Towards secure QKD with testable assumptions on modulation devices

Akihiro Mizutani[1]

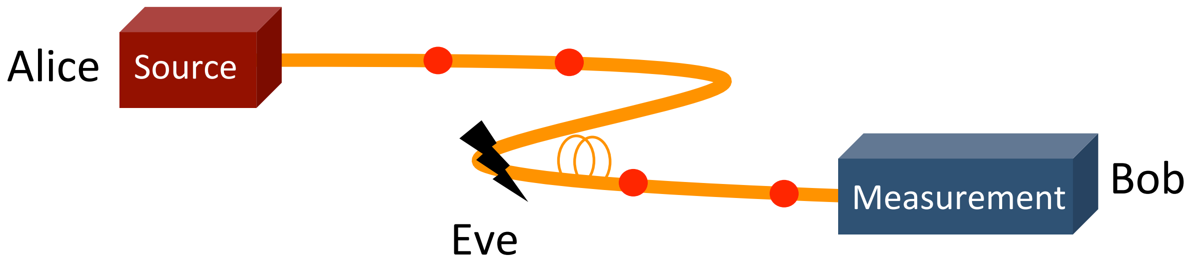
Collaborators:
Yuichi Nagamastu[1], Marcos Curty[2], Hoi-Kwong Lo[3], Koji Azuma[4], Rikizo Ikuta[1], Takashi Yamamoto[1], Nobuyuki Imoto[1], Kiyoshi Tamaki[4]

[1]*Osaka University*
[2]*University of Vigo*
[3]*University of Toronto*
[4]*NTT Basic Research Laboratories*

Practical security of QKD

➢ **The security of most existing implementations of QKD has not been rigorously established yet. Why?**

➡ Security proofs so far make ideal assumptions on the users' devices.



Source imperfections

Realistic imperfections, even major imperfections such as **modulation errors**, are not taken into account in most of security proofs.

Detector blinding attacks

L. Lydersen *et al*., Nat. Photonics **4**, 686 (2010).

Time-shift attacks

Y. Zhao et al., Phys. Rev. A **78**, 042333 (2008).

Detector control

I. Gerhardt *et al,* Nat. Commun. **2**, 349 (2011).

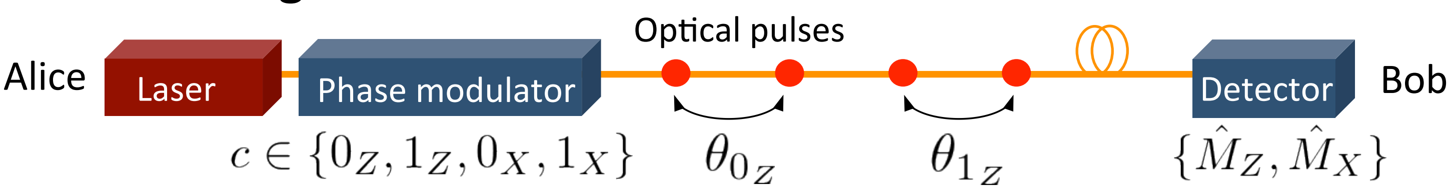
➡ Measurement-device-independent (MDI) QKD

H. K. Lo *et al,* Phys. Rev. Lett. **108**, 130503(2012).

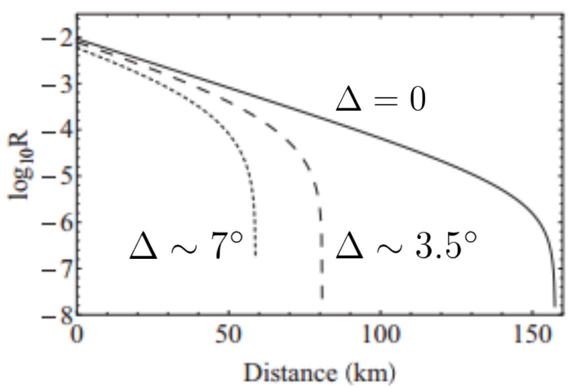
GLLP security proof

- **Phase-encoding BB84**

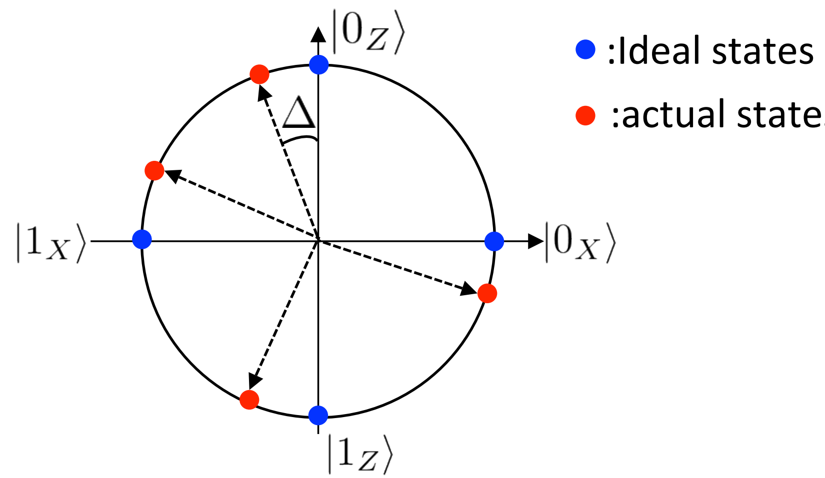
D. Gottesman *et al.*, Quant. Inf. Comput. **4**, 325 (2004).



<u>GLLP analysis</u>



<u>Qubit space of 2 consecutive pulses</u>

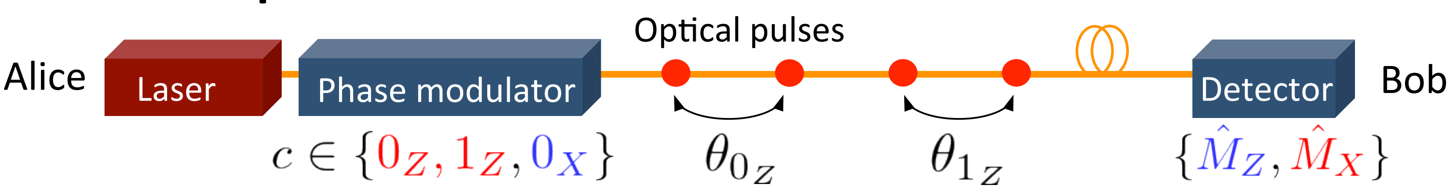


Even under the small phase modulation errors, the achievable distance and the key rate drastically decrease.

Loss-tolerant protocol

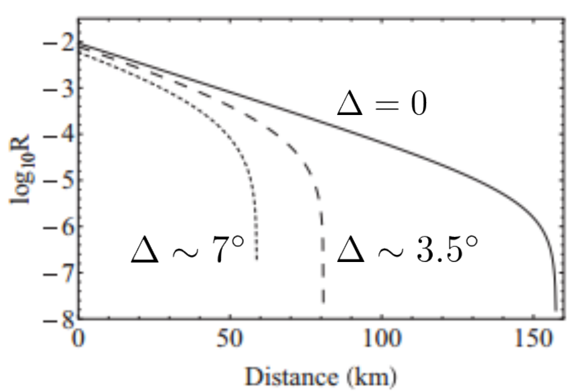
- **Loss-tolerant protocol**

K. Tamaki *et al*., Phys. Rev. A **90**, 052314 (2014).

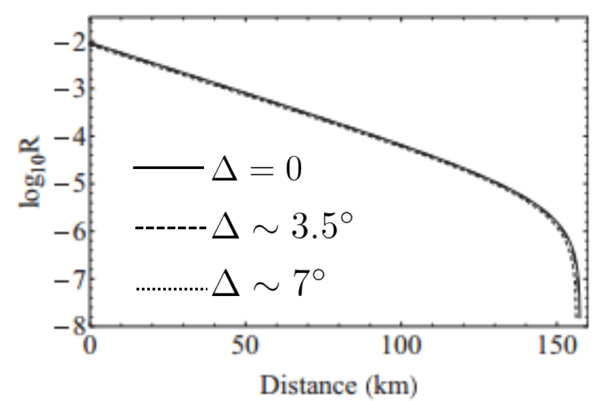


The main idea:
Utilizing the "basis mismatched events" to estimate Eve's leaked information.

GLLP analysis



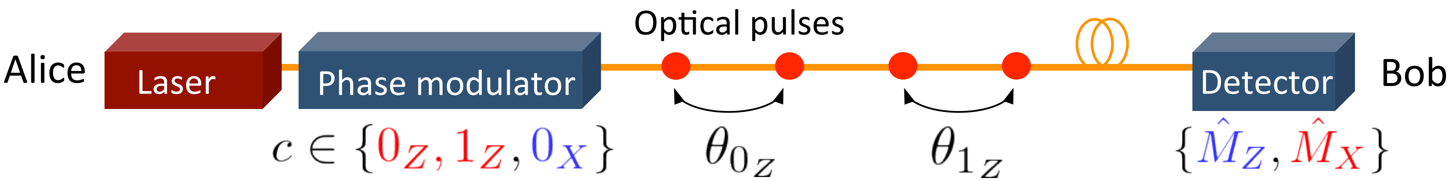
Loss-tolerant protocol



Loss-tolerant protocol

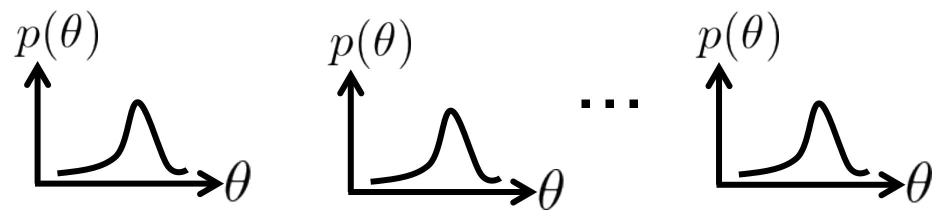
- **Loss-tolerant protocol**

K. Tamaki *et al*., Phys. Rev. A **90**, 052314 (2014).



The LT protocol assumes that the phase modulation errors follow **IID**.

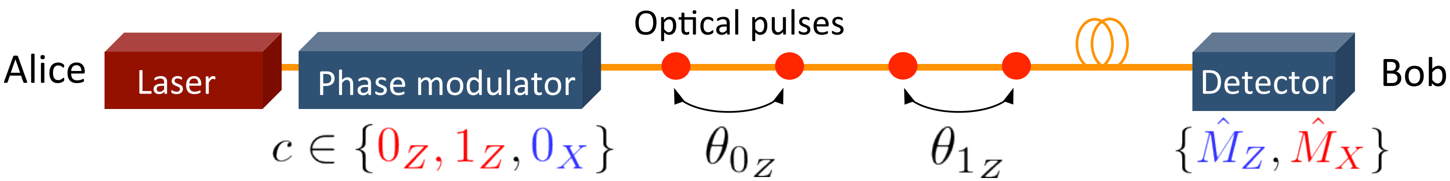
IID distribution on modulation device



Loss-tolerant protocol

- **Loss-tolerant protocol**

K. Tamaki *et al*., Phys. Rev. A **90**, 052314 (2014).



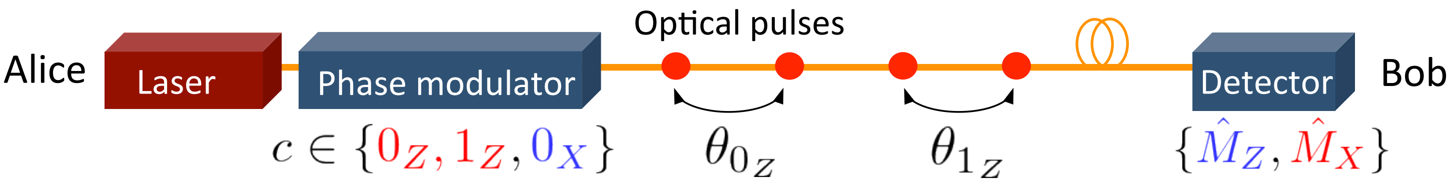
The LT protocol assumes that the phase modulation errors follow IID.

Hard or even impossible to confirm in the experiment.

Loss-tolerant protocol

- **Loss-tolerant protocol**

K. Tamaki *et al*., Phys. Rev. A **90**, 052314 (2014).



The LT protocol assumes that the phase modulation errors follow IID.

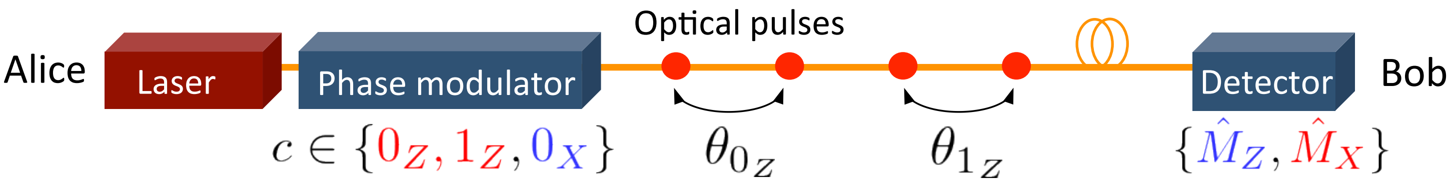
Hard or even impossible to confirm in the experiment.

We need more relaxed assumptions on the source.

Loss-tolerant protocol

- **Loss-tolerant protocol**

K. Tamaki *et al.*, Phys. Rev. A **90**, 052314 (2014).



The LT protocol assumes that the phase modulation errors follow IID.

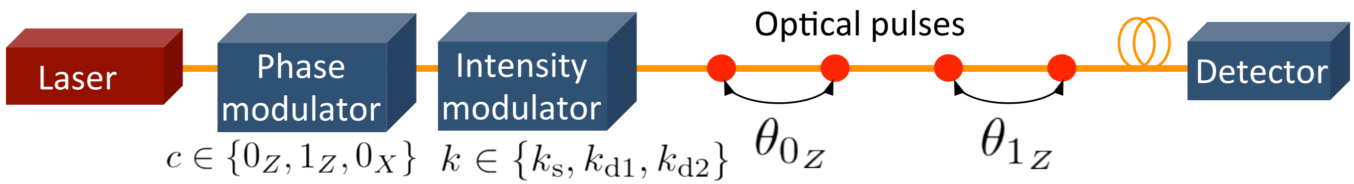
Hard or even impossible to confirm in the experiment.

We need more relaxed assumptions on the source.

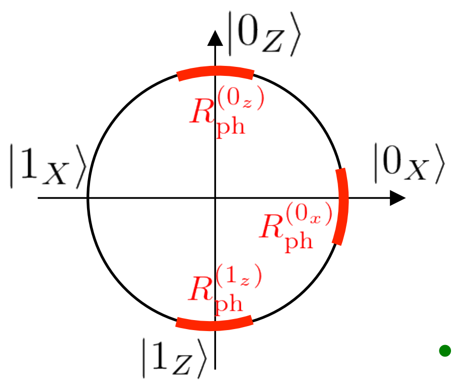
Towards secure QKD with testable assumptions on modulation devices (see arXiv soon!)

Characterization of modulation devices

- **Loss-tolerant protocol**



Phase modulator:



All the pulses emitted with c

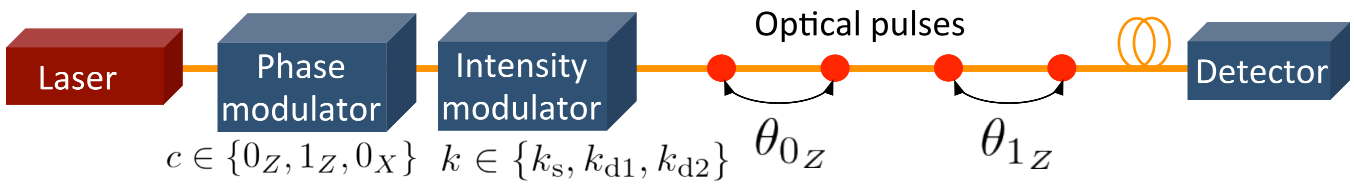
$$\Pr\left[\left|\{i_c|\theta_{i_c} \in R_\mathrm{ph}^{(c)}\}\right| \geq N_c - \delta_c\right] \geq 1 - \epsilon_c$$

Phase interval | Tagged pulses | Failure probability

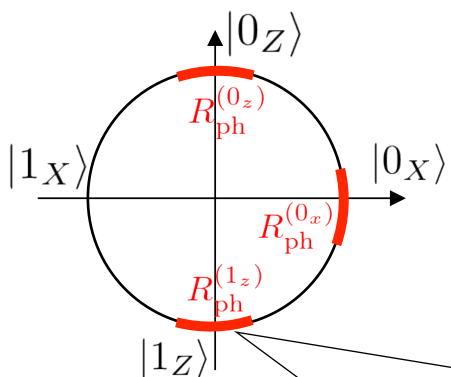
- Untagged signal: Pulse whose phase lies in the interval
- Tagged signal: Pulse whose phase does not lie in the interval

Characterization of modulation devices

- **Loss-tolerant protocol**



Phase modulator:



$$\Pr\left[|\{i_c|\theta_{i_c} \in R_{\rm ph}^{(c)}\}| \geq N_c - \delta_c\right] \geq 1 - \epsilon_c$$

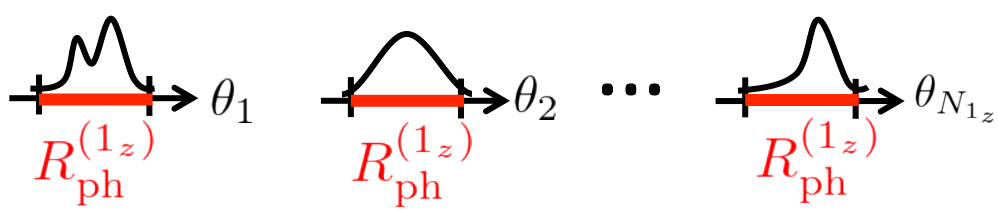
All the pulses emitted with c (N_c)

Phase interval ($R_{\rm ph}^{(c)}$)

Tagged pulses (δ_c)

Failure probability (ϵ_c)

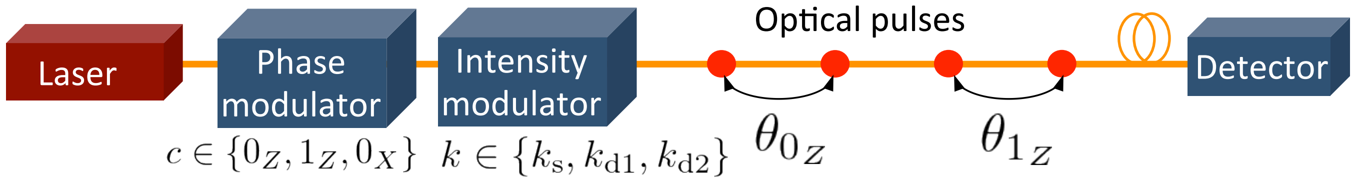
- Non-IID modulation errors are accommodated.



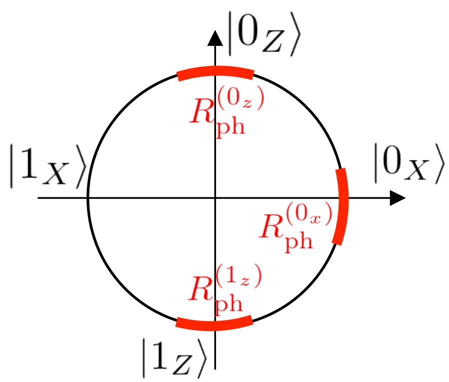
- Intervals are potentially testable in experiments.

Characterization of modulation devices

- **Loss-tolerant protocol**



Phase modulator:

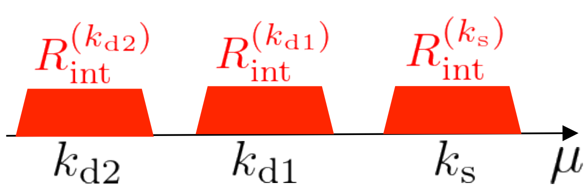


All the pulses emitted with c

$$\Pr\left[|\{i_c|\theta_{i_c} \in R_{\rm ph}^{(c)}\}| \geq N_c - \delta_c\right] \geq 1 - \epsilon_c$$

Phase interval | Tagged pulses | Failure probability

Intensity modulator:



All the pulses emitted with k

$$\Pr\left[|\{i_k|\mu_{i_k} \in R_{\rm int}^{(k)}\}| \geq N_k - \delta_k\right] \geq 1 - \epsilon_k$$

Intensity interval | Tagged pulses | Failure probability

- Tagged events occur independently of k

Simulation results

Finite-key length

see arXiv soon!

- **Secure key length against coherent attacks:**

$$\ell \geq S_1^{\mathrm{u}}\Big(1 - h(e_{\mathrm{ph}}^{\mathrm{u}})\Big) - \lambda_{\mathrm{EC}}$$

Number of Z-basis detected events from untagged single-photon emissions

Leaked information for the untagged single-photon emissions

Bits exchanged in reconciliation

- **Estimation for the parameters:**

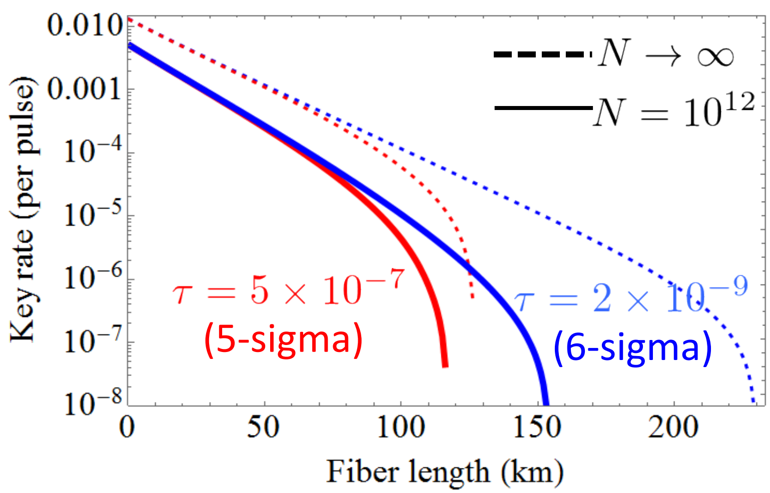
M. Curty *et al*., Nat. Commun., **5**, 3732 (2014).

S_1^{u} : Extend the "decoy-state method" based on our intensity interval assumption.

$e_{\mathrm{ph}}^{\mathrm{u}} := \frac{N_{\mathrm{ph}}^{\mathrm{u}}}{S_1^{\mathrm{u}}}$: Phase error rate for the untagged single photon emissions among the Z-basis untagged single-photon emissions.

Key rate against distance

- **Key rate**=key length per signal transmission.
- Secrecy parameter $\epsilon_{\mathrm{s}} = 10^{-10}$
- Correctness $\epsilon_{\mathrm{cor}} = 10^{-10}$
- Loss in the optical fiber=0.2dB/km
- Detection efficiency=46%, dark count=1.5×10^{-8} Y-L. Tang *et al.*, Phys. Rev. Lett. **113**, 190501 (2014).



Modulation devices

Phase interval: F. Xu *et al.*, PRA **92**, 032305 (2015).

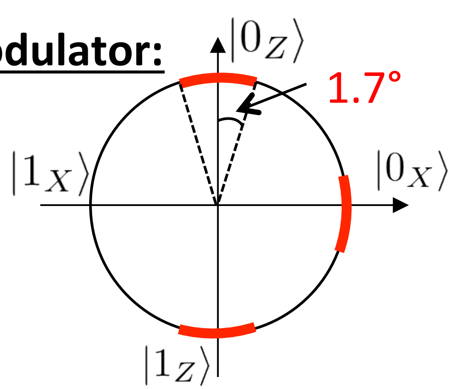
$$R_{\mathrm{ph}} = [\theta_c - 1.7°, \theta_c + 1.7°]$$

Intensity interval (±3%):

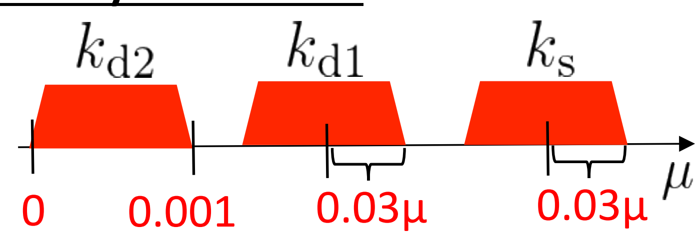
$$R_{\mathrm{int}} = [\mu(1-0.03), \mu(1+0.03)]$$

τ=Probability (per pulse) of being outside the interval

Phase modulator:

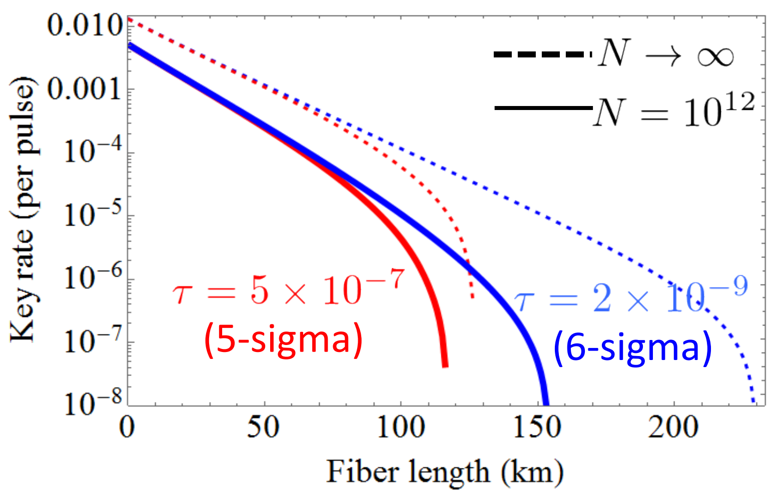


Intensity modulator:



Key rate against distance

- **Key rate**=key length per signal transmission.
- Secrecy parameter $\epsilon_{\mathrm{s}} = 10^{-10}$
- Correctness $\epsilon_{\mathrm{cor}} = 10^{-10}$
- Loss in the optical fiber=0.2dB/km
- Detection efficiency=46%, dark count=1.5×10^{-8} Y-L. Tang *et al.*, Phys. Rev. Lett. **113**, 190501 (2014).



Modulation devices

Phase interval: F. Xu *et al.*, PRA **92**, 032305 (2015).

$$R_{\mathrm{ph}} = [\theta_c - 1.7°, \theta_c + 1.7°]$$

Intensity interval (±3%):

$$R_{\mathrm{int}} = [\mu(1 - 0.03), \mu(1 + 0.03)]$$

τ =Probability (per pulse) of being outside the interval

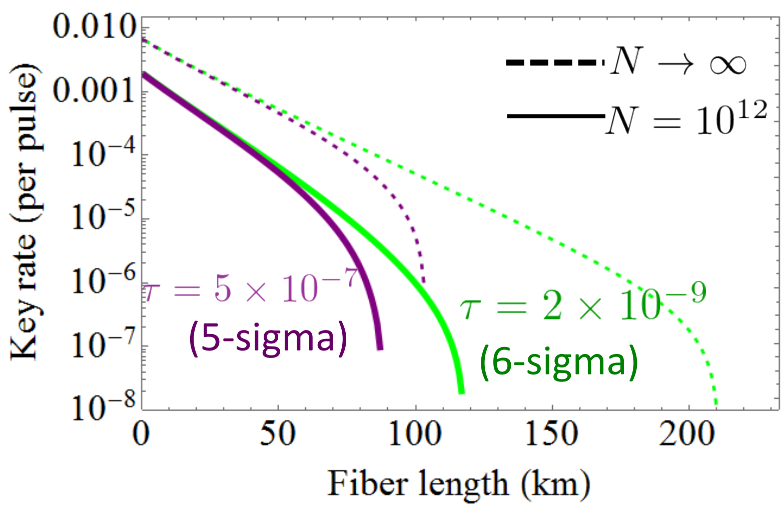
Notice

1) If τ increases, the number of pulses that do not lie within the intervals also increases. The *tagged signals* become problematic especially in the *high loss regime*.

2) If the intervals are guaranteed by 5-sigma confidence level, more than 100km secure QKD is possible within reasonable number of signal transmissions.

Key rate against distance

- **Key rate**=key length per signal transmission.
- Secrecy parameter $\epsilon_{\mathrm{s}} = 10^{-10}$
- Correctness $\epsilon_{\mathrm{cor}} = 10^{-10}$
- Loss in the optical fiber=0.2dB/km
- Detection efficiency=46%, dark count= 1.5×10^{-8} Y-L. Tang *et al.*, Phys. Rev. Lett. **113**, 190501 (2014).



Modulation devices

Phase interval: F. Xu *et al.,* PRA **92**, 032305 (2015).

$$R_{\mathrm{ph}} = [\theta_c - 1.7^\circ, \theta_c + 1.7^\circ]$$

Intensity interval (±5%):

$$R_{\mathrm{int}} = [\mu(1-0.05), \mu(1+0.05)]$$

τ =Probability (per pulse) of being outside the interval

Notice

Even if we assume ±5% intensity fluctuations with guaranteeing the 5-sigma confidence level, secure QKD over about 90 km is possible with a reasonable number of signal transmissions.

Conclusions & Outlook

- **Device characterizations on modulation devices:**
  1. Remove the **IID assumption**.
  2. **Intervals** are the sufficient condition and **no detailed characterization is needed**, such as an error distribution and the independence among the actual phases and intensities.

- **High performance:**
  Long distant secure QKD is possible up to (with $N = 10^{12}$ pulse emissions)

$$\ell \sim 90\mathrm{km}$$

  with realistic assumptions on the modulation devices of

  $\pm 5\%$ intensity and $\pm 1.7^\circ$ phase intervals.

- **Experimental scheme for the characterization:**
  How to guarantee the phase and intensity intervals are important future works.

- **Application to another QKD setting:**
  To apply our theory to another setting, say the MDI setting.