Implementation security of quantum key distribution

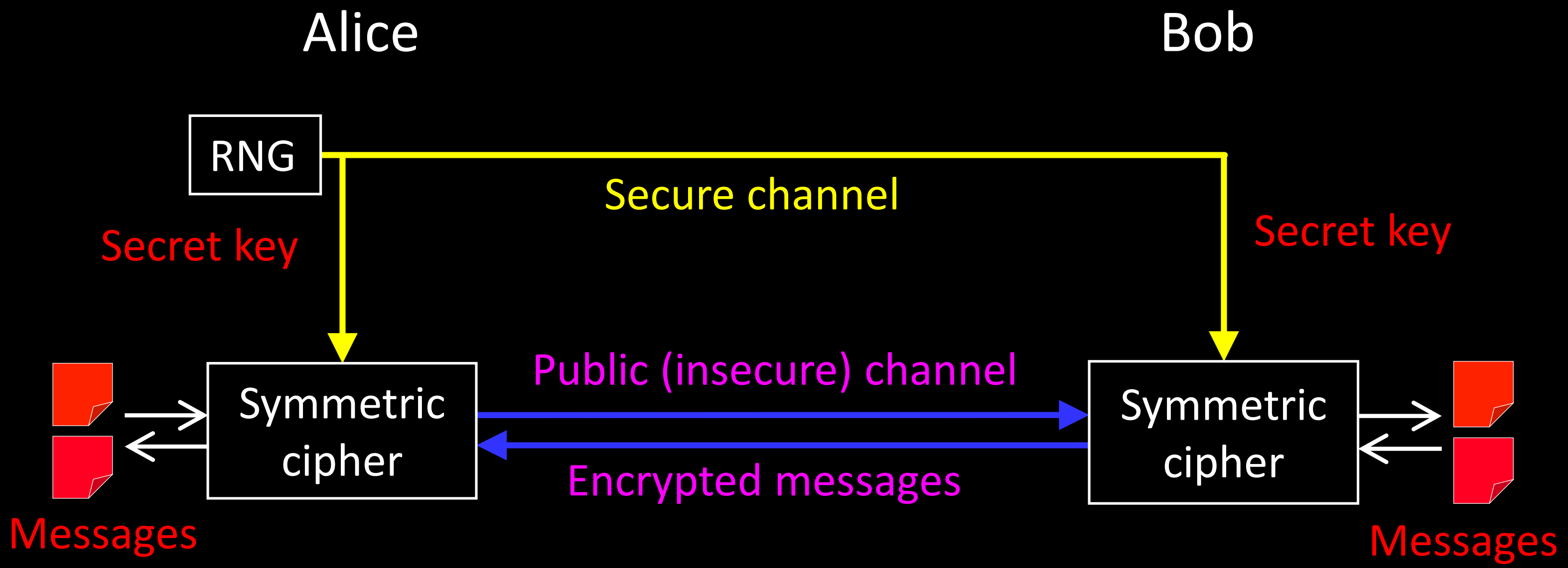
Anqi Huang

2022-11-08 ITU Workshop

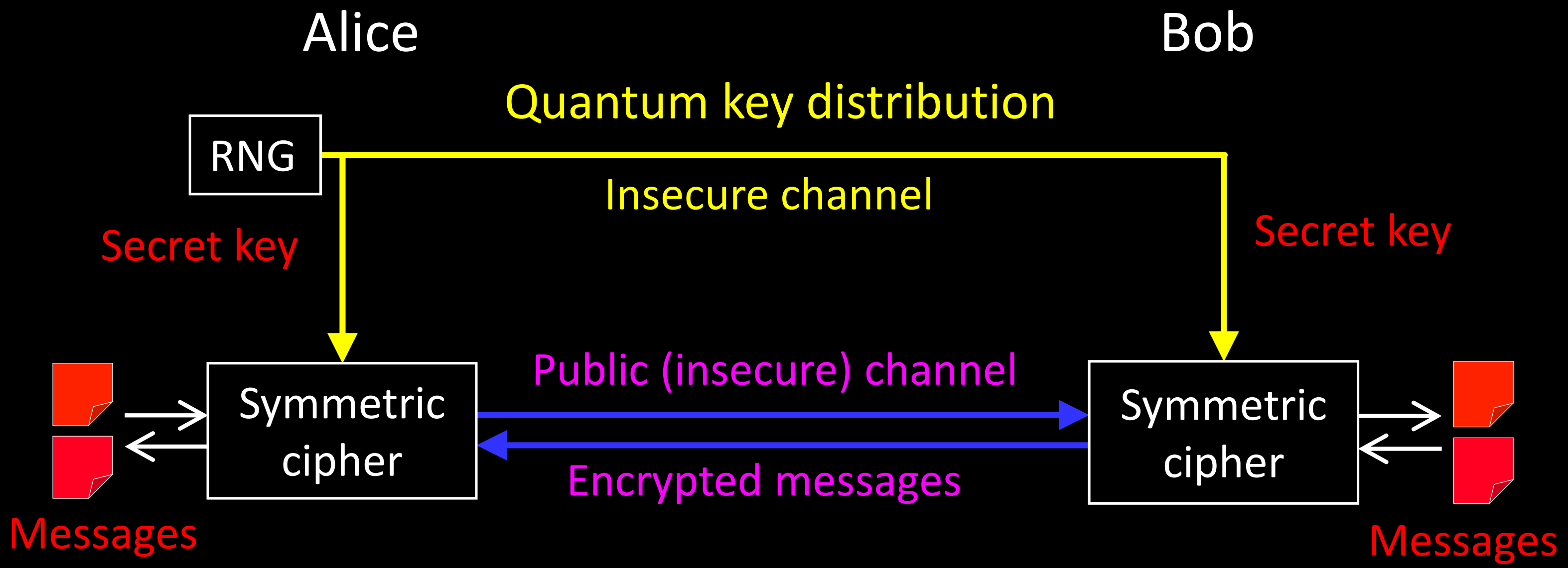
HPCL
State Key Laboratory of High Performance Computing

Secure connection among communication network

Key distribution for encryption

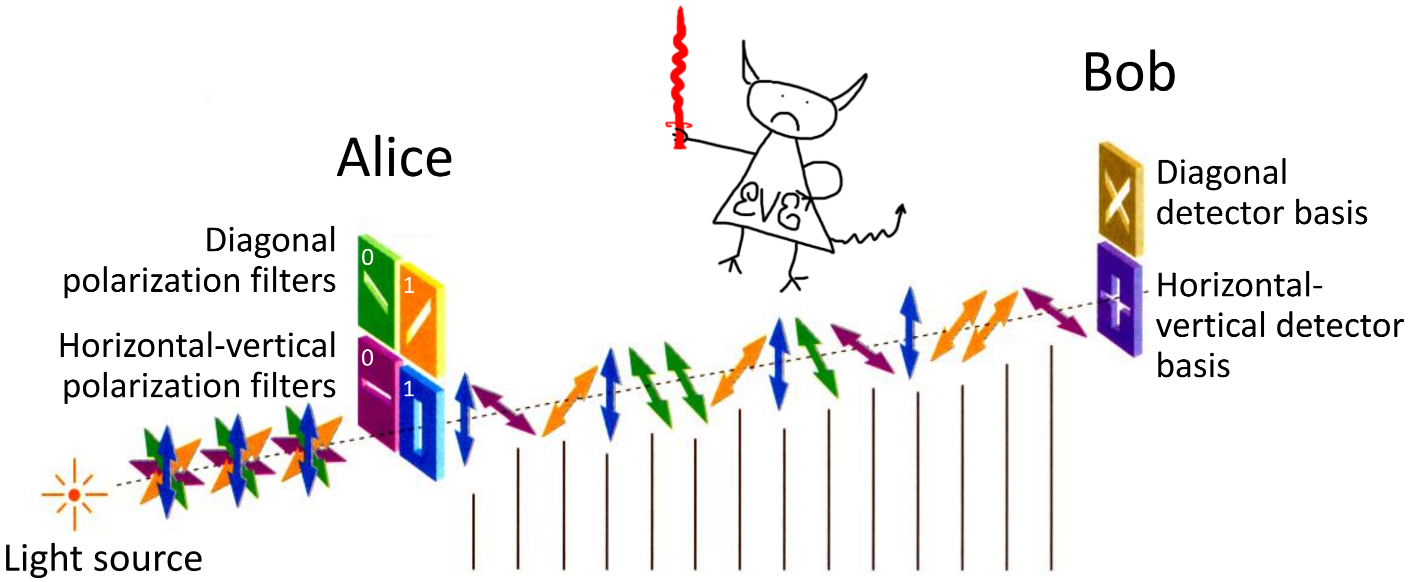


Quantum key distribution



Quantum key distribution transmits secret key by sending quantum states over *open channel.*

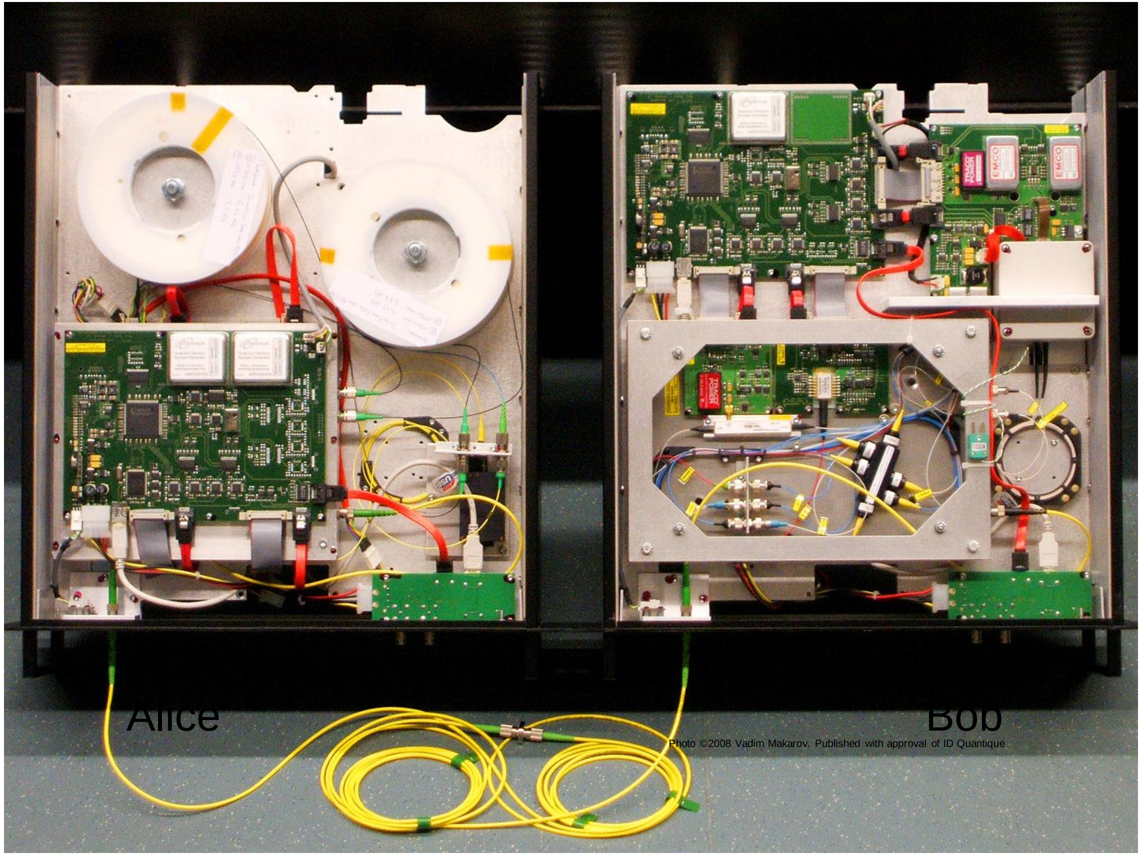
Bennett-Brassard 1984 (BB84) QKD protocol



Alice's bit sequence	1	0	1	1	0	0	1	1	0	0	1	1	1	0
Bob's detection basis	+	×	+	+	×	×	+	+	×	+	×	×	+	+
Bob's measurement	1	0	0	1	0	0	1	1	0	0	0	1	0	0
Retained bit sequence	1	–	–	1	0	0	–	1	0	0	–	1	–	0

Image reprinted from article: W. Tittel, G. Ribordy & N. Gisin, "Quantum cryptography," Physics World, March 1998

Point-to-point commercial QKD system from ID Quantique

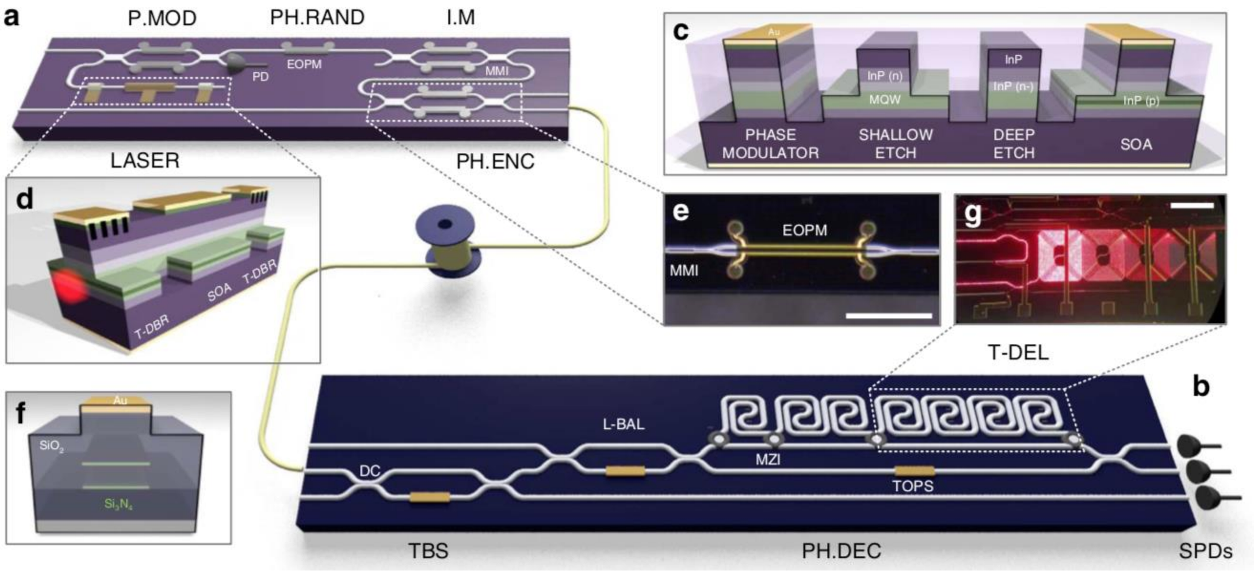


Hybrid QKD network

Satellite-to-ground QKD at 1 kbit/s

S.-K. Liao et al., Nature 549, 43 (2017)

QKD chips



P. Sibson *et al.,* Nat. Communications **8,** 13984 (2017)

Challenges for Large-scale Secure Quantum Communication

Security ?

Long distance ?

Applications ?

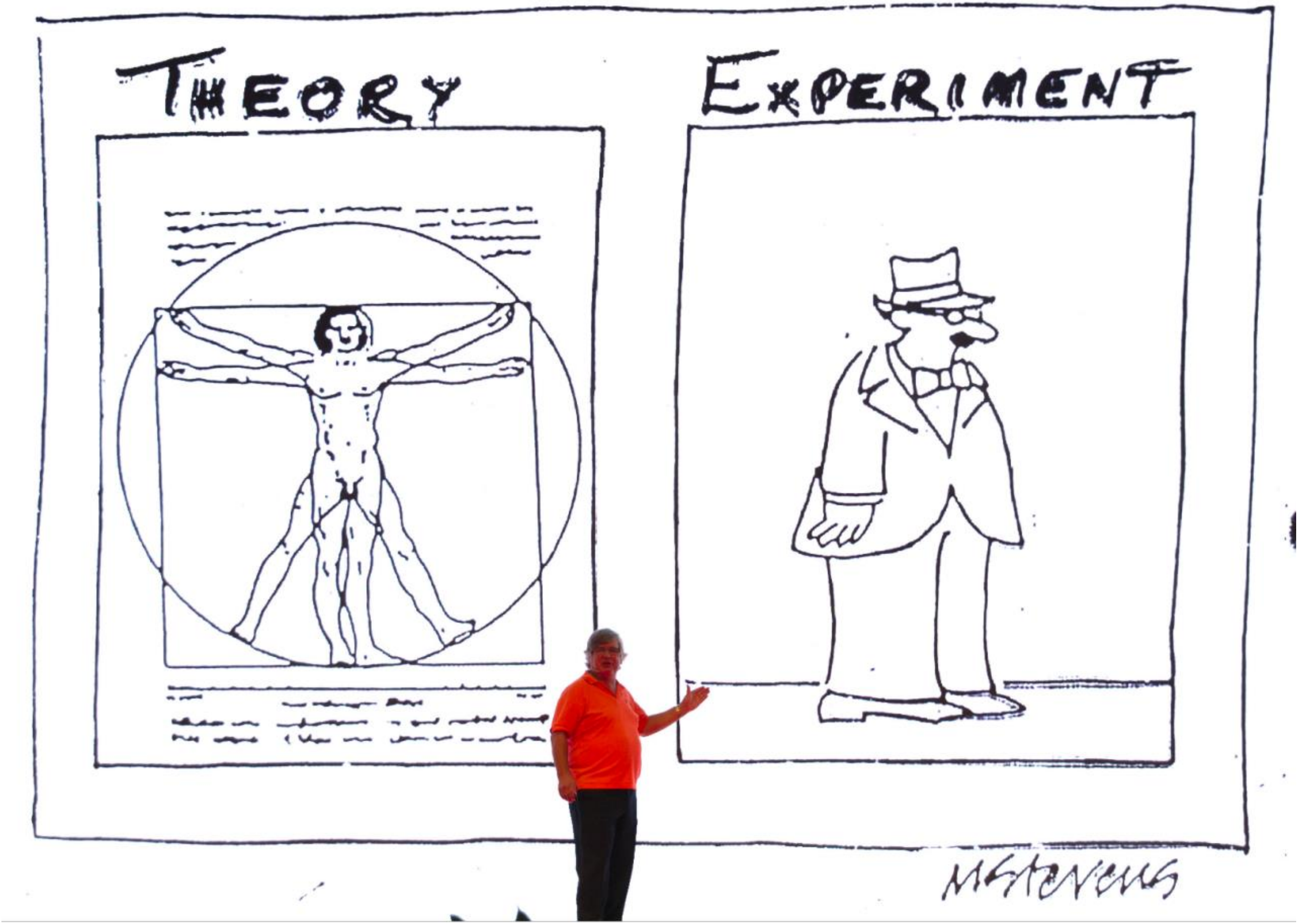
Challenges for Large-scale Secure Quantum Communication

Security ?

Long distance ?

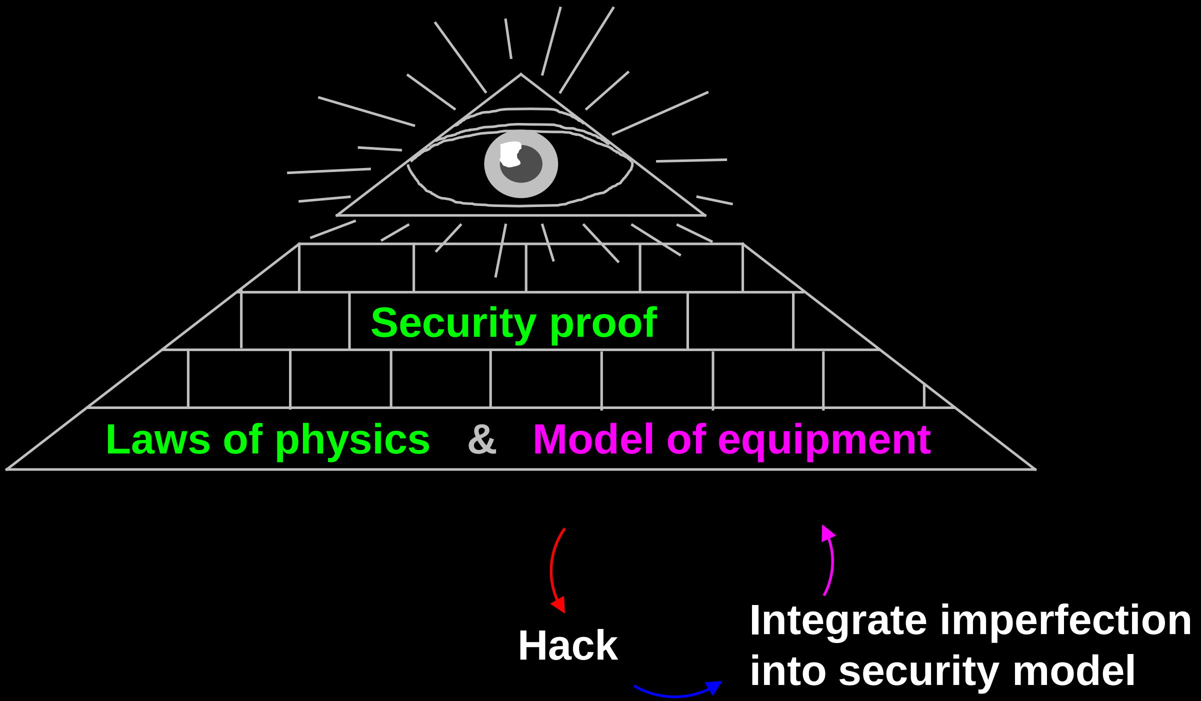
Applications ?

Gap between theory and experiment

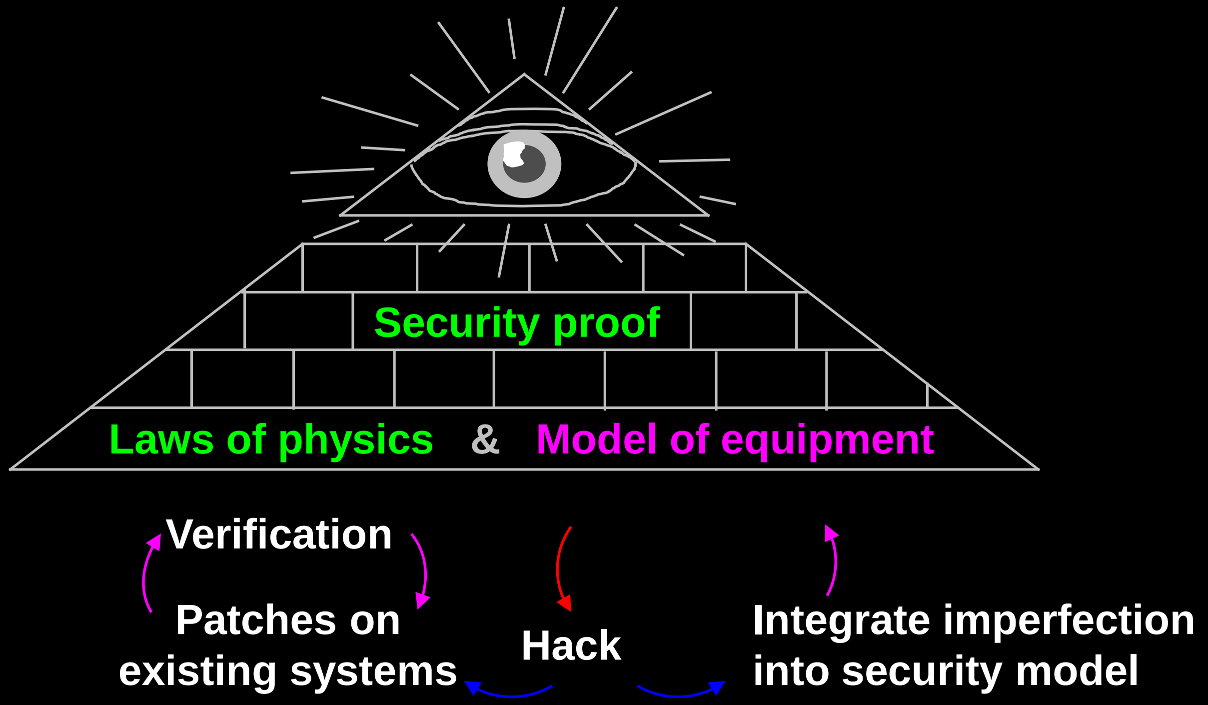


Attack	Target component	Tested system
Distinguishability of decoy states A. Huang *et al.,* Phys. Rev. A **98**, 012330 (2018)	laser in Alice	3 research systems
Intersymbol interference K. Yoshino *et al.,* poster at QCrypt (2016)	intensity modulator in Alice	research system
Laser damage V. Makarov *et al.,* Phys. Rev. A **94**, 030302 (2016); A. Huang *et al.,* Phys. Rev. Appl. **13**, 034017 (2020)	any	5 commercial & 1 research systems
Spatial efficiency mismatch M. Rau *et al.,* IEEE J. Sel. Top. Quantum Electron. **21**, 6600905 (2015); S. Sajeed *et al.,* Phys. Rev. A **91**, 062301 (2015)	receiver optics	2 research systems
Laser-seeding S. Sun *et al*., Phys. Rev. A **92**, 022304 (2015), A. Huang *et al.,* Phys. Rev. Appl. **12**, 064043 (2019)	laser in Alice	3 research systems
Trojan-horse I. Khan *et al.,* presentation at QCrypt (2014)	phase modulator in Alice	SeQureNet
Trojan-horse N. Jain *et al.,* New J. Phys. **16**, 123030 (2014); S. Sajeed *et al.,* Sci. Rep. **7**, 8403 (2017)	phase modulator in Bob	ID Quantique
Detector saturation H. Qin, R. Kumar, R. Alleaume, Proc. SPIE 88990N (2013)	homodyne detector	SeQureNet
Shot-noise calibration P. Jouguet, S. Kunz-Jacques, E. Diamanti, Phys. Rev. A **87**, 062313 (2013)	classical sync detector	SeQureNet
Pulse illumination Z. Wu, A. Huang *et al.,* Opt. Express **28**, 17 (2020)	single-photon detector	research system
Multi-wavelength H.-W. Li *et al.,* Phys. Rev. A **84**, 062308 (2011)	beamsplitter	research system
Deadtime H. Weier *et al.,* New J. Phys. **13**, 073024 (2011)	single-photon detector	research system
Channel calibration N. Jain *et al.,* Phys. Rev. Lett. **107**, 110501 (2011)	single-photon detector	ID Quantique
Faraday-mirror S.-H. Sun, M.-S. Jiang, L.-M. Liang, Phys. Rev. A **83**, 062331 (2011)	Faraday mirror	(theory)
Detector control L. Lydersen *et al.,* Nat. Photonics **4**, 686 (2010); A. Huang *et al.*, IEEE J. Quantum Electron **52**, 11 (2016)	single-photon detector	ID Quantique, MagiQ, research systems

Implementation security of quantum communications

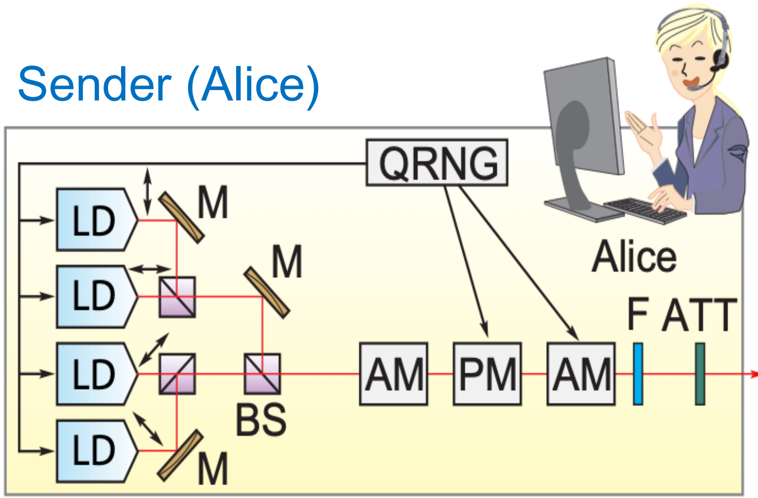


Implementation security of quantum communications

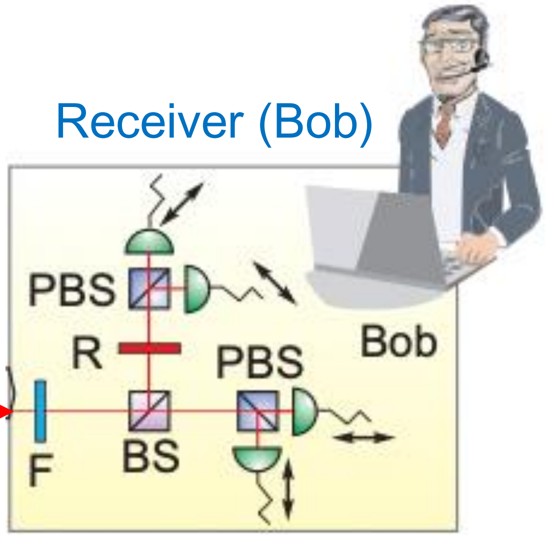


Active attacks on QKD

Sender (Alice)

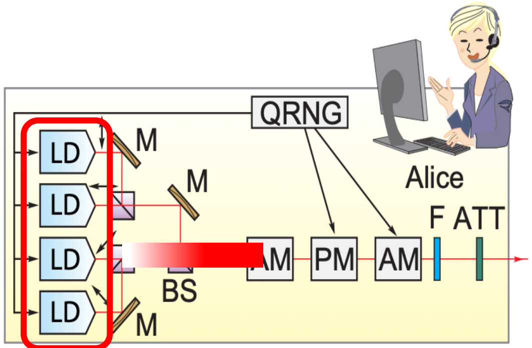


Receiver (Bob)

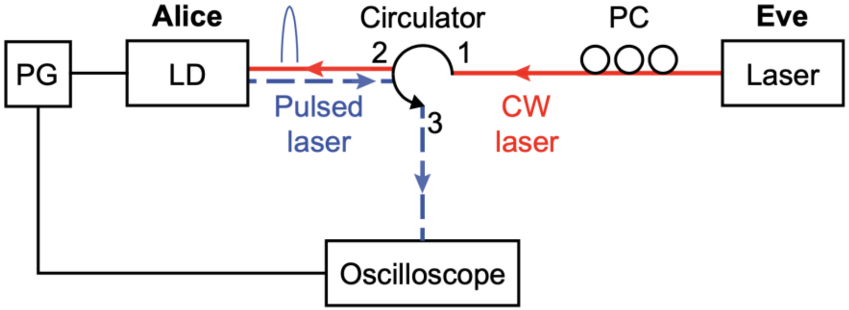


Eavesdropper (Eve)

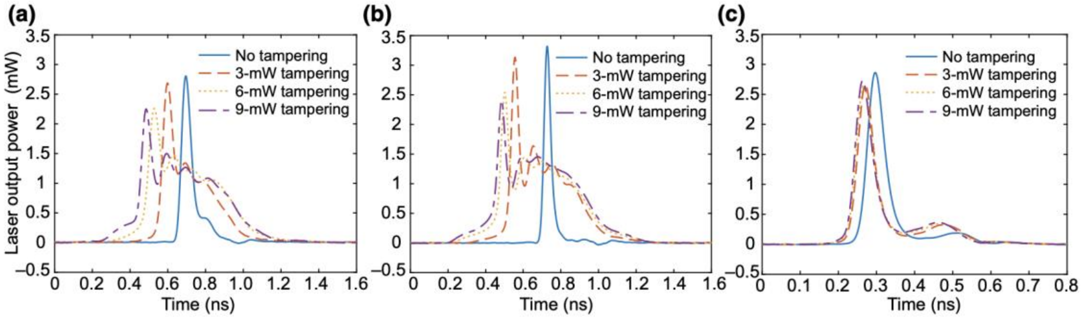
Active attacks on the source：Laser seeding attack



Laser seeding attack

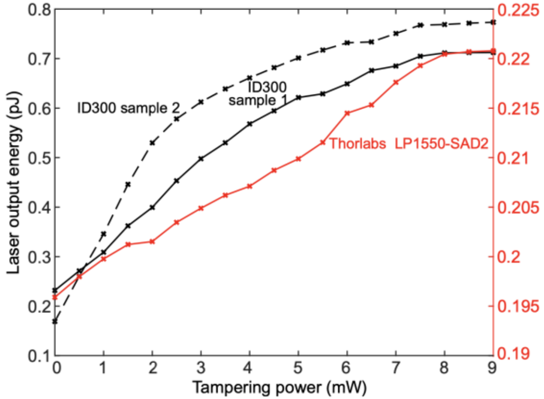


Photon number increases 1.13～4.57 times



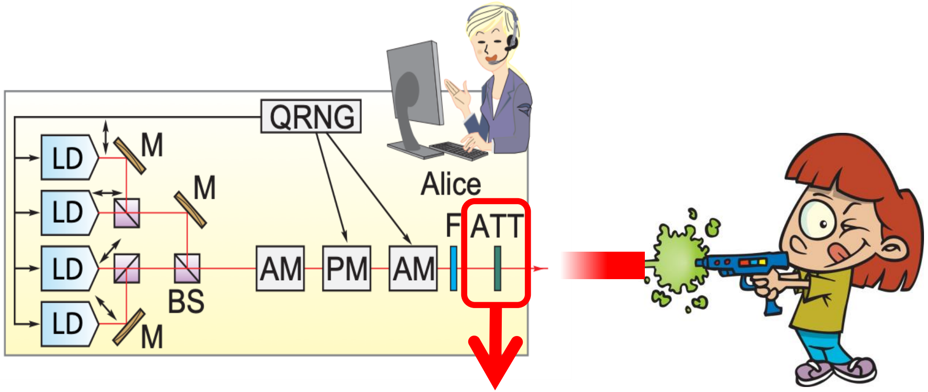
ID Quantique ID300

Thorlabs LP1550

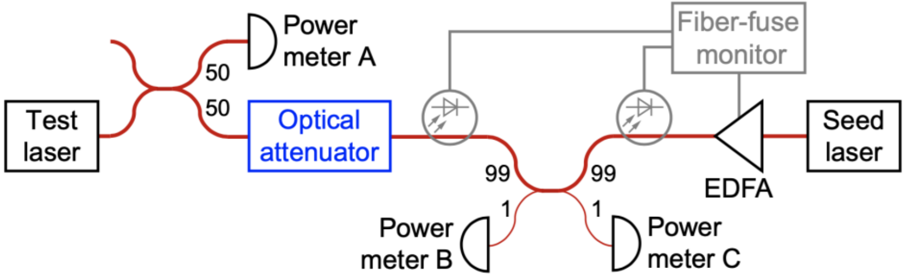


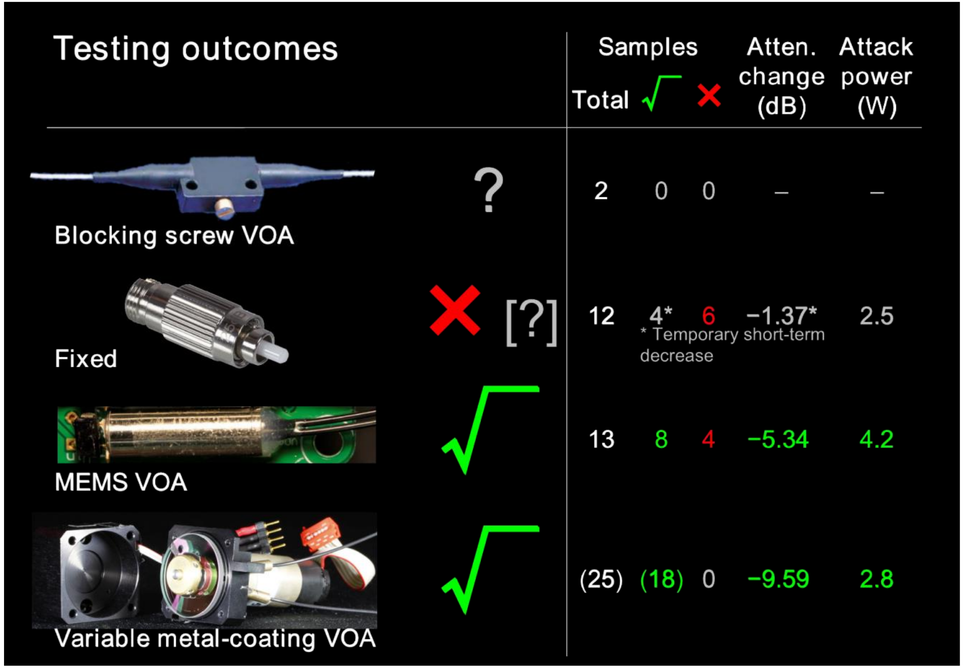
Anqi Huang, et. al., Phy. Rev. Appl. (2019)

Active attacks on the source：Laser damage attack



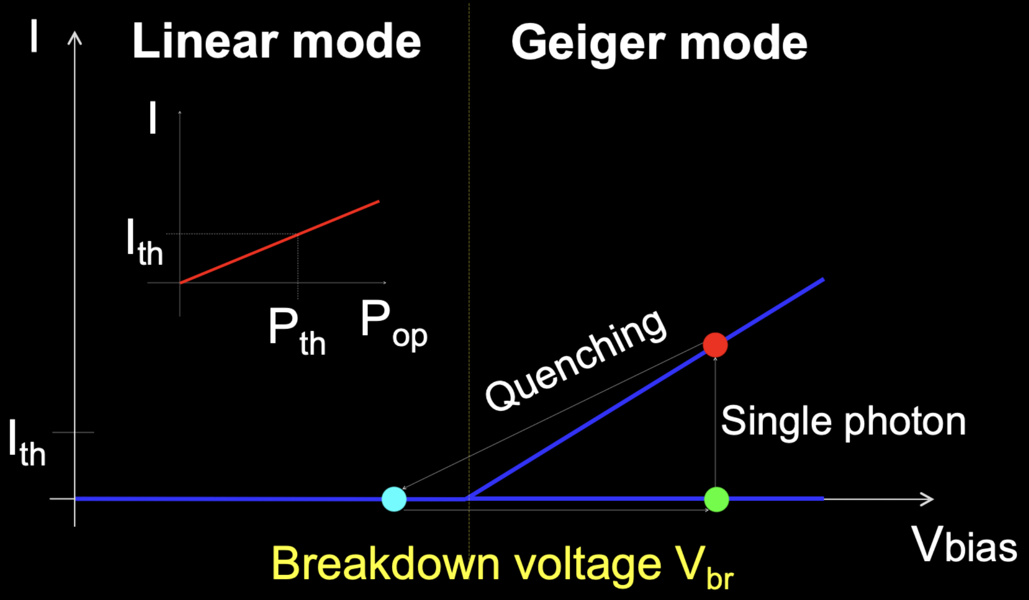
Laser damage attack



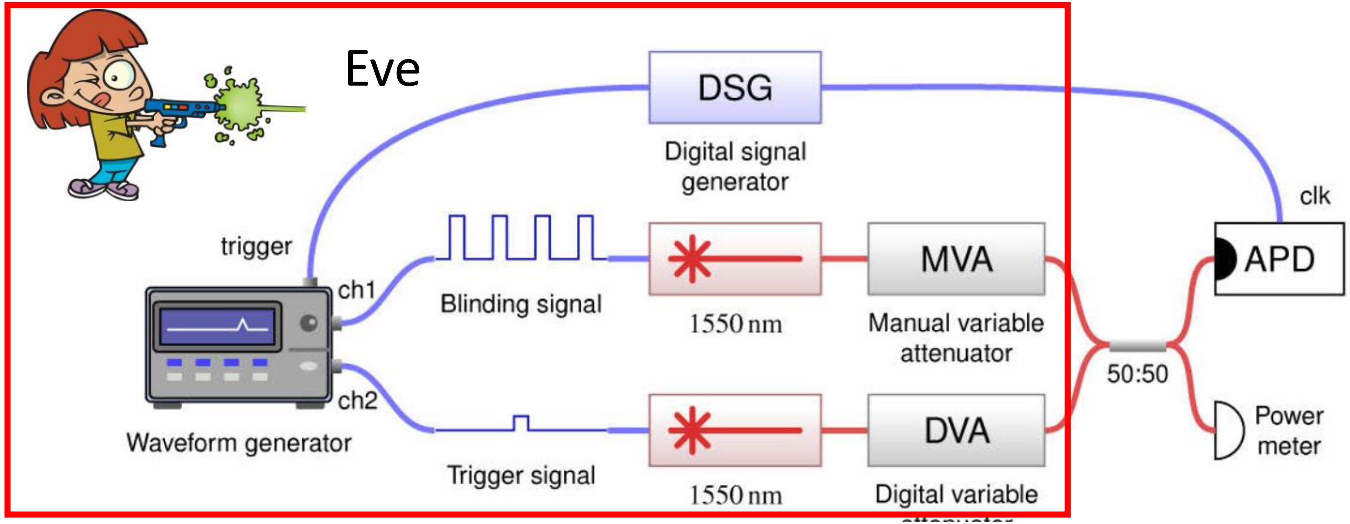


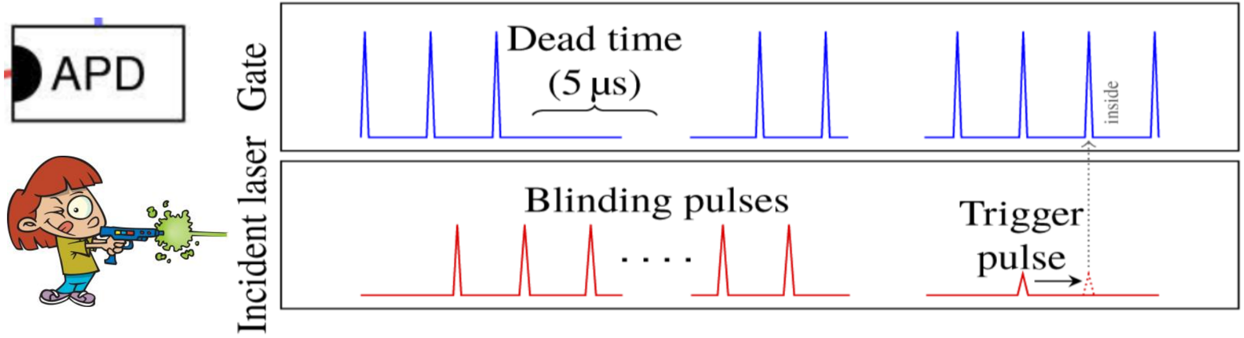
A. Huang, R. Li, S. Tchouragoulov, V. Egorov, V. Makarov, Phy. Rev. App. (2020)

Blinding attack on avalanche photodetectors (APDs)



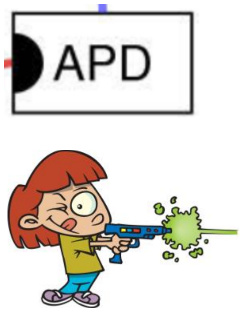
Active attack on the detection: pulse illumination attack on APD

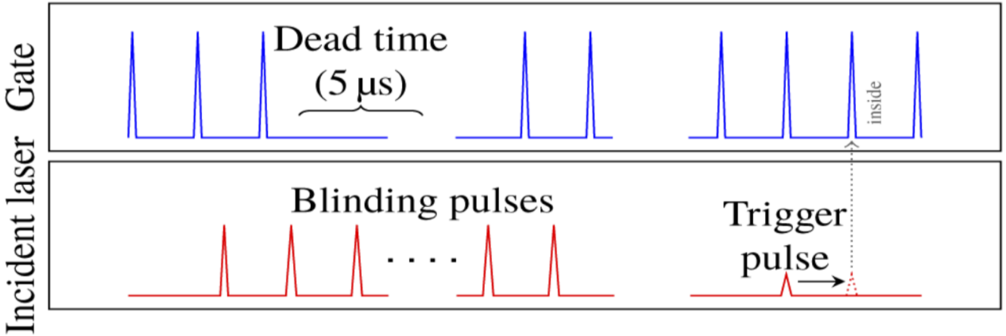


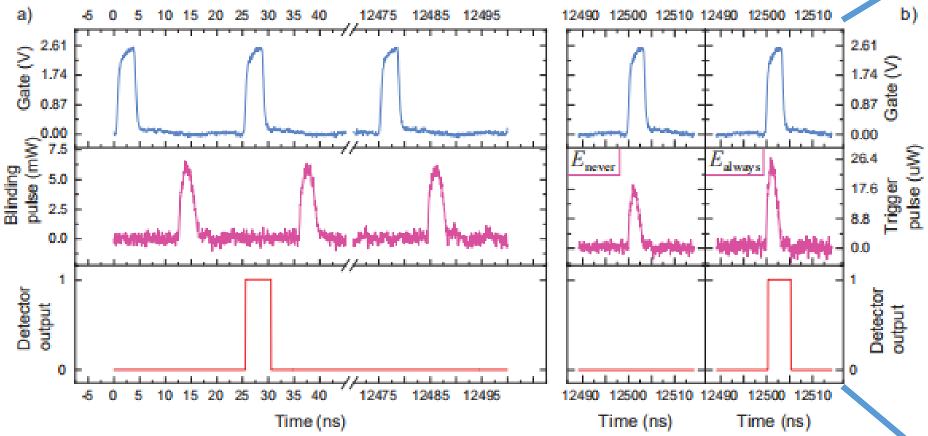


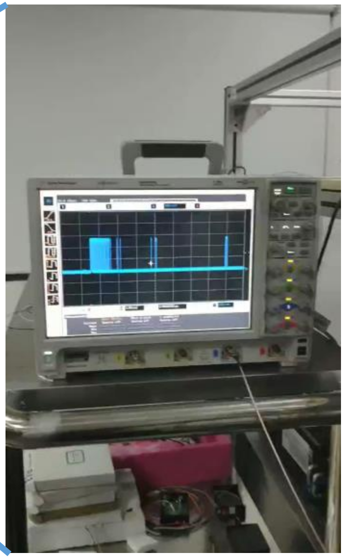
Zhihao Wu, Anqi Huang, and et. al., Opt. Exp. (2020)

Active attack on the detection: pulse illumination attack on APD



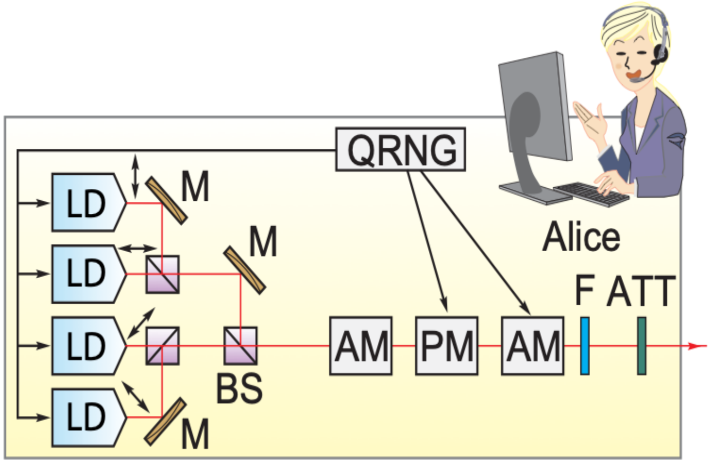




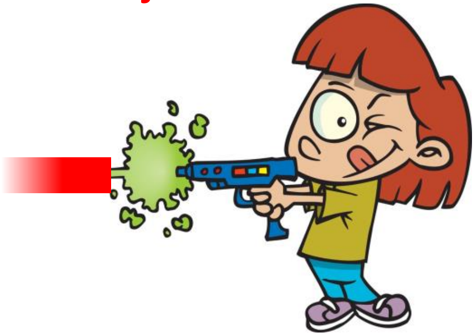


Zhihao Wu, Anqi Huang, and et. al., Opt. Exp. (2020)

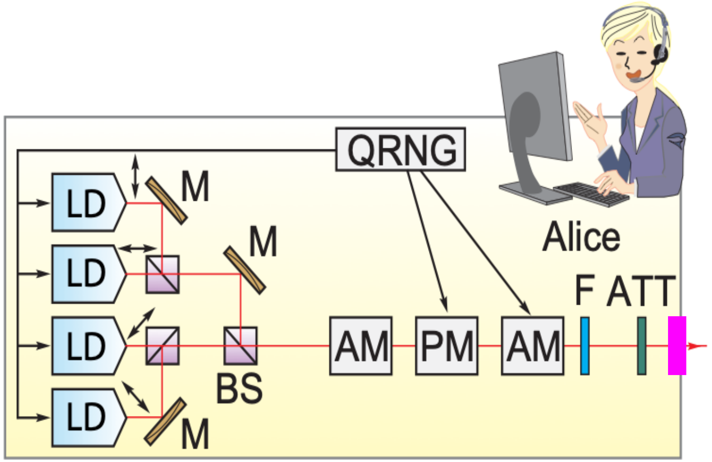
Countermeasure against active attacks on the source



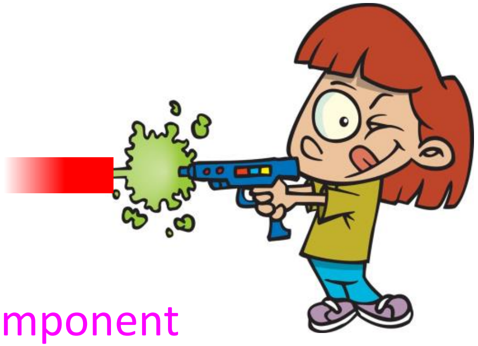
Light injection attacks:
Laser-seeding attack
Laser damage attack
Trojan-horse attack



Countermeasure against active attacks on the source

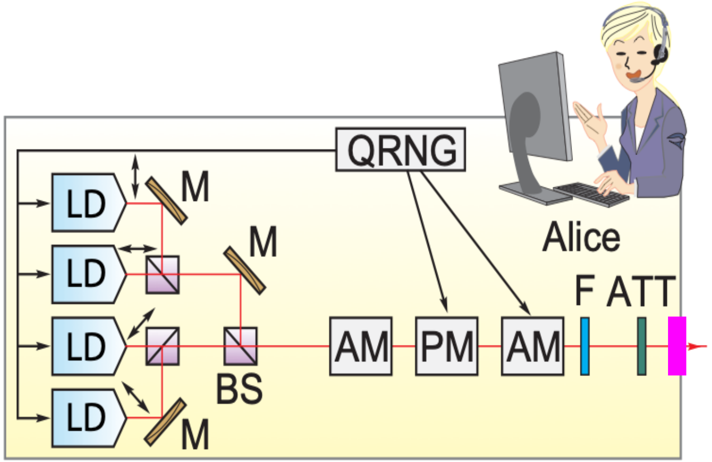


Light injection attacks

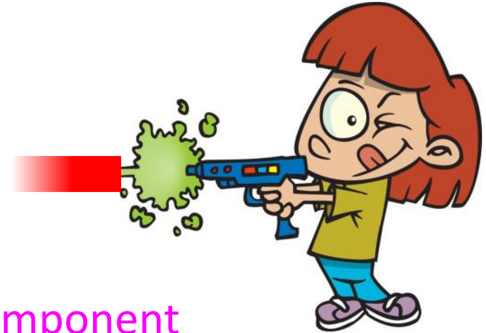


Add an isolation component
(Isolator / circulator)

Countermeasure against active attacks on the source



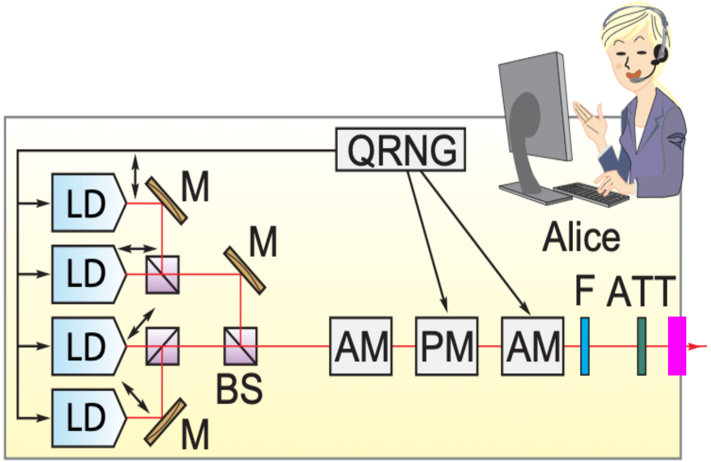
Light injection attacks



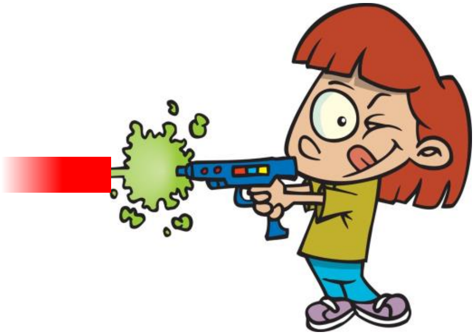
Add an isolation component
(Isolator / circulator)

Is it effective? Should be verified!

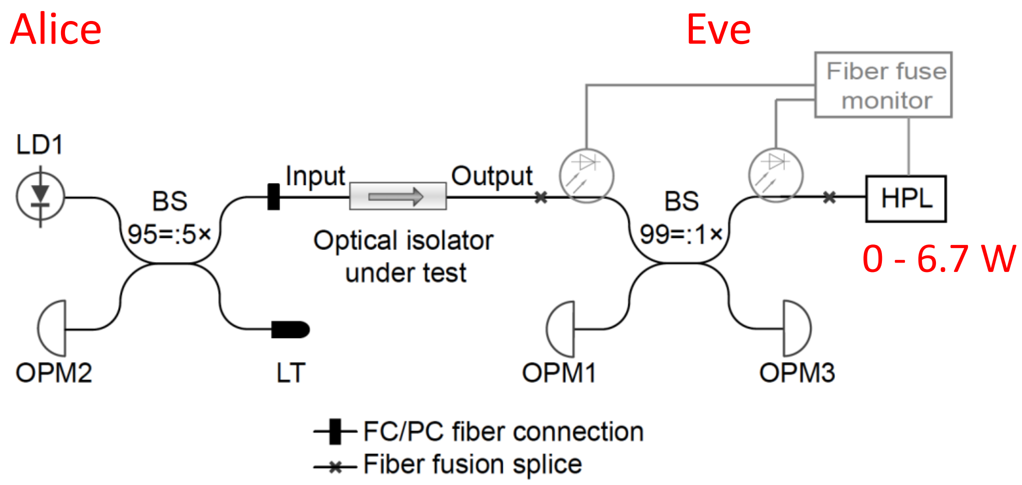
Countermeasure verification: isolation component



c.w. high-power laser



Countermeasure verification: isolators



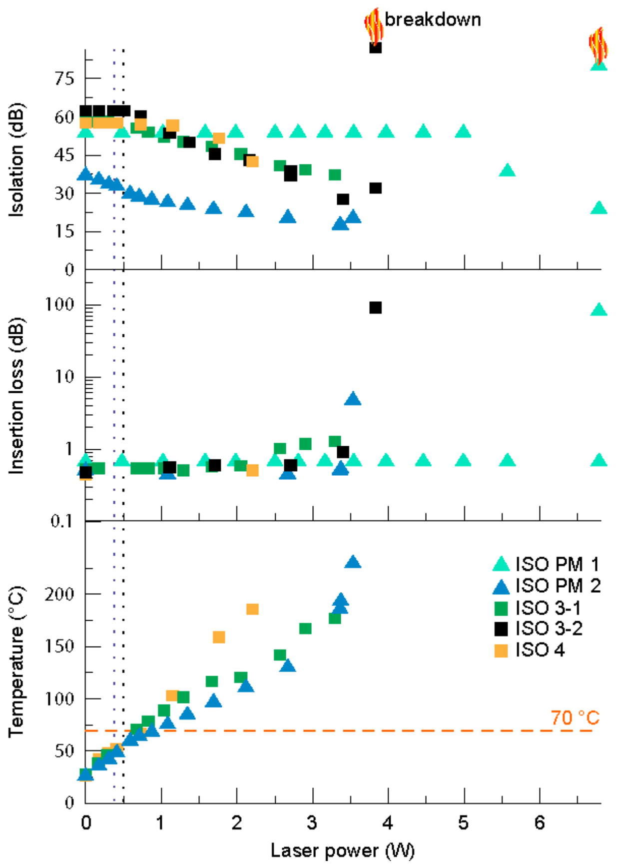
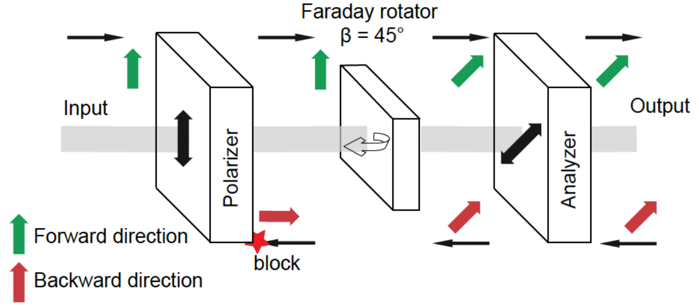


TABLE I: Testing results of isolators. All measurements are at 1550 nm.

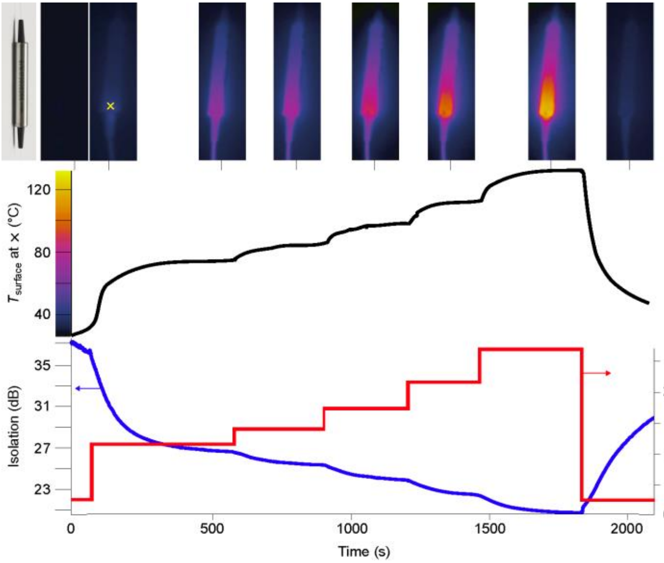
Sample	Specified minimum isolation (dB)	Initial Insertion loss (dB)	Initial Isolation (dB)	Minimum isolation (dB)	Maximum decrease of isolation (dB)	Irreversible damage at
ISO PM 1	46	0.66	53.7	21.8 @ 6.7 W, 360 s	31.9	6.7 W, 900 s
ISO PM 2	28	0.50	37.0	17.2 @ 3.37 W, 820 s	19.8	was not tested
ISO 3-1	46	0.45	58.1	37.1 @ 3.3 W, 260 s	21.0	was not tested
ISO 3-2	46	0.55	62.1	27.6 @ 3.4 W, 800 s	34.5	3.8 W, 90 s
ISO 4	55	0.52	57.6	42.4 @ 2.2 W, 200 s	15.2	was not tested

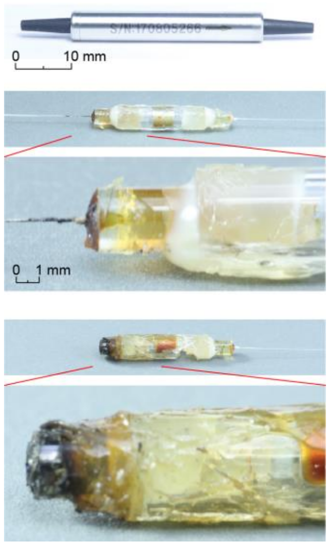
A. Ponosova, D. Ruzhitskaya, P. Chaiwongkhot, V. Egorov, V. Makarov, and A. Huang, PRX Quantum

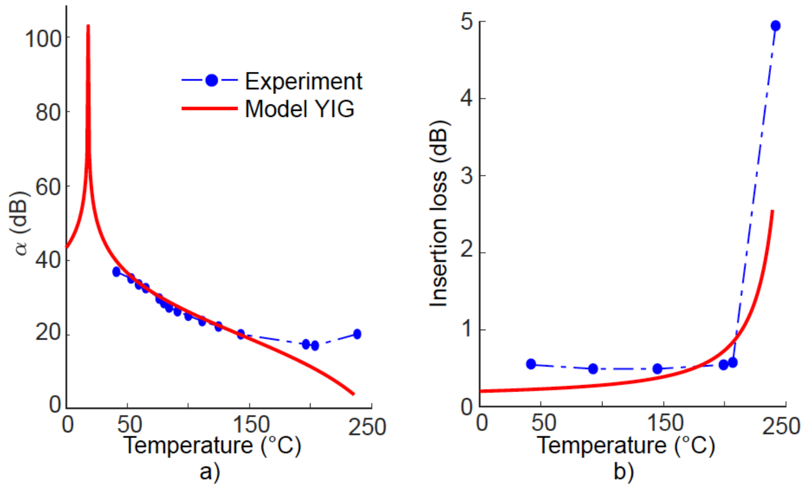
Countermeasure verification: isolators



$$\alpha(T) = -10\log\left[\beta + \frac{V(T)}{V(25\ °\mathrm{C})}\cdot k\right]$$

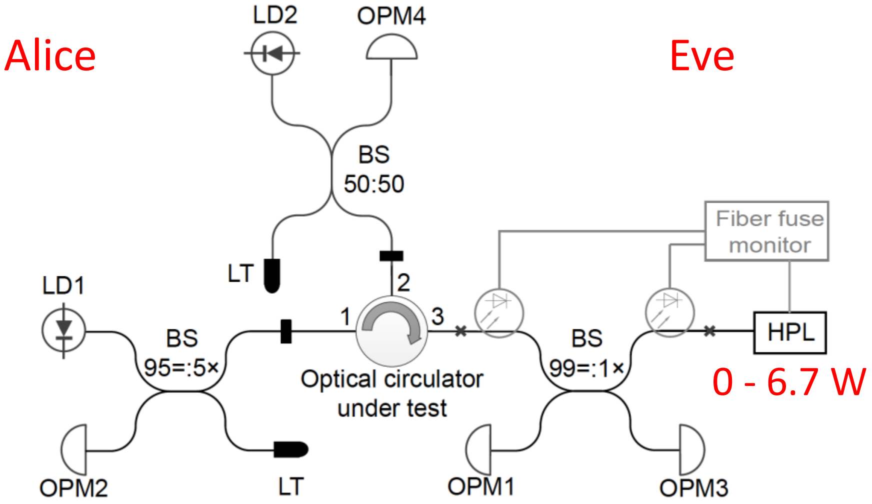






A. Ponosova, D. Ruzhitskaya, P. Chaiwongkhot, V. Egorov, V. Makarov, and A. Huang, PRX Quantum

Countermeasure verification: circulators



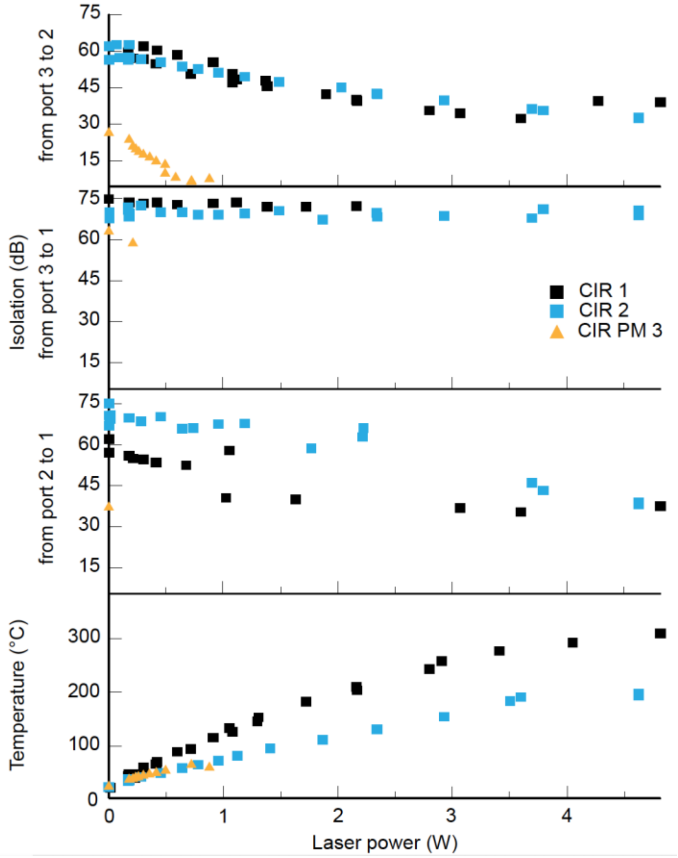


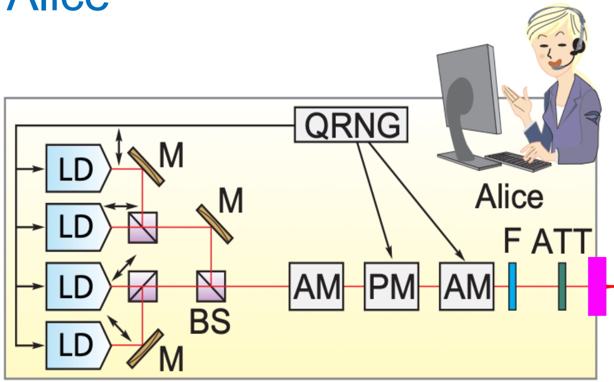
TABLE II: Testing results of circulators. All measurements are at 1550 nm.

Sample	Specified minimum isolation for all ports (dB)	Initial: Insertion loss (dB) 1 to 2	Initial: Insertion loss (dB) 2 to 3	Initial: Isolation (dB) 2 to 1	Initial: Isolation (dB) 3 to 2	Minimum isolation (dB) 2 to 1	Minimum isolation (dB) 3 to 2	Maximum decrease of isolation (dB) 2 to 1	Maximum decrease of isolation (dB) 3 to 2	Irreversible damage at
CIR 1	45	1.03	1.07	61.4	60.6	34.7 @ 3.6 W	32.2 @ 3.6 W	26.7	28.4	was not tested
CIR 2	40	0.72	0.83	67.0	65.7	38.3 @ 4.6 W	32.3 @ 4.6 W	28.7	33.4	4.6 W, 910 s
CIR PM 3	25	1.00	0.80	37.0	27.0	was not tested	6.4 @ 0.7 W	was not tested	20.6	0.9 W, 90 s

A. Ponosova, D. Ruzhitskaya, P. Chaiwongkhot, V. Egorov, V. Makarov, and A. Huang, PRX Quantum

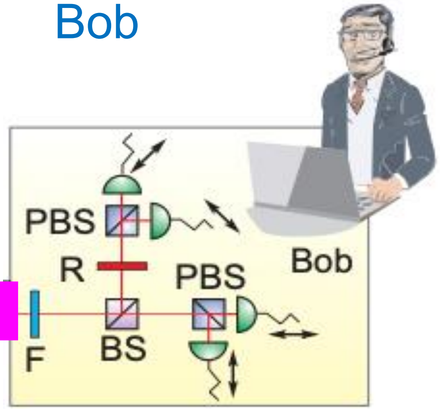
Countermeasure against active attacks on QKD

Alice



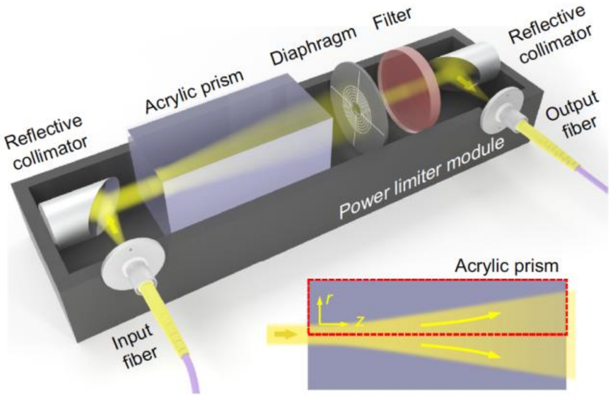
Eve

Bob



Power limiter

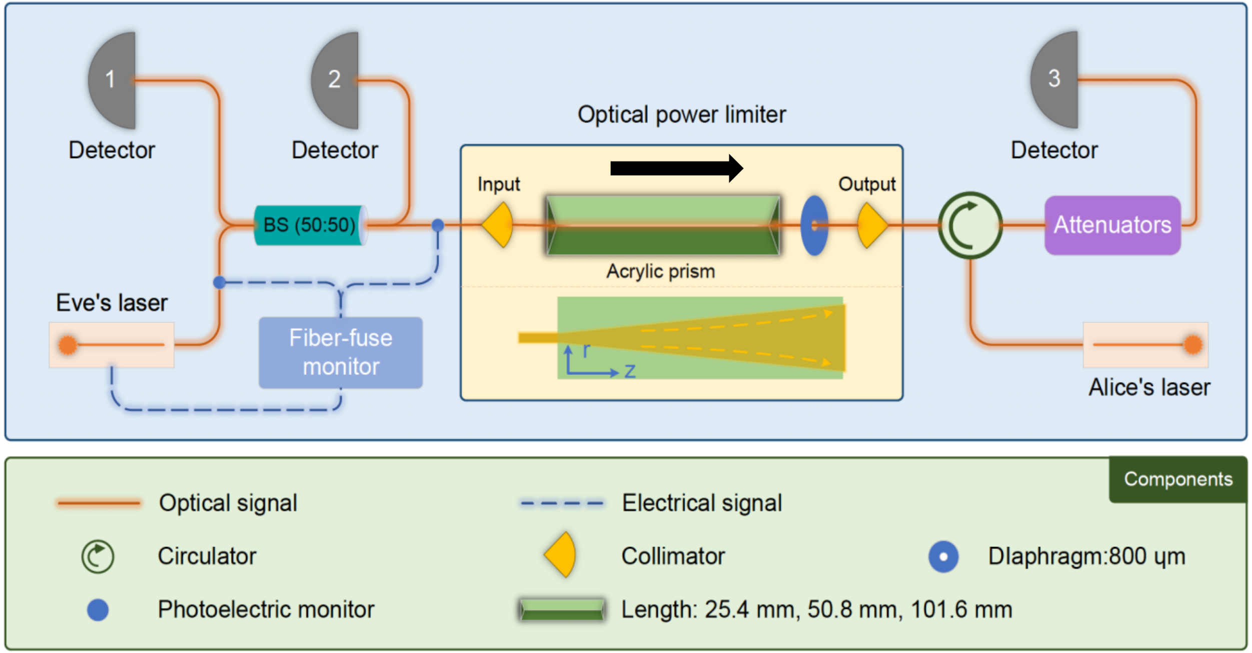
Power limiter



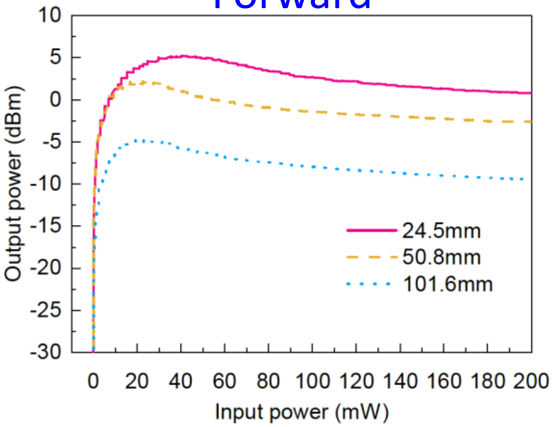
Can limit optical power well?
Should be verified!

Gong Zhang and et. al., PRX Quantum (2021)

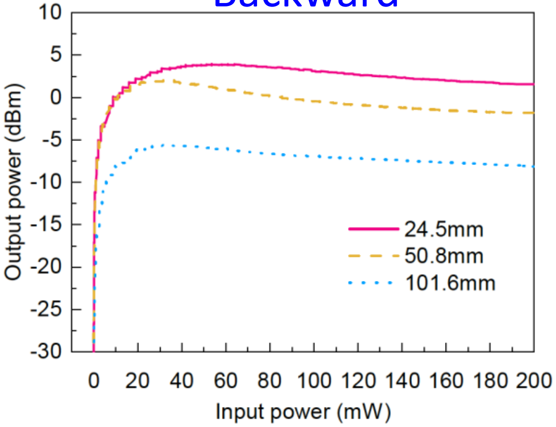
Countermeasure verification: Power limiter



Forward



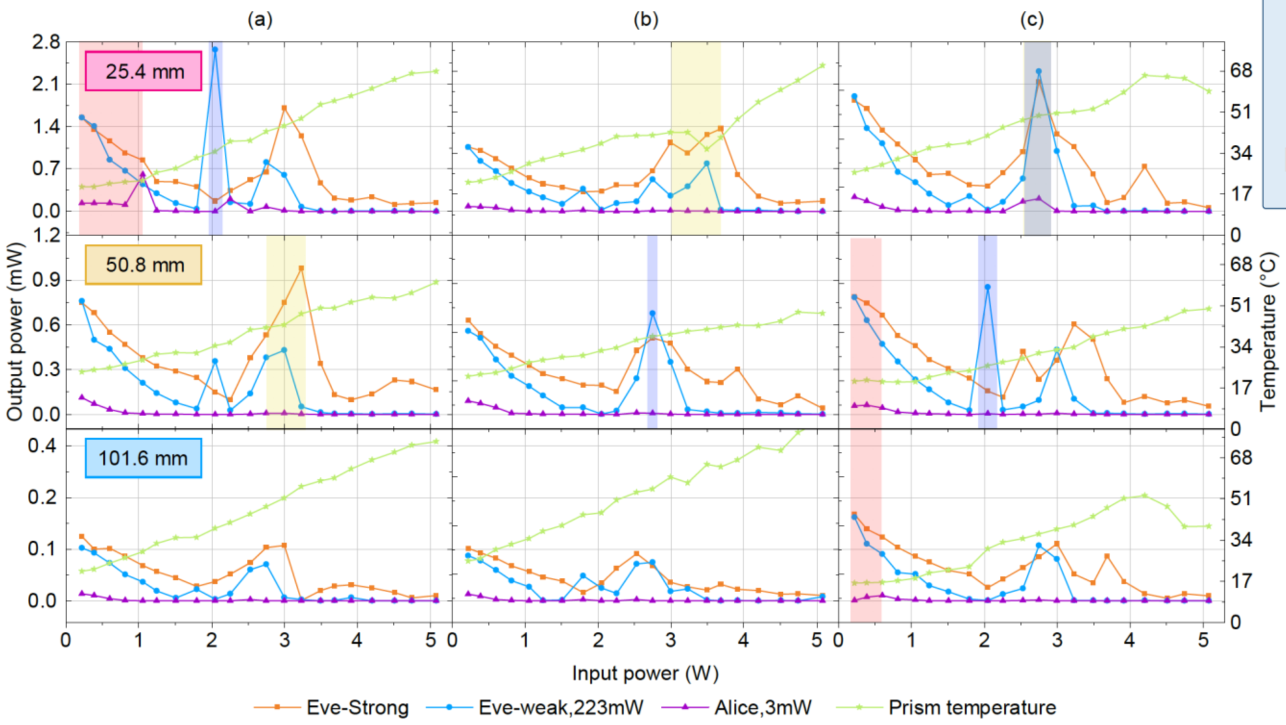
Backward

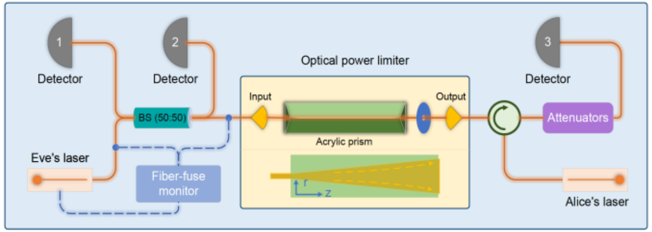


Q. Peng, A. Huang, and et. al., manucript in preparation

Countermeasure verification: Power limiter

c.w. high-power laser testing





Step 1

Eve-strong test: 223 mW - 5W

Step 2

Eve-weak test: 223 mW

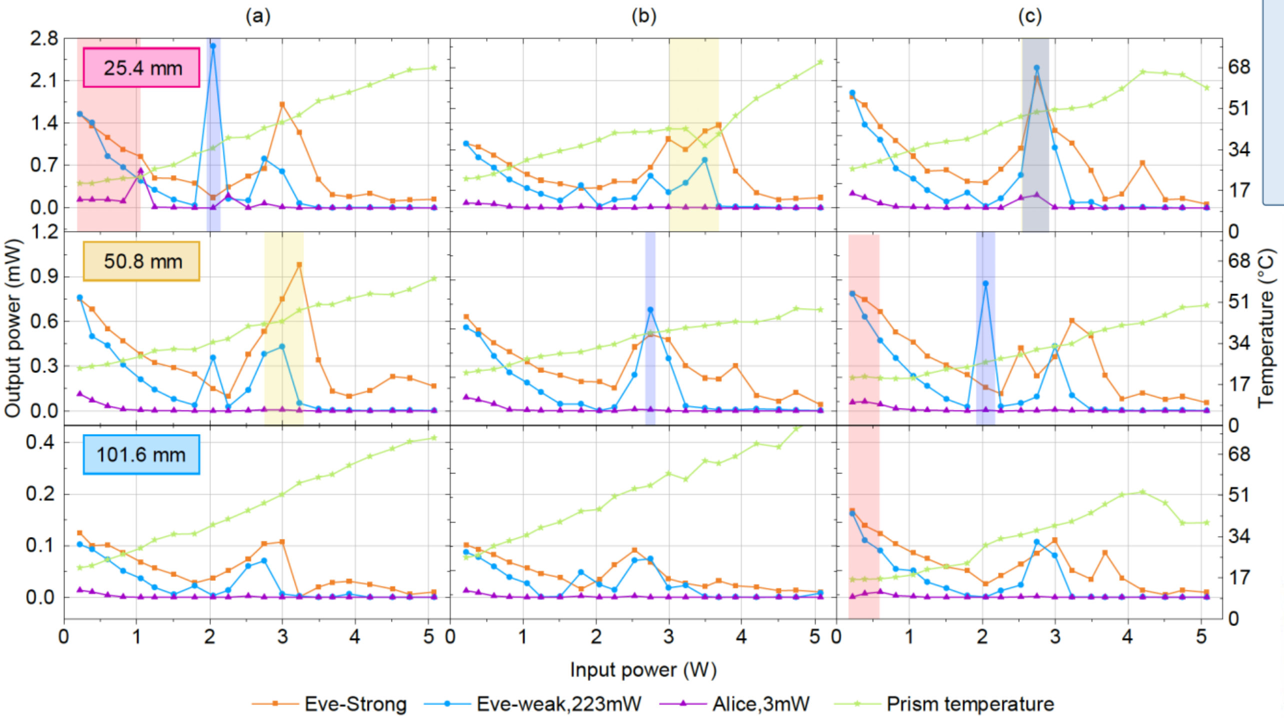
Step 3

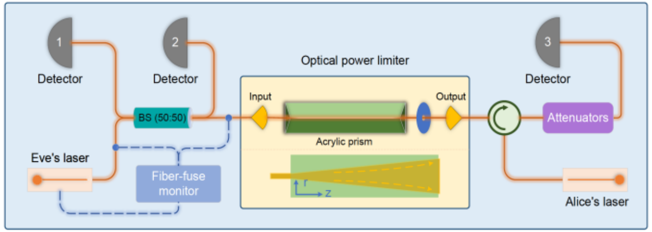
Alice test: 3 mW

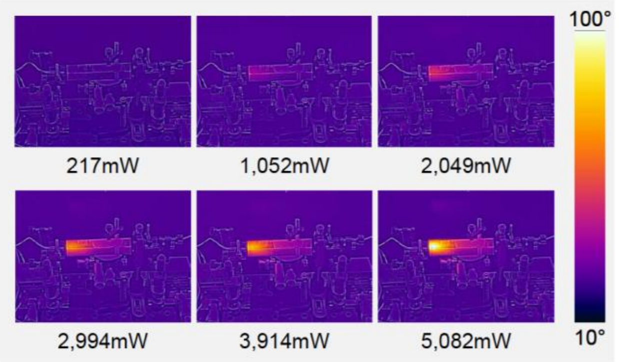
Q. Peng, A. Huang, and et. al., manucript in preparation

Countermeasure verification: Power limiter

c.w. high-power laser testing







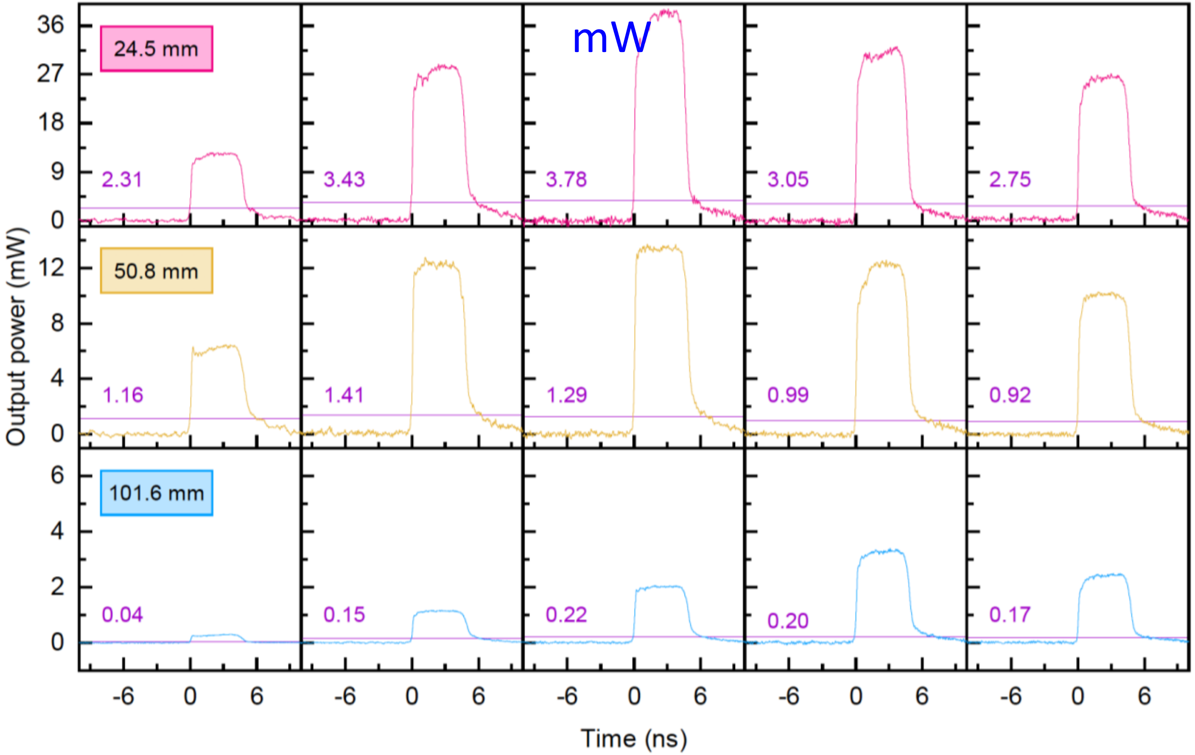
Q. Peng, A. Huang, and et. al., manucript in preparation

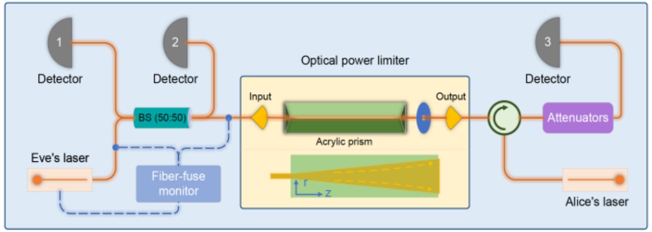
Countermeasure verification: Power limiter

40-MHz pulsed laser testing

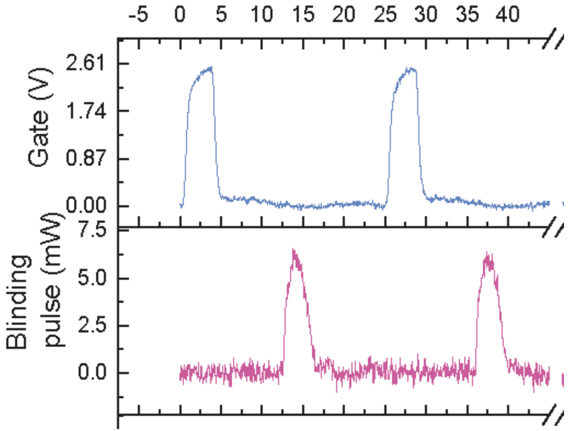
Eve average

10 mW 20 mW 30 mW 60 mW 80 mW





Pulsed illumination attack



Zhihao Wu, Anqi Huang, and et. al., Opt. Exp. (2020)

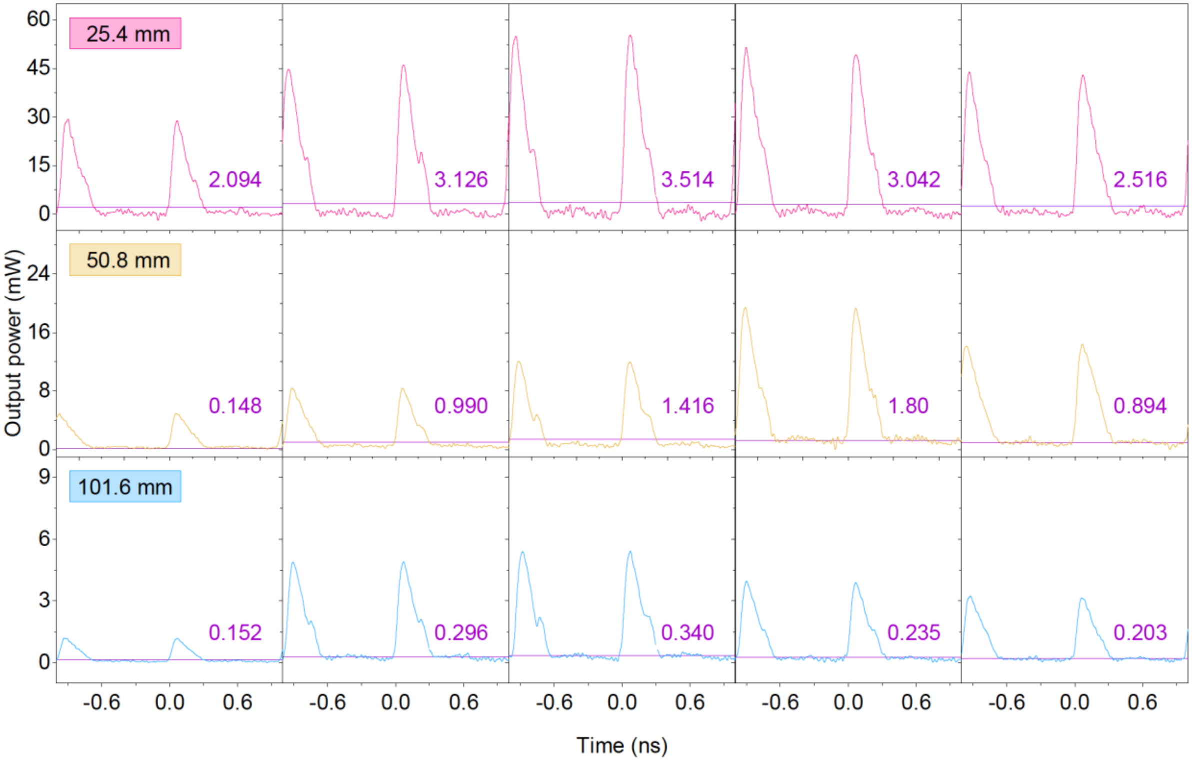
Q. Peng, A. Huang, and et. al., manucript in preparation

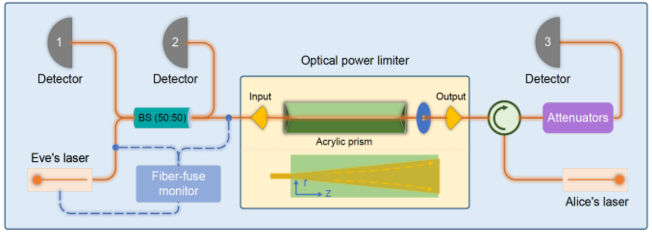
Countermeasure verification: Power limiter

1-GHz pulsed laser testing

Eve average

10 mW 20 mW 30 60 mW 80 mW





May help Trojan-horse attack on high-speed QKD system

Q. Peng, A. Huang, and et. al., manucript in preparation

Take home message

- The security of a QKD system might be compromised due to practical attacks

- Countermeasure shall be verified to investigate the security boundary

Thank you!