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

Artur Gleim\textsuperscript{1,2}, Vladimir Egorov\textsuperscript{1}, Simon Smirnov\textsuperscript{1}, Vladimir Chistyakov\textsuperscript{1}, Oleg Bannik\textsuperscript{1}, Andrey Anisimov\textsuperscript{1}, Sergei Kynev\textsuperscript{1}, Sergei Khoruzhnikov\textsuperscript{1}, Sergei Kozlov\textsuperscript{1}, Vladimir Vasiliev\textsuperscript{1}

agleim@qcphotonics.com

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

Photonics-2016, Berlin
Our research team:
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

\[ E = Ae^{i\omega t} + iAAa \cdot \cos\left(\frac{\varphi_a - \varphi_b}{2}\right) \cdot \left( e^{i\left((\omega+\Omega)t+\frac{\varphi_a+\varphi_b}{2}\right)} + e^{i\left((\omega-\Omega)t+\frac{\varphi_a+\varphi_b}{2}\right)} \right) \]
Subcarrier wave Quantum Key Distribution

Principle scheme of a Subcarrier wave QKD system (SCW QKD)\(^1\)

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

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]

Previous result

- Demonstrated SCW QKD with 180 bit/s rate at 200 km distance operating with a two-state phase protocol\(^1\)

Aims of this work

- Increase SCW QKD key generation rate and maximum distance
- Develop passive polarization distortion compensator
- Develop practical SCW-QKD network in optical telecom fiber

Polarization insensitive 100 MHz Clock Subcarrier Quantum Key Distribution over 45 dB Loss Optical Fiber Channel

Subcarrier wave QKD setup

Principal scheme of the developed Subcarrier wave QKD system
Polarization insensitive 100 MHz Clock Subcarrier Quantum Key Distribution over 45 dB Loss Optical Fiber Channel
Electrical modulating signals

Control signal summation result depends on the relative phase shift

 Achieved visibility $V > 98.5\%$

Polarization insensitive 100 MHz Clock Subcarrier Quantum Key Distribution over 45 dB Loss Optical Fiber Channel
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
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

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

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, $\Delta$ – single photon fraction, $h(x)$ – Shannon binary entropy function

Single photon fraction is calculated using Poissonian statistics:

$$\Delta = 1 - \frac{1}{e} \left( (1 + \frac{m}{e}) - e^{-m} \right)$$
QBER value can be calculated as:

\[ QBER = \frac{1}{2} V + \frac{p}{4} \left( \frac{1}{10} \right)^{L+10} \]

where 
- \( V \) is interference pattern visibility,
- \( \beta \) is the loss in Bob module,
- \( p \) is the dark count probability per bit,
- \( \alpha \) is the optical fiber attenuation coefficient at the central wavelength,
- \( L \) is the optical fiber length and is the detection efficiency,
- \( \mu \) is mean photon number,
- \( \eta \) is quantum efficiency of the SNSPD.
QBER and experimental results

BB84 protocol with strong reference operates with a key fraction defined by $\Delta$, effectively increasing the QBER by its inverse value.
Key generation rate. Results

Experimental and calculated key rates depending on transmission distance

Polarization insensitive 100 MHz Clock Subcarrier Quantum Key Distribution over 45 dB Loss Optical Fiber Channel
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)

Polarization insensitive 100 MHz Clock Subcarrier Quantum Key Distribution over 45 dB Loss Optical Fiber Channel
### Network parameters

<table>
<thead>
<tr>
<th>Distance (km)</th>
<th>Loss (dB)</th>
<th>Attenuation (dB)</th>
<th>Loss Sum (dB)</th>
<th>DB/km</th>
<th>Type of segment</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1.537</td>
<td>1.534</td>
<td>0.000</td>
<td></td>
<td>1.4600</td>
</tr>
<tr>
<td>&gt;5.03282</td>
<td></td>
<td></td>
<td>17.365</td>
<td>0.224</td>
<td>1.4600</td>
</tr>
</tbody>
</table>

- The number of welding points – 4
- Operating temperature -
Multi photon state number control

Mean photon number $\mu=1$
Quantum channel power $p = 12.4 \text{ pW}$
## Experimental results

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

![Graph showing QBER (%) vs Distance (km) with experimental data points and a linear fit. The graph demonstrates an increase in QBER with increasing distance.](image-url)
Secure key rate dependence on distance

Average bitrate, kbit/s vs. Distance, km

- Theoretical curve
- Experimental data
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
Thank you for your attention!

agleim@qcphotonics.com

Rochester, 2015