Int. J. Communications, Network and System Sciences, 2014, 7, 30-36
Published Online January 2014 (http://www.scirp.org/journal/ijcns)
http://dx.doi.org/10.4236/ijcns.2014.71004

Testing of the Entangled QKD System EPR S405 Quelle (AIT) in Commercial 1550 nm Fiber Network

Damian Melniczuk[1], Monika Jacak[1,2]
[1]Institute of Physics, Wroclaw University of Technology, Wroclaw, Poland
[2]CompSecur Sp z o.o., Wroclaw, Poland
Email: ljacak@pwr.wroc.pl

Received October 31, 2013; revised November 30, 2013; accepted December 7, 2013

ABSTRACT

In this communication, we report results of running tests on standard telecommunication metropolitan network 1550 nm fiber applied to a quantum channel to EPR S405 Quelle prototype systems installed in National Laboratory for Quantum Technologies WUT and in CompSecur Wroclaw. Testing was carried out by means of the original design by us and applied special data card collecting parameters of functioning system allowing for assessment of quality of quantum channel. We have performed several trials using various configurations of standard 1550 nm fiber patch-cord up to length of 6.5 km with additional usage of various patch-cords with weldings and connectors which typically present in already installed commercial metropolitan communication networks. The implementation of this testing indicated that the rigorous maintenance of photon polarization is required for quantum information exchange upon EPR S405 Quelle functioning. The polarization of optical signal turned out to be, however, very unstable for the tested connection which resulted in very rapid QBER rise precluding practical usefulness of this connection for secure quantum exchange of cryptographic key over practically significant distances. We have identified that the main obstacle was the polarization decoherence caused by weldings and connectors in standard patch-cords and accidental strains in fibers as well as generally poor transmitting properties of 1550 nm fiber for much shorter wave-length photons used by the Quelle system. To maintain the quantum channel active, very frequent manual corrections of polarization control were required. So we expect that by design and application of an automatic polarization control module, one would stabilize visibility ratio and lower QBER to an acceptable level conditioning possible future implementation of entangled QKD system in commercial networks.

KEYWORDS

QKD; Entagled System; QBER

1. Introduction

Quantum Key Distribution (QKD) systems both entangled, like EPR S405 Quelle by Austrian Institute of Technology (AIT) and non-entangled, like Clavis 2 by idQuantiqe, were not sufficiently tested for usage in commercial fiber networks already implemented in standard metropolitan communication systems. Especially interesting question is the verification of the possibility of application of such commercial network to establish dark quantum channel for EPR S405 Quelle system which employs polarization entangled photon pairs as flying qubits for quantum Alice-Bob communication, because of a fragile character of entanglement and polarization coherence requirements. Laboratory dark channel communication in this system employs open space communication or in 810 nm optical fiber networks, but rather not 1550 nm wave-length fibers. Therefore to answer the question about whether it is possible to use Quelle system in commercial networks seems to be of high significance for future QKD practical utilization.

1.1. EPR S405 Quelle System

Designed and manufactured by AIT (*Austrian Institute of*

Technology, Vienna University spin-off) EPR S405 Quelle is a QKD system using entangled photons [1-5]. Two Quelle systems are installed and available in Wroclaw at NLQT WUT and in laboratory of CompSecur. The role of mobile qubits for quantum communication are played in Quelle system by photons with quantum states encoded in their polarization.

Quelle QKD system was designed to implement E91 protocol [1]. It is based on polarization measurement on entangled pairs of photons. By using BBO (*beta barium borate*) crystals one can generate large enough number of entangled photon pairs used next for communication. Entangled photon pairs are created in the process called *Parametric Down Conversion* [6] in a birefringent crystal BBO. In the crystal, photon with energy $\hbar\omega$ decay upon nonlinear process into two photons, each with half the original energy $\hbar\omega/2$. The crystal is also birefringent, which means that generated photons travel along various paths depending on the polarization. With the crystal appropriately configured, there are created two conical beams, the upper one with vertical polarization and the lower one with horizontal polarization. At the intersection of the two beams the photons do not have a defined polarization—there is created an entangled state of two photons. In EPR S405 Quelle system there is used BBO crystal illuminated by laser diode (power 500 mW and wavelength 405 nm [violet]). The laser beam is concentrated on the surface of about 25 μm radius in an appropriately cut crystal 4 mm in length. Entangled photons have wavelength 810 nm [near infrared] and are separated by small prism mirrors. In the next step both beams are concentrated on half-wave plates by lenses with focal distance 1.5 cm and then directed at additional small (0.5 mm thick) crystals BBO in order to compensate the delay of signals with different polarization (due to birefringence, the signals with different polarizations move in the crystal with different speeds). The process of generating entangled photons takes place in a component located in Alice station. 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) [7]. 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.

Using pairs of entangled photons to transfer information over quantum channel is based on E91 key distribution protocol [1]. The source of pairs of entangled photons sends one of the photons to Alice and the other one to Bob. In Quelle system, the source is located in Alice block, but it may be as well a separate element of the system. The entangled photons are delivered to Alice and Bob detectors, in which their polarization is measured in randomly selected ON bases (of the two possible ones-vertical-horizontal and diagonal $\pi/4$, $3\pi/4$). In the next step Alice and Bob use public channel to determine only those of the measurements in which the same bases were selected by both parties. That way a shared secret key is generated in 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 [8], is in fact equivalent to the latter. It is also believed that using entangled states positively influences security level, but it has not yet been proven. Analyzes of attack detections in case of entangled carriers, however, indicate this systems better performance. In his work [1], Ekert 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 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 exceeds 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 thus achieved is a fraction of percent, which is considered a result good enough to use the cryptographically generated, quantum shared key in communication between Alice and Bob.

Quelle set allows for two ways of transmitting photons between parties in quantum communication, depending on the users' decisions. 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). Alice module does not contain a built-in telescope [5]—this is a separate segment. However, for metropolitan communication net-

work the optical fiber connections would be of more interest because of highly developed already infrastructure of a city communication systems.

1.2. Why 1550 nm Wave-Length Optical Fiber Networks?

For generating photon pairs in Quelle system it is used 405 nm laser beam which generates pairs of photons of 810 nm wave-length. 810 nm fits to the so-called first telecommunication window, which was suitable to transmit light within 800 - 900 nm band. 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 wave-length. Current optical networks are, on the other hand, build 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.

In the present report we summarize the series of tests which has 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 by using the specially designed data card. The main parameter is the 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 fiber connection especially in view of coherence losses and polarization perturbation (the latter induced also by weldings, random strain in fibers and by connectors). The measurement procedure and the results are presented in the following sections.

2. Desrciption of the Test Preocedure

2.1. Control of Polarization

We know that photons in pair in Quelle system are perfectly correlated in such way, that second photon is perpendicularly polarized to the first one. After transmission in single mode fiber this property is lost. Photons are still correlated but we do not know at which angle. To restore perpendicularity we are using manual polarization controller.

After putting two perpendicularly aligned linear polarizers on both paths just before SMF we can restore original polarization relation. 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 perpendicular to applied polarizers).

After one obtains the values of counts as low as possible, one can, based on the correctly correlated photon number and the incorrectly correlated photons number, calculate the so-called visibility ratio. This ratio when is higher than 0.9 is considered as good enough to start communication over the quantum channel (**Figures 1** and **2**).

2.2. Methodology of the Test-Measured Parameter

For measuring quality of quantum channel we decided to observe QBER (Quantum Bit Error Rate) value over some time. QBER is most practical parameter describing quality of quantum channel because it allows us to estimate how much information could a potential eavesdropper get. In situation when there is no eavesdropper, QBER shows how much perturbations are introduced by imperfections of optics and electronics.

For detecting if there are any external perturbation factors that are influencing quantum key distribution, we applied control charts to gather the observed data.

2.3. Standard-Mode Working System

For testing undisturbed quantum connection we prepared two 1 m long 810 nm patchcords which are then used to connect both parties (Alice and Bob subsystems). Stable room temperature was maintained (ca. 20˚C). When short patchcord connection is used, photon count numbers at both communication sides are at similar level (130 k to 150 k counts). After restoring the polarization correlation system was restarted and the appropriate logfile from the observed process was written out in duration of ca. 15 minutes. Then the system was stopped, the logfile 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 the **Figure 2**, the corresponding process of generation of secret key using the quantum channel with wave-length 810 nm referencing fibers in 15 minutes time window is stable.

2.4. Testing of 1550 nm Wave-Length Fiber for Quantum Connection in Quelle System

For testing the ability to coherently transmit photons in third telecommunication window networks we have used SMF-28 fiber with the following parameters:

- core diameter [μm]: 8.2;
- cladding diameter [μm]: 125 ± 0.7;
- coating diameter [μm]: 242 ± 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

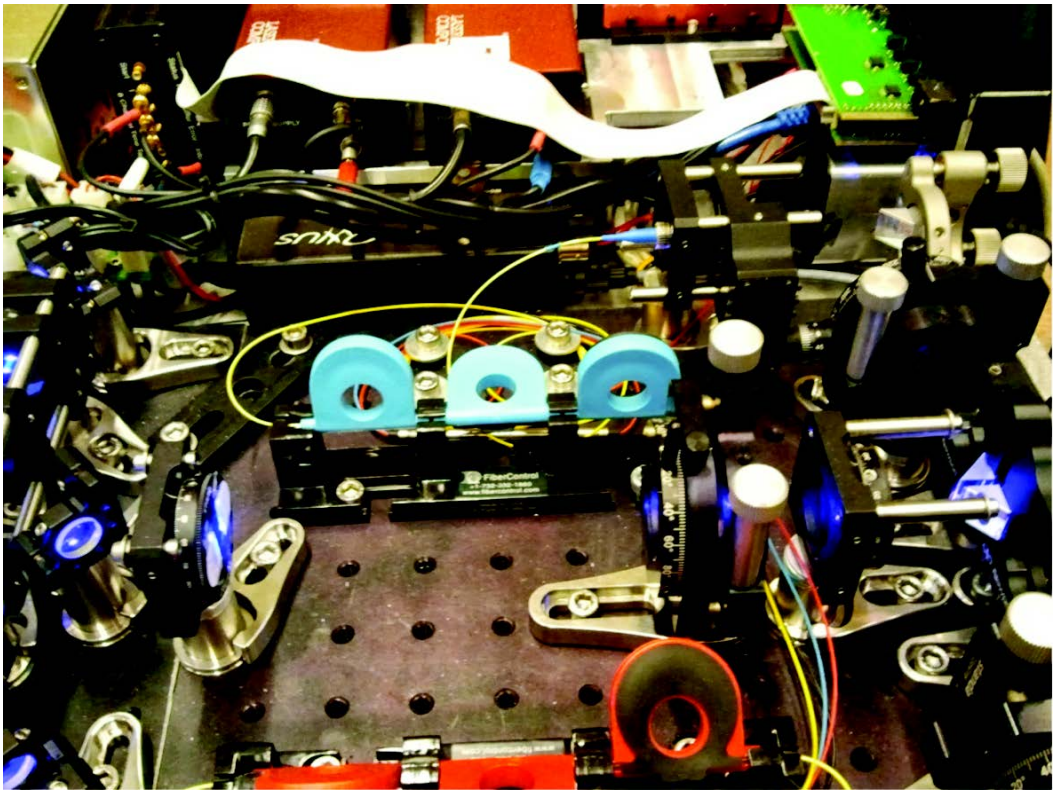

Figure 1. View at the setup of manual polarization controller in Quelle system.

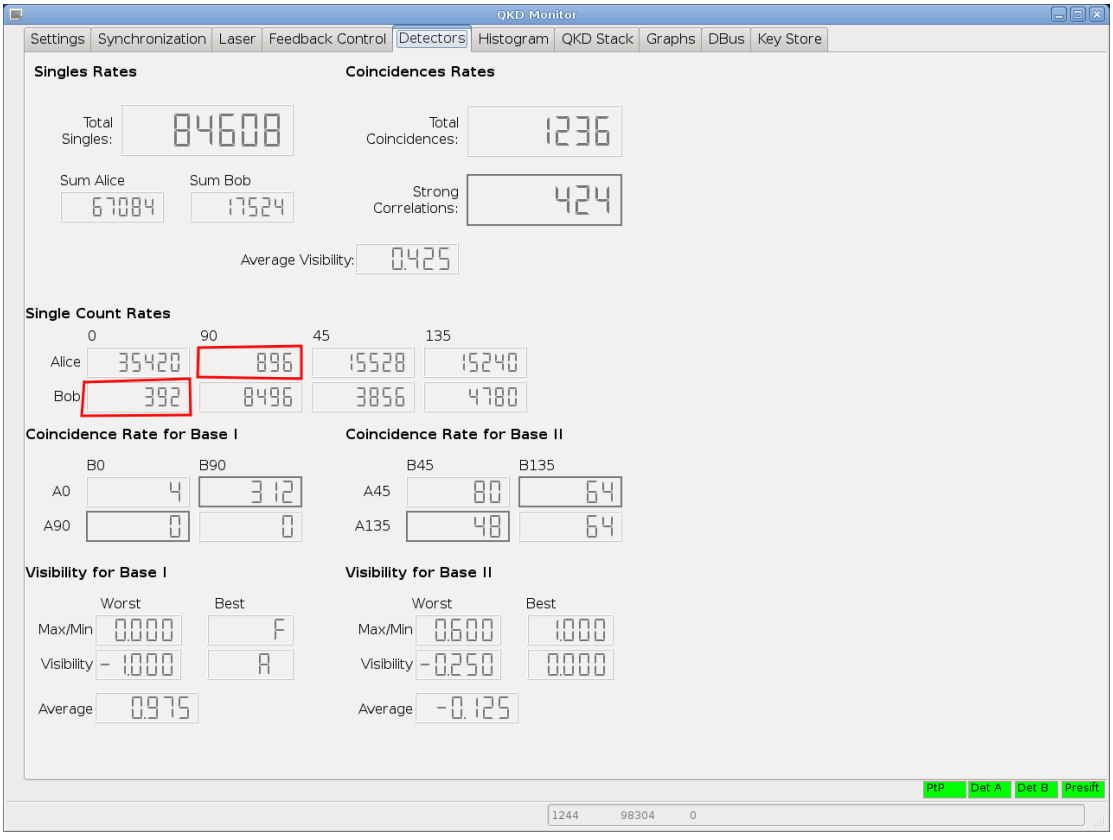

Figure 2. Example of minimized values of counts on detectors during polarization control.

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 ± 10;
- number of weldings/connectors in patch-cord of 6.5 km for length: 5 - 7.

After restoring the proper polarization correlation (in the same way 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 three following images, **Figures 3-6**.

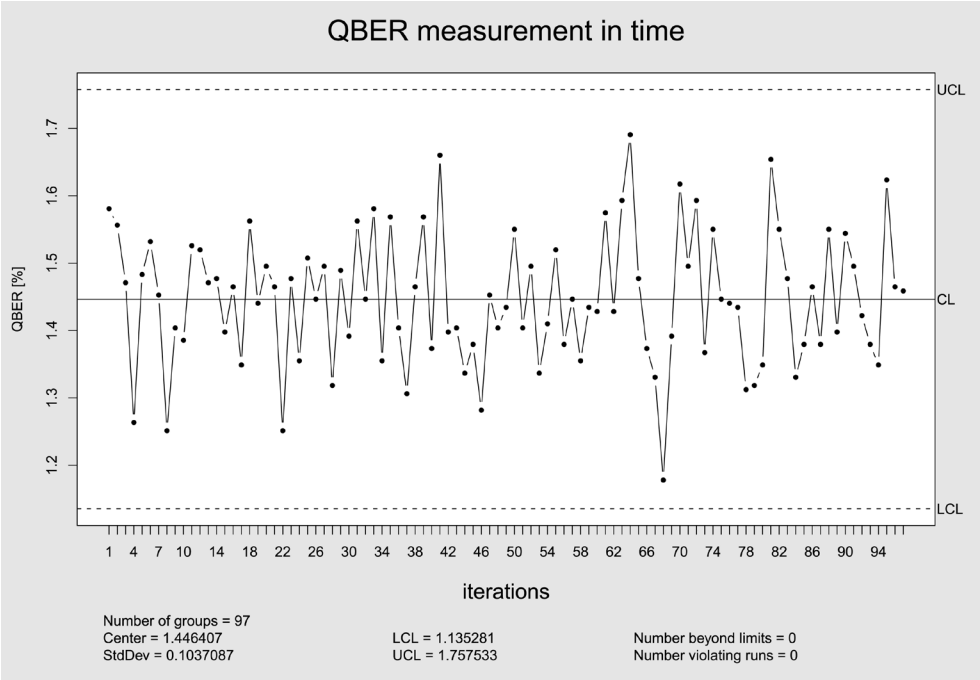

Figure 3. An exemplary plot of QBER from properly functioning system.

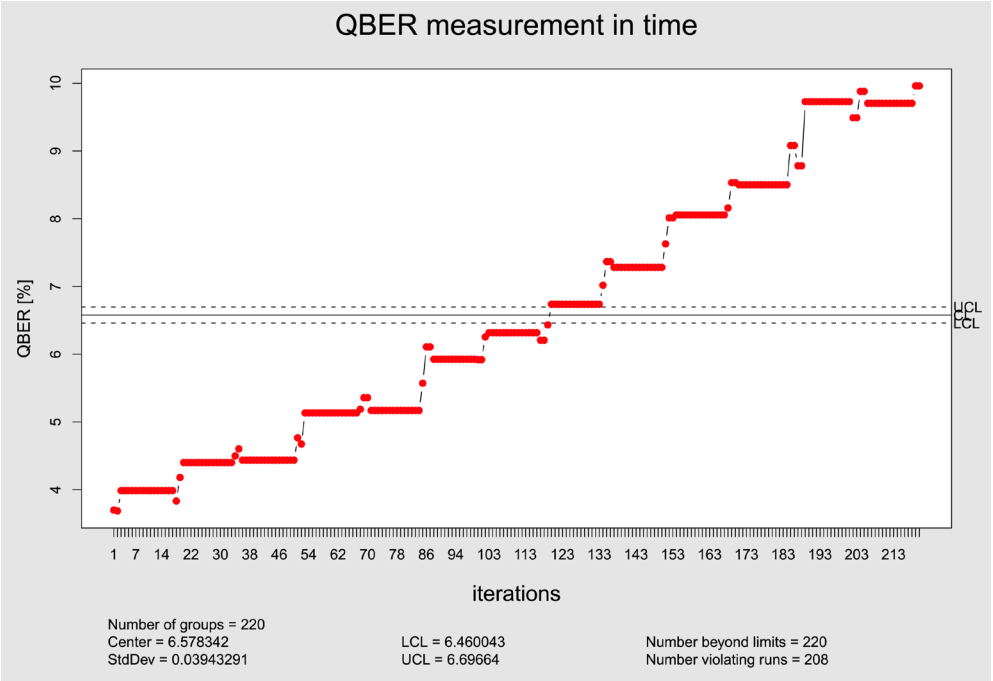

Figure 4. Improperly functioning system 1 (454 seconds).

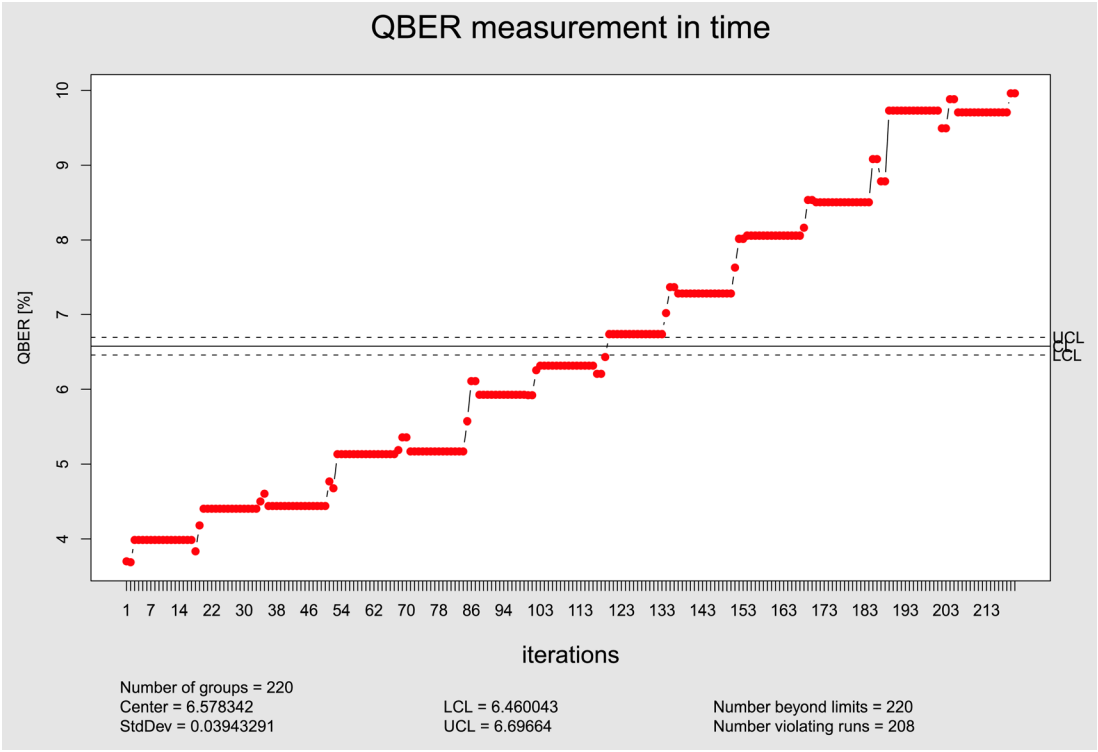

Figure 5. **Improperly functioning system 2 (438 seconds).**

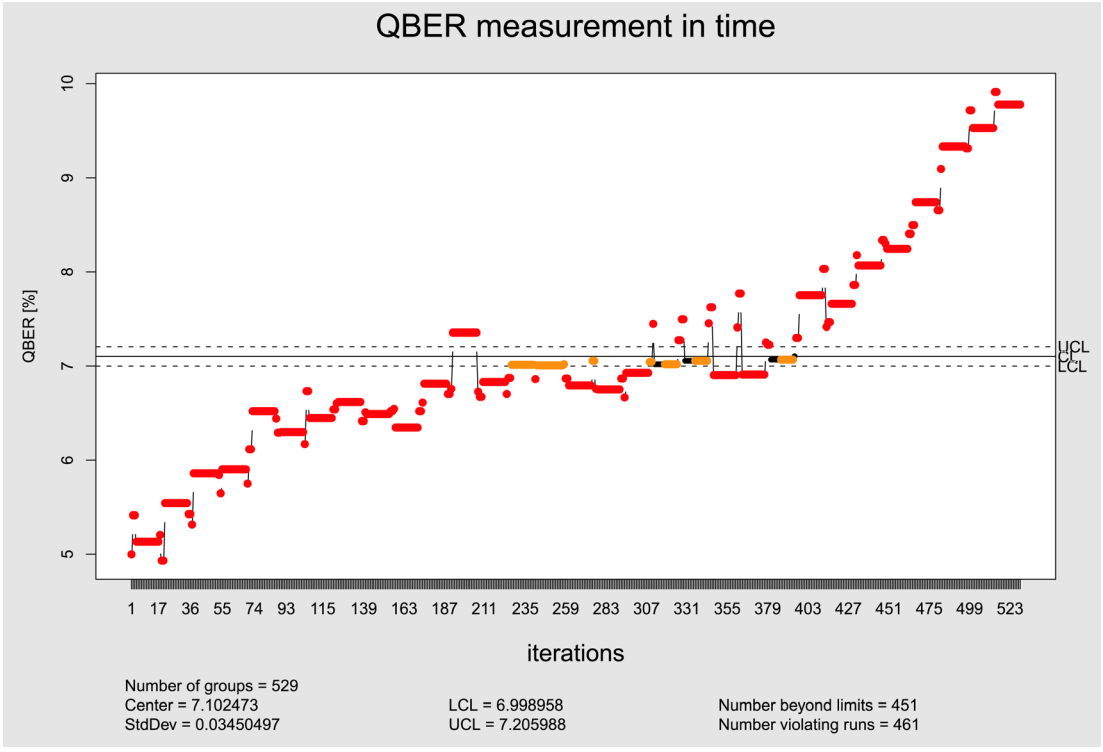

Figure 6. **Improperly functioning system 3 (1000 seconds).**

Control charts generated for above measurements show clearly that there are strong external or internal decoherence/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 be-

cause 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).

3. Conclusions

Current implementation of entanglement photon pairs based key distribution system suffers from the lack of sufficient automatic polarization stability allowing arranging quantum signal exchanges when the connection between Alice and Bob uses standard 1550 nm fiber. By polarization stability, we have ability to properly recognize pairs with perpendicular polarization in both communicated parties. Without this ability, the data transmitted through the quantum channel are randomly identified with the constantly rising number of errors, which quickly interrupt the connection. To restore communication, the 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 improvement of the Quelle system would result in maintaining a low and stable value of QBER ratio allowing entangled QKD over commercial network, though it is not longer distance than ca. 1 km and without weldings and connectors. As it follows from our tests, the welding decreases the quality of the quantum channel in critical manner, which is probably connected with an additional polarization mishmash due to a strain and imperfections in the region of welding or connector.

REFERENCES

[1] A. Ekert, "Quantum Cryptography Based on Bell's Theorem," *Physical Review Letters*, Vol. 67, 1991, pp. 661-663. http://dx.doi.org/10.1103/PhysRevLett.67.661

[2] D. Enzer, P. Hadley, R. Gughes, C. Peterson and P. Kwiat, "Entangled-Photon Six-State Quantum Cryptography," *New Journal of Physics*, Vol. 4, 2002, pp. 45.1-45.8.

[3] J. Pan, C. Simon, C. Brukner and A. Zeilinger, "Entanglement Purification for Quantum Communication," *Nature*, Vol. 410, 2001, pp. 1067-1070. http://dx.doi.org/10.1038/35074041

[4] A. Ekert, J. Rarity, P. Tapster and G. M. Palma, "Practical Quantum Cryptography Based on Two-Photon Interferometry," *Physical Review Letters*, Vol. 69, 1992, pp. 1293-1295. http://dx.doi.org/10.1103/PhysRevLett.69.1293

[5] M. Lindenthal, "Long-Distance Free-Space Quantum Communication with Entangled Photons," Ph.D. Thesis, Vienna University, Vienna, 2006.

[6] D. C. Burnham and D. L. Weinberg, "Observation of Simultaneity in Parametric Production of Optical Photon Pairs," *Physical Review Letters*, Vol. 25, 1970, pp. 84-87. http://dx.doi.org/10.1103/PhysRevLett.25.84

[7] Austrain Institute of Technology, AIT QKD Software Project Documentation, 2010.

[8] 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*, Bangalore, 10-12 December 1984, pp. 175-179.

[9] J. S. Bell, "On the Einstein-Podolsky-Rosen Paradox," *Physics*, Vol. 1, No. 3, 1964, pp. 195-200.

[10] M. Curty, M. Lewenstein and N. Lutkenhaus, "Entanglement as Precondition for Secure Quantum Key Distribution," *Physical Review Letters*, Vol. 92, 2004, Article ID: 217903. http://dx.doi.org/10.1103/PhysRevLett.92.217903

[11] A. Garg and N. D. Mermin, "Detector Inefficiencies in the Einstein-Podolsky-Rosen Experiment," *Physical Review D*, Vol. 35, No. 12, 1987, pp. 3831-3835. http://dx.doi.org/10.1103/PhysRevD.35.3831