ITMO UNIVERSITY

Maintaining security against photon-number-splitting attacks in subcarrier wave quantum communication systems

Vladimir Egorov, Andrei Gaidash, Vladimir Chistyakov, Oleg Bannik, Anton Kozubov, Artur Gleim

viegorov@corp.ifmo.ru

ITMO University, Saint Petersburg, Russian Federation

Photonics-2016, Berlin

Outline

- Photon-number splitting attack (PNS) in quantum communication (QC)
- Subcarrier wave quantum communication (SCWQC)
- The problem: protecting SCW against PNS:
  - Quasi-single-photon source (classic approach)
  - Strong reference
  - Decoy states
  - Photon-number-resolving detectors
- Conclusion

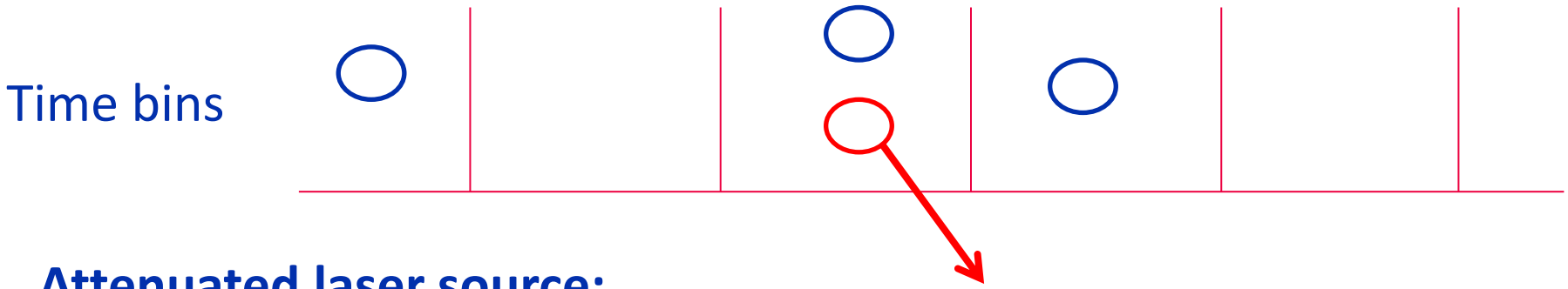
Secure quantum communication and PNS attack

Quantum communication (QC) systems grant information security in optical communication based on the fundamentals of quantum physics.

Every interference (attack) in the quantum channel induces disturbance in it and can be revealed by monitoring error rate (QBER)…

…if a “true” single photon source is used

Beamsplitting: a unique attack that does not increase QBER!



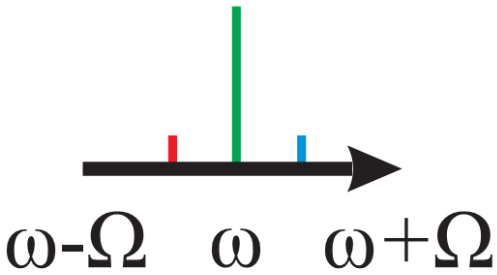
Attenuated laser source:
Mean photon number (μ) ~ 1

Multiphoton states are split by Eve

Subcarrier wave quantum communication

- Quantum channel is formed at sidebands of an optical carrier as a result of phase modulation. Each pair of subcarriers operates as an independent quantum channel.

$$E = Ae^{i\omega t} + iAa \cdot \cos\left(\frac{\varphi_a - \varphi_b}{2}\right) \cdot \left(e^{i\left((\omega+\Omega)t+\frac{\varphi_a+\varphi_b}{2}\right)} + e^{i\left((\omega-\Omega)t+\frac{\varphi_a+\varphi_b}{2}\right)}\right)$$



Key advantages:

- Interferometric stability not affected by distance
- Compliance with existing telecommunication lines
- Spectral efficiency up to 40% compared to 4% for modern QKD systems

Problem: choosing the best counter-PNS strategy

- Possible ways of countering PNS attack:
  - Classic approach
  - Strong reference
  - Decoy states
  - Photon-number-resolving detectors
- Currently no analysis has been conducted for countering PNS in SCW architecture:
  - What are the hardware requirements?
  - Which is optimal in terms of key generation rate and hardware requirements?

Experimental parameters used in calculations

- Phase change (state encoding) frequency: 100 MHz
- Signal visibility: V = 98,5%
- Fiber losses (*Corning SMF28-ULL*): α = 0.17 dB/km
- Losses in receiver (Bob) module: β = 6.4 dB
- Detector quantum efficiency: η = 20%
- Detector dark count rate: f_{dark} = 10 Hz; $p = f_{dark}/F$
- L – fiber length (km)
- Laser power in transmitter (Alice): 10 mW
- Mean photon number (μ) varies with the protocol

$$R_{sift} = F\mu\eta 10^{\frac{-\alpha L-\beta}{10}}$$

$$QBER = \frac{1-V}{2} + \frac{p}{2\mu\eta 10^{\frac{-\alpha L+\beta}{10}}}$$

Secure key generation rate limit [1]

- Secure key rate limit for a coherent state source is given by:

$$R_{\text{sec}} = R_{sift} \cdot (\Delta \cdot (1 - h(Q/\Delta)) - h(Q))$$

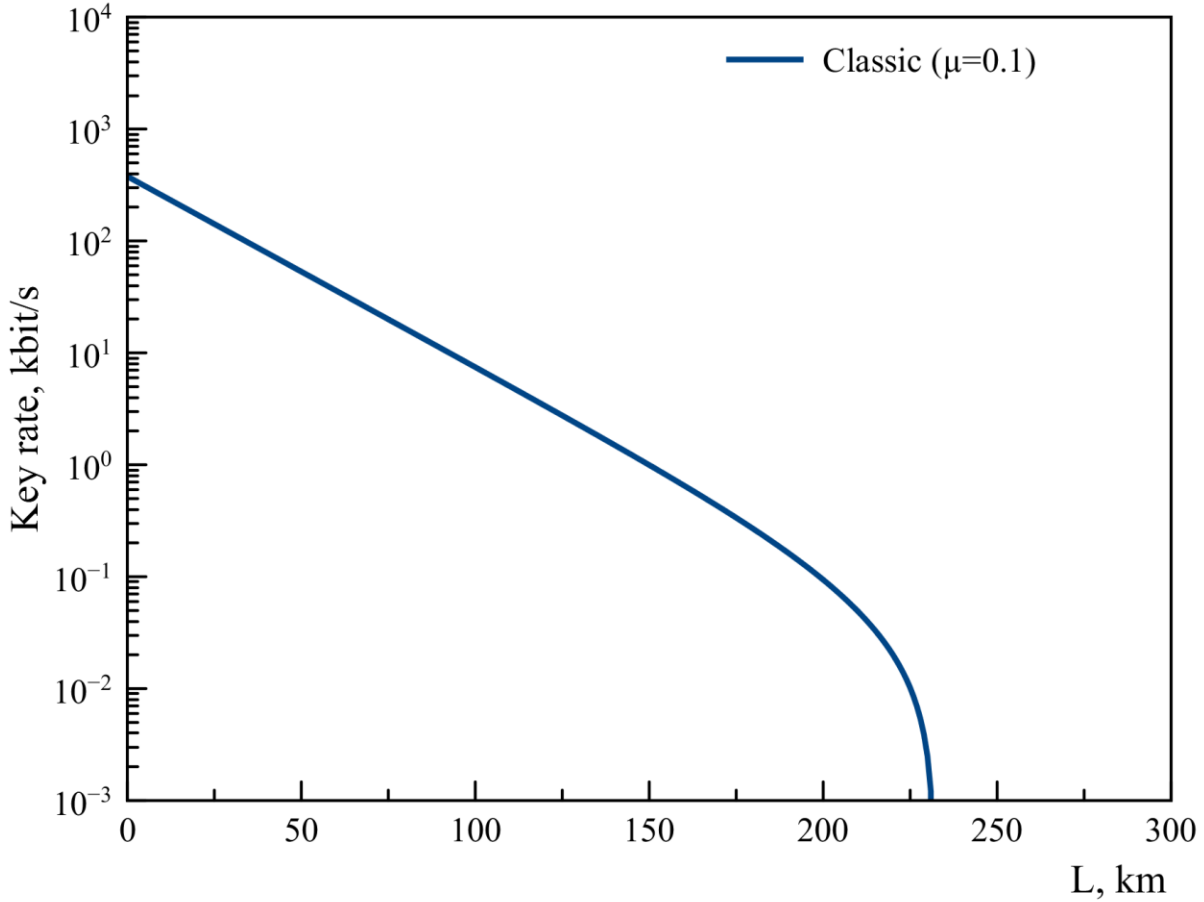
Where F is the sifted key rate, Q – QBER, Δ – single photon fraction, h(x) – Shannon binary entropy function

- Single-photon fraction of the key Δ, which is not known to Eve, is calculated using Poissonian statistics of the attenuated laser:

$$D = 1 - \frac{1 - (1+m)e^{-m}}{1 - e^{-m}}$$

I. Classic approach: low mean photon number

- BB84 protocol requirements: QBER < 11%, μ ~ 0.1



Lower sifted key rate, *but* only Δ~5% of key information must be removed due to PNS attack (quasi-single photon source)

II. BB84 protocol with strong reference [1]

- Secure against photon-number splitting (PNS) attack, if two conditions are met:
  - A strong reference is included in the transmission of the quantum channel, and mixed with it
  - The reference is always monitored by Bob
  - In this case, Eave's information about multiphoton states does not depend on channel loss and can be removed:

$$I_E = 1 - \Delta = \frac{1 - (1+\mu)e^{-\mu}}{1 - e^{-\mu}}$$

- These conditions are naturally satisfied in the SCW approach

1. O. Guerreau, F. J. Malassenet, S. W. McLaughlin, J.-M. Merolla // Photon. Tech. Lett. **17(8)**, 1755 (2005)

Strong reference in SCW: protocol requirements

- Source parameters for realistic SR protocol (~100% reference detection in 0 - 40 dB channel):

a) Classical detector threshold ~ 10 nW => min W_{Alice} ~ 100 μW
W_{quant} ~ 10 pW => required high filter extinction: **50-90 dB!**

b) Single-photon detector for *n* photons:

$$CDE = 1 - (1 - \eta)^n$$

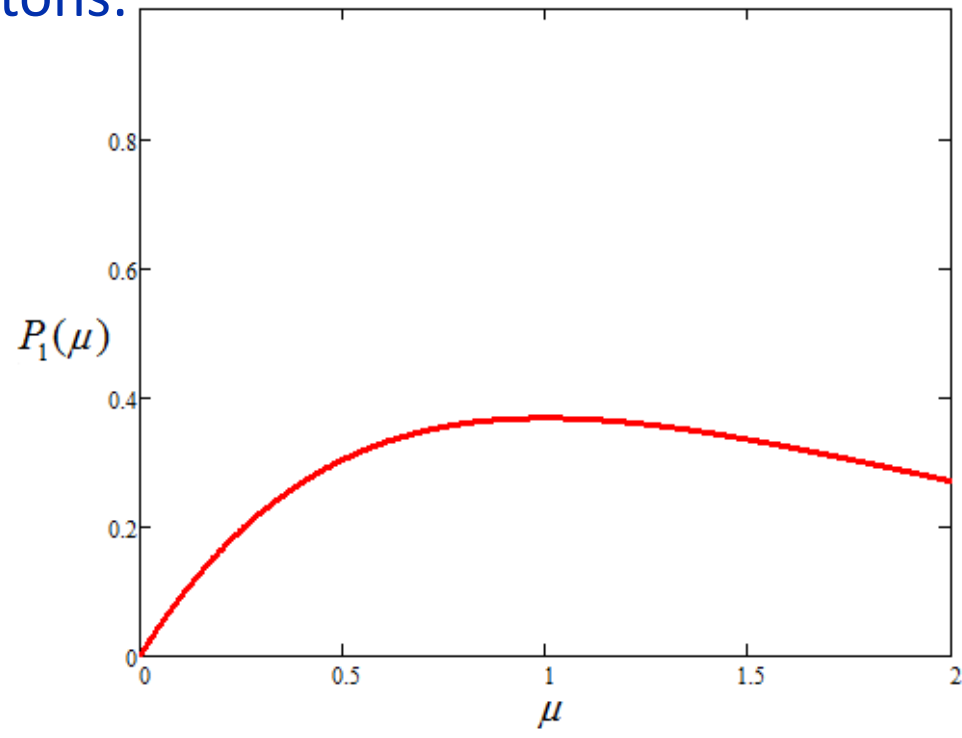
W_{Alice} ~ 10 μW or "weak reference"

- Optimal μ = 1 (see figure)

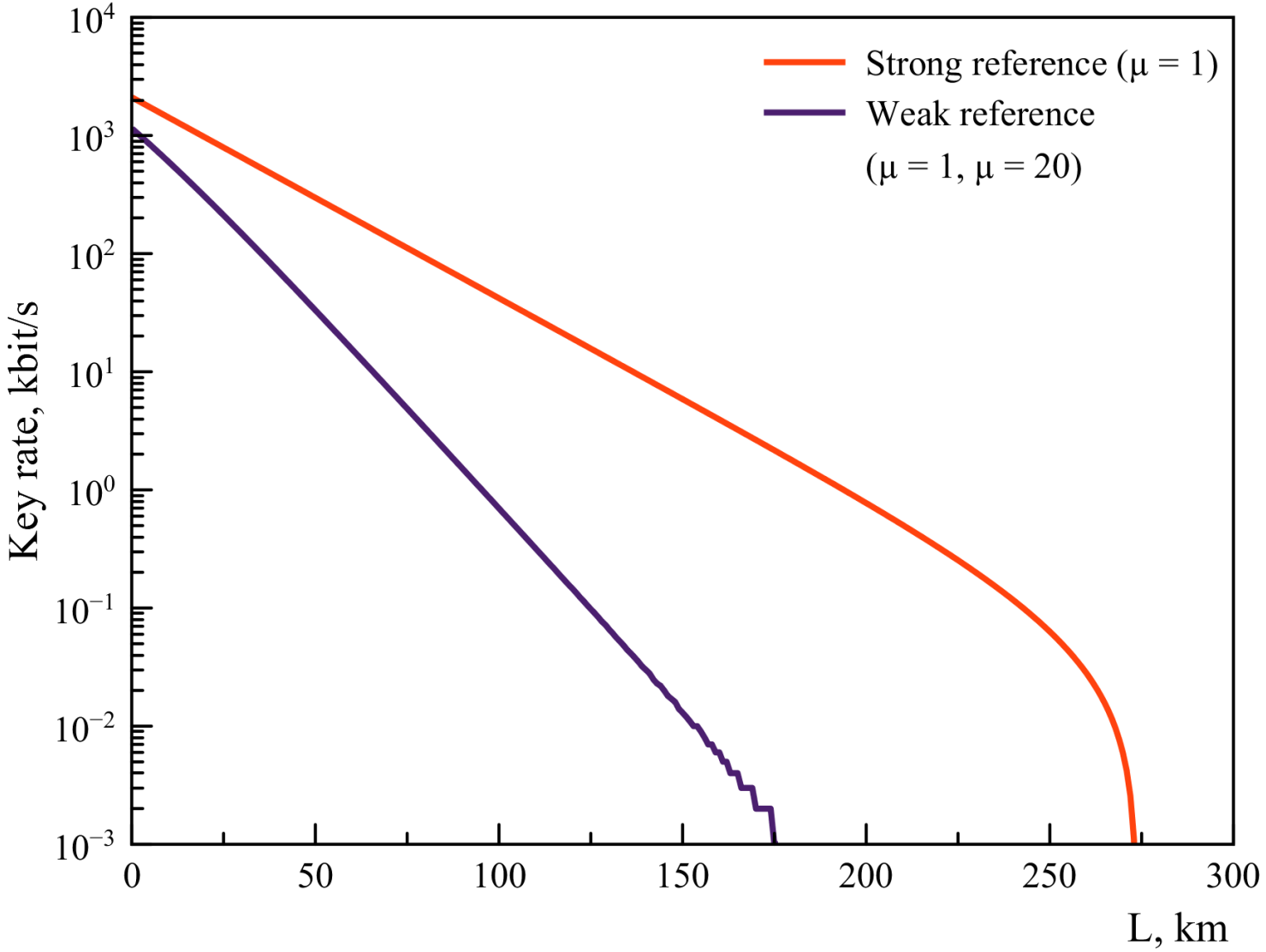
$$P_1(\mu) = \mu \exp(-\mu)$$

- Decreased QBER limit:

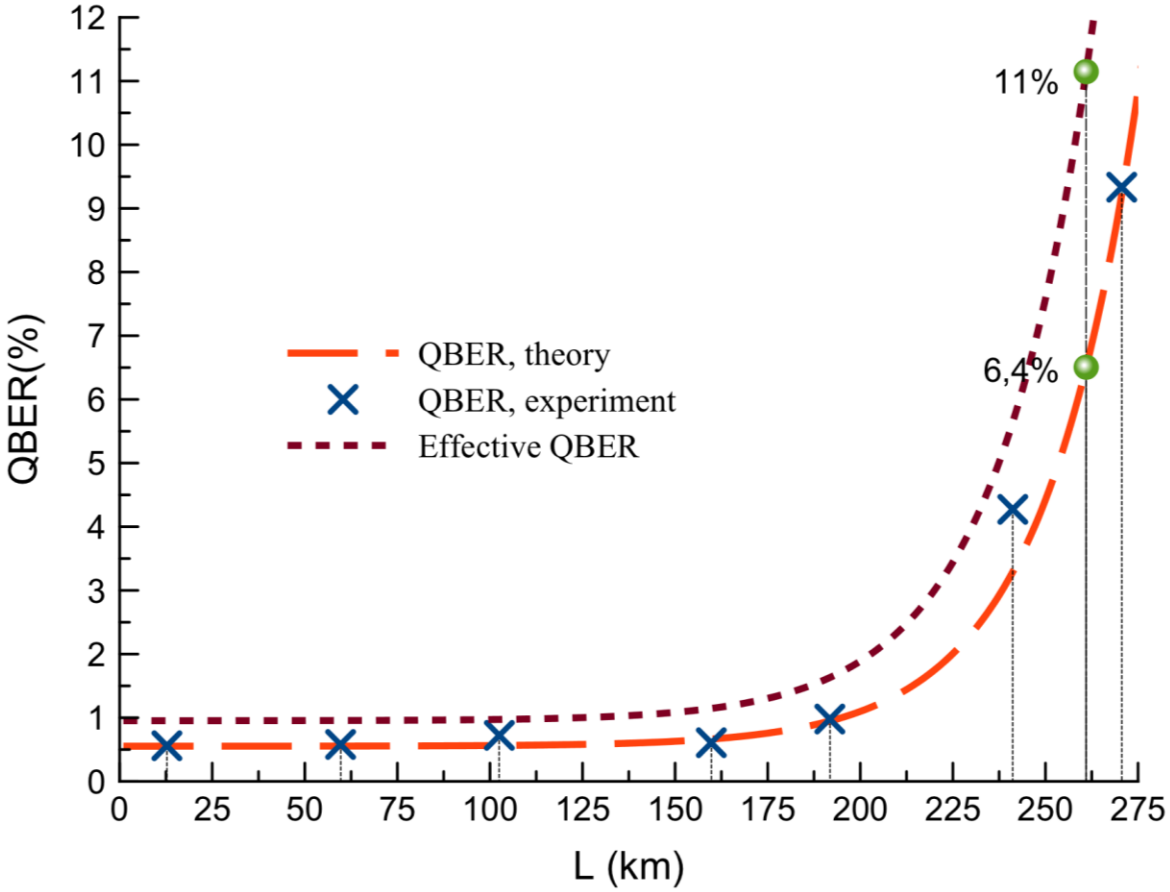
$$QBER_{eff} = QBER / \Delta = 6.4\%$$



Strong reference protocol results: key rate



Strong reference protocol results: QBER



BB84 protocol with strong reference operates with a key fraction defined by Δ, effectively increasing the QBER by its inverse value

Realistic decoy states in SCW QC

We must ensure that the eavesdropper cannot identify the decoys by monitoring the fluctuations of intensity of light at the carrier!

$$I_0 = A^2 \cdot J_0^2(m) = \mu_L \cdot J_0^2(m) = \mu_C,$$
$$I_{\pm 1} = A^2 \cdot J_1^2(m) = \mu_L \cdot J_1^2(m) = \mu_Q,$$

μ_L, μ_Q, μ_c – average photon number per pulse: initial (L), quantum channel (Q) at the carrier (C)

$$(1-\mu_{Qs}) \cdot \exp(-\mu_{Qs}) = \frac{f \cdot H_2(e_{\det})}{1-H_2(e_{\det})},$$

Optimal μ_Q value (signal) according to decoy states theory

$$QR = \frac{\mu_{Qd}}{\mu_{Qs}} = 0.05$$

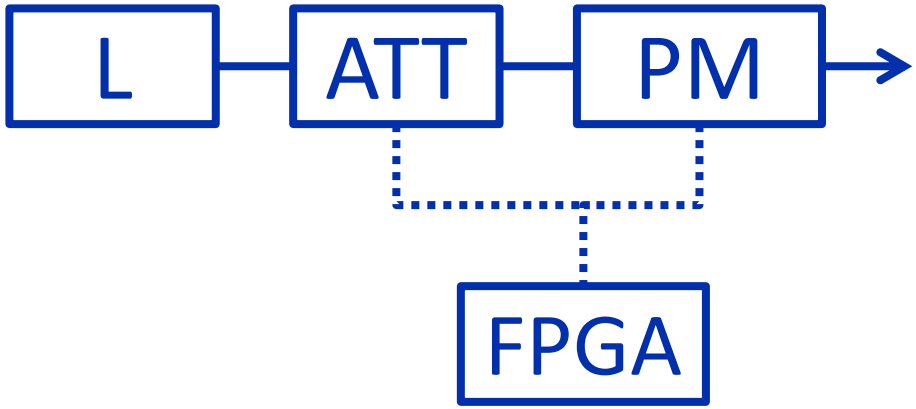
$$\mu_L \sim 20$$

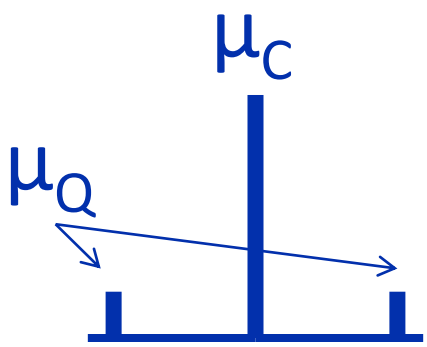
Realistic decoy and carrier powers

$$Att = 10\log_{10}\left(\frac{h \cdot c \cdot \nu \cdot \mu_L}{\lambda \cdot W_0}\right)$$

Attenuation coefficient at transmitter side

Decoy states in SCW: results





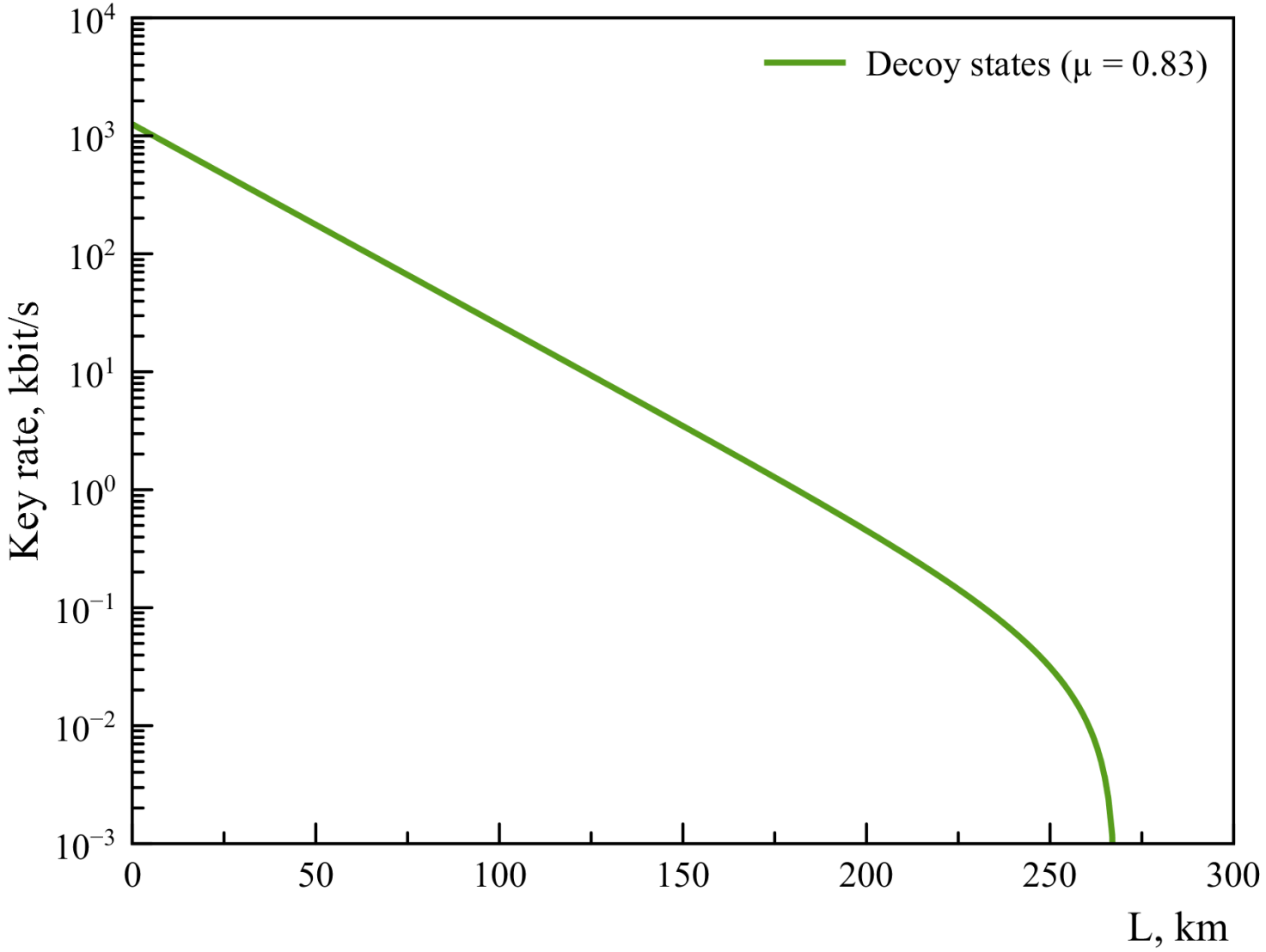
Proposed experimental setup of the SCW QC source with carrier intensity regulated by a programmed amplitude modulator

Calculation results:

$\mu_{Qs} \approx 0.831$ $\mu_{Ls} = 21.68$ $Att_s = -75.6$ dB

$\mu_{Qd} = 0.041$ $\mu_{Ld} = 20.08$ $Att_d = -75.9$ dB

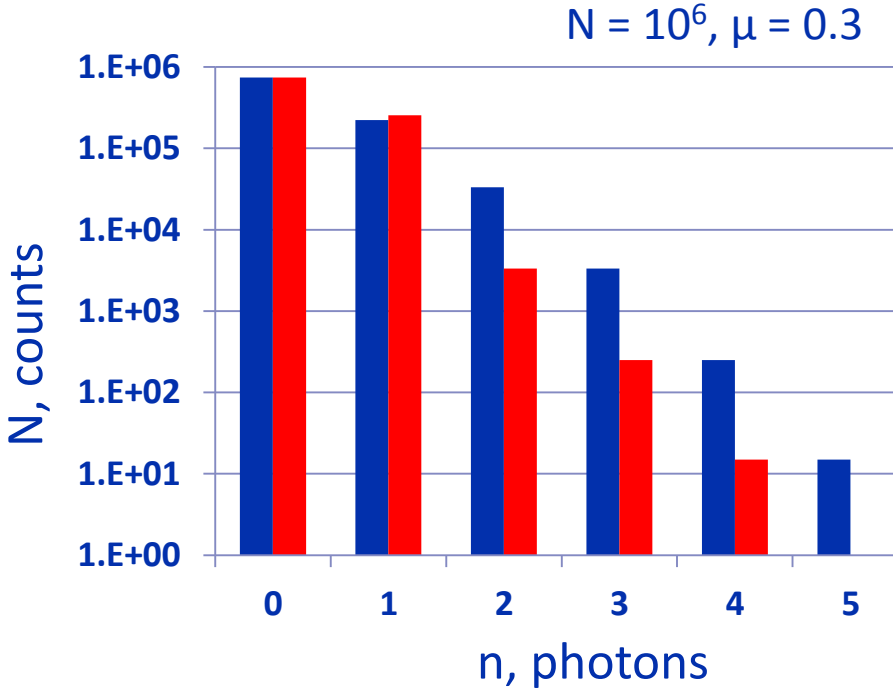
Decoy state: secure key rate limit



Photon-number-resolving detectors: approach

When Eave attacks using beamsplitting, she modifies (red) the initial (blue) Poissonian statistics of photon numbers per pulse, i.e.:

$$P_E(\mu,n)=\begin{cases} P_A(\mu,0), & for \quad n=0 \\ P_A(\mu,1)+P_A(\mu,2), & for \quad n=1 \\ P_A(\mu,n+1), & for \quad n\geq 2 \end{cases}$$



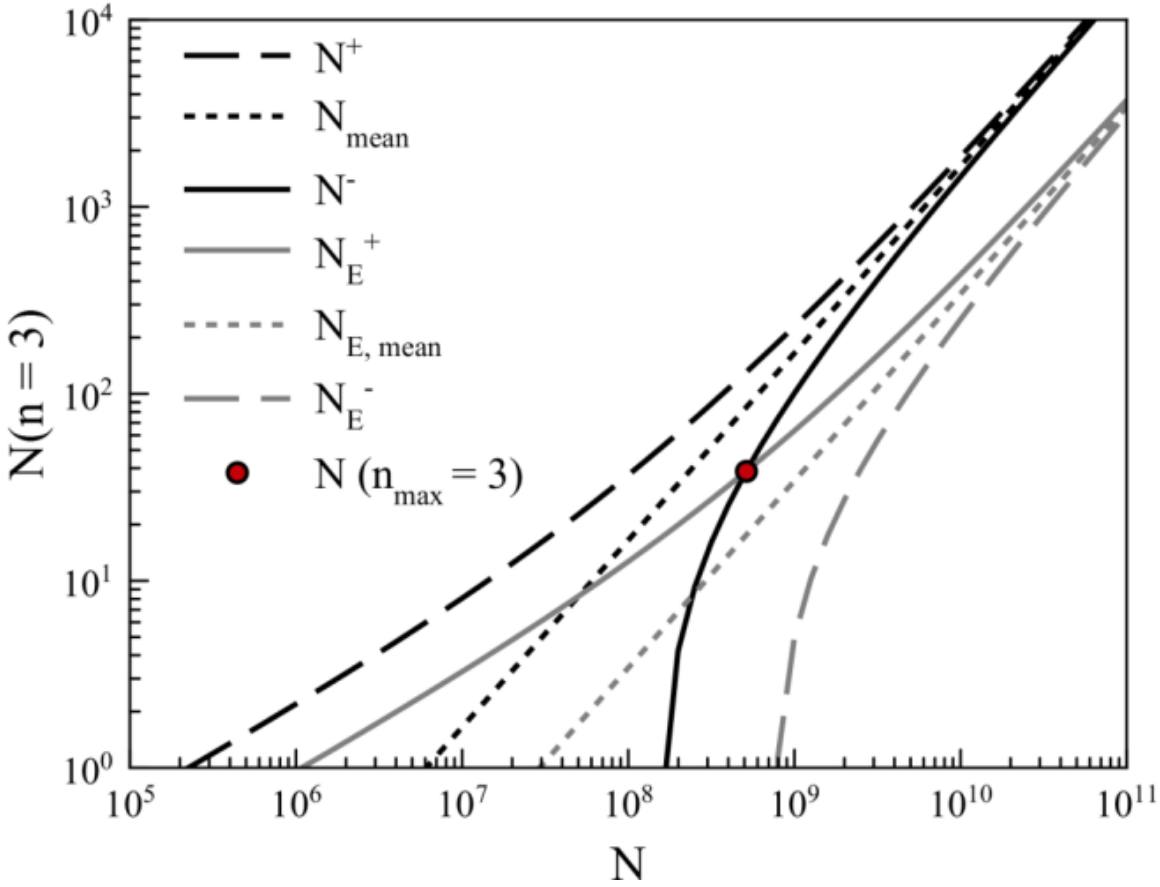
it can be used for revealing the PNS attack with a given probability for each N and n:

$$N > \left(z \cdot \frac{\sqrt{P_B(n)} + \sqrt{P_E(n)}}{P_B(n) - P_E(n)} \right)^2$$

Efficient detector that can resolve photon numbers [1] is required

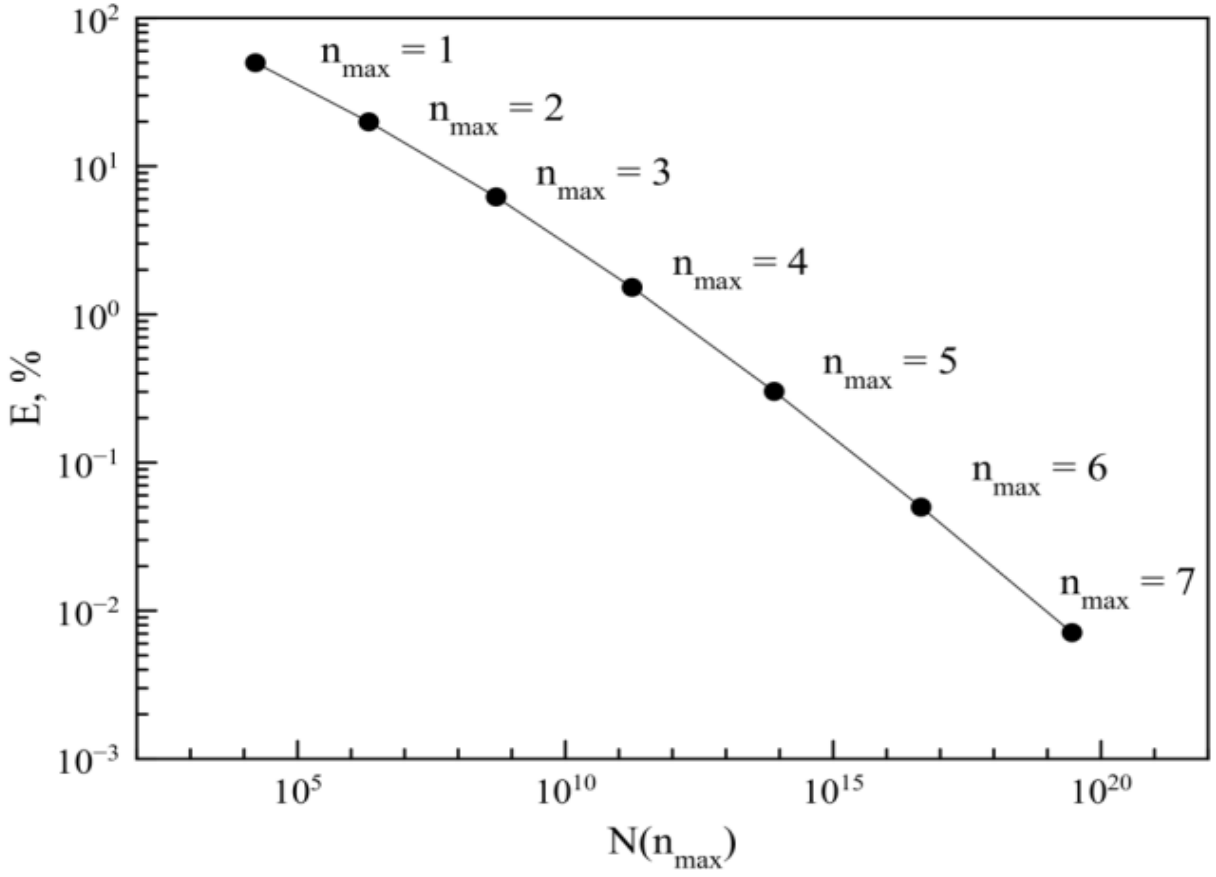
1. Z. Zhou, S. Jahanmirinejad, F. Mattioli et al. “Superconducting series nanowire detector counting up to twelve photons,” Optics Express **22**, p. 3475 (2014).

Photon-number-resolving detector: results



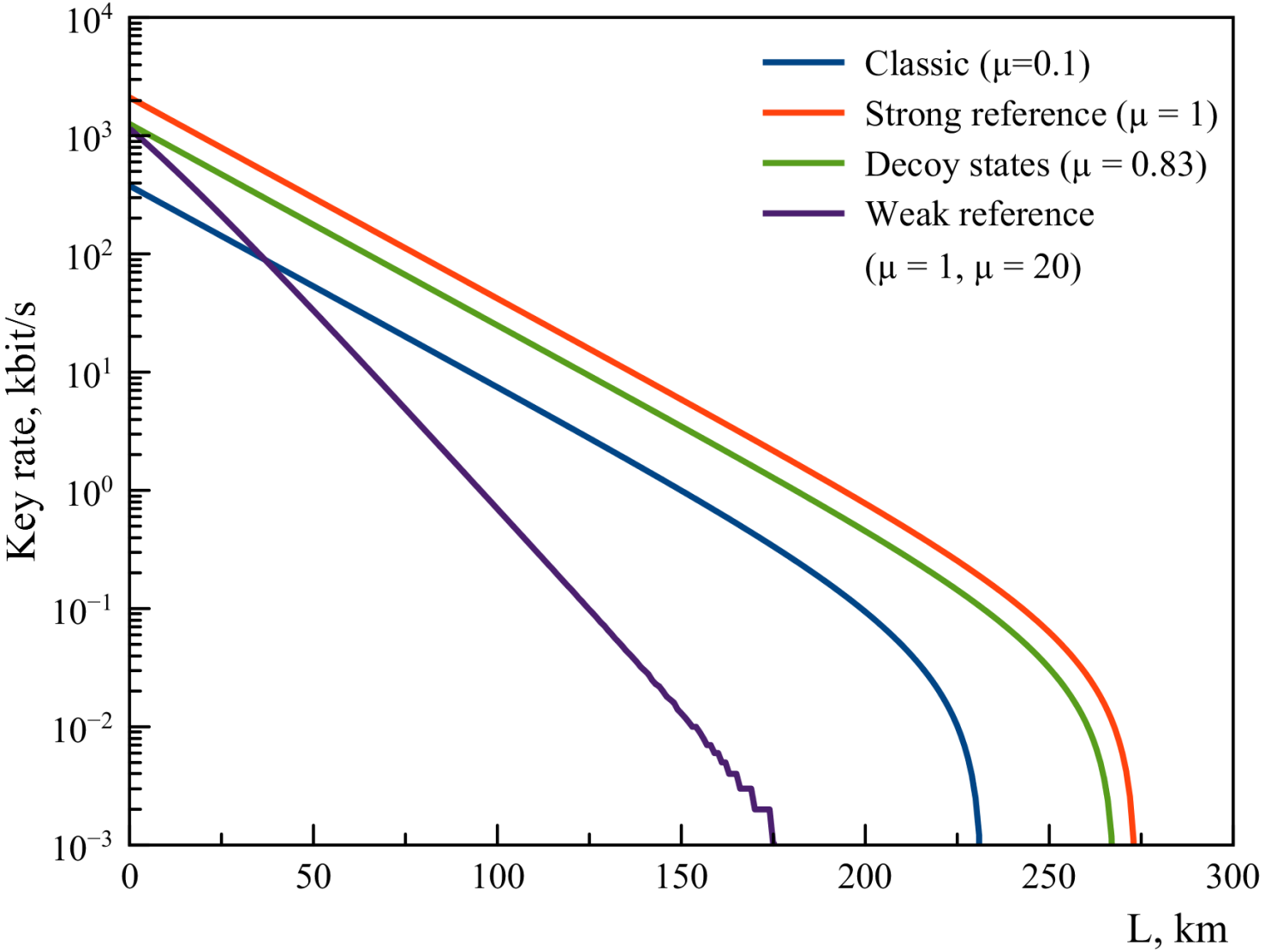
Change in pulse detection statistics with n = 3 in the presence of PNS attack. The crossing point (marked by a dot) defines the minimal *N* required to reveal the attack. Channel loss 20 dB, μ = 1, z = 5.

Photon-number-resolving detector: results



Raw key fraction known to Eve versus total number of pulses. Channel loss 20 dB, μ = 1. Higher n_{max} decreases Eve's information but leads to an increase of the minimal necessary *N*

Results: calculated secure key rate limits



Results & conclusion

Protocol	Advantage	Disadvantage
Classic (low μ)	No hardware requirements	Low bitrate
Strong reference	Highest key rate limit; Tolerant to parameter fluctuations	Higher requirements to filtering and QBER
Decoy states	Simpler hardware than strong reference	Highly dependent on detector parameters
Photon-number-resolving (PNR)	No protocol or setup modification	Absence of commercial PNR detectors

Strong reference remains the best candidate for countering PNS



ITMO UNIVERSITY

Thank you for you attention!

viegorov@qcphotonics.com

Berlin, 2016