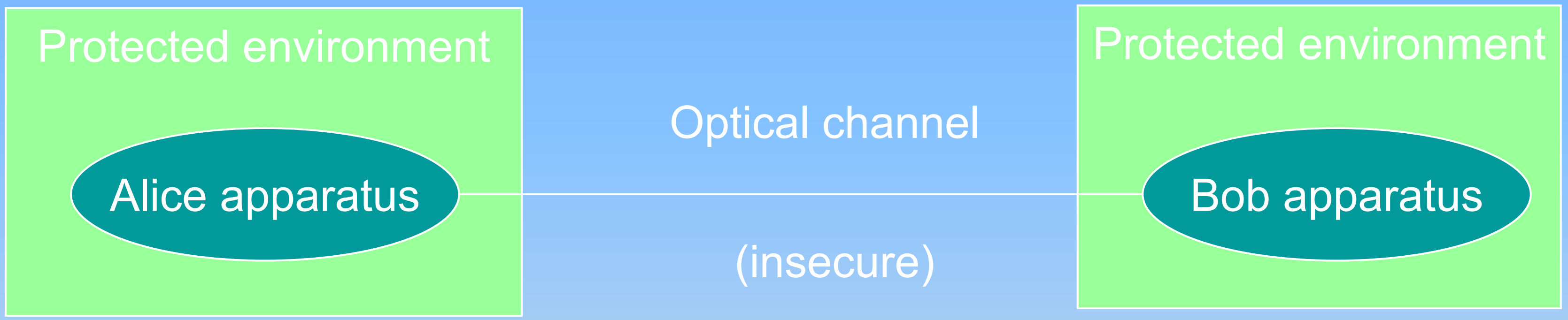
Practical aspects of QKD security

Alexei Trifonov
Audrius Berzanskis
MagiQ Technologies, Inc.

Secure quantum communication



Quantum cryptographic apparatus is located in the secure environment

The task for the quantum cryptography is to protect the channel from the eavesdropping

$$\text{Quantum Cryptography} \in \text{Cryptography} \in \text{Security}$$

Mutual information, key distillation criterion

$$I(A,B) = 1 + \varepsilon \log_2 \varepsilon + (1-\varepsilon)\log_2(1-\varepsilon)$$

Bob information gain, ε - quantum bit error rate

$$I(A,E) = 1 + \xi \log_2 \xi + (1-\xi)\log_2(1-\xi)$$

Eve information gain by Eve, ξ - error rate by Eve

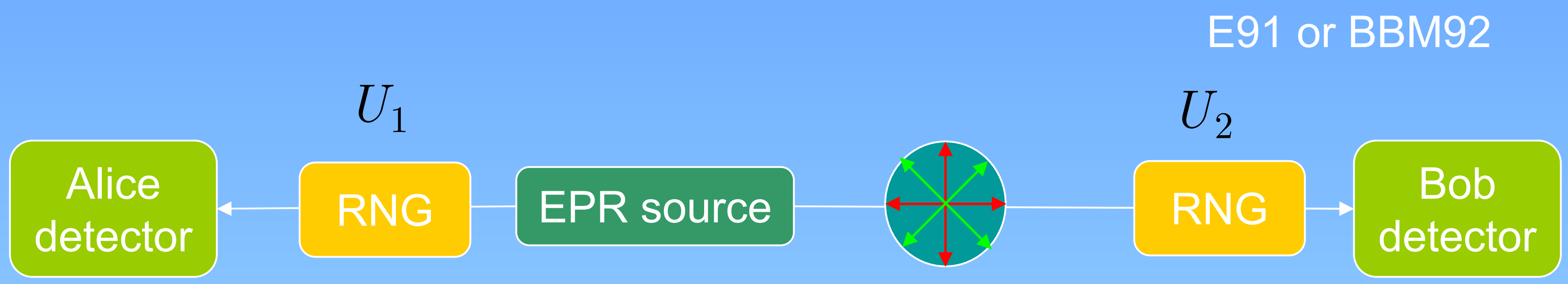
$$S(A,B \,||\, E) \geq \max\left(I(A,B) - I(A,E), I(A,B) - I(B,E)\right)$$

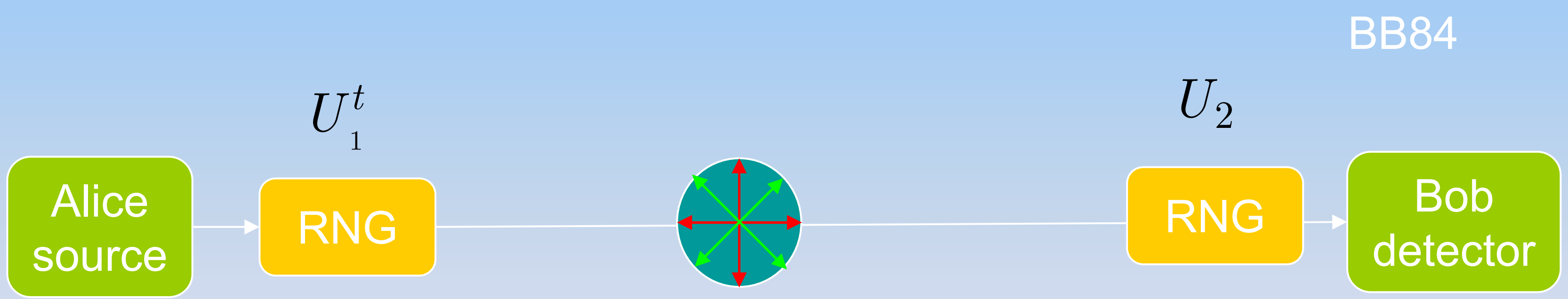
IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-24, NO. 3, MAY 1978 339

Broadcast Channels with Confidential Messages

IMRE CSISZÁR AND JÁNOS KÖRNER

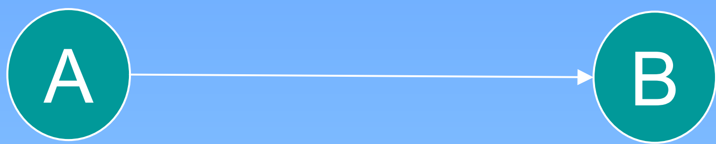
Quantum channel





$$U_1 \otimes U_2 \Phi^{(+)} = \mathbf{1} \otimes U_2 U_1^t \Phi^{(+)}$$

State estimation



State distinguishability

$$D \leq \| \rho_+ - \rho_- \|$$

$$D = \sqrt{1 - p_+ p_- |\langle \psi_+ | \psi_- \rangle|^2}$$

Helstrom bound

Likelihood of guessing correctly

$$L = \max\{w_+, w_-\} = \frac{1+D}{2}$$

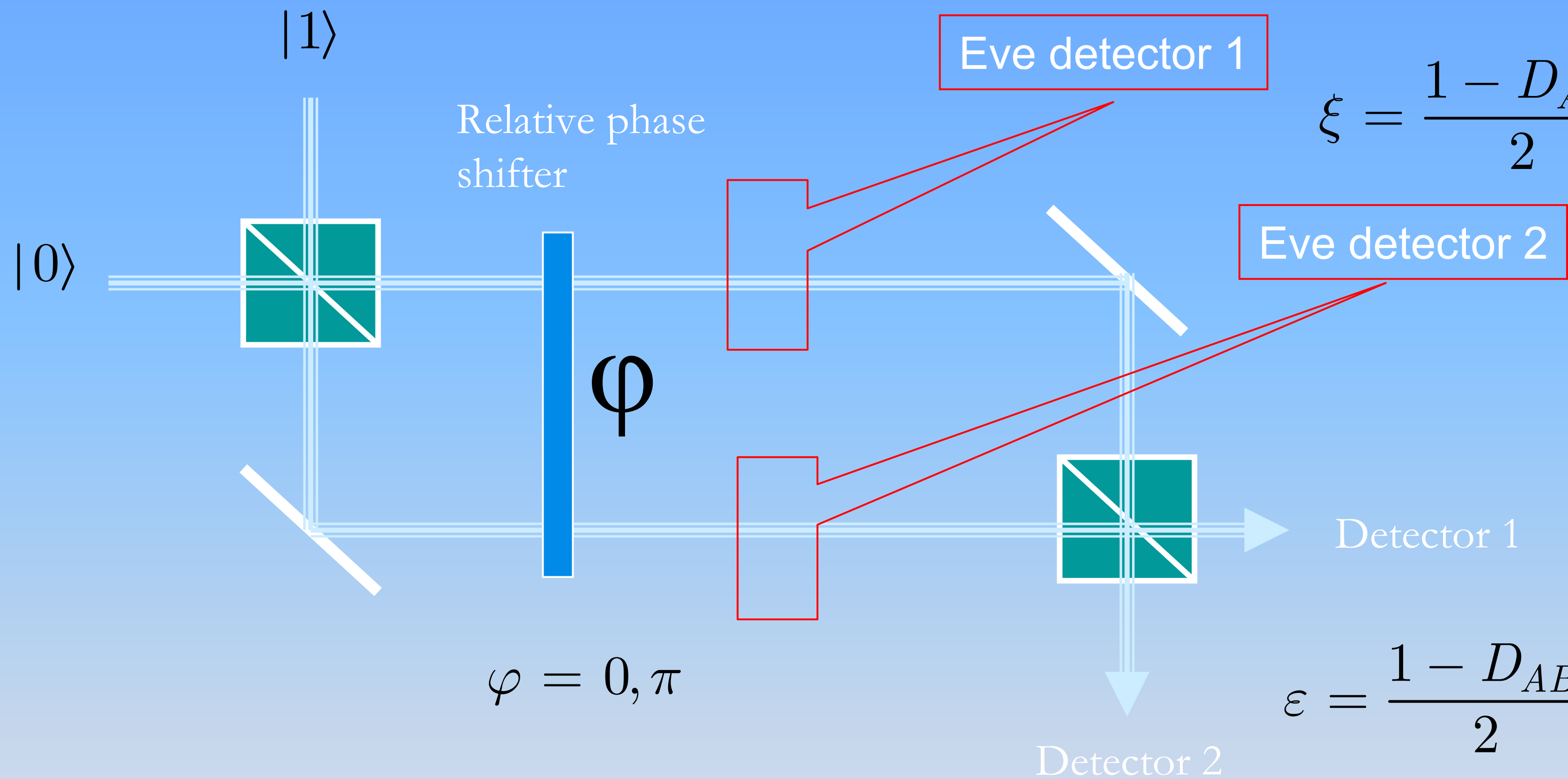
Likelihood of error

$$\varepsilon = 1 - L = \frac{1-D}{2}$$

Mutual information

$$I(A,B) = 1 + \varepsilon \log_2 \varepsilon + (1-\varepsilon)\log_2(1-\varepsilon)$$

Mach-Zehnder interferometer



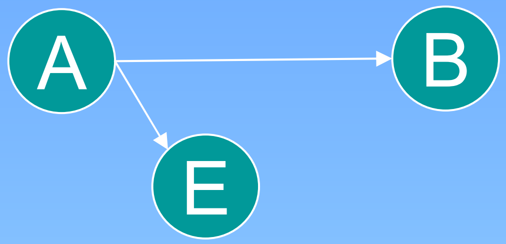
$\varphi = 0, \pi$

$$\xi = \frac{1 - D_{AE}}{2}$$

$$\varepsilon = \frac{1 - D_{AB}}{2}$$

$$D_{AB} = V$$

Complementarity relations



Error rates

$$\varepsilon = \frac{1-V}{2}$$ Bob

$$\xi = \frac{1-D}{2}$$ Alice

The main task is to break
the symmetry in mutual information
Quantum physics provides us with solution

$$D^2 + V^2 \leq 1$$ Complementarity relation

Keeping V high enough we can make sure that $I(A,B) > \max\{I(A,E), I(B,E)\}$

$$I(A,B) = I(A,E) \rightarrow D = V \rightarrow \varepsilon = \xi = \frac{1-\sqrt{2}}{2} \approx 15\%$$

Error rate threshold
for key distribution

What is good about QKD?

- Does not depend on mathematical complexity or any type of unproven computational algorithm
- Works as intrusion detector
- Unclonable – leaves no copy of the information sent

What is bad about QKD?

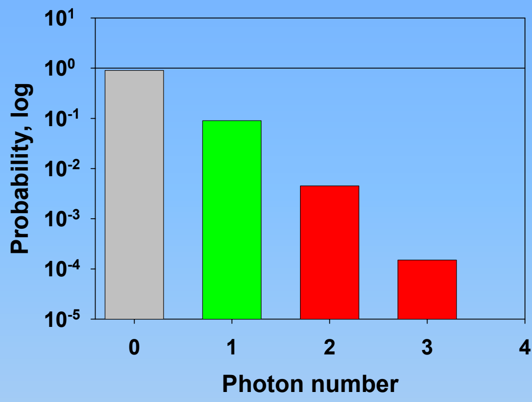
- Intrinsically based upon single photon interferometry – very sensitive to loss and decoherence
- Incompatible with optical amplifiers – distance limitation!
- Uses single photon counters – slow!

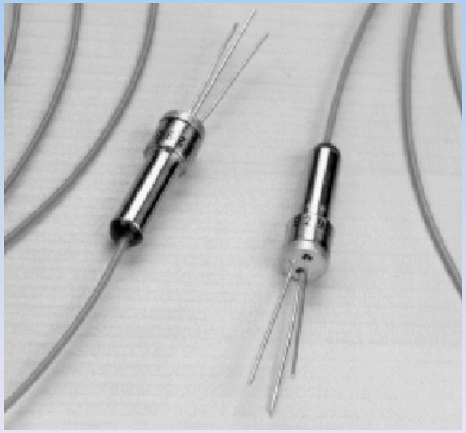
Major components affecting the performance of QKD system

- Source
  - Ideally – true single photon source
  - really – weak laser pulse, nonzero probability for more than one photon in a pulse
- Interferometer – visibility up to 30 dB is real
- Apparatus loss – progress in telecom made it simple!
- Fiber loss – typically 0.2- 0.3 dB/km, affects the rate and distance - beyond the control
- Detector quantum efficiency and dark current noise – rate and distance

The questions to the designer of the QKD system

- How to adjust average photon number?
- How to tune the performance of the single photon counter?





Outline detector problem

- The main parameters of the detector of interest
- Requirements from security of QKD system
- Real detector characterization
- Comparison of true single photon and weak coherent pulse QKD
- Summary

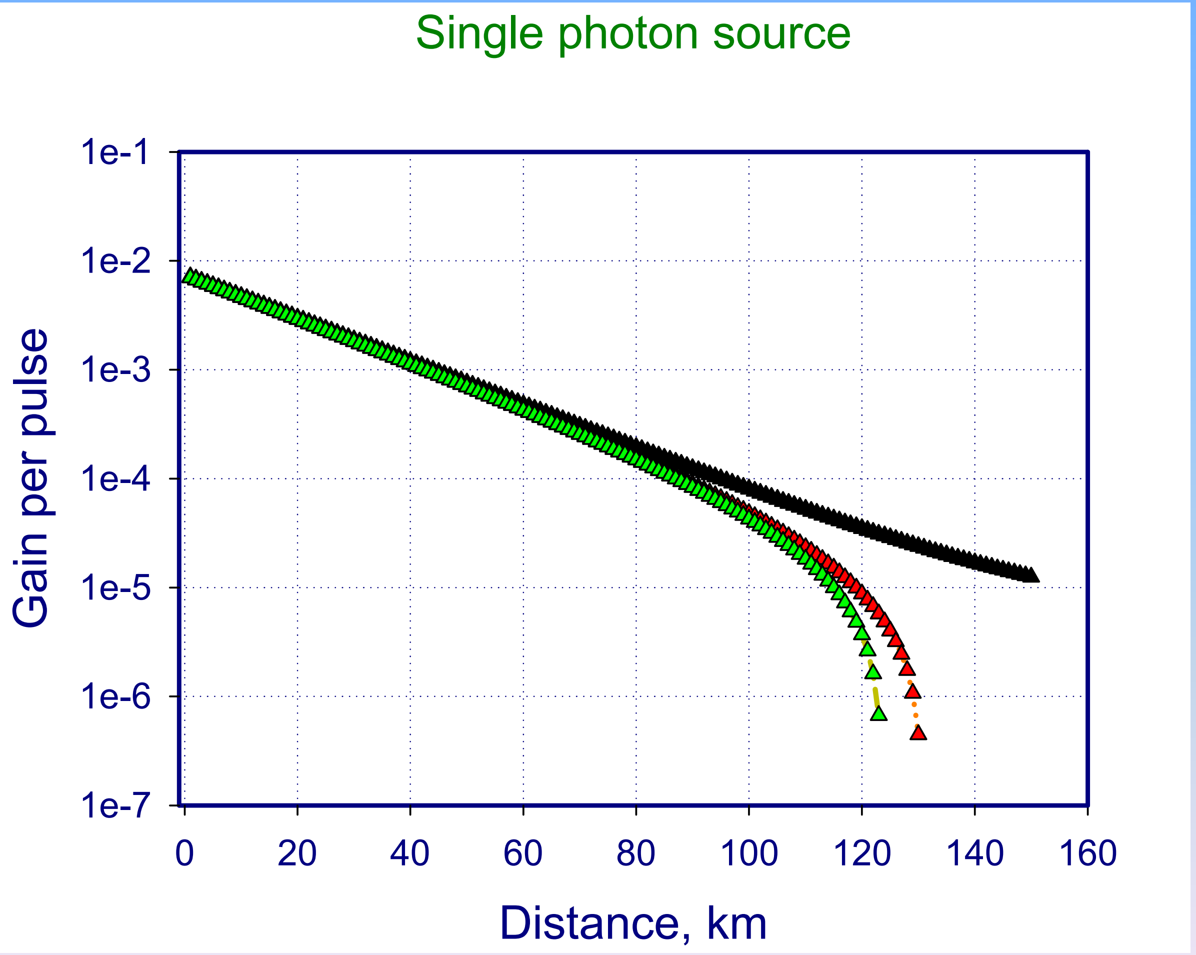
Detector problem

- Good silicon detector for the first telecom window 830nm or free-space QKD
- Second and third telecom window are much more transparent: typical losses are 2-3 dB/km for 830nm, 0.3-0.4 dB/km for 1310nm, and 0.2-0.3 dB/km for 1550nm.
- Long-haul system (10+ km) can be built only with 1310 or 1550, the later is preferable.
- Ge detector can be used only for 1310nm (cooling -> band gap shift).
- InGaAS detectors have huge afterpulsing -> decrease in capacity.
- Solution: careful detector selection, short pulse gating, plus electronic suppression of the gating pulses after the event.

Main parameters of the single photon detector

- Quantum efficiency – the probability of getting a response from a single quanta η
- Dark current probability - the probability of the false click p_{DC}
- The speed of “recharging” the detector – maximum rate
- Afterpulsing probability – the increase probability of getting a subsequent false click

Performance of the QKD system with true single photon source



Parameters

$\mu_B = 0.3$

$\eta = 10\%$

$p_{DC} = 10^{-5}$

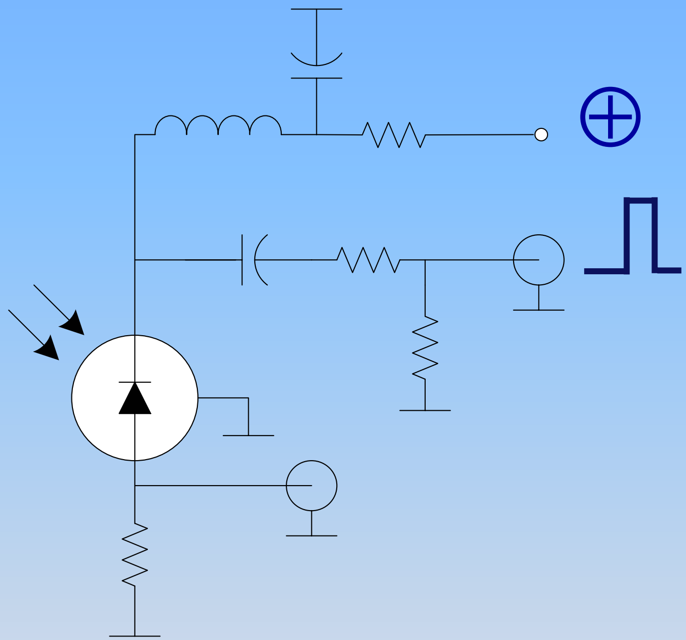
$\alpha = 0.2\ dB/km$

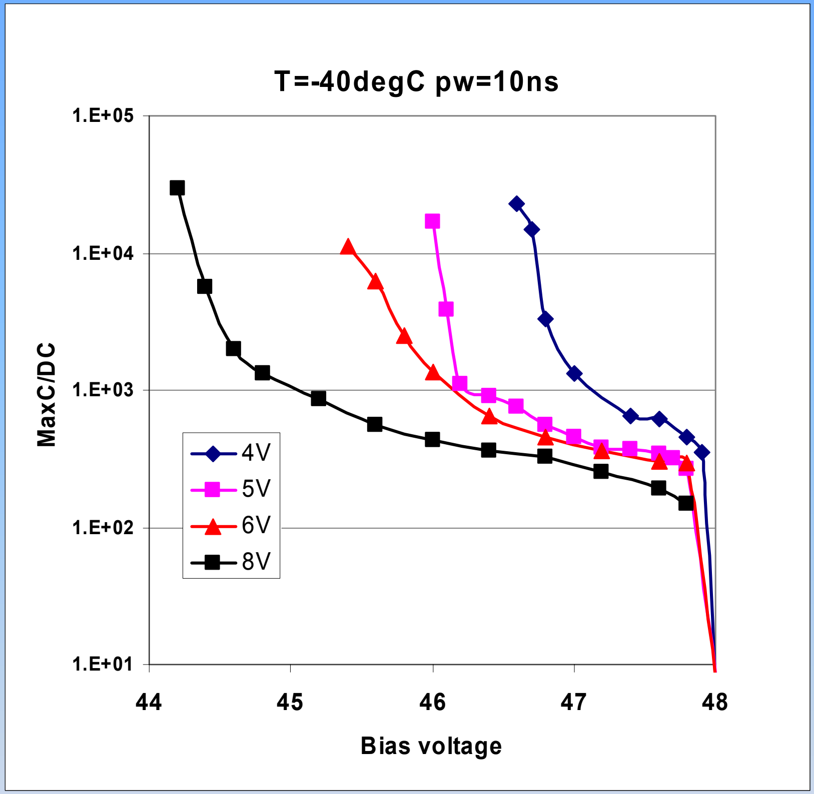
$\eta_B = 0.5$

Performance

- Dark current probability is high, solution – fast gating + cooling. Detector is below the breakthrough voltage and is gated above only within the time window containing the photon
- Parameters
  - Base voltage
  - Gate pulse width
  - Gate pulse amplitude
  - Working temperature

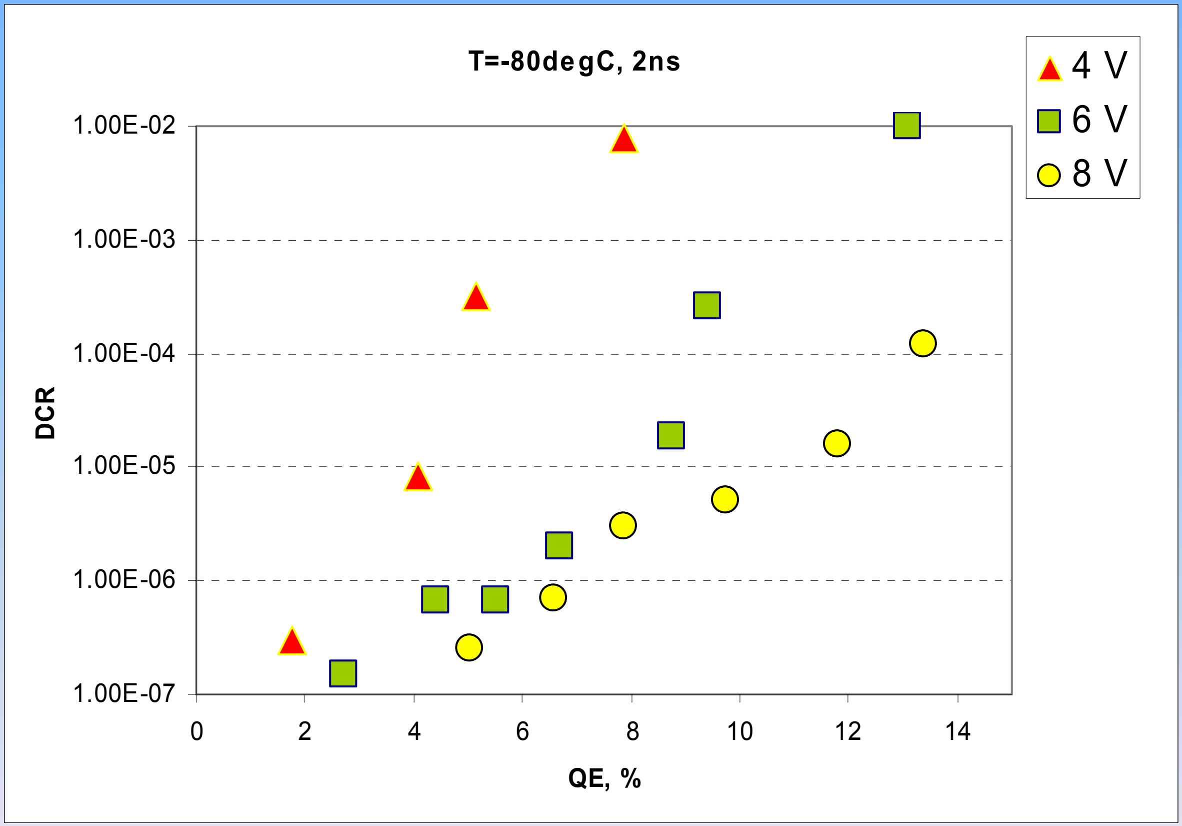
Detector performance



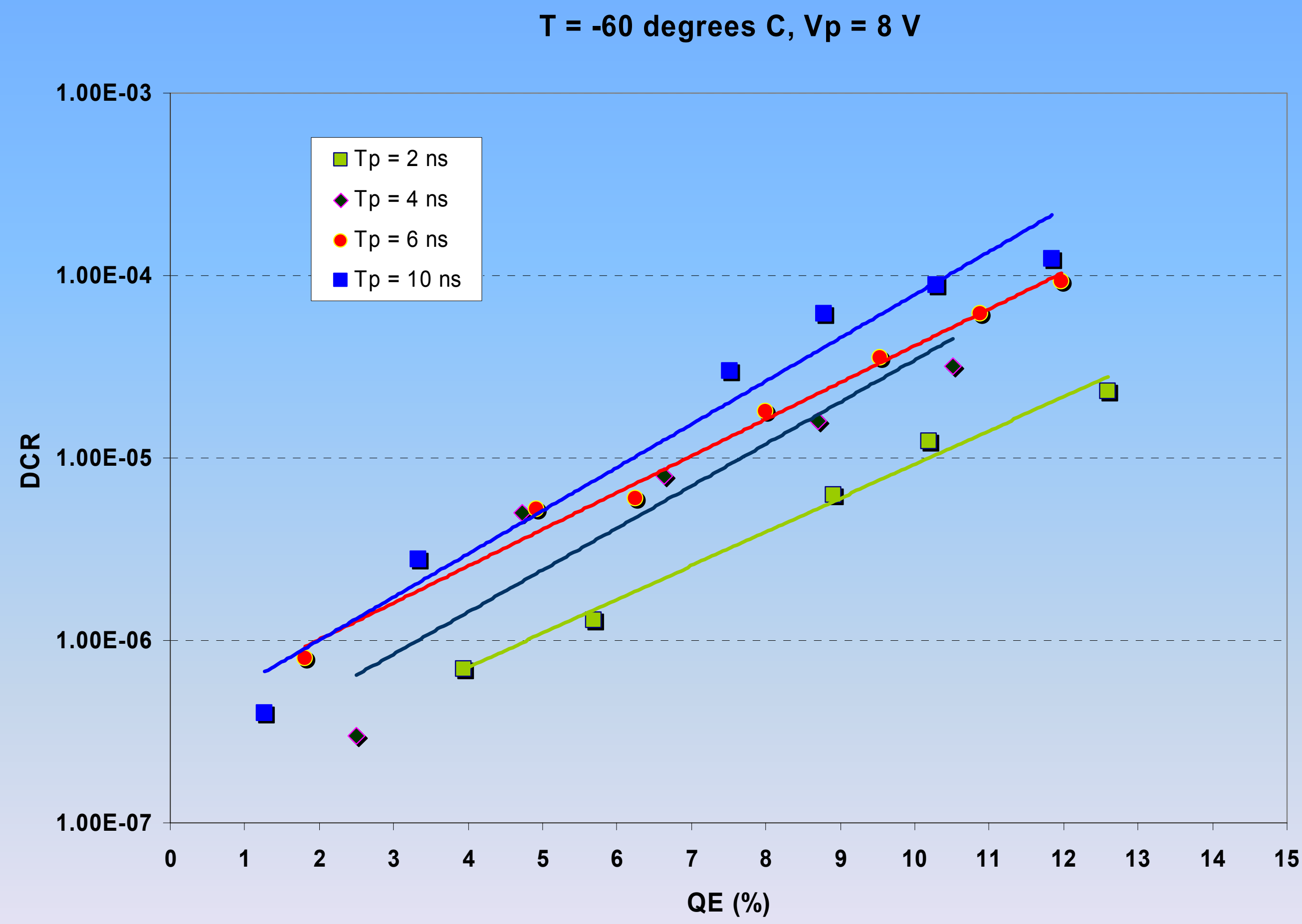


Ratio of Max Count/ Dark count vs Bias voltage for 10ns gating pulse

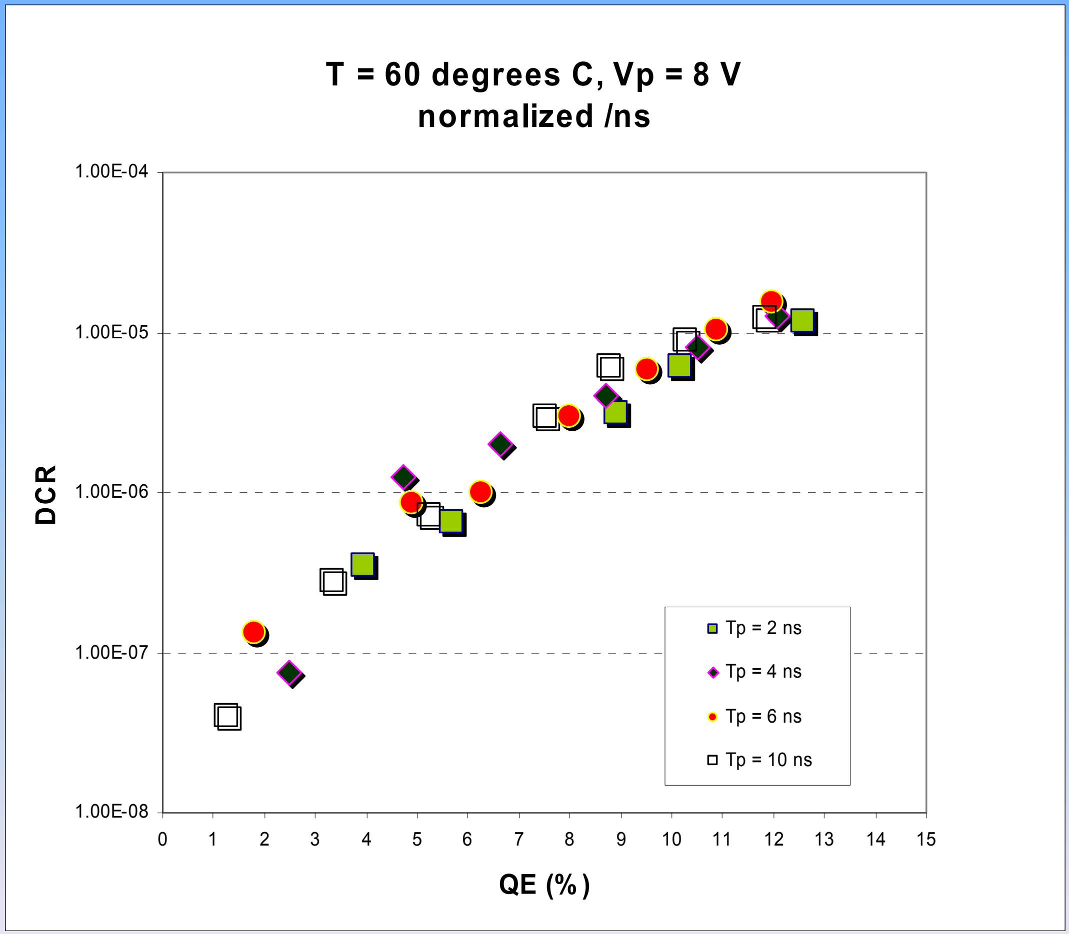
Gating Amplitude Dependence
-80deg C, Gating 2ns



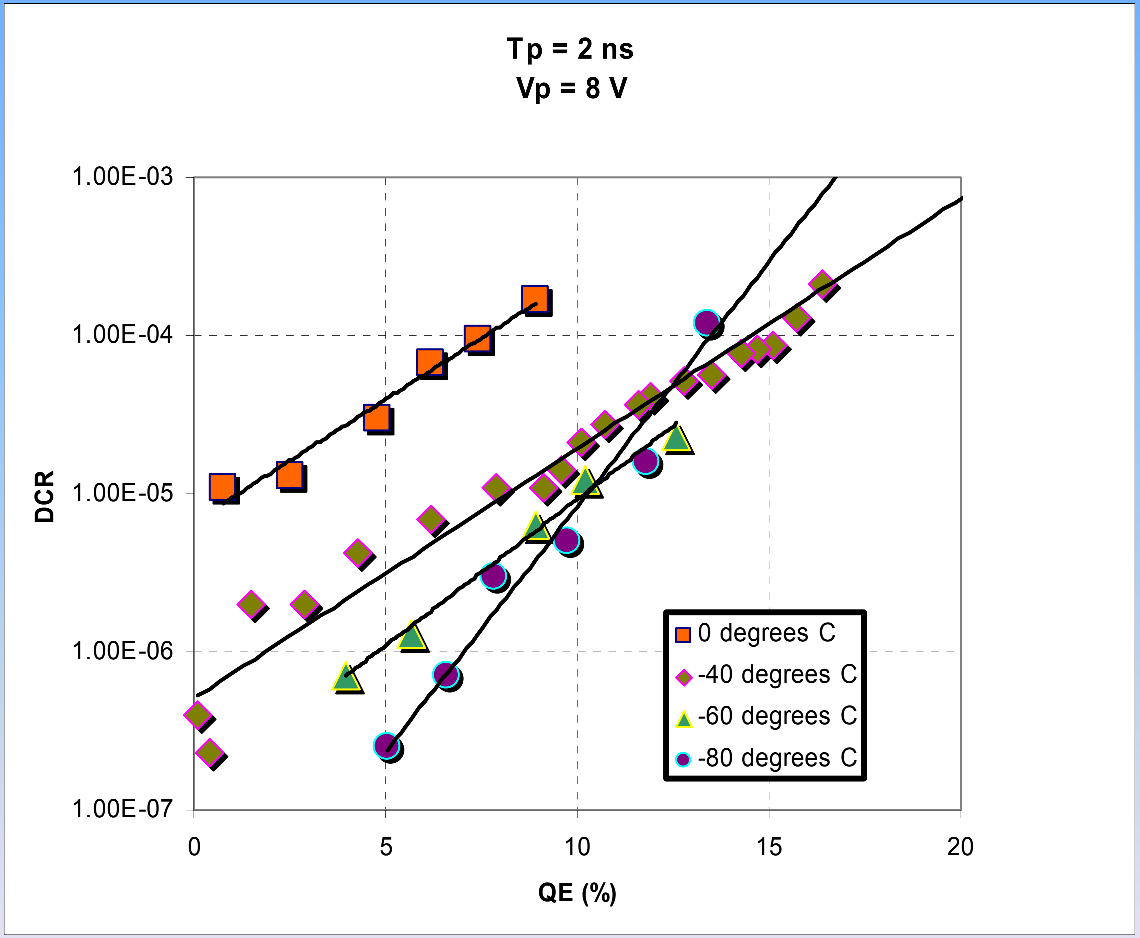
Gating Pulse Width Dependence
-60deg C, Gating amplitude 8V



Gating Pulse Width Dependence: normalized
-60deg C, Gating amplitude 8V



Temperature Dependence
Gating 2ns, 8V

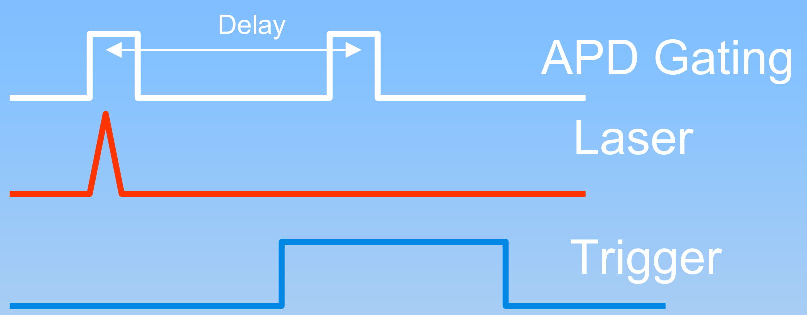


APD AfterPulsing Testing

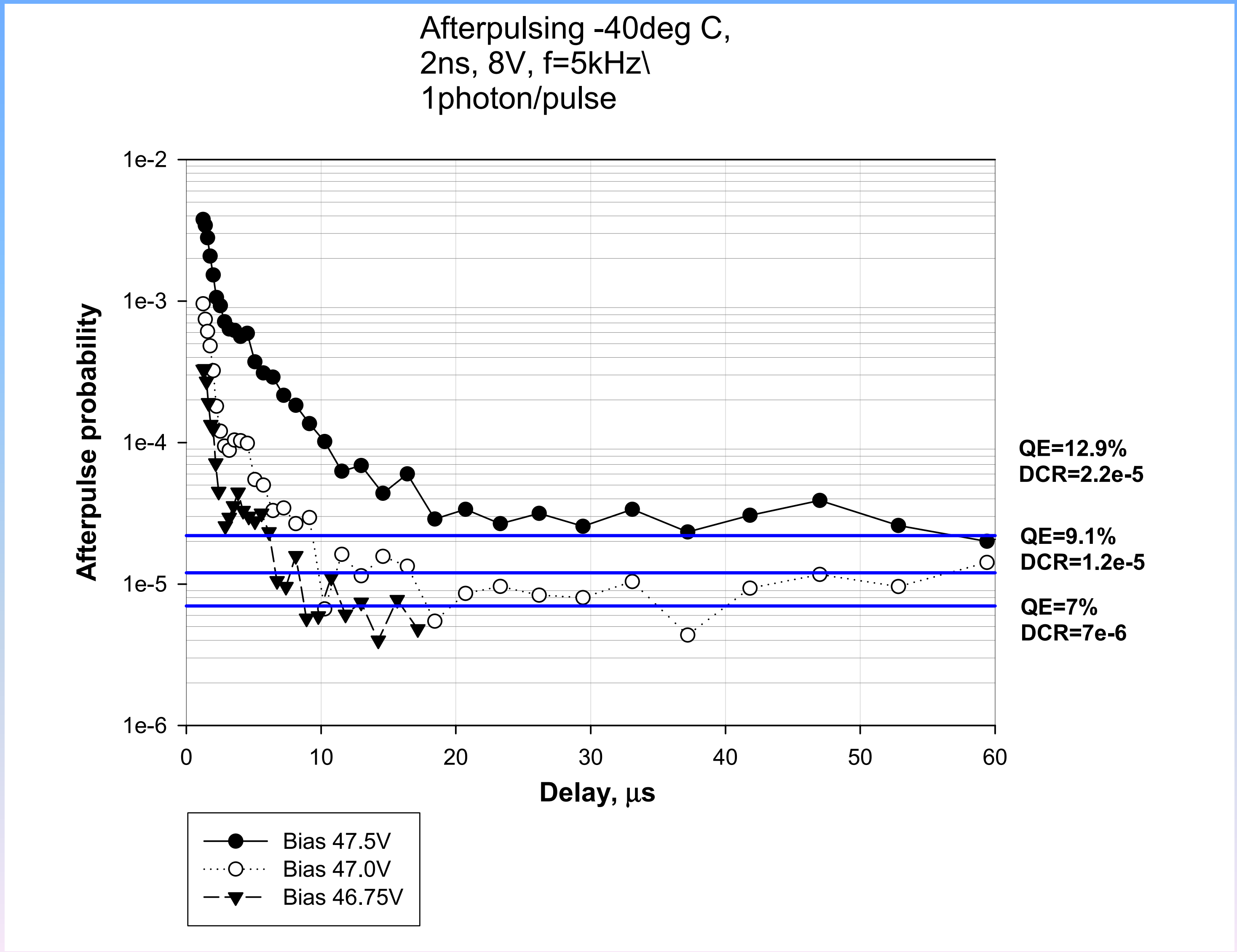
Parameters
V gate: 8V
T gate: 2ns
Temperature: -80 and -40 deg C

Laser λ=1553.4nm
P into APD =-122dBm
1photon/pulse (@5kHz)

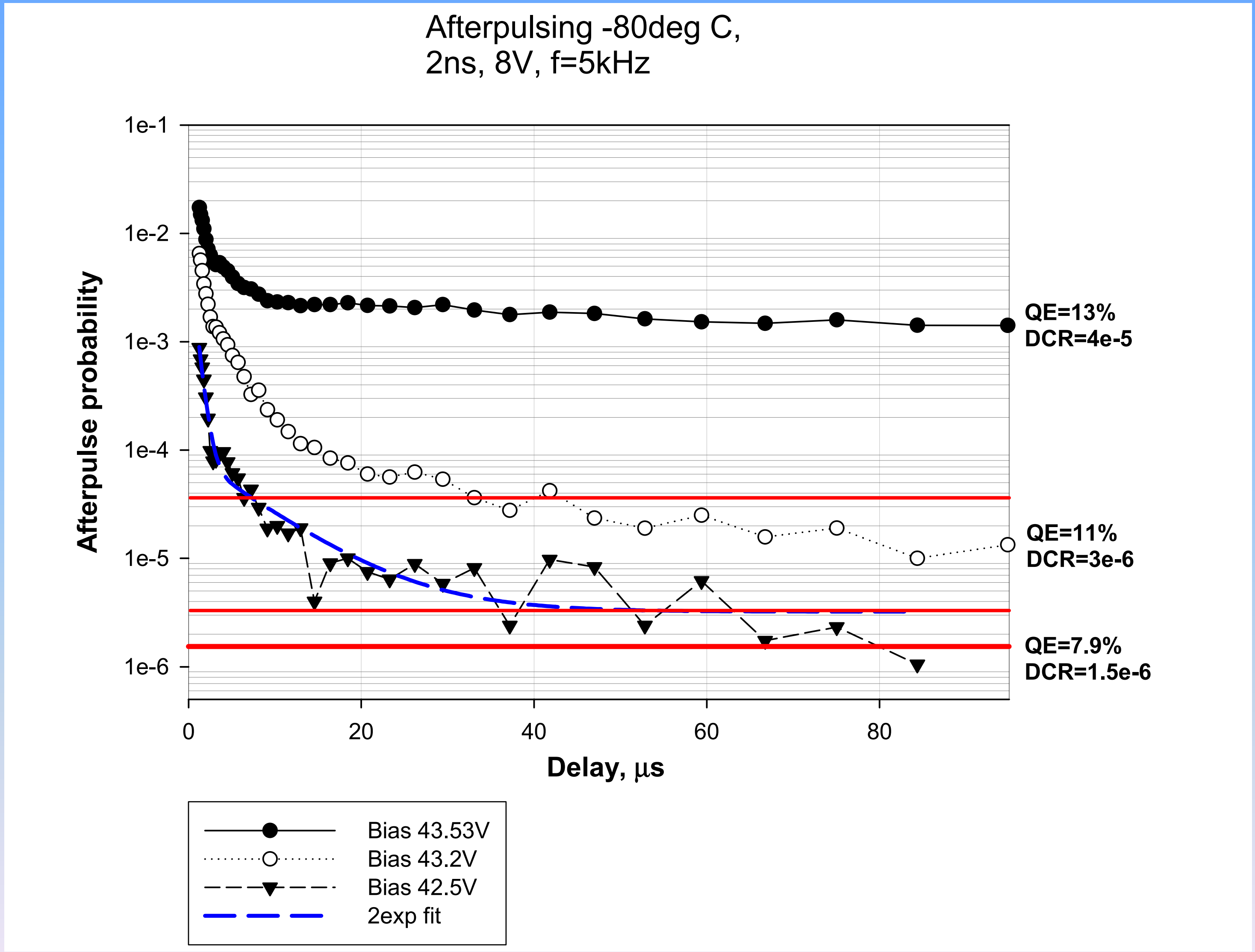
Discriminator trigger pulse 200ns



APD AfterPulsing Testing



APD AfterPulsing Testing



Conclusion – detector problem

- Both quantum efficiency and dark current are decreasing with cooling
- At the same time afterpulsing effect becomes significant at low temperature
- To maximize the system performance careful tweaking of the parameters must be done with respect to actual experimental conditions

Quantum Key Distribution: w/ Attempted Eavesdropper

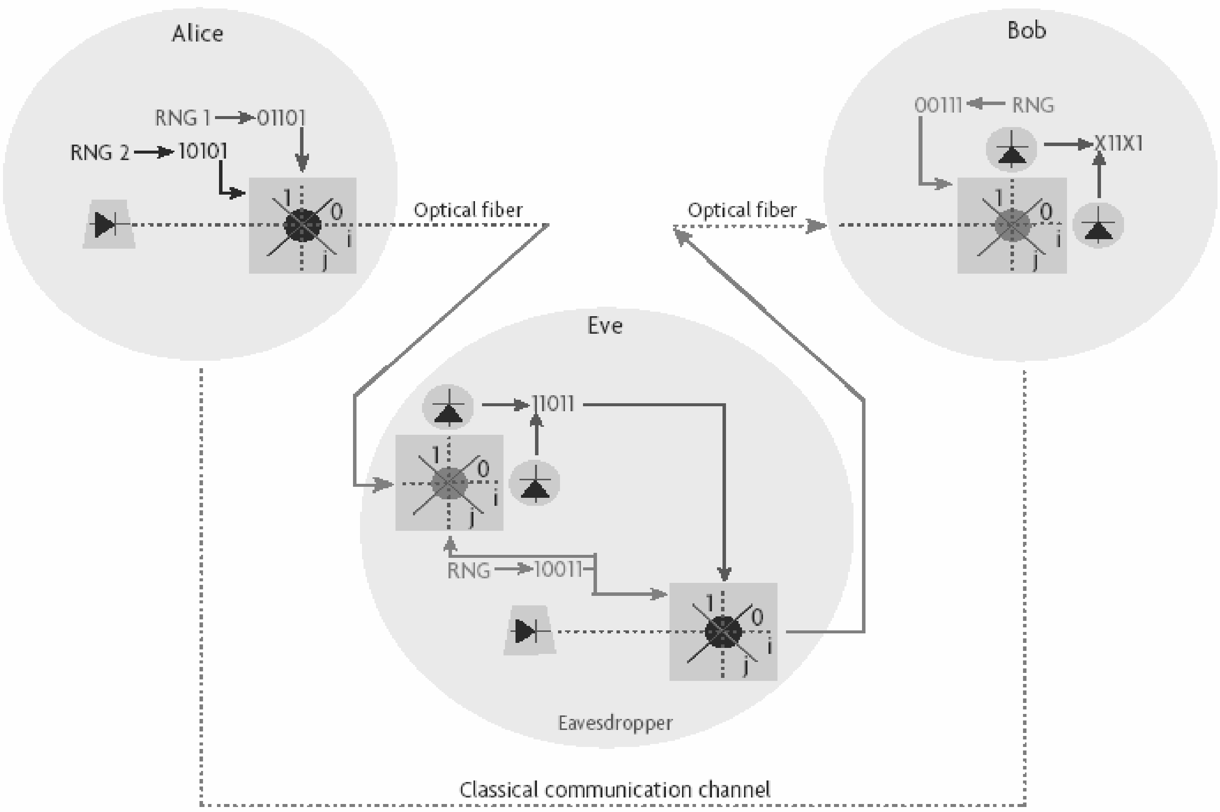


FIGURE 4: SCHEMATIC OF QKD SYSTEM WITH ATTEMPTED EAVESDROPPER

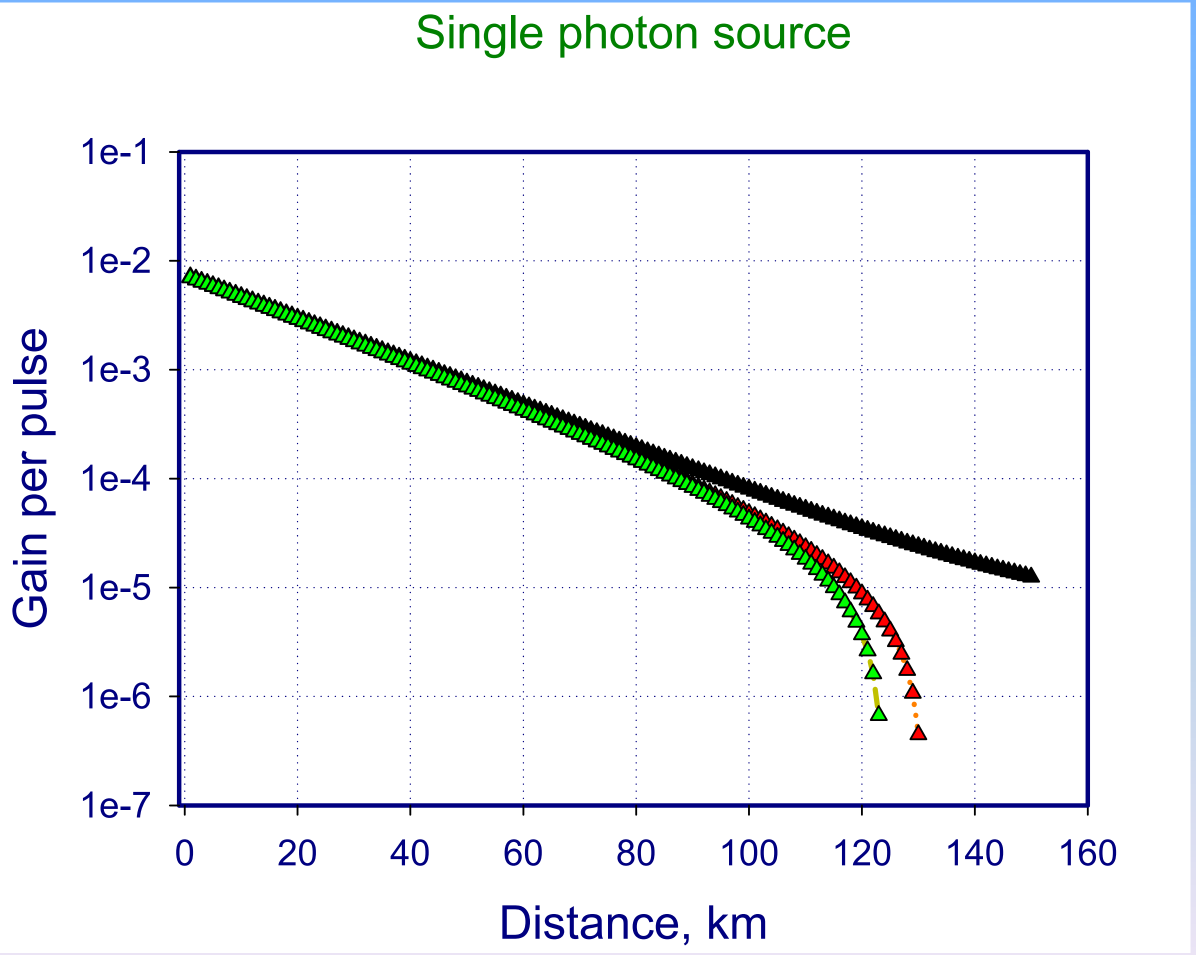
Algorithms

- Authentication
- Sifting $$p_{sift} = \frac{1}{2} p_{signal}$$
- Error correction $$H = -\varepsilon \log_2 \varepsilon - (1-\varepsilon) \log_2 (1-\varepsilon)$$
- Privacy amplification $$\tau = 1 + \log_2 \left(\frac{1}{2} + 2\varepsilon - 2\varepsilon^2 \right)$$
- Final key $$G = p_{sift} (1 - \tau - f \cdot H)$$

ε - quantum bit error rate

H - Shannon entropy

Performance of the QKD system with true single photon source



Parameters

$$\mu_B = 0.3$$

$$\eta = 10\%$$

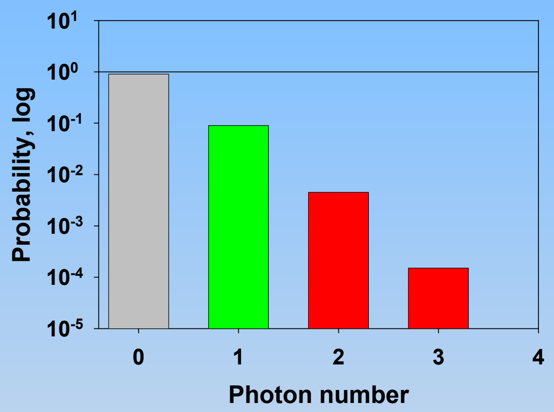
$$p_{DC} = 10^{-5}$$

$$\alpha = 0.2\ dB/km$$

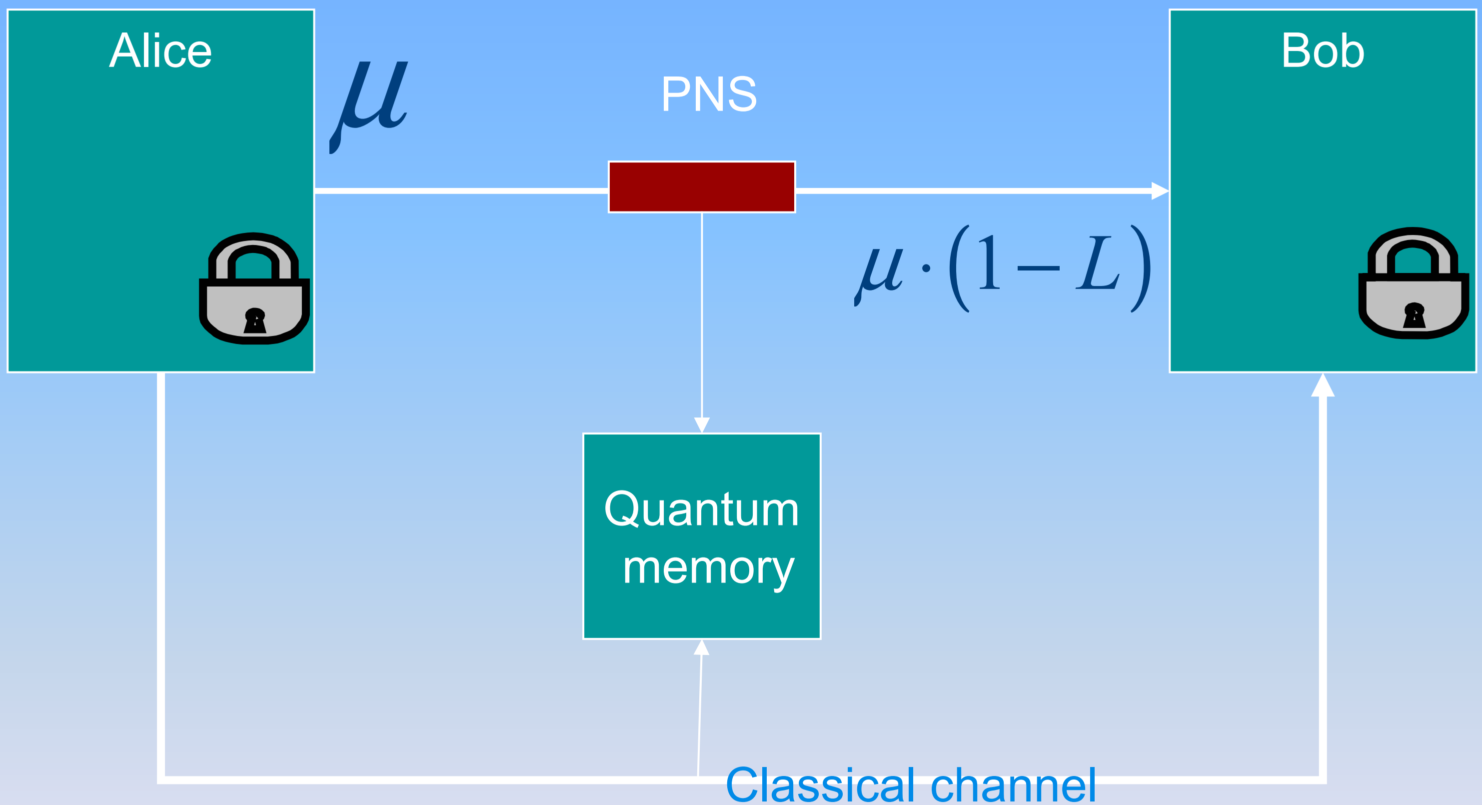
$$\eta_B = 0.5$$

Eavesdropping model

- Eve can perform POVM attack (cloning)
- Eve has QND apparatus to distinguish total photon number of the pulse
- Eve can use photon number splitting PNS attack (PNS + quantum memory)
- Eve can substitute the fiber with the loss-free channel or use quantum teleportation to deliver the (unknown) single photon state to Bob



Photon number splitting attack

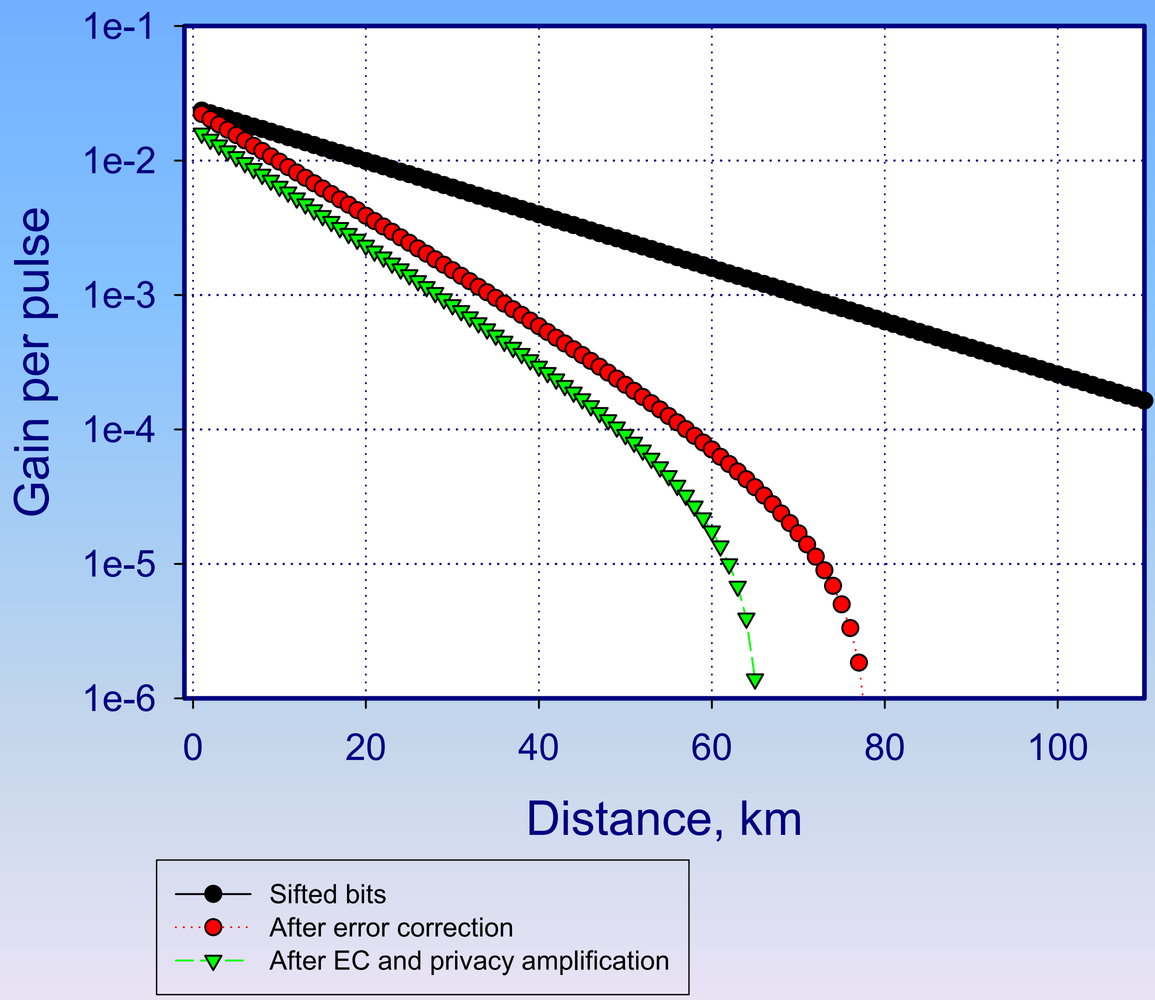


Eve can use only channel loss, not Bob apparatus loss or detector QE

How dangerous is the PNS attack??

- Can Eve get use of all the loss in the system or she can modify and take advantage only upon the channel loss?
- Alice and Bob apparatus assume to be physically protected from intrusion, Eve cannot use any type of amplification
- Conclusion: only the channel loss should be taken into account

WCP QKD performance



Parameters

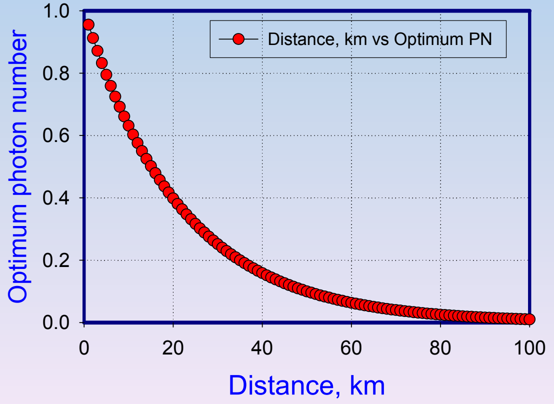
μ_B – optimum!

$\eta = 10\%$

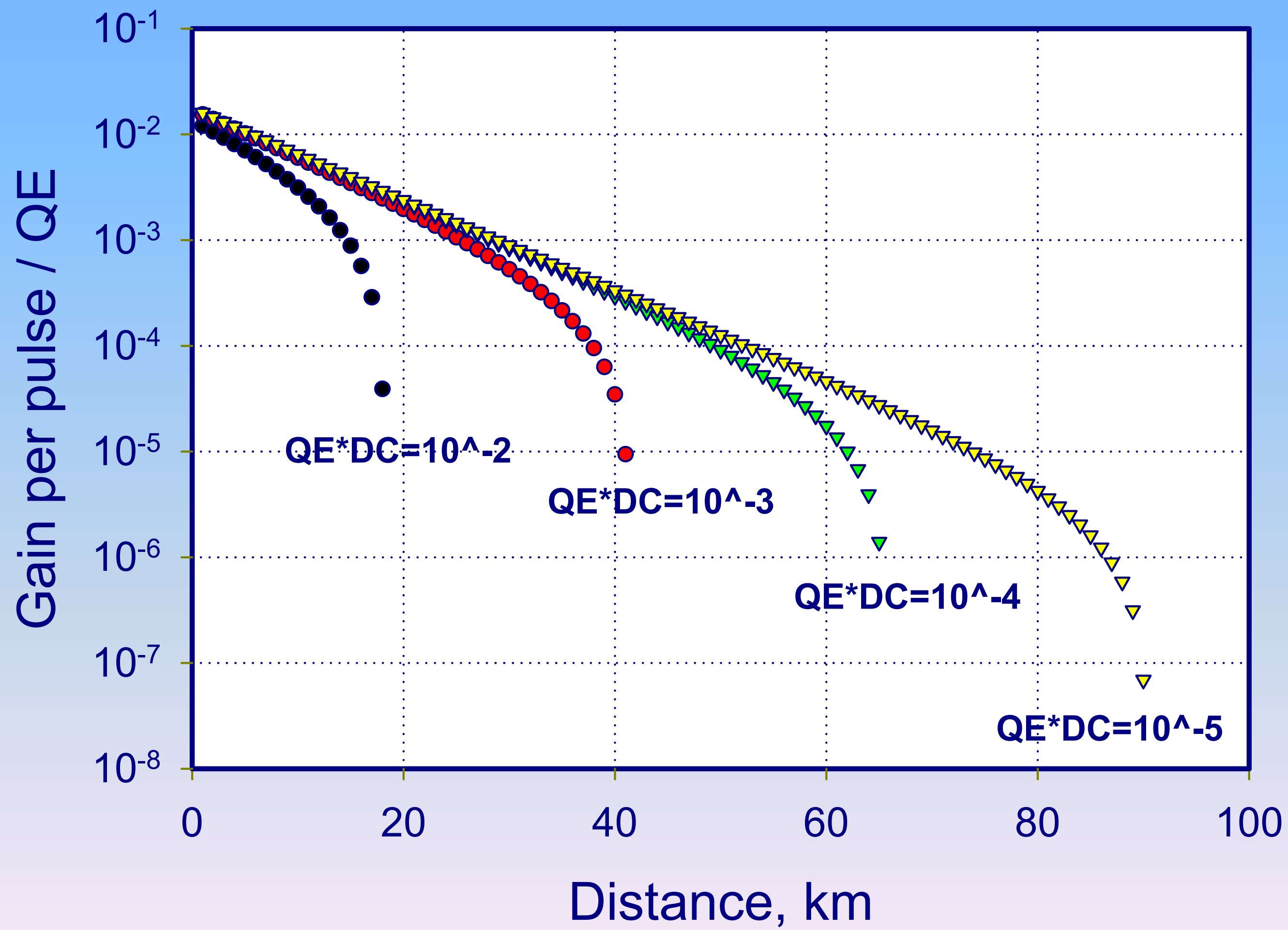
$p_{DC} = 10^{-5}$

$\alpha = 0.2\ dB/km$

$\eta_B = 0.5$



The influence of the dark current on the distance of QKD



Conclusion

- Secure QKD is possible with commercially available components
- Performance of the system depends on the combination of parameters and should be optimized for a certain experimental conditions
- Future progress in performance of QKD systems depends significantly on the progress in single photon counting technique, this is probably the most obvious and feasible source of improvement

- Thanks to Norbert Luetkenhaus
Darius Subacius
Anton Zavriyev