Testing of feasibility of QKD system deployment in commercial metropolitan fiber networks

Monika Jacak
National Laboratory of Quantum Technology
Wrocław, Poland
jacak.monika@gmail.com

Damian Melniczuk and Lucjan Jacak
Institute of Physics
Wrocław University of Technology
Wrocław, Poland
lucjan.jacak@pwr.edu.pl

Ireneusz Jóźwiak and Piotr Jóźwiak
Institute of Informatics
Wrocław University of Technology
Wrocław Poland
ireneusz.jozwiak@pwr.edu.pl

***Abstract*—A description of test-assessment of TELECOM 1550 nm optical fiber used for a quantum channel in entangled Quantum Key Distribution (QKD) setup, EPR S405 Quelle (Austrian Institute of Technology) is presented. The system at work was observed and parameters related to dark quantum channel were collected by an appropriately designed test card. Series of measurements were carried out for various configurations of 1550 nm (optimal transmission wave-length) optical fiber patch-cord the same as used in standard metropolitan TELECOM networks including distances up to 6.5 km long. The particular attention has been paid to model the real lines with welding points and connectors in view of rigorous requirements regarded conservation of photon polarization in EPR S405 system. Tests allowed for assessment of Qantum Bit Error (QBER) level in standard telecommunication fiber infrastructure when trying to implement entangled QKD system vulnerable in particular to polarization perturbations. Another drawback, incommensurability of the central transmission wave-length in fiber with the wave-length of photons in EPR S405 system, was also assessed and the possibility of implementation of QKD EPR S405 system with 1550 nm optical fibers has been verified.**

Keywords–Quantum Key Distribution; TELECOM network; optical fibers; quantum cryptography; quantum entanglement; photon polarization

I. INTRODUCTION

Quantum cryptography is a newly developed field in the security information area [1]. It is closely related to progress in Quantum Information Processing (QIP) and utilizes advances in practical implementation of quantum technology [1][2]. Recently reported achievements in construction of large quantum computer additionally enhance significance of cryptography methods which would be resistant against attack of quantum computer. Such a technique is linked to quantum cryptography, which is regarded as absolutely safe, at least in theory. Growing importance of security of information in classical communication systems create also challenging problems for sufficient level of safety for communication at least for some special applications. In this regard, quantum cryptography also offers in principle unconditional safe protocols for secret key distribution which can be used for encryption/decryption of classical communication in OTP (One-Time-Pad) scheme. The quantum cryptography offers with this respect a method of quantum key distribution (QKD) over quantum channel of communication [1]. This channel is, however, extremely fragile and vulnerable to various perturbations. Requirement to ensure the sufficient level of so-called quantum coherency needed for error-less and safe communication is the major drawback of QKD technology severely limiting distance of quantum protected information exchange to ca. 100 km over uniform well selected laboratory optical fibers. Because TELECOM optical fiber networks used commercially in metropolitan communication systems do not meet prohibitive requirements for quantum communication as were provided in laboratory installations, there arose the question of assessment of possible usage of commercial already installed optical fiber networks to deploy QKD protected communication. This is the aim of the reported here investigation carried out in National Laboratory of Quantum Technology (Wrocław) in collaboration with a TELECOM company. In this report we summarize tests of commercial communication patch-cords of optical fibers supplied by the TELECOM company, which are the same as typically installed in metropolitan network. In particular, the tested lines where attributed with numerous weldings of fibers and standard connectors also typical in telecommunication practice. The length of tested quantum lines varied between several meters up to 6.5 km. The commonly used fibers works at transmission window close to 1550 nm (infra-red) and the usefulness of such fibers to apply as quantum channel was an especially important question to answer.

The object for testing was the QKD system on entangled photons, EPR S405 Quelle designed and manufactured by Austrian Institute of Technology (AIT) [3]. Verification of the possibility of application of commercial network fibers to establish dark quantum channel for EPR S405 Quelle system was performed with emphasizing the role played by polarization characteristics of optical fibers because the tested system employs polarization of photons as flying qubits for quantum Alice-Bob communication. The photon polarization has a fragile character and high level of coherence (conservation of particular quantum state) is required by QKD protocol utilizing quantum entanglement phenomenon in terms of photon polarization.

Moreover, the photons for the dark channel of communication in the original EPR S405 system have wave-length 810 nm near infra-red photons while the standard 1550 nm wave-length fibers poorly fit with their transmittance maximum to the carrying qubit photon wave-length. Therefore, to answer the question whether is it possible to use EPR S405 system in commercial networks 1550 nm, commonly utilized at present

 ISBN: 978-1-61208-365-0

in city networks in already installed optic fiber connections, seems to be of high significance for QKD practical implementation without additional cost for new connection lines better adjusted to photon wave-length.

II. Short characterization of QKD EPR S405 Quelle system

Generally, there are two types of QKD systems: one type create systems using nonentangled photons for dark quantum communication, and the second type–systems employing entangled pairs of photons. The former are more popular and encode quantum information in the phase of the light, additionally using quantum generator of random numbers for tossing the phase. In this sense, they are not strictly quantum and as a matter of fact it is not proved their equivalence to real quantum systems with discrete variables, though such a installations allow for successful implementation of the fundamental QKD protocol, BB84 [4] and its modifications like SARG04 [5]. The system on entangled photons is more fundamentally quantum, as utilizes completely nonclassical phenomenon of quantum entanglement. At present there is only one such system produced by Austrian Institute of Technology spin-off Vienna University conducted by Zeilinger's group [3]. This system called EPR S405 Quelle (the acronym EPR indicates linkage to commonly known Einstein-Rosen-Podolsky paradox positively resolved by experiment of Aspect in eighties of the last century [6]). Entanglement takes advantage of linear property of tensor product of Hilbert spaces, and corresponds to the decomposition of the wave function of larger system onto components related to subsystems A and B,

$$\Psi_{AB} = \sum_{i,j} c_{ij} \psi_A \otimes \psi_B. \quad (1)$$

Due to this simple property, none of two subsets A or B is its own pure quantum state as due to summation many various pure states of both systems $\psi_{A(B)}$ contribute to the total wave function Ψ_{AB}. The latter state is called as entangled if the formula (1) cannot be factorized [1]. In such a case, both subsystems are linked in quantum sense and have mutually exchanged information symmetrically imprinted in both (according to so-called Schmidt representation) [1][2]. The mutual dependence of entangled photons utilized in EPR S405 system provides higher level of security for QKD precluding possibility of some class of hacker attacks in the case of imperfect opto-electronics of cryptography devices. This costs, however, the lower tolerance for various, even small perturbations, because entanglement is extremely vulnerable and fragile. Therefore, a verification of stability of this system in conditions of real imperfect optical fiber networks is of particular importance. Two EPR S405 systems are installed and available in Wroclaw at NLQT WUT and in laboratory of CompSecur.

EPR S405 QKD system was designed to implement E91 protocol [7] accommodated to entangled carriers of information, i.e., flying qubits. In EPR S405 system, flying qubits are associated with polarization of photons because entangled pairs are created here in the process called *Parametric Down Conversion* [8] in a birefringent nonlinear crystal beta Barium Borate (BBO). In BBO crystal, a photon with energy $\hbar\omega$ decays upon nonlinear process into two photons, each with half the original energy $\hbar\omega/2$. Birefringence allows then for

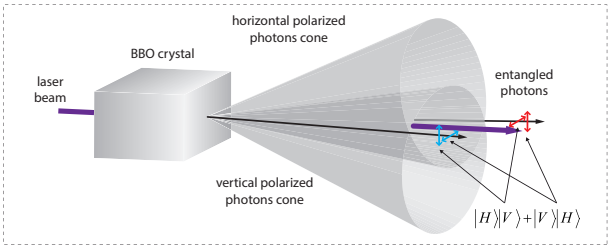

Figure 1. Generation of entangled photon pair in birefringent, nonlinear crystal BBO as a result of photon decay into two photons with half energy each; in the birefringent crystal there are created two conical photon beams with opposite polarization (upper beam with vertical polarization and lower beam with horizontal polarization); at the intersection of the cones, the states have not determined polarization—they are mixed states of entangled photons

creation of two conical beams, the upper one with vertical polarization and the lower one with horizontal polarization; see Fig. 5. At the intersection of the two beams the photons do not have a defined polarization and there are created entangled states of photons. In EPR S405 Quelle system there is used BBO crystal illuminated by laser diode (power 500 mW and wave-length 405 nm [violet]). The wave-length of entangled photons is thus 810 nm [near infra-red]. Photons are then separated by prism mirrors and guided along appropriately selected paths to realize E91 protocol. Generation of entangled photon pairs takes place in a component located in Alice station and still entangled photons travel then separately, one of them to the distant Bob station. Due to quantum link between both entangled photons any perturbation over the Alice-Bob channel could be detected by the counterpart photon at Alice which protect the system against eavesdropping by third party (Eve), but also rises sensitivity to any noise caused decoherence. EPR S405 Quelle system allows to organize communication between Alice and Bob blocks over quantum fiber channel or, alternatively, with telescope open-air connection. According to the producer (AIT), fiber connection has the range of about 50 km, while telescopic connection has the range of approximately 1 km (provided little optical perturbations along the open-air connection) [3]. In EPR S405 Quelle system, Alice block is more complicated than Bob one—it contains a component generating pairs of entangled photons. Although Bob block is less complicated, both blocks contain complete sets of avalanche detectors (four in Alice station and four in Bob station). Each of the stations is connected to separate computers, which control the system and quantum key distribution process.

A. Why 1550 nm wave-length optical fiber networks?

EPR S405 set allows for two ways of transmitting photons between parties in quantum communication, depending on the user decision. If telescopes are chosen, there should be some modifications done compared to fiber connection (other configuration elements and classical channel do not need to be modified). However, for metropolitan communication network the optical fiber connections would be of more interest because of highly developed already infrastructure of a city communication systems.

For generating photon pairs in EPR S405 system it is used 405 nm laser beam which generates pairs of photons

 ISBN: 978-1-61208-365-0

of 810 nm wave-length (in principle it could be shifted as the properties of BBO crystal are maintained in larger range and an application of another laser would result in distinct wave-length, accommodated to optimal Alice-Bob transmission requirements). 810 nm fits to the so-called first telecommunication window, which was suitable to transmit light within $800 - 900$ nm band. The problem with such a window is that fibers have relatively high losses at these wave-lengths. Further development of fiber networks led to proposing of the so-called second telecommunication window. This window is defined around 1300 nm wavelength. Current optical networks are, on the other hand, built based on 1550 nm window (called as third telecommunication window) because of better transmission properties of optical signal with this wave-length even over relatively long distances.

Even though the large incommensurability between photon wave-length and optimal transmission window in the present standard TELECOM networks it is interesting to verify efficiency of quantum communication over such lines. In the case of insufficient effectiveness of system work in such incommensurability condition one would take into account that the better matching of wave-length can be achieved by changing either the laser in the system or the network fiber. The latter solution is, however, especially inconvenient as connected with high cost of new large scale metropolitan network installation.

In the present report, we summarize the series of tests which have been carried out on the prototype system EPR S405 Quelle (AIT) using various configurations of standard 1550 nm wave-length optical fibers for quantum dark channel between Alice and Bob stations of the system. The parameters of the system functioning were collected using the specially designed data card and referred to the optimal functioning of the system at laboratory conditions. The main parameter is the Quantum Bit Error (QBER) which is observed in time when the secret key is created and distributed between Alice and Bob over the quantum channel. The collected series of measurements by use of this card allows for assessment of quality of the quantum communication over the fiber connection especially in view of coherence losses and polarization perturbations. This is a central problem, even more important than the signal attenuation caused by discrepancy of the optimal transmission window of the fiber with photon wave-length, because polarization is the information carrier in the considered system. Unpredictable perturbations of the polarization are induced due to birefringence of glass material of fibers connected with random strain in fibers and also by weldings and connectors typically used in conventional optical already installed networks. The measurement procedure and the results are presented in the following sections.

B. Polarization of photons as flying qubit in quantum channel

Using pairs of entangled photons to transfer information over quantum channel is based on E91 key distribution protocol [7]. The source of pairs of entangled photons sends one of the photons to Alice and the other one to Bob. The quantum state of photons is regarded as entangled one with respect to their polarizations. In the mixed state of single photon of the entangled pair none polarization is determined, i.e., this is a mixture of both mutually orthogonal polarizations according to rules of entanglement. Measurement of the polarization in this mixed state restores its value and violates entanglement. The same causes any perturbation and noise along the transmission line similarly damaging quantum coherence required for QKD protocol realization. In EPR S405 system the source is located in Alice block, but it may be installed as a separate element of the system somewhere in between Alice and Bob. The entangled photons are delivered to Alice and Bob detectors, in which their polarizations are measured in randomly selected ON bases (of two possible bases–vertical-horizontal and diagonal $\pi/4,\ 3\pi/4$). In the next step Alice and Bob use the public channel to determine only those of the measurements in which the same bases were selected by both parties, but not revealing the particular measurement results. That way a shared secret key is generated in a raw form, which then undergoes classical treatment (error correction and privacy amplification), identical to all cryptographic key generation procedures, including QKD. The first part of E91 protocol, although different in photon entanglement from standard BB84 procedure [4], is in fact equivalent to the latter. It is, however, believed that using entangled states positively influences security level, but it has not yet been proved with all details. Nevertheless, analysis of attack detections in case of entangled carriers indicates better performance of such systems. Ekert [7] suggested that his protocol security level could be increased by using Bell inequality [9], which is connected to quantum entanglement and direct application of this criterion for detecting a possible eavesdropper (unfortunately, it requires using a third basis and developing the system with more detectors) [10][11]. This approach also allows to directly verify entanglement of the states of photons emitted by the source.

The measure of quantum transmission quality is the total number of errors called Quantum Bit Error, shortly QBER, as in case of other QKD systems. To reduce its value there are used error correction procedures and privacy amplification procedures performed over public connection. The reasons of errors are technical imperfections of the system and possible eavesdropper. In case the number of errors exceed a preset error limit, the connection is considered to be eavesdropped and the whole key is discarded. In case the number of errors does not exceed the limit, correction procedures allow to eliminate errors efficiently (to any desired level), but at the cost of reducing the length of original raw key. The QBER achieving a fraction of percent up to single percent is considered as a result good enough to use the cryptographically generated quantum shared key in communication between Alice and Bob.

III. DESRCIPTION OF THE TEST PROCEDURE

A. Control of polarization

In the case of photon pair produced and utilized to communication in EPR S405 system, the mutual correlation of polarization of both counterparts of the entangled pair is fixed after measurement by Alice, which encoded a bit of cypher into it. This correlation can be, however, perturb in due of transmission of the photon to Bob in a fiber. This is caused by a polarization drift in the fiber due to its bending, strain induced birefringence, defects in connectors and in welding regions. Photons are still correlated, but we do not know at which angle. To restore perpendicularity we are using manual polarization controller.

 ISBN: 978-1-61208-365-0

After putting two perpendicularly aligned linear polarizers on both paths, we can restore original polarization correlation. To achieve it, we are changing polarization controller manipulators toward to minimize the number of counts on each path (on detectors which are counting photons with polarization perpendicular to applied by polarizers). After one obtains the values of counts as low as possible, one can, basing on the properly correlated photon number and the improperly correlated photons number, get the so-called visibility ratio (the ratio of these two amounts of photons). This ratio, when is higher than 0.9, is assumed as good enough to start communication over the quantum channel.

B. Methodology of the test—measured parameter

For quality assessment of quantum channel the observation of QBER (Quantum Bit Error Rate) value over some time is convenient. QBER is the most practical parameter displaying by the system software and describing the quality of quantum channel because it allows to estimate how much information could a potential eavesdropper get. This is because that any action of eavesdropper unavoidably causes errors which is registered and rises actual QBER. In situation when there is no eavesdropper, QBER indicates the influence of all perturbations caused by imperfections of optics and electronics in the system and in the quantum channel. Therefore, the QBER is a suitable characteristics for assessment of quality of transmission in the optical fiber used as the quantum channel. The varying in time QBER can be registered and displayed graphically by the use of special card gathering observed data and displaying them in the form of an appropriate chart.

C. Standard-mode working system

As the reference ideal quantum channel we used two 1 m long 810 nm patch-cords and we connected both parties (Alice and Bob subsystems) by them. Stable room temperature was maintained (around 20^{o}C). When short patch-cord connection is used, photon count numbers at both communication sides are at similar level (130 k to 150 k counts). In this case, we assume that the system works in an optimal manner without information losses in the quantum channel. Errors are cased only by other imperfections of the system out of the channel. After restoring-polarization-correlation as was described above, the system was restarted and the appropriate log-file from the observed process was written out in duration of around 15 minutes. Then, the system was stopped, the log-file was copied and used as an input file for GNU R script which was responsible for the extracting, formatting and plotting data.

As we see from Fig. 2, the corresponding process of generation of secret key using the quantum channel with wavelength 810 nm referencing short fibers in 15 minutes time window is stable, which we assume as the standard-mode of system operation.

D. Testing of 1550 nm wave-length fiber for quantum connection in EPR S405 system

For testing the ability to coherently transmit photons in commercially used telecommunication window (1550 nm), we have used SMF-28 fiber with the following parameters:

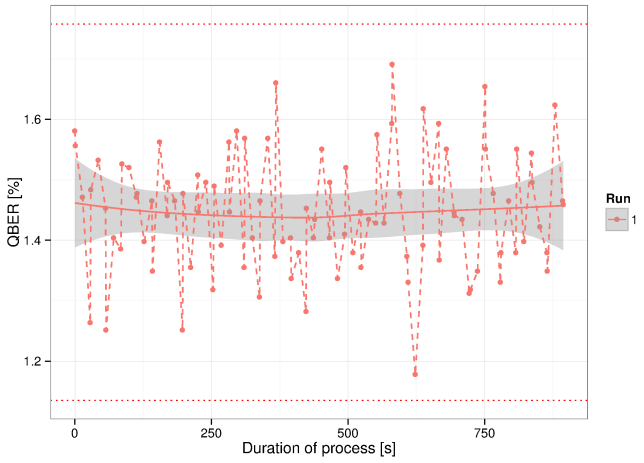

Figure 2. Plot of Quantum Bit Error Rate (QBER) in percents during functioning of EPR S405 system versus time measured in seconds. After termination of process, there were additional values calculated—local regression smoothing function (LOESS) with confidence interval and mean value with two lines: upper control limit (UCL) and lover control limit (LCL). Smoothing function is marked with solid line with gray area around which represents 95% confidence interval. UCL and LCL lines which are placed in distance 3 times standard error from mean value, are horizontal dotted lines. Since all data points are placed between UCL and LCL one can assume that plotted results were obtained in fairly stable process.

- core diameter [μm]: 8.2;
- cladding diameter [μm]: 125 $\pm$ 0.7;
- coating diameter [μm]: 242 $\pm$ 5;
- maximum attenuation for 1310 nm [dB/km]: 0.33 to 0.35;
- maximum attenuation for 1550 nm [dB/km]: 0.19 to 0.20;
- maximum attenuation for 1625 nm [dB/km]: 0.20 to 0.23;
- dispersion for 1310 nm [ps/nm km]: less than 1.0;
- dispersion for 1550 nm [ps/nm km]: less than 18.0;
- dispersion for 1625 nm [ps/nm km]: less than 22.0;
- temperature dependence [C]: -60 to +85;
- single fiber length [m] in patch-cord: 802 $\pm$ 10;
- number of weldings/connectors in patch-cord of 6.5 km for length: $5 - 7$.

Such fibers were fixed to the system output/input establishing in this way quantum connection between Alice and Bob. After restoring the proper polarization correlation before each measurement (in the same manner as described previously) and achieving an acceptable QBER level, we started recording the measurement of QBER value over iterating series of repeating process. The collected results are summarized and plotted in Fig 3, where three distinct runs of the system with 600 m length dark channel are illustrated. In Figs. 4 and 5, the QBER observation for dark channel 1550 nm fiber with length 200 m, 400 m and 800 m, for comparison are plotted.

 ISBN: 978-1-61208-365-0

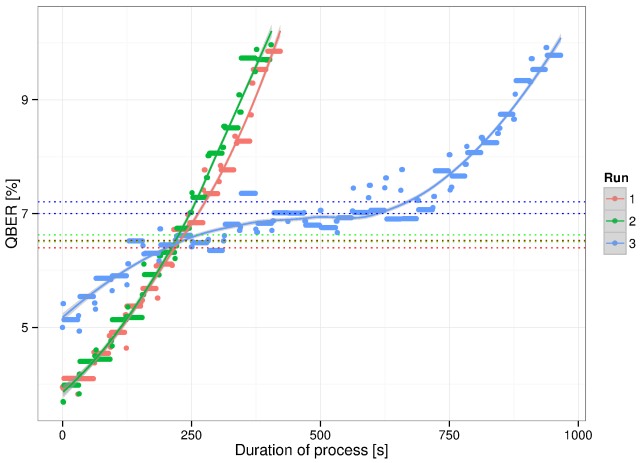

Figure 3. Improperly functioning system: plot of Quantum Bit Error Rate (QBER) in percents during three runs of EPR S405 system versus time measured in seconds. After termination of process, there were additional values calculated—local regression smoothing function (LOESS) with confidence interval and mean value with two lines: upper control limit (UCL) and lover control limit (LCL). Smoothing function is marked with the solid line (which color corresponding to color of data points) with gray area marked represents 95% One can notice the tendency to rapidly achieve critical level of QBER, precluding stable quantum communication.

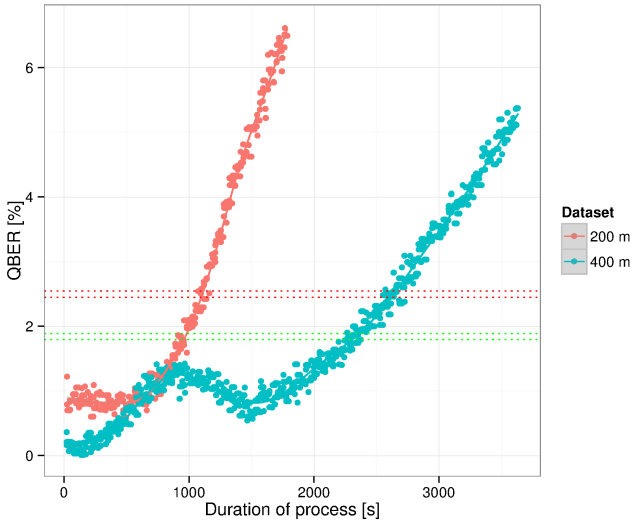

Figure 4. Multiple plots represents QBER measured for connection with 200 and 400 m (+- 10 m) optical fiber 1550 nm. Time window for measurement was one hour. Despite repeated measurements, connection based on shorter fiber was less stable. The shorter fiber brought higher ratio of polarization drift probably because of quality loss near FC/PC connectors.

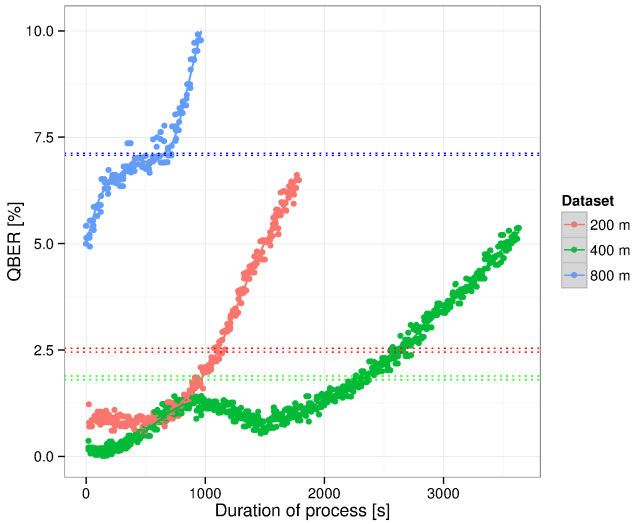

Figure 5. Multiple plots represents QBER observed for connection with 200, 400 and 800 m (+- 10 m) fiber 1550 nm. Time window for measurement was one hour. Despite repeated measurements, connection based on shorter fiber (200 m) was less stable than on two times longer fiber (400 m). The longest fiber produced accordingly to expectations the highest instability.

Control charts generated for above measurements show clearly that there are strong external or internal decoherent/destructive factors that are affecting the whole process. The initial QBER is quickly and continuously rising during the process. Moreover, after obtaining QBER value higher than 10 percent, the system stops because of too high value of error ratio. During the measurements 1 and 2 this too high value was obtained very quickly (after 454 and 438 seconds, correspondingly).

IV. Conclusion

Current implementation of entanglement photon pairs based key distribution system in EPR S405 suffers from the lack of efficient automatic polarization stability control allowing to instantly verify and improve quantum signal exchanges when connection between Alice and Bob uses standard 1550 nm fiber. By polarization stability, we mean ability to properly recognize pairs with perpendicular polarizations in both communicated parties, i.e., with required polarization correlation in the entangled pair after measurement. Without this ability, the data transmitted through the quantum channel are randomly identifying with constantly rising number of errors, which interrupts quickly the connection. To restore communication, the thorough and time-consuming manual regulation of polarization is necessary, which makes all the communication practically impossible.

To overcome this highly inconvenient tendency we propose to replace the manual polarization control with an highly-efficient automatic one. Automatic polarization controller would instantly compensate polarization drift and recover the system functionality. Such an improvement of the EPR S405 system would result in maintaining a sufficiently low and stable value of QBER ratio allowing entangled QKD over commercial network, though still for not longer distance than ca. 1 km and without weldings and connectors. The performed

 ISBN: 978-1-61208-365-0

tests indicated also that in order to improve quality of 1550 nm quantum channel, the shift of wave-length of photons is necessary by application of lower energy laser activating BBO crystal. This would allow for better matching of optimal window for transmission of the standard 1550 nm fiber. As it follows from our tests, the welding decreases quality of quantum channel in a critical manner, which is probably connected with additional polarization mishmash due to a strain and imperfections in the region of welding or standard connections. Thus, for establishing of efficient quantum channel avoiding of weldings and connectors is necessary.

The polarization of optical signal turned out to be very unstable for the tested connections, which resulted in very rapid QBER rise precluding practical usefulness of this connection for secure quantum exchange of cryptographic key over practically significant distances. The main obstacle was the polarization decoherence as well as generally poor transmitting properties of 1550 nm fiber for much shorter wave-length photons used by EPR S405 system. As mentioned above, in order to maintain the quantum channel active very frequent manual corrections of polarization control were required so we expect that by designing and applying of an automatic polarization control module one would stabilize visibility ratio and lower QBER to an acceptable level conditioning. Such a solution together with the change of laser activation energy toward longer wave-length, might admit future implementation of entangled QKD systems in commercial networks.

REFERENCES

[1] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information. Cambridge: Cambridge UP, 2000.

[2] D. Bouwmeester, A. Ekert, and A. Zeilinger, The Physics of Quantum Information. Berlin: Springer, 2000.

[3] Austrian Institute of Technology, “AIT QKD Software project documentation,” 2010.

[4] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, 1984, p. 175.

[5] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, “Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations,” Phys. Rev. Lett., vol. 92, 2004, p. 057901.

[6] A. Aspect, P. Grangier, and G. Roger, “Experimental realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A new violation of Bells inequalities,” Phys. Rev. Lett., vol. 49, 1982, p. 91.

[7] A. Ekert, “Quantum cryptography based on Bell’s theorem,” Phys. Rev. Lett., vol. 67, 1991, p. 661.

[8] D. C. Burnham and D. L. Weinberg, “Observation of simultaneity in parametric production of optical photon pairs,” Phy. Rev. Lett., vol. 25, 1970, p. 84.

[9] J. S. Bell, “On the Einstein-Podolsky-Rosen paradox,” Physics, vol. 1, 1964, p. 195.

[10] M. Curty, M. Lewenstein, and N. Lutkenhaus, “Entanglement as precondition for secure quantum key distribution,” Phys. Rev. Lett., vol. 92, 2004, p. 217903.

[11] A. Garg and N. D. Mermin, “Detector inefficiencies in the Einstein-Podolsky-Rosen experiment,” Phys. Rev. D, vol. 35, 1987, p. 3831.

 ISBN: 978-1-61208-365-0