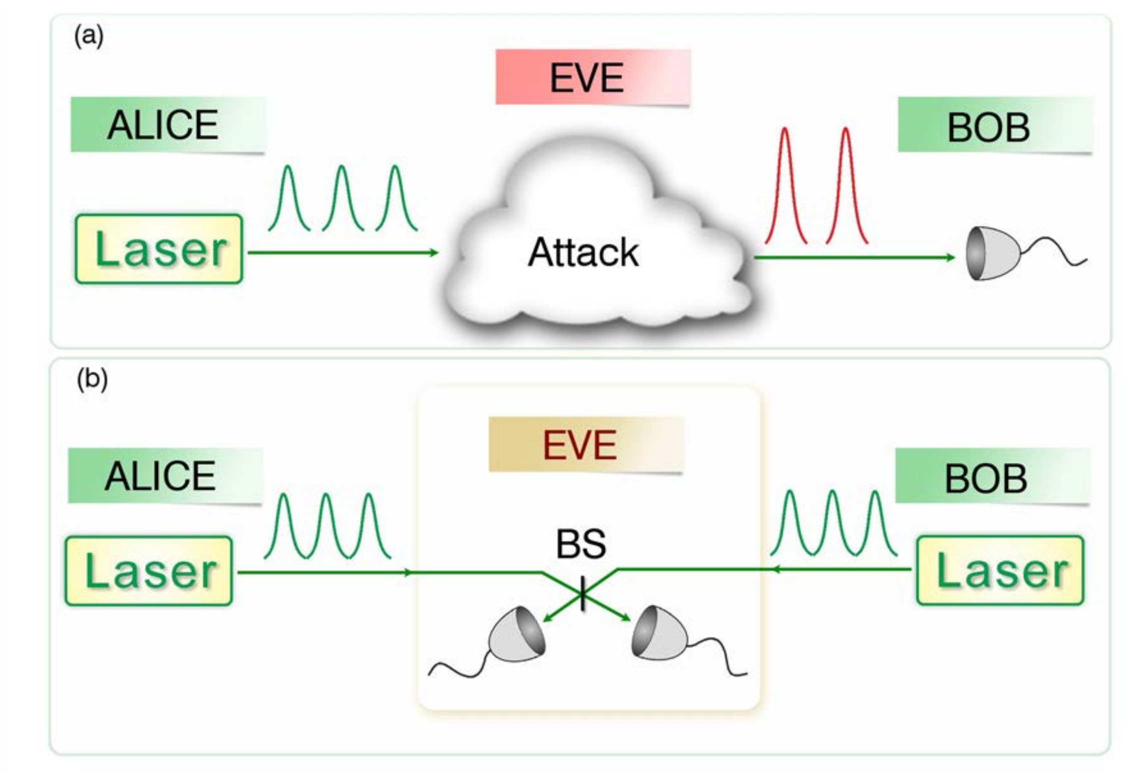
☒ **Time-shift attack: detection efficiency is time-dependent**

Qi *et al.*, Quant. Info. Compu. 7, 73 (2007)

Measurement Device Independent-QKD

Immune to any attacks on detector

Scheme: Lo *et al*., PRL 108, 130503 (2012)



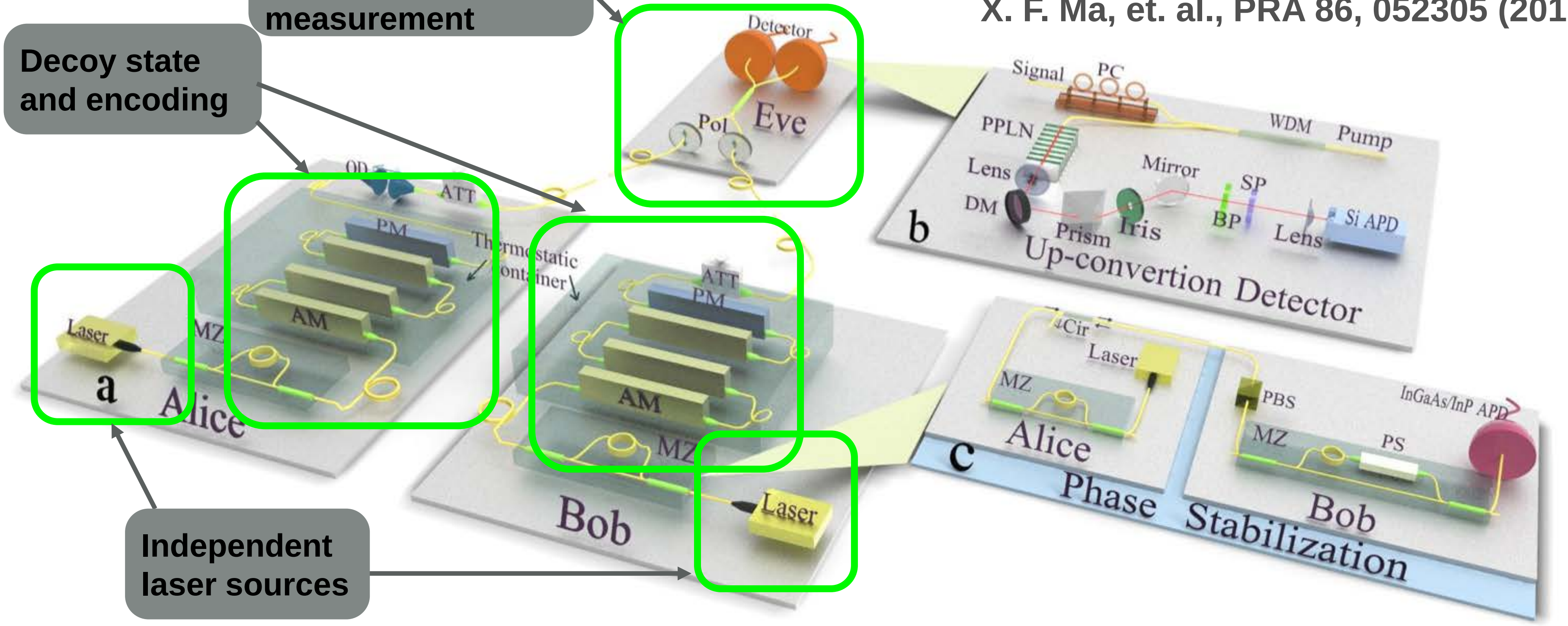
☑ **Creating raw key: If Alice and Bob's polarization choice are same, there would not be coincidence event**

Implementation of MDI-QKD

Final Secure key: 25 kbit @50 km

Postprocessing:
Linear programming

X. F. Ma, et. al., PRA 86, 052305 (2012)



Bell state measurement

Decoy state and encoding

Independent laser sources

Liu *et al.*, PRL 111, 130502 (2013);
Also: Tittel group, Weid group, Lo group

Interference of two independent laser

- **Spatial Mode**

  single mode fiber

- **Polarization**

  in-line polarizer

- **Wavelength**

1550.200 nm with FWHM 10 pm

Temperature stabilization/TEC

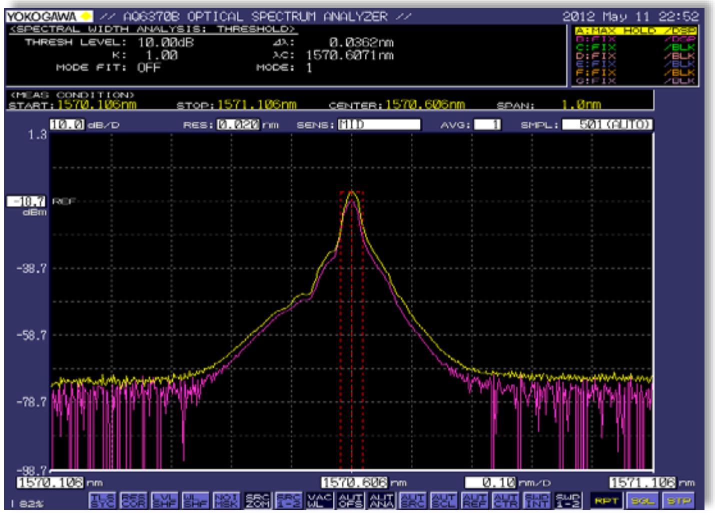
Adjust with a precision of 0.1 pm

- **Timing**

2 ns pulse width

Low timing jitter (10ps)

Adjust with Optical Delay (10ps)



YOKOGAWA // AQ6370B OPTICAL SPECTRUM ANALYZER // 2012 May 11 22:52

<SPECTRAL WIDTH ANALYSIS: THRESHOLD>

THRESH LEVEL: 10.00dB Δλ: 0.0362nm

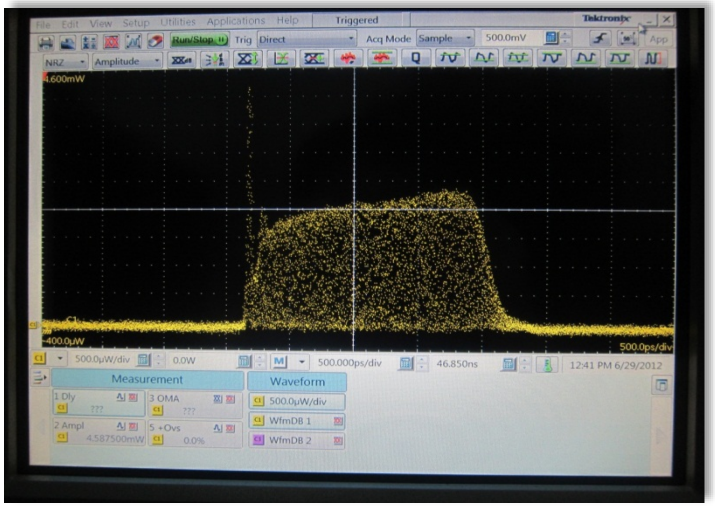
K: 1.00 λc: 1570.6071nm

MODE FIT: OFF MODE: 1

<MEAS CONDITION>

START: 1570.106nm STOP: 1571.106nm CENTER: 1570.606nm SPAN: 1.0nm

10.0 dB/D RES: 0.020 nm SENS: MID AVG: 1 SMPL: 501 (AUTO)



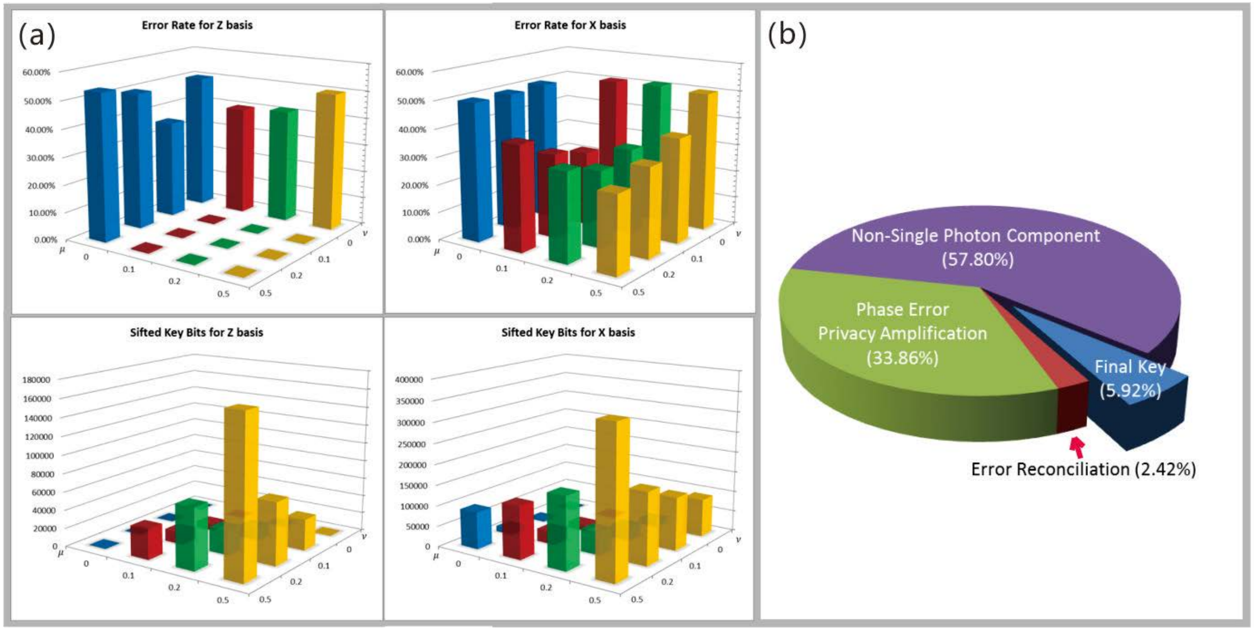
Trig: Direct Acq Mode: Sample 500.0mV

C1 500.0µW/div 0.0W 500.000ps/div 46.850ns 12:41 PM 6/29/2012

Measurement: 1 Dly ??? 3 OMA ??? 2 Ampl 4.587500mW 5 +Ovs 0.0%

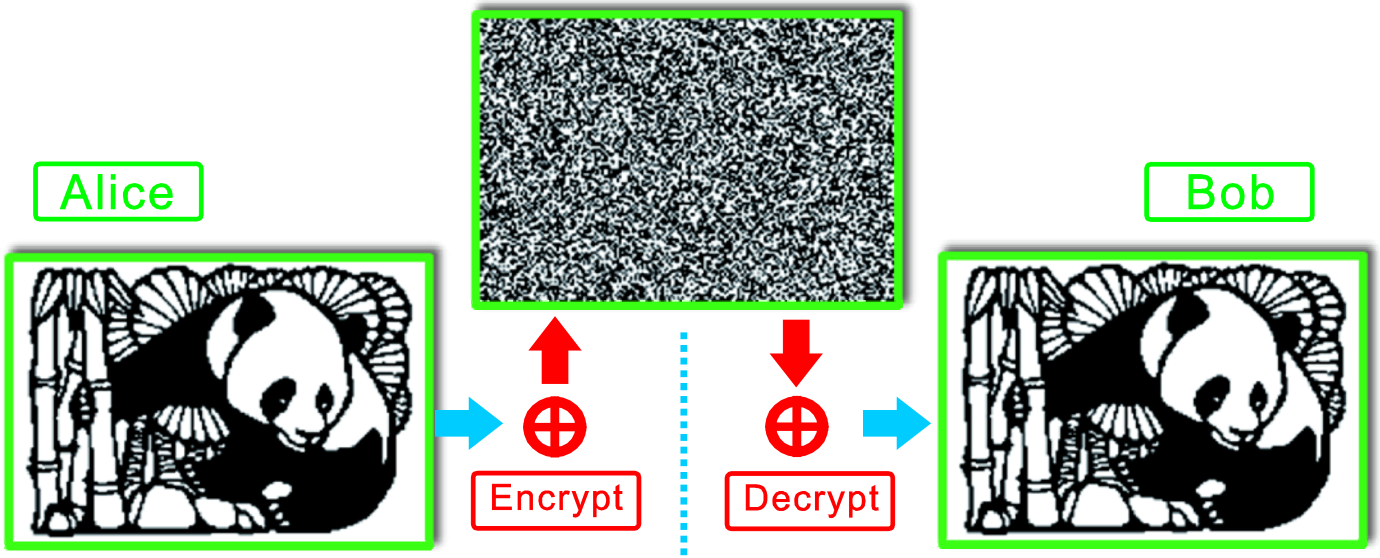
Waveform: C1 500.0µW/div WfmDB 1 WfmDB 2

Implementation of MDI-QKD



System frequench: 1 MHz

Total pulse: 2*10^11



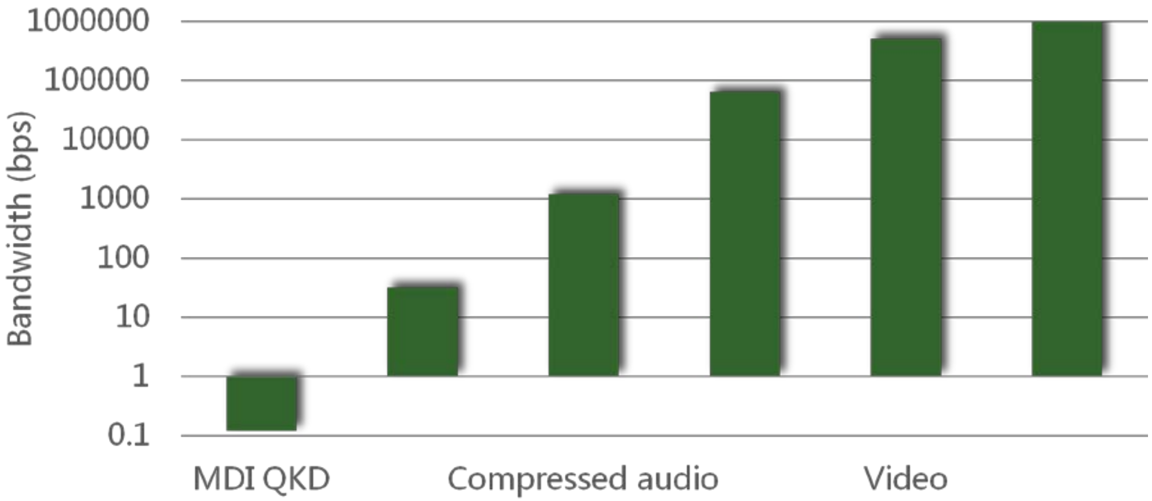
Limitation of Previous Work

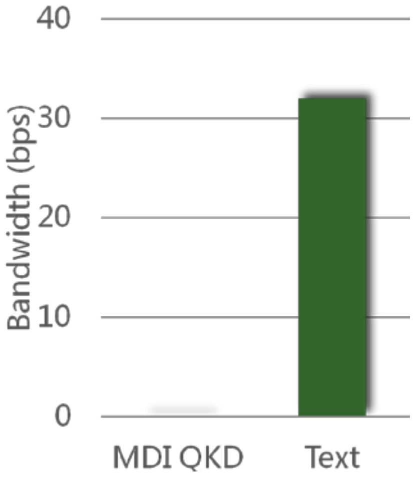
☒ **Limited Distance: <50 km**

☒ **Low Key Rate: < 1 bps**

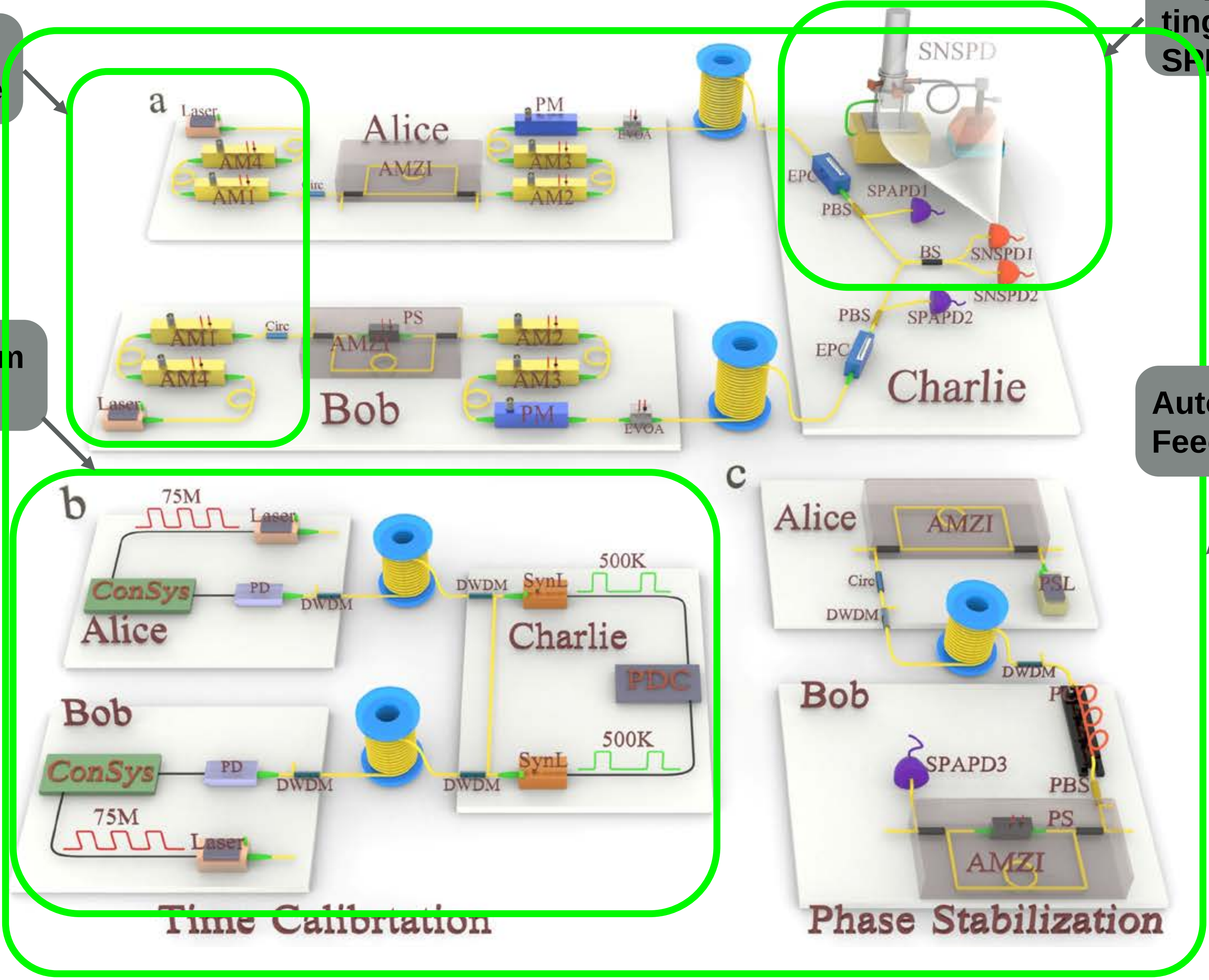
☒ **In Lab: No Field Test**

Goal: 200 km, 30 bps at 50 km, Field Test





200 km MDI-QKD



Better interference

Higher system frequency

Superconducting nanowire SPD

Automatically Feedback

Tang *et al.*, arXiv:1407.8012

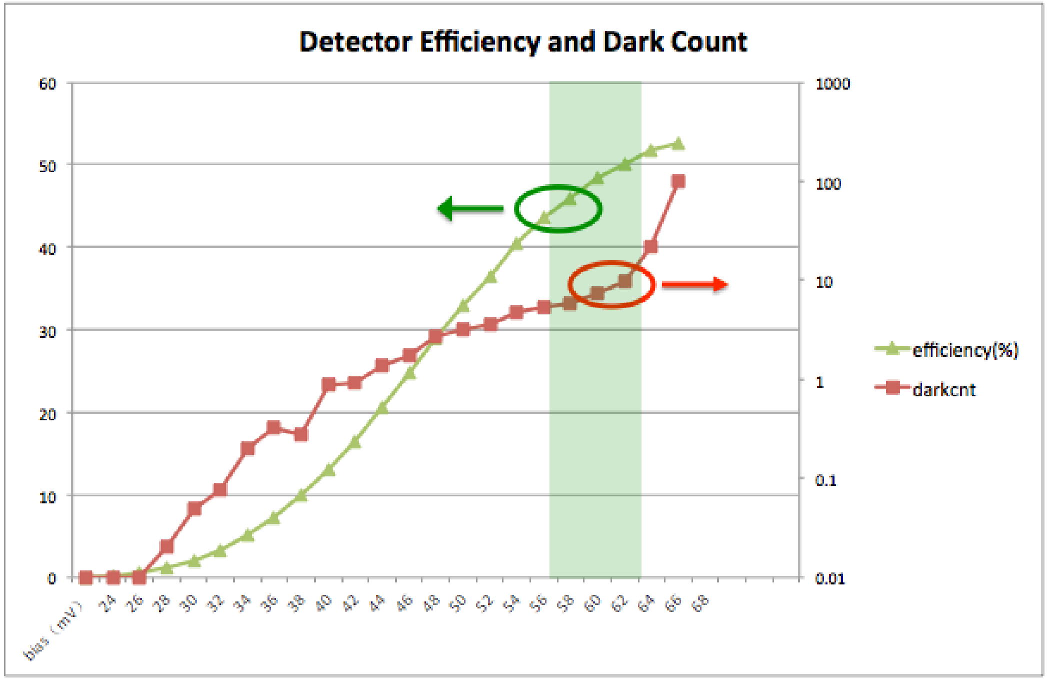
Controlling system jitter

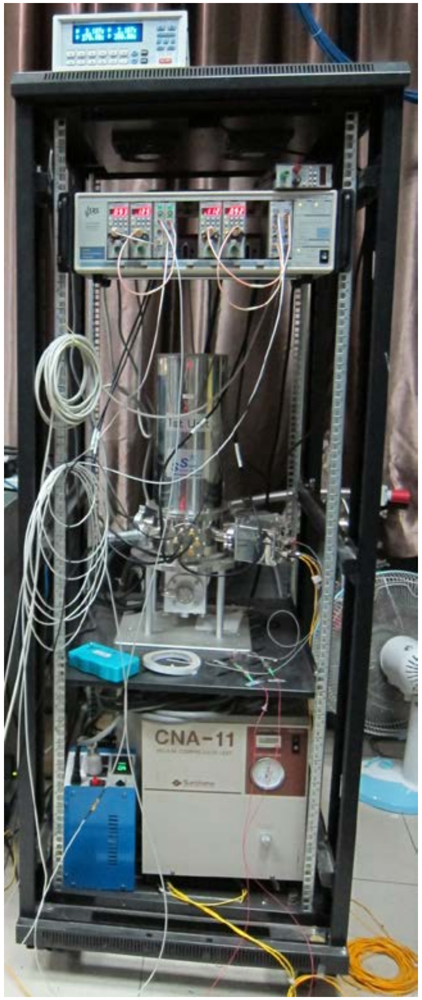
Source	Estimated jitter
Synchronical laser	~10 ps
Synchronical detection	~20 ps
Electronic boards	~10 ps
Fiber fluctuation (100 km)	~30 ps
Fiber drift (20 mins, 200 km)	~200 ps
Fiber chromatic dispersion (200 km)	700 ps
Superconducting SPD	<100 ps
TDC recording (accuracy)	~200 ps

Superconducting nanowire SPD

Nanowire structure on ultra-thin NbN film on SiO_2/Si substrate

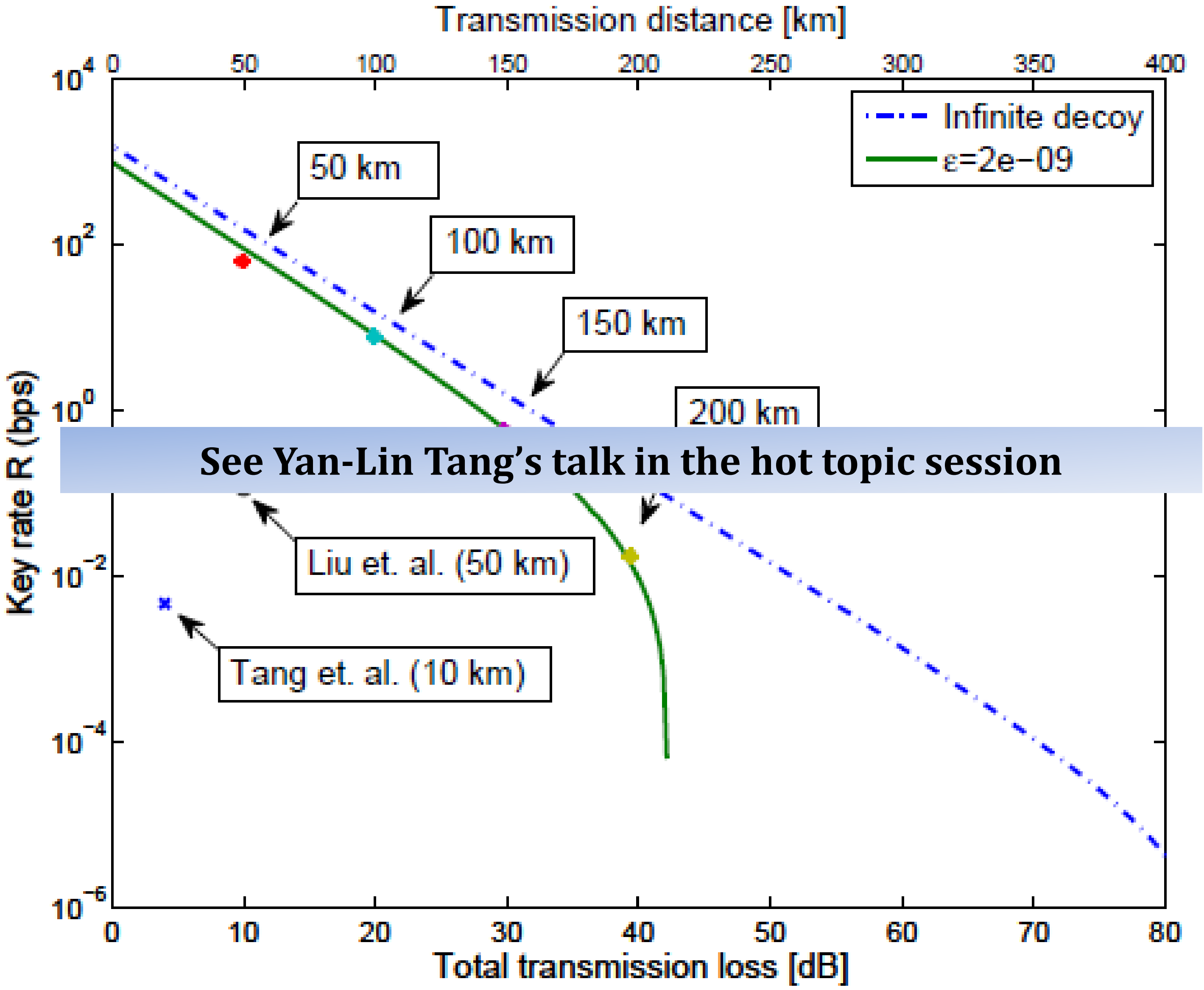
Operated at 2.2 K (Superconducting temp.)





L. You *et al.*, AIP Advances 3, 072135 (2013)

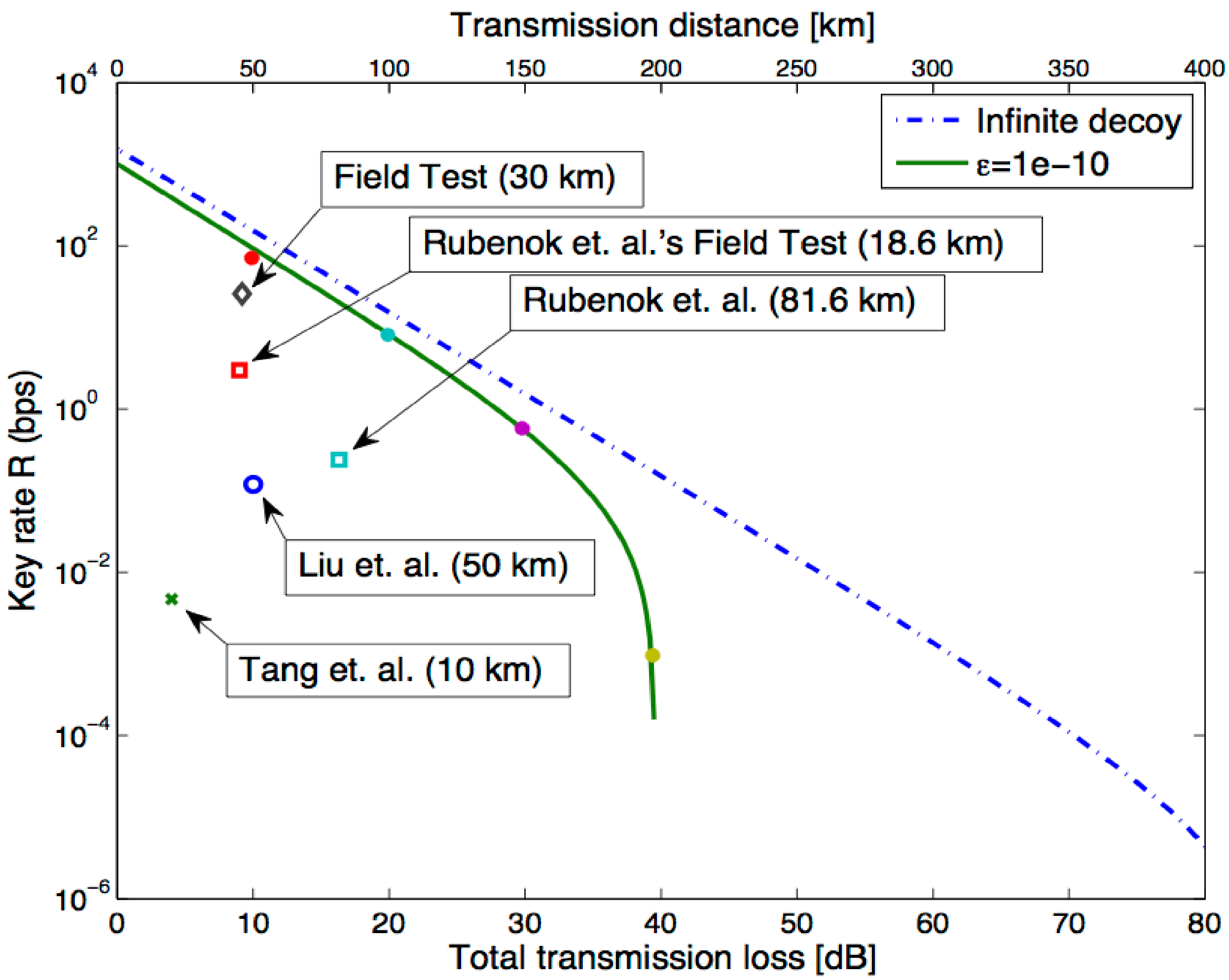
Experimental Result



See Yan-Lin Tang's talk in the hot topic session

Tang *et al.*, arXiv:1407.8012

Field Test of MDI-QKD

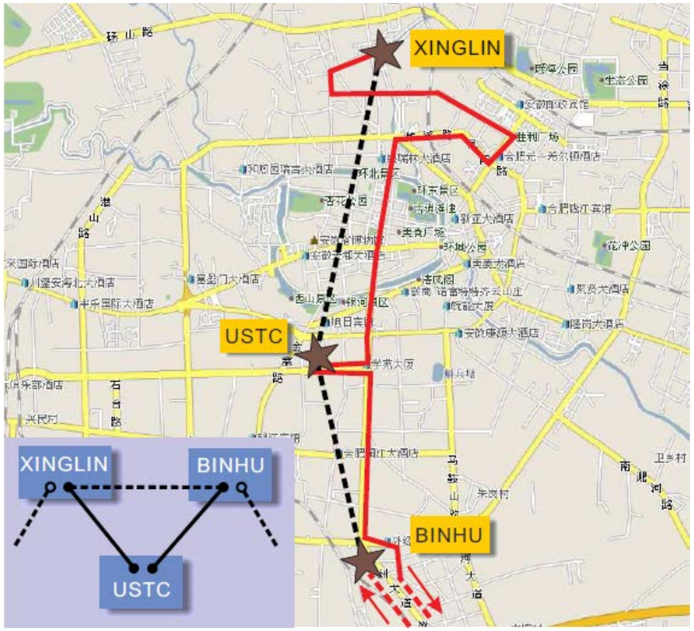


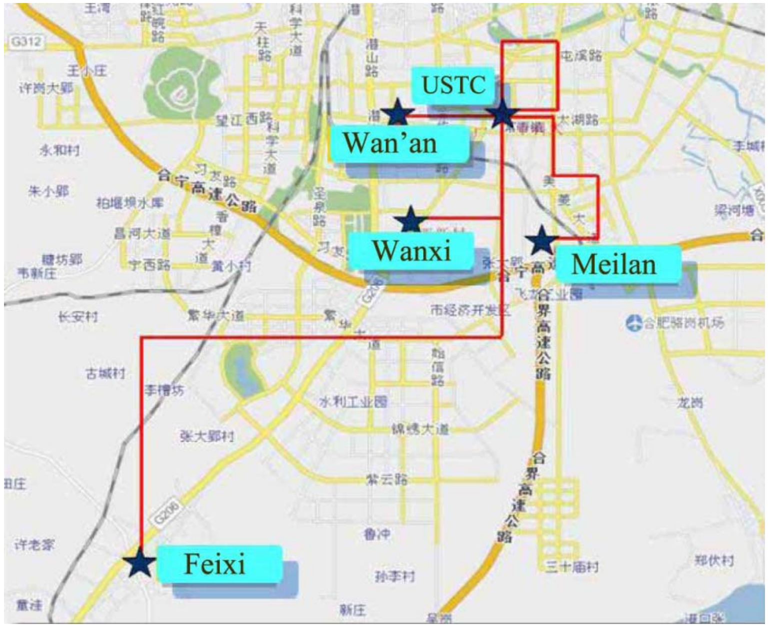
Tang *et al.*, arXiv:1408.2330

Content

- Research in the Lab
- **Field test & Practical quantum network**
- Future: Quantum Backbone and Satellite

Field test





- **Three node quantum telephone network**

Decoy state; Real time application for voice telephone; 20 km fiber between each node; Key rate > 1 kb/S; Chen *et al*., Optics Express 17, 6540 (2009)

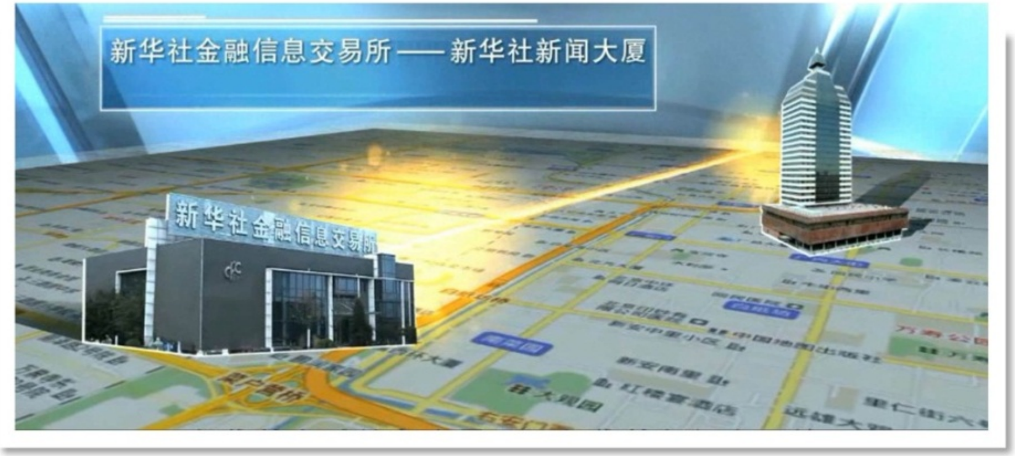
- **Five node all-pass quantum network**

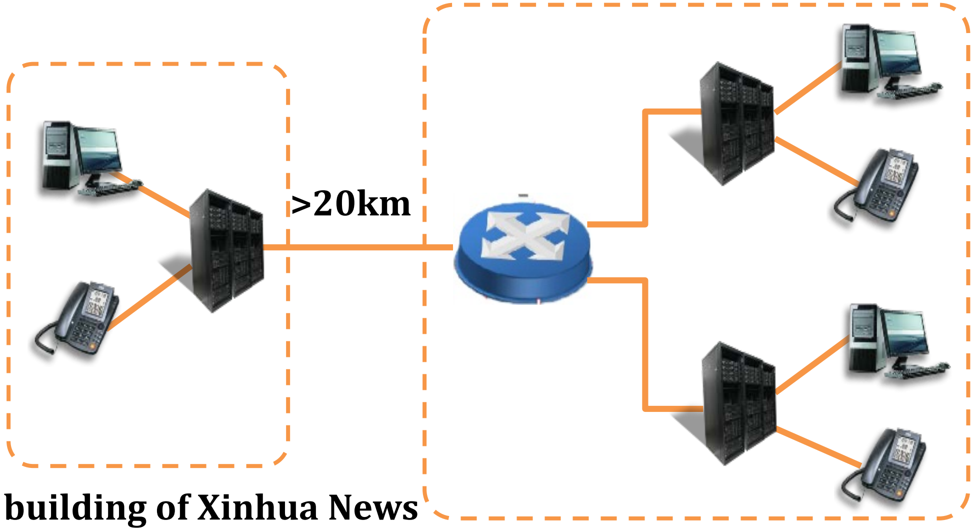
Decoy state; Real time; Optical switch for all-pass; Trusted relay for 130 km; Key rate > 1 kb/S; Chen *et al*., Optics Express 18, 027217 (2010)

Trustable Relay Approach

	A	Relay	B
Initial	K_{AR}	K_{AR}、 K_{RB}	K_{RB}
Step 1		Announce $K_{AR} \oplus K_{RB}$	
Step 2			$K_{AR} \oplus K_{RB} \oplus K_{RB}$
Final	K_{AR}		K_{AR}

Quantum-communication based financial information network

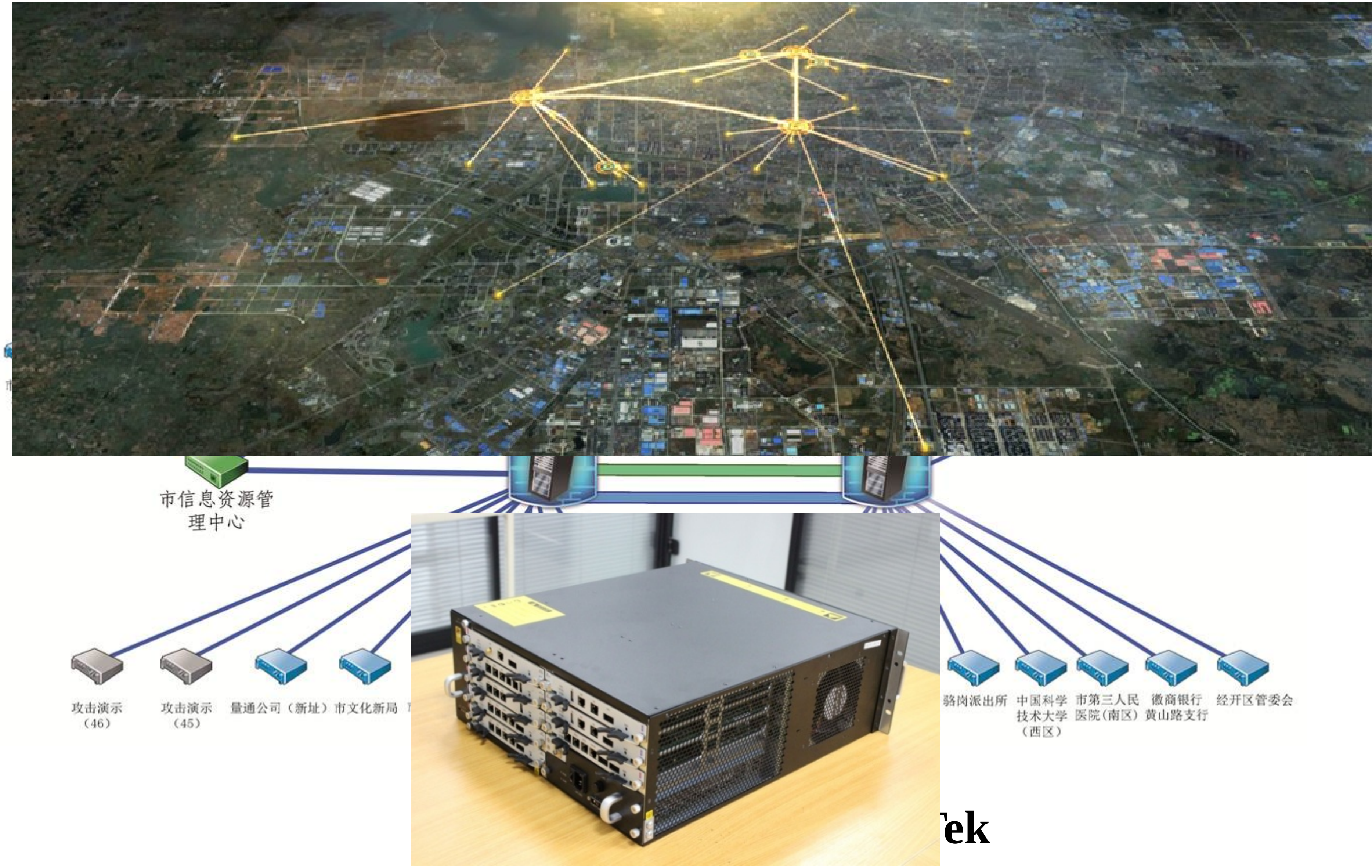




News building of Xinhua News Agency

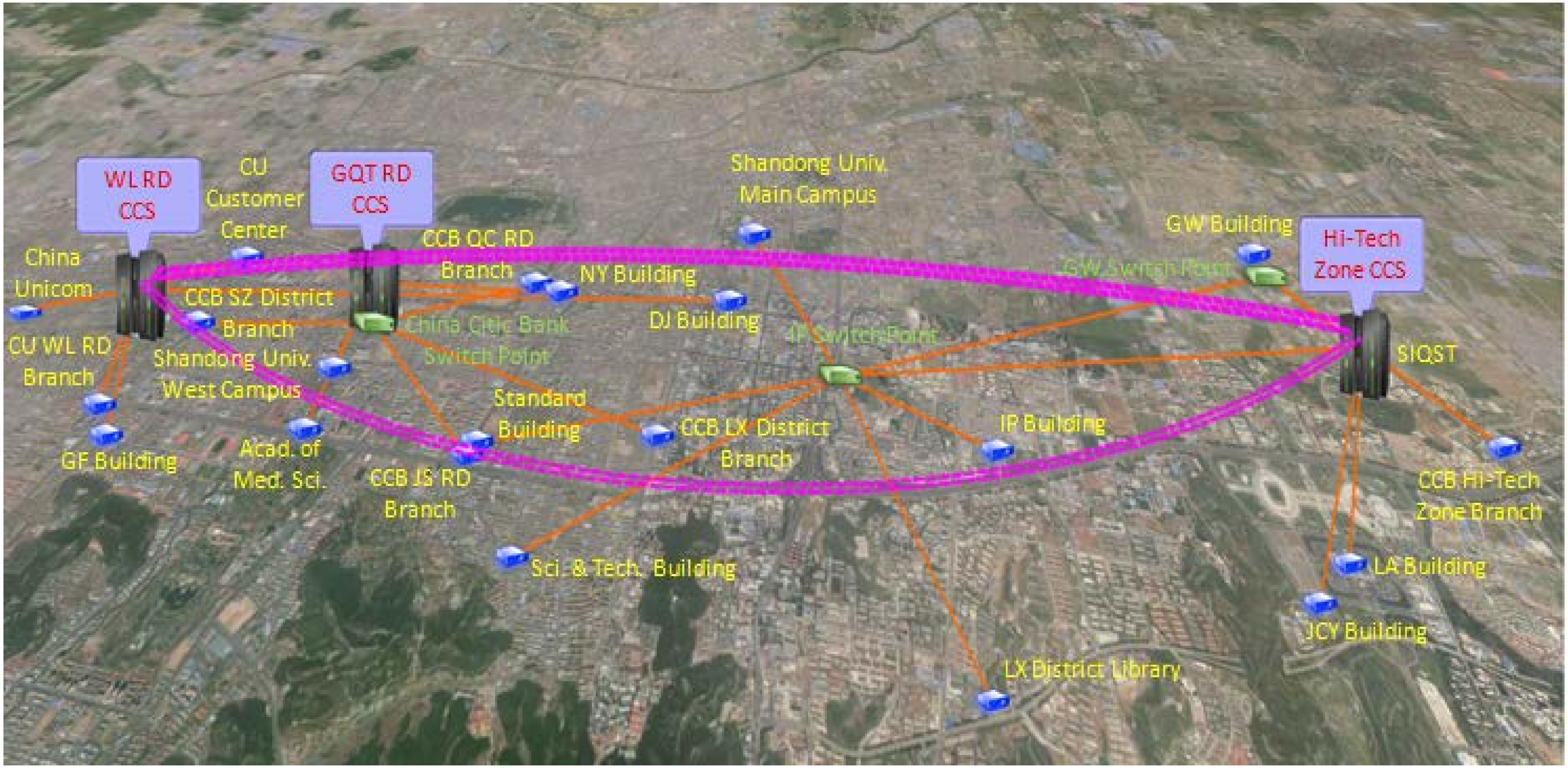
Financial Information Exchange Center of Xinhua News Agency

Hefei Intracity Quantum network



Tek

Jinan Quantum Communication Network

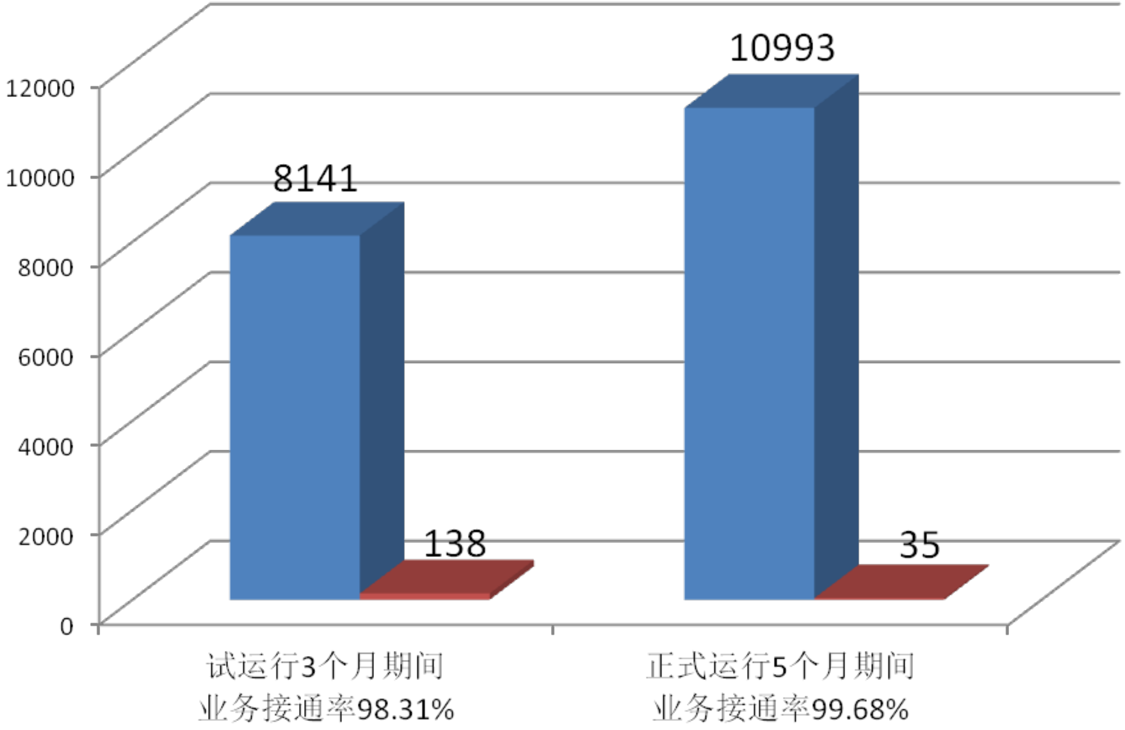


Curtsey of Shandong Institute of Quantum Sci. & Tech. Co., Ltd. (SIQST)

50 nodes, 28 institutions, 90 users and over 70 km^2 covering area has been well established.

Practical Metropolitan QKD Networks

Test running since 2013



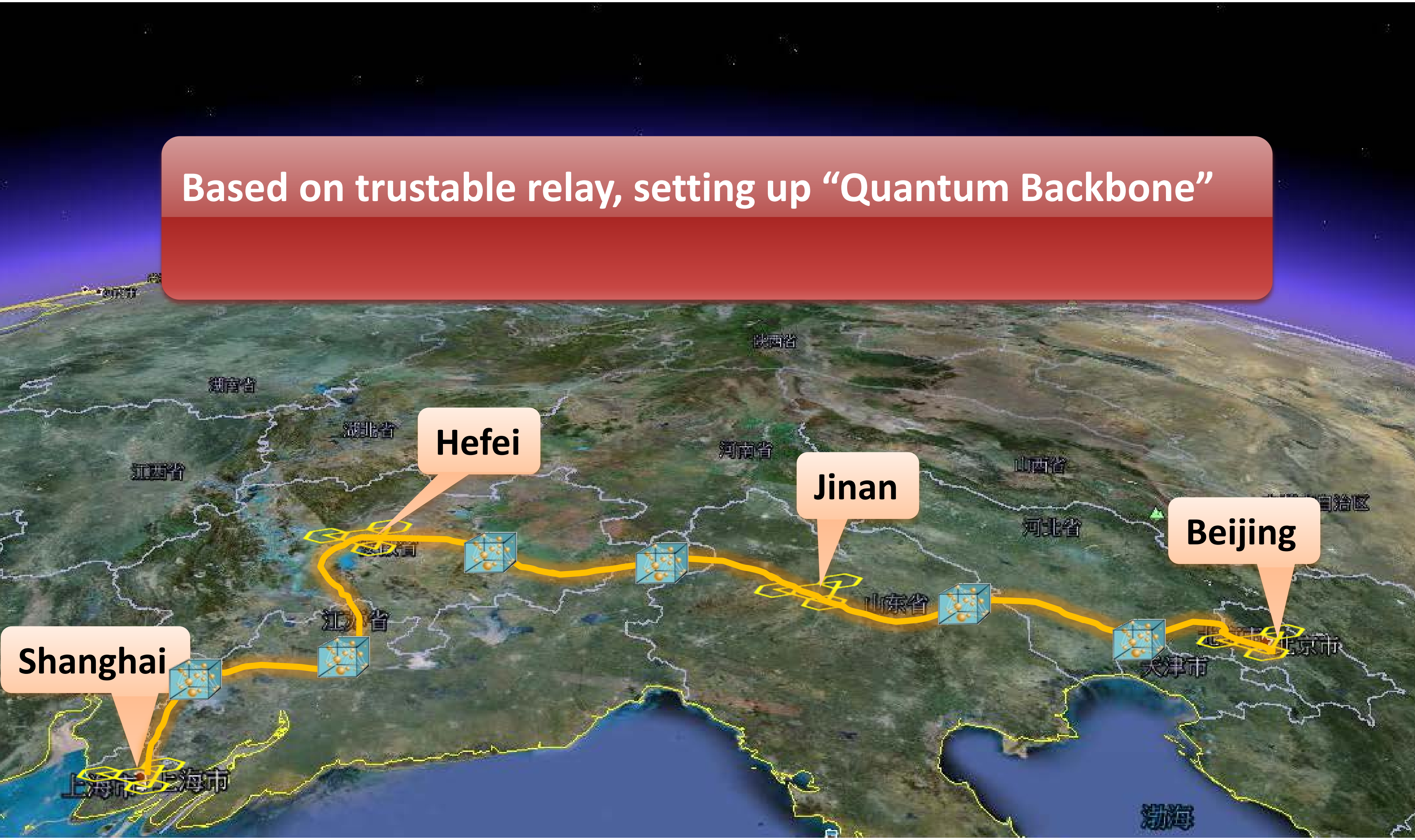
See: Yong Zhao’s talk in Industrial Session

Content

- Research in the Lab
- Field test & Practical quantum network
- **Future: Quantum Backbone and Satellite**

Quantum Backbone

Based on trustable relay, setting up "Quantum Backbone"



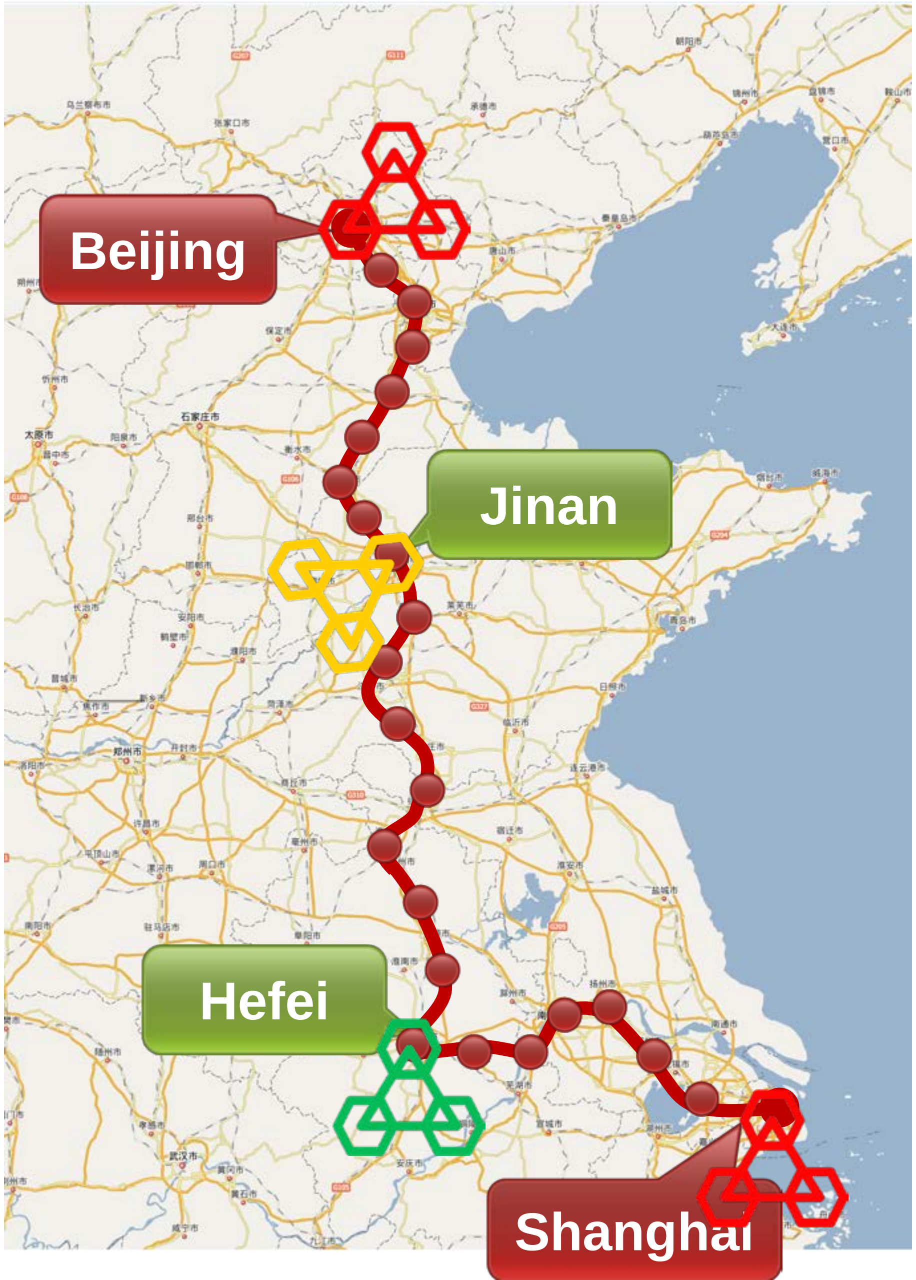
Quantum Backbone

- Total Length 2000 km
- 2013.6-2016.12
- 32 trustable relay nodes

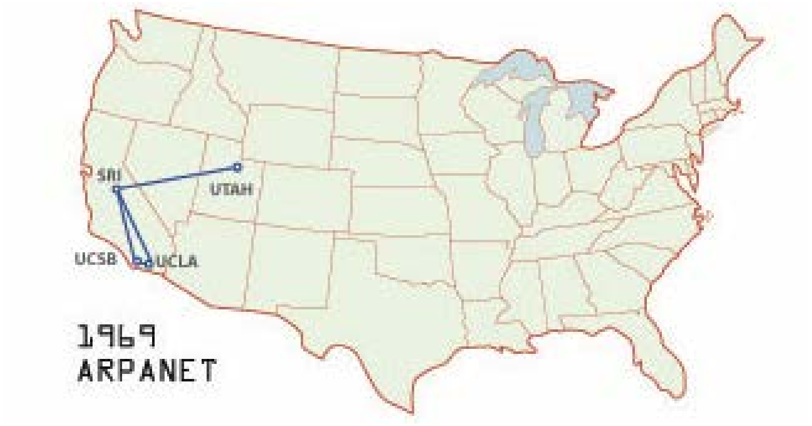
  31 fiber links
- Metropolitan networks

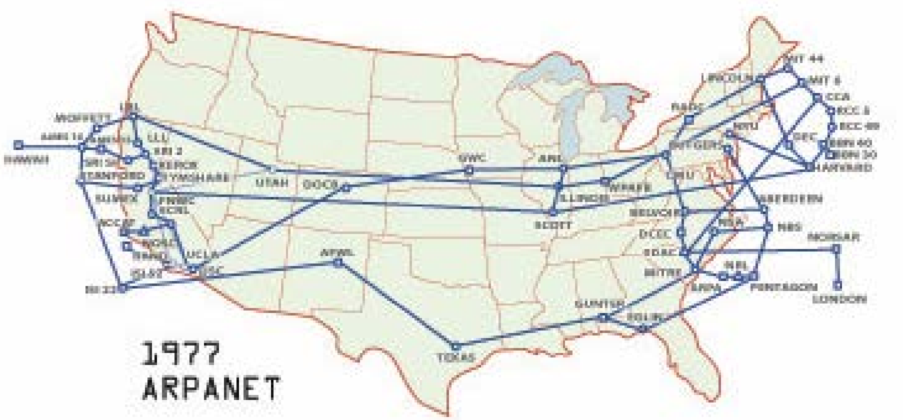
  Existing: Hefei, Jinan

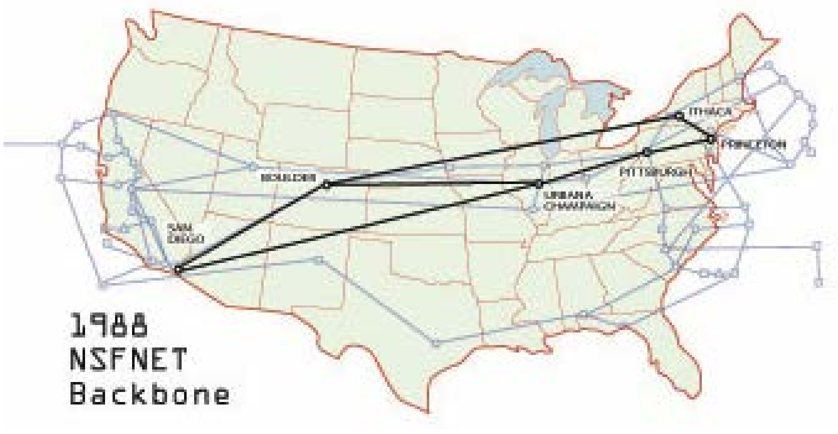
  New: Beijing, Shanghai
- Customer: China Industrial & Commercial Bank; Xinhua News Agency; CBRC

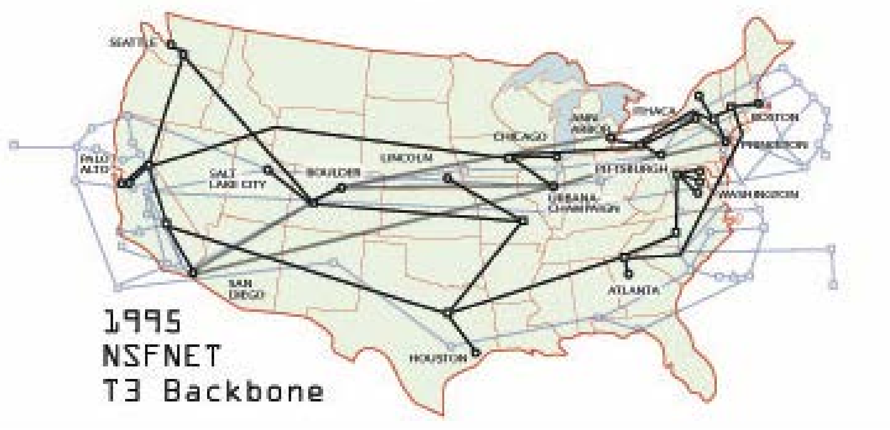


The Growth of the Internet

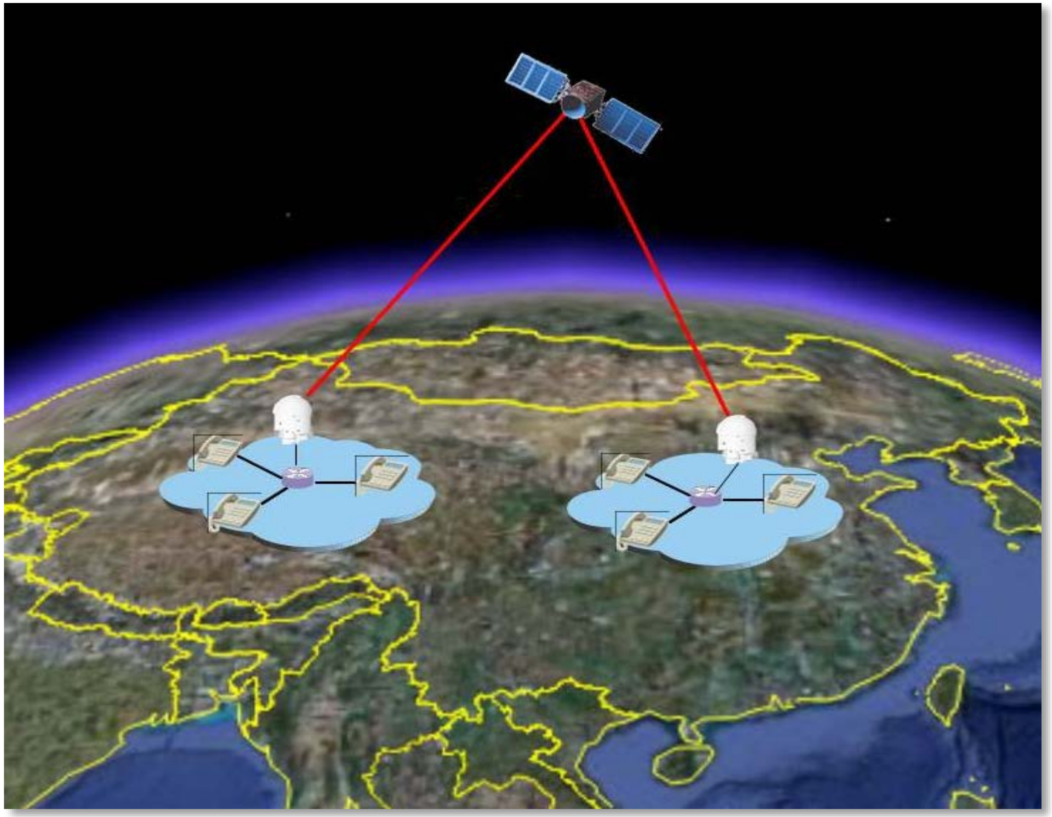






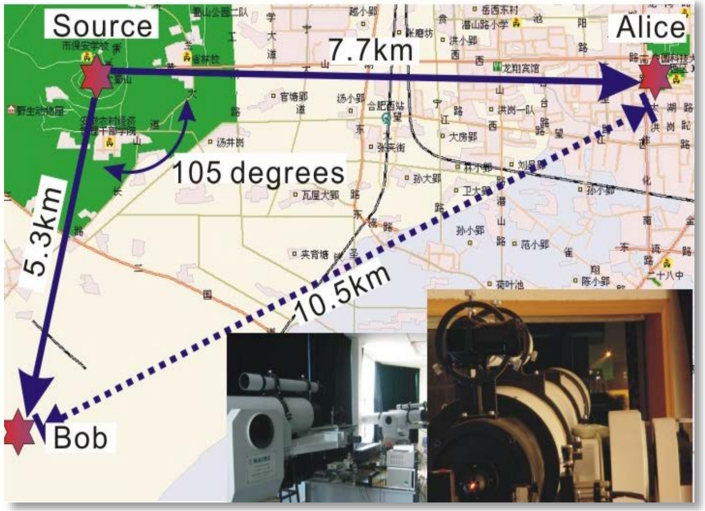


Free-Space Quantum Communication



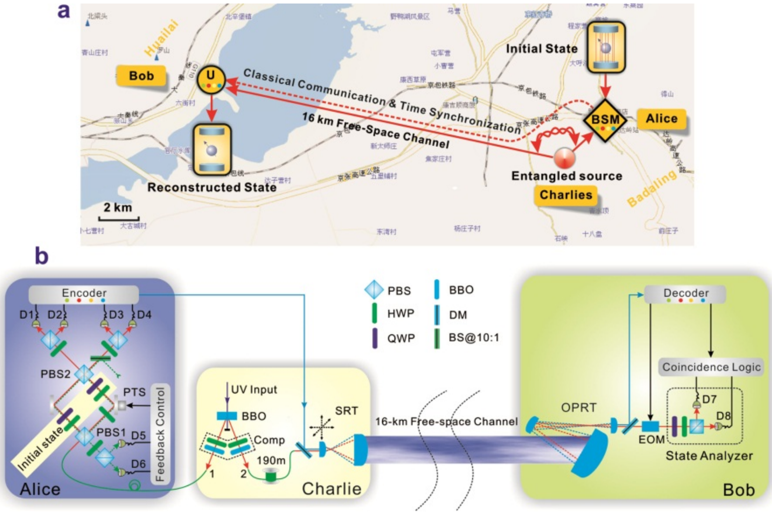
- ☑ Non-obstruction from terrestrial curve and barrier
- ☑ Effective thickness of atmosphere is only 5-10km
- ☑ No decoherence in outer space

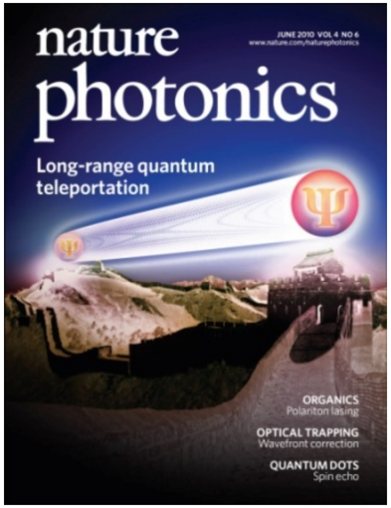
Free-Space Quantum Communication



- Free-space quantum entanglement and key distribution (13km)

  Peng *et al.*, PRL 94, 150501 (2005)





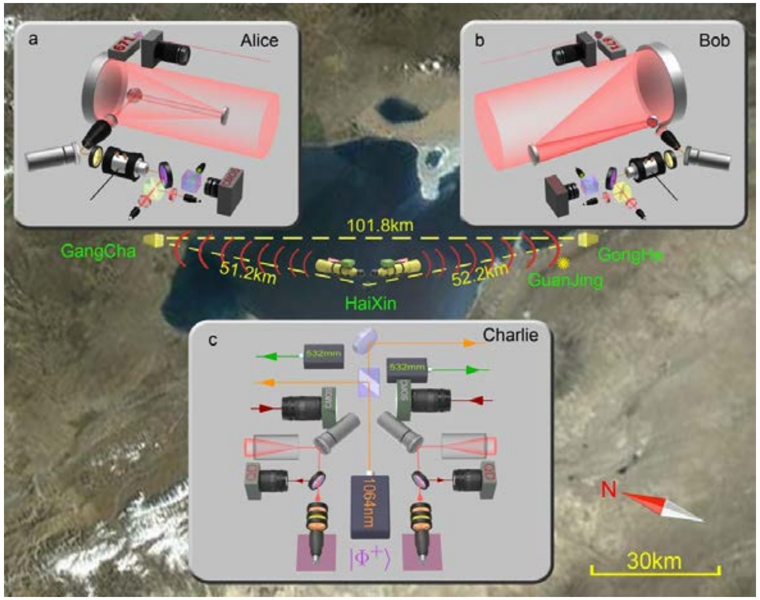
- Free-space quantum teleportation (16km)

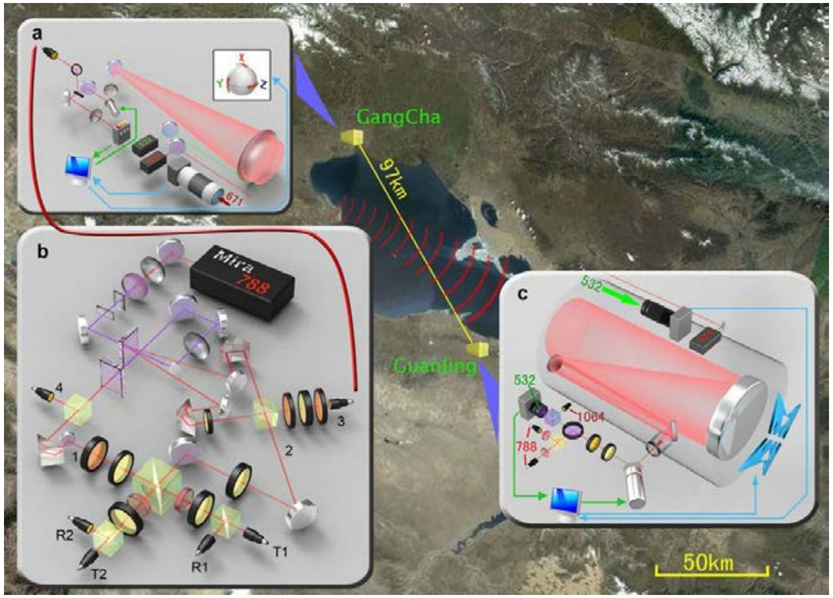
  Jin *et al.*, Nature Photonics 4, 376 (2010)

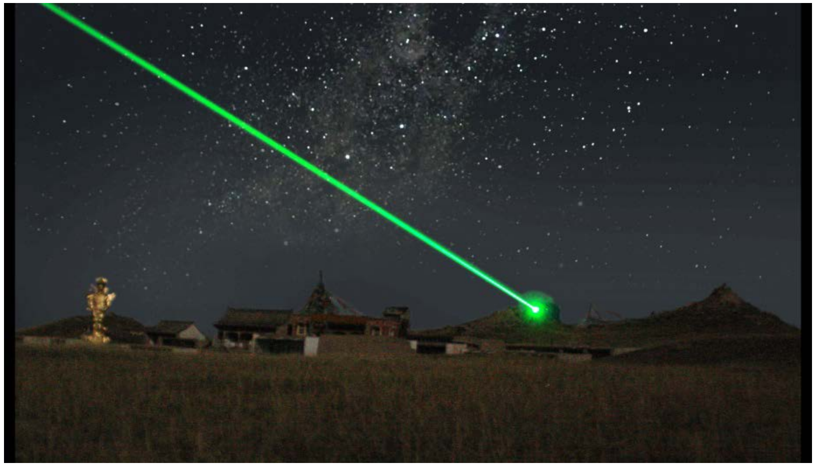
Well beyond the effective thickness of the aerosphere!

Free-Space Quantum Communication

- Free-space quantum teleportation and entanglement distribution (~100km) [Yin *et al.*, Nature 488, 185 (2012)]







Demonstrating the feasibility for satellite-based quantum communication through high-loss space-ground link

Ground Test of Satellite-based Photon Transmission

- Single photon transmission between satellite and ground at the distance of 400km (2009)
- Direct and full-scale experimental verifications towards ground-satellite QKD

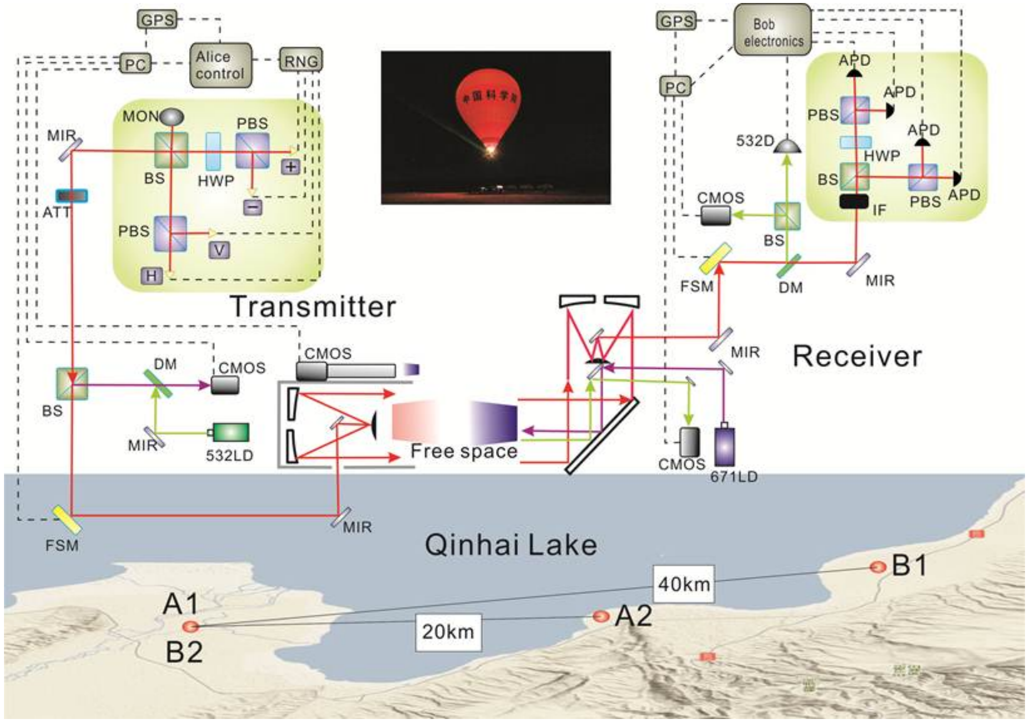
  Wang *et al.*, submitted to Nature Photonics (2012), under review

Overcoming all the demanding conditions for ground-satellite QKD

☑ A moving platform through a turntable (40 km)

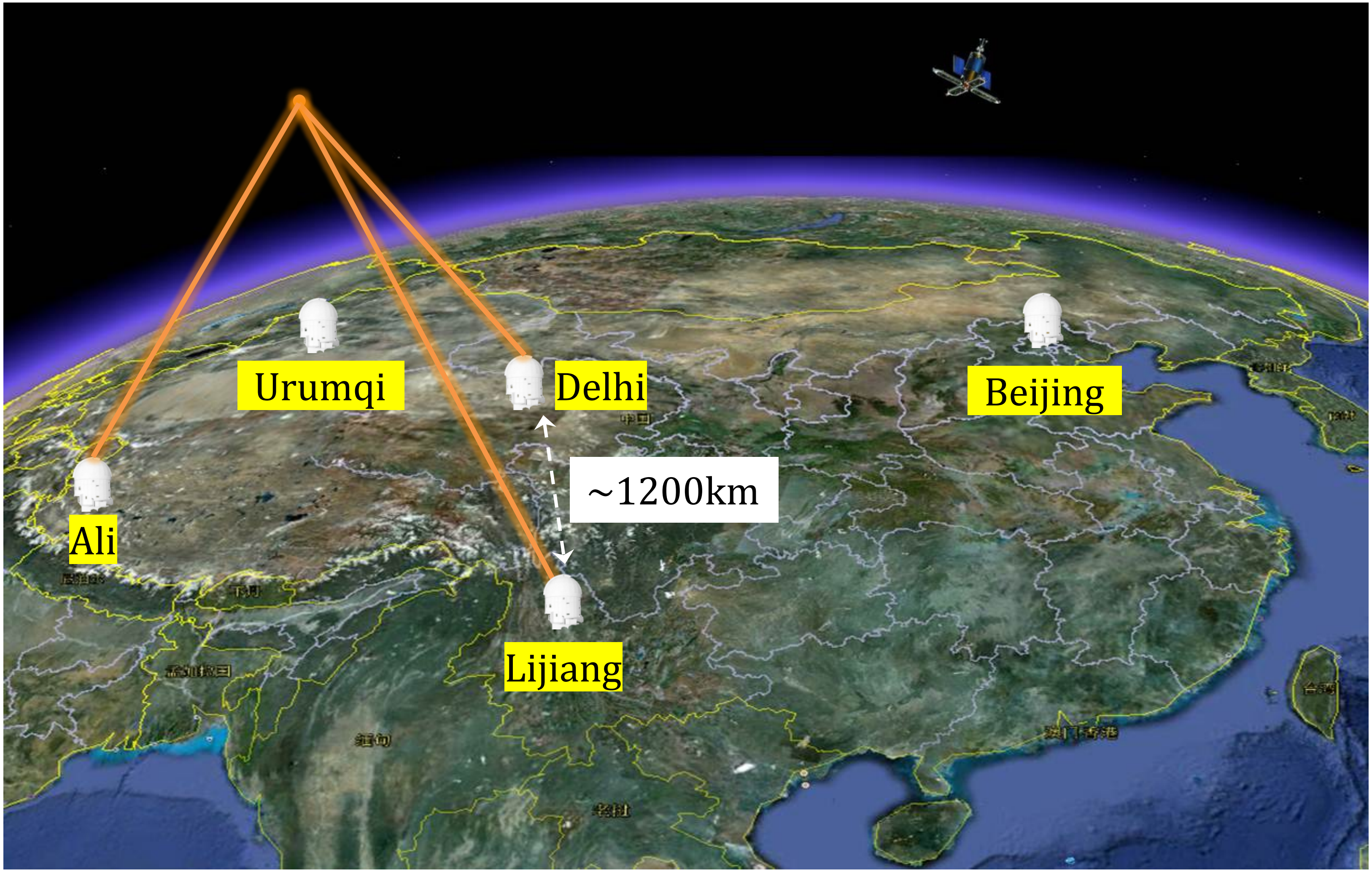
☑ A floating platform through a hot-air balloon (20 km)

☑ A huge loss channel (about 50 dB loss, 97 km)

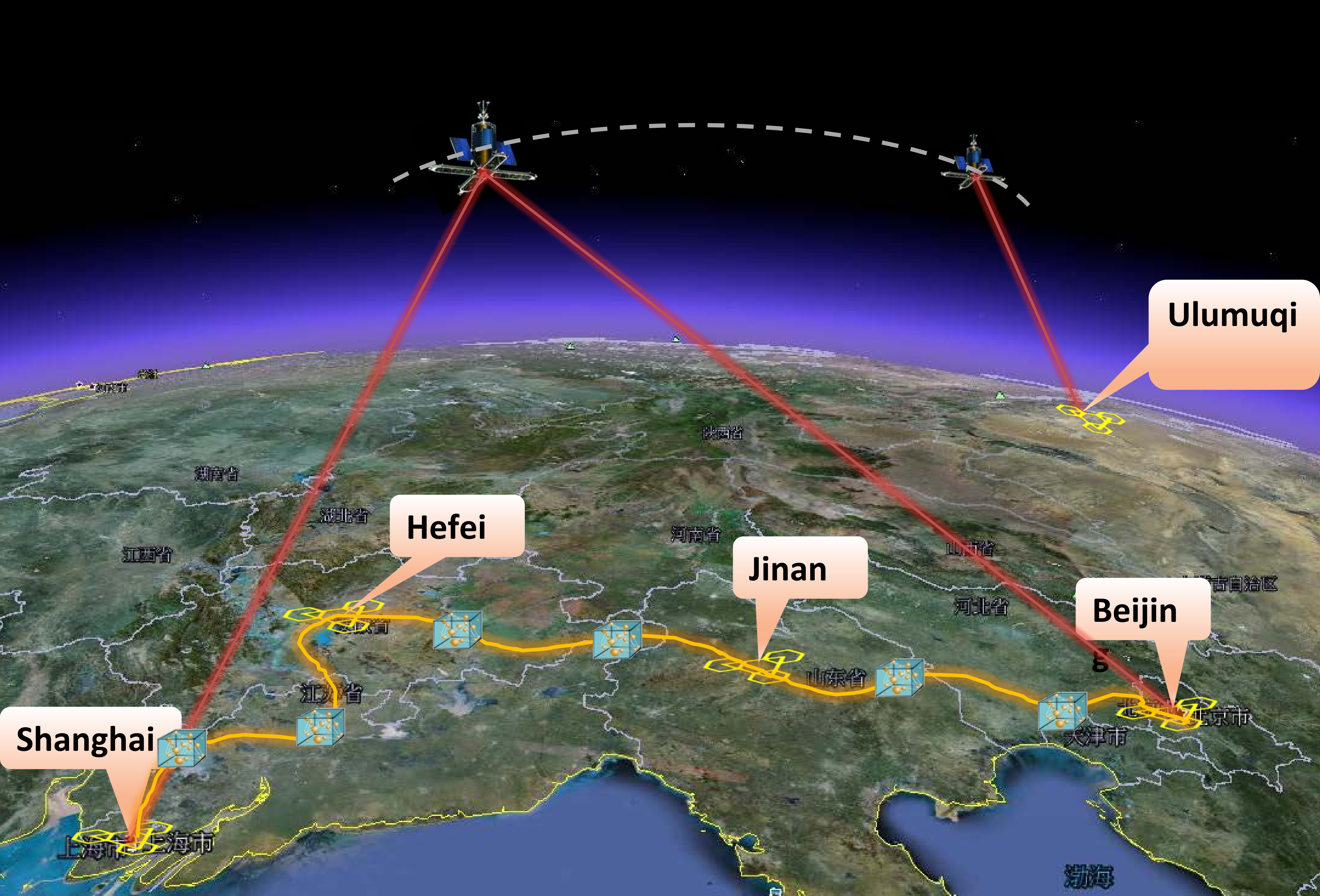


China's Quantum Experiments Plan in Space

- High-rate QKD between satellite and ground
- Quantum entanglement distribution from satellite, test of Bell's inequality over macro-scale
- Quantum teleportation between satellite and ground



Future


Ulumuqi
Hefei
Jinan
Beijin
g
Shanghai
陕西省
湖南省
湖北省
河南省
江西省
山西省
内蒙古自治区
河北省
安徽省
山东省
江苏省
北京市
天津市
上海市
渤海

Thanks for your attention!

Students and Postdocs: Yang Liu, Guoliang Shentu, Qichao Sun, Yanlin Tang, Hualei Yin

Postdocs are welcome!

Colle ngzhi Peng, Jason Pelc, Marty Fejer, Lixin You, Zhen Wang, Yong Zhao, Jian-Wei Pan

973

C·H·I·N·A

国家重点基础研究发展计划

NSFC

中国科学院

CHINESE ACADEMY OF SCIENCES