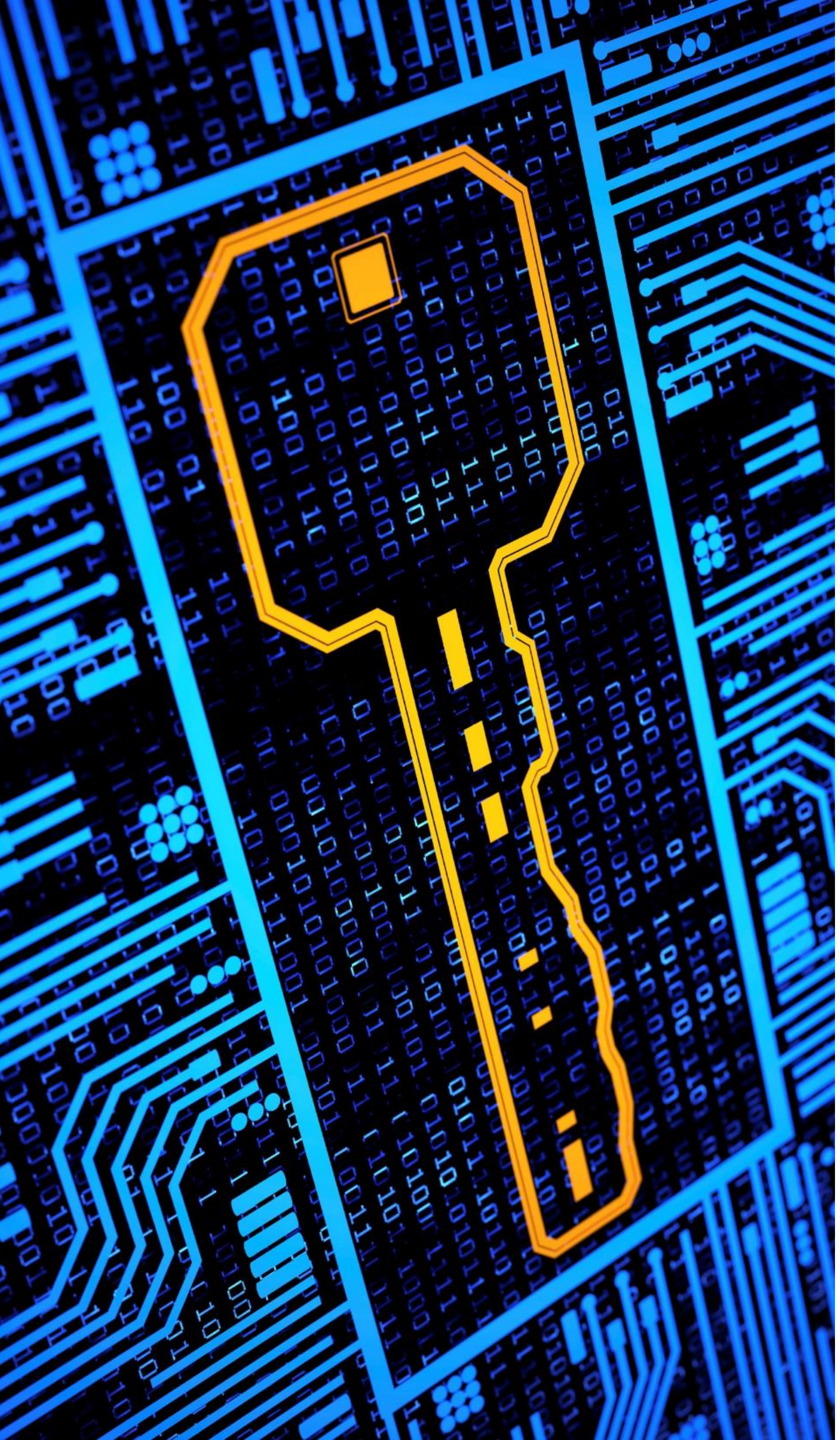


High-speed MDI-QKD with silicon photonics: experiment and side channels

arXiv: 1911.00690 (2019)

Wei Li, Feihu Xu

Kejin Wei, Hao Tan, Hao Min, Xiao Jiang, Sheng-Kai Liao, Cheng-Zhi Peng, and Jian-Wei Pan

National Laboratory for Physical Sciences at the Microscale,

University of Science and Technology of China (USTC)

QKD networks

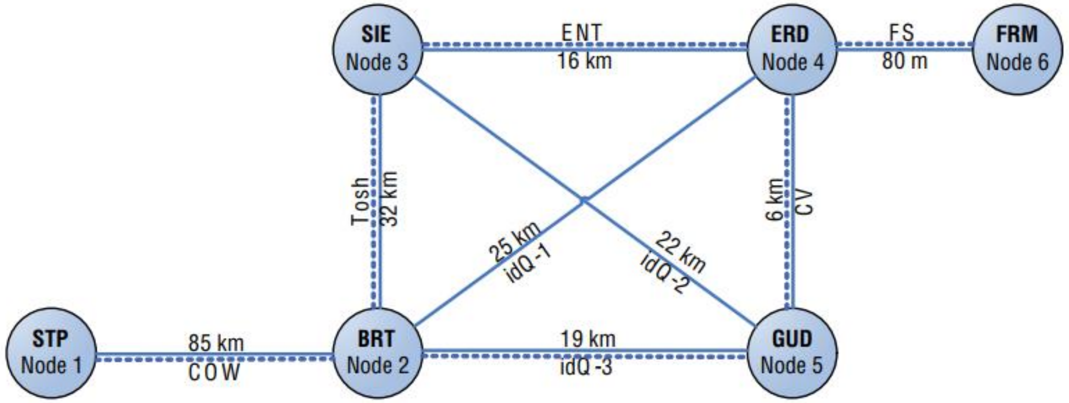


Fig. a

- C. Elliott, arXiv: quant-ph/0503058 (2005). **U.S.**
- M. Peev et al., New J. Phys. 11, 075001 (2009). **Europe**
- T.-Y. Chen et al., Opt. Express 18, 27217 (2010). **China**
- M. Sasaki et al., Opt. Express 19, 10387 (2011). **Japan**

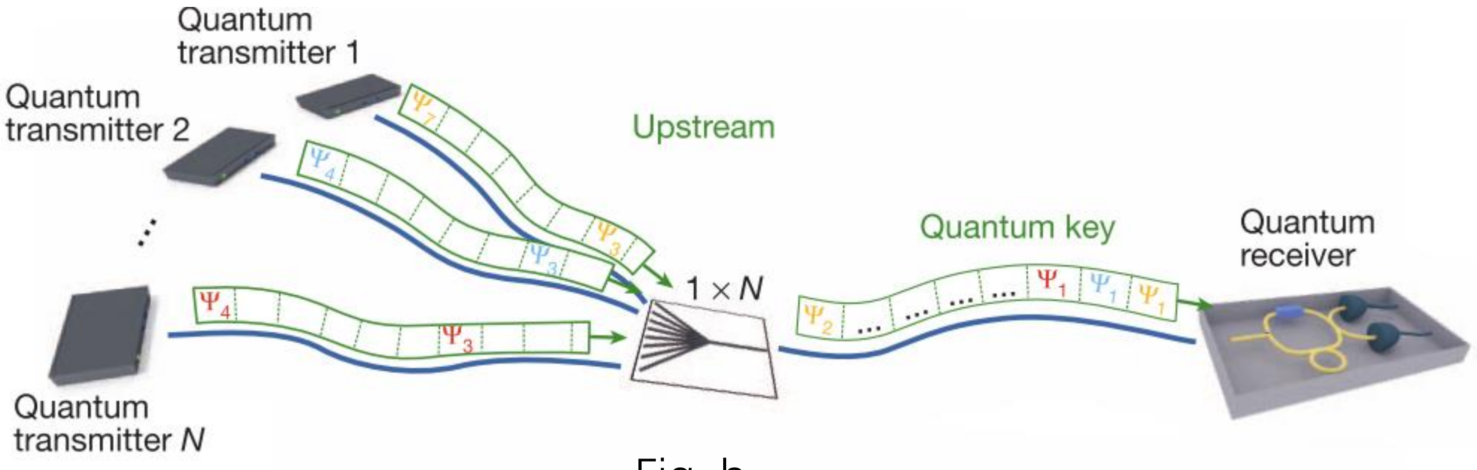


Fig. b

- B. Frohlich et al., Nature 501, 69 (2013).
- R. J. Hughes et al., arXiv:1305.0305 (2013).

QKD networks with *untrusted* relay is needed

Chip-based QKD

Si

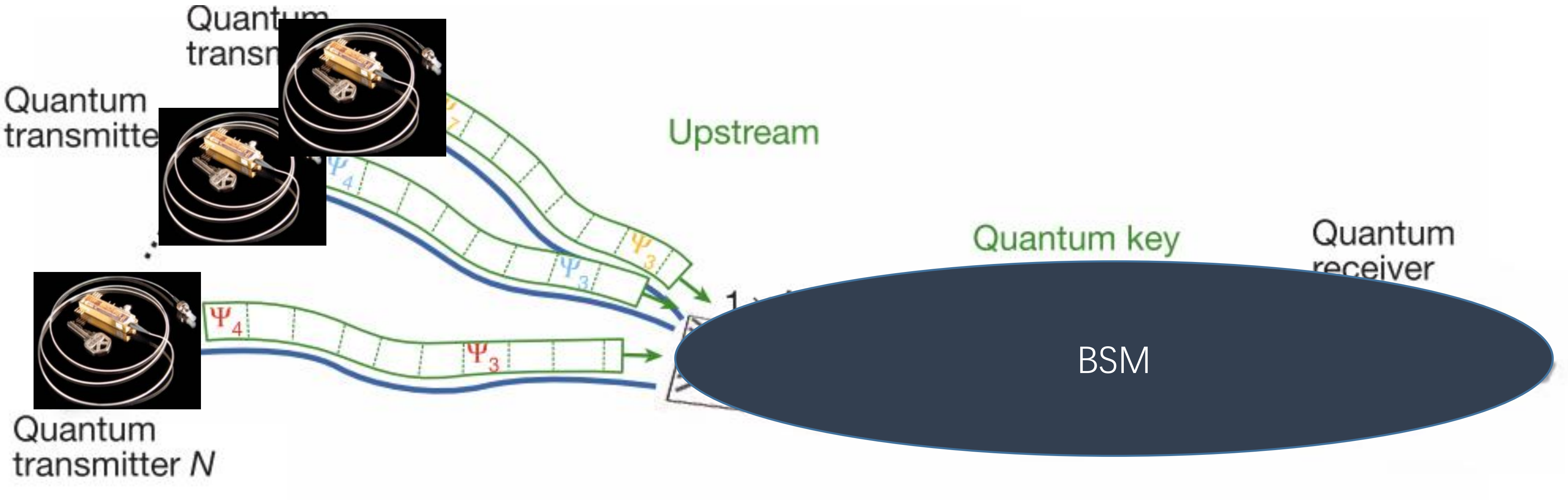
- C. Ma et al., Optica 3, 1274 (2016). (**Transmitter, BB84**)
- P. Sibson et al., Optica 4, 172 (2017). (**COW, BB84**)
- D. Bunandar et al., PRX 8, 021009 (2018) (**BB84 field test**)
- C. Agenesi et al., Optics Letters 2, 44 (2019). (**Laser for MDI**)
- G. Zhang et al., Nat. Photonics 13, 839 (2019). (**Continuous variable**)

InP

- P. Sibson et al., Nat. Commun. 8, 13984 (2017). (**COW, BB84, DPS**)
- H. Semenenko et al., Optics Letters 2, 44 (2019). (**Laser for MDI**)
- H. Semenenko et al., Optica 7, 238 (2019). (**MDI, concurrent with our work**)

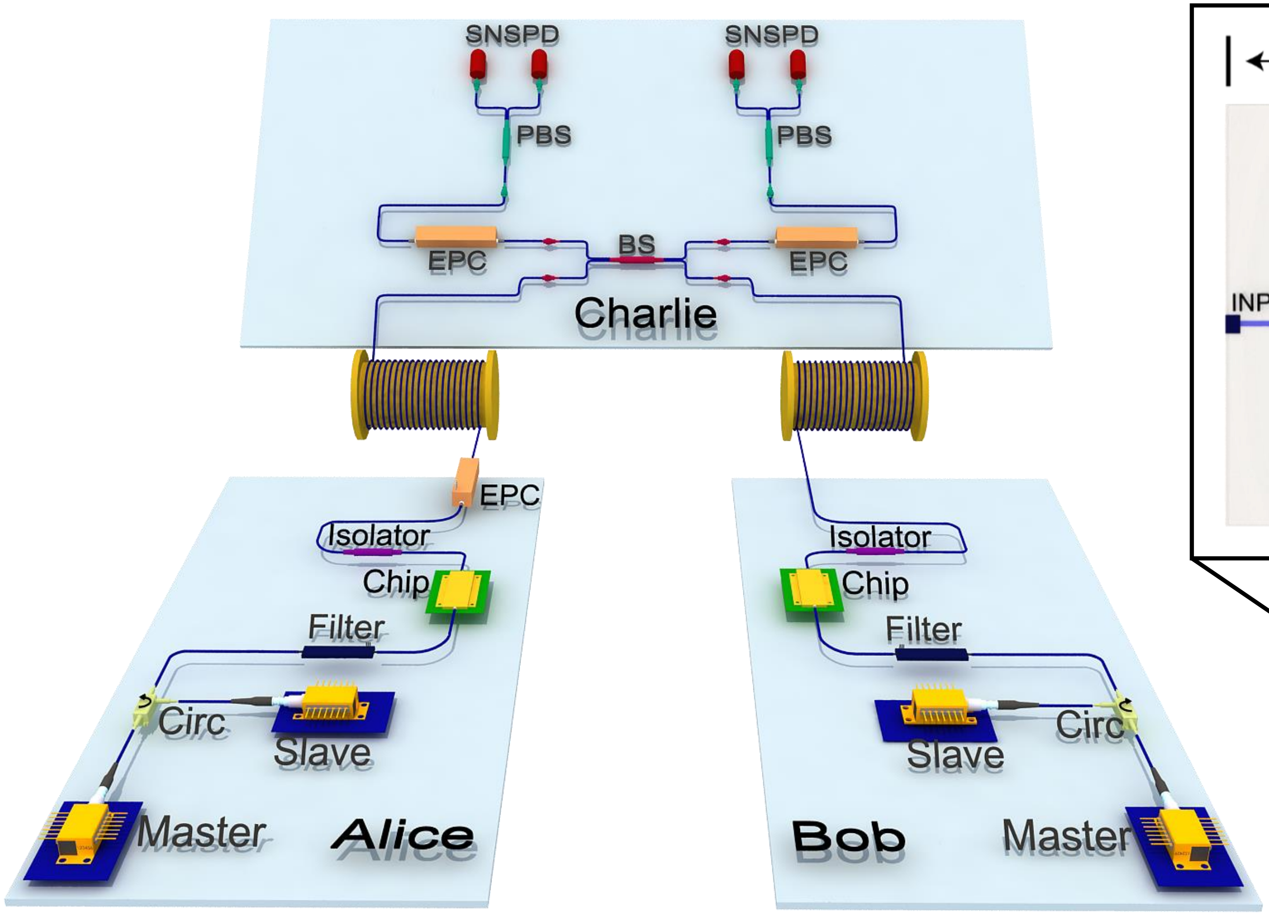
Integration is inevitable for future developments

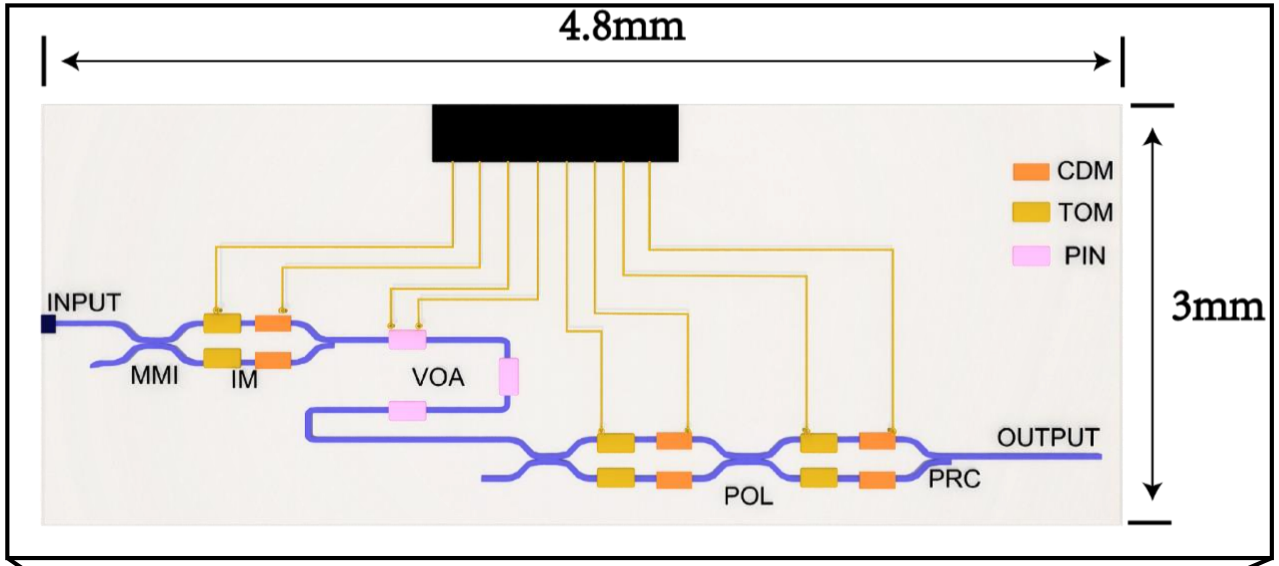
Chip-based MDI-QKD network

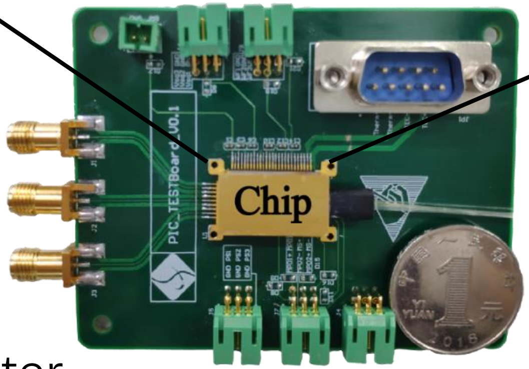


- Enhanced security: *untrusted* relay
- Low cost: mass production
- Scalable: star-type topology
- Chip: transmitter only, free of loss

GHz chip-based MDI-QKD setup





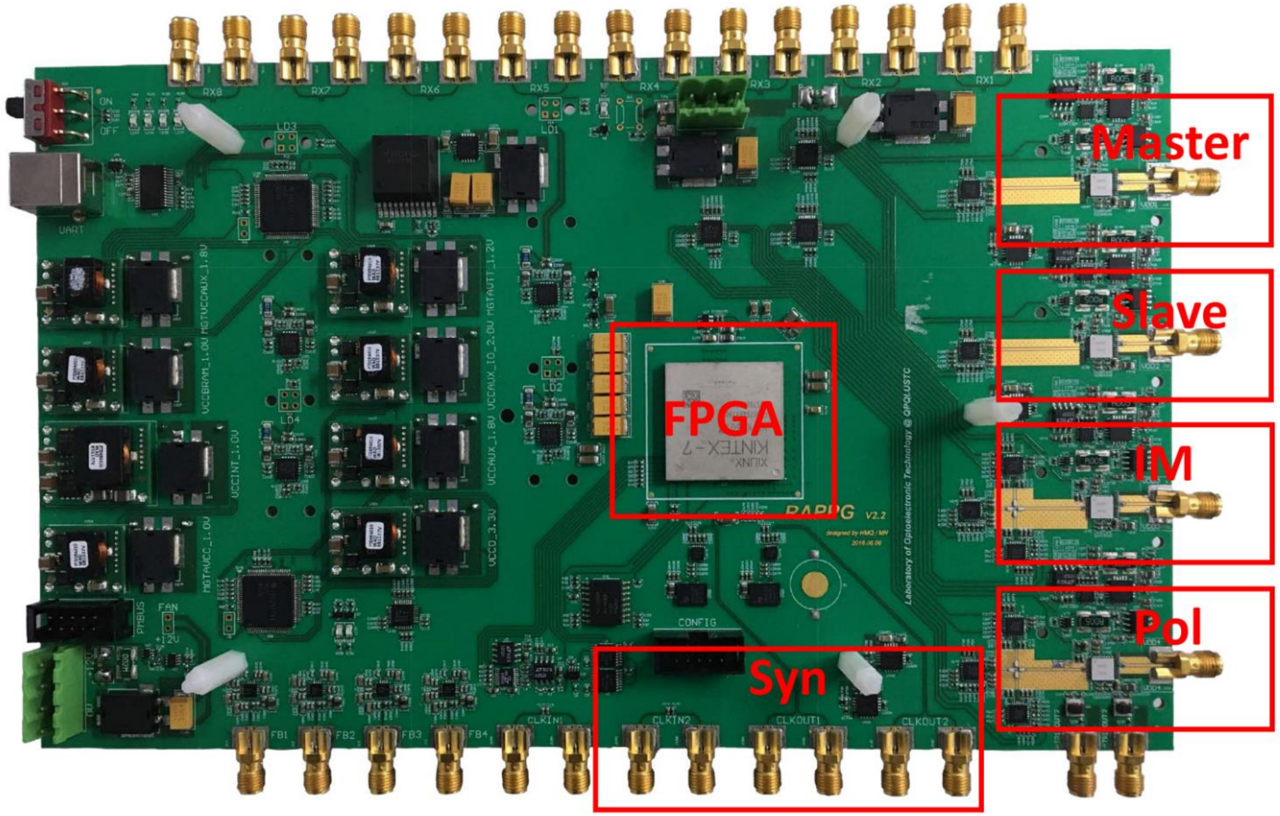


- 1.25 GHz chip-based MDI-QKD with random modulations
- Si chip integrates all the encoding components for transmitter

K. Wei*, W. Li* et al., arXiv: 1911.00690 (2019), accepted by PRX.

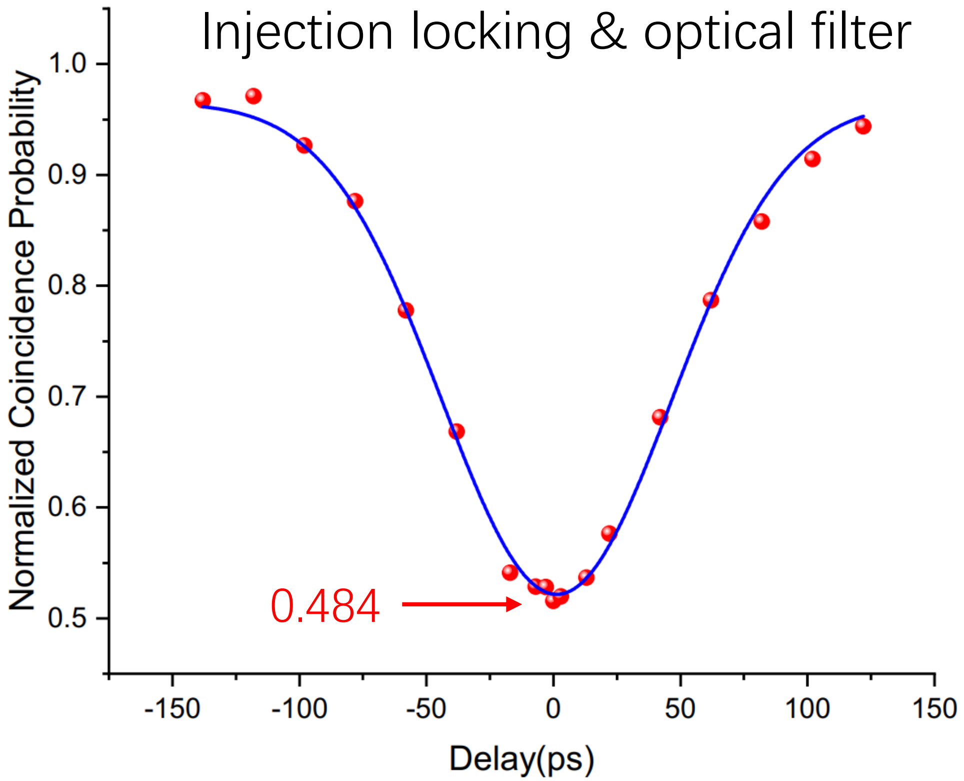
Experimental challenges

1.25 GHz modulation

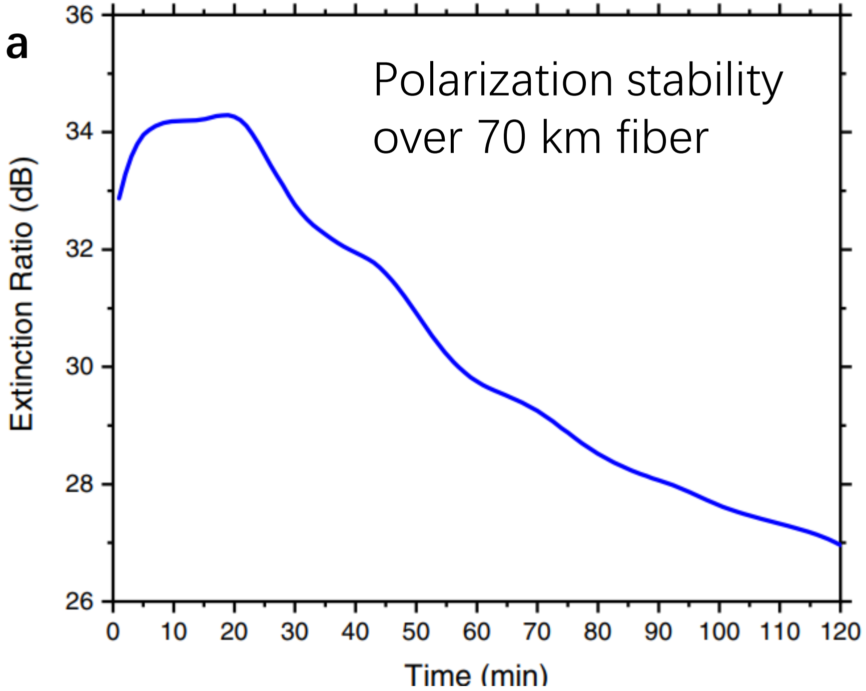


- Four independently adjustable levels
- 10 GSa/s, 7.5 Vpp
- DC coupled

High-visibility independent laser sources

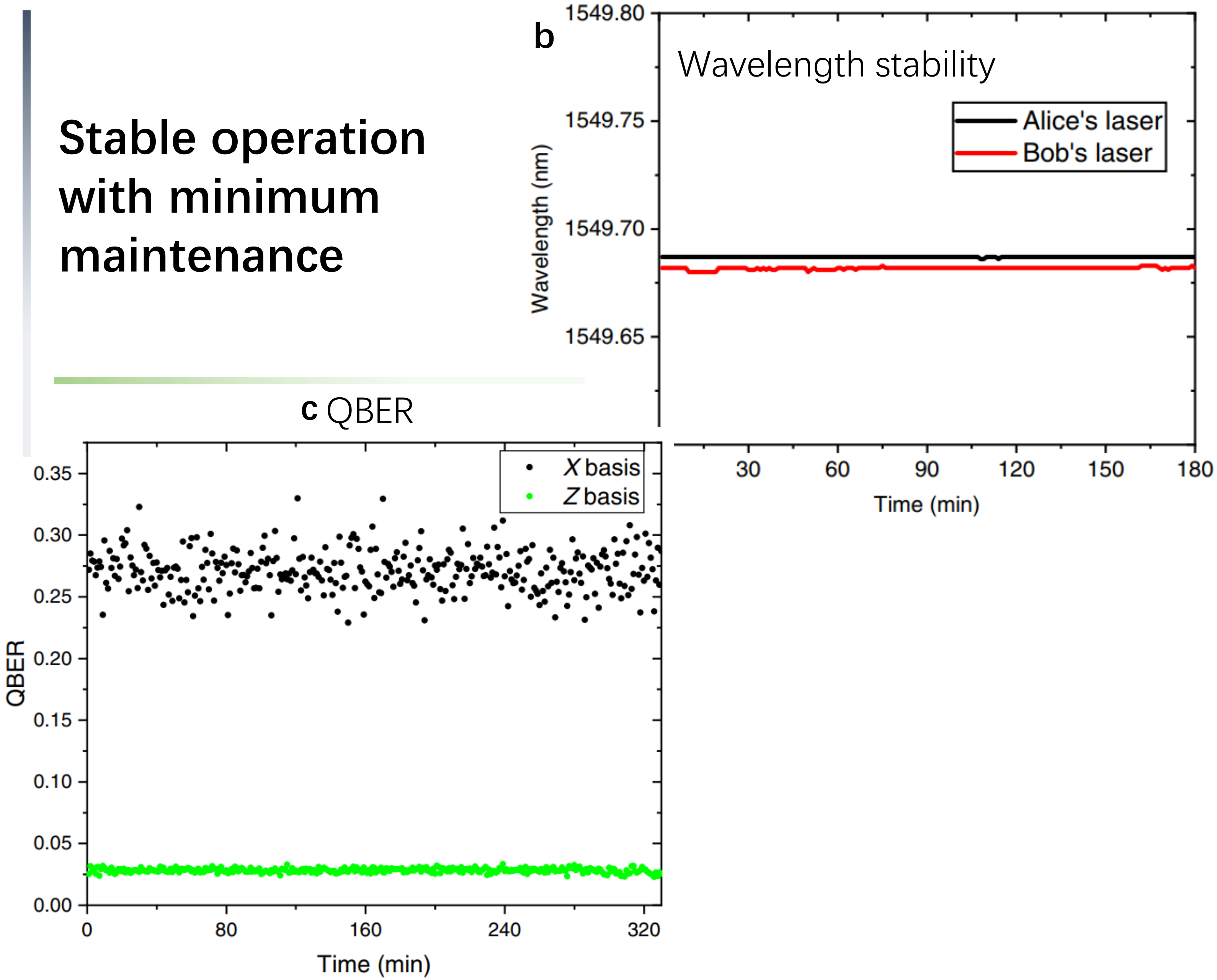


Stable operation

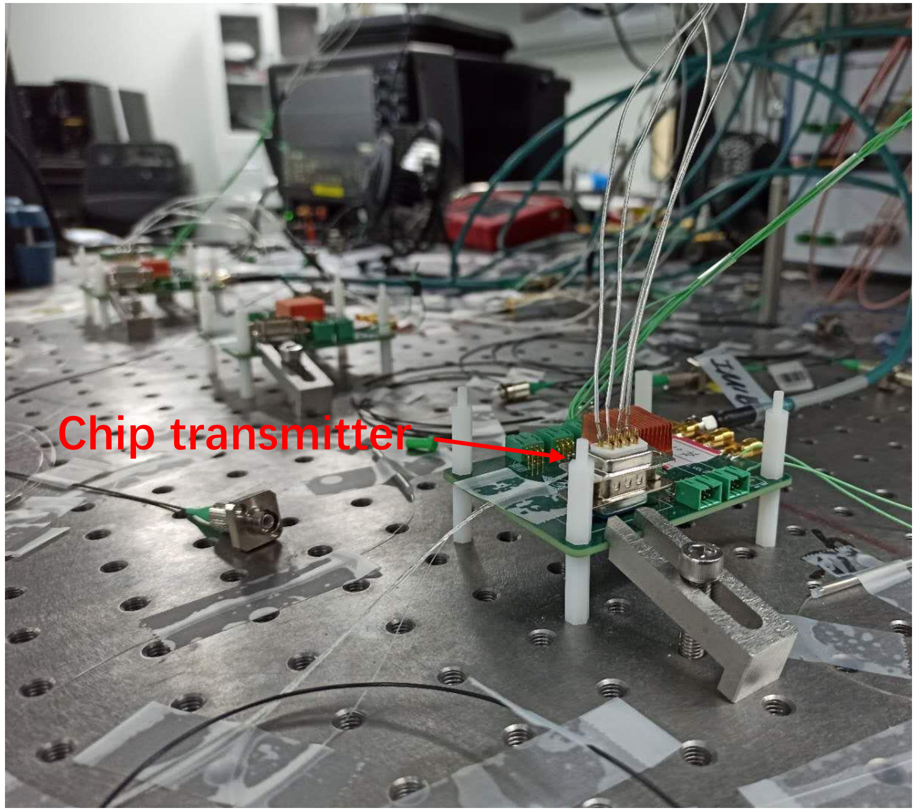


Mode	Maintenance
Polarization	Yes
Time	Yes
Wavelength	No
Intensity	No

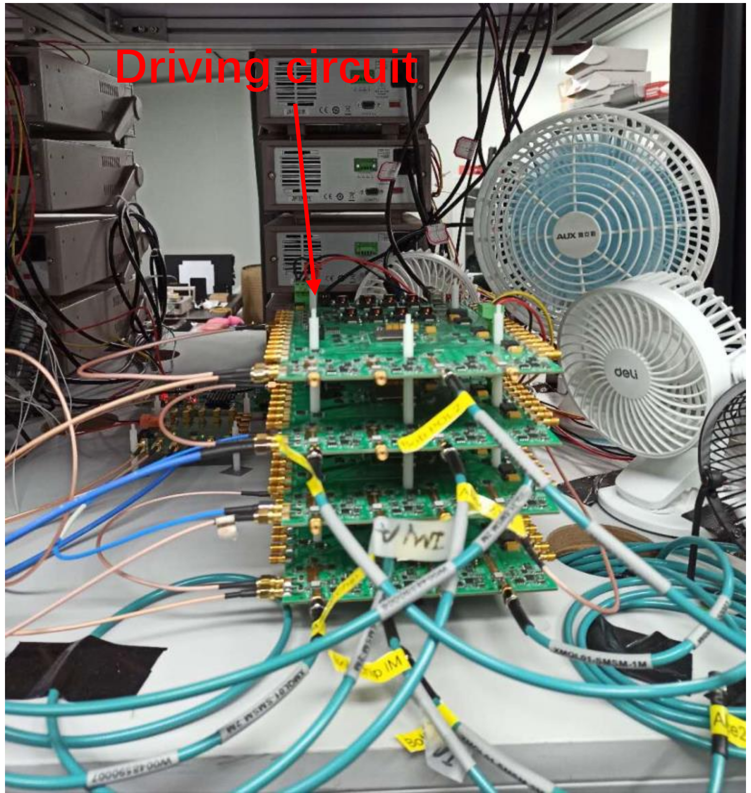
Stable operation with minimum maintenance

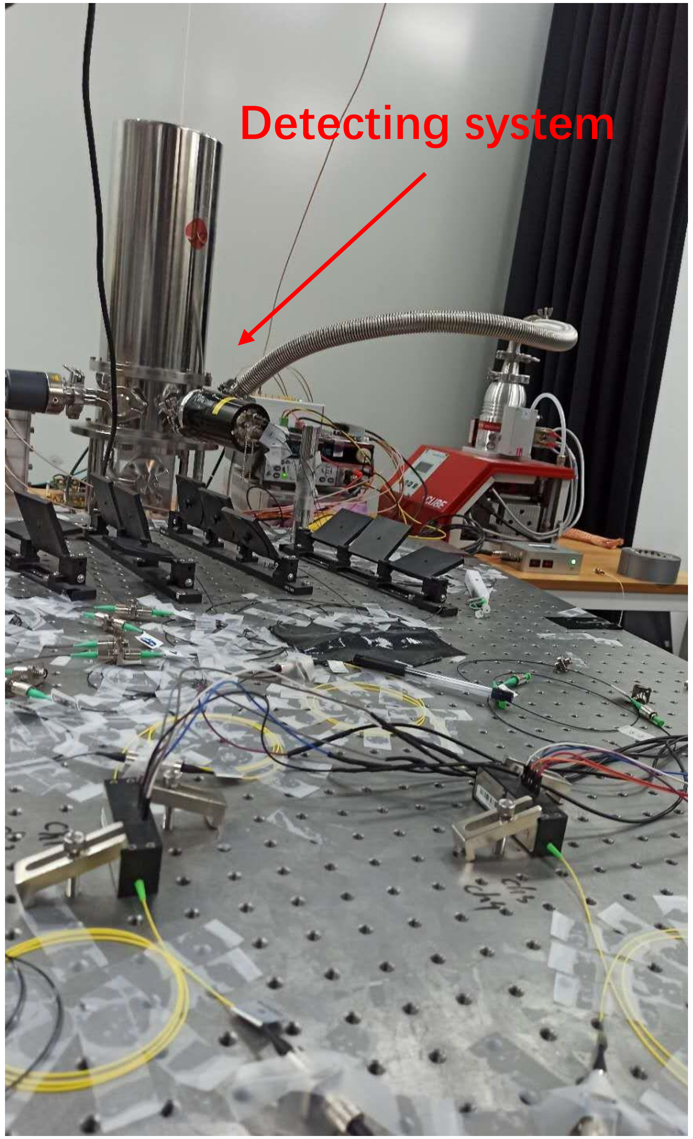


Lab view

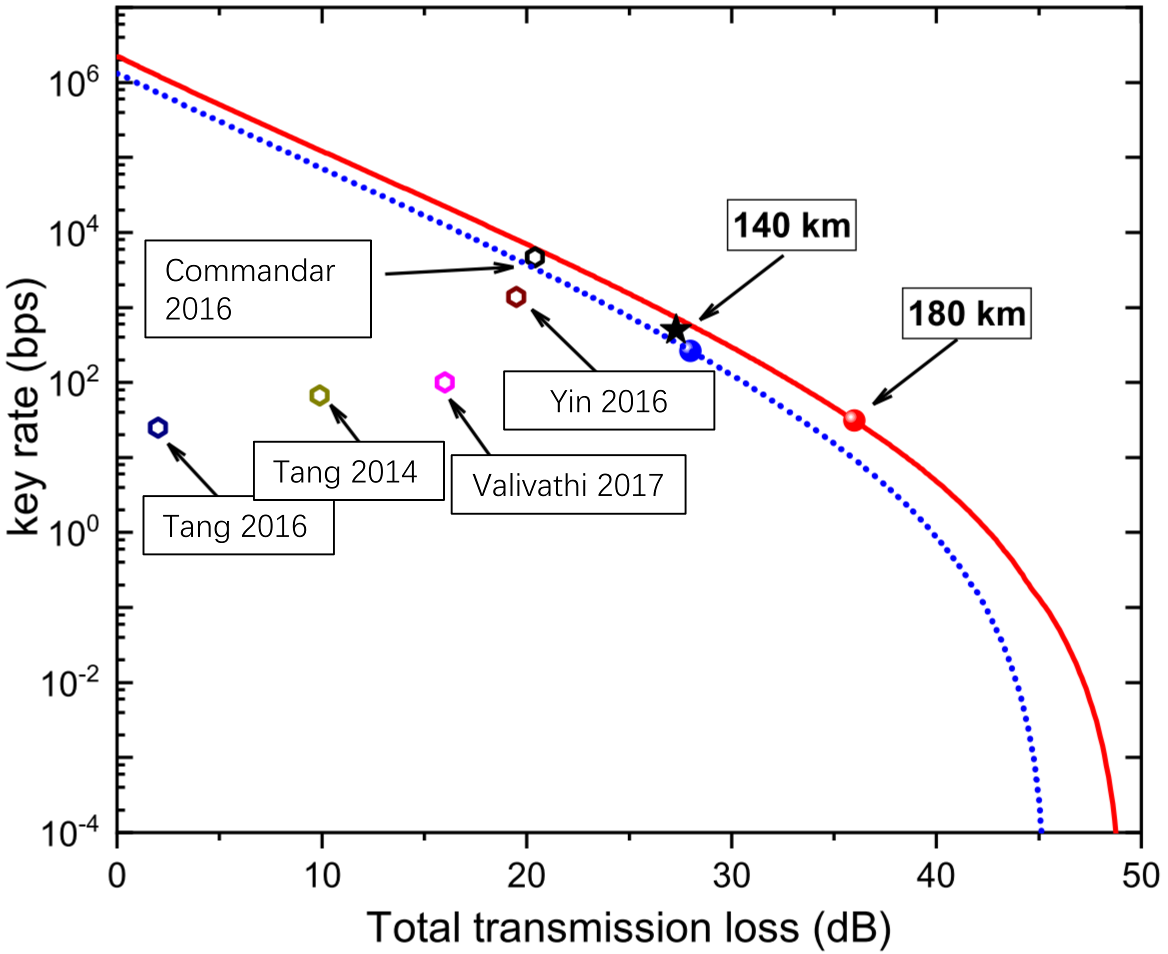


The transmitter is ready to be enclosed in a shoebox-size chassis





Result



Reference	Clock rate(MHz)	Channel loss(dB)	Secret key rate(bps)	finite-key
Tang et al., 2016	10	2.0	25	10^{-3}
Tang et al., 2014	75	9.9	67	10^{-9}
Valivathi et al., 2017	20	16.0	100	Asymptotic
Yin et al., 2016	75	19.5	1380	10^{-10}
Comandar et al., 2016	1000	20.4	4567	10^{-10}
Ours	1250	20.4	6172	10^{-10}
		28.0	268	10^{-10}

Fastest MDI-QKD system and highest reported key rates

Security loopholes

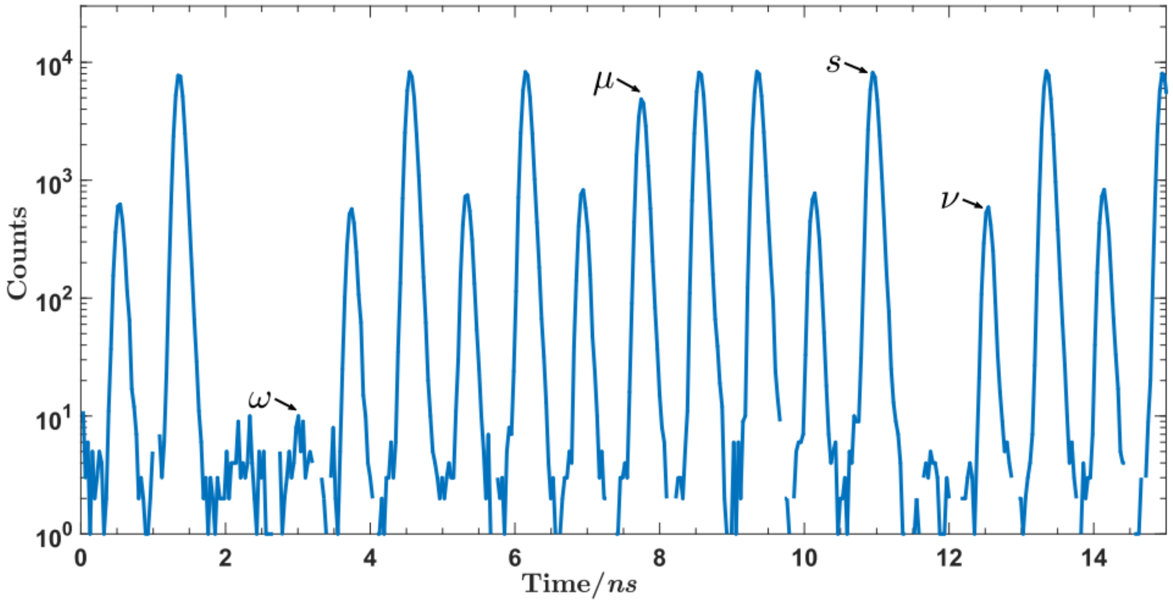
- Side channels in high-speed QKD

- Side channels in chip-based QKD

Patterning effect on modulation

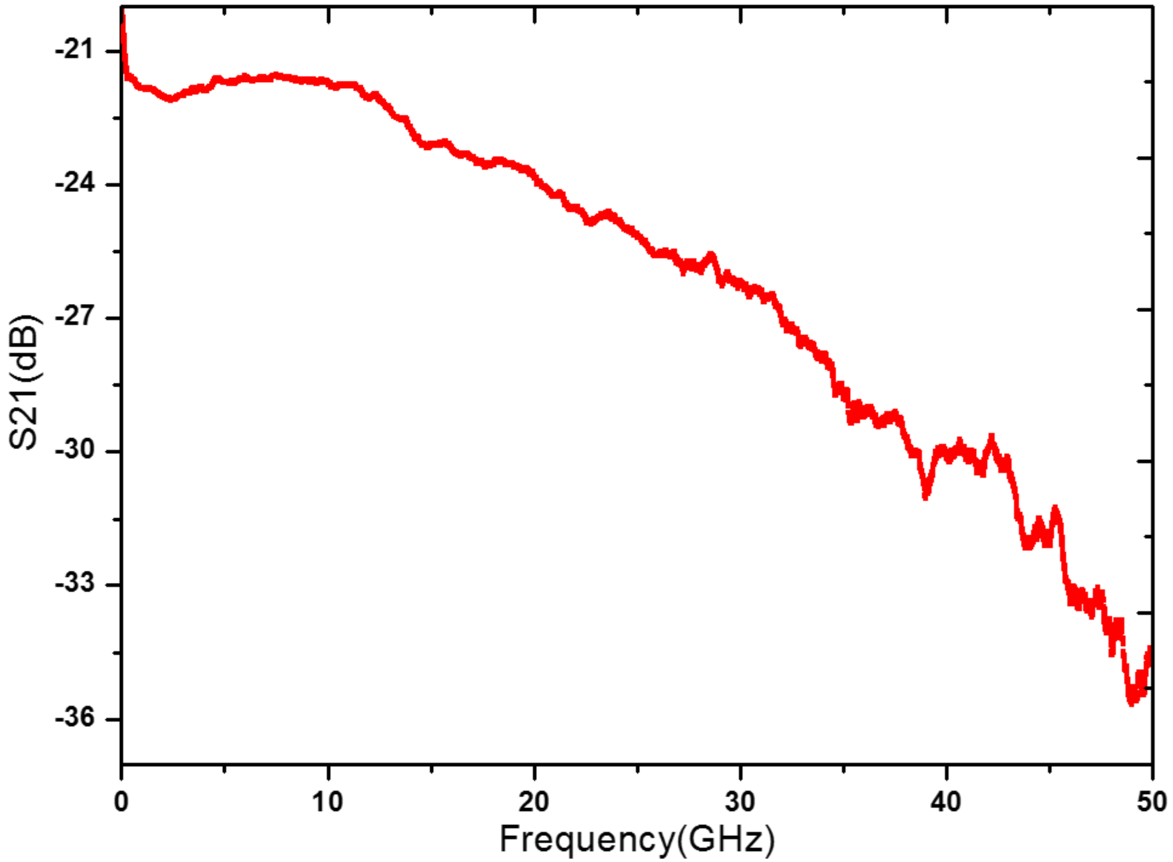
Pattern	average intensity of second pulse	deviation from s → x
s → s	1.000	-
μ → s	1.002	0.24%
υ → s	1.003	0.32%
0 → s	1.003	0.27%
s → μ	0.617	-
μ → μ	0.626	1.51%
υ → μ	0.610	-1.08%
0 → μ	0.632	2.44%
s → υ	0.029	-
μ → υ	0.027	-5.57%
υ → υ	0.025	-11.95%
0 → υ	0.027	-5.90%

Intensity deviation is less than 12%

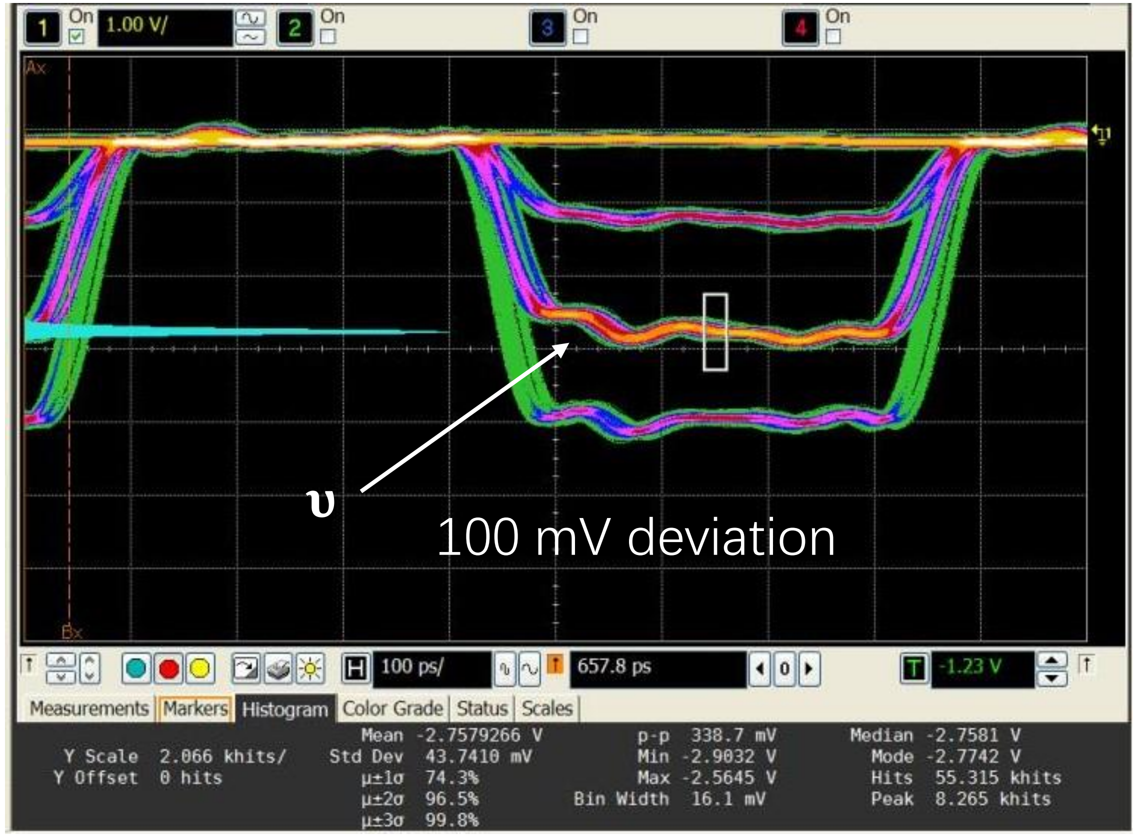


K.-i. Yoshino et al., npj Quantum Inf. 4, 8 (2018).

Patterning effect: modulator + driving signal



Carrier depletion modulator
18 GHz @3 dB



υ

100 mV deviation

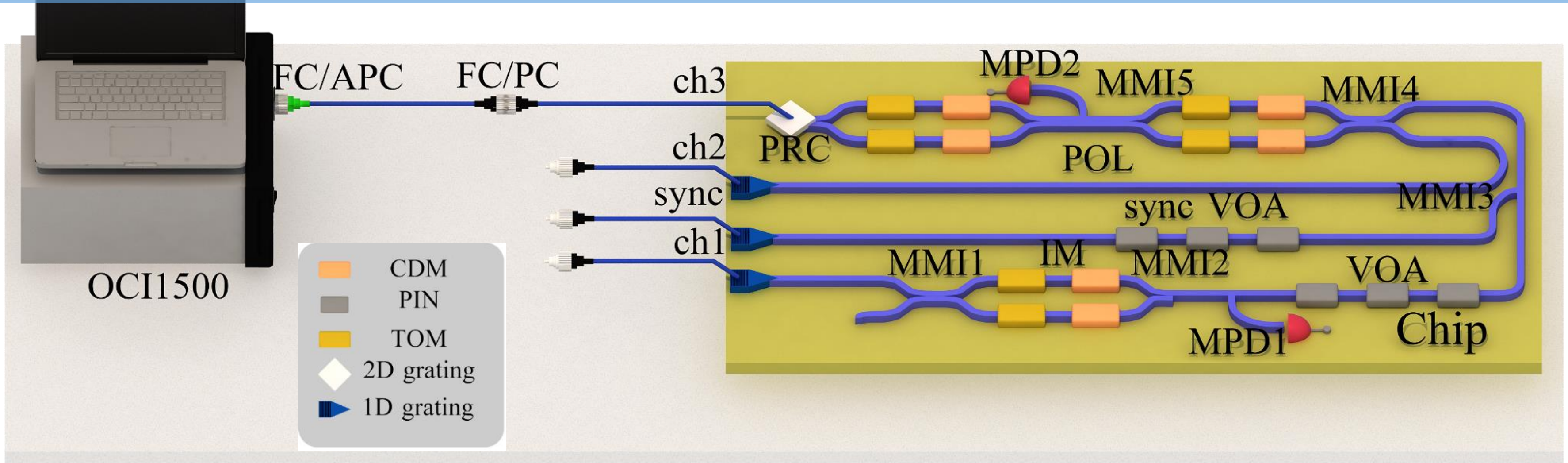
```
                     Mean -2.7579266 V       p-p  338.7 mV    Median -2.7581 V
 Y Scale  2.066 khits/  Std Dev  43.7410 mV        Min -2.9032 V    Mode -2.7742 V
Y Offset  0 hits         μ±1σ  74.3%              Max -2.5645 V    Hits  55.315 khits
                         μ±2σ  96.5%        Bin Width  16.1 mV     Peak  8.265 khits
                         μ±3σ  99.8%
```

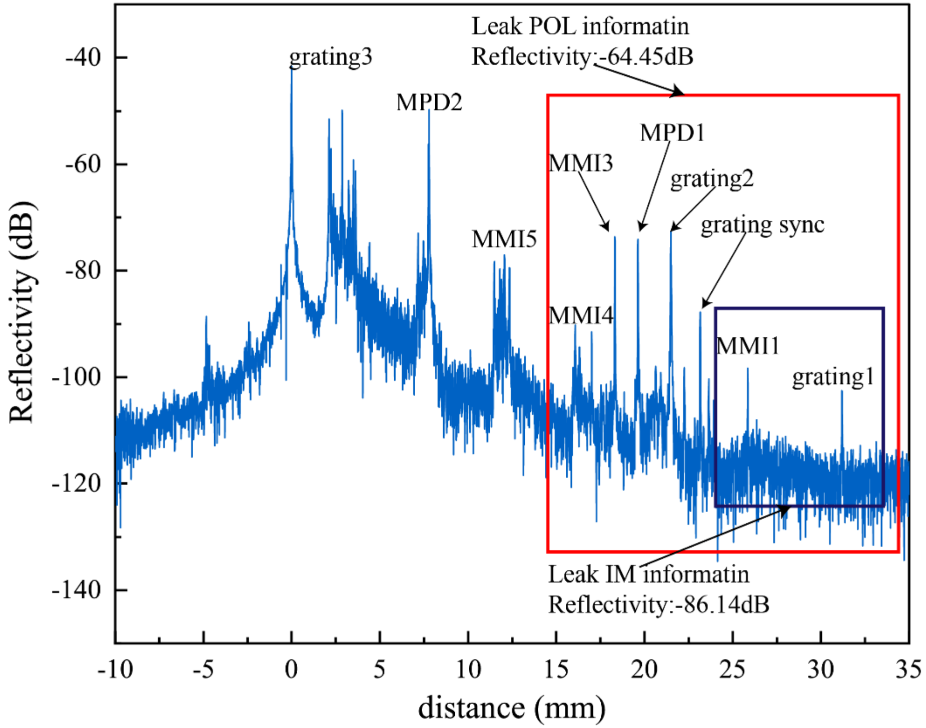
DC coupled is better than AC coupled

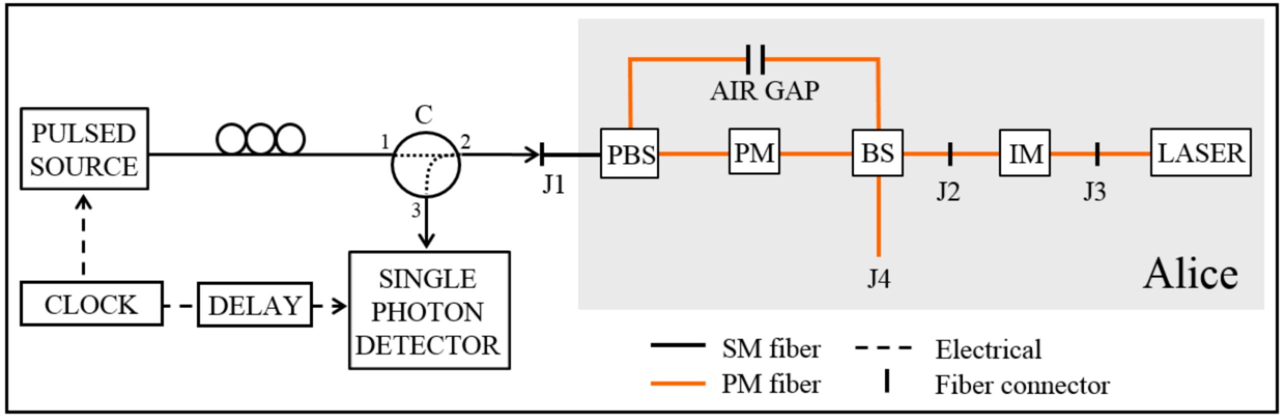
Security loopholes

- Side channels in high-speed QKD
- Side channels in chip-based QKD

Trojan Horse attack





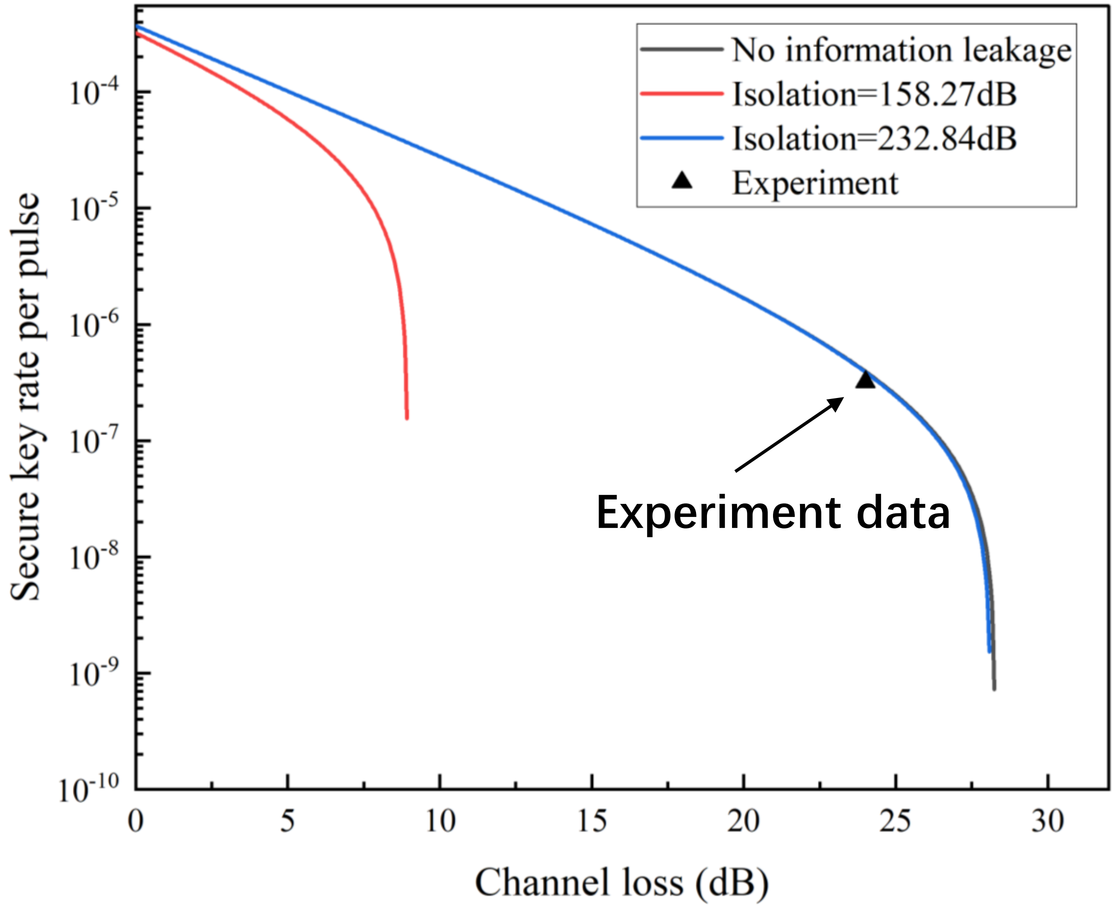


Time-bin encoding transmitter reflectivity: -42.87dB

Lucamarini et al., Phys. Rev. X 5, 031030 (2015).

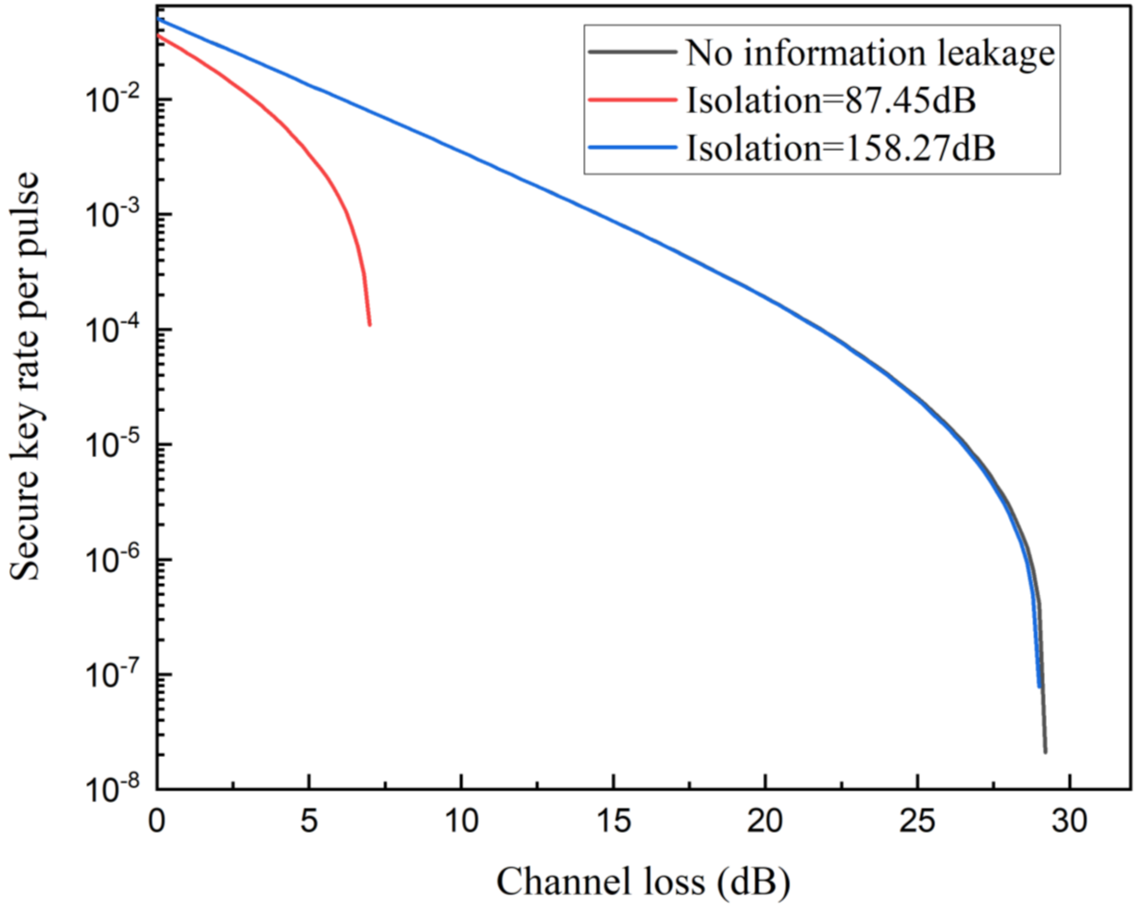
Reflectivity of our chip is smaller

QKD against Trojan Horse attack



Experiment data

Chip-based MDI-QKD



Chip-based BB84 protocol

MDI-QKD is more vulnerable to Trojan Horse attack

K. Tamaki et al., New Journal of Physics 18, 065008 (2016).

Other side channels

- Polarization dependent loss

  Less than 0.8 dB

- Intensity fluctuation

  Less than 0.04 dB

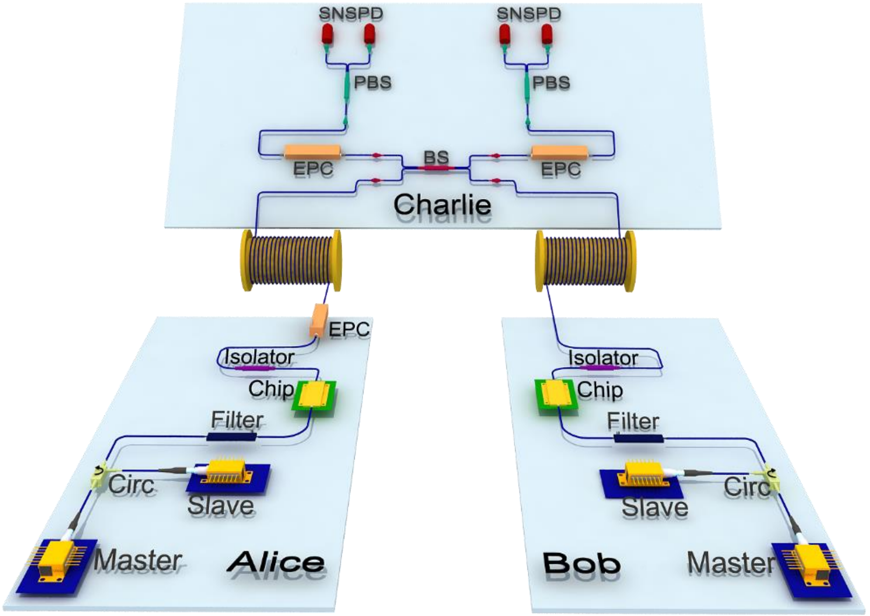
- Phase randomization

  T. Kobayashi et al., Phys. Rev. A 90, 032320 (2014).

Solution?

K. Tamaki et al., Phys. Rev. A 90, 052314 (2014).
M. Pereira et al., npj Quantum Inf. 5, 62 (2019).

Summary



- Silicon photonic chip-based MDI-QKD
- 1.25 GHz random modulation
- Highest secret key rate
- Side channels are characterized

K. Wei*, W. Li* et al., arXiv: 1911.00690 (2019), accepted by PRX.

- Patterning effect
- Trojan Horse attack
- Polarization dependent loss
- Intensity fluctuation
- Phase randomization

Acknowledgement

Prof. Feihu Xu

Prof. Jian-Wei Pan

回想自己一生，经历过许多
坎坷，唯一希望的就是祖国繁荣
昌盛，科学发达，我们已经尽了
自己的力量，但国家尚未摆脱贫
穷与落后，尚需当今与后世无私

Funding

中国科学院
CHINESE ACADEMY OF SCIENCES

国家自然科学基金委员会
NSFC

中华人民共和国科学技术部
Ministry of Science and Technology of the People's Republic of China

Thank you for your attention!

Email: weil@ustc.edu.cn