Piotr Rydlichowski

QKD linie implementation between Poznań and Warsaw

61-139 Poznań
ul. Jana Pawła II 10
phone: (+48 61) 858-20-01
fax: (+48 61) 852-59-54
office@man.poznan.pl
www.psnc.pl
Poznań Supercomputing and Networking Center

**Center of e-Infrastructure**
- National Research and Education Network PIONIER
- Research Metropolitan Area Network - POZMAN
- HPC Center
- Data repositories and Digital Libraries Federation

**Center of Research & Development**
- New Generation Networks
- HPC, Grids & Clouds
- Grand challenge applications
- New media and visualization technologies
- Knowledge Platforms
- Future Internet - Technology, Applications and Services for IS
- Cyber Security
- Quantum Communication and Computing - use cases, practical scenarios and connecting/building community
Poznań Supercomputing and Networking Center

PSNC LOCATIONS

- Laboratories
- PSNC HQ
- Data Center
- Living Labs
- Coworking space
- POZMAN network: 287 km fibers, Research community - 110 connections in city and 8 connections in Wielkopolska region
- Backup Data Center
The PIONIER Consortium brings together 21 MAN Networks and 5 HPC Centers

<table>
<thead>
<tr>
<th>Type of connected unit</th>
<th>Number of units</th>
</tr>
</thead>
<tbody>
<tr>
<td>Research institutions</td>
<td>221</td>
</tr>
<tr>
<td>Universities</td>
<td>196</td>
</tr>
<tr>
<td>Post-secondary schools</td>
<td>21</td>
</tr>
<tr>
<td>High schools, secondary schools, primary schools and vocational schools</td>
<td>234</td>
</tr>
<tr>
<td>Healthcare</td>
<td>59</td>
</tr>
<tr>
<td>Public safety</td>
<td>27</td>
</tr>
<tr>
<td>Government administration</td>
<td>27</td>
</tr>
<tr>
<td>Provincial administration</td>
<td>59</td>
</tr>
<tr>
<td>District, municipality and city administration</td>
<td>73</td>
</tr>
<tr>
<td>Other administration</td>
<td>9</td>
</tr>
<tr>
<td>Court and public prosecutor’s office</td>
<td>26</td>
</tr>
<tr>
<td>Cultural institutions</td>
<td>104</td>
</tr>
<tr>
<td>Other educational</td>
<td>27</td>
</tr>
</tbody>
</table>
NLPQT PROJECT

National Laboratory for Photonics and Quantum Technologies

The main goal of the project is development of modern infrastructure in the fields of photonics and quantum technologies with particular attention paid to the needs of industry.

As part of the project, they will be built:

- The National Facility for Generation and Distribution of Reference Optical Sources
- Photonic Technology Laboratories
- Quantum Technology Laboratory
- NIKWIM
- COPEMICS

Photonics is a well-established yet still thriving field of research and technology. It is also behind many innovations which have transformed our lives. Lasers, optical telecommunication, cameras in our phones, LED lighting in our homes, computer screens & TV sets are just a few examples of how photonics has changed technology. As photonics has the potential to enhance innovations across several industries, it is included in Europe's Key Enabling Technologies (KET) of the 21st Century.
The National System for Generation and Distribution of Reference Optical Carrier

Coordinator

PIOTR MASIOWSKI
pima@fizyka.umk.pl
0000-0001-8882-7106

The main goal of the National System for Generation and Distribution of the Reference Optical Carrier is to create an ultrastable laser system that can be linked to an optical atomic clock, along with a distribution network using fiber optic links. The optical reference signal with low phase noise will be sent to the participants of the NLPQT consortium, where it will be available to interested industry partners. The System will enable implementation of a number of services addressed to the photonic, optical, chemical and related industries in the areas listed below:
NLPQT PROJECT

• **Metro QKD** research and operational infrastructure, integration of QKD solutions
  – QKD infrastructure (operational and R&D QKD devices, encryptors and quantum random number generators)

• **Construction of the long distance QKD Poznań - Warsaw link** – June 2022
  – experiments related to quantum communication between University of Warsaw nodes and PSNC in Warsaw.
  – Experiments related to sources and detectors of single photons
  – Integration of the infrastructure with the optical carrier infrastructure
  – Next generation QKD prototypes testing (based on entanglement)
NLPQT PROJECT – METRO QKD SYSTEMS

IDQ Centauris encryptors
IDQ Clavis 3 R&D QKD system
IDQ QUANTIS QRNG
IDQ Centauris 3 production QKD system
PSNC – VSB crossborder testbed

First intercity and international trial in CZ
Ostrava-Cieszyn line – fibre itself 75km, 16 dB
QKD channel in 1550 nm band, will be disturbed by parallel traffic
Line is very close to maximum system performance
QKD system „fibre hungry”, service OOK channel will consume 2 additional optical channels
Offer for additional fibre pair uncompetitive
All data (incl. QKD service channel) moved into bidi DWDM

Management and use case node
DWDM system interconnection
QKD node

First cross-border trial of quantum key distribution sharing fiber line with data and accurate time transmissions

Abstract
The contribution focuses on experimental verification of the QKD system deployment in a multi-domain network environment managed by Czech and Polish National Research and Educational Network (NREN) operators. We demonstrate full functionality of such a solution for transmission of secret keys in boundary conditions, and with this we open up new possibilities for further use of extremely secure communication between two neighboring network entities, and the services built upon it. Moreover, we have shared the cross-border link among strong QKD service channels, accurate time, and classical data channels together with weak quantum channel to reduce the total number of optical fibers needed for transmission. To our
QUANTUM COMMUNICATION ACTIVITIES

TNC21 conference demo – Secure Key Management for Multi Vendor Interoperable Quantum Key Distribution Network

Key Relay using ADVA FSP150
Machine Learning-based Optical and QKD Network Monitoring

ADVA and PSNC

1ADVA Optical Networking, Fraunhoferstrasse 9a, Martinsried, Germany, 82152
2Christian-Albrechts-Universität zu Kiel, Kaiserstr. 2, Kiel, Germany, 24143
3PSNC, Wieniawskiego 17/19, 61-704, Poznań, Poland
mwenning@adva.com

Abstract: We demonstrate a fiber network monitoring system based on machine learning which can detect and diagnose fiber faults and hardware failures in an optical network. Our system also has the capability of monitoring the performance of QKD links.
Quantum-Safe communication solution

ARISTA DCS 7280CR3

4x 10Gbps Encrypted with AES-256

Standard Interface (ETSI REST API - QKD 0.14)

Quantum Channel & Service Channel

ARISTA DCS 7280CR3

IDQ Cerberis XG - Alice

Primary Datacenter

IDQ Cerberis XG - Bob

Backup Datacenter
• The demanding links from the distance point of view were tested first using existing metro QKD equipment
• Procured IDQ Cerberis XG system tested and configured in the lab
• Deployed on sites over 3 days
• ISK (Initial Shared Key) required to start QKD exchange needs to be set manually and physically over each node
• Network addressing scheme to integrate Key, KMS and MGMT services
• At the first stage only point to point links were deployed
• At the second stage trusted node approach and key relay mechanism was implemented.
• Monitoring services implementation with NOC.
• System under constant adjustment and modification (new software, new consumers)
• Measures to improve budget margin on two longest, critical links.
• System uses COW 4 states protocol
• System uses four different channels – quantum, service, KMS, managements. Apart from that we have key and encrypted traffic services. All these elements can be potentially multiplexed and with different combinations
Keys, KMS, MGT services can be implemented on different physical interfaces

System uses **three** dedicated fibers – one fiber for quantum channel and one pair for service and sync channel (can be multiplexed with existing traffic and systems)
• Does not need perfect single-photon devices
• Uses phase-randomized weak coherent pulses
• Decoy states help deal with PNS (Photon Number splitting) attacks but limits performance
• Systems during initialization need time to align monitor and data timebins
• Bits are encoded using pair of coherent and vacuum pulses
• Monitoring line (MZ) checks coherence between pulses
• Bob measures TOA of coherent pulses and reports to ALICE clicks but without exact timeslot. Alice discloses if it was key generation or decoy state.
• **QKD protocols and its implementation are still under theoretical analysis**
SUMMARY

• Implementation of Metro and long distance QKD links
• Infrastructure supports various research activities
• Possible support for EuroQCI and EuroQCS initiatives
• Cooperation with vendors and R&D partners
• Integrating and supporting communities