Investigations on Continuous-variable (CV) Quantum Key Distribution (QKD)

Guihua, Zheng

Peng Huang, Xueqin Jiang, Tao Wang, Shiyu Wang, Hongxin Ma, Dengwen Li

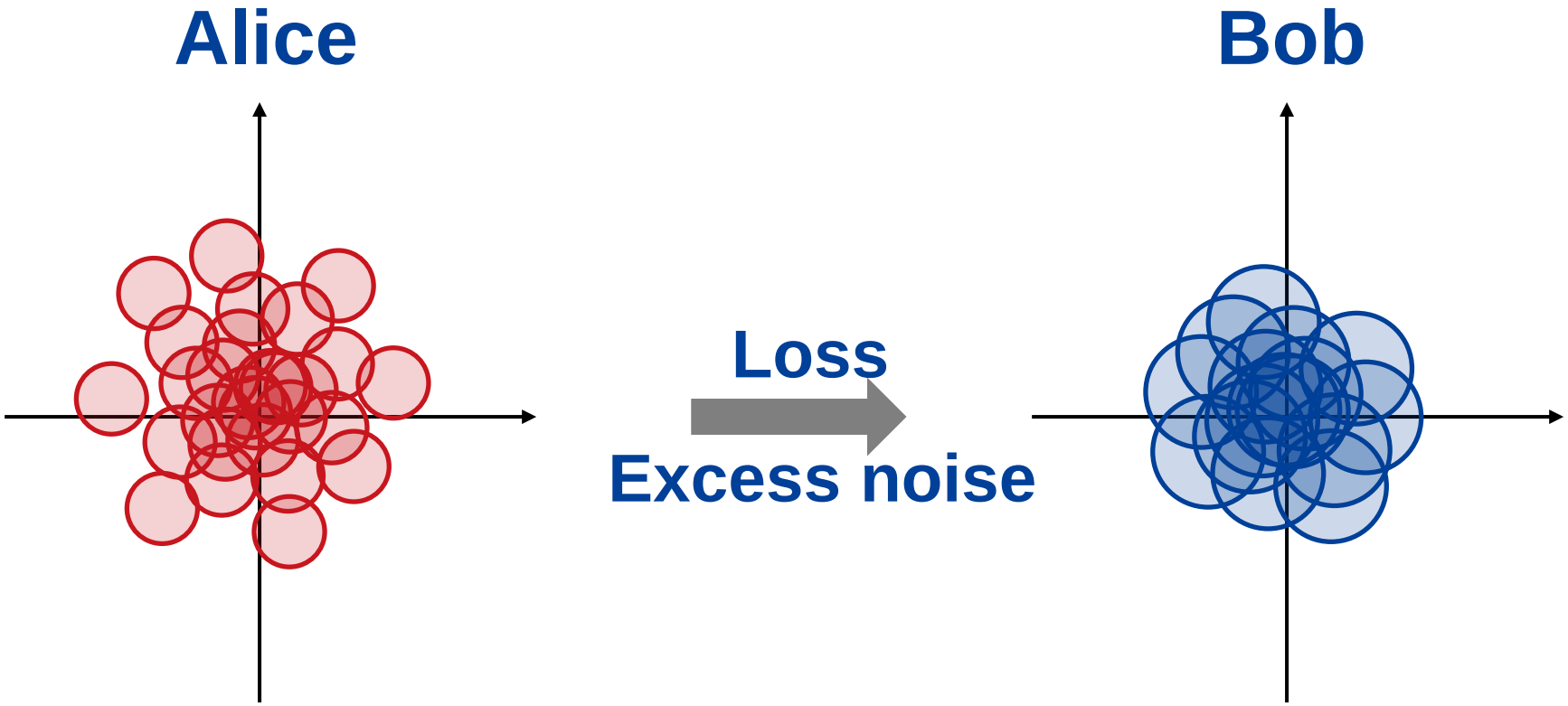
State Key Laboratory of Advanced Optical Communication Systems and Networks,
Center of Quantum Information Sensing and Processing,
Shanghai Jiao Tong University

Contents

The protocols

- Gaussian modulated coherent-state (GMCS) protocol
  - GG02 (F. Grosshans and P. Grangier, 2002)
  - Dual-phase modulation (SJTU, 2009)
- Discrete modulated coherent-state (DMCS) protocol
- Squeezed-state protocol
- Entanglement-based protocol
- …

The protocols



Gaussian-modulated coherent states

Technical developments

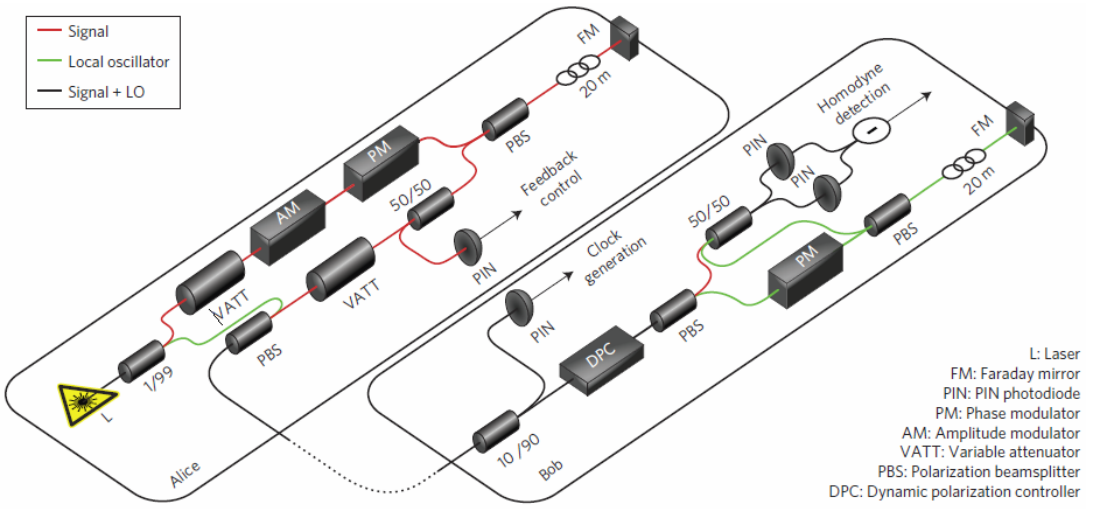
- Long-distance CVQKD
- High-key-rate CVQKD
- Free-space CVQKD
- Practical security

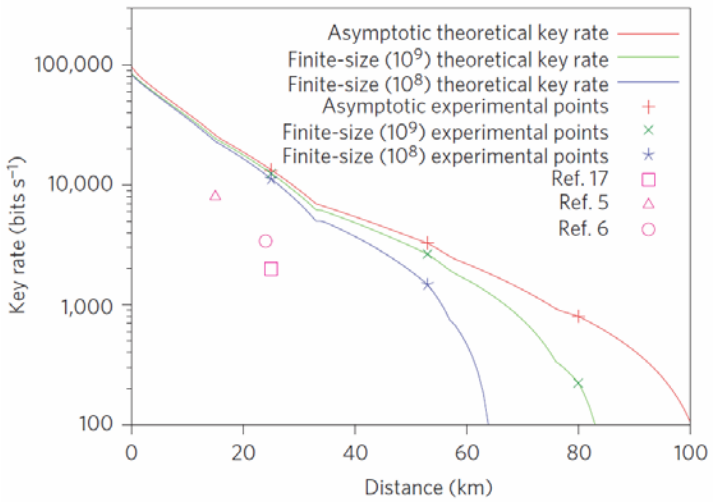
Long-distance CVQKD

- **Problems**
  - **Excess noises (caused by phase and polarization fluctuations, leakage of LO, etc.)**
  - **Loss of LO (make detectors unable to achieve the shot-noise limit.)**
  - **Responsivity of detectors (cannot detect weak signals)**
  - **Reconciliation algorithms (for low SNR)**
  - **Finite-size effects**
  - **…**
- **(Partly) Solved by**
  - **Excess noise control (Scientific Reports 6: 19201 (2016))**
  - **Better detectors (CLEO, FM3A.5, 2014)**
  - **Noiseless amplifier (Phys. Rev. A 86, 012327 (2012))**
  - **High-efficiency reconciliation (Nature photonics 7, 378-381 (2013))**
  - **Post selection (Phys. Rev. A 87, 020303(R) (2013))**
  - **…**

Long-distance CVQKD

- **Transmission distance: 80 km (2013)**
- **The main breakthrough: A high-efficiency reconciliation algorithm, 95%.**

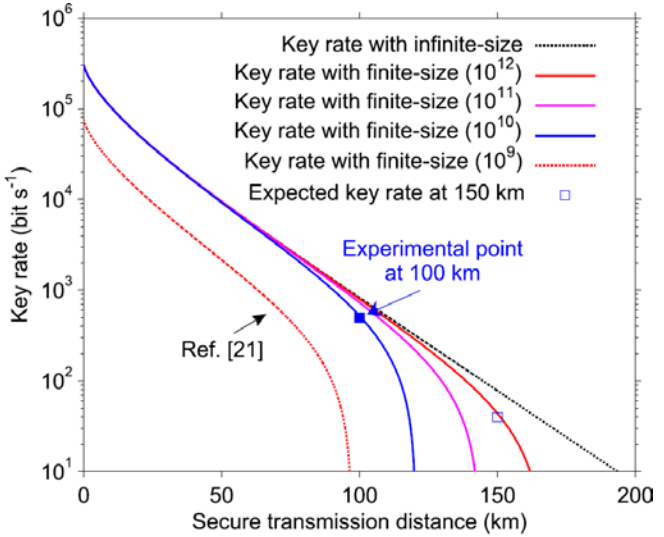




Jouguet, Paul, et al. *Nature photonics* 7.5 (2013): 378.

Long-distance CVQKD

- Transmission distance: 150 km (2016)
- Achieved by using
  - A high-responsivity detector, achieve shot-noise limit at LO intensity of 10^6 photons
  - A high-efficiency reconciliation algorithm, 95.6%
  - A high-precision phase compensation algorithm at low SNR



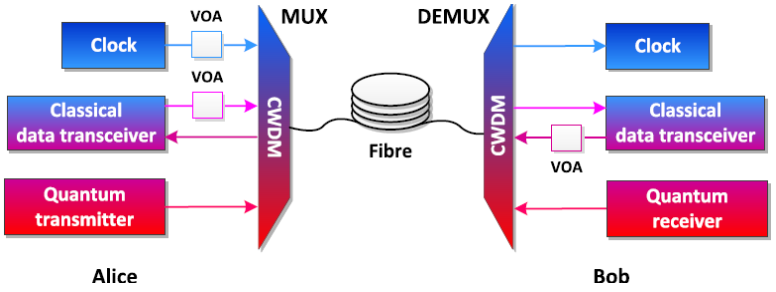
Huang, Duan, et al. Scientific reports 6 (2016): 19201.

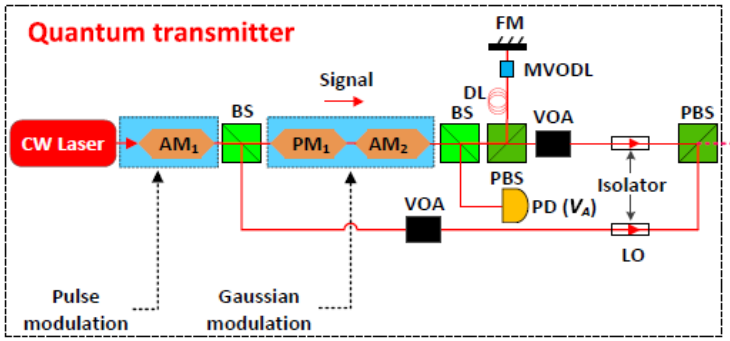
High-key-rate CVQKD

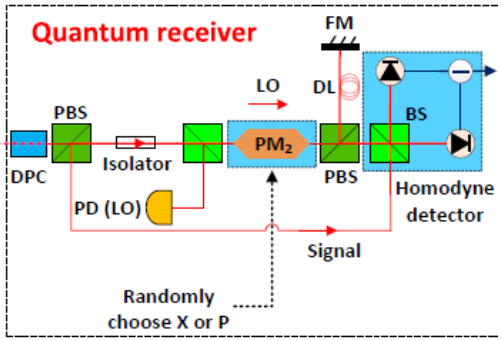
- **Problems**
  - **Excess noises**
  - **Loss of LO**
  - **Finite-size effects**
  - **Detector bandwidth (for high pulse repetition rate)**
  - **Reconciliation algorithms & data acquisition cards (for high-speed data processing)**
  - **…**
- **(Partly) Solved by**
  - **Wideband detectors (Chin. Phys. Lett. 30.11 (2013): 114209.)**
  - **High repetition rate (OE 23.13 (2015): 17511-17519.)**
  - **DWDM/CWDM techniques (New J. Phys. 17.4 (2015): 043027; ECOC. IEEE. 2018. 8535421.)**
  - **Local LO scheme (OL, 40: 3695 (2015); PRX, 5, 041010 (2015); PRA, 94, 032305, (2016); OE, 26: 2794, 2018)**
  - **…**

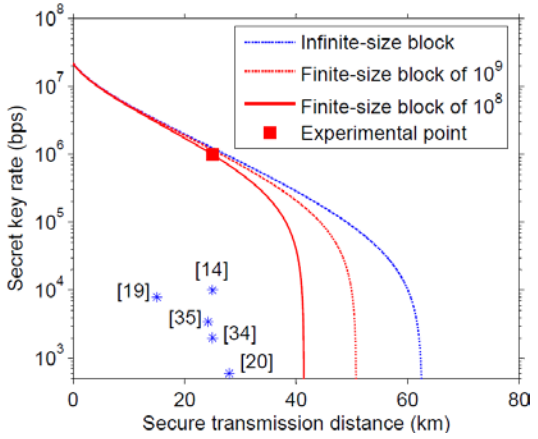
High-key-rate CVQKD

- Average key rate: 1 Mbps @ 25 km (2015)
- Achieved by using
  - A 1-GHz-bandwidth detector
  - 50-MHz repetition rate
- Performed in a CWDM environment





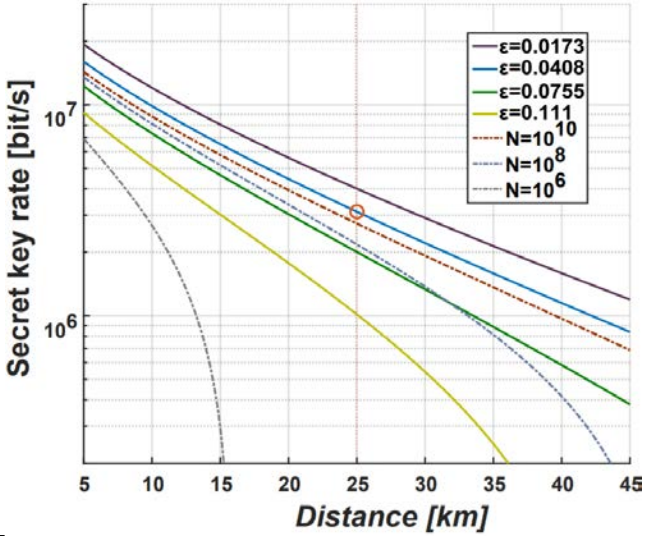


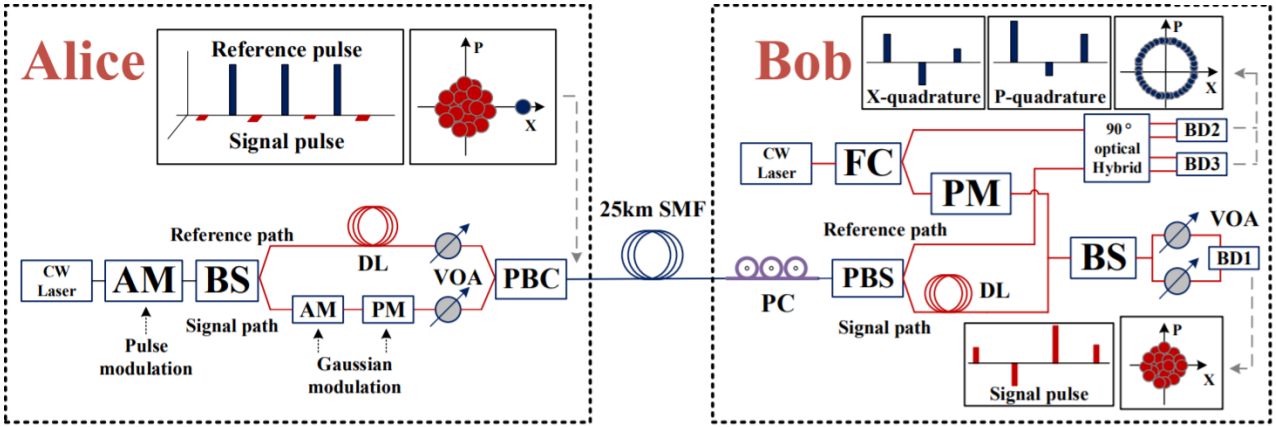


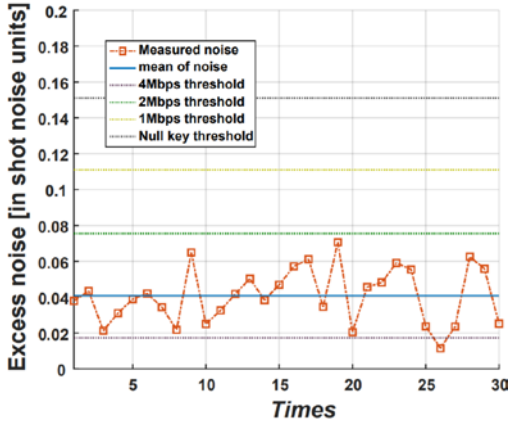
Huang, Duan, et al. Optics express 23.13 (2015): 17511-17519.

High-key-rate CVQKD

- Achievable key rate: **3.14 Mbps @ 25 km** (2018)
- Achieved by
  - **Generating LO locally** (real LO at Bob)
  - Simultaneous generation and detection of reference and signal pulses (ultra-low phase excess noise)
  - **50-MHz repetition rate**



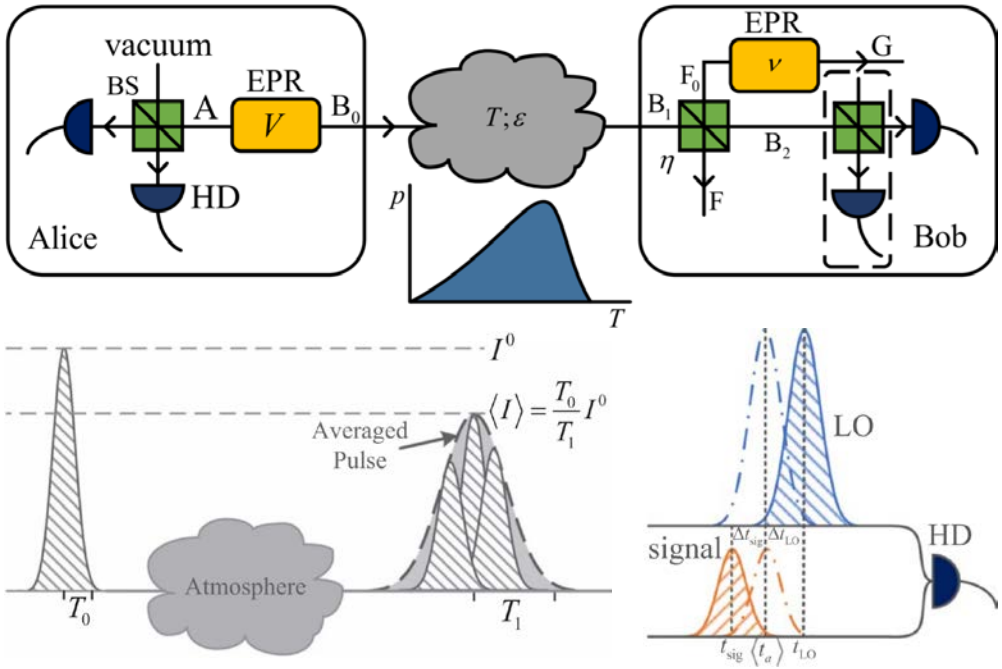




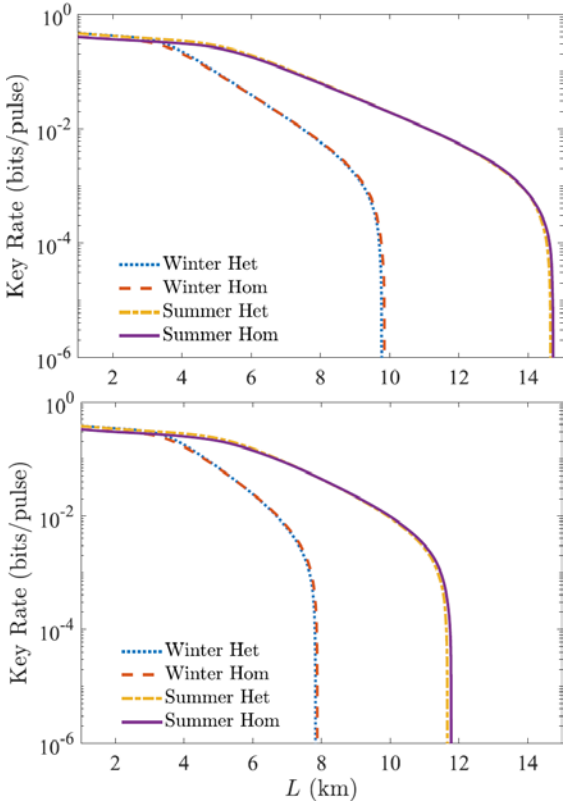
Wang, Tao, et al. Optics express 26.3 (2018): 2794-2806.

Free-space CVQKD

- A theoretical analysis (2018)
- Fixed up key rate calculations under imperfect detections
- Built a transmission model



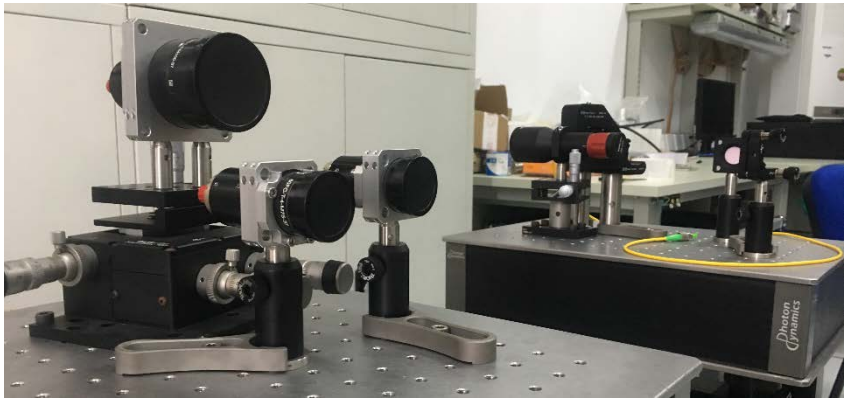
Wang, Shiyu, et al. New J. Phys 20.8 (2018): 083037.

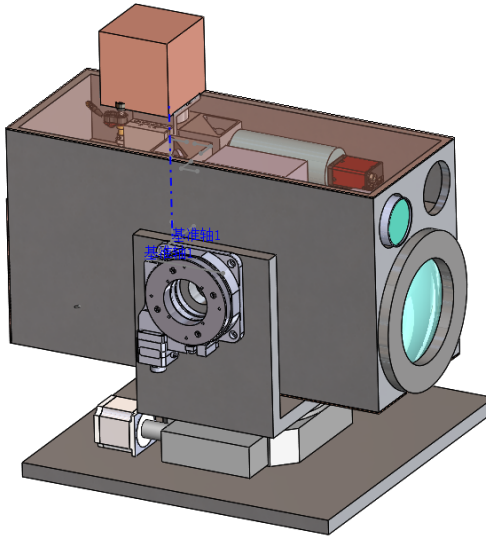


Discrete modulation:
Heim, Bettina, et al. New J. Phys. 16.11 (2014): 113018.
Günthner, Kevin, et al. Optica 4.6 (2017): 611-616.

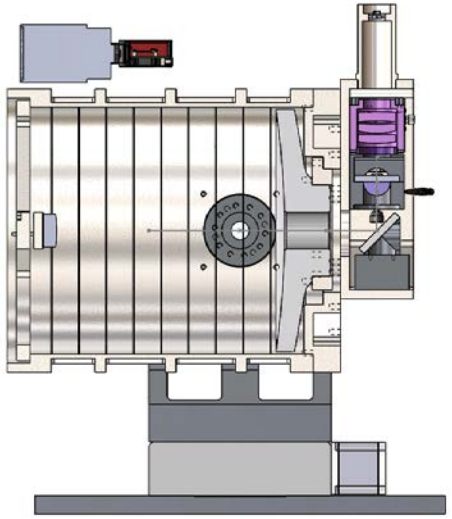
Free-space CVQKD

- In progress
- A fiber-to-freespace link
- Goal: over 10 km
- Short-range verification





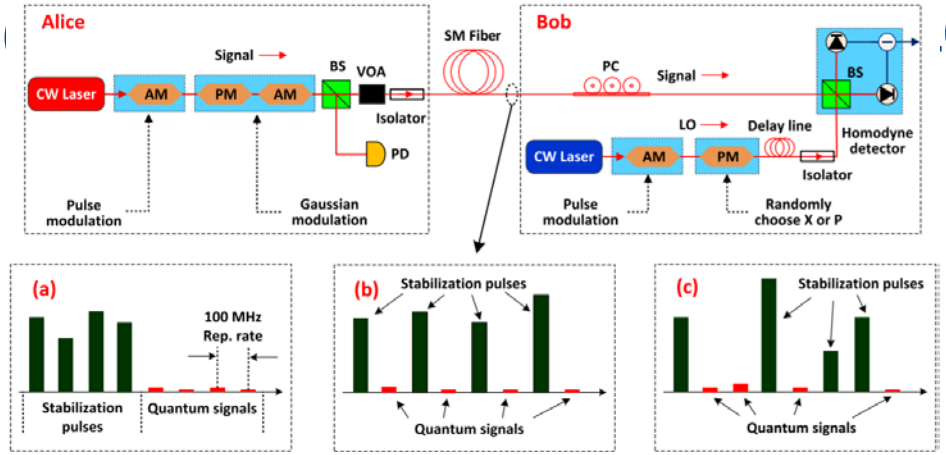
Transmitter

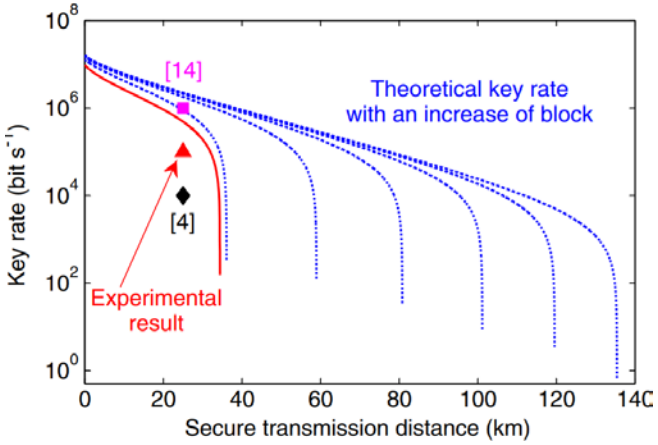


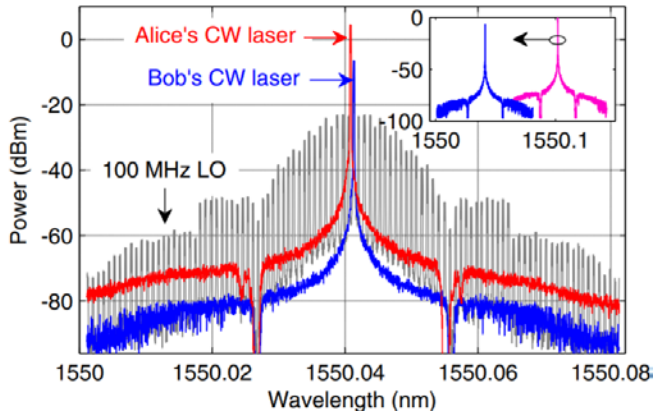
Receiver

Practical security

- Closing loopholes by generating LO locally
- First to implement the local generation scheme (2015)
- Average key rate: 100 kbps @ 25 km
- 100-MHz repetition rate
- Independently proposed by other two groups several months later (PRX 5.4 0)



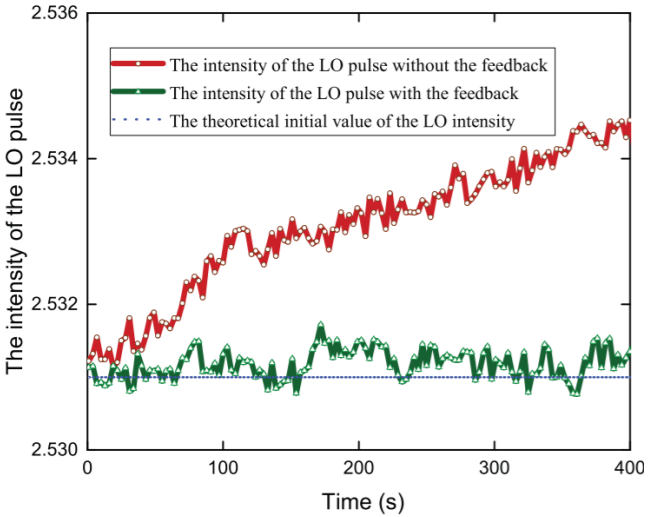


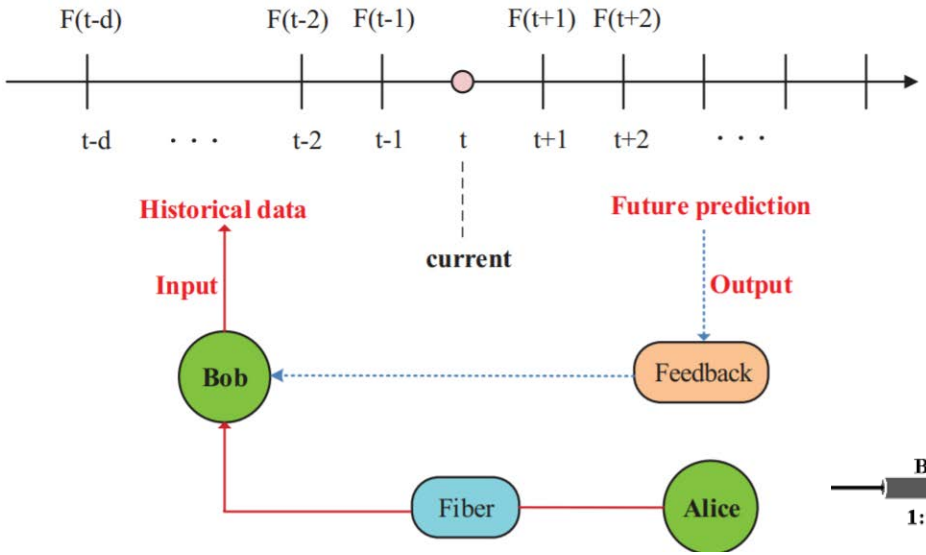


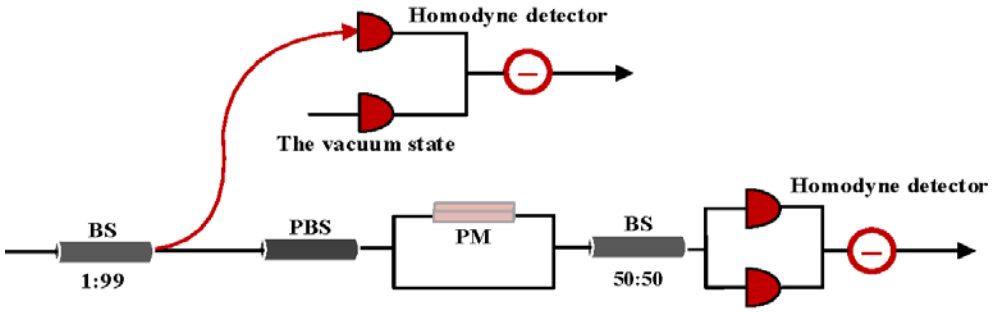
Huang, Duan, et al. Optics letters 40.16 (2015): 3695-3698.

Practical security

- Monitoring practical security by
  - Monitoring LO fluctuations (2017)
  - Predicting system parameters via machine learning: using a support vector regression (SVR) model (2018)



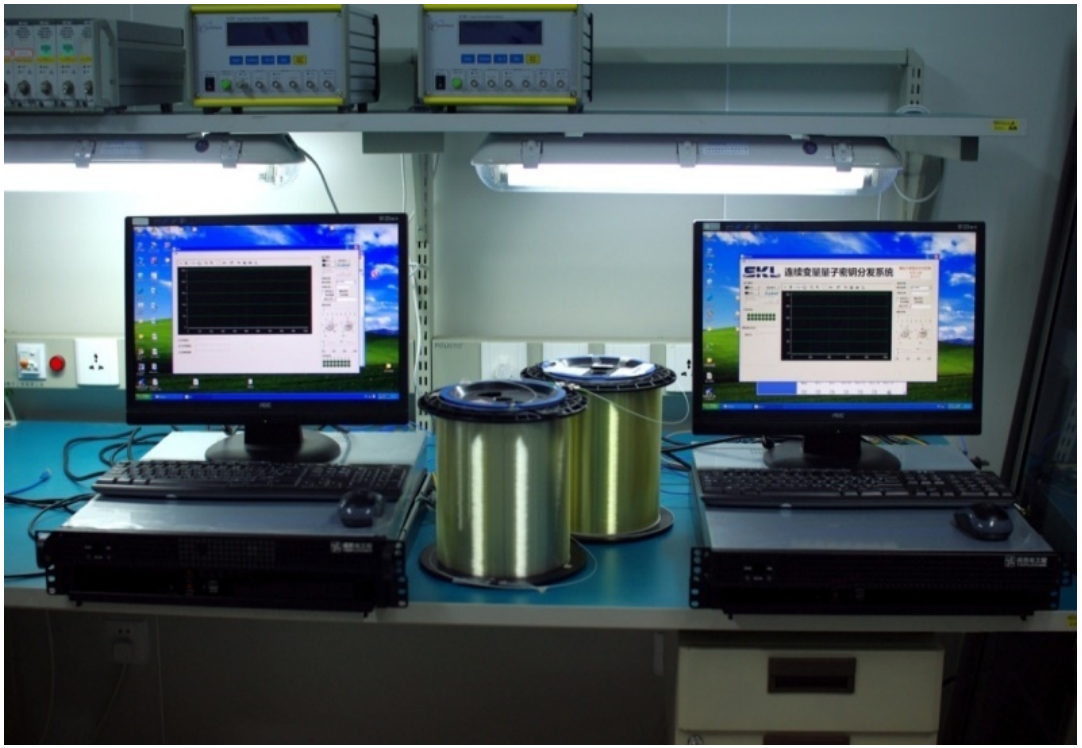




Liu, Weiqi, et al. Optics express25.16 (2017): 19429-19443.
Liu, Weiqi, et al. Physical Review A 97.2 (2018): 022316.

Applications & commercialization

- Prototypes (2015 - 2016)
- 52 kbps @ 50 km

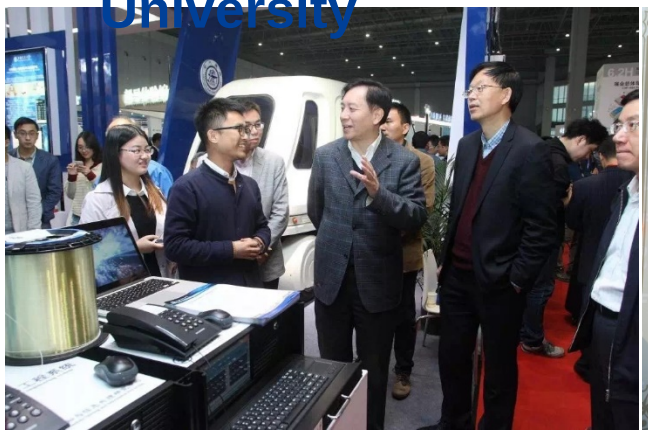


Wang, Chao, et al. Scientific reports 5 (2015): 14607.

Applications & commercialization

For Huawei Co., Ltd

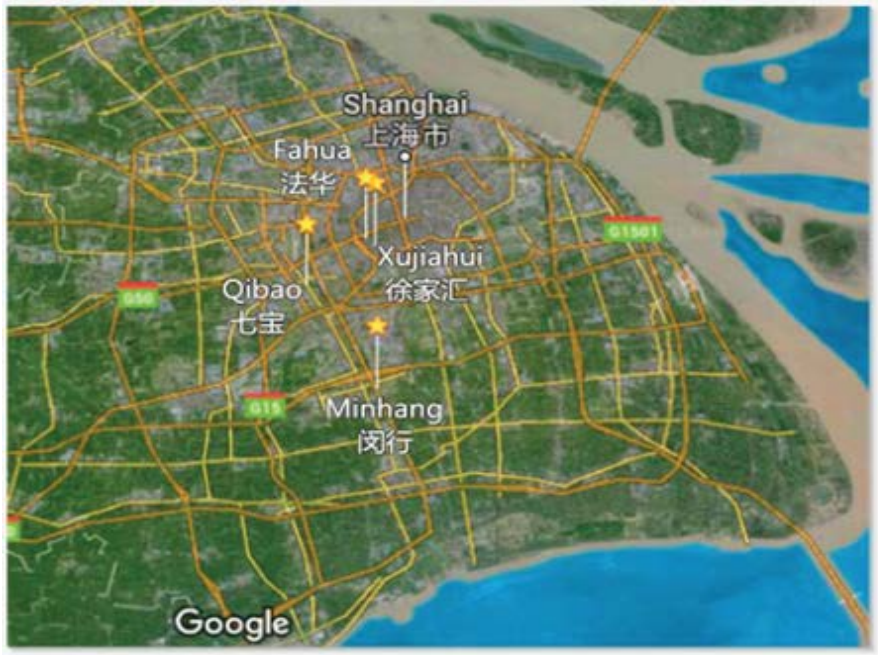
For Northwest University



The demo in China Hi-Tech Fair (2016)

Applications & commercialization

- 2016
- Field demonstration of a CVQKD network
- 4 nodes in Shanghai



Huang, Duan, et al. Optics letters 41.15 (2016): 3511-3514.

Applications & commercialization

循态量子
XTQuantum

www.xtquantech.com

Quantum Security Gateway

QKD Quantum Key Distribution Manageme...

QKD Quantum Key Distribution Equipment

Wavelength Division Multiplexing Equipment

Conclusion

- Some developments have been made on long-distance & high-key-rate issues. Only capable of supporting metropolitan area network (MAN)
- To achieve high key rates at long-distance regime, generating LO locally might be a promising way
- Extending to free space. How far we can go? Technical? Fundamental?
- Practical security. Find loopholes and monitor systems.
- Being commercialized. On the way to engineering design, networks, and standardization

Thank you!