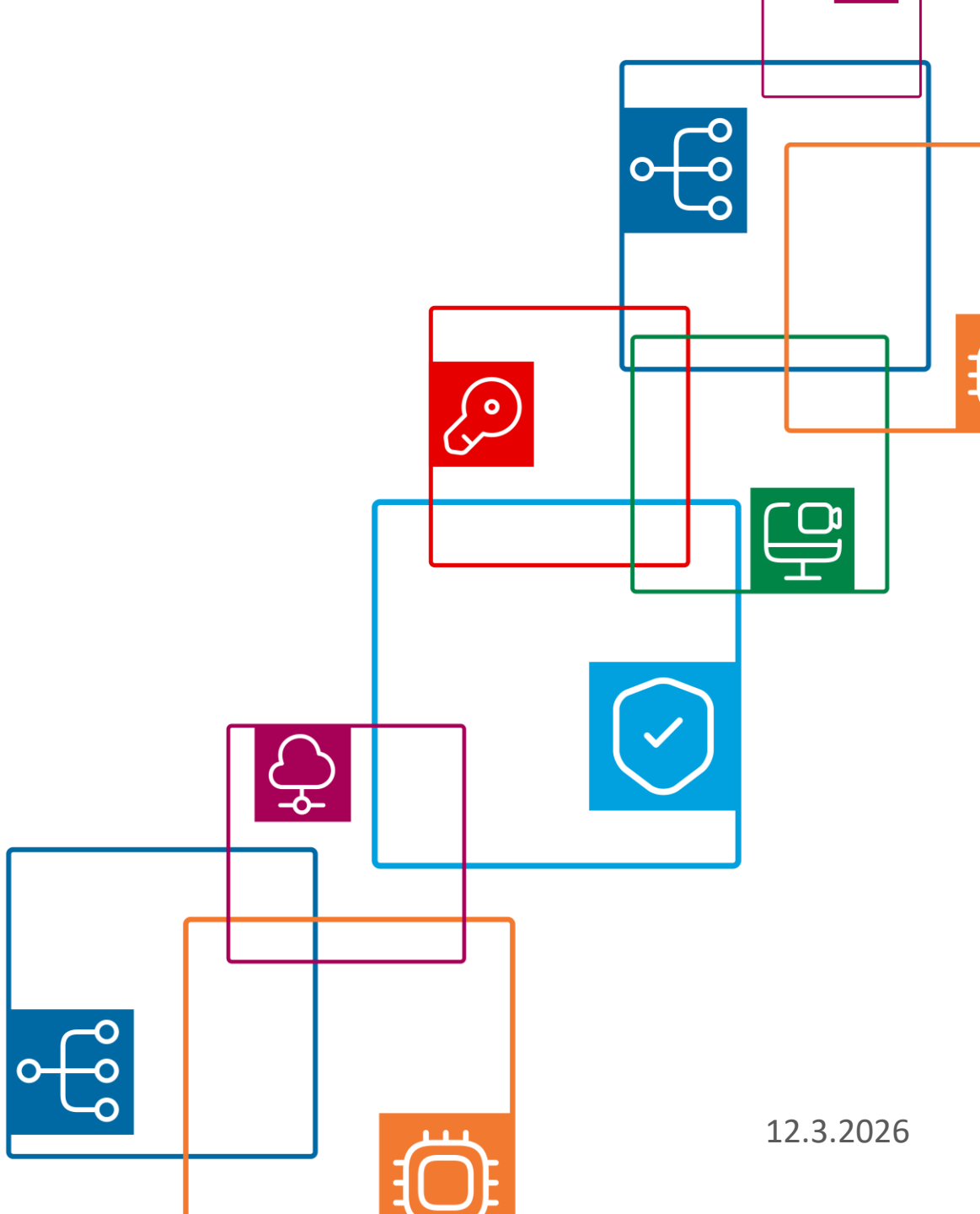
cesnet

Přenosy velmi přesného času a QKD ve sdílených sítích

Josef Vojtěch

Seminář Sítě FTTx v roce 2026, Brno



12.3.2026

Agenda – Přesný čas a QKD

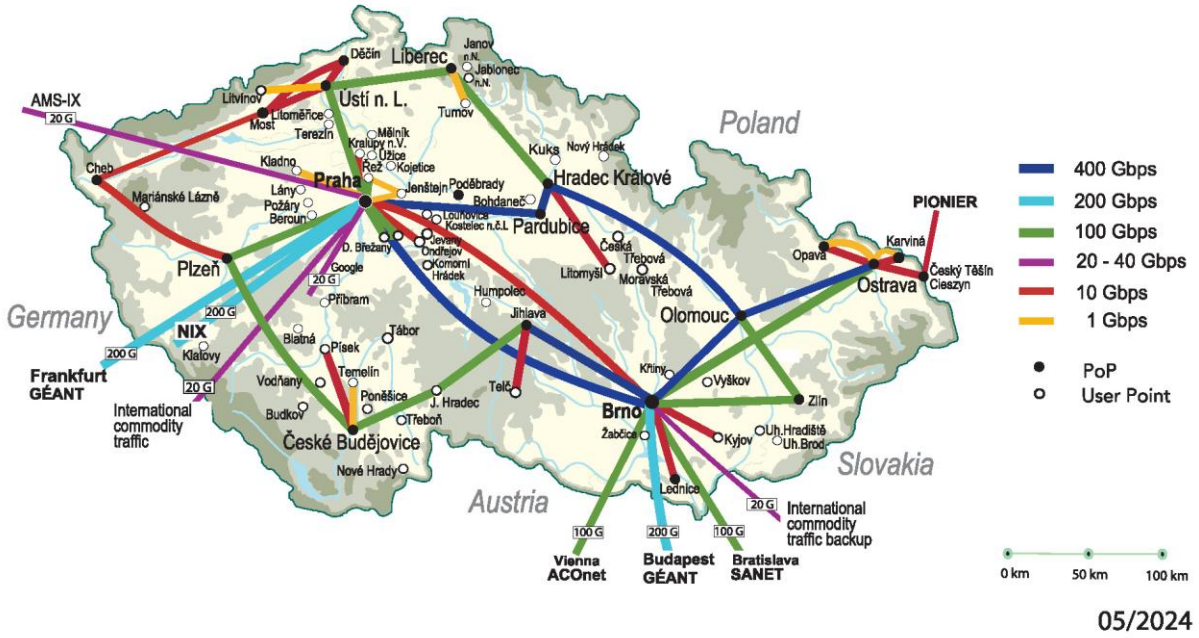
- Motivace
  - Proč přesný čas?
- TF síť CESNETu
- GÉANT
- Laboratorní měření – souběh přesného času a
- Měření na reálné trase

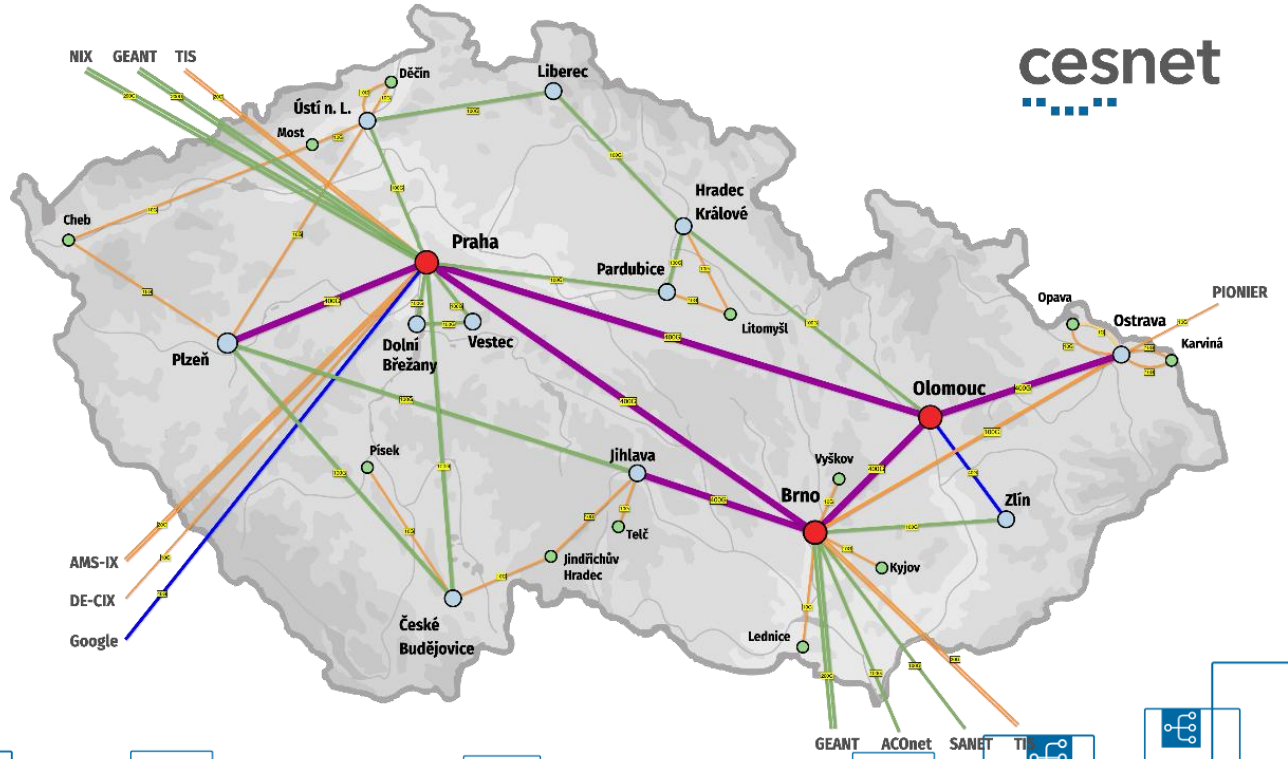
- Motivace
  - Proč QKD?
- Souběhy QKD a přesného času a dat
  - Nekoherentních a koherentních signálů 400 Gb/s.
  - Spontánní Ramanův rozptyl
- Závěr

- Poděkování spoluautorům
  - Ondřej Havliš, Tomáš Novák, Vladimír Smotlacha, Jaromír Šíma, Martin Šlapák, Jan Radil

CESNET – Přesný čas a QKD

- Založen 1996 jako zájmové sdružení právnických osob
- Členové: veřejné a státní vysoké (26) školy, akademie věd
- Přidružení členové: Extreme Light Infrastructure ERIC,Národní muzeum, Moravská galerie v Brně,……





Motivace – Přesný čas a QKD

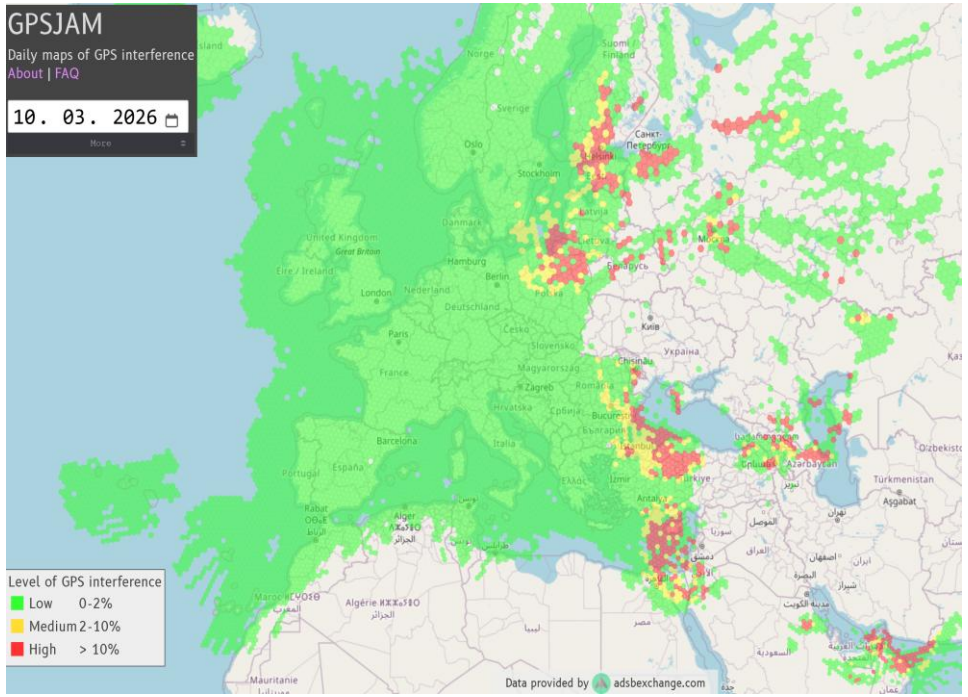
- **Kde jsou přesný čas a stabilní frekvence potřebné?**

Transport

Telecomm

Data centers

Finance



Defence

Power grids

Navigation

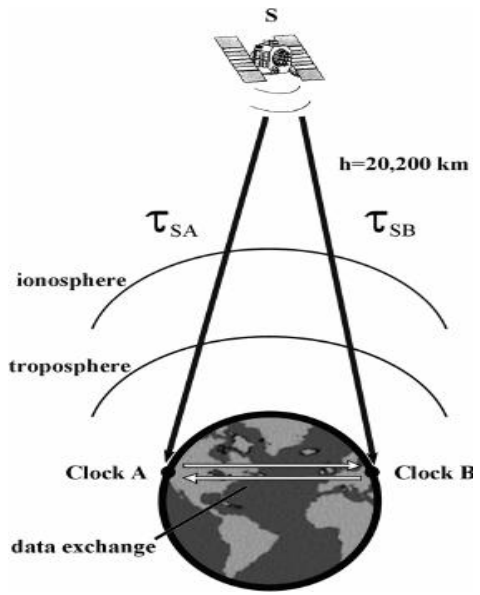
Úvod – Přesný čas a QKD

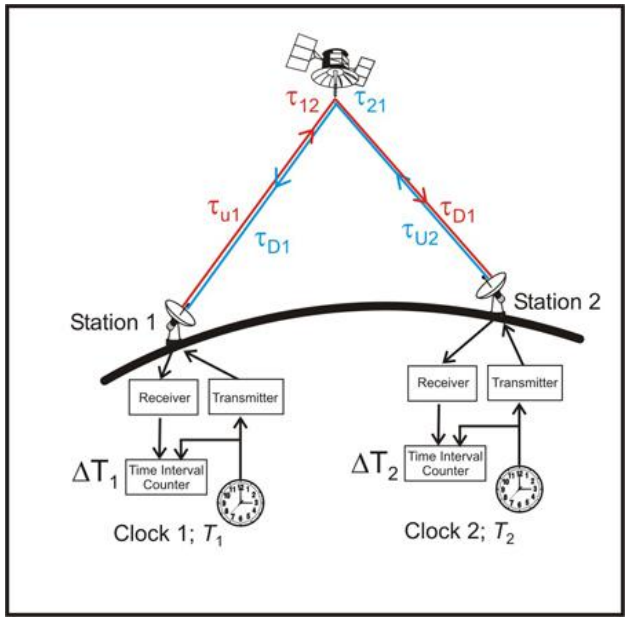
GNSS (GPS, Galileo, Glonass, Beidou)

- Běžný přijímač s výstupem 1 PPS
  - chyba 50 ns – 1μs
- Metoda Common-View (CV)
  - chyba < 10ns

Geostacionární satelity (2 x 36000 km)

- Metoda TWSTFT
  - přesné (~ 1ns), velmi drahý provoz
- Prakticky dosažitelná nejistota v síti
  - time 1 s
  - NTP 1 ms (rozsáhlá síť, PC se standardním krystalem)
    10 μs (LAN, kvalitní oscilátor, HW podpora v serveru)
  - IEEE-1588 1 μs (lokální síť, Ethernet, podpora v přepínačích)
  - White Rabbit < 1 ns (synchronní Ethernet)

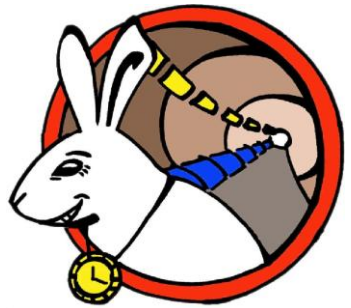




Úvod – Přesný čas a QKD

White Rabbit

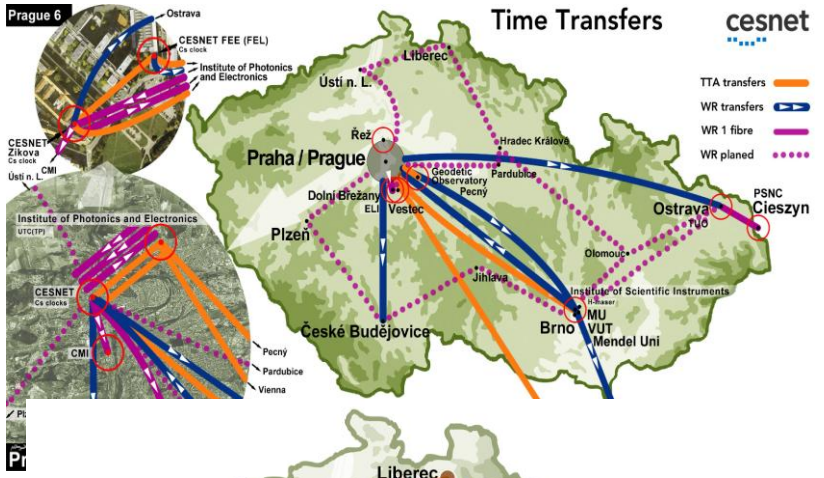
- Open-source projekt vyvinutý pro potřeby distribuce přesného času a frekvence v CERNu
- Možnost velkého množství odběrných míst (tisíce)
- Sub-nanosekundová přesnost synchronizace s rozlišením v řádu pikosekund
- Klíčové komponenty
  - rozšíření PTP protokolu (přesný timestamping)
  - synchronní Ethernet
  - přesné měření fáze a real-time kompenzace zpoždění

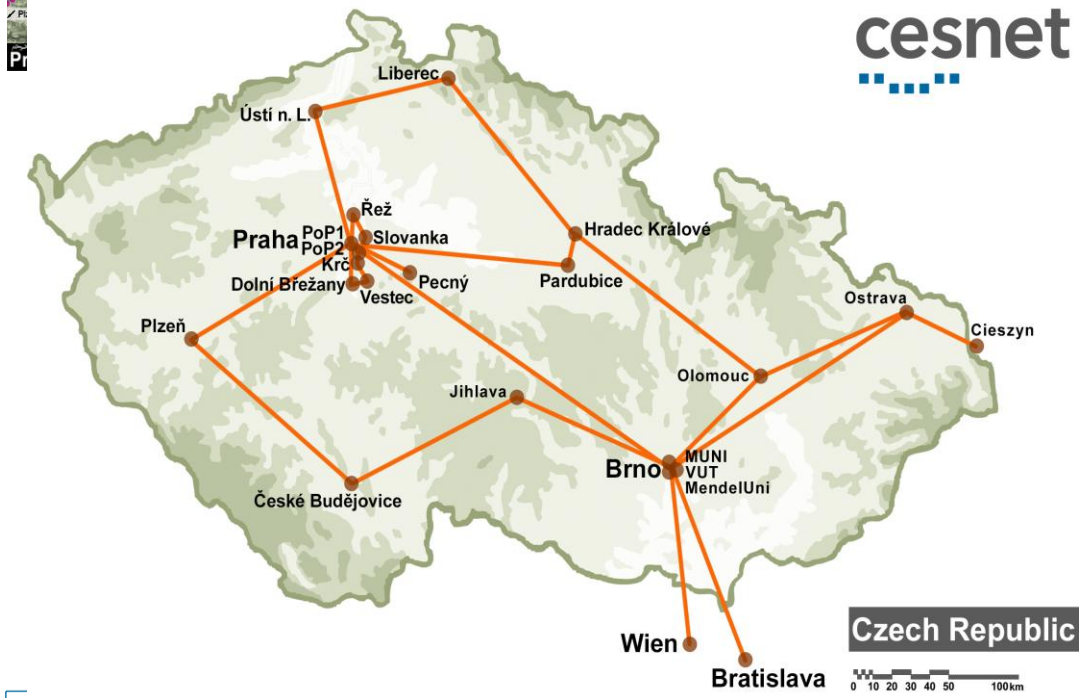


TF síť CESNET – Přesný čas a QKD

- 20 Points-of-Presence, každý WR switch
  - WR PoPy i u sousedů: Vienna, Cieszyn, Bratislava
- Pokročilé WR switche
  - přenos časové stupnice
  - distribuční infrastruktura
  - Možnost více referencí, přepínatelné
  - Redundantní zdroje
- Služby: primárně PTP a White Rabbit

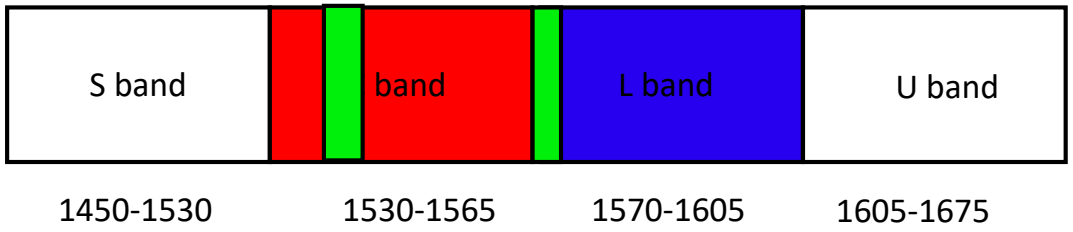
  omezeně i 10 MHz a 1PPS
- Spektrum sdíleno s datovými přenosy
- Obousměrné bidi EDFA
- Dva zdroje času sledovatelné k UTC(TP)
  - H-maser Cesnet (Praha) a UPT AVCR (Brno)

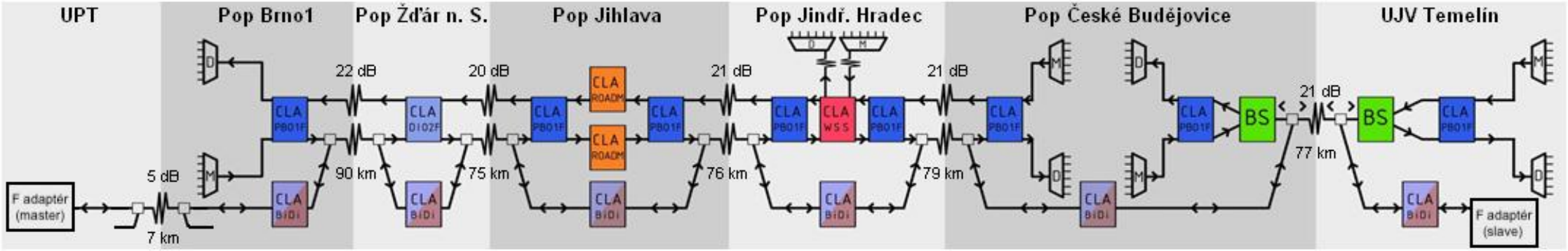




TF síť CESNET – Přesný čas a QKD

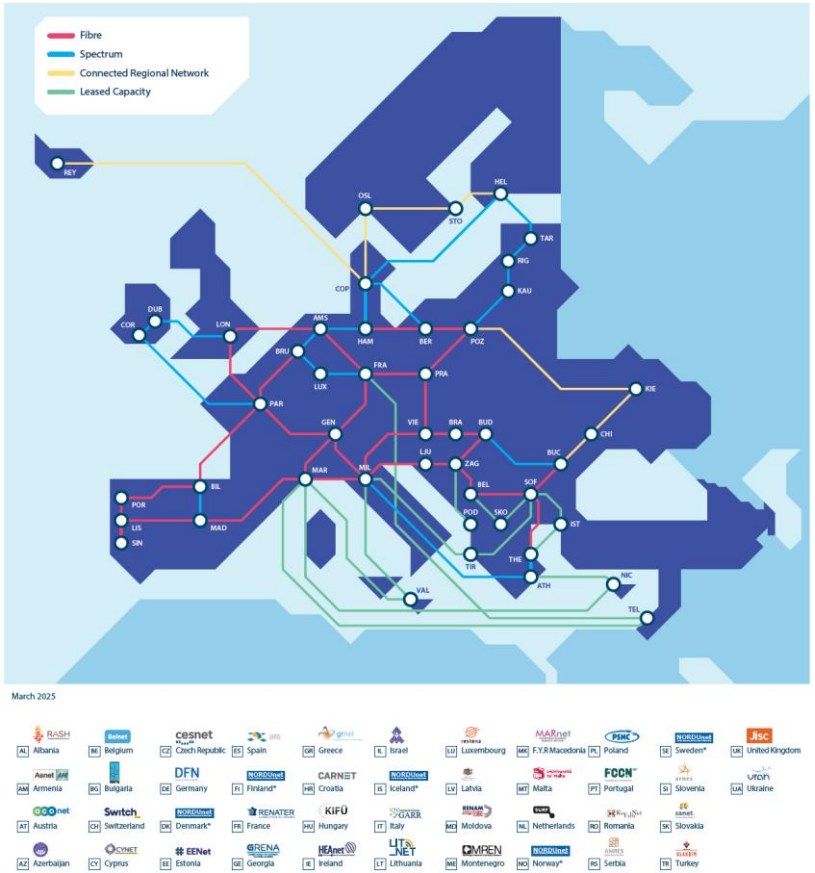
- S pomocí OADM rezervováno optické spektrum v páteři (bypassy)
- Sdílení vlákna s daty
- Nasazeno zhruba 120 OADM, 2500km tras, dual window: kanály 46-39 a 9-6
- Dual band bidi EDFAs pro pokrytí ztrát kanálů
- Jedna „specialita“ zesilované 1458nm propojení optických Ca+ hodin





GÉANT – Přesný čas a QKD

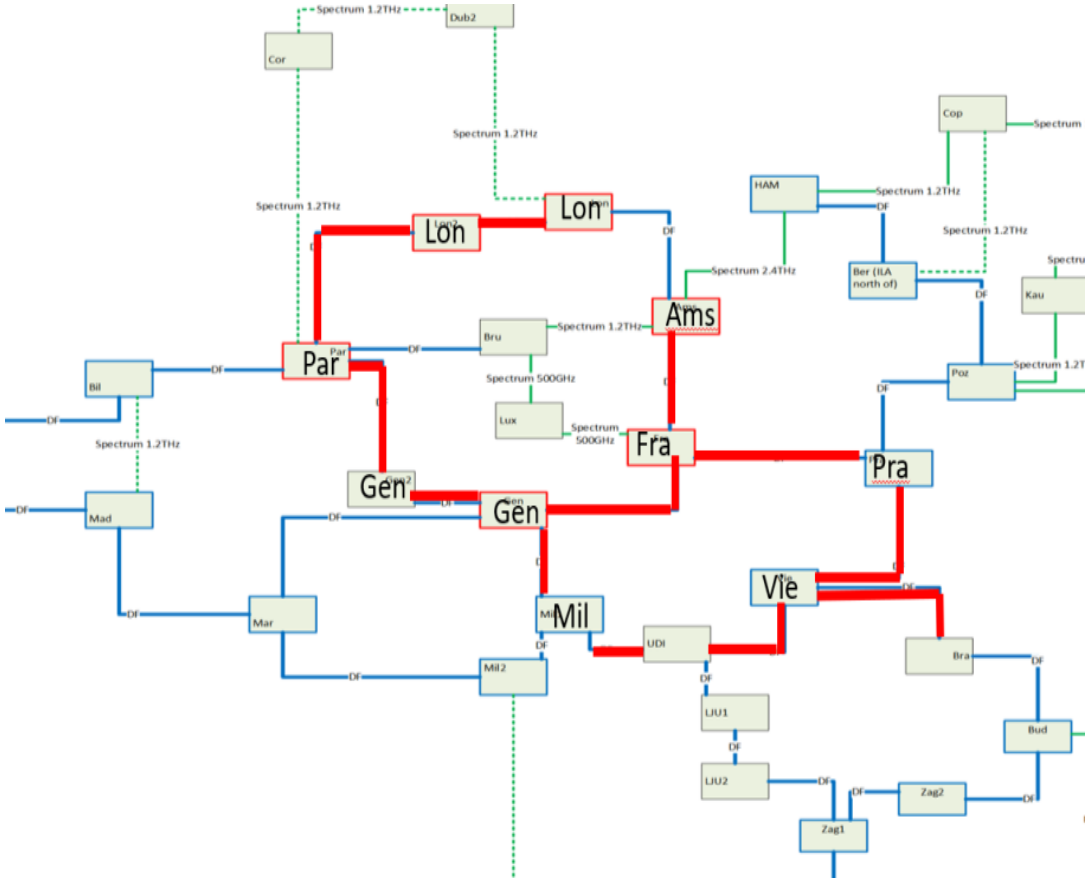
- Series of projects for pan-EUROPEAN network (almost 30 years), 38 partners
- Special Interest Group for the Time and Frequency Network (SIG-TFN) formed 2024
- Support: PTB, REFIMEVE, GUM, INRIM, NPL, METAS, Observatoire de Paris, Observatoire de Bruxlelles, VSL, IPE/UFE, FAMO, CERN,…



https://wiki.geant.org/spaces/SIG/pages/735051873/SIG-TFN+Homepage

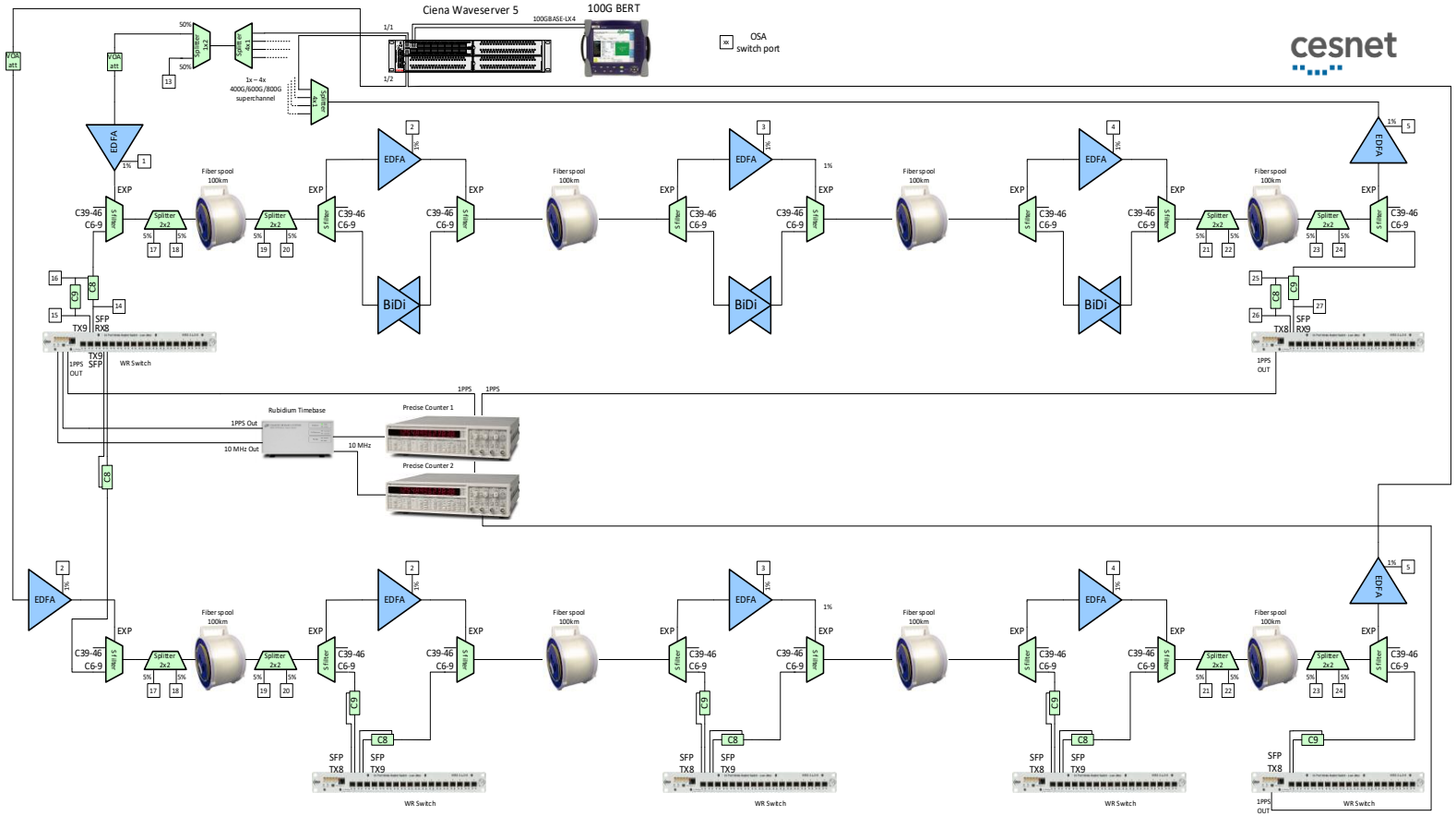
GÉANT – Přesný čas a QKD

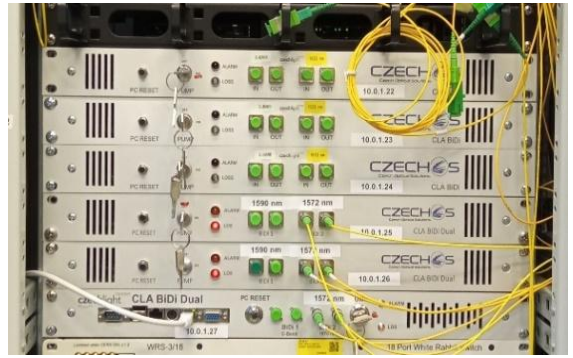
- GEANT initiated a GN5-2 WP6 NETDEV Incubator project led by SIKT on long-haul WR time service over DWDM networks.
- Partners: GEANT, SIKT, CESNET, SUNET, FUNET, GARR
- Goals:
  - Survey of current WR deployments in Europe
  - Evaluate the available solutions, including field-trial on GEANT link Prague-Vienna
    - Geant backbone link Prague – Vienna
    - Infinera DWDM system
    - 2x 400G DP-16QAM data channel in C-band
    - WR in L-band
  - Performance-cost analysis of the different solutions
  - Best practice recommendation to NRENs on how to deploy WR in their long-haul DWDM networks.
- Key challenges for long-haul is regeneration at In-line Amplification Sites (ILA). Solutions to be evaluated:
  - Bidirectional amplifiers
  - WR switches for regeneration
  - Optical-Electrical-Optical media converters



Laboratorní ověření – Přesný čas a QKD

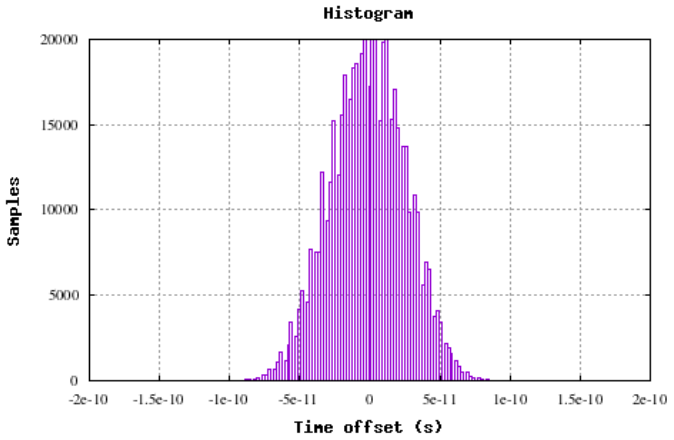
- Laboratorní setup
  - Kanály 8 a 9, 400km



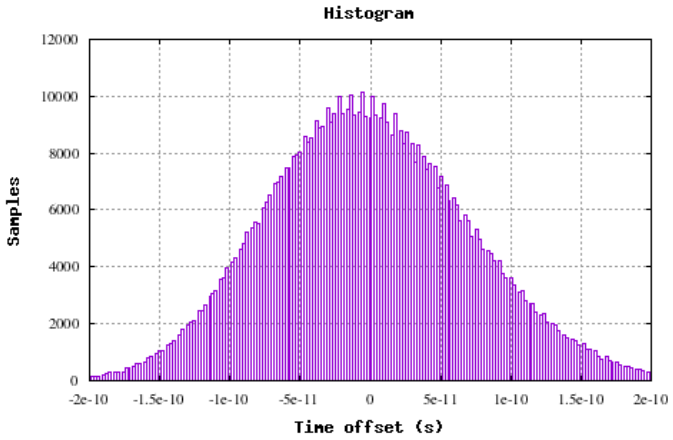


4x 100 km Cesnet Test White Rabbit / Superchannel 400/800G – BiDi EDFA version plus repeater version

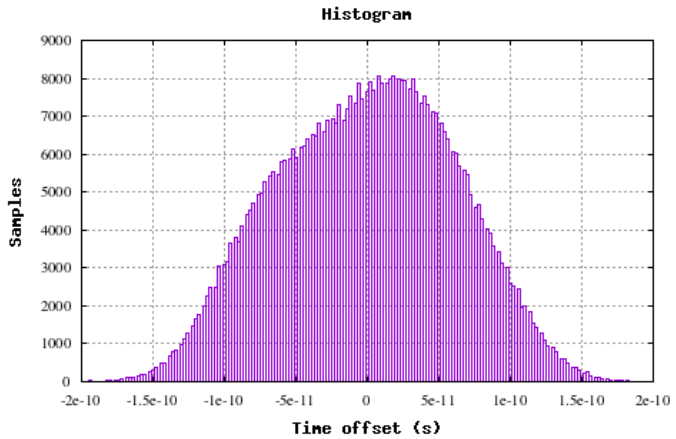
Laboratorní ověření – Přesný čas a QKD



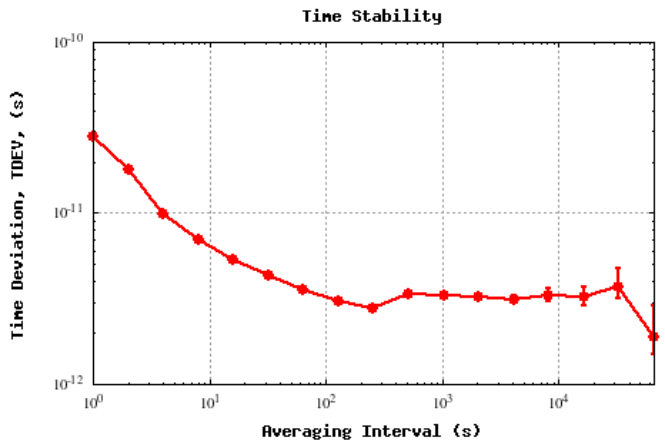
Opticky zesilované

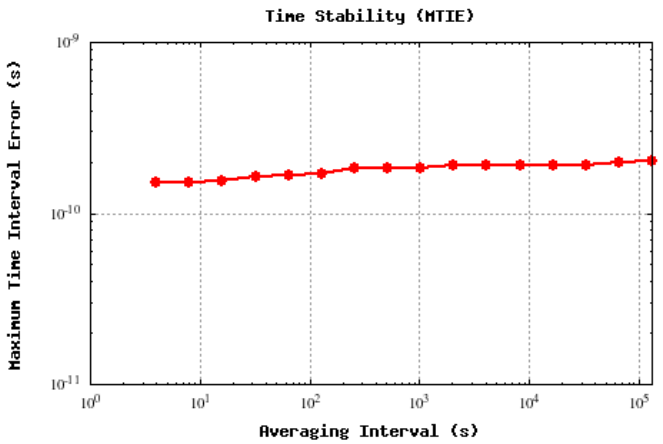


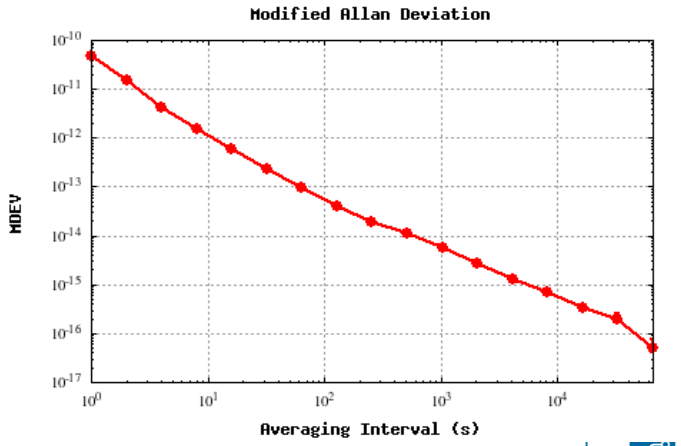
3R regenerované WRs



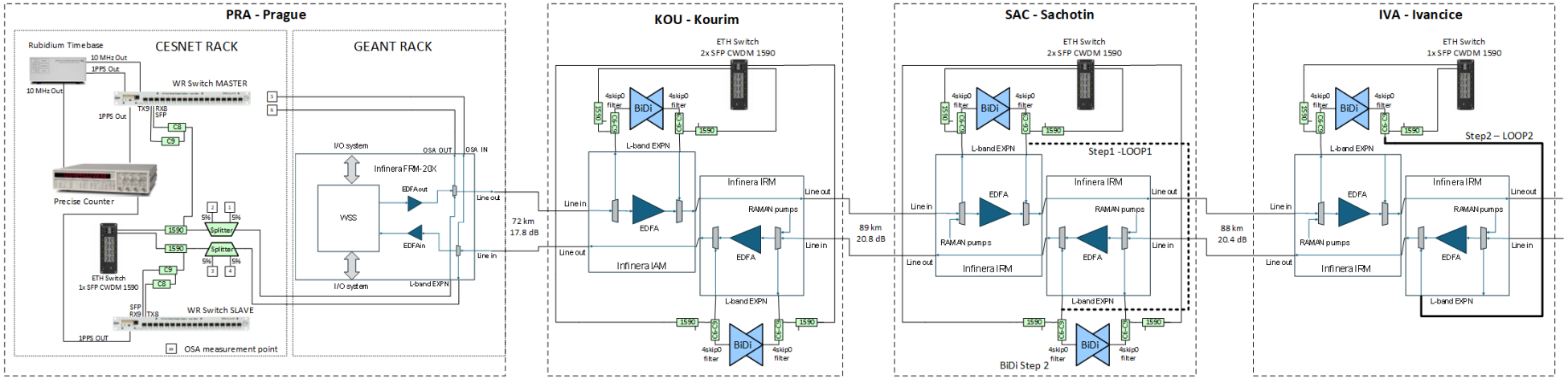
2R OEO převody



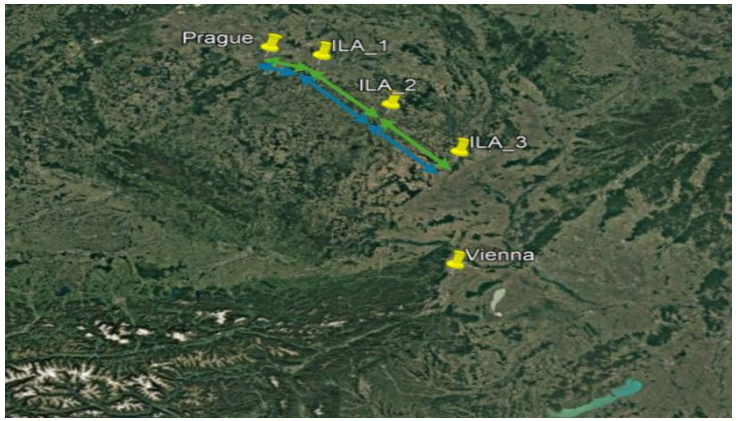




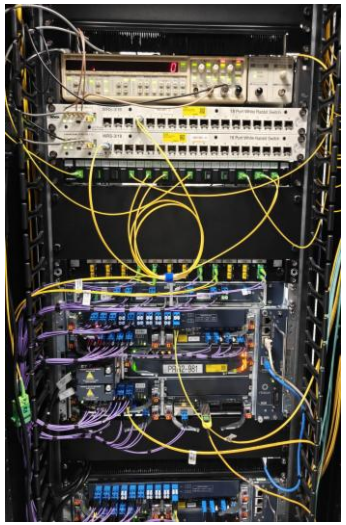
Měření na živé trase – Přesný čas a QKD



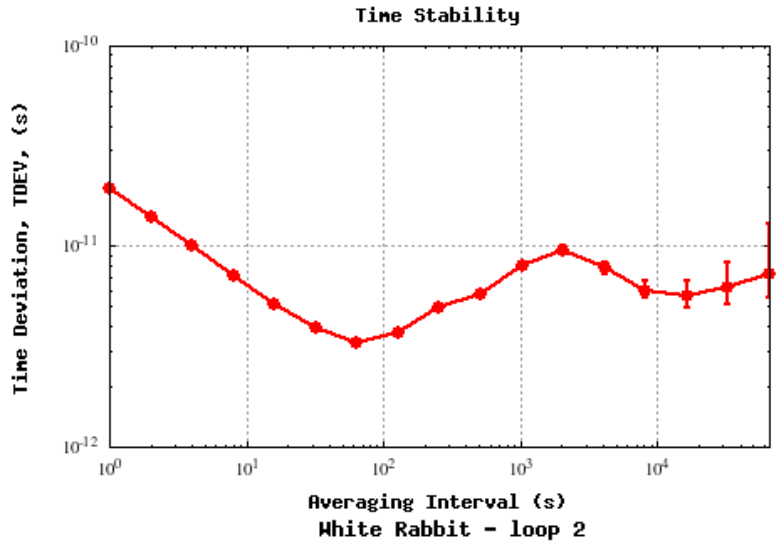
GEANT - CESNET Trial Test White Rabbit BiDi EDFA Precise Time
1. step: 3x BiDi, 322 km
2. step: 5x BiDi, 498 km

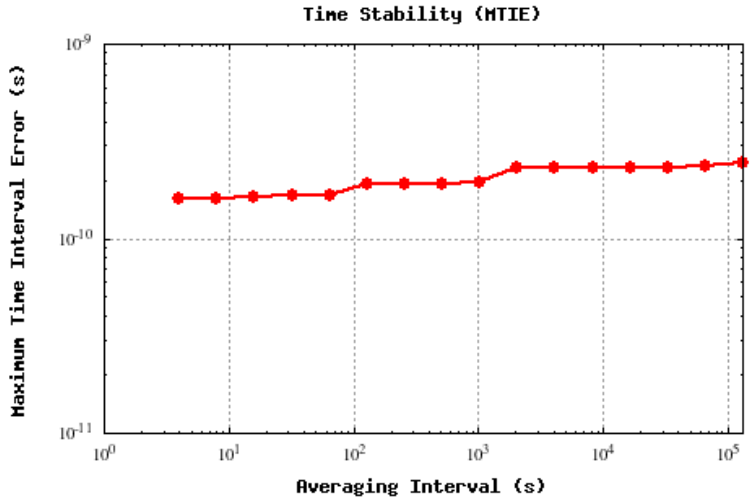


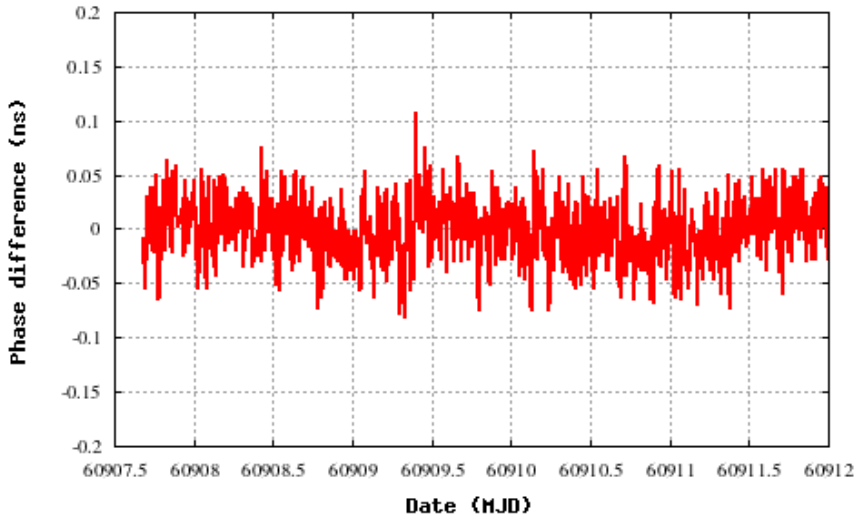
Field-trial on GEANT Prague – Vienna link
498 km optical link loop

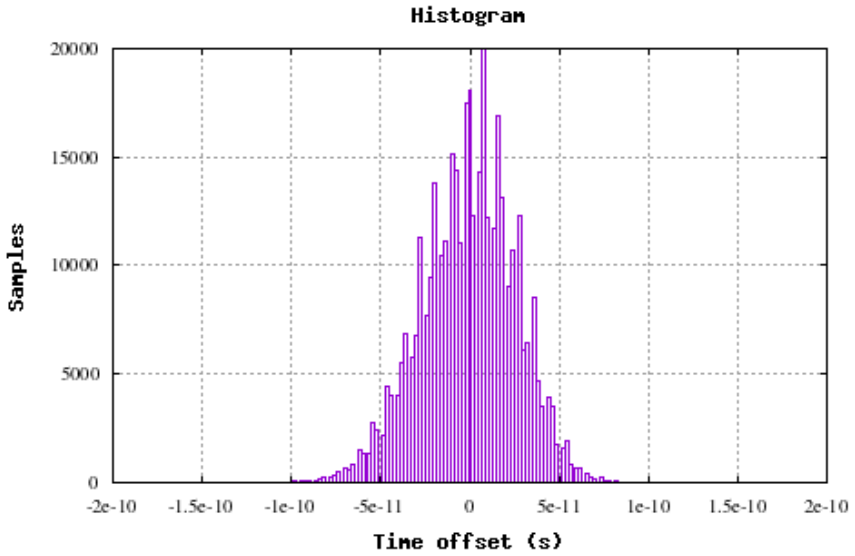


Měření na živé trase – Přesný čas a QKD









Výsledky:

- Nebyl pozorován žádný vliv na Q faktor
- St. dev. σ = 33ps
- MTIE < 250 ps
- TDEV < 10 ps (Δ > 4s)

https://www.gna-g.net/wp-content/uploads/2025/12/GNA-G_LongHaulWR-_incubator_Vojtech_short.pdf

Úvod QKD – Přesný čas a QKD

- Motivace!
- QKD – kvantová distribuce klíčů
  - Klíče pro symetrickou kryptografii (důkaz existuje)
- Využití fyzikálních principů (kvantová mechanika) pro zabezpečení přenosu informace.
- Asymetrická kryptografie je ohrožena rozvojem kvantových počítačů
  - Shorův algoritmus QC řeší v lineárním čase atd.
- Reakce:PQC a QKD
- Přenáší se pouze klíč, následně se použijí klasické šifrovací metody (AES).
- Existuje řada QKD protokolů:
  - BB84 (Bennett a Brassard), využívá se polarizace fotonů, jde o statistiku.
  - E91 (Eckert) kvantové provázání – entanglement. A. Einstein a EPR paradox
  - BBM92 (BB+Mermin) kvantové provázání

Úvod QKD – Přesný čas a QKD

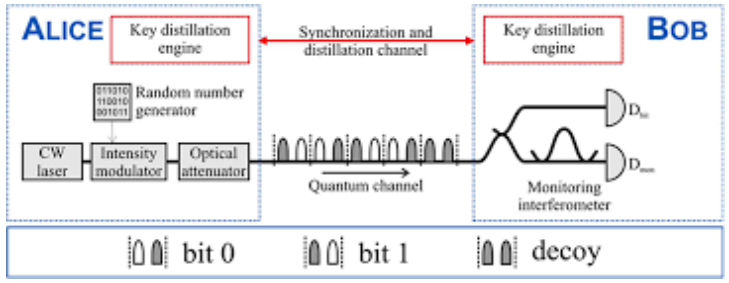
- QKD – komerčně dostupné
- Dnešní systémy se dělí do dvou kategorií:
  - CV, continuous variable, světlo jako vlny.
  - DV discrete variable, světlo jako částice - fotony.
- DV – delší vzdálenosti, nižší tzv. key rate, single foton detekce, velmi citlivé na parallní přenosy
- CV – kratší vzdálenosti, vyšší key rate, podobné telko světu koherentní detekce, málo citlivé na paralelní přenosy

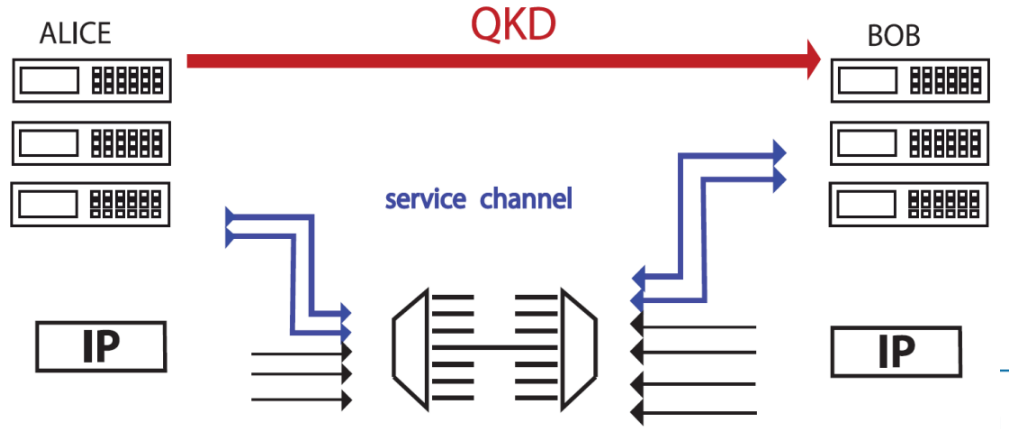
Úvod QKD – Přesný čas a QKD

- Problémy!
- QKD – kvantová distribuce klíčů.
  - Omezený dosah, nemáme kvantové opakovače.
- Využití satelitů.
- QKD přenos lze ohrozit.
  - Nikoliv fyzikální princip, ale vše v reálném světě musí být nějak vyrobeno a naprogramováno.
- Kvantová mechanika je stále předmětem diskuzí.
  - Průzkum Nature z roku 2025 odhalil překvapivé rozpory, dokonce mezi nobelisty. Známe jen pravděpodobnosti a to někoho znepokojuje.

Paralelní přenosy – Přesný čas a QKD

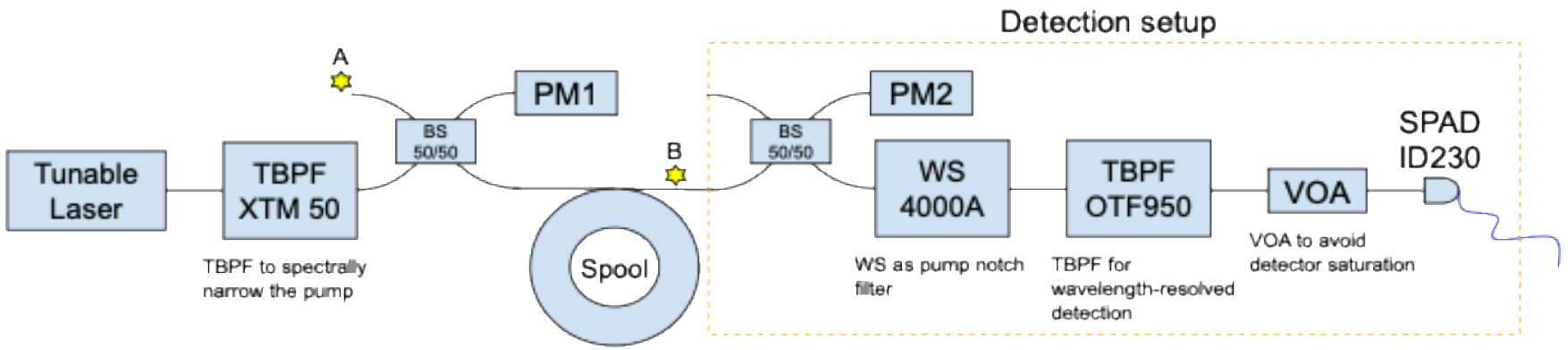
- 2021 1st intercity trial in CZ
- OpenQKD, cooperation with PSNC and TUO,
- Urban cross border fibre pair – 65 km, 16 dB
- Used by IM – DD 10 Gbps traffic
- Parallel White Rabbit precise time transfer
- Available QKD system
- Coherent one Way protocol (Nicolas Gisin et al. 2004)
- Max performance 75km / 18 dB





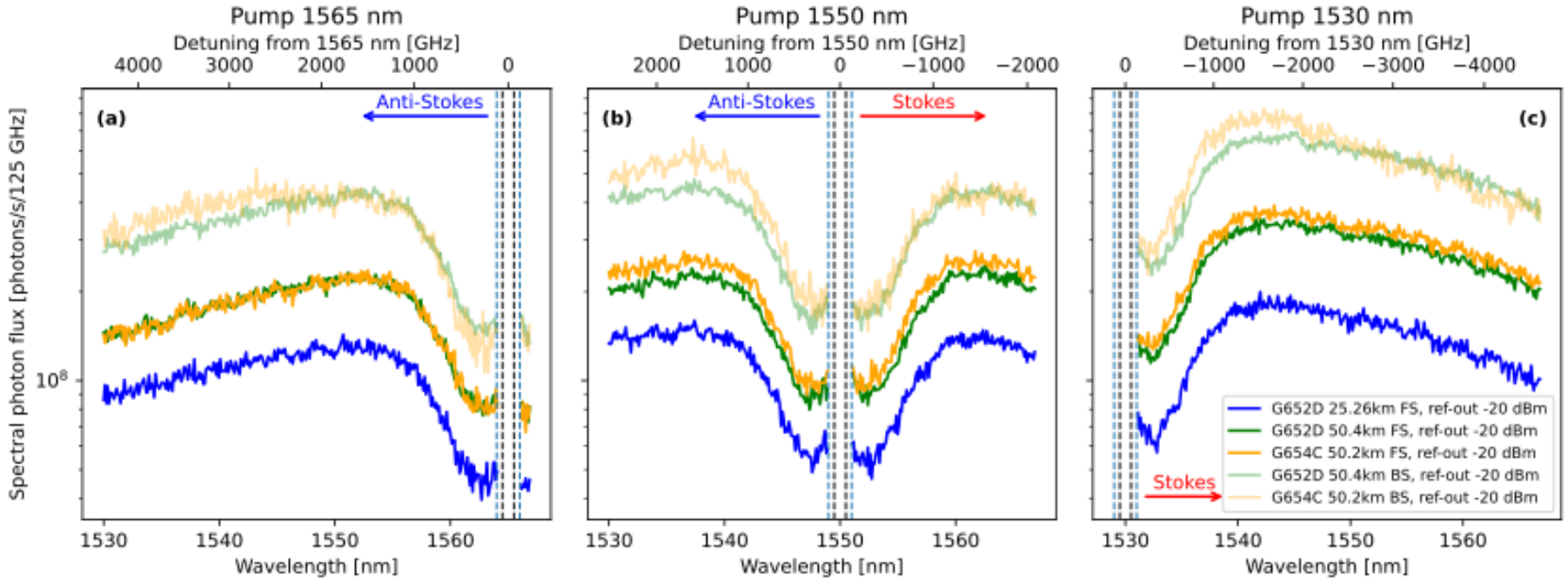
Ramanův rozptyl – setup – Přesný čas a QKD

- Single-photon counting testbed:
- Narrowband CW source in C- and O-band emulate WR channels (wavelengths and launch powers).
- Fiber under test: G.652D, G.654C, G.655; 25 km and 50 km spans.
- Forward and backward Raman noise measured with a potential quantum receiver.
- Tunable band-pass filter (C: OTF-950, O: OTF-980), WaveShaper / O–C filter stacks provide high-extinction pump rejection, ID230 SPAD + VOA operated below saturation; all losses calibrated.
- Raw SPAD count rate is corrected for dark counts using an effective dark-count model.
- Dead-time correction (non-paralyzable model) gives an estimate of the true photon rate at the detector input.



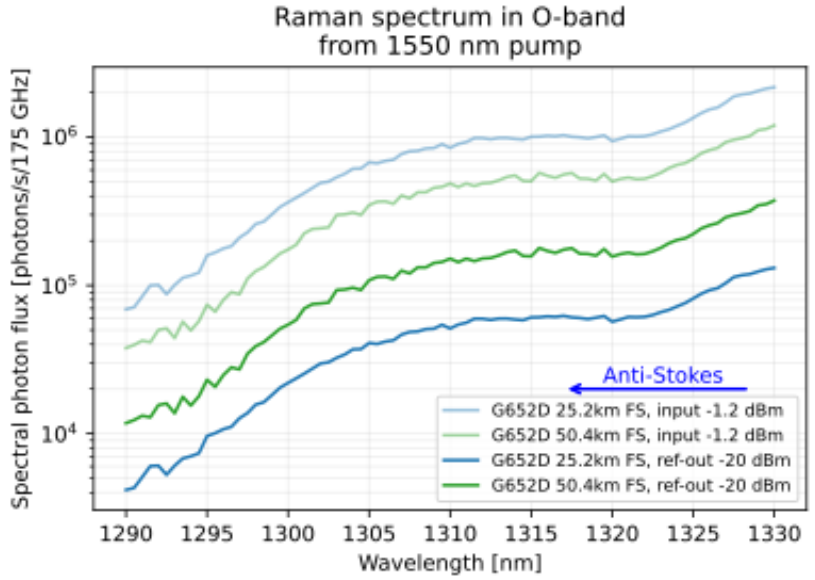
Ramanův rozptyl – inband C do C – Přesný čas a QKD

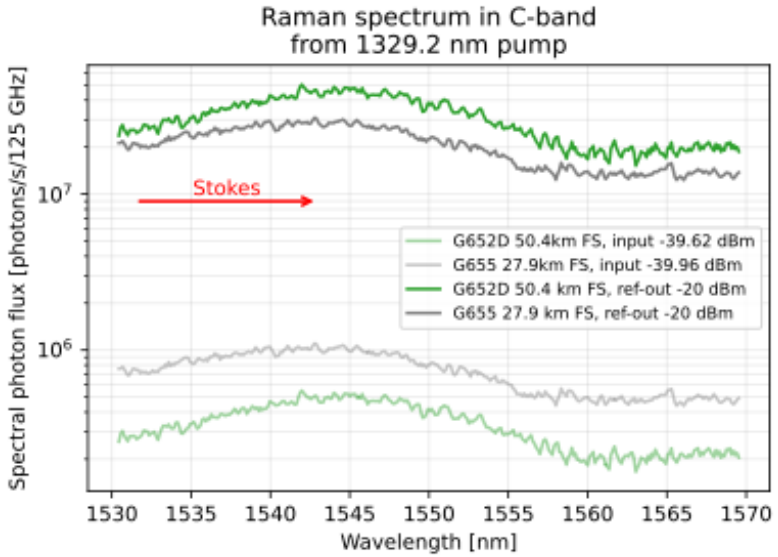
- Pumps at 1530 nm, 1550 nm and 1565 nm over G.652D and G.654C:
- Forward (FS) and backward (BS) Raman scattering measured for 25 km and 50 km spans.
- Backward Raman (BS) noise is higher than forward due to pump power decay along the span.
- Stokes and anti-Stokes contributions are both visible within the C-band region of interest.
- Spectral photon flux is reported as Φ_{125} [photons/s/125 GHz] in C-band



Ramanův rozptyl – C do O, O do C– Přesný čas a QKD

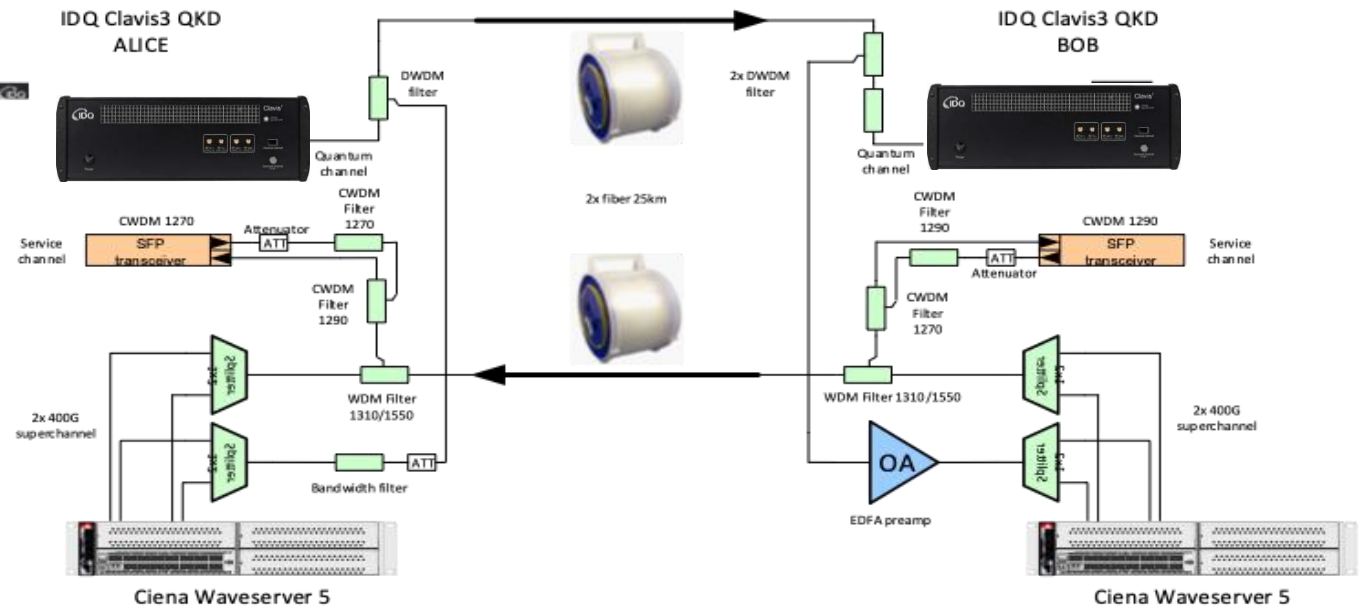
- C-band pump at 1550 nm, Raman noise measured around 1310 nm:
- Spans: 25.2 km and 50.4 km G.652D.
- TBPF scanned in O-band with reference bandwidth 175 GHz.
- Raman fluxes are below the C→C case, but noticeably higher than C→O for comparable output powers.
- Asymmetry between C→O and O→C originates from the asymmetry of the Stokes and anti-Stokes spectrum.
- For comparable output powers, C→O Raman noise is strongly reduced compared to in-band C→C.
- Most convenient option for coexistence





Paralelní přenosy – Přesný čas a QKD

- Project NESPOQ
- Parallel 2 x 400 Gbps data and White Rabbit precise time transfer
- Available QKD system
- Coherent one Way protocol (Nicolas Gisin et al. 2004)

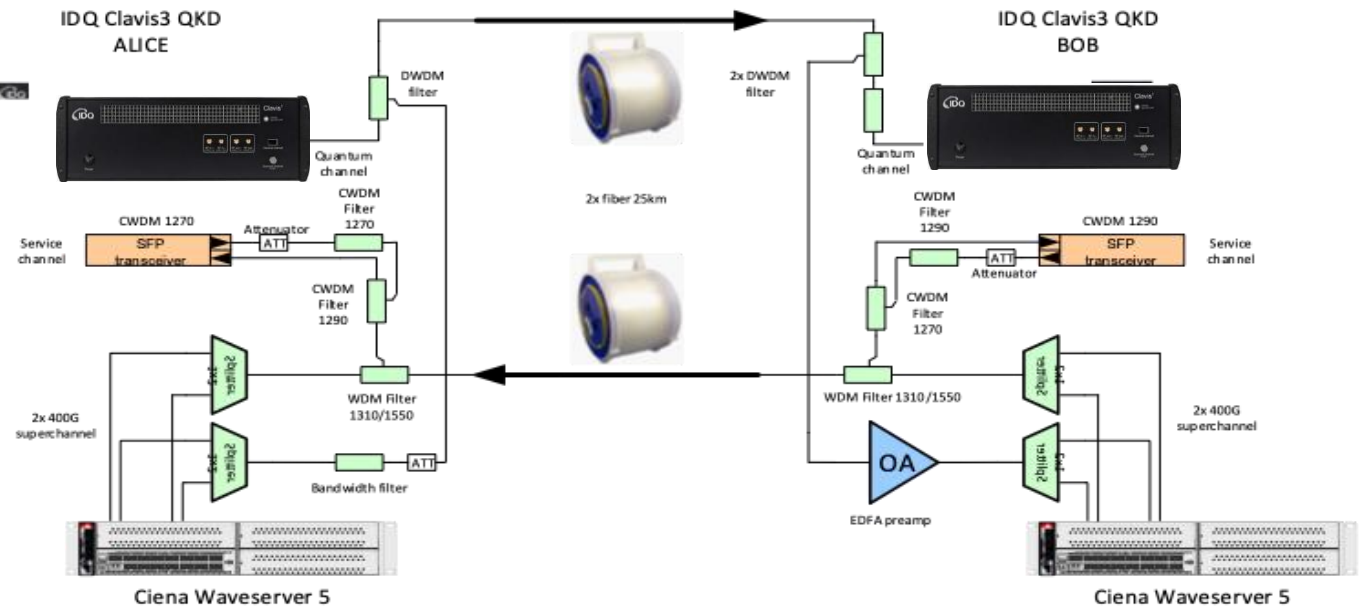


CESNET test - Superchannel 2 x 400Gbit/s plus QKD system

Jan Radil, et al "Quantum and Data Signals in a Single Fiber – Multiplexing by Smart Use of High-Grade Filters," in IEEE Communications Letters, doi: 10.1109/LCOMM.2025.3545315

Paralelní přenosy – Přesný čas a QKD

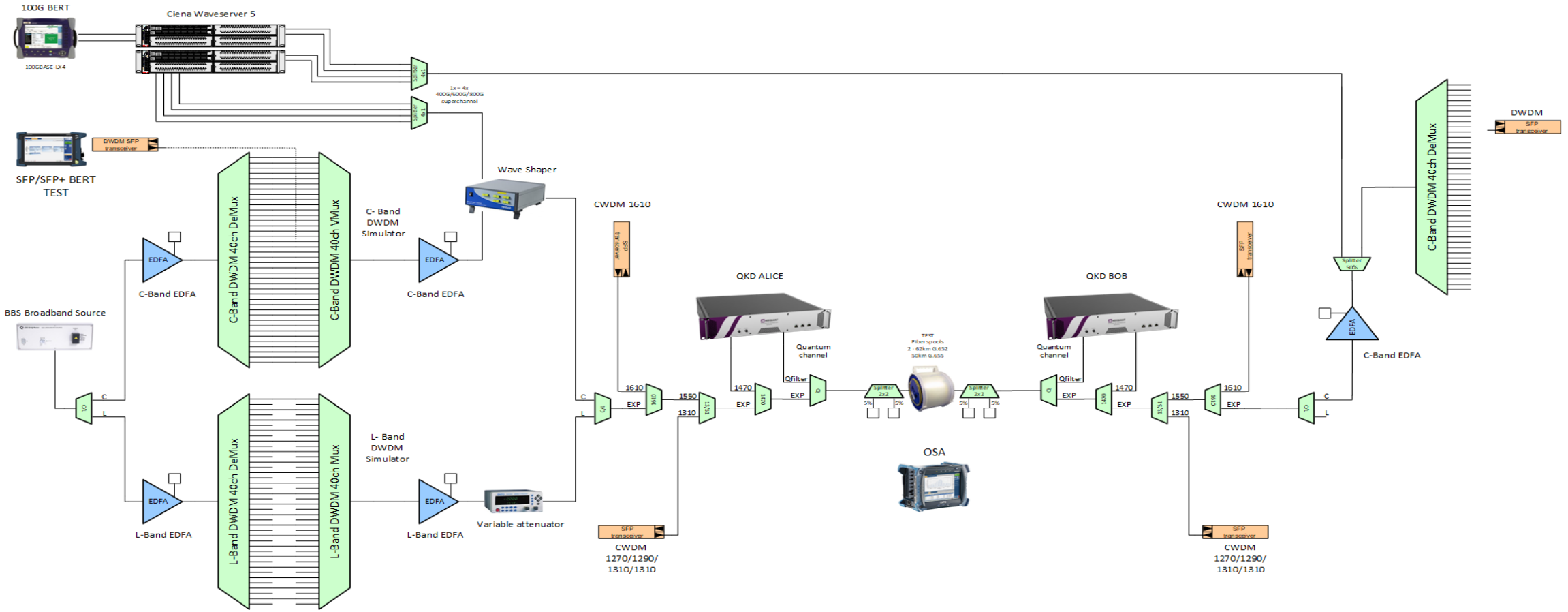
- Project NESPOQ
- Parallel 2 x 400 Gbps data and White Rabbit precise time transfer
- Available QKD system
- Coherent one Way protocol (Nicolas Gisin et al. 2004)



CESNET test - Superchannel 2 x 400Gbit/s plus QKD system

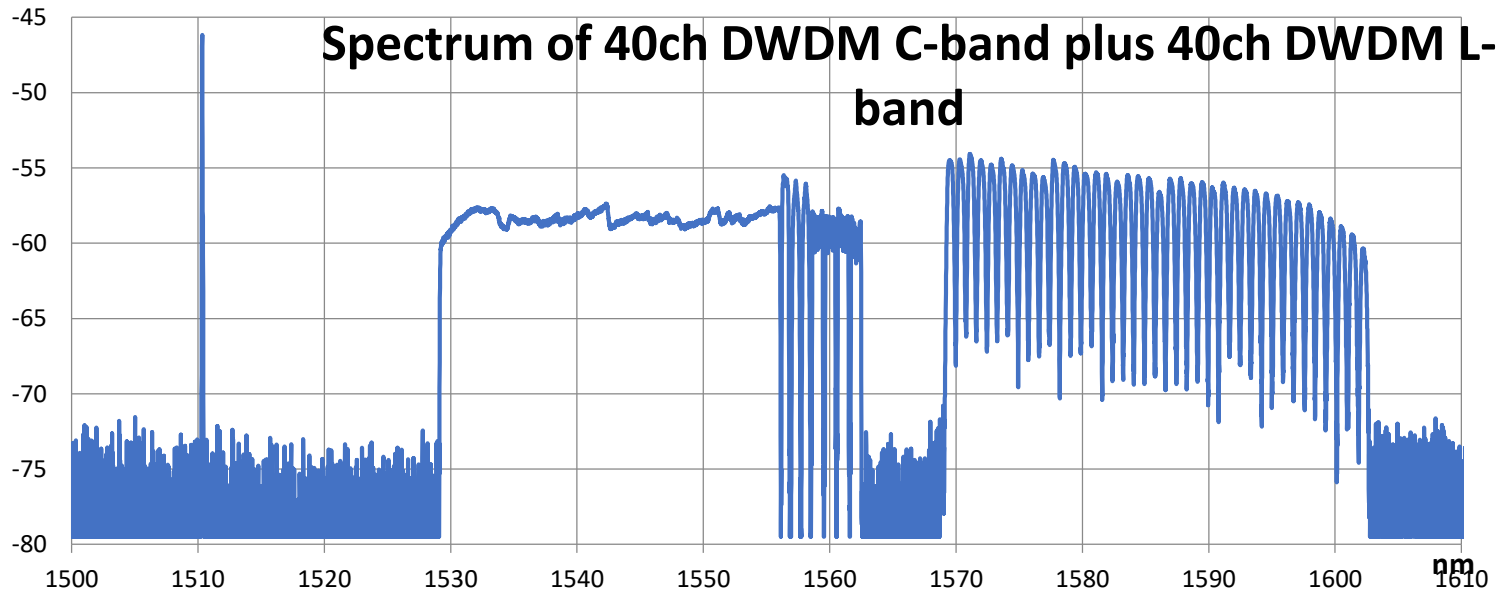
Jan Radil, et al "Quantum and Data Signals in a Single Fiber – Multiplexing by Smart Use of High-Grade Filters," in IEEE Communications Letters, doi: 10.1109/LCOMM.2025.3545315

- CV-QKD system test (project SEQRET) ¨- succesfull CV QKD operation with fully loaded spectrum by 40 channels in C and L band



https://www.cesnet.cz/en/news/quantum-security-moves-closer-cesnet-validates-a-new-generation-of-data-encryption-288

- CV-QKD system test (project SEQRET) - succesful CV QKD operation with fully loaded spectrum by 40 channels in C and L band



https://www.cesnet.cz/en/news/quantum-security-moves-closer-cesnet-validates-a-new-generation-of-data-encryption-288

Závěr – Přesný čas a QKD

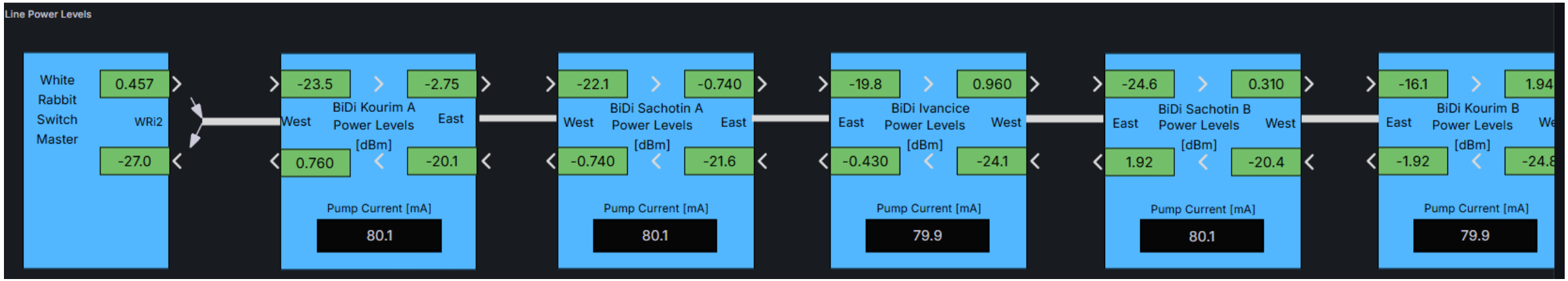
- Dosaženo:
  - Srovnání technik prodloužení dosahu, řazeno dle stability: bidi optické zesilování > 2R s OEO > 3R
  - Na reálné trase téměř 500km v roce 2025 dosaženo: MTIE < 250 ps, TDEV < 10 ps (Δ > 4s)
- ToDo:
  - Dokončit integraci moitoringu optické and WR vrstvy, osadit v ČR cca 20 linek
  - Měření kvality přenosu bidi linek (M. Slapak at al: Stabilization of super coherent frequency transfers via amplifier cascade balancing. https://doi.org/10.1016/j.yofte.2024.103910)
- Ověřeno:
  - C → C trpí nejvyšším Ramanovským šumem, existuje lokální minimum
  - C→C ≫ O→C (až o 1 řád),
  - O→C ≫ C→O (až o 2 řády) -- umístění QKD kanálů je z tohoto pohledu nejvýhodnější v O pásmu
  - Pro 25–50 km spany romanovský šum roste zhruba lineárně s délkou spanu, to je v souladu s teorií malosignálového ramanova spontánního rozptylu
  - Koexistence dat a WR úspěšně dosazena pro DV QKD systémy se slabými pulsy (COW, BB84) a CV QKD systémem
- ToDo:
  - Ověření koexistence s DV QKD systémy založenými na provázanosti

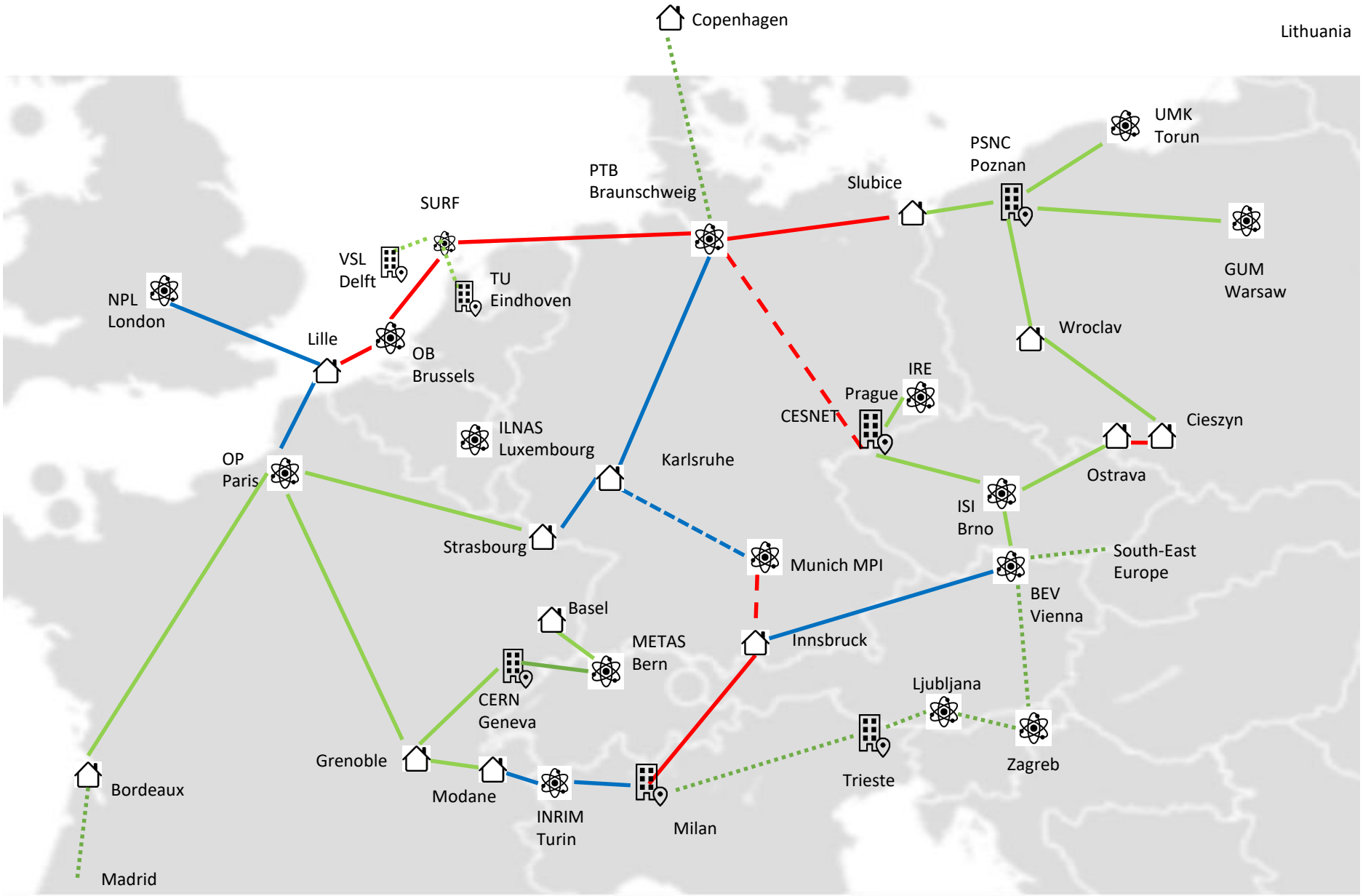
Děkuji za vaši pozornost!

Otázky prosím?

vojtech@cesnet.cz

- Field-Trial Results – No Impact on Data Channels
- 2 x 400G channels (in C-band) running in parallel with the white rabbit T&F service (in L-band)
- Both pre-FEC-BER and Q-margin before and after white rabbit activation, are at the same level





Included:

- 10-year IRU for fibre on red routes
- Bidirectional amplifiers as needed to light the fibre on the red routes

Excluded:

- Green lines – fibre built by NRENs
- Blue lines – fibre bult by NMIs
- Dashed green – proposed future links
- flywheels, counters frequency combs needed are to be funded by the national time/frequency providers
- Time/Frequency overlay services

NMI Frequency reference

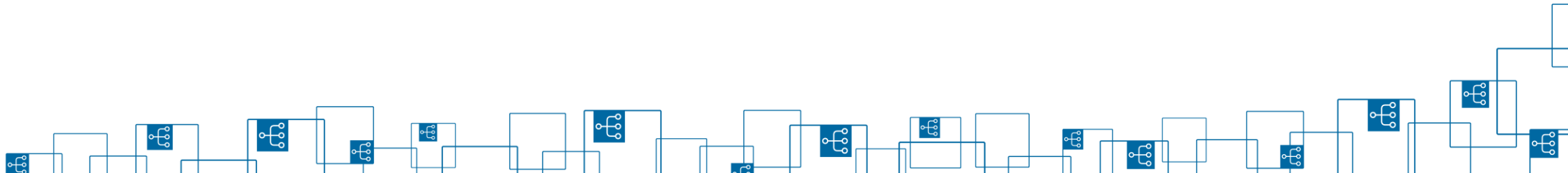
Research institute

Hut for housing RLS

Adopted from Guy Roberts

Financování – Přesný čas a QKD

- This work was supported by:
- the Ministry of Education, Youth and Sport of the Czech Republic as part of the e-INFRA CZ project LM2023054



Literatura – Přesný čas a QKD

- Guy Roberts et. al: *Quantum Key Distribution in the GÉANT network*, Cambridge 2017. https://tnc17.geant.org/core/presentation/24
- http://www.feynmanlectures.caltech.edu/III_01.html basic
- https://www.feynmanlectures.caltech.edu/III_18.html entanglement
- https://www.nature.com/articles/d41586-025-02342-y