Wrocław University of Technology
WUT Institute of Physics
WUT Institute of Informatics

CompSecur IT Solutions

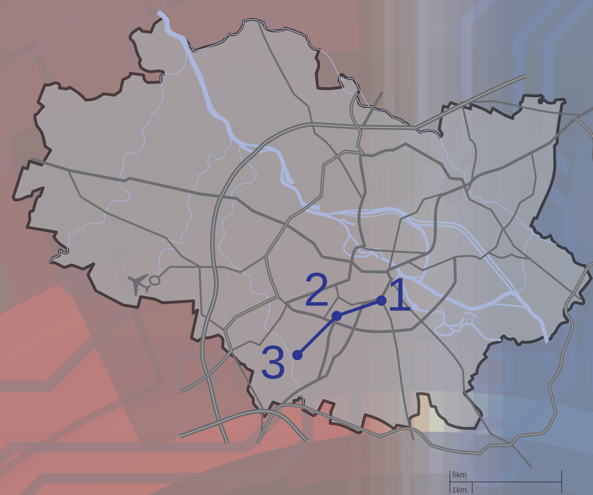
Wroclaw Quantum Network – QKD deployment in a metropolitan network

M. Jacak[2], T. Martynkien[1], A. Janutka[1], J. Jacak[1], D. Melniczuk[1], W. Donderowicz[3], J. Gruber[2], I. Jóźwiak[2]
[1] Institute of Physics, Wrocław University of Technology, Wyb. Wyspiańskiego 27, 50-370 Wrocław, Poland
[2] Institute of Informatics, Wrocław Univeristy of Technology, Wyb. Wyspiańskiego 27, 50-370 Wrocław, Poland
[3] CompSecur sp. z o.o. R&D Department, ul. Piłsudskiego 74/309, 50-020 Wrocław, Poland

City Wroclaw
Country - Poland
Voivodeship - Lower Silesian
Population (2012) - 631 188
Area - 292.92 km^2
Main river - Odra

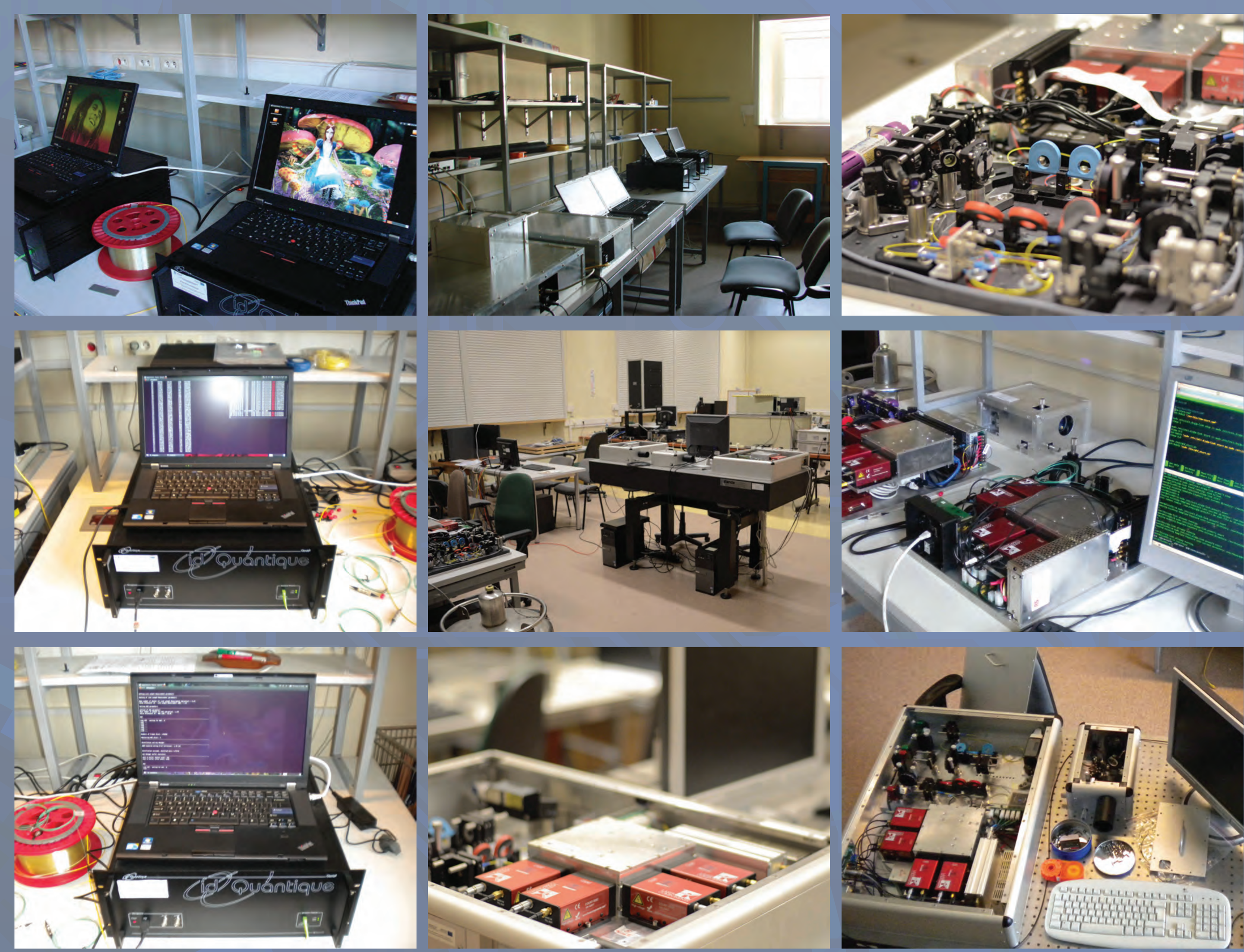
Due to significant investments in Wrocław University of Technology laboratory equipment encompassing current state-of-the-art quantum cryptography technologies within the Polish National Quantum Technologies Laboratory NLTK network programme, as well as technological partnerships with internationally leading vendors of quantum cryptographic systems and national information security institutions and companies, city of Wroclaw now hosts a unique metropolitan quantum network research and development project.

National Quantum Technologies Laboratory NLTK, Wrocław University of Technology

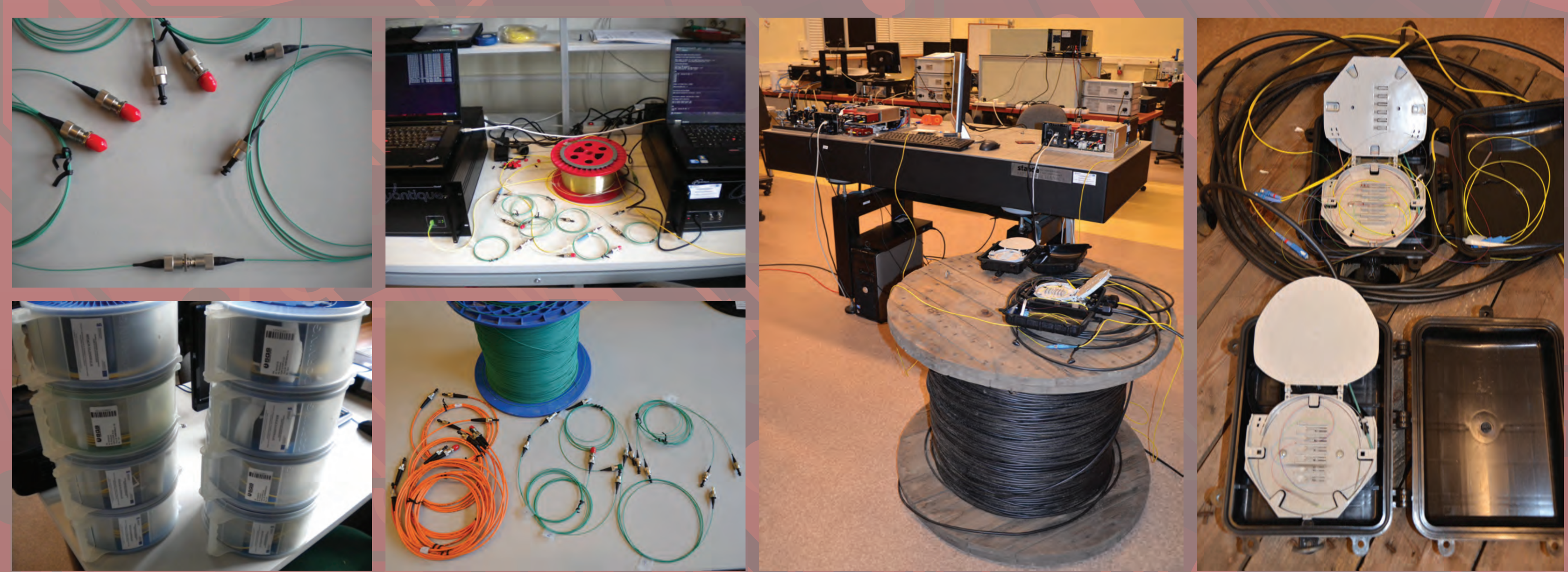


1 Wrocław University of Technology
2 CompSecur
3 CompSecur

Experimental and even early commercial QKD implementations are very susceptible to technical conditionings of the transmitting media (i.e. optical fiber infrastructure and associated alignment of the quantum optics) therefore deployment of QKD systems in real metropolitan optical fiber infrastructure network poses a challenge



The optical infrastructure is determined by the city telecommunication canalization layout. Dark fibers connecting two, even not very distant metropolitan locations physically sharing an industry-standard telecom line with many parallel fibers (constituting the initial P2P topology and medium for QKD network) are divided in a series of thermally welded interconnections and junctions at telecom canalization crossings, which are main reason for decoherence and quantum signal losses, resulting with increased QBER and with infeasibility of key distribution in practical scenarios (this is specifically addressed to dark fiber infrastructure of metropolitan backbone telecom networks with multiple interconnections of telecommunication optical lines, which are implemented by thermal weldings – a connection between two locations separated by ca. 4-5 km distance, is usually divided by even several fiber weldings)



Research on QKD deployment in practical telecommunication network environments resulted in evaluation of boundary conditions for QKD feasibility versus quantum channel and transmission parameters and a successful resolution of channel quality problem by proper alignment of experimental QKD setups. The fiber optics line of the SMF28 standard has been used to test different connection and welding configurations for two R&D QKD approaches based on the IdQuantique Clavis2 setup (non-entanglement QKD, encoding qubits on interfering phase shifts of laser impulses in Mach-Zehnder interferometers) and the AIT Quelle setup (entanglement QKD, encoding qubits on polarizations of entangled photon pairs generated in non-linear PDC process in a BBO crystal). The main optics fiber line (single mode SMF28 standard) has been subsequently modified in laboratory test runs by welded or interconnected F3000/APC and FC/PC adapters. The interconnectors resulted with high QBER increases, thus favoring thermal welding which in proper proximity distribution were characterized by ca. 10 times lower loss induction than interconnectors (ca. 0.01 dB per welding, depending on the proximities). Next the industry standard telecom fiber optics line tests have been carried out towards welding and interconnections configuration optimizing in regard to QBER and conditioning of the metropolitan network deployment. Primary focus was directed towards the non-entanglement based setup which turned out to be operating properly with an acceptable raw key exchange rate (RKER) generating targeted amount of distilled secret bits (DSB) under laboratory simulation of real optic fiber backbone metropolitan network configuration with required optimization of interconnections and welding infrastructure. The entanglement based QKD has been tested for the first time in a real telecom network environment and proved to be also feasible but within a very narrow gap of optical elements alignment and poor (unpractical) values of QBER and RKER with high additional instability of operation parameters. This research allowed for the current deployment of the QKD metropolitan network in Wroclaw.

Sample characteristics of non-entanglement QKD deployment setup:

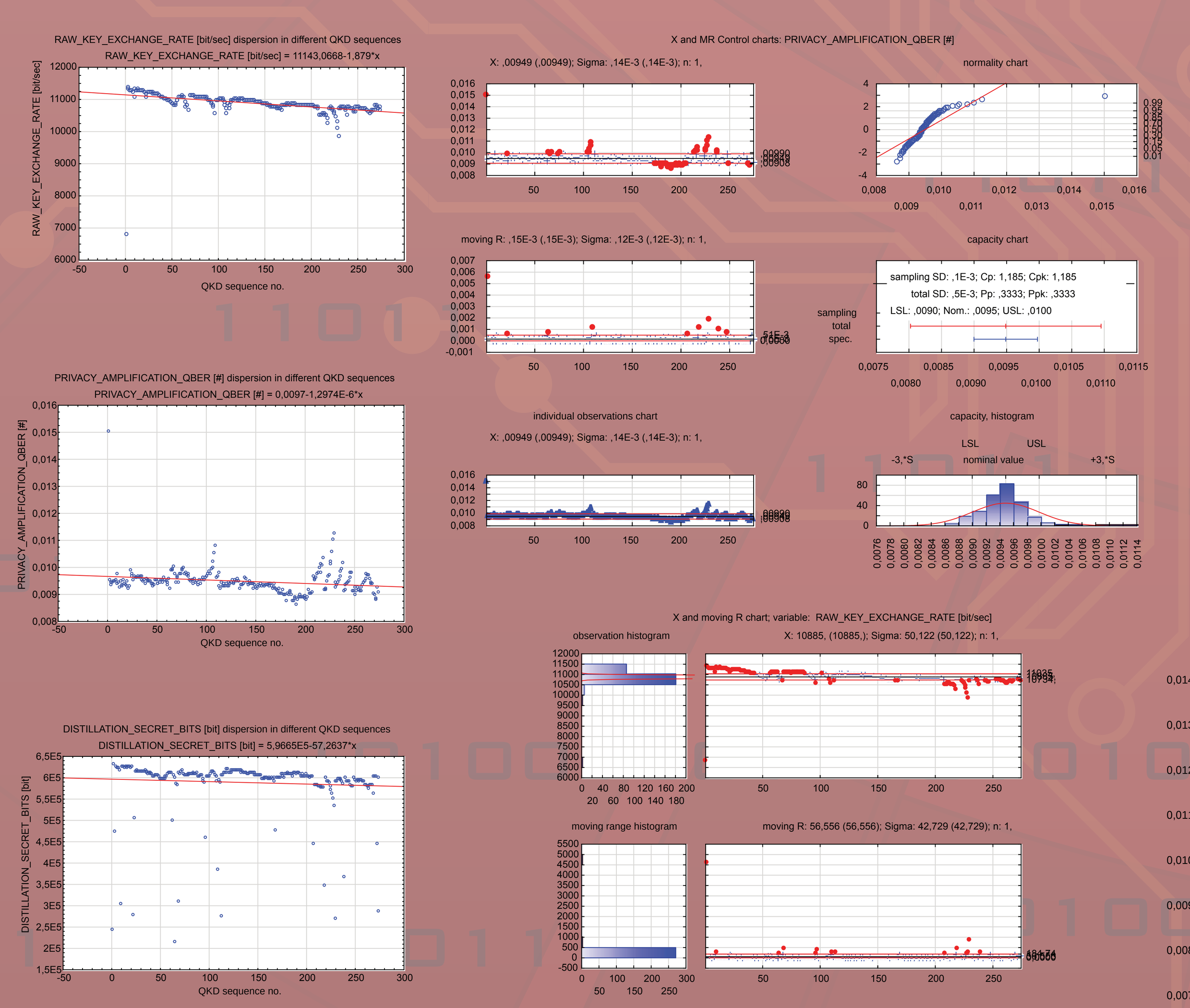
- Quantum optics and electronic components assembled in an integrated R&D system performing quantum key distribution (QKD) without using of quantum entanglement:
  - Quantum opto-electronic setups integrated within 2 end-stations connected by optical fibres (WDM compatibility) and computer controlled with a hardware/software architecture
  - Including laser photon source and avalanche photodiode detectors (temperature stabilized)
  - Featuring photon phase qubit coding (interferometers with auto-compensation)
  - Featuring implementation of BB84, B92, SARG04 QKD protocols
  - Including software suite (containing programming libraries)
  - QKD distance: at least 50 km
  - Keyrate: at least 1 Kbit/s on a 25 km distance
  - Temperature of operation between 10 and 30 °C

Sample characteristics of entanglement based QKD deployment setup:

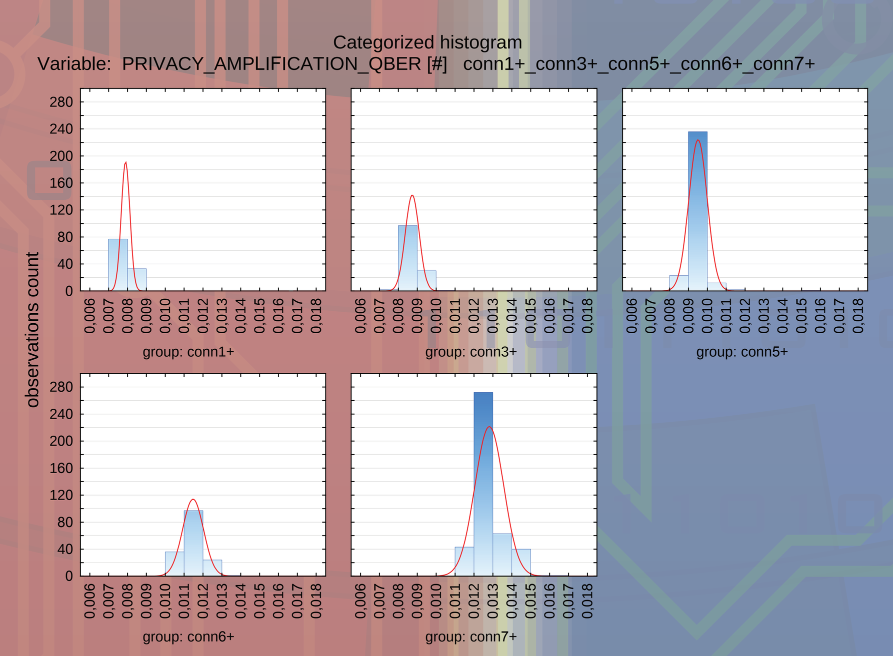
- Quantum optics and electronic components assembled in an integrated R&D system performing quantum key distribution (QKD) by means of quantum entanglement:
  - Quantum opto-electronic setups generating quantum entanglement in photons polarizations, integrated within 2 end-stations in both optical fibres (WDM compatibility) and telescopic (free laser beam) configurations, computer controlled with a hardware/software architecture
  - Featuring non-linear crystal implementation of the parametric down conversion procedure of quantum entanglement production in photon polarizations states (carrier of the information implemented on the polarization of photons in quantum entangled states)
  - Including laser photon source and avalanche photodiode detectors (temperature stabilized)
  - Featuring implementation of entanglement based QKD protocol (including implementation of key sifting, key distillation, error correction and privacy amplification functional layers)
  - Featuring integrated electronic control and interface systems (including synchronization systems)
  - Including software suite (containing programming libraries)
  - QKD distance: at least 5 km
  - Keyrate: at least 0,2 Kbit/s on a 5 km distance
  - Temperature of operation between 10 and 30 °C

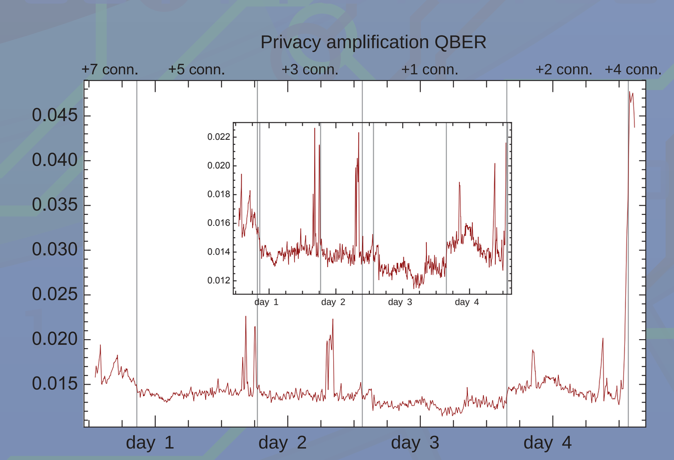
Measurements were performed for different number of fiber interconnections, different fiber types and different weldings number in quantum channel between Alice and Bob stations [7 km fiber spool SMF28 with F3000/APC, telecom standard single-mode optical dark fiber line of ca. 4.8 km and 4 up to 14 weldings (thermal optical fiber weldings), few 1-meter SMF28 fiber segments with F3000/APC and FC/PC connectors, few 2-meter SMF28 fiber segments with FC/PC connectors (interconnected via FC/PC symmetric adapters)]

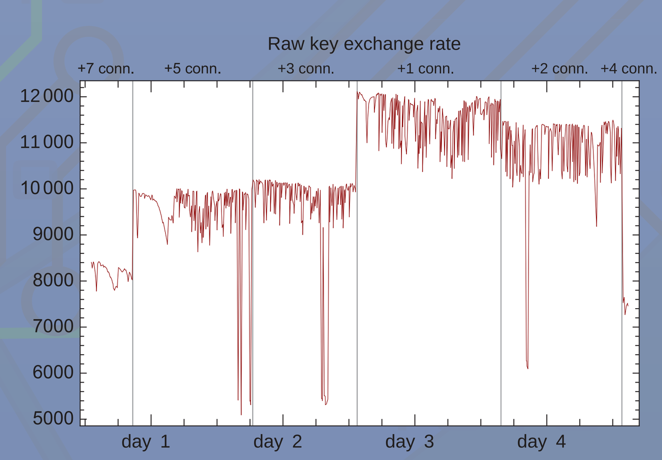
The entanglement based QKD has been tested for the first time in a real telecom network environment and proved to be also feasible but within a very narrow gap of optical elements alignment and impractically poor values of QBER and RKER with additional high instability of operation parameters. Results of the presented laboratory research were analyzed within X-R Shewhart control charts of RKER and QBER and proved as feasible deployment of the QKD metropolitan network in Wroclaw, which is currently taking place.

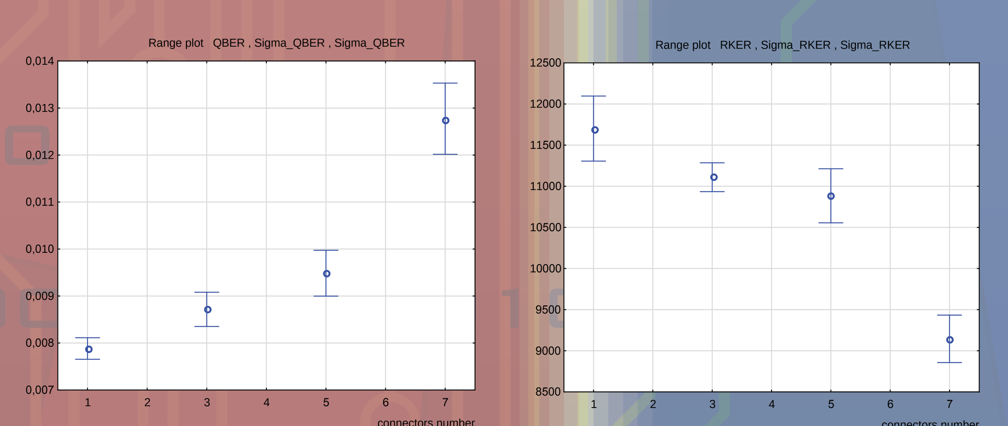


Statistical analysis: dispersion of RKER, QBER and BSD based on 274 quantum key distribution sequences









- Statistical analysis points that QBER distribution character seems not to be universal (for both systems - non-entanglement and entanglement based)
- Important issue of lack of repeatability of systems parameter measurements (for statistical analysis) - strong influence of external factors (e.g. temperature). It is difficult to observe steady work character of systems. Different passes on the same quantum channel can result with quite different results.
- Possible problems with end terminals synchronization can have some influence on measurement data.
- Observed characteristics seems to present discrete step changes of parameters - inter alia due to procedures of self-diagnostics/recalibration of systems but also due to unpredicted reactions to external factors.
- Observed QBER value, despite the difficulties resulting from unpredictable system behavior, show expected raise with the increase of connectors (introducing higher disturbance) and weldings (introduction lower disturbance) number.
- Tested systems seems to maintain efficiency only up to ca. 5 km in case of a real telecom commercial fiber

INNOVATIVE ECONOMY
NATIONAL COHESION STRATEGY

"Research and development towards commercial applications of quantum cryptography in non-entanglement and entanglement based systems" under the Action 1.4 of the Operational Programme for Innovative Economy of the Polish National Cohesion Strategy (supported by the Polish Agency of Enteprise Development PARP and National Research and Development Center of Poland NCBiR)

EUROPEAN UNION
EUROPEAN REGIONAL DEVELOPMENT FUND