Second Generation QKD System over Commercial Fibers

Laszlo Bacsardi
Institute of Informatics and Economics
University of West Hungary
Sopron, Hungary
bacsardi@inf.nyme.hu

Zsolt Kis
Wigner Research Center for Physics
Hungarian Academy of Sciences
Budapest, Hungary
kis.zsolt@wigner.mta.hu

Sandor Imre
Department of Networked Systems and Services
Budapest University of Technology and Economics
Budapest, Hungary
imre@hit.bme.hu

***Abstract*—Security of the communications could be ensured using cryptography protocols. While asymmetrical protocols can be cracked using quantum computers, the symmetrical protocols stand against quantum attacks. However, the keys need to be exchanged in a secure way. A method is offered by the quantum key distribution (QKD) protocols. The QKD system should operate close to the fundamental quantum noise level. A possible attack is to steal some photons during the communication, but every change will result in some excess noise. This is why it is important to know the base noise level of the system, and every possible solutions need to be considered to reduce the noise of the system. To foster the research in this field, we started to develop a second generation QKD system over a 16 km long single mode, ordinary telecommunications fiber and focused on noise reduction.**

CV-QKD, noise reduction, secure communication

I. INTRODUCTION

The information is crucial in our digital world and security plays an important role in nowadays used systems. Several attacks were carried out against different companies and agencies and the number of the unpublished attacks cannot be neglected as well. To ensure the secure information transfer, asymmetrical or symmetrical coding should be used between the communications parties. Mathematically, the asymmetrical coding protocols could be cracked if the attacker has unlimited time. In practical way, the nowadays used crypto protocols e.g., RSA, needs large amount of time from an attacker until being corrupted. But it will be changed with the quantum computers which can crack asymmetrical cryptography protocols in a really short amount of time. Although the quantum mechanics based world offers many good solutions, e.g., quantum teleporting [1], superdense coding [2], quantum parallelism [3], it threatens the nowadays used asymmetrical cryptographic protocols [4]. But some symmetrical protocols stand against the quantum attacks [5]. The only question is how the keys will be exchanged between the communication parties in a post-quantum world. The quantum key distribution (QKD) is based on the laws of quantum mechanics and offers the possibility of a key exchange process which cannot be attacked or eavesdropped without the notification of the communication parties, since any attempt of eavesdropping the key will disturb the quantum states revealing the presence of an eavesdropper [6]. The result of the exchange process is a classical string of bits, which can be further applied in nowadays used symmetrical coding protocols. This means that QKD could enhance the security of our existing systems since the commercial fiber cables could be used for the communication. The only limitation originates from the nature of the quantum physics since an active repeater cannot be part of the system [7].

The currently used QKD solutions have two generations. The first generation protocols use quasi-single-photon sources, while coherent laser is used and the wave properties of light is exploited in the second generation protocols. This first approach is named as Discrete Variable QKD (DV-QKD), the second one is named as Continuous Variable QKD (CV-QKD) [8]. Since 1984, when the first QKD protocol was published, several key exchange methods were introduced. However, sources which emit only a single photon at a time are technically complicated, and the detection of single photons is a challenge. This is why the second generation of QKD protocols has appeared where typically 60-80 photons carry the quantum information. When the two communicating parties, Alice and Bob have the necessary quantum information, they perform some classical steps and the key for symmetrical coding will appear at both sides. The system should operate close to the fundamental quantum noise level. A possible attack is to steal some photons during the communication, but every changes will result in some excess noise. This is why it is important to know the base noise level of the system, and every possible solutions need to be considered to reduce the noise of the system. To foster the research in this field, we started to develop a second generation QKD system over a 16 km long

978-0-9928-6265-7/16/$31.00 ©2016 IEEE

single mode, ordinary telecom fiber and focused on noise reduction.

This paper is organized as follows. A short overview of QKD systems is discussed in Section 2. Our CV-QKD system is introduced and detailed in Section 3. The challenges of noise reduction are answered in Section 4, while Section 5 concludes our paper.

II. Overview of QKD Systems

There are two main technologies of QKD, discrete variable (DV) where key information is encoded on the properties of single photons such as the polarization or phase, and continuous variable (CV) where key information is encoded into the quadrature variables of coherent or squeezed states. DV-QKD systems detect the information by single photon measurements, which are replaced in CV-QKD protocols by the homodyne or heterodyne detection techniques.

DV-QKD systems started their carrier with single photon solutions in 1984. The first workable quantum key distribution protocol was invented by Bennett and Brassard [9, 10]. The earliest discussion of privacy amplification can be found in [11]. Later it was extended in [12, 13]. Bennett reduced the number of handshaking of the BB84 protocol in 1992, this solution is often referred as the B92 protocol [14]. Although this protocol proves to be safe theoretically because non-orthogonal states cannot be measured and copied without perturbation, unfortunately it has some drawbacks in practice. This lies in the fact that in exchange of some losses the states can be distinguished unambiguously [15]. To realize these losses, Alice and Bob have to monitor the attenuation of the channel, however, if Eve is able to influence this property of the channel then she can trick out the communicating parties. Compared to the two-state B92 and four-state BB84 protocols, an obvious step ahead is if one considers a two-state protocol for instance as Bruss [16] in 1998 or Bechmann and Gisin [17] did in 1999. The applied six states belong to three different basis. This causes on one hand that the probability of using the same basis by Alice and Bob reduces to 1/3, on the other hand, the bit error ratio originating from Eve's action increases to 33% instead of 25% experienced at the BB84 protocol.

The first successful experiment related to quantum key distribution was carried out at IBM by in 1989 [12]. Bennett and his team managed to transfer keys over a short link 30 cm of length. Muller and his colleagues [18] at University of Geneva, Switzerland increased this distance first to 1100 m in 1993, which was extended [19, 20] to 23 km in 1995. They implemented the BB84 protocol over a traditional optical fiber under Lake Geneva, which was the first experiment outside a laboratory. In the meantime, Huttner and his colleagues [21] (1996) and Clarke et al. [22] (2000) have demonstrated how to eavesdrop the B92 protocol in practice. Due to the nature of the communications, there are several differences between the fiber-based and free-space QKD including the devices and the noises appearing in the quantum channels. Jacobs and Franson [23] were the first who managed to demonstrate outdoor free space key distribution over 75 m in 1996. Ursin and his team reached 144 km over terrestrial free-space links in 2007 [24]. Quantum communication over global scale can be established by means of satellite links [25,26]. As the most dynamically developing area in quantum computing, the quantum key distribution has already reached the commercialization phase, see e.g., [27]. DV-QKD systems suffer two drawbacks, namely it is hard to generate and detect single photons. Therefore CV-QKD solutions offers more efficient operation.

The basic CV-QKD protocols use Gaussian distributed classical information encoded into coherent states [28,29,30] of a laser field. Due to the quantum channel noise this results in two correlated sets of so called raw data that form an information theoretic connection between Alice and Bob. Classical ciphering keys can be extracted from this information by means of using classical reconciliation and post-processing techniques.

There are two major problems with CV-QKD systems that limit the practical distance for communication. On one hand the presence of excess noise combined with high losses (~0.2 dB/km) in the optical channel limits the communication. On the other hand the classical reconciliation efficiency means serious bottleneck. Different solutions exists for noise reduction including using self-reference signals by Soh et al. [31]. Commercial optical fibers have been serving as high speed physical links between distant points for decades. They are deployed all over the world offering medium for QKD systems if these systems are able to handle both quantum and the corresponding classical communication protocols over the same fiber.

III. The Proposed System

The scheme of our system is shown in Fig. 1. It is a fiber optic interferometer of Mach-Zender type, where the sender (operated by Alice) and the receiver (operated by Bob) units are separated by a standard single mode telecom fiber, whereas the sender and receiver units are realized by polarization maintaining fiber optic elements. At Alice side, the sender produces a stronger reference light pulse and a weak, amplitude and phase controlled signal pulse. The light source is a continuous wave (CW), narrow linewidth of ~100 kHz, temperature and current stabilized diode laser, radiating at the 1.55 μm telecom wavelength. A standard fiber optic amplitude modulator (CHOP) is used to chop the CW light to 400 ns long pulses, with repetition time 4 μs. Then a beam splitter BS1 is used to divide the light pulses to a reference pulse (red, reference arm) and a signal pulse (blue, signal arm). In the signal arm subsequent electro optic amplitude and phase modulators (AM and PM1, respectively) are used to set the amplitude and relative phase of the signal pulse with respect to the reference pulse. Finally, an attenuator reduces further the intensity of the signal pulse. The next element is a delay line (DL1) causing 500 ns time delay for the signal pulse with respect to the reference pulse. The pulses propagating in the reference and signal arms are combined at the polarizing beam splitter PBS1, so that their polarization states are orthogonal at the output.

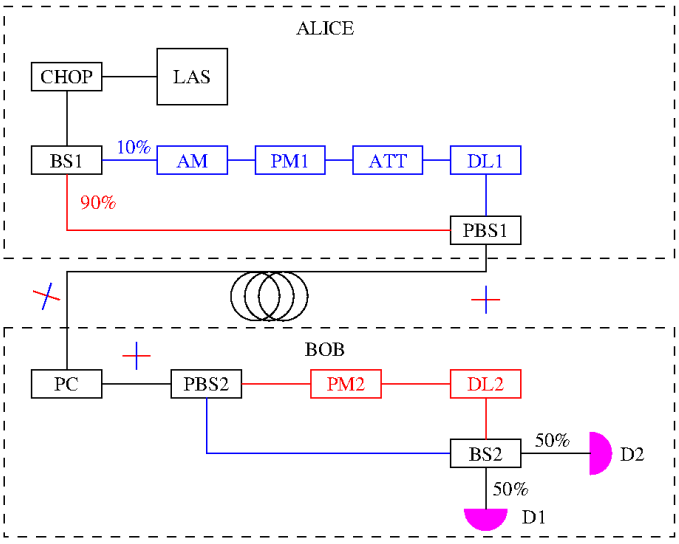

Figure 1. The scheme of our system, see the text for detailed explanation about the arrangement.

After the reference and signal pulses leave Alice's device, they travel through a 16 km long single mode, ordinary telecom fiber. At the other end of the fiber, the polarization state of the light pulses should be restored by the polarization controller PC. At Bob side, the reference and signal pulses are separated by the polarizing beam splitter PBS2. In the reference arm, the phase modulator PM2 and delay line (DL2) conditions the reference pulses to measure the Q or I quadrature of the signal pulses with a homodyne detector, realized by the 50:50 beam splitter BS2 and two linear photodetectors, and the currents of the photodetectors are subtracted and the difference current is amplified with a large bandwidth, low noise transimpedance amplifier. Alice and Bob units are controlled by one-one PCs furnished with high speed DAQ cards.

The quantum information to be sent is coded to the field quadratures of the signal pulses created by Alice. The two quadratures have independent Gaussian distributions. Bob's goal is to measure one of the quadrates of the received signal pulses.

IV. NOISE REDUCTOIN

As we mentioned in Sec. 3, Alice's and Bob's devices together form an extended fiber optic interferometer. In Alice's sender and Bob's receiver the reference and signal paths are separated, as in an ordinary interferometer. The peculiarity of this interferometer is that the signal and the reference pulses travel together in a fiber link which connects the sender and the receiver. From interferometric stability point of view, this linkage is the most stable part of the interferometer, since both pulses traverse the same path with very little time delay. However, the polarization state of the pulses can rotate freely in the single mode fiber (although their orthogonality is maintained), hence without precise control at Bob input port, the reference and signal pulses would be confused in Bob's receiver. In our system, the polarization state is controlled by a very low insertion loss fiber optic polarization controller, the error signal emerges at the homodyne detector. The polarization controller is operated manually.

Another source of noise originates from the fluctuating arm length difference in Alice and Bob unit. At the beam splitter BS2 of the homodyne detector, the reference and signal pulses are superimposed. The electric field intensities at the two outputs of the beam splitter are given by

$$I_1 = \frac{1}{2}\left(I_R + I_s + 2\sqrt{I_R I_s}\cos(\varphi_R - \varphi_S)\right) \quad (1a)$$

$$I_2 = \frac{1}{2}\left(I_R + I_s - 2\sqrt{I_R I_s}\cos(\varphi_R - \varphi_S)\right), \quad (1b)$$

where φ_R/φ_S and I_R/I_S are the phases and intensities of the reference and signal pulses just before BS2, respectively. The electric signal at the output of the homodyne detector is proportional to the difference of the two light intensities

$$V \approx I_1 - I_2 = 2\sqrt{I_R I_s}\cos(\varphi_R - \varphi_S). \quad (2)$$

From this formula, it follows that any fluctuation in the phases φ_R/φ_S cause fluctuation in the observed signal. Therefore, it is crucial to keep the phase difference $\varphi_R - \varphi_S$ stable with respect to the unavoidable fluctuation of the arm length difference of the interferometer. Our observations show that the time scale of the fluctuation is rather long, several seconds, hence it seems feasible to eliminate this type of fluctuation (we rather call it phase drift). To this end our strategy is to send so called 'decoy' pulses between the signal pulses, shown in Fig. 2. The decoy pulses serve as reference signals, having well defined phase and amplitude.

In Fig. 2, the arrows colored in green are the decoy signals, time flows from left to right. They are always parallel to the Q axis, hence their phase is 0. Therefore, between any two useful signals (red arrows) there is always a decoy signal. In order to detect and correct the phase drift in the observed signal, Bob measures alternately the Q and I quadratures of the decoy signals. Let us say, for every odd number decoy signals the Q quadrature is measured, while for every even ones the I quadrature is retrieved. Ideally, the values of the I quadrature measurements should be zero.

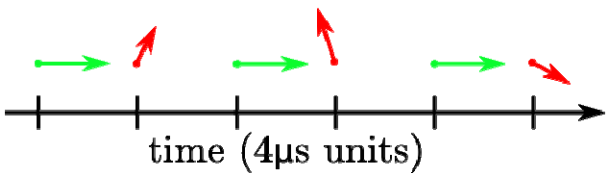

Figure 2. Pulse sequence sent by Alice. Green arrows represent the decoy signals, while red arrows represent the useful signals.

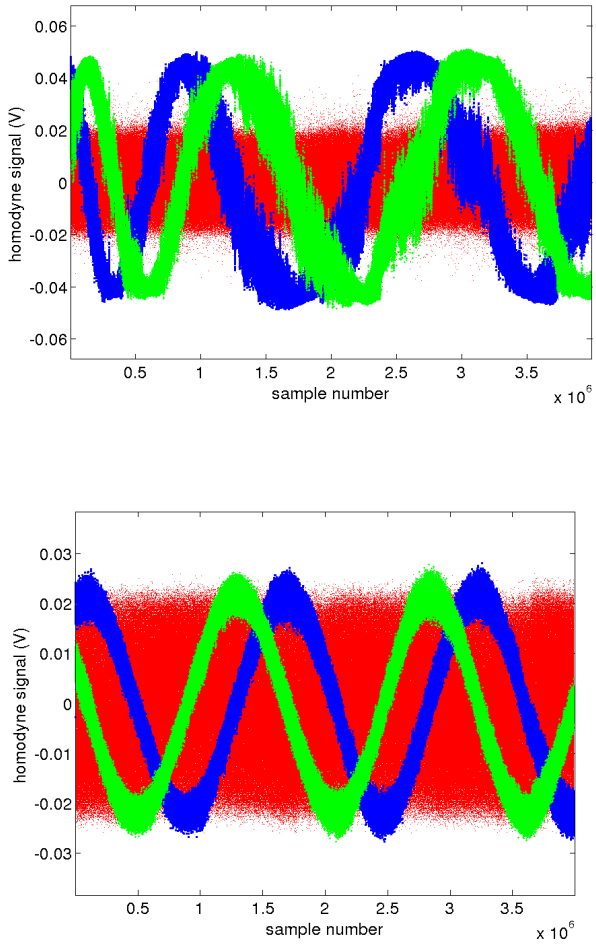

Figure 3. Pulse sequence sent by Alice detected on Bob's side: (up) received signal without arm length equalization; (down) with arm length equalization.

From the obtained *Q* - *I* pairs, the phase drift of his local coordinate system can be determined and corrected. In a recent publication [31], a similar approach has been presented. However, in that work the retrieved angle of rotation of the reference frame at Bob side has been sent back to Alice to transform her generated data set. In our case, we are going to shift the reference angle of Bob's phase modulator, i.e., follow the rotation of the reference frame with a local transformation. For slow enough phase drift, the two methods are equivalent. Furthermore, in this case it is not necessary to send decoy signals between any two useful signals. In the presented measurement in Fig. 3 (down), the period of a full rotation of Bob's local frame is 6.4s, hence it seems sufficient to send decoy pairs at 20 Hz rate.

Finally, we identified a noise source which is related to the unbalanced length of the signal and reference arms of the interferometer. In principle, this length difference matters only if it is close or larger than the coherence length of the laser. The linewidth of our laser is about 100 kHz, hence its coherence length is a few kilometers. After building the full system, the length difference between the reference and signal arms was about 2m, which is equivalent with 10ns delay, much shorter than the 400ns pulse duration. The noise of the received signal on the homodyne detector was rather high, see Fig. 3 (up). Then we added 2m extra fiber to balance the arm length difference and the noise reduced significantly, as shown in Fig. 3 (down). There is still some periodic noise of classical origin in the system that we have to reduce. Our estimation is that the width of the sinusoidal curves of the decoy signals (blue and green) is about five times larger, than the inherent shot noise limit. The consequence of all these efforts is that the system gets closer and closer to the quantum limit to the accuracy of the quadrature measurement, where further noise reduction is not possible, hence any increase in this base noise level is a hint for possible attack.

V. SUMMARY

In this paper, we presented our second generation quantum key distribution system and showed our results in noise reduction. In our CV-QKD solution, there is always a decoy signal between any two useful signals that serve as reference signals to correct the phase drift in the interferometer. We identified a noise source which is related to the unbalanced length of the signal and reference arms of the interferometer. There is still some excess classical noise in the system over the quantum noise level, hence further work is needed to identify and eliminate it.

ACKNOWLEDGMENT

The authors acknowledge the support of the Hungarian Scientific Research Fund (OTKA K112125).

REFERENCES

[1] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," Phys. Rev. Lett., vol. 70, no. 13, pp. 1895–1899, Mar 1993.

[2] C. H. Bennett and S. J. Wiesner, "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states," Phys. Rev. Lett., vol. 69, no. 20, pp. 2881–2884, Nov 1992.

[3] M. A. Nielsen and I. L. Chuang. "Quantum Computation and Quantum Information," Cambridge University Press, 2000

[4] L. Bacsardi, "On the Way to Quantum-Based Satellite Communication", IEEE Comm. Mag.51:(08) pp. 50–55., 2013.

[5] S. Imre and B. Ferenc, Quantum Computing and Communications: An Engineering Approach. Wiley, 2005.

[6] L. Hanzo, H. Haas, S. Imre, D. O'Brien, M. Rupp and L. Gyongyosi, "Wireless Myths, Realities, and Futures: From 3G/4G to Optical and Quantum Wireless", Proceedings of the IEEE, Vol: 100 , Issue: Special Centennial Issue, pp. 1853–1888.

[7] S. Imre, "Quantum Computing and Communications –Introduction and Challenges" COMPUTERS & ELECTRICAL ENGINEERING 40:(1) pp. 134–141, 2014.

[8] Raúl García-Patrón and Nicolas J. Cerf, "Continuous-Variable Quantum Key Distribution Protocols Over Noisy Channels", Phys. Rev. Lett. 102, 130501, 2009

[9] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing", Int. conf. Computers, Systems & Signal

Processing, pages 175–179, Bangalore, India, December 10–12 1984. e-print http://www.research.ibm.com/people/b/bennetc/bennettc198469790513.pdf .

[10] C. H. Bennett and G. Brassardm "Quantum public key distribution system", IBM Tehnical Disclosure Bulletin, 28:3153–3163, 1985.

[11] C. H. Bennett, G. Brassard and J.-M. Robert, "Privacy amplification by publicdiscussion", SIAM Journal on Computing, 17:210–229, 1988.

[12] C. H. Bennett, F. Bessette, L. Salvail and J. Smolin, "Experimental quantum cryptography", Journal of Cryptology, 5:210–229, 1992.

[13] C. H. Bennett, G. Brassard , C. Cr´epeau and U. M. Maurer, "Generalized privacy amplification", IEEE Transaction on Information Theory, 41:1915–1923, 1995.

[14] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states", Phys. Rev. Lett., 68:3121–3124, 1992. e-print http://www.research.ibm.com/people/b/bennetc/qc2nos.pdf.

[15] A. Peres, "How to differentiate between two non-orthogonal states", Phys. Lett. A, 128(19), 1988.

[16] D. Bruss, "Optimal eavesdropping in quantum cryptography with six states", Phys. Rev. A, 81:3018–3021, 1998. e-print quant-ph/9805019.

[17] H. Bechmann-Pasquinucci and N. Gisin, "Incoherent and coherent eavesdropping in the 6-state protocol of quantum cryptography", Phys. Rev. A, 59:4238–4248, 1999. e-print quant-ph/9807041.

[18] A. Muller, J. Breguet and N. Gisin, "Experimental demonstration of quantum cryptography using polarized photons in optical fiber over more than 1 km", Europhysics Lett., 23:383–388, 1993.

[19] A. Muller, H. Zbinden and N. Gisin, "Underwater quantum coding", Nature, 378:449–449, 1995.

[20] A. Muller, H. Zbinden and N. Gisin, "Quantum cryptography over 23 km in installed under-lake telecom fibre", Europhysics Lett., 33:335–339, 1996.

[21] B. Huttner, J. D. Gautier, A. Muller, H. Zbinden, N. Gisin. Unambiguous quantum measurement of non-orthogonal states. Phys. Rev. A, 54:3783–3789, 1996.

[22] M. Clarke, R. B. M. A. Chefles, S. M. Barnett and E. Riis, "Experimental demonstration of optimal unambiguous state discrimination", Phys. Rev. A, 63:040305, 2001. e-print quant-ph/0007063

[23] B. Jakobs and J. Franson, "Quantum cryptography in free space". Rev. Sci. Inst. 71, 1675–1680, 1996. e-print quant-ph/9912118.

[24] R. Ursin, et al., "Entanglement-based quantum communication over 144km," Nature Phys. 3, 481, 2007.

[25] P. Villoresi et al., "Experimental verification of the feasibility of a quantum channel between space and Earth," New J. Phys. 10, 033038, 2008.

[26] T. Jennewein and B. Higgins, "The quantum space race," Physics World 26, 52, 2013.

[27] B. Korzh. C. Ci Wen Lim, R. Houlmann, N. Gisin, Ming Jun Li, D. Nolan, B. Sanguinetti, R. Thew, Zbinden, "Provably secure and practical QKD over 307 km of optical fibre", Nature Photonics 9, 163, 2015.

[28] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N.J. Cerf and P. Grangier, "Quantum key distribution using Gaussian-modulated coherent states", Nature 421, 238, 2003.

[29] Lodewyck J. et al., "Quantum key distribution over 25 km with an all-fiber continuous-variable system", Phys. Rev. A 76, 042305, 2007

[30] L. Gyongyosi and S. Imre, "Long-distance continuous-variable quantum key distribution with advanced reconciliation of a Gaussian modulation", Proc. SPIE 8997, Advances in Photonics of Quantum Computing, Memory, and Communication VII, 89970C, February 2014; doi:10.1117/12.2038532

[31] D.B.S. Soh, C. Brif, P.J. Coles, N. Lütkenhaus, R.M. Camacho, J. Urayama, M. Sarovar, "Self-referenced continuous-variable quantum key distribution protocol", Phsys. Rev. X 5, 041010, 2015.