中国科学技术大学
University of Science and Technology of China

Measurement-device-independent quantum key distribution in practical scenarios

Chao Wang **Advisor: Prof. Zheng-Fu Han**

email: wongchao@mail.ustc.edu.cn

University of Science and Technology of China
Key Laboratory of Quantum Information, CAS

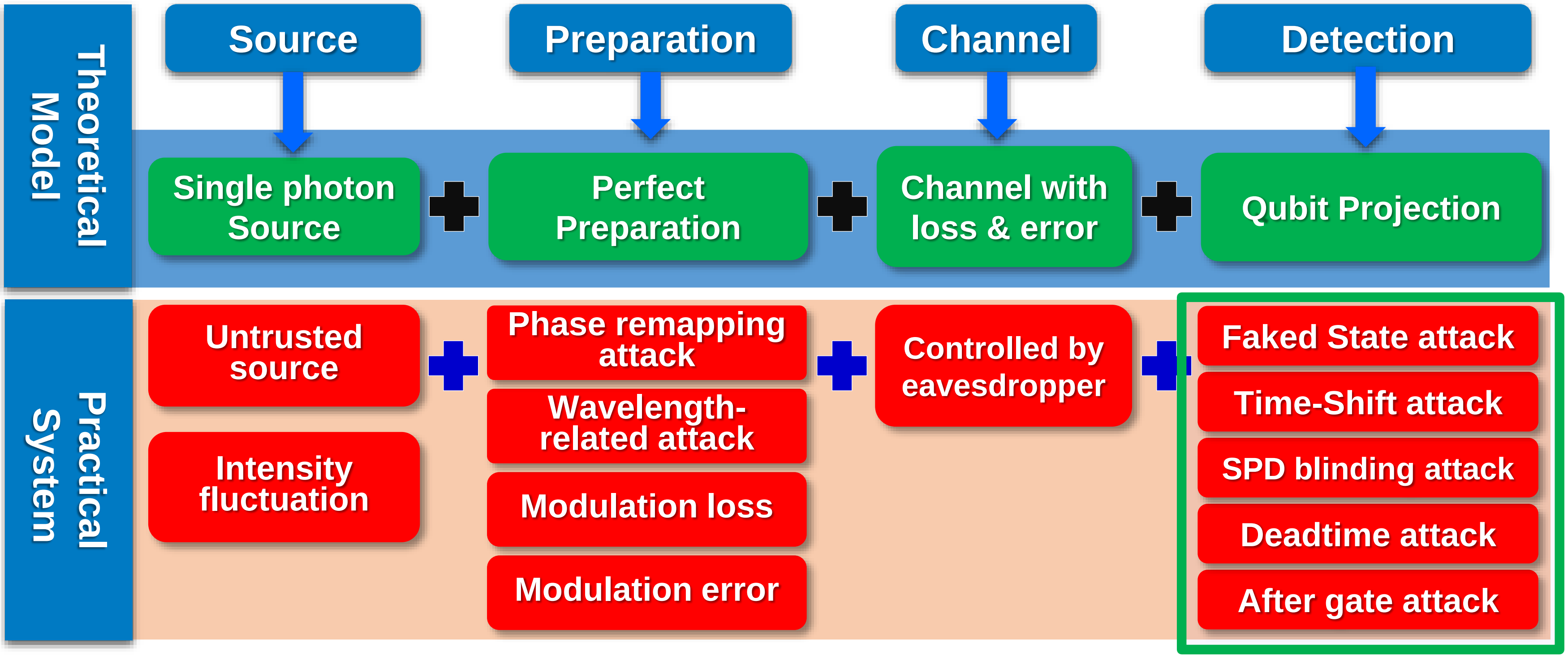
Qcrypt 2017, Cambridge, UK Sept. 19th, 2017

Outline

1. Motivations
2. Eliminate the calibration of reference frames
   - Reference-frame-independent MDI QKD
   - MDI QKD robust against environmental disturbances
3. Eliminate the source characterization
   - MDI QKD with uncharacterized encoding
4. Conclusions

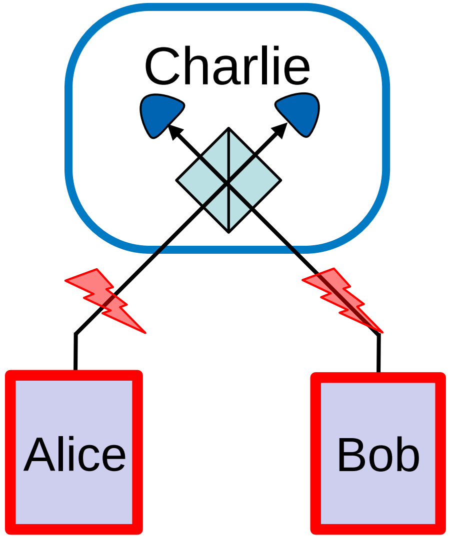
Motivations: Practical Security

- Quantum key distribution (QKD) provides unconditional theoretical security;
- Real-life devices & systems compromise the practical security.



Motivations: MDI QKD protocol

- ❑ Based on time-reversed entanglement protocol,
- ❑ Immune to all possible measurement attacks,
- ❑ Great balance between security and practicability,
- ❑ Promising for star-type QKD networks.



- ❑ Suffers from ***reference frame drift***,
- ❑ Still requires ***trustworthy*** quantum state preparation.

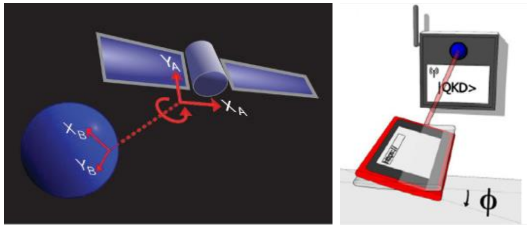
Phys. Rev. Lett. 108, 130503 (2012). Phys. Rev. Lett. 108, 130502 (2012).

Motivations

- Eliminate the calibration of reference frames
- Eliminate the source characterization

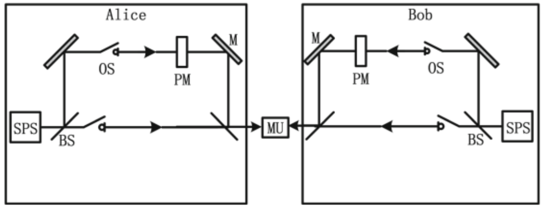
Reference calibrations in MDI QKD

Polarization coding



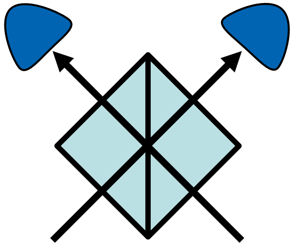
Phys. Rev. A 82, 012304 (2010).
New J. Phys. 15, 073001 (2013).

Phase coding



Quantum Inf. Process. 13, 1237 (2014).

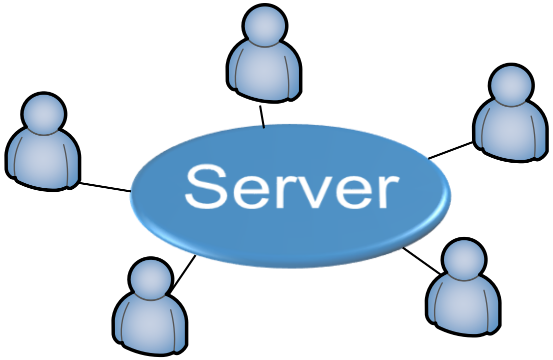
Indistinguishable photons



✓ Spectrum
✓ Timing
✓ Polarization

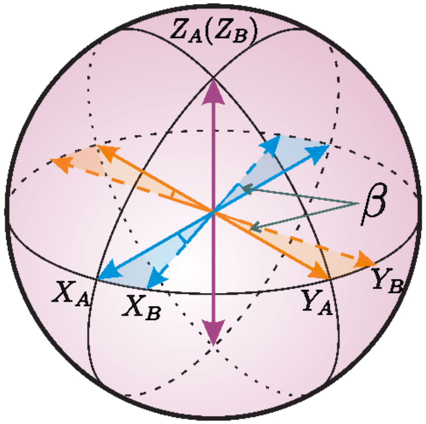
Phys. Rev. Lett. 108, 130502 (2012).

- ❑ Compromise the practical security;
- ❑ Poor performance with inefficient calibration;
- ❑ Result in extra overheads.



"Device calibration impacts security of quantum key distribution." Phys. Rev. Lett. 107, 110501 (2011).

"An attack aimed at active phase compensation in one-way phase-encoded QKD systems." Eur. Phys. J. D 68, 1 (2014).



- The Z basis states are well defined;
- The X, Y basis states may vary with the reference drift $\boldsymbol{\beta}$.

Z basis states: $|0\rangle$,$|1\rangle$ Robust!

X basis states: $\frac{1}{\sqrt{2}}(|0\rangle + e^{i\beta_{A(B)}}|1\rangle)$,$\frac{1}{\sqrt{2}}(|0\rangle - e^{i\beta_{A(B)}}|1\rangle)$

Y basis states: $\frac{1}{\sqrt{2}}(|0\rangle + ie^{i\beta_{A(B)}}|1\rangle)$,$\frac{1}{\sqrt{2}}(|0\rangle - ie^{i\beta_{A(B)}}|1\rangle)$

$$C = (1-2e_{XX})^2 + (1-2e_{YY})^2 + (1-2e_{XY})^2 + (1-2e_{YX})^2$$

- Does not change with $\boldsymbol{\beta}$;
- Effective for bounding Eve's information.

A. Laing *et al.*, Phys. Rev. A 82, 012304 (2010). Z-Q. Yin *et al.*, Quantum Inf. Process. 13, 1237 (2014).

RFI MDI QKD

Wavelength-locking laser
- Center wavelength locked to 1542.38nm;
- Center wavelength accuracy: 0.0001 nm (10 MHz);
- Frequncy linewidth after wave chopping: 400MHz.

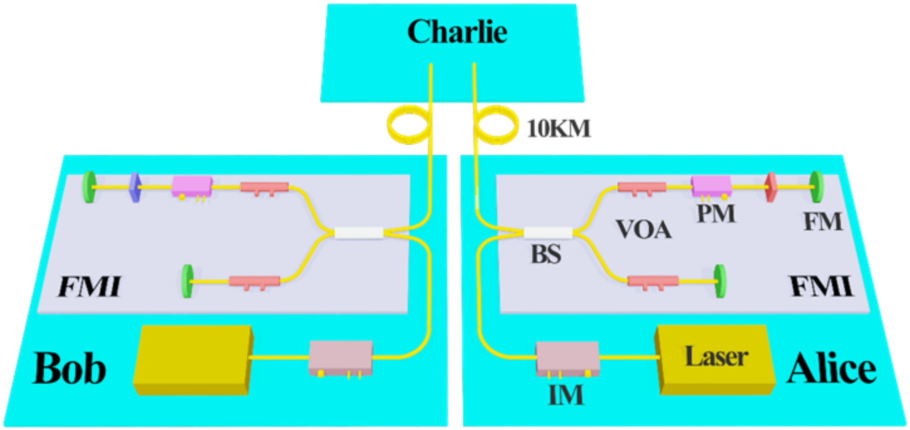
Fine-tuned timing system
- Pulse generating with a duration of 2.5 ns;
- Trigger signal for all devices;
- 10 ps resolution of adjustment.

Faraday-Michelson Interferometer
- Two time-bins with 24.5 ns delay;
- Arbitrary qubit preparation with high efficiency;
- Intrinsically stable to polarization fluctuations.

Electrical polarization controller
- Arbitrary polarization state transformation;
- Check the HOM dip every 30 min.

Qasky WT-SPD 100
- Gate width: 2.5 ns;
- Average efficiency: 12%;
- Dark count rate: 9.79×10^{-6} per gate;
- Dead time: 5 μs.

C. Wang *et al.*, Phys. Rev. Lett. 115, 160502 (2015).



Challenges ahead

Performance of the practical MDI system

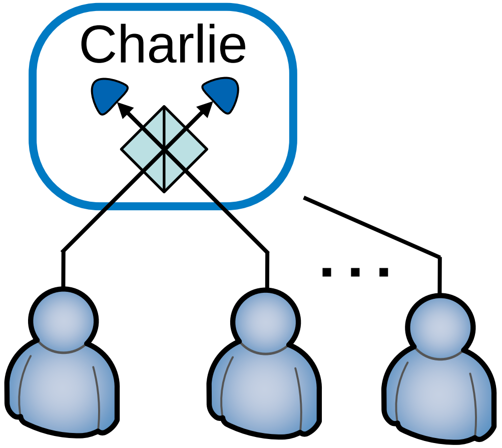
↑

Bell state measurements (BSM)

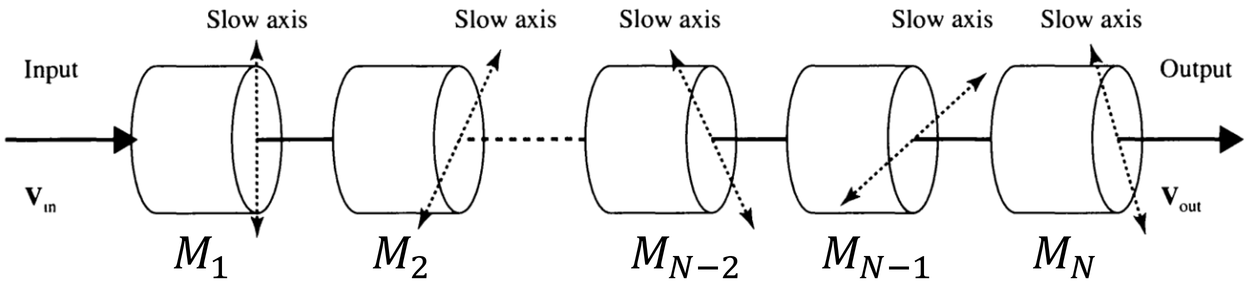
↑

Indistinguishability of incident photons

- ✓ **Spectrum**
- ✓ **Timing**
- **Polarization**



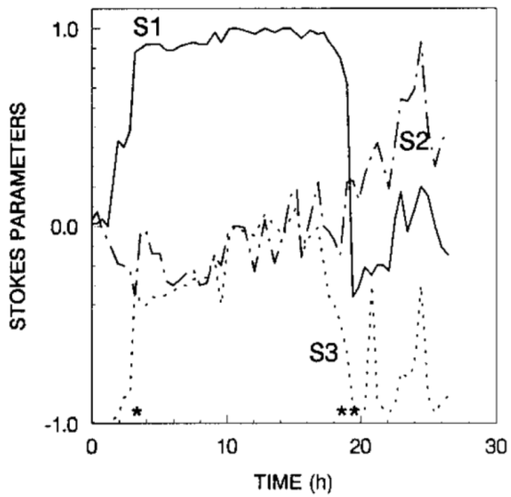
The fiber birefringence can be affected and accumulated by environmental disturbances.



$$V_{out} = M_N M_{N-1} \cdots M_3 M_2 M_1 V_{in}$$

Polarization in field fibers

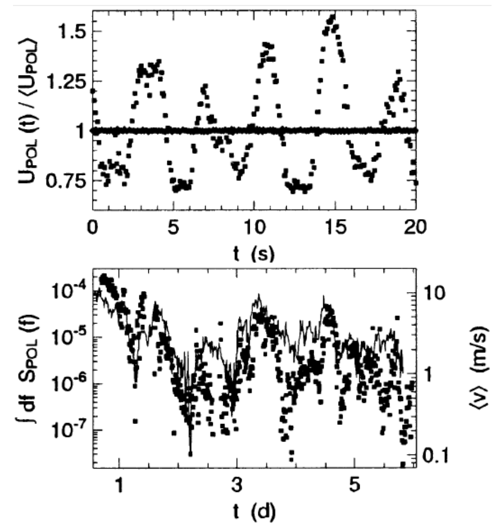
Temperature



57km terrestrial fiber:
100% variation of Stokes in 20min.

JLT **10**, 552 (1992).

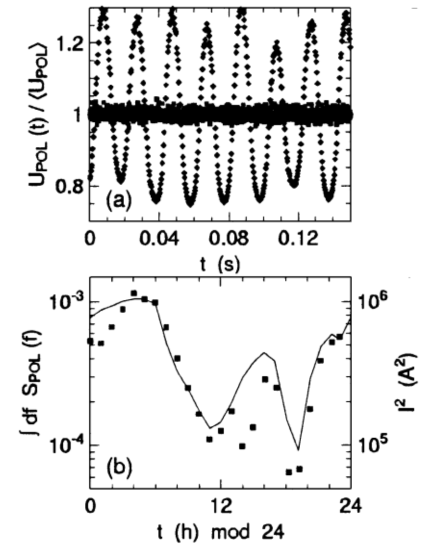
Stress(wind)



180km aerial fiber

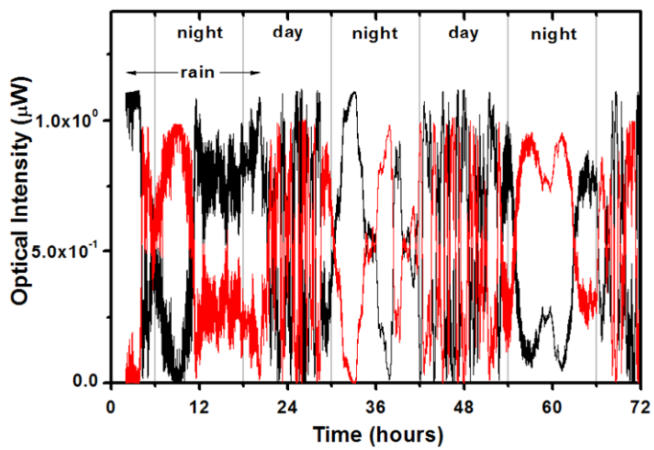
IEEE Photon. Tech. Lett. **15**, 882 (2003).

Current



180km aerial fiber, with 220KV-50Hz AC line

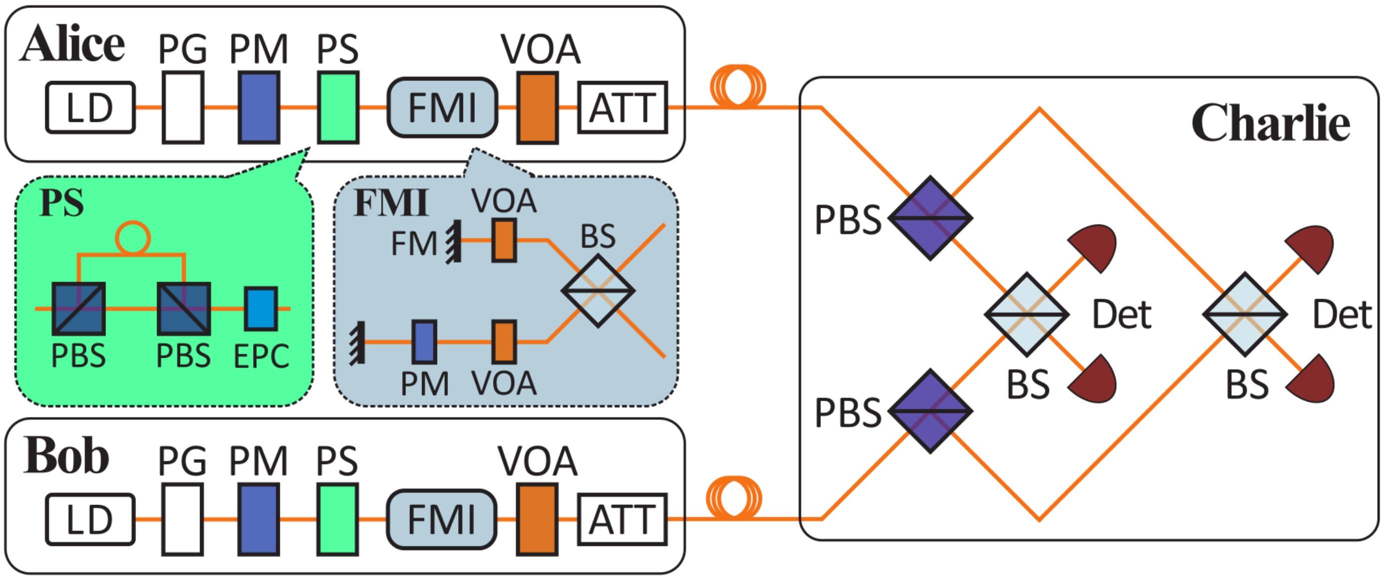
IEEE Photon. Tech. Lett. **15**, 882 (2003).



45km installed fiber in Tokyo

OE, 20, 16339 (2012)

Robust MDI QKD



LD: laser diode
PM: phase modulator
PG: pulse generation
PS: polarization scrambling
EPC: E-polarization controller
FMI: Faraday-Michelson interferometer
FM: Faraday mirror
VOA: variable optical attenuator
ATT: attenuator
BS: beam splitter
PBS: polarizing beam splitter
Det: detector (Qasky)

✓ Frequency-locked lasers
✓ Timing calibration
✕ Phase reference calibration
✕ Polarization calibration

❑ MDI QKD with minimum auxiliary equipment for calibration;
❑ Robust against extreme channel conditions and multi-user networks.

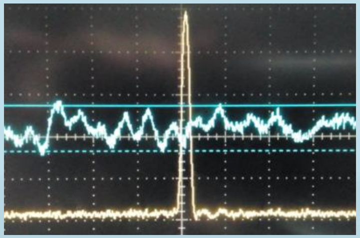
C. Wang *et al.*, Optica 4, 1016 (2017).

Motivations

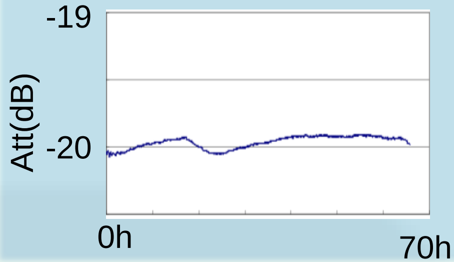
- Eliminate the calibration of reference frames
- **Eliminate the source characterization**

State preparation errors

Voltage fluctuations

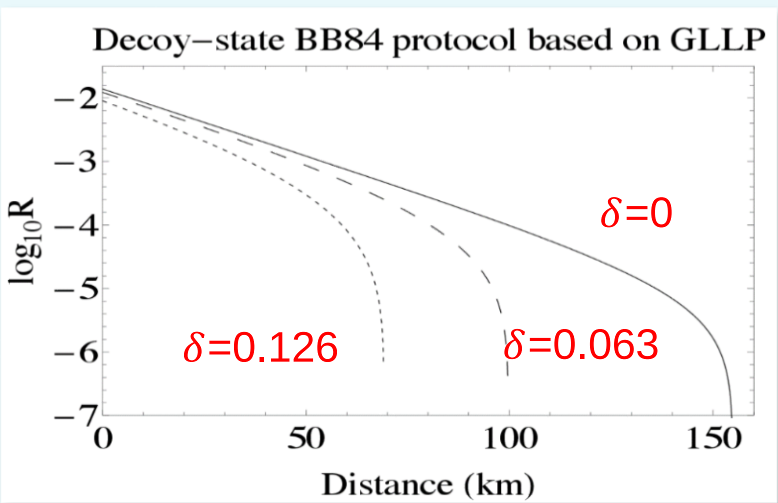


Device instability

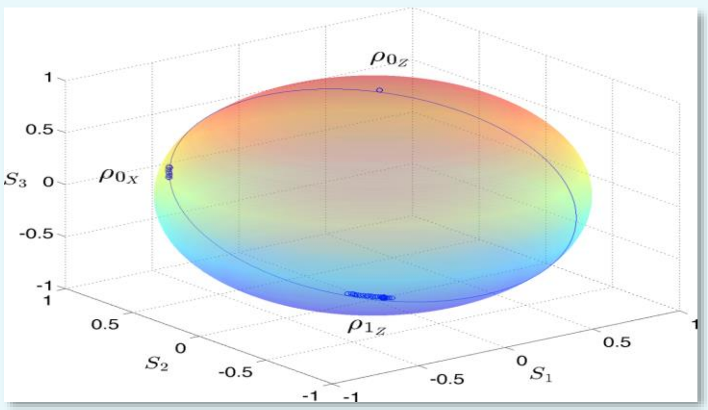


- ❑ ***Inevitable*** imperfections of the preparation states.
- ❑ Compromise the practical security of MDI systems.

Existing solutions: Full characterizations required.



D. Gottesman *et al.*, Quantum Inf. Comput. 5, 325 (2004).



- **Full characterization of the signal states**
- **Rejected-data analysis**

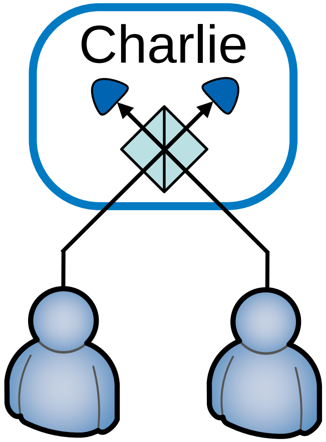
K. Tamaki et al., Phys. Rev. A 90, 052314 (2014).
Z. Tang et al., Phys. Rev. A 93, 042308 (2016).

Mismatched-basis statistics

- Why mismatched-basis statistics can be used for security:

Projection states: BSM: $\begin{cases} |\phi^+\rangle = (|0\rangle|0\rangle + |1\rangle|1\rangle)\sqrt{2} \rightarrow \text{message: } 1 \\ others \rightarrow \text{message: } 0 \end{cases}$

Encoding states: $Z\ basis: \begin{cases} 0: |0\rangle \\ 1: |1\rangle \end{cases}$ $X\ basis: \begin{cases} 2: |+\rangle = (|0\rangle + |1\rangle)/\sqrt{2} \\ 3: |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2} \end{cases}$



z \ x,y	0,0	0,1	1,0	1,1	2,2	2,3	3,2	3,3
0	1/2	1	1	1/2	1/2	1	1	1/2
1	1/2	0	0	1/2	1/2	0	0	1/2
z \ x,y	0,2	0,3	1,2	1,3	2,0	3,0	2,1	3,1
0	3/4	3/4	3/4	3/4	3/4	3/4	3/4	3/4
1	1/4	1/4	1/4	1/4	1/4	1/4	1/4	1/4

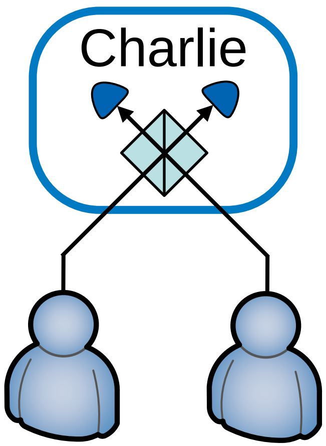
In MDIQKD protocol, Alice and Bob know their encoding states, then above probability table guarantees the security of key bits.

Z. Yin *et al*., Phys. Rev. A **90**, 052319 (2014).

Mismatched-basis statistics

- Why mismatched-basis statistics can be used for security:

Projection states: BSM: $\begin{cases} |\phi^+\rangle = (|0\rangle|0\rangle + |1\rangle|1\rangle)\sqrt{2} \rightarrow \text{message: } 1 \\ others \quad\quad\quad\quad\quad\quad\quad\quad \rightarrow \text{message: } 0 \end{cases}$



Encoding states: $Z\ basis: \begin{cases} 0: |0\rangle \\ 1: |1\rangle \end{cases}$ $X\ basis: \begin{cases} 0: |0\rangle \\ 1: |1\rangle \end{cases}$

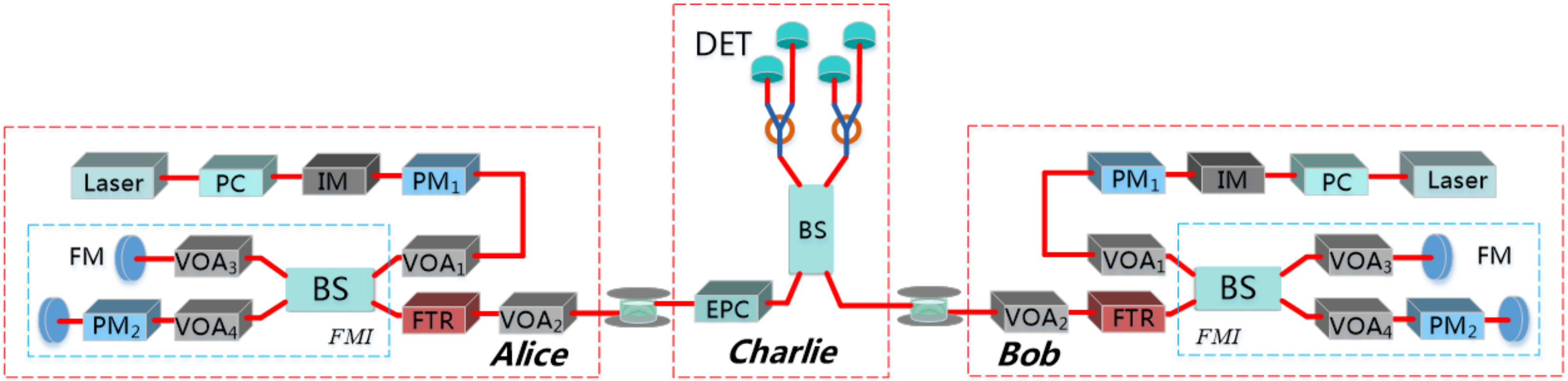
z \ x,y	0,0	0,1	1,0	1,1	2,2	2,3	3,2	3,3
0	1/2	1	1	1/2	1/2	1	1	1/2
1	1/2	0	0	1/2	1/2	0	0	1/2

z \ x,y	0,2	0,3	1,2	1,3	2,0	3,0	2,1	3,1
0	1/2	1	1	1/2	1/2	1	1	1/2
1	1/2	0	0	1/2	1/2	0	0	1/2

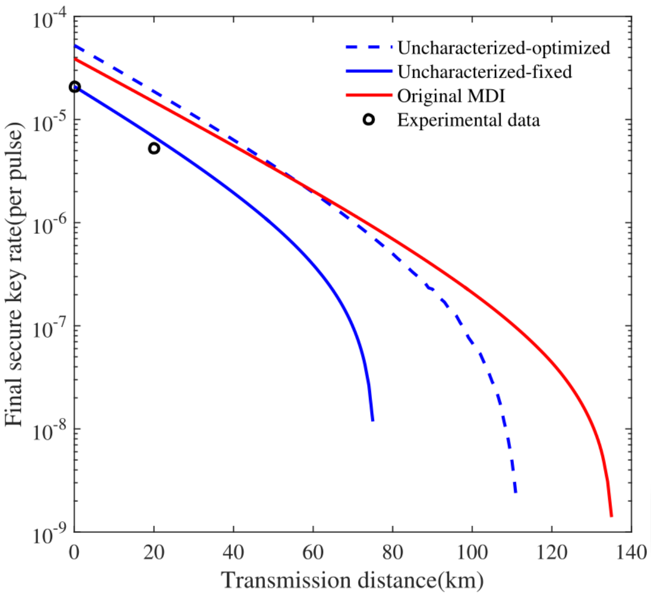
If Alice and Bob's devices are spoiled and send $|0\rangle$ for bits 0 and 2, $|1\rangle$ for bits 1 and 3, then above probability table ***cannot*** guarantee the security!

Z. Yin *et al.*, Phys. Rev. A **90**, 052319 (2014).

MDI QKD with uncharacterized encoding



Rebound the Phase error rate: $e_p \leq e_b + \varepsilon$ related to mismatched data



Realistic modulation error: 0.033 rad, can't even obtain a positive secure key rate with GLLP-SPF method.

- Preparation perfection or error characterization is no longer required;
- Only two-dimensional quantum states are demanded;
- Higher security with simpler constructions.

Z. Yin *et al*., Phys. Rev. A **90**, 052319 (2014). C. Wang *et al*., Optics Letters **41**, 5596 (2016).

Conclusion

1. **MDI QKD with encoding reference calibration eliminated**
    1) **avoids potential loopholes from additional process;**
    2) **mitigates expensive alignment overheads.**
2. **MDI QKD robust against environmental disturbances**
    1) **further lessens the calibration requirements**
    2) **stable in extreme channel conditions**
3. **MDI QKD with uncharacterized encoding**
    1) **source error characterization no longer required**
    2) **higher security with simpler constructions**

… …

Thank you for your attention

Our QKD group from USTC