ITMO UNIVERSITY

KQC

Polarization-independent subcarrier quantum communication system and its application in ITMO University quantum network

Artur Gleim[1,2], Vladimir Egorov[1], Simon Smirnov[1], Vladimir Chistyakov[1], Oleg Bannik[1], Andrey Anisimov[1], Sergei Kynev[1], Sergei Khoruzhnikov[1], Sergei Kozlov[1], Vladimir Vasiliev[1]

agleim@qcphotonics.com

1. ITMO University, Saint Petersburg, Russian Federation
2. Kazan Quantum center, Kazan, Russian Federation

Photonics-2016, Berlin

Our research team:



Prof. S.A. Kozlov



Dr. A. V. Gleim



Dr. V.I. Egorov



Dr. A.A. Anisimov



A. A. Gaidash



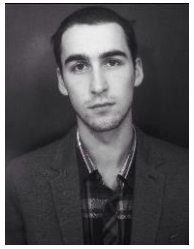
S.V. Smirnov



S.M. Kynev



O.I.Bannik



V.V. Chistyakov



A.V. Kozubov

Outline

- Latest progress in Subcarrier wave QKD
- Aims in research & development
- Experimental setup
- Formation of quantum channel
- Optical synchronization
- Polarization dependence compensation
- Secure protocol discussion
- Experimental results
- Conclusion

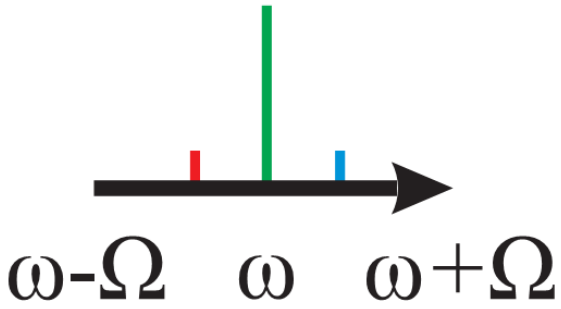
Quantum cryptography in telecom channels

- Operating in standard fibers (e.g. Corning SMF-28e)
- High spectral efficiency
- Multiplexing potential & multi-user operation
- Large distribution distance
- Scalable and compatible with network architecture
- No strict requirement on polarization stability
- Low sensibility to external factors
- Optical synchronization



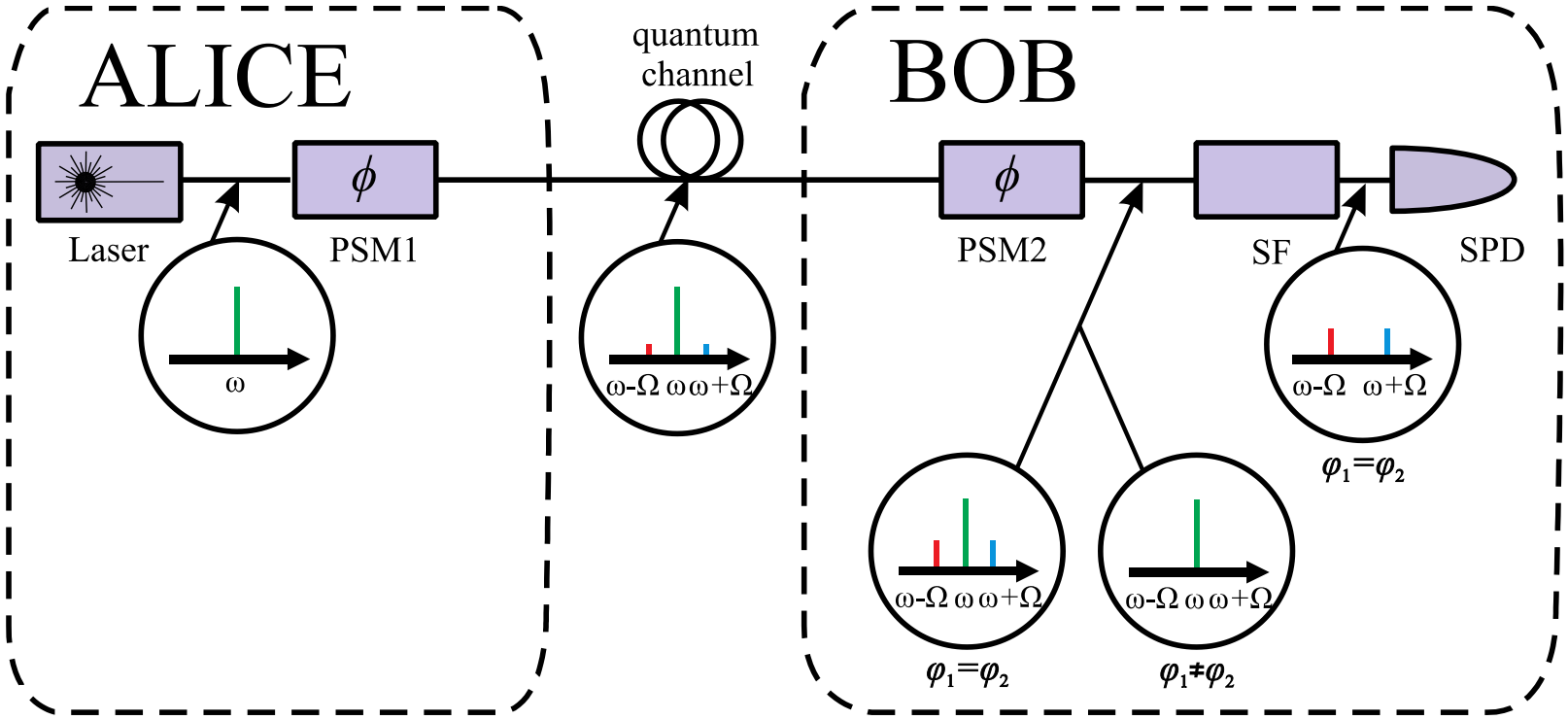
Subcarrier wave Quantum Key Distribution

- Quantum channel is formed at sidebands of an optical carrier as a result of phase modulation
- The optical properties of light at subcarriers are set by modulation parameters used by Alice and Bob
- Each pair of subcarriers can operate as a separate quantum channel



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

Subcarrier wave Quantum Key Distribution



Principle scheme of a Subcarrier wave QKD system (SCW QKD)[1]

1. Jean-Marc Merolla, Yuri Mazurenko et al. //Phys. Rev. Let. V.82, 8, 1656-1659 (1999)

Subcarrier Wave QKD advantages

- Interferometric stability not affected by distance
- Compliance with existing telecommunication lines
- Spectral efficiency up to 40% compared to 4% for modern QKD[1]
- Broad multiplexing capabilities
- Maximum distance limited only by detector properties
- Persistent against natural conditions
- Modulation frequency (i.e. bitrate) not limited by the system architecture

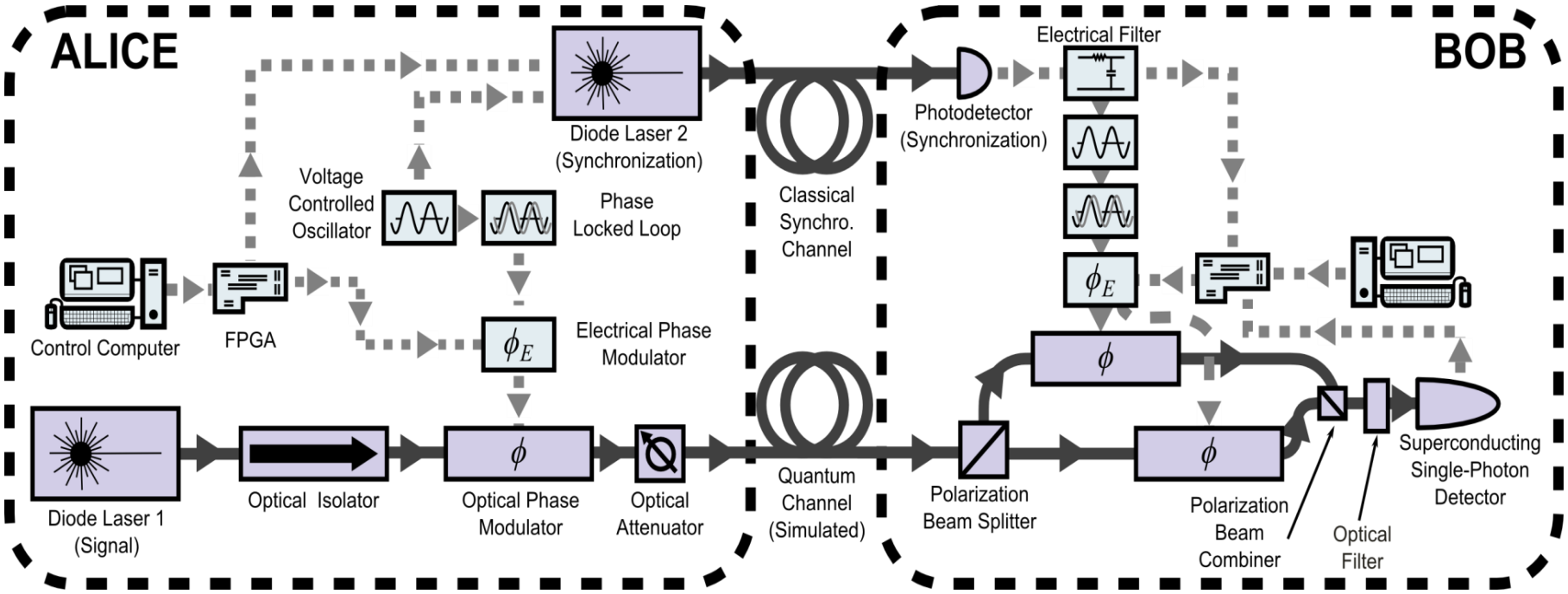
1. J. Mora, A. Ruiz-Alba, J. Capmany el al. // Opt. Lett. 37, 2031-2033 (2012).

Progress in subcarrier wave QKD development

- WDM synchronization at moderate distance (40 km) [1]
- Subcarrier multiplexing [2-5]
- Decoy-state protocol [7]
- BB84 protocol with strong reference (μ=1) [4-6]
- Bitrate: 20 kbit/s at 40 km [1,3]

[1] O. Guerreau, J.-M. Merolla et al. //IEEE J. Sel. Top. Quantum Electron. 9(6), 15331540 (2003)
[2] A. Ortigosa-Blanch, J. Capmany // Phys. Rev. A 73, 024305, (2006).
[3] J. Mora, A. Ruiz-Alba, J. Capmany el al. // Opt. Lett. 37, 2031-2033 (2012).
[4] J.Capmany // Opt.Express 17(8), 6457-6464 (2009).
[5] J. Capmany, C.R. Fernandez-Pousa // J. Lightwave Technol. 29(20), 3061-3069 (2011).
[6] O. Guerreau, F. J. Malassenet, S. W. McLaughlin, J.-M. Merolla // IEEE Photon. Technol. Lett. 17(8), 1755 - 1757 (2005).
[7] S. Bhattacharya and P. Kumar // J. Opt. Soc. Am. B 30, 782-787 (2013)

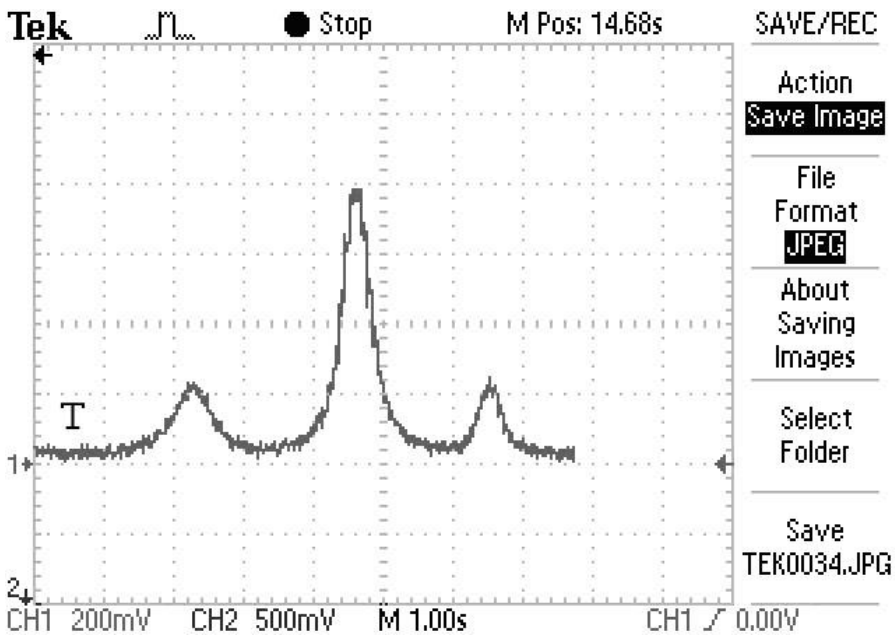
Subcarrier wave QKD setup

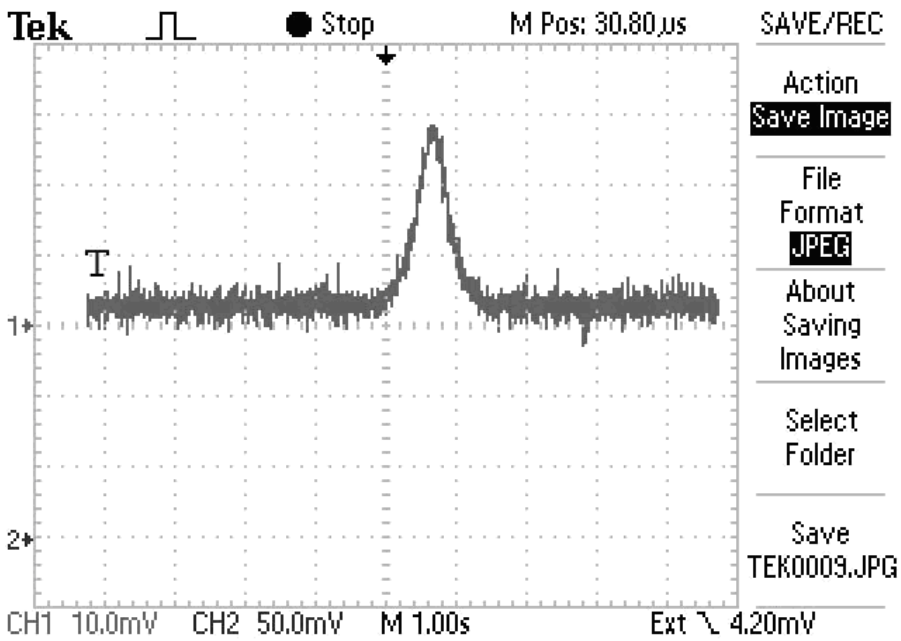


Principal scheme of the developed Subcarrier wave QKD system


КВАНТОВЫЕ
КОММУНИКАЦИИ

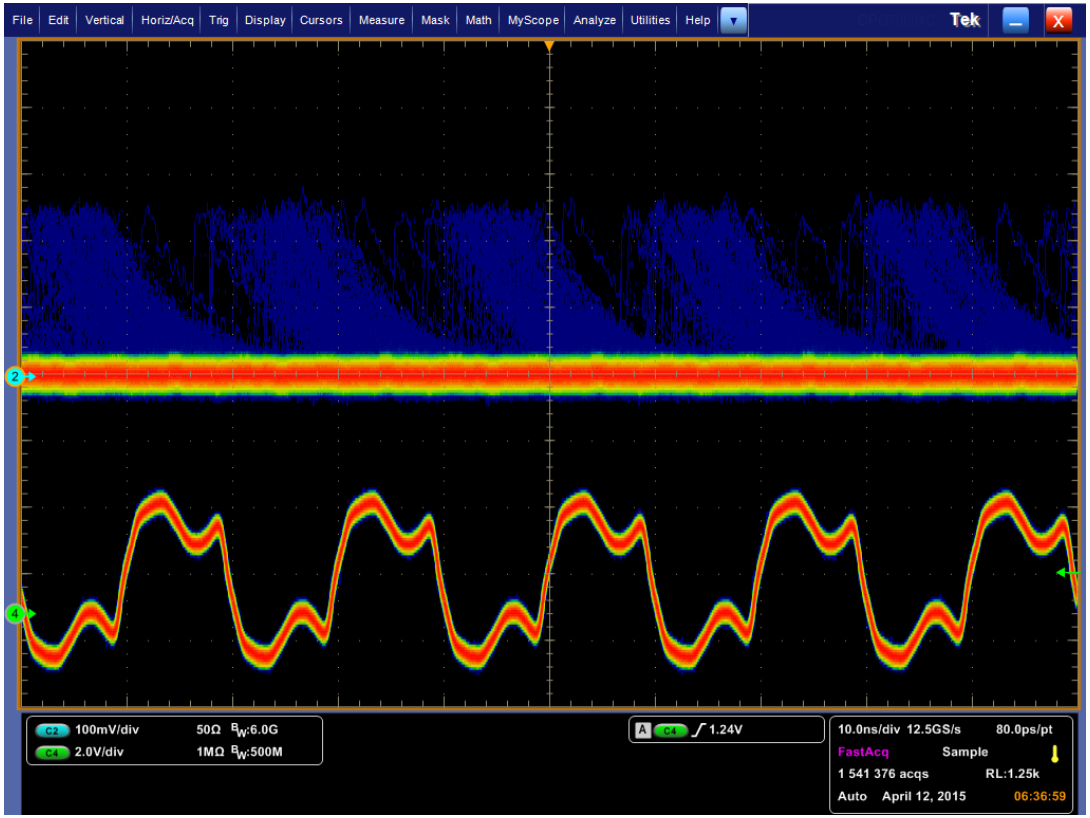
Quantum channel formation





Optical signal spectra at Alice output in the case of constructive (left) and destructive (right) additions of high-frequency phase modulation signals

Optical detector response



Oscillogram of registered change of SNSPD response (above) based on relative phase introduced by Alice and Bob (below).

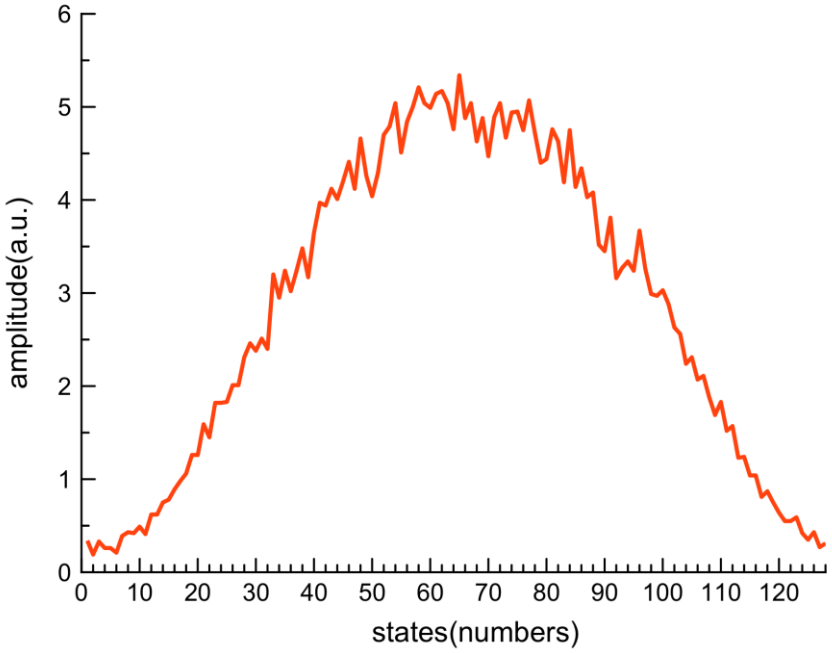
Quantum signal filtration

A thermally stabilized FBG optical filter is used for quantum channel separation in Bob module.

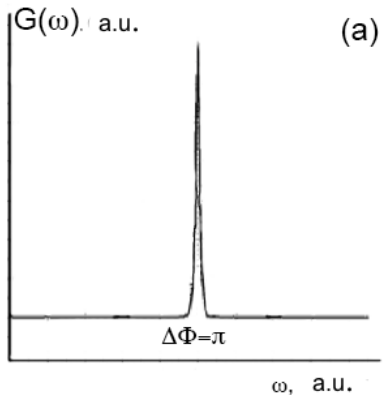
- Filter bandwidth: 7.5 GHz
- Reflection coefficient: > 99.99%
- Extinction ratio: > 40 dB
- Loss: 1 dB
- Long-term stability: tested for 1 month

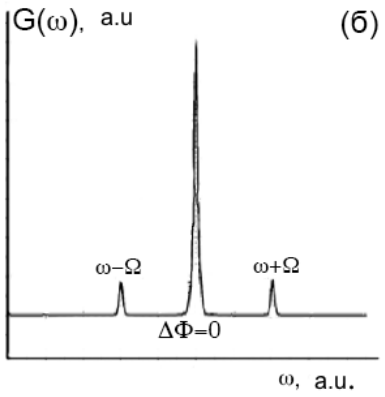
Synchronization of sender and receiver modules

- Performed in a separate optical fiber
- Two step procedure:
  - VCO frequency adjustment
  - Automatic phase calibration
- Calibration parameters:
  - Calibration period: 10 ms
  - Key generation period: 50 ms
  - Number of phase states: 4
  - Phase setting accuracy: 2.4 degrees



Electrical modulating signals



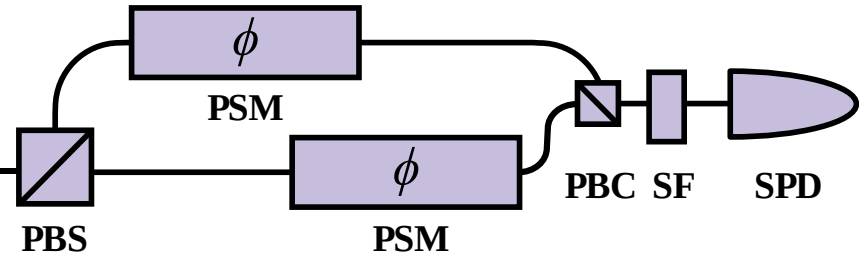




Achieved visibility
V > 98.5%

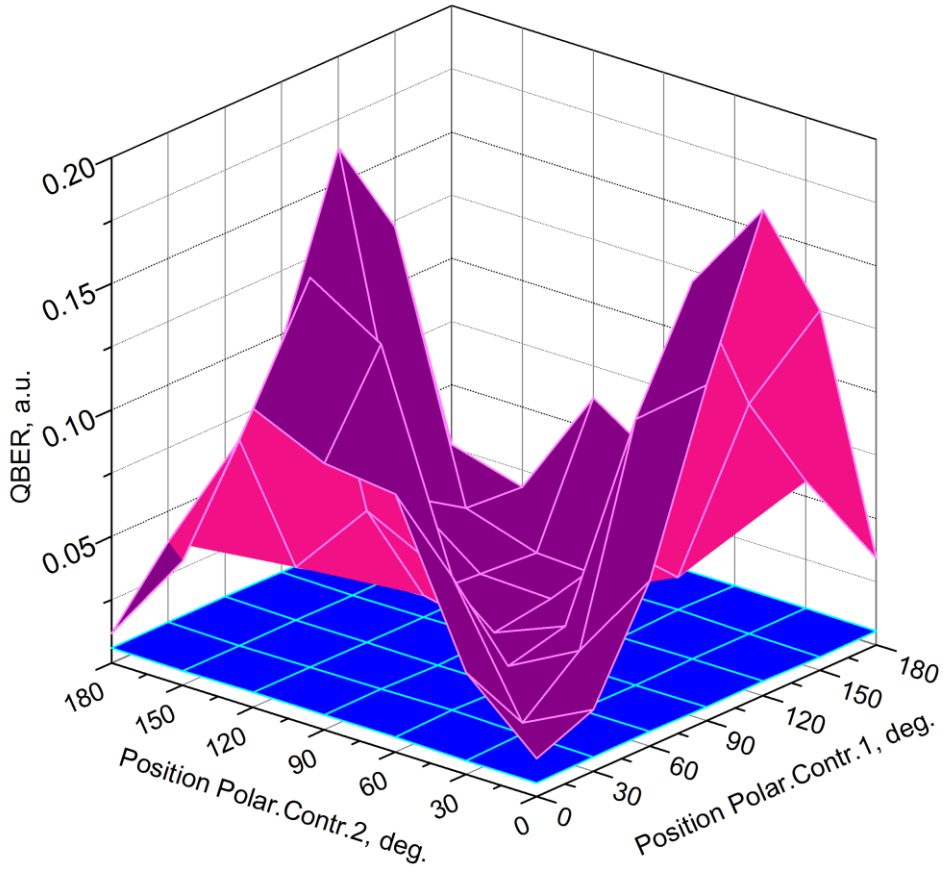
Control signal summation result depends on the relative phase shift

Polarization dependence compensation



Compensation scheme:

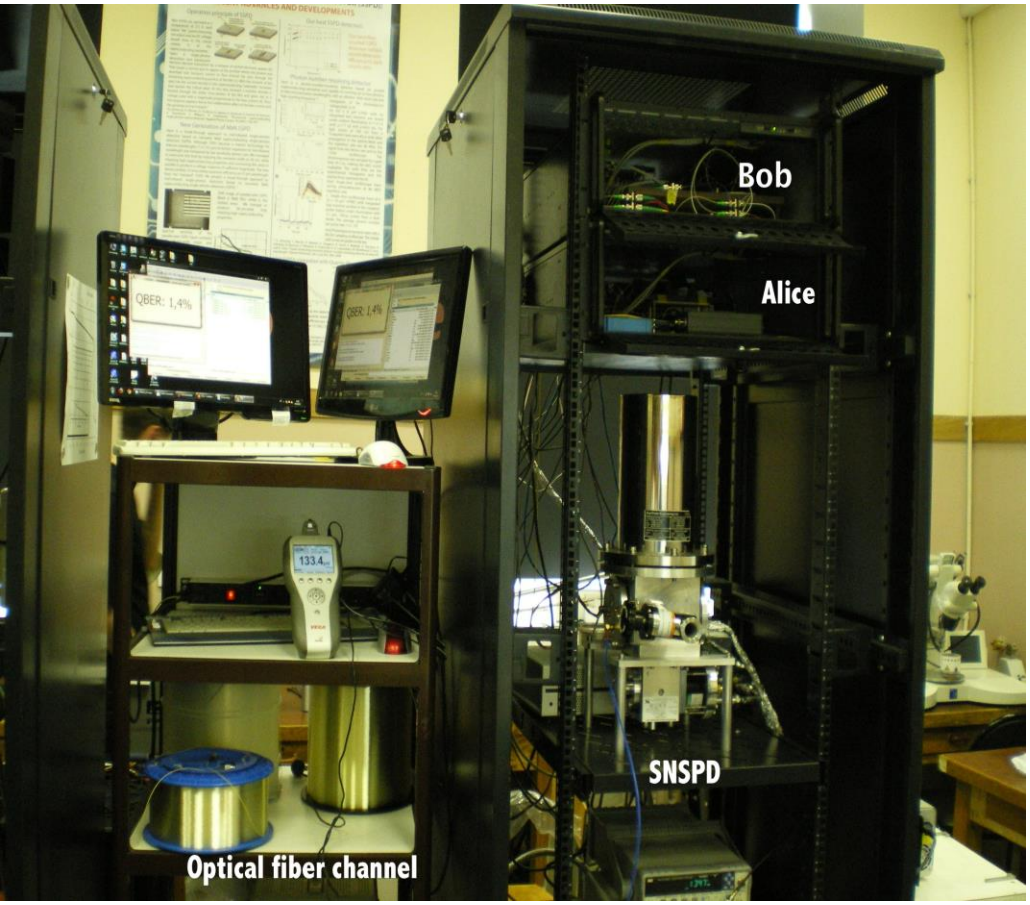
PBS – Polarization Beam Splitter,
PSM – Phase Shift Modulators
PBC – Polarization Beam Combiner
SF – Spectral Filter
SPD – Single Photon Detector



Loss in Bob module: 6,4 dB

Dependence of QBER on polarization distortion value.
Purple surface – without, blue surface – with the compensation scheme.

Experimental setup



- Central wavelength: 1550.12 nm
- Laser spectral width: 5kHz
- Modulation index: 0.05
- Total signal power: 257 pW
- Mean photon number: 1
- Modulation frequency: 4.2 GHz

- Clock frequency: 100 MHz
- Synchronization frequency: 10 MHz
- Loss in the receiving unit: 6,4 dB
- Total Loss in the optical channel: 45 dB

- SNSPD quantum efficiency: 20%
- Dark count rate: 10 Hz

Experimental subcarrier QKD setup with a superconducting nanowire single photon detector (SNSPD)

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 can be removed:

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

- These conditions are naturally satisfied in the SCW approach
- Reference monitoring not implemented in the test-bed system

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

Key generation rate. Theory

- Secure key rate is calculated using the formula:

$$F_s = F \cdot (\Delta \cdot (1 - h(Q/\Delta)) - h(Q)))$$

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

- Single photon fraction is calculated using Poissonian statistics:

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

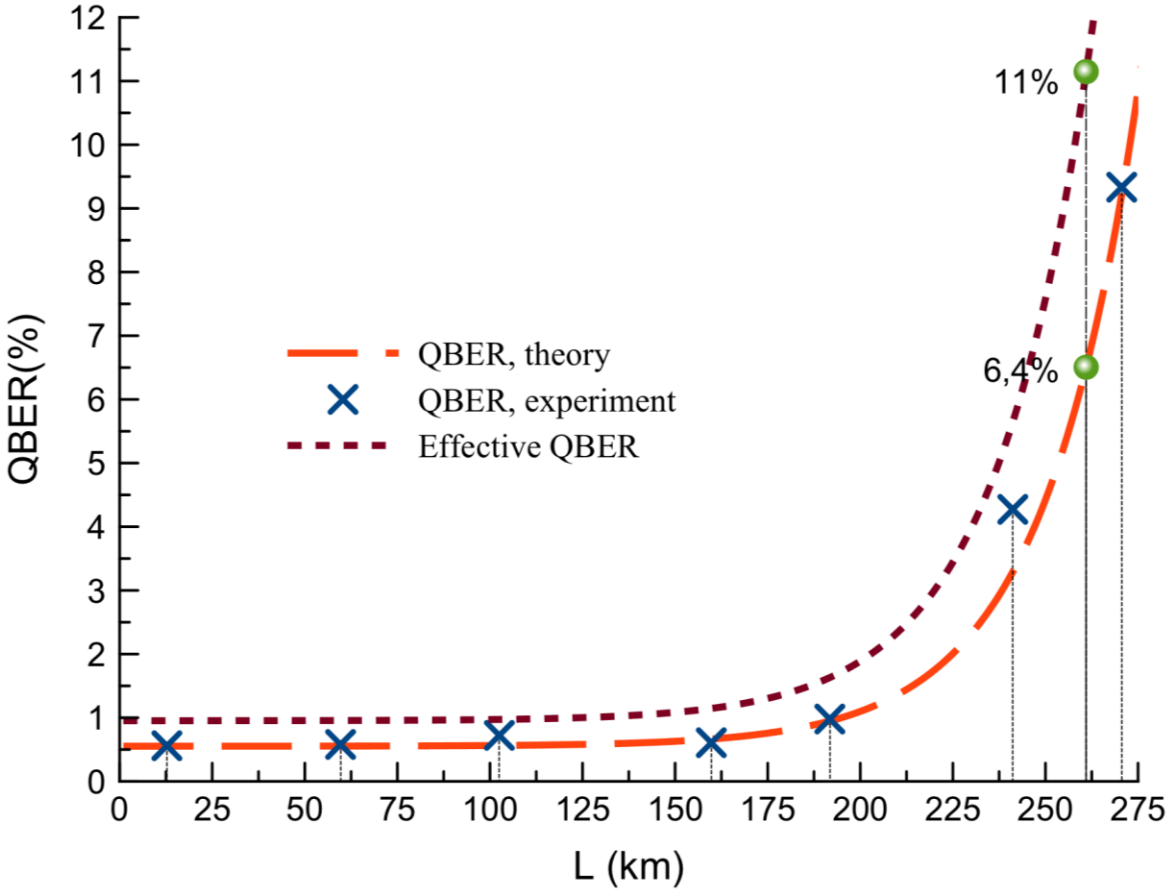
QBER Calculation

- QBER value can be calculated as:

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

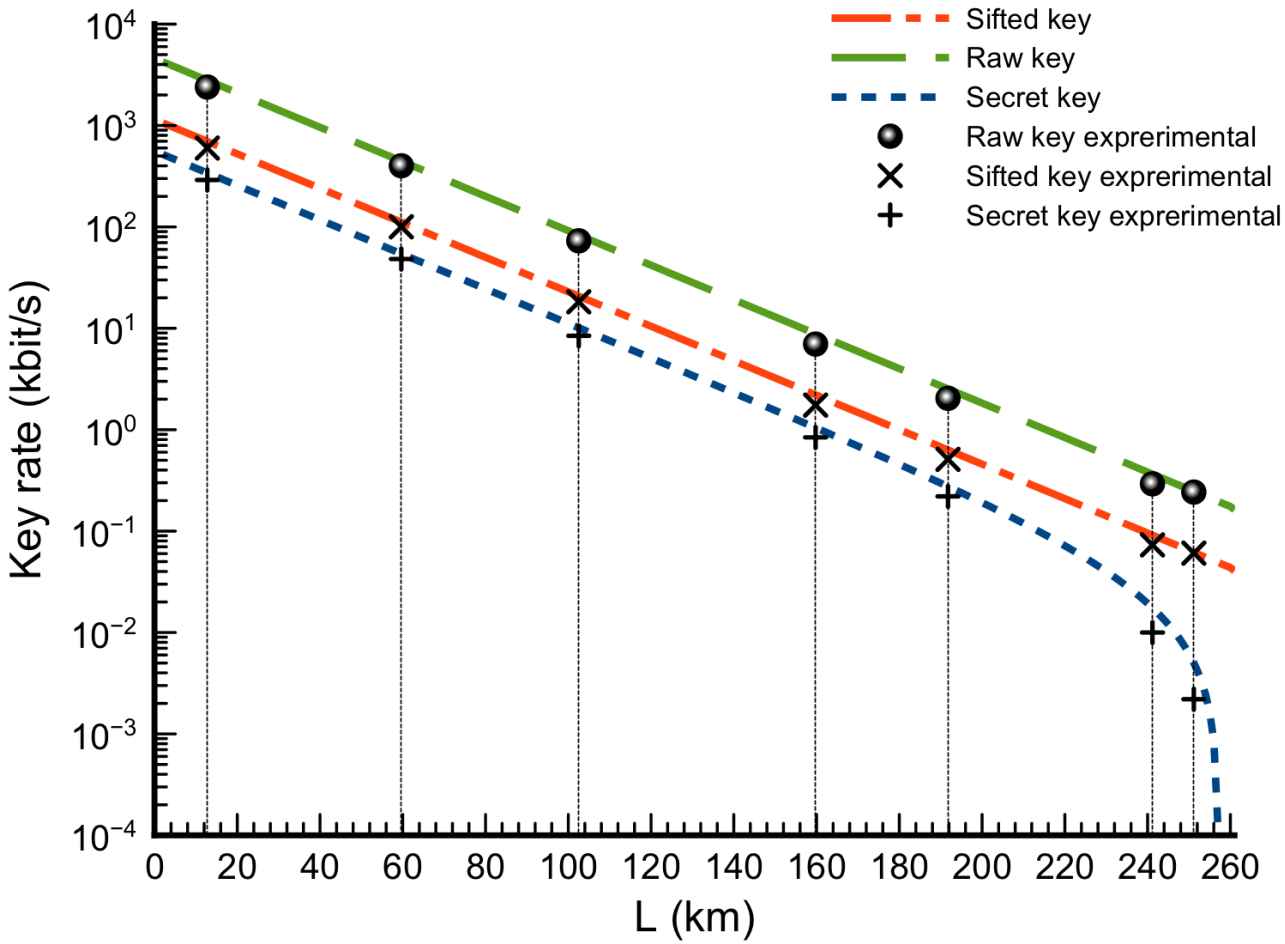
where **V** is interference pattern visibility,
β is the loss in Bob module,
p is the dark count probability per bit,
α is the optical fiber attenuation coefficient at the central wavelength,
L is the optical fiber length and is the detection efficiency,
μ is mean photon number,
η is quantum efficiency of the SNSPD.

QBER and experimental results



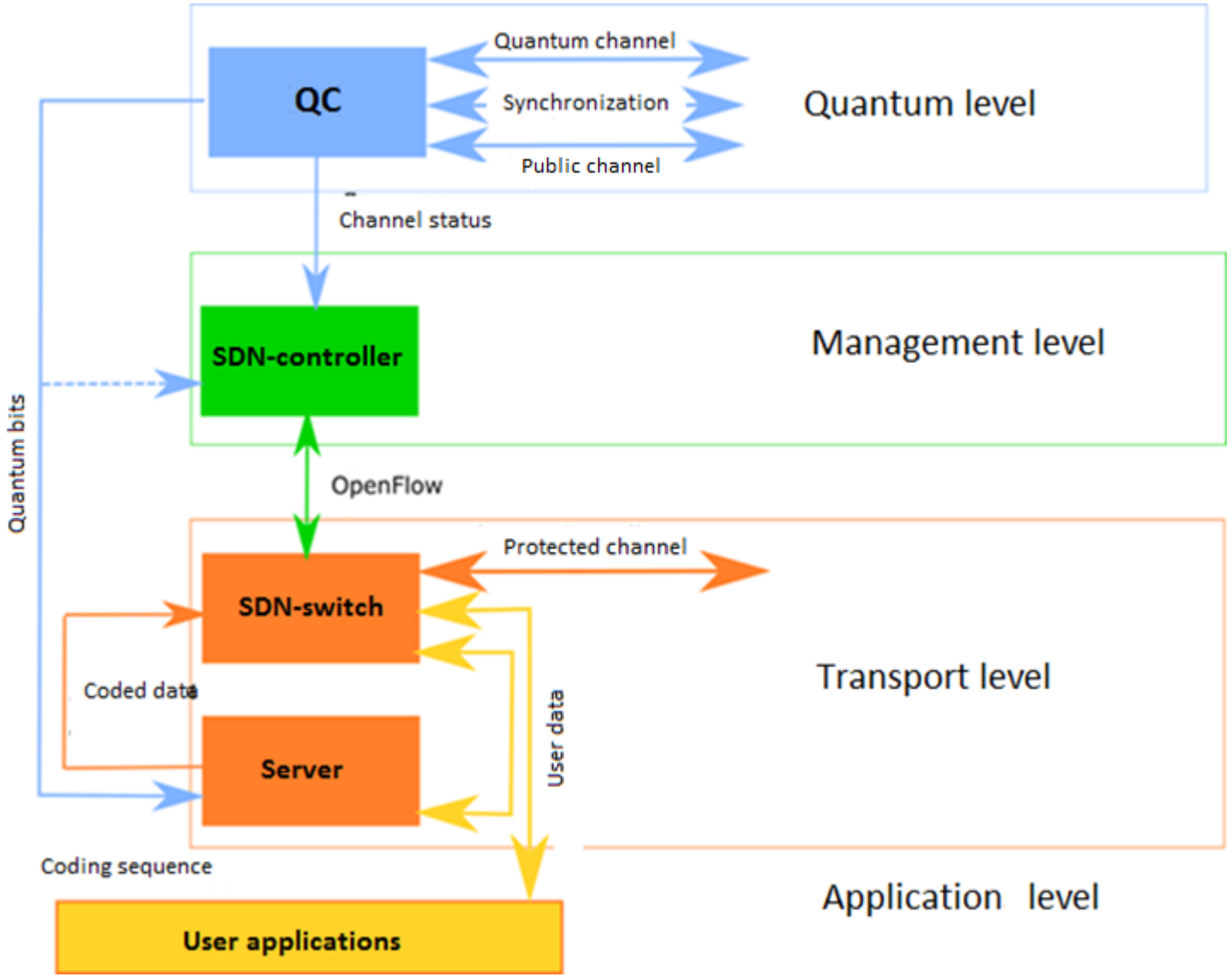
BB84 protocol with strong reference operates with a key fraction defined by Δ, effectively increasing the QBER by its inverse value

Key generation rate. Results

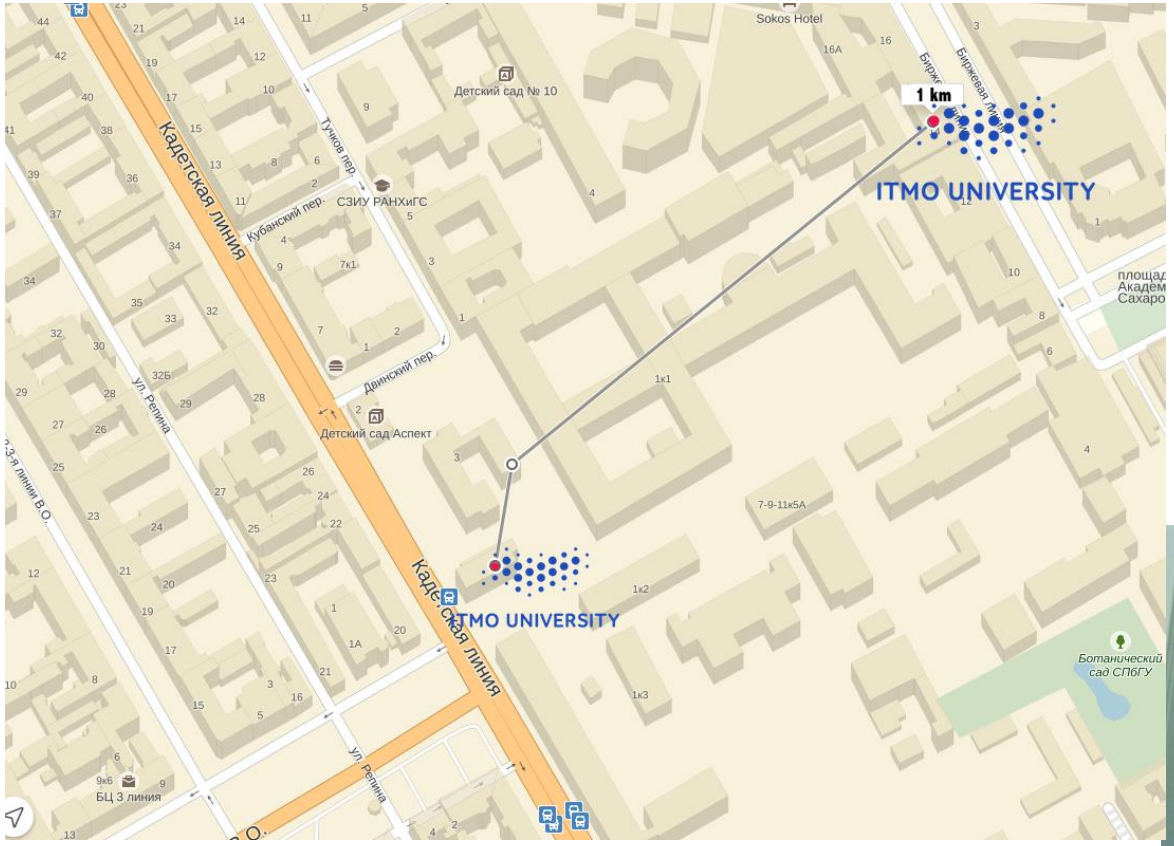


Experimental and calculated key rates depending on transmission distance

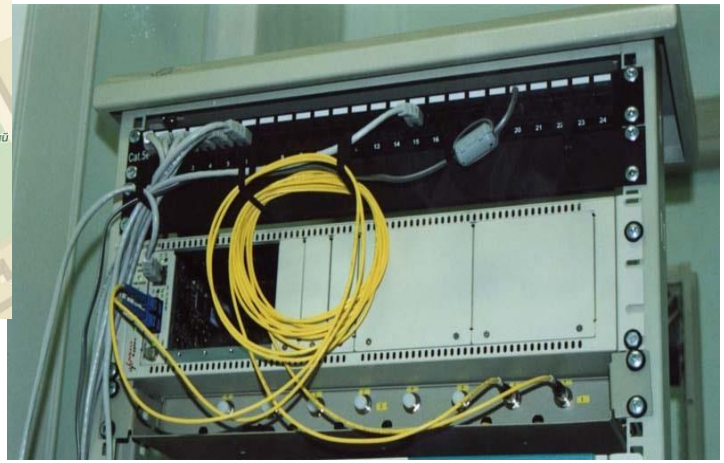
Quantum node scheme



Demonstration in a metropolitan network

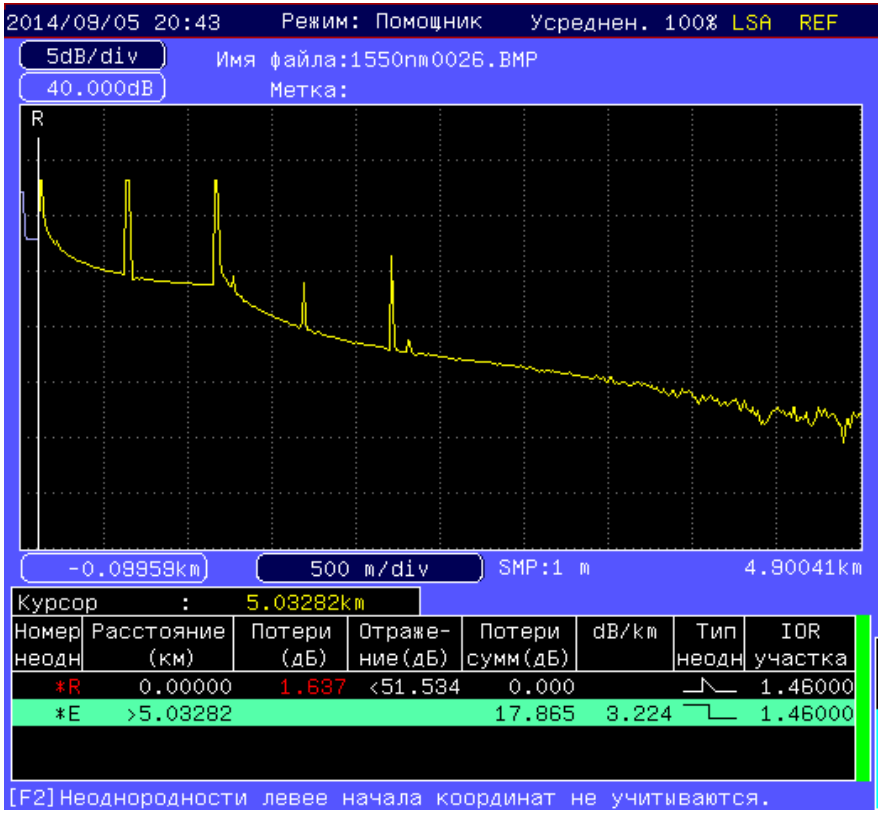


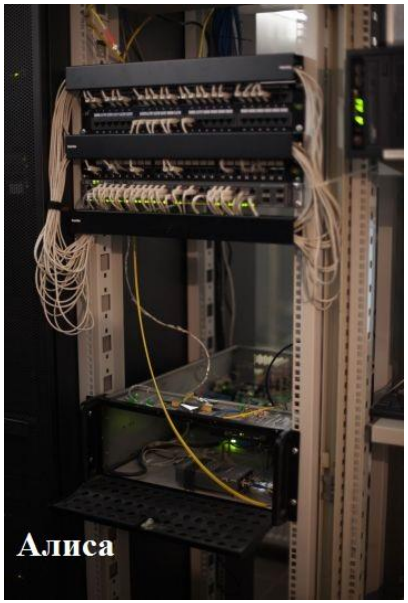
- Location:
  ITMO University
  Saint Petersburg
- Number of nodes: 2
- Channel loss: 1,6 dB
- Channel length 1 km
- Medium: telecom optical cable (SMF-28 fiber)

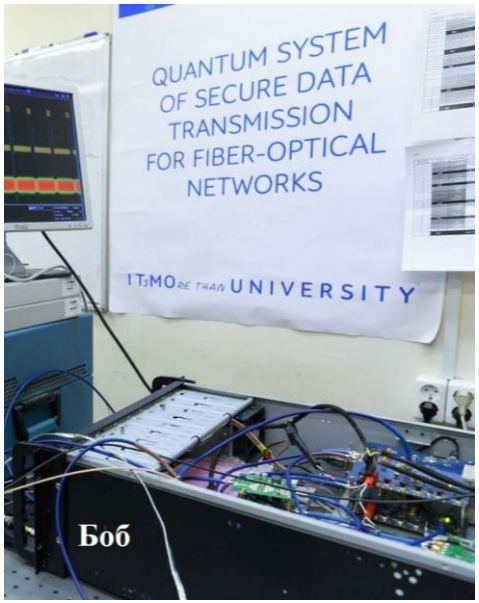


Network parameters

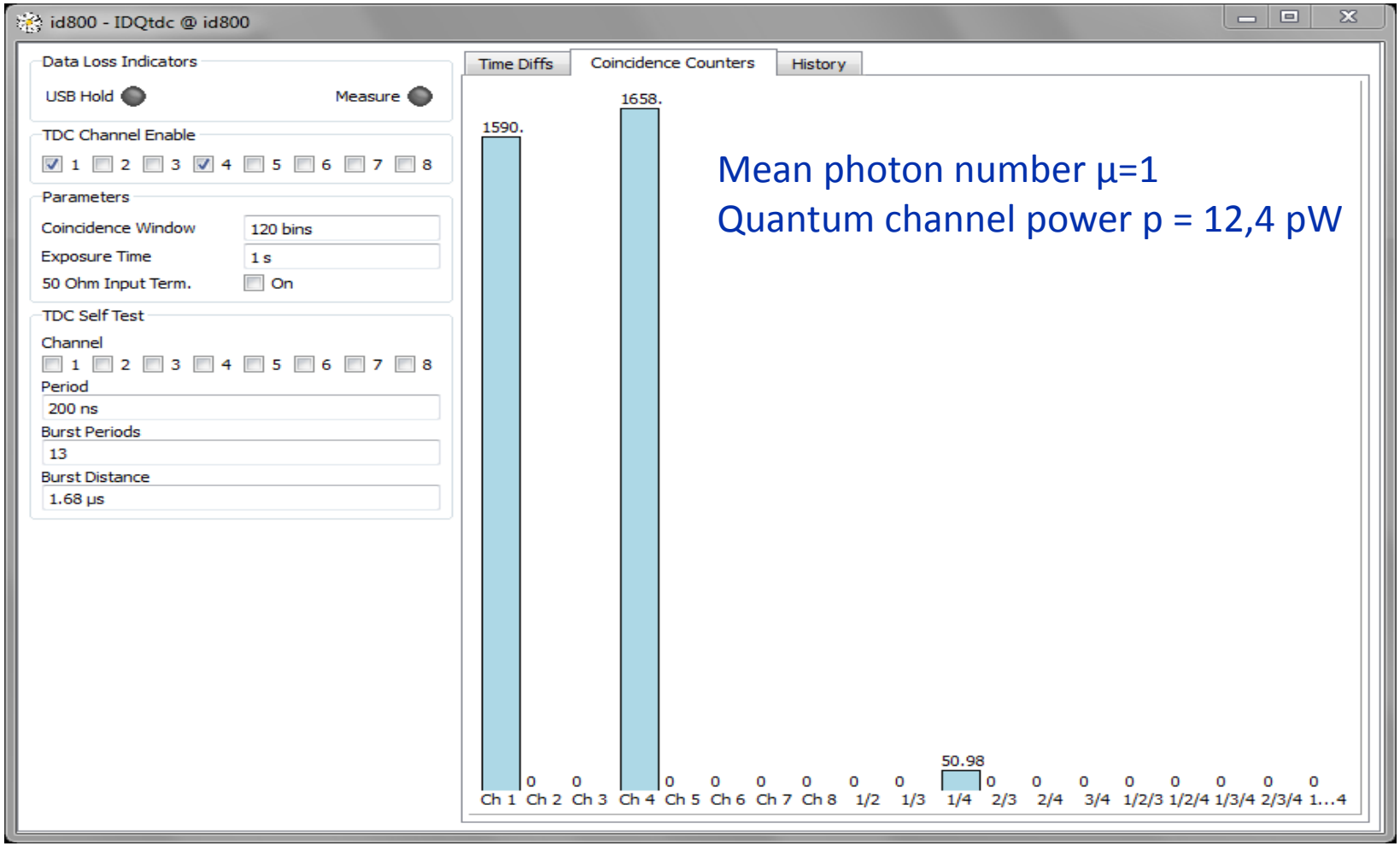
The number of welding and joining points – 4







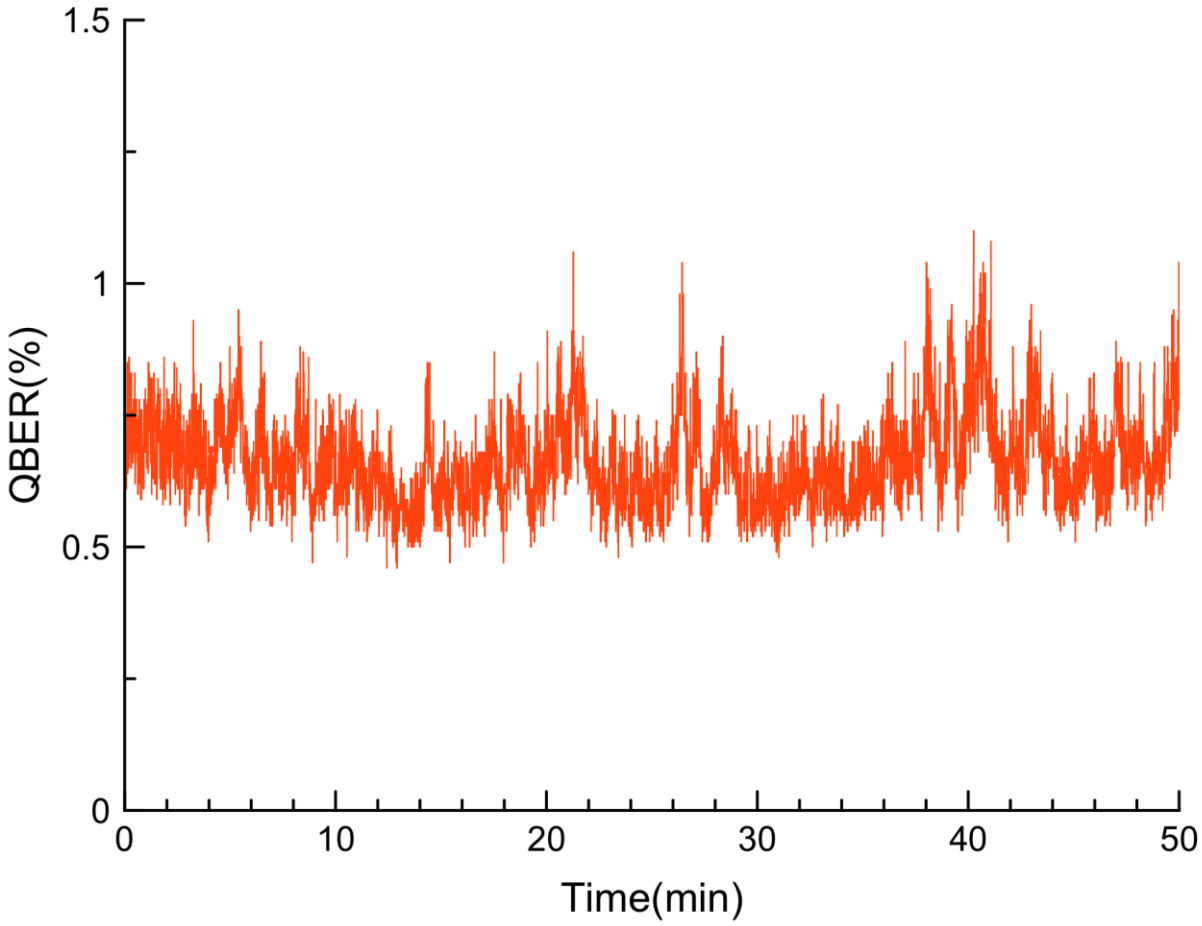
Multi photon state number control



Experimental results

Key number	Sifted key length, byte	QBER, %	Key generation rate, Kbit/s	Calculated key generation rate for 50 km (10 dB), Kbit/s
0000E149	11647	0,87	931	135
0000E14A	11729	0,91	938	136
0000E14B	10523	1,2	841	122
0000E15A	15205	1,1	1216	176
0000E15E	16249	1,05	1299	189
0000E168	14564	0,94	1165	169
Mean value:	**13319**	**1,01**	**1065**	**155**

Dynamic of QBER fluctuation



QBER fluctuations in time monitored in the course of normal system operation

ITMO University test beds

- **Saint Petersburg** (ITMO University quantum network)

The first metropolitan network in Russia

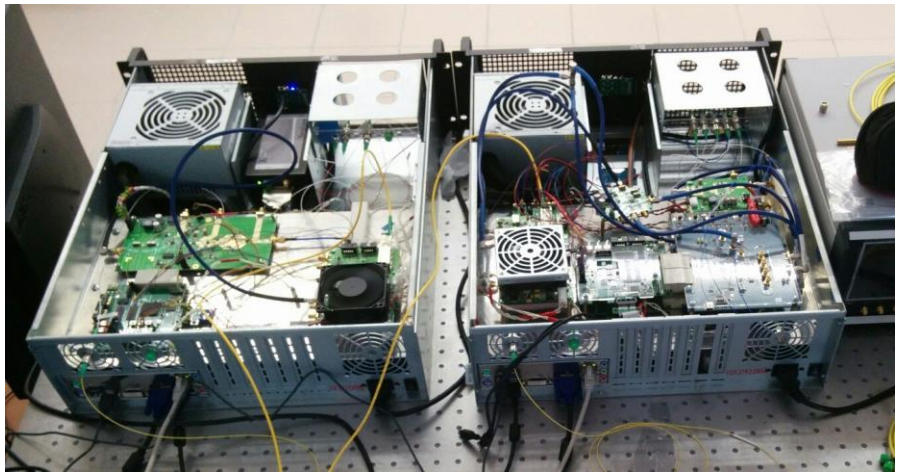
- **Kazan** (Collaborative project with telecom operator)

Multi node quantum network building

- **Samara** (Collaborative project with IT-company)

Software defined quantum networks development

Kazan quantum network





Fiber length 1 km

Insertion loss – 0,5 dB

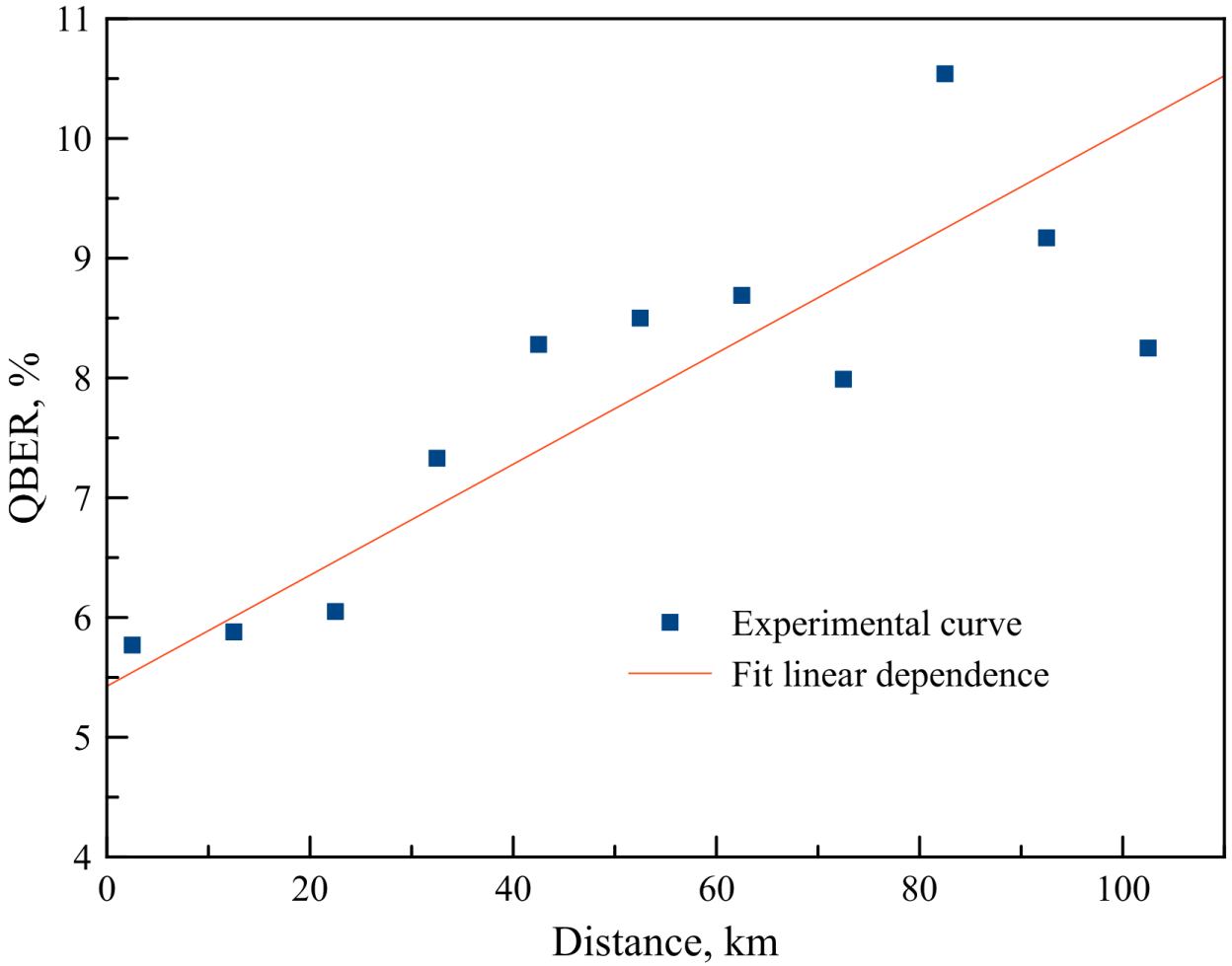
Detector type – APD

Pulse generation rate – 100 MHz

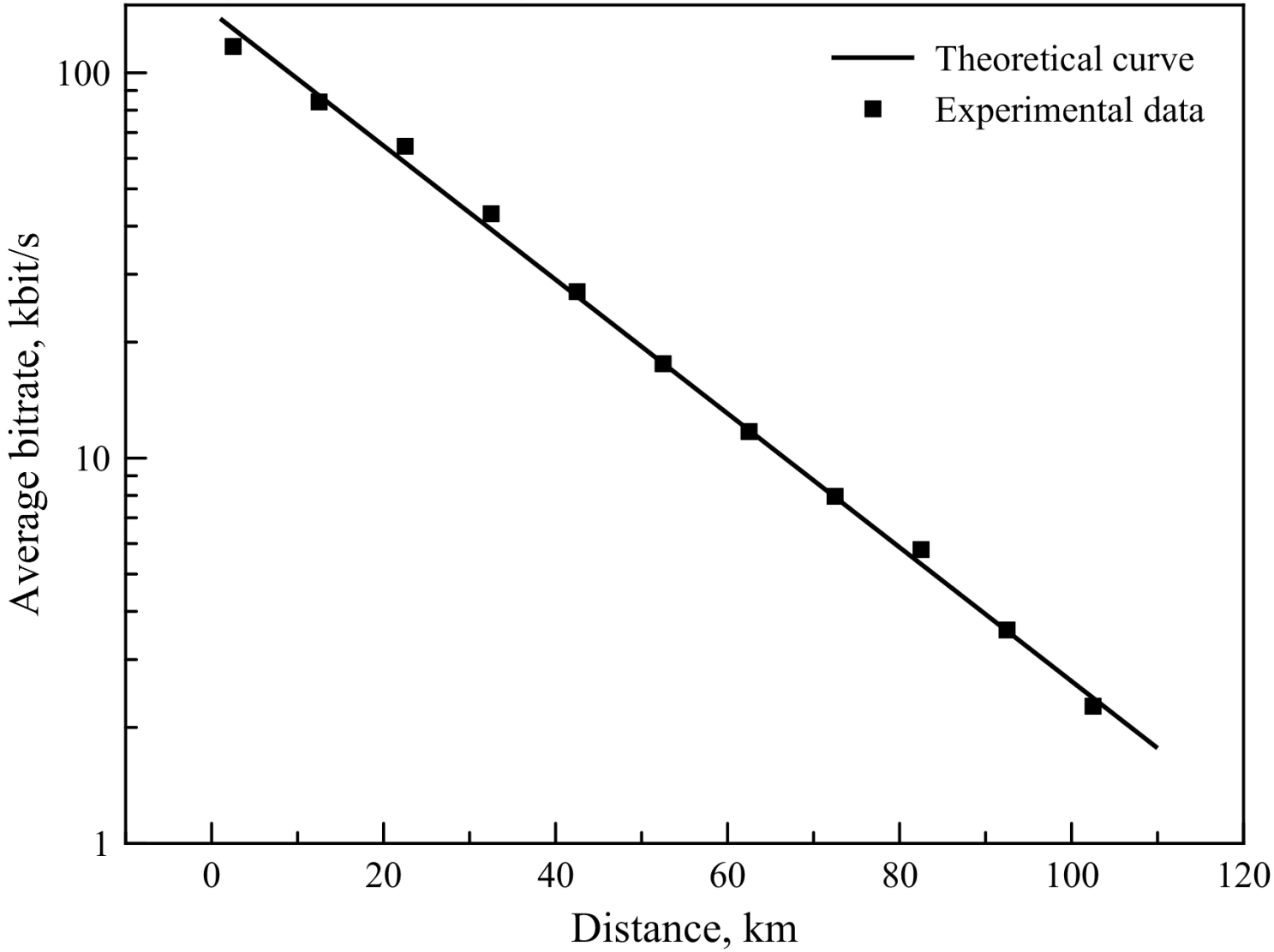
Detector quantum efficiency – 7,5%

Dark count probability 10^{-6}

Results verification: Kazan quantum network with APD-detector system



Secure key rate dependence on distance



Conclusion

- We demonstrated quantum key distribution using SCW method at **1,06 Mbit/s** rate in an metropolitan network
- The system is robust against environmental fluctuations and has optical synchronization
- At **43 dB** channel loss, the quantum bit error rate did not exceed 5.5%, thus allowing using BB84 protocol with strong reference for secure key generation
- Two test beds in Saint Petersburg and Kazan with different detectors type are created: for SSPD max. distance **265 km** and for APD max. **102 km** possibility was experimentally demonstrated



ITMO UNIVERSITY

Thank you for you attention!

agleim@qcphotonics.com

Berlin, 2016