Securing Practical Quantum Cryptography with Optical Power Limiters

Gong Zhang[1,*], Ignatius William Primaatmaja[2],
Jing Yan Haw[1], Xiao Gong[1], Chao Wang[1,†], and Charles C.-W. Lim[1,2,‡]

*zhanggong@nus.edu.sg †wang.chao@nus.edu.sg ‡charles.lim@nus.edu.sg

[1]Department of Electrical & Computer Engineering,
National University of Singapore, Singapore

[2]Centre for Quantum Technologies,
National University of Singapore, Singapore

NUS National University of Singapore

Outline

- Background
  - Importance of power limiter in quantum cryptography
  - Introduction of thermo-optic defocusing
- Experimental and simulation results
- Possible attack consideration
- Application in plug-and-play MDI-QKD
- Conclusion

Hacking Practical QKD

Detector-blinding attack Makarov 2009, Lydersen 2010

Receiver laser damage attack Bugge 2014, Makarov 2016

Time-shift attack Qi 2007, Zhao 2008

Wavelength attack Huang 2013, Li 2011

Back-flash attack Kurtsiefer 2001

Channel calibration Jain 2011

Detector deadtime Weier 2011

Spatial efficiency mismatch Rau 2015, Sajeed 2015

Target: **Receiver**

Solution
Measurement-device-independent
MDI-QKD

Trojan-horse attack Gisin 2006, Jain 2014

Intensity information Jiang 2012

Modulation pattern effect Yoshino 2016

Source laser damage attack Huang 2020

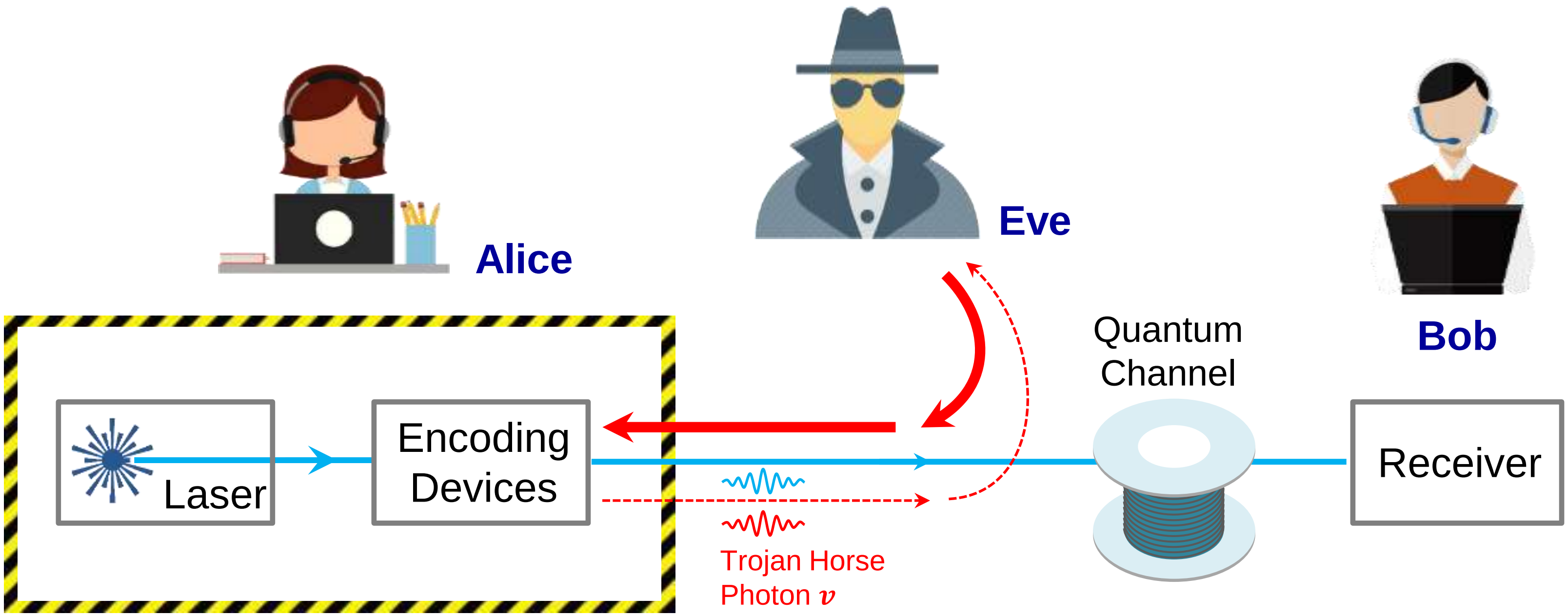
Phase-remapping attack Fung 2007, Xu 2010

Phase information Sun 2012, 2015, Tang 2013

Target: **Source**

Lo, H. K., et al. (2014). Nature Photonics, 8(8), 595-604.
Scarani, V., et al. (2009). Reviews of modern physics, 81(3), 1301.

Trojan-Horse Attack



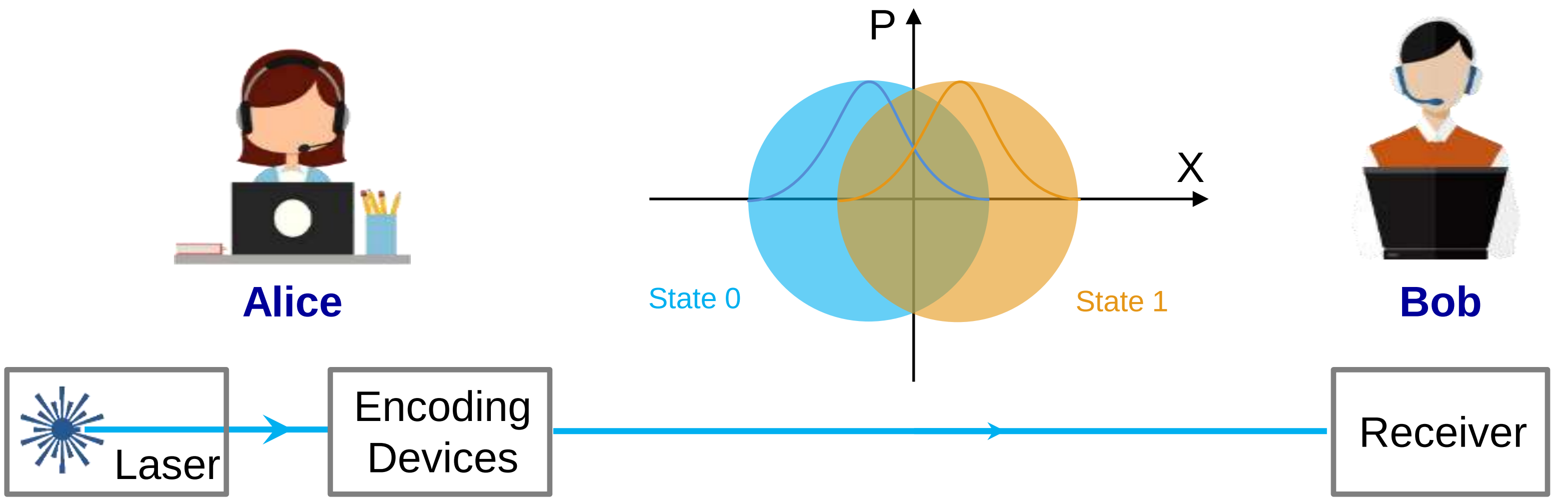
Current countermeasures

- Phase randomize (Reduce I_{eve}[1])
- Watchdog detector (Can be bypassed[2])
- Passive components such as isolators (Limited degree-of-freedom, one-way application only, high isolation)

Basic idea is to limit the amount of unauthorized input power.

[1] Gisin, N., et al. (2006). Physical Review A, 73(2), 022320. Jain, N., et al. (2014). New Journal of Physics, 16(12), 123030.
[2] Sajeed, S., et al. (2015). Physical Review A, 91(3), 032326.

Semi-DI with Energy Bound



- Bound on the mean energy is one way to provide a practical Semi-Device-Independent (Semi-DI) framework.
- Use energy bound to bound the overlap between the prepared states.
- Energy bound could lead to certifiable quantum randomness.

Again, a power limiting device is important here!

Avesani, M., et al. (2020). arXiv:2004.08344v1.
Van Himbeeck, T., et al. (2017). Quantum, 1, 33.
Van Himbeeck, T., et al. (2019). arXiv:1905.09117.
Rusca, D., et al. (2019). Physical Review A, 100(6), 062338..

Proposal: Quantum Optical Fuse / Power limiter

The device should ideally have the following properties:

- ❑ Provides a **reliable and characterizable** power limiting threshold (in the order of a few photons to hundreds of photons).
- ❑ If the input energy exceeds the threshold, the device will stop the communication channel.
- ❑ **Cost-effective, passive, and easily replaceable**.
- ❑ Power limiting effects are **independent of other degree of freedoms**, e.g., frequency, polarization, etc.

It is **timely to develop such devices**, for we now have **a wide range of security proof methods with possible energy constraints features**:

Lucamarini et al 2015, Tamaki et al 2016, Van Himbeeck et al 2019, Pereria et al 2019, Primaatmaja et al 2019, Navarrete et al 2020, just to name a few.

Review of Optical Power Limiter

Fiber damage

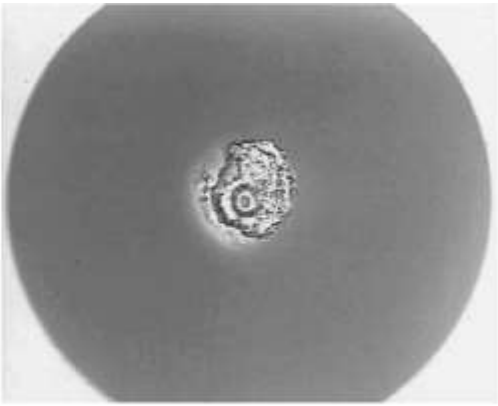


Figure 1 Damage to connector endface.

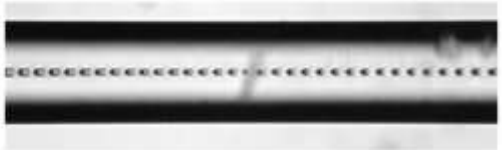


Figure 2 Optical fiber after fuse propagation.

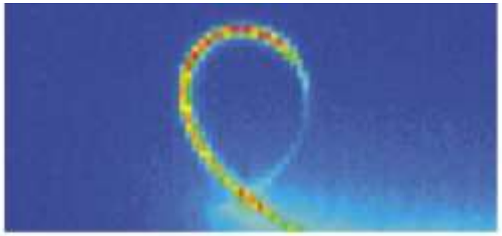
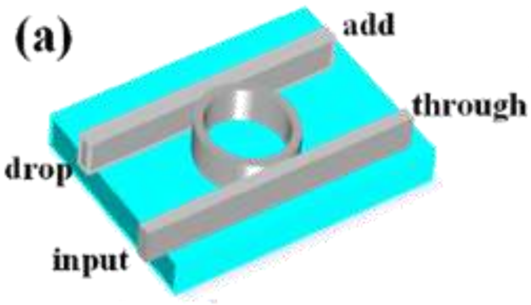
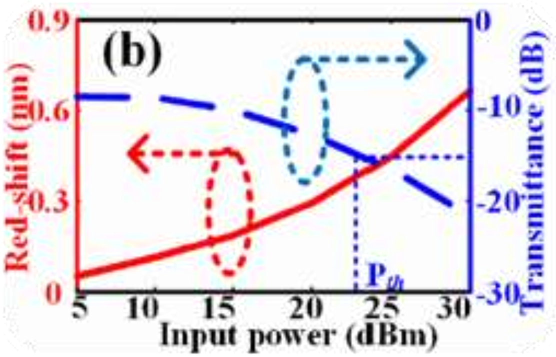


Figure 10 Observation by thermo-viewer.

- $10^2 – 10^3$ mW level

Filter based





- Using thermo-optic effect or optical force to tune the filter center wavelength
- Narrow operation bandwidth, limited extinction ratio
- $10 – 10^2$ mW level

Nonlinear effect

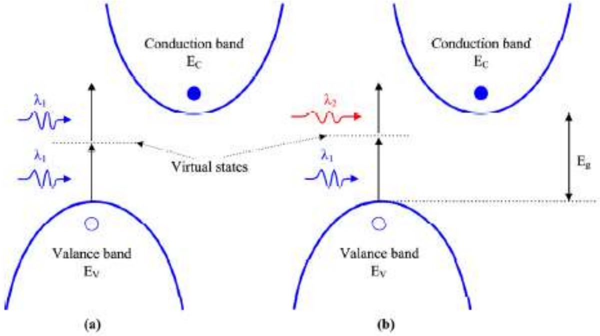
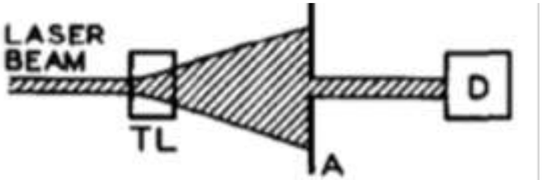
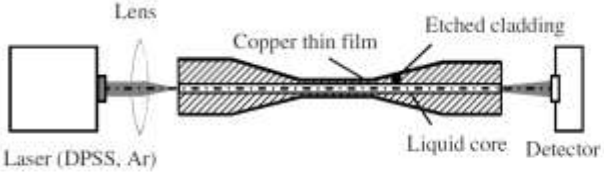


Fig.1. Schematic illustration of TPA in silicon. (a) degenerate TPA.(b) non-degenerate TPA.

Two-photon absorption

- $10 – 10^3$ mW level



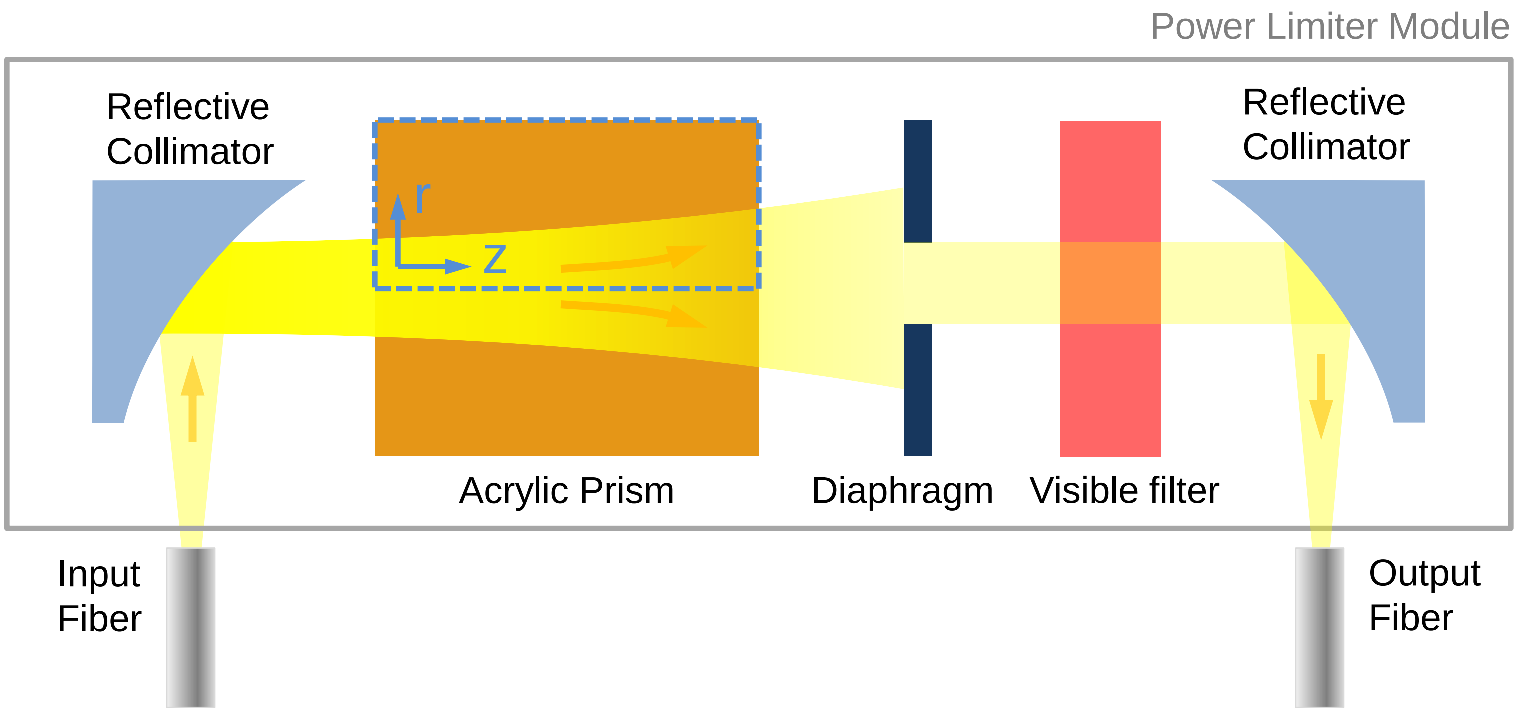


Thermo-optical defocusing

- $10 – 10^2$ mW level

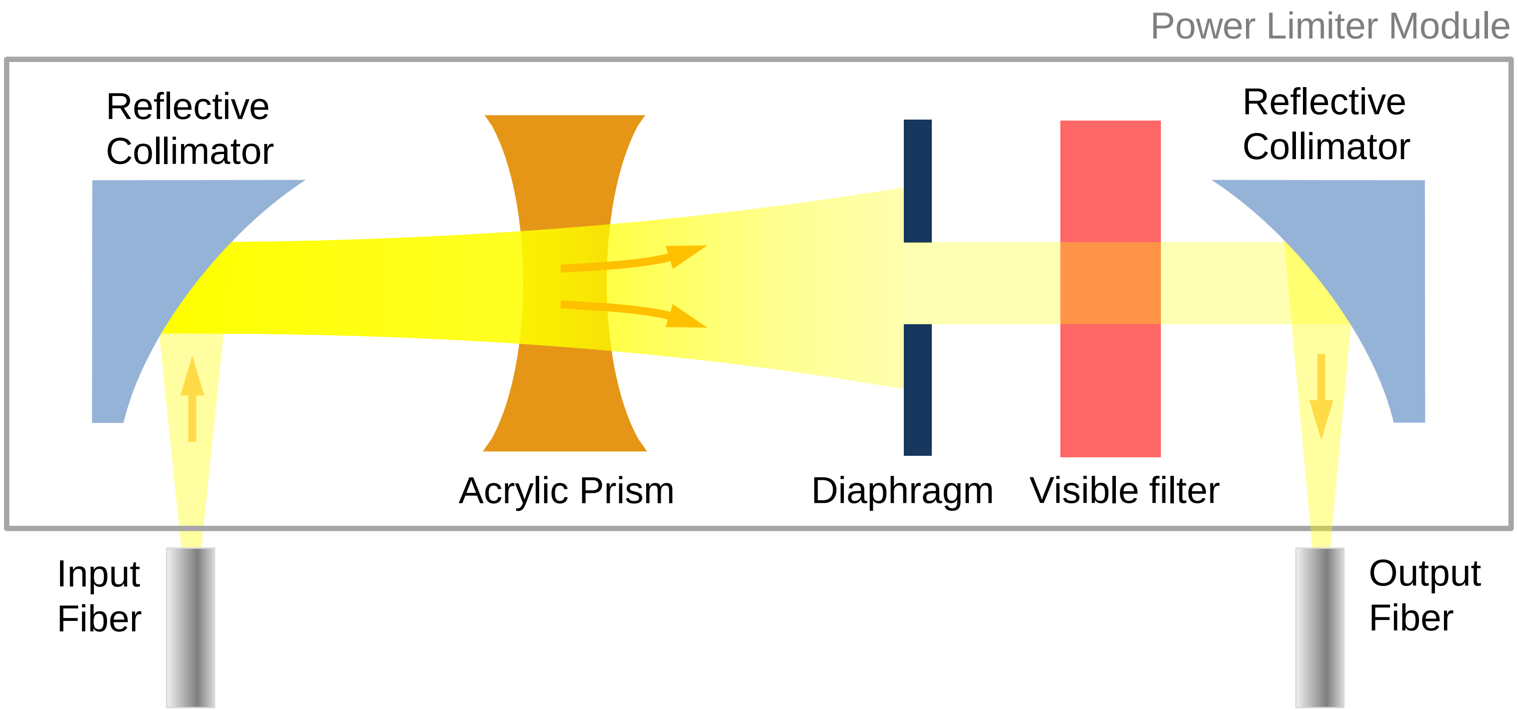
Seo, K., et al. (2003). Furukawa Review, 24(24), 17-22.
Dini, D., et al. (2016). Chemical reviews, 116(22), 13043-13233.
Yan, S., et al. (2014). Scientific reports, 4, 6676.
Sang, X., et al. (2009). Journal of optoelectronics and advanced materials, 11(1), 15.
Martincek, I., et al. (2011). IEEE Photonics Technology Letters, 24(4), 297-299.

Our Choice: Thermo-Optical Defocusing



- Negative thermo-optic coefficient of acrylic: $\frac{dn}{dT} = -1.3 \times 10^{-4}\ K^{-1}$
- Higher absorbed power diverges the input light more
- A tunable diaphragm controls the received power
- Robust and stable performance, compact and cost-effective design

Our Choice: Thermo-Optical Defocusing



- Negative thermo-optic coefficient of acrylic: $\frac{dn}{dT} = -1.3 \times 10^{-4}\ K^{-1}$
- Higher absorbed power diverges the input light more
- A tunable diaphragm controls the received power
- Robust and stable performance, compact and cost-effective design

Theoretical Modeling

- Angular divergence of a paraxial light ray passing through a refractive index gradient

$$\frac{\partial \theta_r}{\partial z} = \frac{1}{n}\left(\frac{\partial n}{\partial T}\right)\left(\frac{\partial T}{\partial r}\right)$$

- Absorbed laser power I is balanced with the heat transfer mechanism (Assume heat transfer in r-direction only)

$$\alpha I = -\frac{k}{r}\frac{\partial}{\partial r}\left(r\frac{\partial T}{\partial r}\right)$$

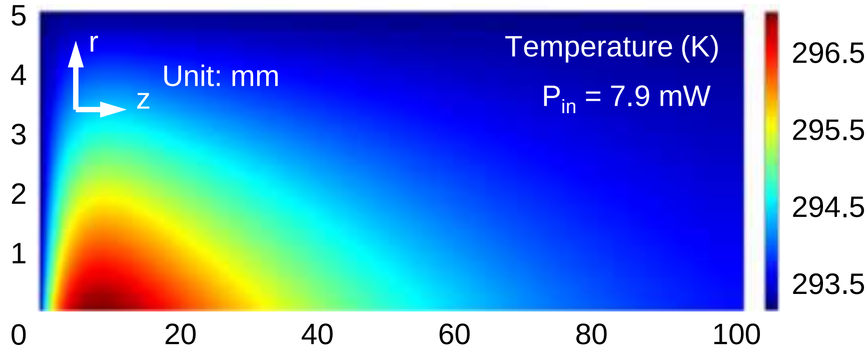
- Laser intensity at position (r, z)

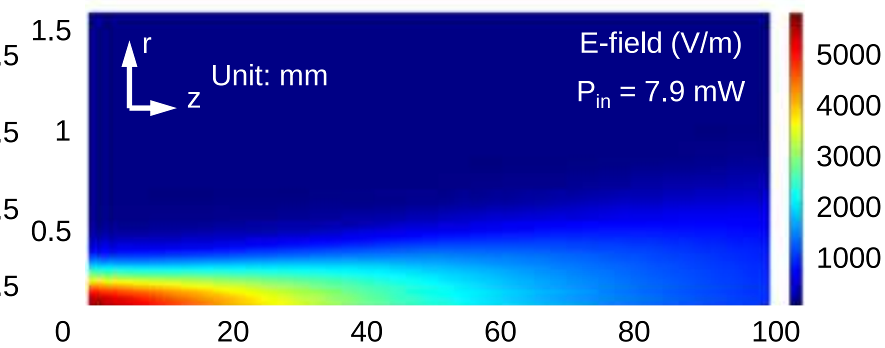
Gaussian beam shape

$$I(r,z) = I(r,0)\cdot \exp\left(-\alpha z + \frac{\frac{\partial n}{\partial T} P e^{-\frac{r^2}{a^2}}\left(z - \frac{1}{\alpha}\left(1 - e^{-\alpha z}\right)\right)}{\pi k n a^2}\right)$$

Absorption

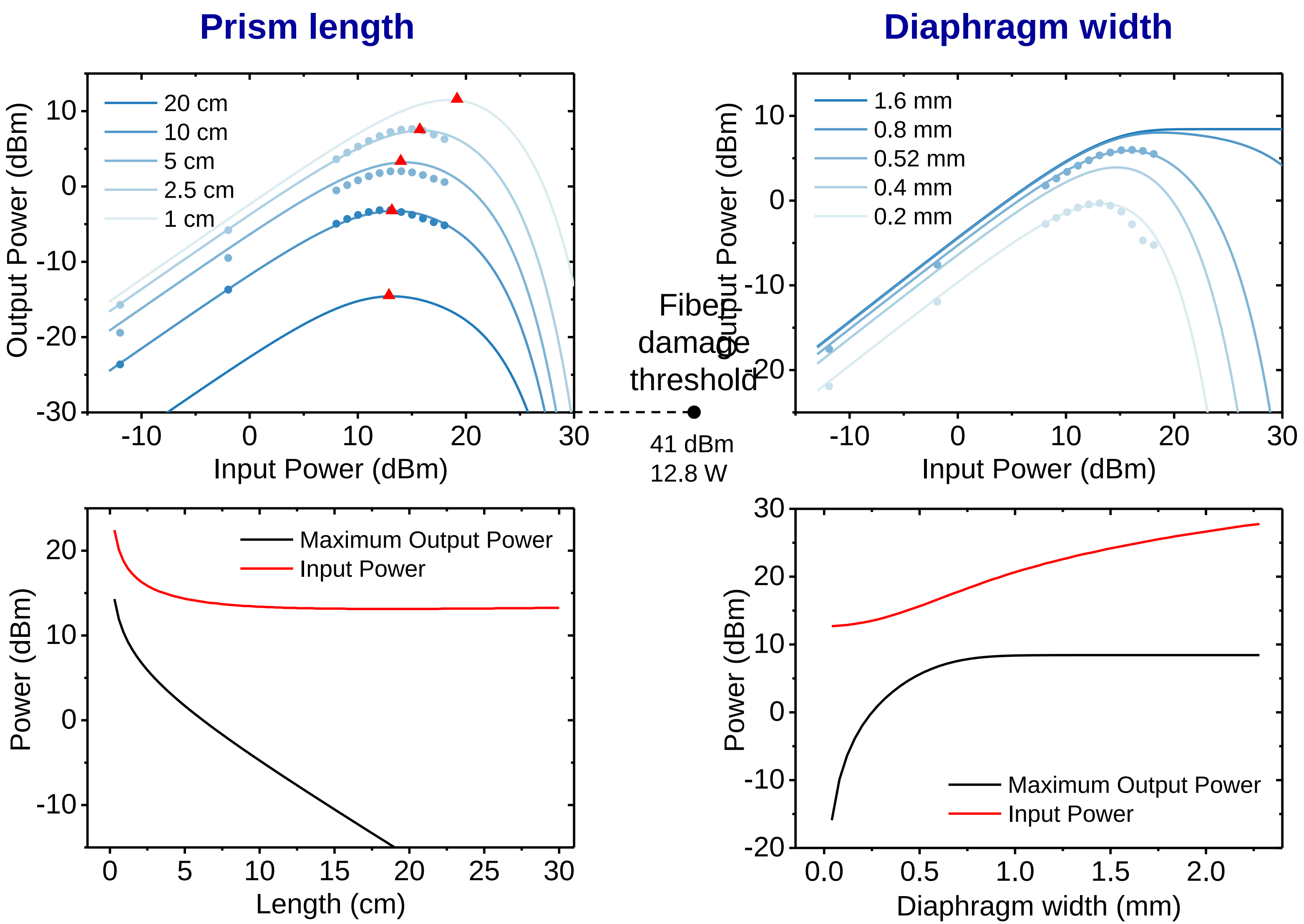
- COMSOL simulation





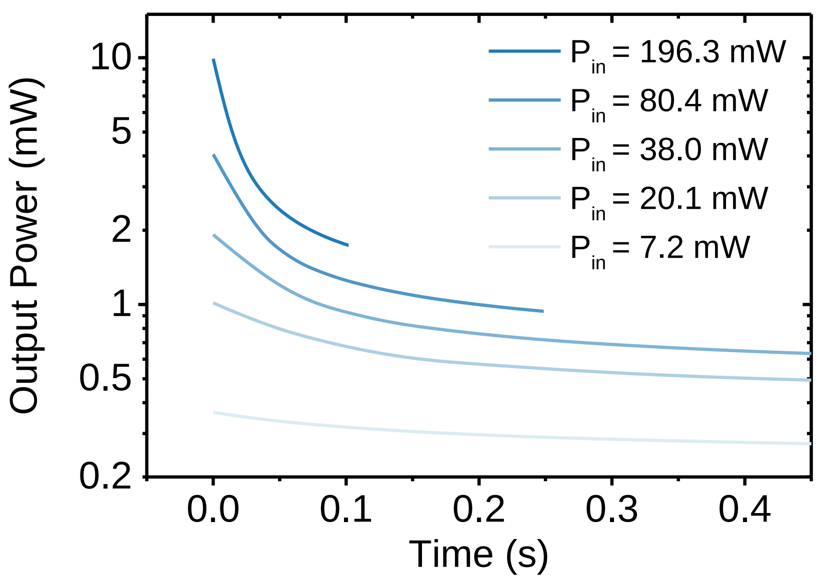
Smith, D. (1969). IEEE Journal of Quantum Electronics, 5(12), 600-607.
DeRosa, M. E., et al. (2003). Applied optics, 42(15), 2683-2688.

Input-Output Power Relationship

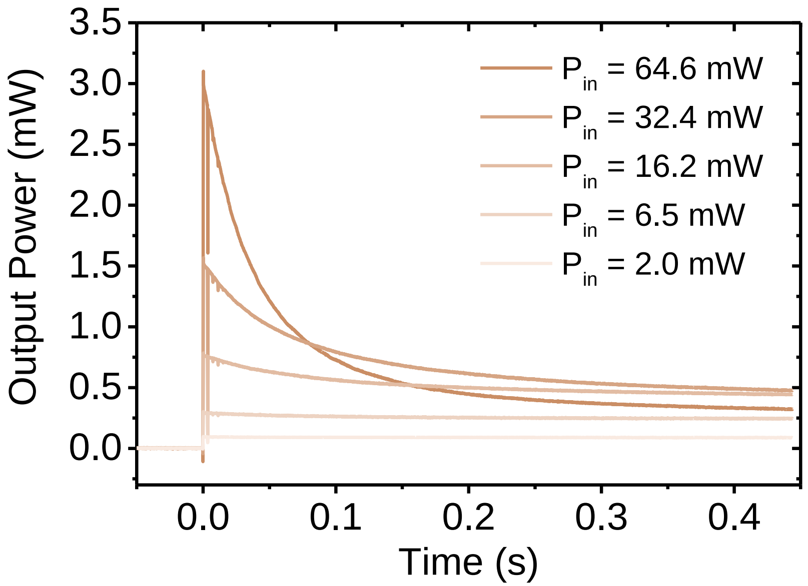


Lucamarini, M., et al. (2015). Physical Review X, 5(3), 031030.

Response Time Consideration



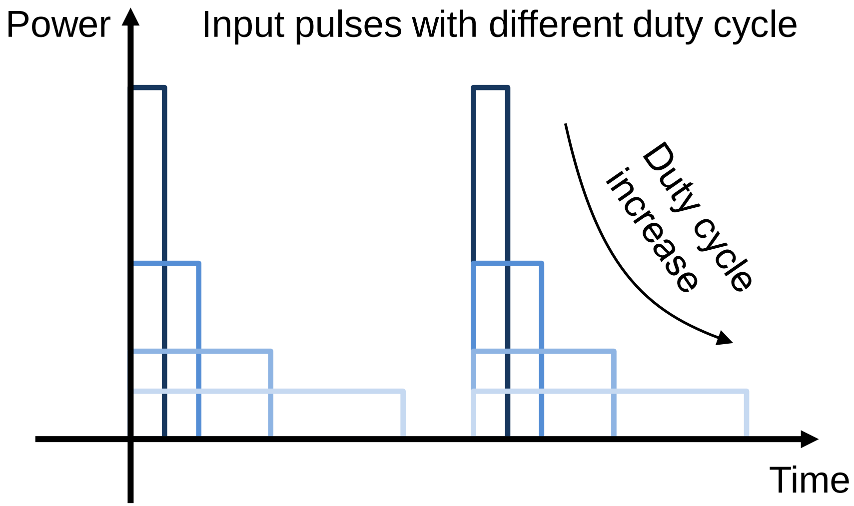
Simulation Results

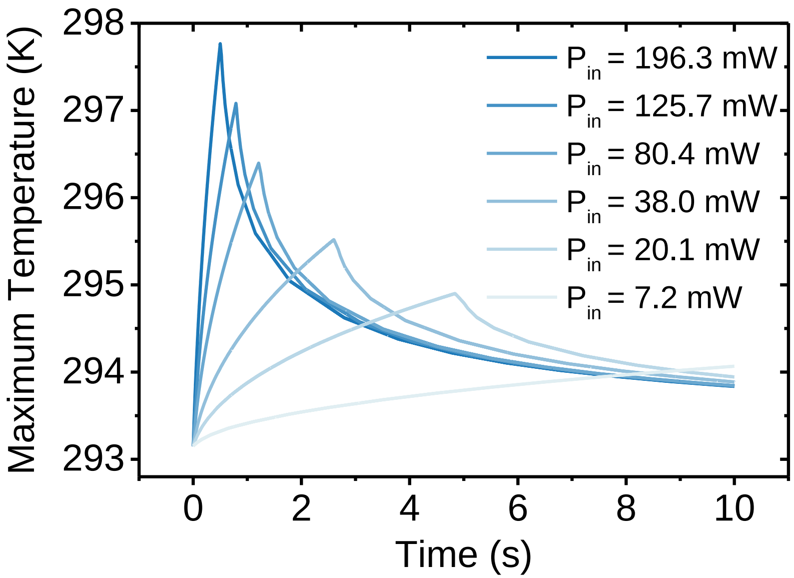


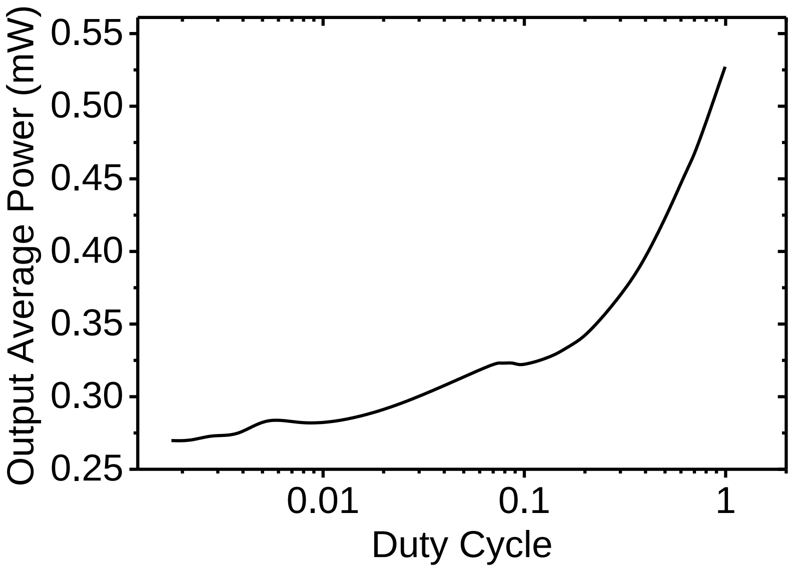
Experimental Results

Shorter pulse ➡ Higher output power **?**

Pulsed Response Simulation







- Assume 20 mW average input power (Based on prior experiment)
- Pulsed input experiences **greater power-limiting effect** comparing to the continuous-wave cases

Wavelength Dependence

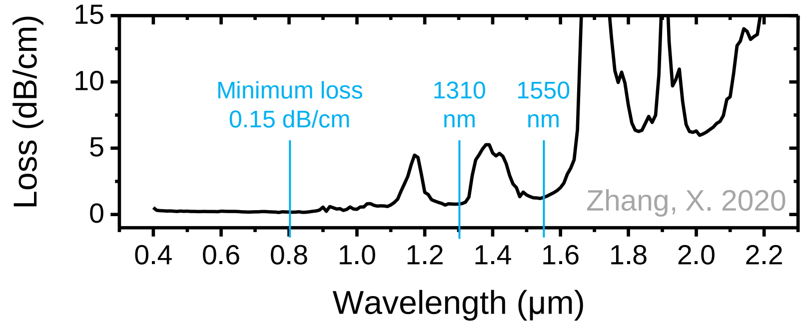
Thermo-optic coefficient

$$TOC = \frac{dn}{dT} = \frac{(n^2-1)(n^2+2)}{6n}(\Phi - \beta)$$

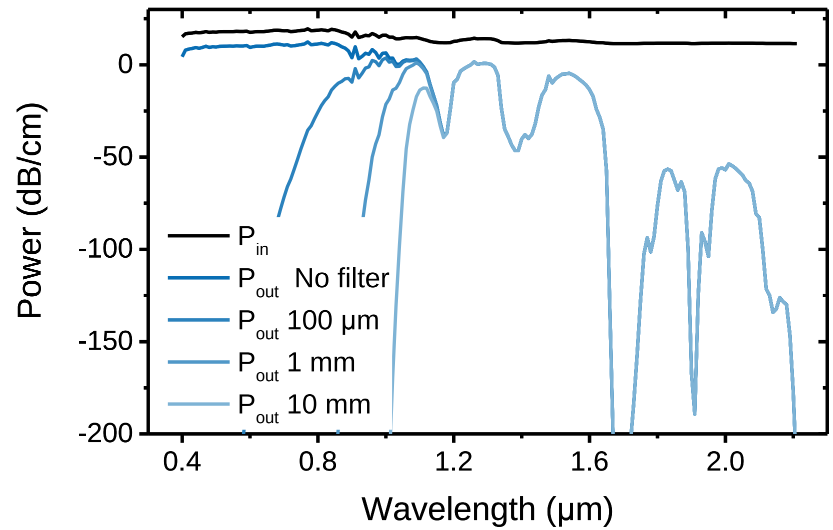
- Electronic polarizability $\Phi > 0$ typically
- Volumetric expansion β is dominant in polymer

Wavelength (nm)	dn/dT (x10^4 /K)
472.9	-1.37
780.4	-1.37
1055.7	-1.30
1308.9	-1.33
1550	-1.3

Material absorption



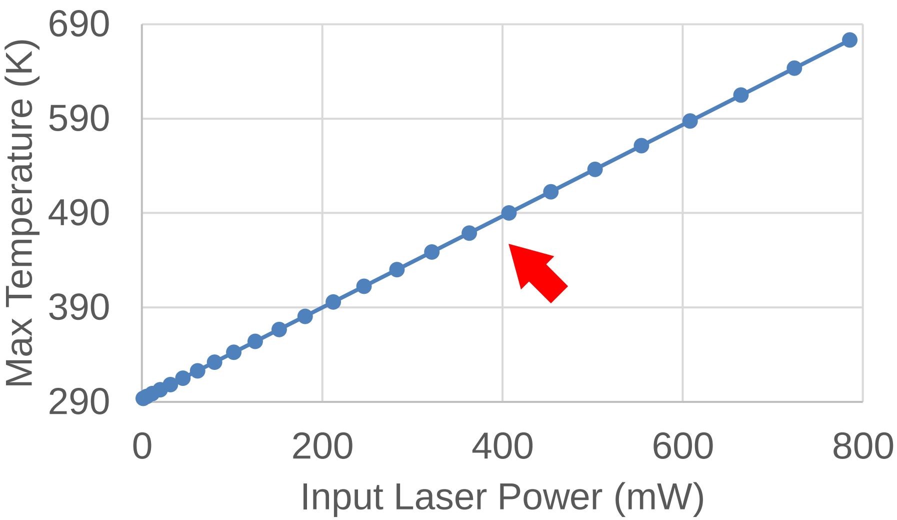
- Consider fiber damage threshold 12.8W
- Silicon absorber limit visible light



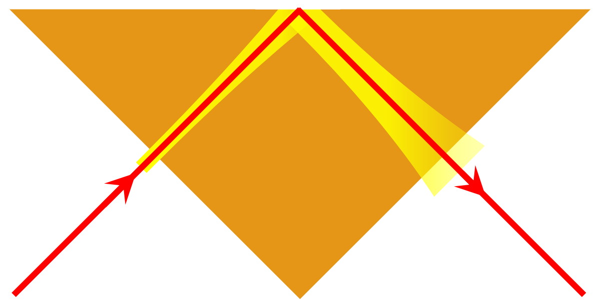
Zhang, Z., et al. (2006). Polymer, 47(14), 4893-4896.
Beadie, G., et al. (2015). Applied optics, 54(31), F139-F143.
Zhang, X., et al. (2020). Applied Optics, 59(8), 2337-2344.
Lucamarini, M., et al. (2015). Physical Review X, 5(3), 031030.

Laser Damage Attack

Property	Value
Melting Point (K)	404
Boiling Point (K)	473
Evaporation rate (g/s)	log w = 5.87-6.77x10³/T



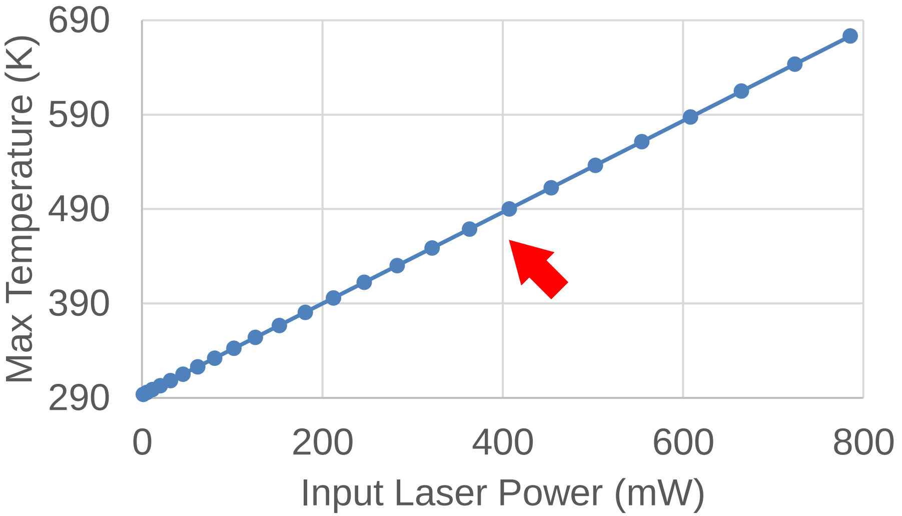
- Material could be **melted and evaporated** under strong laser beam. As a result of the evaporation and assist gas pressure, the material is thrown out of the hole.
- A reflection structure could be implemented to permanently fuse the optical path.



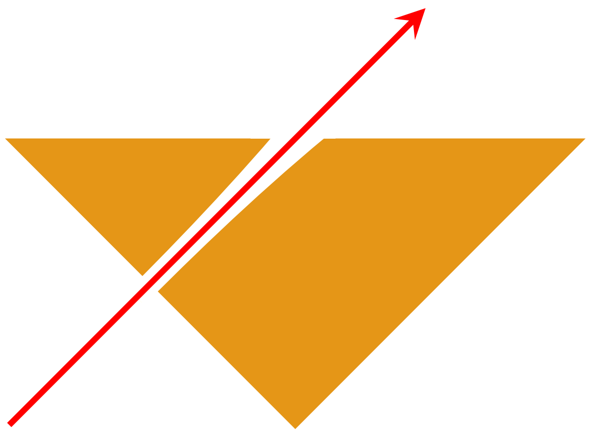
Berrie, P. G., et al (1980). Optics and Lasers in Engineering, 1(2), 107-129.
M Taha, R. (2014). Diyala Journal of Engineering Sciences, 7(1), 30-39.

Laser Damage Attack

Property	Value
Melting Point (K)	404
Boiling Point (K)	473
Evaporation rate (g/s)	log w = 5.87-6.77x10^3/T

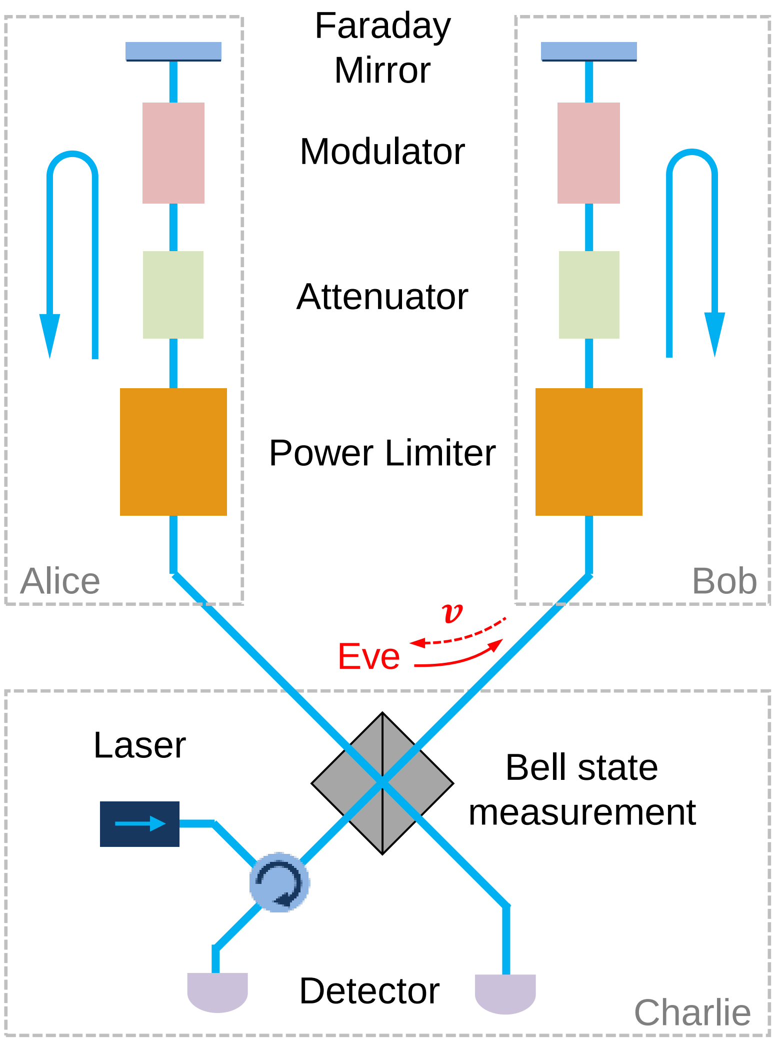


- Material could be **melted and evaporated** under strong laser beam. As a result of the evaporation and assist gas pressure, the material is thrown out of the hole.
- A reflection structure could be implemented to permanently fuse the optical path.



Berrie, P. G., et al (1980). Optics and Lasers in Engineering, 1(2), 107-129.
M Taha, R. (2014). Diyala Journal of Engineering Sciences, 7(1), 30-39.

Application: Plug-and-Play MDI-QKD

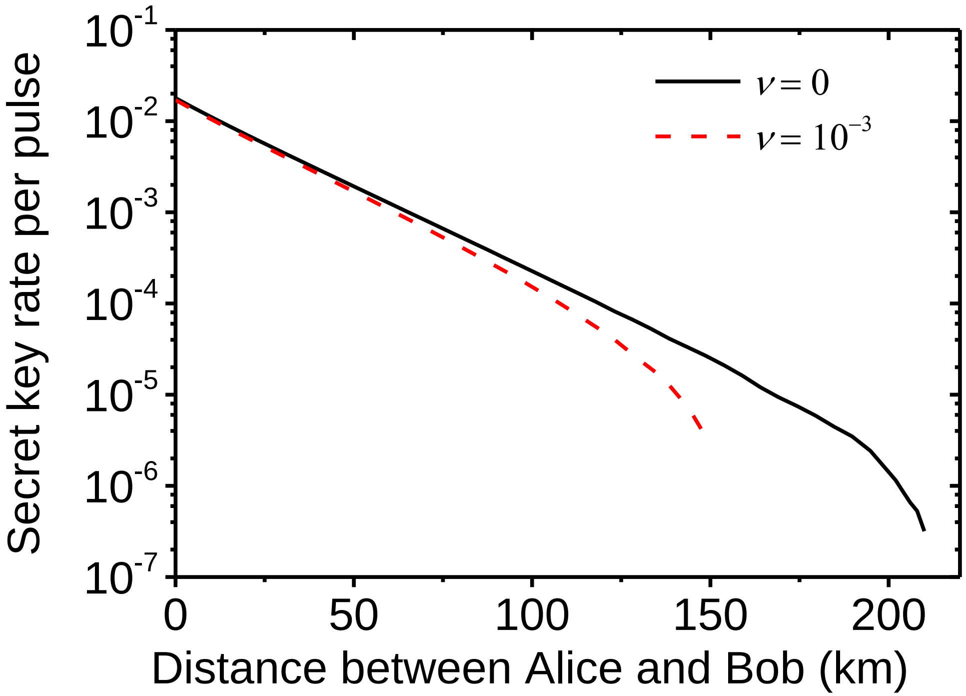


Patent filed: SG Non-Provisional Application No.10202006635S

- Plug-and-play phase-encoding measurement-device-independent (MDI) QKD
  - **Robust performance with simple setup**.
  - Common laser source for all users, enables **identical central wavelength** and **accurate clock synchronization**.
  - Automatically compensate for any **birefringence effects** and **polarization-dependent losses** in optical fibers.
- The average Trojan photon number ν could provide Eve with information about the encoded phase

Xu, F. (2015). Physical Review A, 92(1), 012333.
Lucamarini, M., et al. (2015). Physical Review X, 5(3), 031030.
Tamaki, K., et al. (2016). New Journal of Physics, 18(6), 065008.

Secret Key Rate against THA



Parameters	Value
Detector efficiency	70%
Dark count rate	10^{-7}
Misalignment error	2%
Fiber loss	0.2 dB/km

Consider a repetition rate of 1 GHz, the Trojan-horse photon power is about 1.28 x 10^{-10} mW

- Assume average Trojan photon leakage ν from coherent state (CW and Pulse).
- Proof technique taken here:
  Primaatmaja, I. W., et al. (2019). Physical Review A, 99(6), 062332.

Conclusions and Outlooks

Ideal model

- ❑ Provides a reliable and characterizable power limiting threshold (in the order of a few photons to hundreds for photons).
- ❑ If the input energy exceeds the threshold, the device will stop the communication channel.
- ❑ Cost-effective, passive, and easily replaceable.
- ❑ Power limiting effects are independent of other degree of freedoms, e.g., frequency, polarization, etc.

Our scheme

- ✓ Passive power limiter at mW level. Using additional attenuation for few-photon level limitation.
- ✓ If the input energy exceeds the threshold, the output power will be limited, and start decrease.
- ✓ Cost-effective, passive, and easily replaceable.
- ✓ Power limiting effects for both CW and pulsed light, wavelength and polarization independent.

- ❑ To do: Security analysis of MDIQKD with untrusted light source
- ❑ To do: Measurement with visible wavelength and high-power laser

Acknowledgement

NUS National University of Singapore

Department of Electrical & Computer Engineering
Faculty of Engineering

CQT Centre for Quantum Technologies

We are hiring postdoctoral researchers (theory/experiment)!

Please contact us at charles.lim@nus.edu.sg for more information.

Securing Practical Quantum Cryptography with Optical Power Limiters

Gong Zhang[1,*], Ignatius William Primaatmaja[2], Jing Yan Haw[1], Xiao Gong[1], Chao Wang[1,†], and Charles C.-W. Lim[1,2,‡]

*zhanggong@nus.edu.sg †wang.chao@nus.edu.sg ‡charles.lim@nus.edu.sg

[1]Department of Electrical & Computer Engineering,
National University of Singapore, Singapore

[2]Centre for Quantum Technologies,
National University of Singapore, Singapore