# Practical Approaches to Protecting Quantum Key Distribution Systems against Laser Damage Attack

Alferov Sergei, Optical Engineer

infotecs

# Outline

- Motivation for QKD usage
- QKD: how does it works?
- Types of attack
- LDA: what is it?
- Practical countermeasures to LDA
- Conclusion

# Motivation for QKD usage

Trends

- Higher speed of data transfer: 10Gbps ->100Gbps -> 400Gbps
- Increasing volume of data transfer: 20-25% per year

Risks

- High cryptographic key utilization rate
- Creating an Efficient Quantum Computer
- Compromising by staff

# Motivation for QKD usage

infotecs

## Quantum computing

State of the art:

- 53-qubit Sycamore chip, Google (2019)
- 65-qubit processor Hummingbird r2, IBM (2020)
- 127-qubit processor Eagle, IBM (2021)

A close-up view of an IBM quantum computer

# Motivation for QKD usage

infotecs

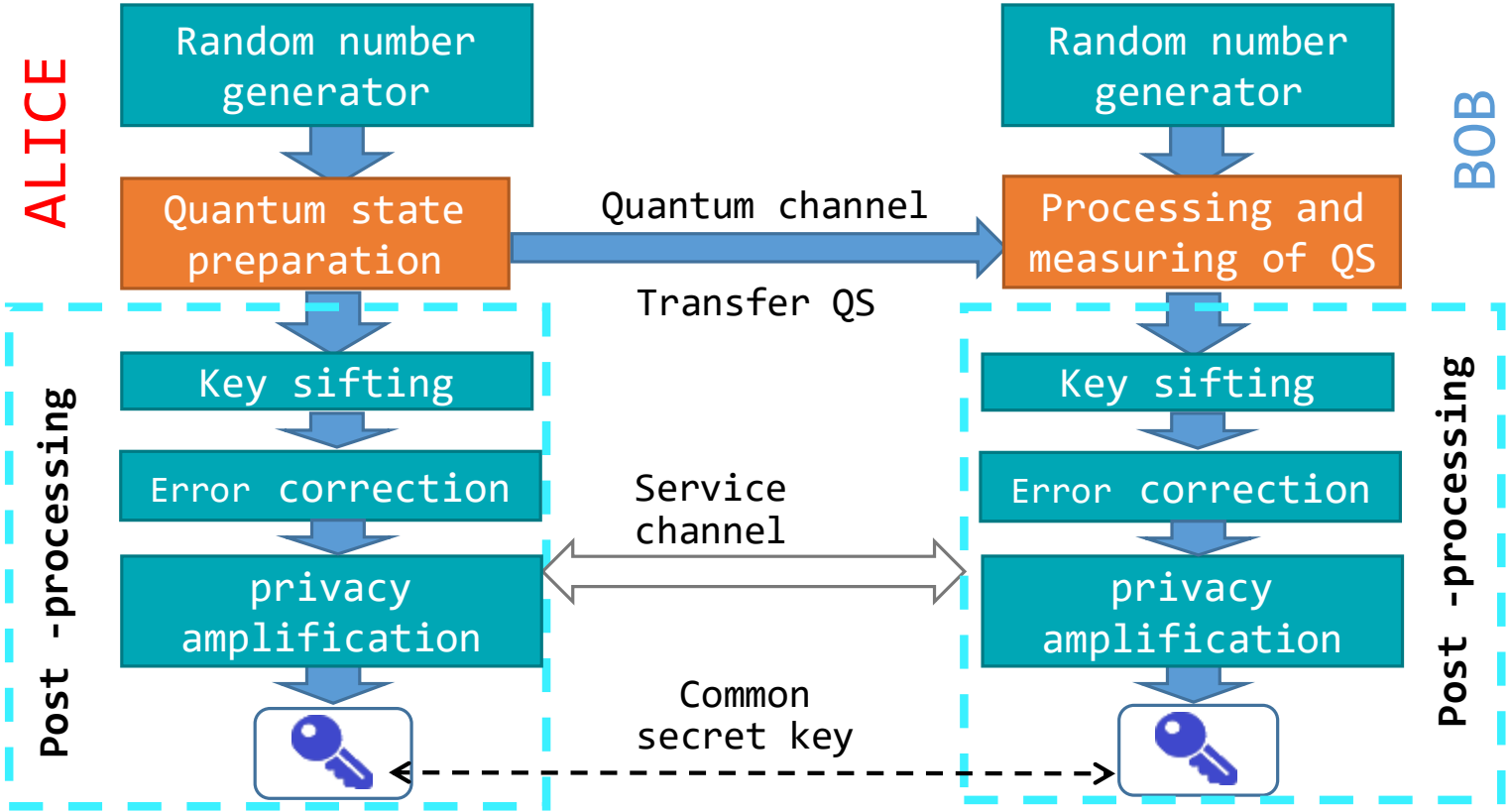
## General approaches to secret key distribution

| | Asymmetrical Cryptography | Key Distribution by Trusted Courier | Quantum Key Distribution |
|---|---|---|---|
| Pros | Frequent key update | Reliable for QC (*) | Reliable for QC (*), High-rate key delivery |
| Cons | Vulnerable for QC (**) | Slow-rate key delivery, Compromising by staff | Engineering tasks, Flaws in implementation |

(*) take into account the speed-up of a brute force attack by Grover's algorithm
(**) “in post-quantum cryptography we trust”

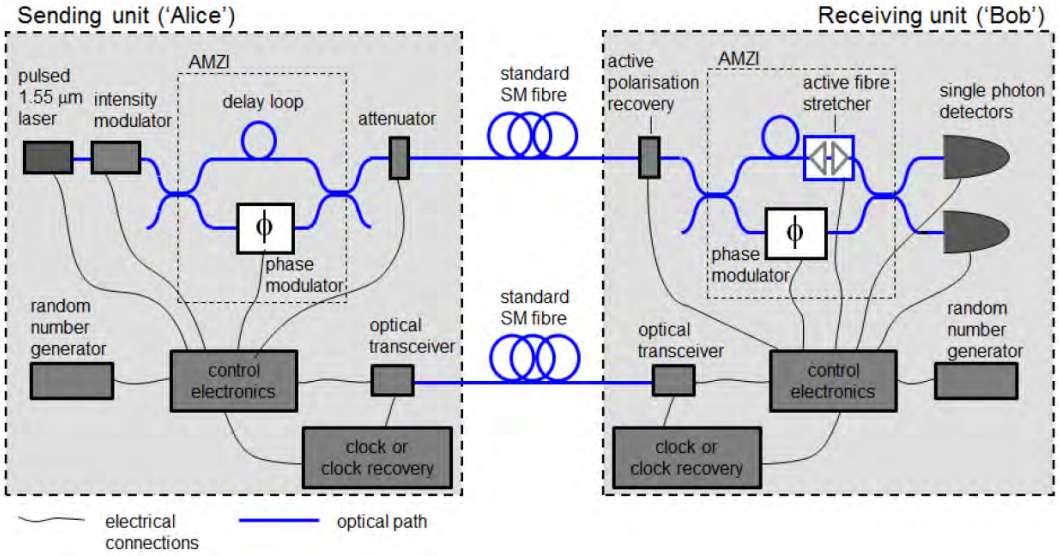
# QKD: how does it works?

infotecs



# QKD: how does it works?

## Behind the Curtain




Example of implementation QKD system [1]

QKD system often uses weak laser pulses (WLP) attenuated to quasi-single level

[1] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, Opt. Express 15, 8465 (2007).

# Types of attack

infotecs

According to [1] there are several types:

1. Attack directly  on quantum states (no access to QKD equipment)
2. Passive attack (side channels like  detection of EM emission)
3. Active attack (probing of optical elements)
4. Modification of  QKD system parameters by Eve (Detectors Mismatch, LDA [2])

We are considering Laser Damage Attack (LDA)

[1] С.Н. Молотков, ЖЭТФ, том 157, вып.6, стр. 963-990 (2020)

[2] V. Makarov, Phys. Rev. Appl. **13**, 034017 (2020).

# LDA what is it?

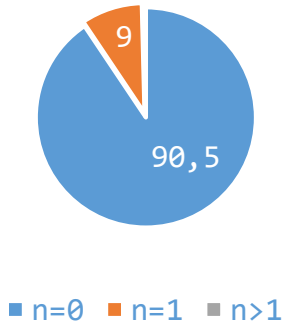
$$P_\mu(n) = e^{-\mu}\frac{\mu^n}{n!}$$

Poisson distribution

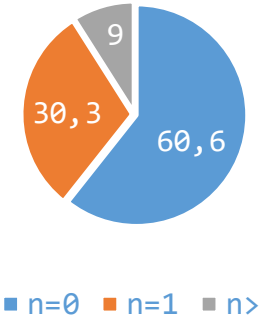
P – probability to find out given number of photons at fixed μ

μ - mean photon number, n- number of photons in pulse

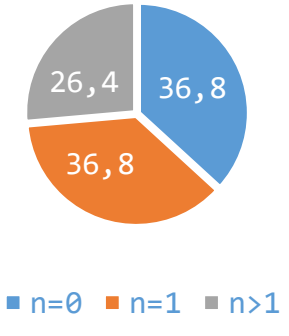
μ=0.1




μ=0.5




μ=1




n>1 are multiphoton pulses - the MAIN GOAL for Eve

# LDA what is it?

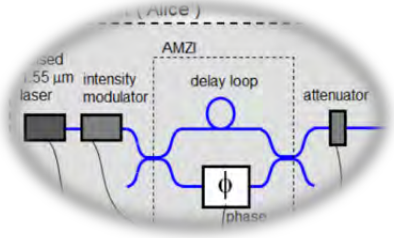
Once upon a time in Wonderland…


Alice
Transmitter

Quantum channel (free space, fiber)

Service channel

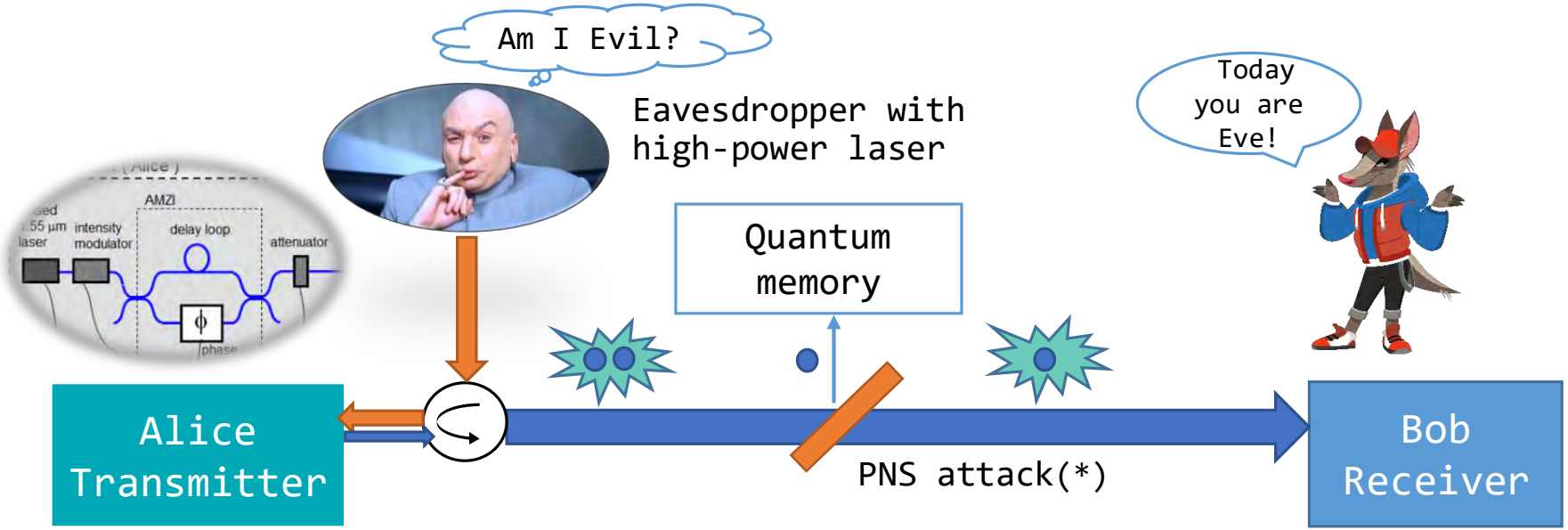
Bob
Receiver




Alice uses optical pulses attenuated to a quasi-single-photon level by an optical attenuator

$\mu_0$ - mean photon number

# LDA what is it?




**Attenuator** – is the nearest element for Eve!

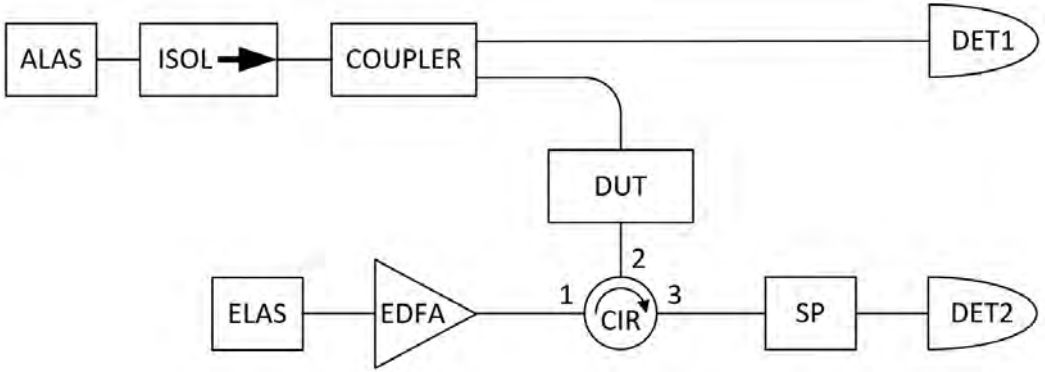
**High power impact-> decrease attenuation-> increase fraction of multiphoton pulses**

(*)- multiphoton pulses reveal vulnerability also for UM-attack, and beam splitter (transparent) attack

# Practical countermeasures to LDA

infotecs

## Experimental setup




Power of ALAS (1544 nm) 18 dBm;

Power of ELAS (1561 nm) 25 ÷ 37.4 dBm, 1 dB step;

Coupler: 10 % - DET1, 90 % - DUT;

Filter suppression of attack radiation > 50 dB;

Acquisition time / time step: 60 sec. / 10 ms


The attenuation of DUT (dB):

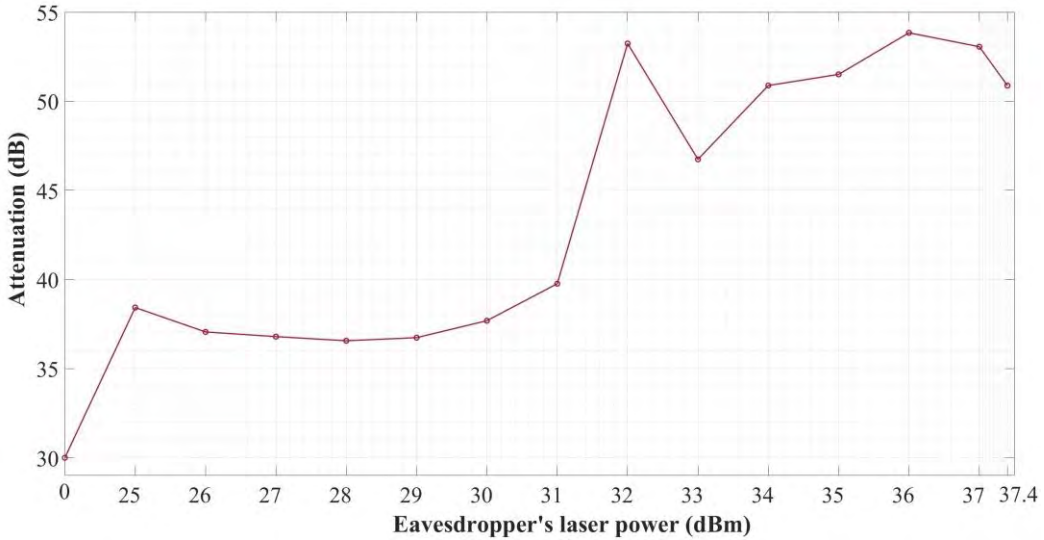
$$A = P_1 + K_c - P_2 - A_s$$

$K_c$ - insertion loss of coupler

$A_s$ - losses btw. the output of the coupler and DET2 (without of the DUT)

# Practical countermeasures to LDA

## Neutral Density Filter [1]





Glass: SZS-16

Holder: NA=0.13

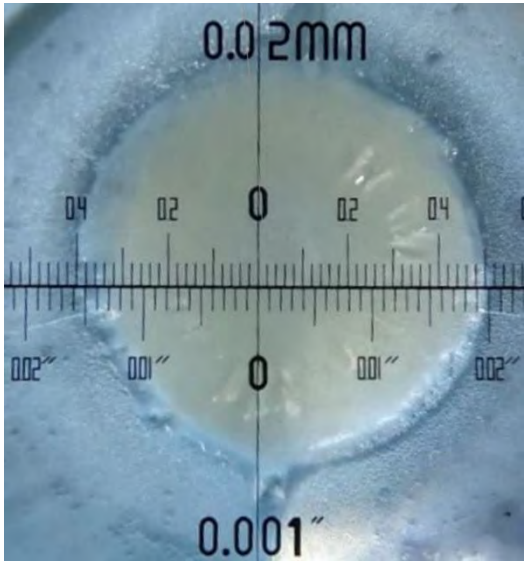
Initial Att. $A_0$ = 30 dB

Size: Ø 12mm; thick. 2mm.

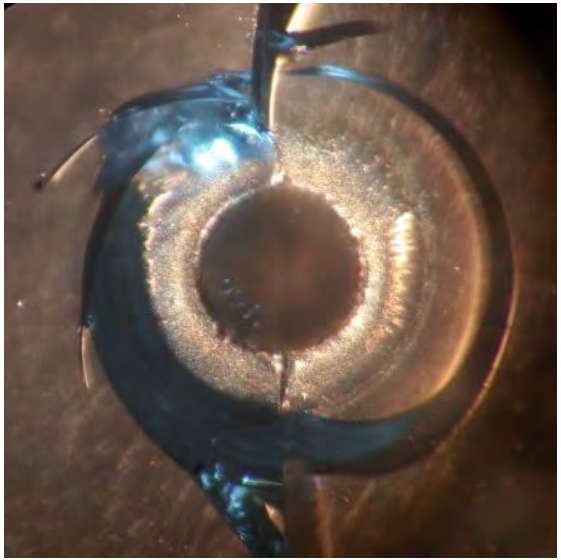
[1] S.V. Alferov, K.E. Bugai, I.A. Pargachev, JETP LETTERS Vol. 116 No.2 (2022)

# Practical countermeasures to LDA

## Neutral Density Filter



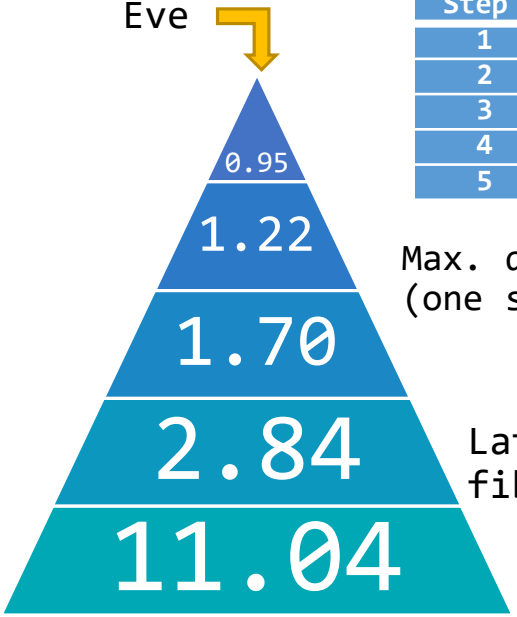

Circular crater with diameter approx. 0.9 mm



Crack around the crater

# Practical countermeasures to LDA

## Uniform Power Dissipation Cascade of Fiber Attenuators




Parameters of Attenuator

| № Step | Target Attenuation, dB | Measured Attenuation, dB | Dissipation power (input 5 W), W | Dissipation power (input 8,4 W), W |
|---|---|---|---|---|
| 1 | 0,95 | 0,9 | 0,94 | 1,57 |
| 2 | 1,22 | 1,2 | 0,98 | 1,65 |
| 3 | 1,7 | 1,8 | 1,05 | 1,76 |
| 4 | 2,84 | 3,8 | 1,19 | 2 |
| 5 | 11,04 | 9 | 0,74 | 1,25 |

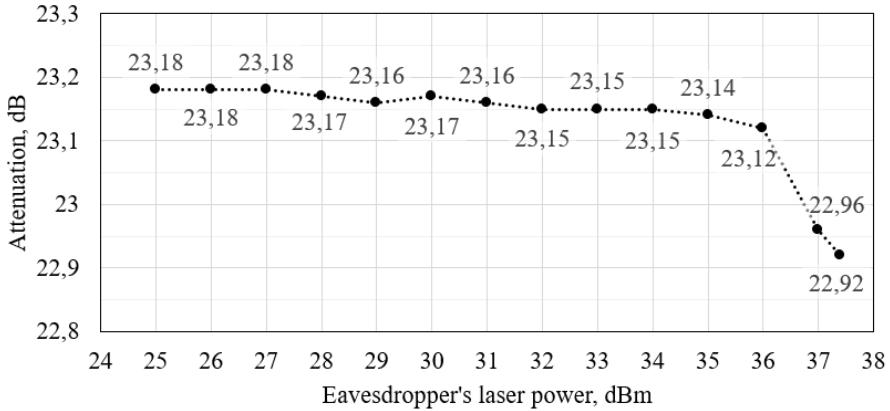
Max. dissipated power: $T_{th} = 2.5\ W$
(one step)

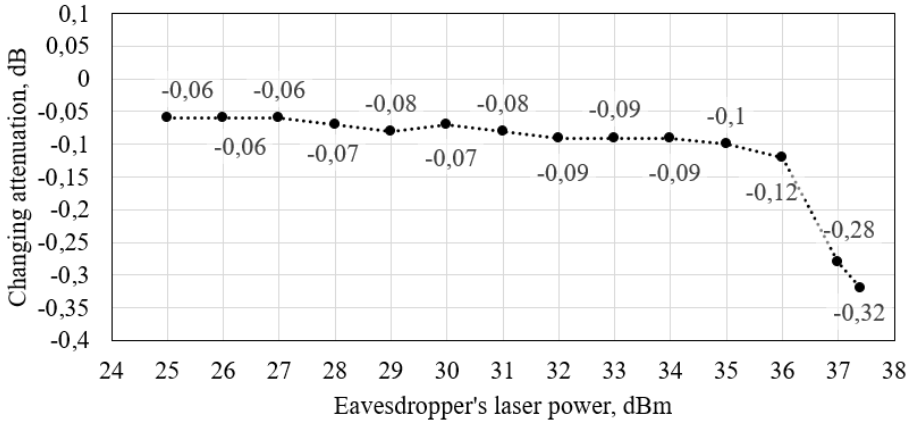
Method of producing:

Lateral misalignment of spliced fibers


# Practical countermeasures to LDA

## Uniform Power Dissipation Cascade of Fiber Attenuators (*)



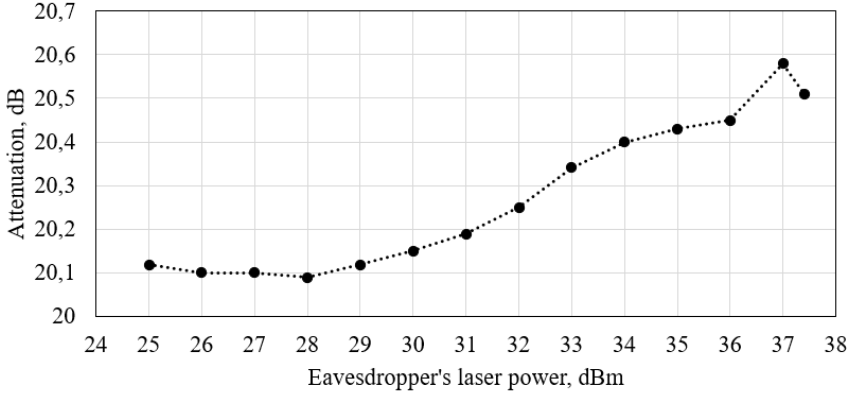

Changing Att. $\Delta A = A - A_0$

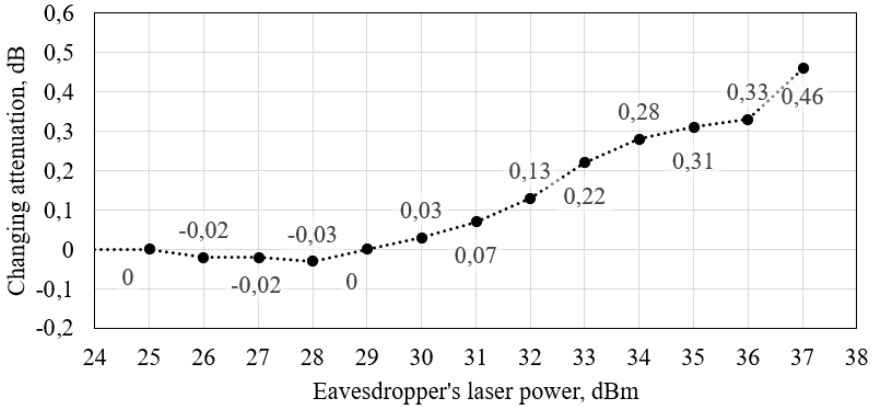
Initial Att. $A_0 = 23.24\, dB$

(*) in the patenting process

# Practical countermeasures to LDA

## Fixed attenuator “female-female”

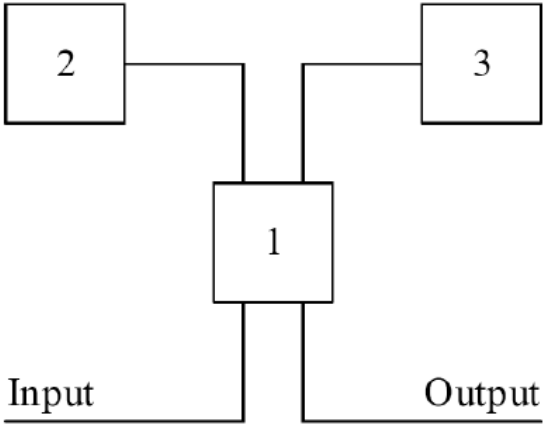


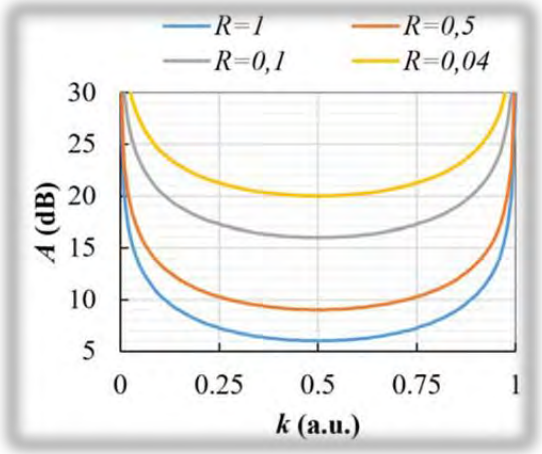




Initial attenuation $A_0 = 20.12\ dB$

# Practical countermeasures to LDA

## Attenuator based on Collapsing Mirror




$$A = -10 \cdot \log(k \cdot (1-k) \cdot R)$$

1 - Fiber Beam Splitter 2x2 (BS);
2 - Absorber;

3 - Collapsing Mirror

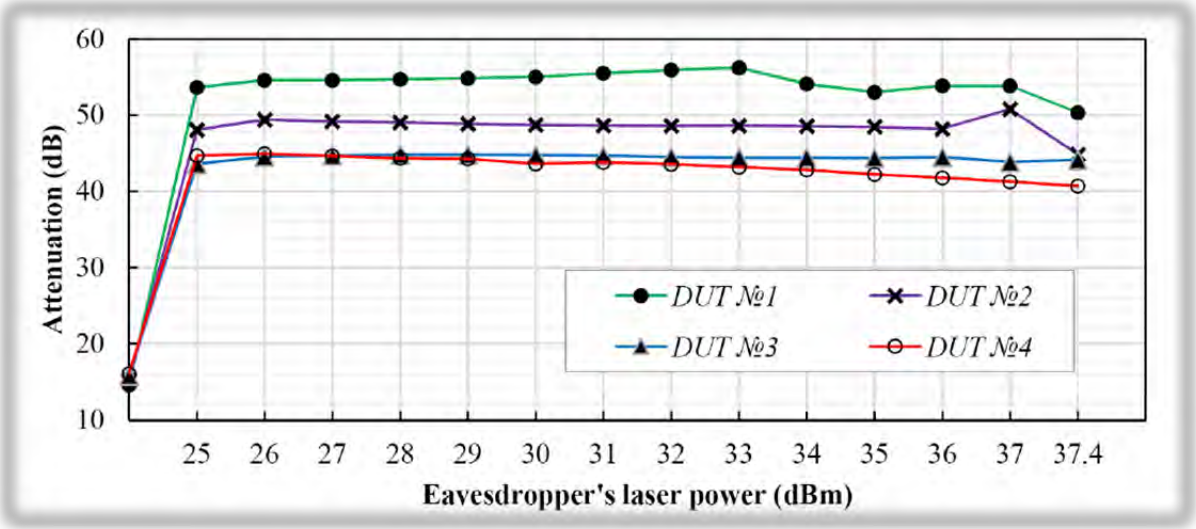
*K* - splitting ratio of BS;

*R* - reflection coefficient of mirror;

*K = 0.5* – min. attenuation for any *R*

# Practical countermeasures to LDA

## Attenuator based on Collapsing Mirror (*)




Reflection: R≈0.1

Initial att. ≈ 16 dB

Material: Chromium

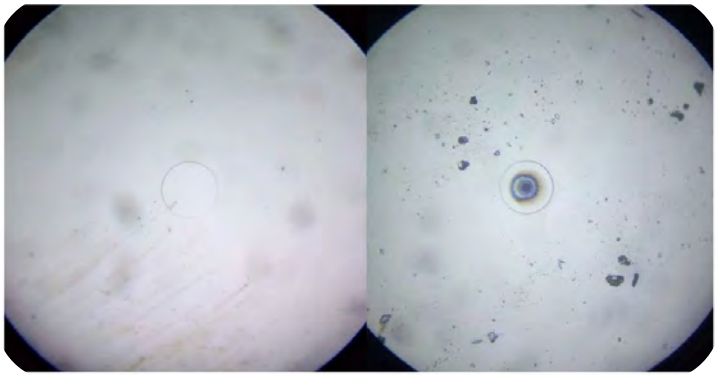
Thick. ≈ 150 nm

(*) in the patenting process

# Practical countermeasures to LDA

## Attenuator based on Collapsing Mirror

Picture of the mirror



before test after test

Pyrometry measurement

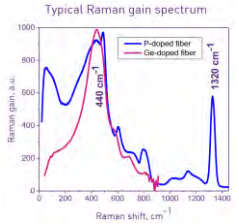

Absorber


FC-FC Adapter

# Practical countermeasures to LDA

infotecs

(*) Single Mode Fixed Fiber Optic Attenuator




(**) Attenuators based on optically active impurities

Please see the posters of Company's employees:

(*) Bugai K.E., Zyzykin A.P., Bulavin D.S. et al., Laser Damage Attack on a Simple Optical Attenuator Widely Used in Fiber-based QKD Systems

(**) Krishtop V.G., Popov V.G., Dvoretskiy D.A., Raman Cooling in Attenuators Doped with Optically Active Impurities

# Conclusion

| Solution | Behavior under LDA | PROS | CONS |
|---|---|---|---|
| NDF | Attenuation increase | Constant wide-range attenuation | High Price, Large size |
| Cascade | Attenuation reduce slightly | Cheap, Attenuation is freely adjustable | Production complexity |
| Fixed Att. | Common trend to increase attenuation | Cheap, Compact | Fixed nominal of attenuation |
| Collapsing Mirror | Attenuation increase | Attenuation is freely adjustable | Production complexity |

- The experimental scheme imitate a hacking scenario for a QKD system
- The choice of one or another approach depends on the goals and technical capabilities of the developers of QKD systems

# Thank you for your attenuation!

Sergey.Alferov@infotecs.ru

Подписывайтесь на наши соцсети

vk.com/infotecs_news

t.me/infotecs_news

rutube.ru/channel/24686363