Optica Applicata, Vol. XLVII, No. 3, 2017
DOI: 10.5277/oa170307

High performance quantum key distribution prototype system using a commercial off-the-shelf solution: experimental and emulation demonstrations

JOSUE AARON LOPEZ LEYVA[1*], JESUS RUIZ HIGUERA[1], ARTURO ARVIZU MONDRAGON[2], JOEL SANTOS AGUILAR[2], RAUL RAMOS GARCIA[3], MIGUEL PONCE CAMACHO[1]

[1] Center of Excellence in Innovation and Design,
Center for Higher and Technical Education (CETYS University),
Camino a Microondas Trinidad s/n. Km. 1, Moderna Oeste, 22860 Ensenada, BC. México

[2] Department of Applied Physics, CICESE Research Center, Baja California, México,
Carret. Ens.-Tij. 3918, Zona Playitas, Ensenada, B.C. 22860, México

[3] Department of Electrical and Computer Engineering, University of Alabama,
Tuscaloosa, AL, 35487, USA

[*] Corresponding author: josue.lopez@cetys.mx

A continuous variable-quantum key distribution system prototype that uses weak coherent states with a diffused phase, commercial off-the-shelf devices, complete free space 90-degrees hybrid and simplified quantum protocol is proposed in this paper. In general, the quantum transmitter-receiver shows an experimental average quantum bit error rate of 30% using auto-homodyne detection with 0.25 photons per pulse in locking phase mode. The emulated final secret key rate measurements were 20 and 40 Kbps for minimum (30 Mbps) and maximum (90 Mbps) throughput, respectively, in a real traffic network using databases for the quantum keys generated by two true random number generators.

Keywords: quantum cryptography, final secret key rate (FSecKR), coherent states.

1. Introduction

Currently, the telecommunication systems require an extremely high security level due to the sensitivity of the information transmitted. The best option until the moment is the quantum key distribution (QKD) system using already the continuous (CV) or discrete (DV) variables; each one with their respective advantages and trade-offs [1–3]. In particular, the protocol used to transmit the quantum raw key (RK) through the private channel (quantum channel) and obtain the final quantum key is extremely important, since this determines the complexity (and trade-offs) of the hardware and software that will be used. For example, the BB84 and cascade protocols are the most common, basic and easiest protocols; however these require a high speed processing in order to counteract the high processing time needed for the distillation algorithms (based on the iterative procedures) developed in the classical channel [4–6]. In addition, in order to embed the QKD systems in the modern high-speed networks, QKD systems have increased the transmission rate of the final quantum key using either central processing unit (CPU), graphics processing unit (GPU) or field-programmable gate array (FPGA) [7, 8]. Thus, current commercial systems work a few kilobits per second (Kbps), although there are proposals that reach megabits per seconds (Mbps) [9, 10]. Particularly, the final secret key rate (FSecKR) is not a limiting factor if block cryptographic techniques and database for quantum keys are used [11, 12]. Moreover, actually the commercial off-the-shelf (COTS) devices have reached a tremendous acceptance in different areas of science and technology (especially in the QKD context), therefore many research and technological projects use such devices in order to make the ideas and applications more accessible and comprehensible [13, 14]. Therefore, it is important to consider the option of simplifying the QKD protocol and the complete system (as a countermeasure to the disadvantages of the COTS devices) without decreasing the security level, as well as maintaining proper cost-benefit concept. In this paper, a CV-QKD system based on weak coherent states with a diffused phase and simplified distillation protocol using a COTS device is presented.

2. Experimental set-up

2.1. Quantum set-up experiment

Figure 1 shows the general block diagram of the overall experimental set-up. A true random number generator (TRNG) based on the auto-homodyne detection of both quadrature components of a vacuum state was used in order to generate two random binary sequences (we reported it previously in [15]). These sequences can be stored in a database-random number (DB-RN) (*i.e.*, reserved memory in the COTS device) to be used in the quantum reconciliation and distillation protocols. Alternatively, both sequences can be used in real time by the digital processor. The random sequences (RSA1 and RSA2) are generated by the TRNG of *Alice* and the RSB1 by the TRNG of *Bob*. In particular, the quantum scheme of *Alice* (Fig. 1**a**) uses attenuators (ATT) for generating weak coherent states (WCS) with the diffused phase at 1550.1 nm reaching up to –130 dB of attenuation. In other words, the receiver optical power corresponds to 0.5 to 0.25 photons per pulse (22.5×10^{-15} and 11.25×10^{-15} W, respectively) considering a raw key rate (RKR) of 350 Kbps and a local oscillator power at 5 mW. The optical power of the RK was monitored using a photodetector (PD) in order to ensure the photons number per pulse and statistical information of the quantum state. Next, the interaction between the quantum transmitter-receiver and the COTS device was emulated. Thus, the *Alice's* digital device uses the RSA1 as the driver signal for the phase modulator (PM)

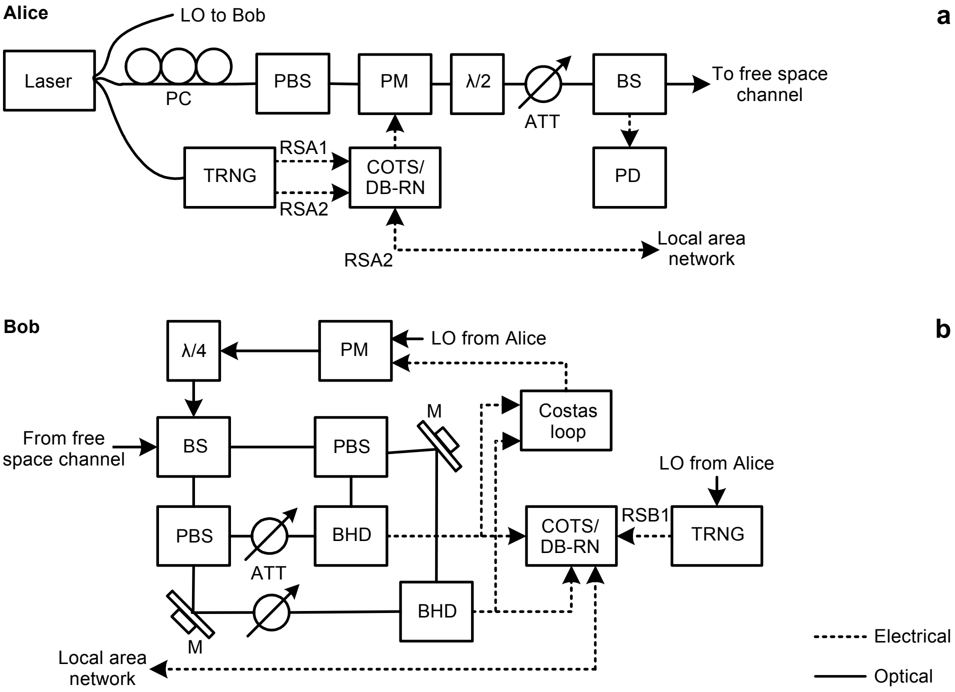

Fig. 1. General block diagram of overall system: *Alice* (**a**) and *Bob* (**b**). PC – polarization controller, BS – beam splitter, PBS – polarizing beam splitter, M – mirror, BHD – balanced homodyne detector.

in the quantum transmitter (using a binary phase shift keying modulation scheme) and it stores the RSA2 in order to perform the reconciliation protocol. Therefore, the RSA1 generates the RK sent through the private channel (free space channel) and it is photodetected by the *Bob's* quantum scheme (Fig. 1**b**). Such scheme uses a 90 deg optical hybrid completely implemented in free space and based on the states of polarization (SOPs) of the RK (linear SOP generated by a half-wave plate, $\lambda/2$) and the LO (circular SOP generated by a quarter-wave plate, $\lambda/4$) in *Bob* in order to detect the quadrature components of the RK in a simultaneous way using an optoelectronic Costas loop for the synchronization phase between the LO and the carrier signal of the RK [16].

2.2. Classical set-up experiment

The performance of the complete system was measured using a Raspberry Pi (single -board computer that uses a system-on-chip (SoC) at 400 MHz standard clock speed) as a COTS device within a local area network (LAN) at 100 Mbps in a client–server environment (*Bob* and *Alice*, respectively). The RK photodetected (*i.e.*, RK in electric and binary format) is stored by *Bob's* digital device in order to perform the reconciliation process based on the BB84 protocol using RSA2 and RSB1. Similarly, *Bob* has the option of using a DB-RN to store the RSB1 too, in real time. Once that the sifted key (SK) was determined, the quantum bit error rate (QBER) is measured according to the coherent detection scheme used in order to detect the existence of a spy (*Eve*) system. If a spy is detected, the communication process is aborted immediately, otherwise, the distillation process will be performed. Next, *Alice* and *Bob* systems detect and eliminate the errors in the SKs in order to reduce the processing time of the COTS devices; the last leads to the reduction in the length of the final key within the digital processing but increases the sifted key rate (SKR), which is regarded as a simplification of the protocol. In addition, the detection and elimination of errors (without correction)

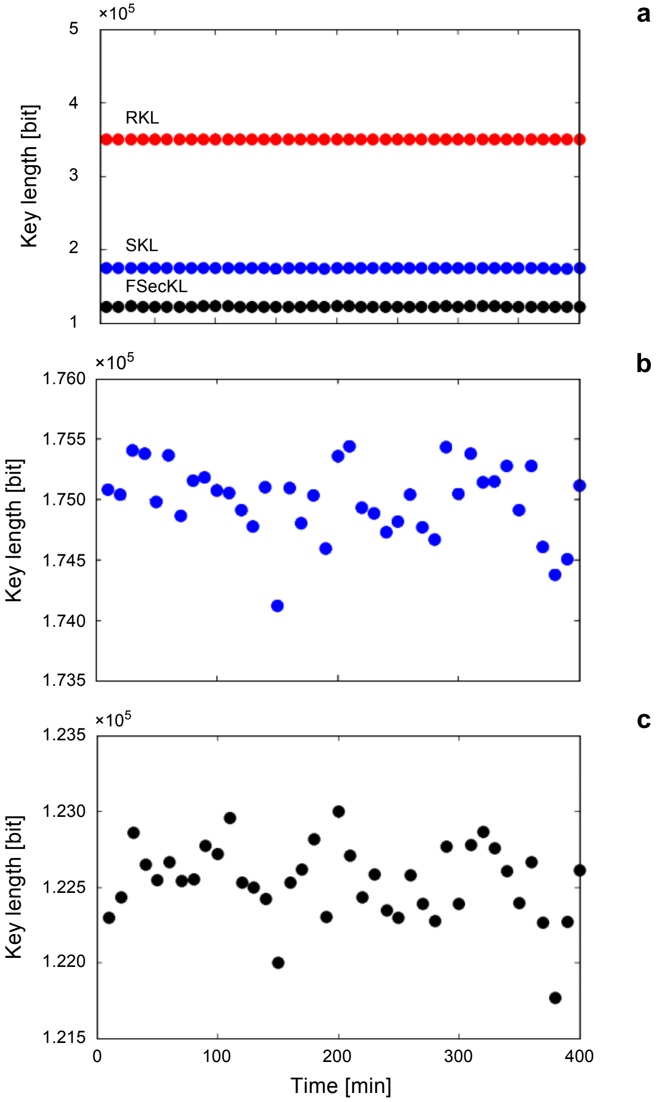

Fig. 2. Measurements of RKL, SKL and FSecKL (**a**). Detailed measurements of SKL (**b**) and FSecKL (**c**).

do not affect the security level of the complete system because this security level is based on the RK true randomly.

3. Experimental results and analysis

Figure 2**a** shows the raw key length (RKL) measurements transmitted by *Alice* with a final result of 350 Kb (kilobits). Therefore and considering the BB84 protocol, the sifted key length (SKL) was ~175 Kb as shown in Fig. 2**b**. Also, Fig. 2**c** shows the final secret key length (FSecKL) with final value ~122 Kb. The RKL, SKL and FSecKL measurements allow to calculate the SKR and the FSecKR considering the processing time of the COTS device used.

Figure 3**a** shows the performance of the SKR using/not using the DB-RN. In particular, when the system uses the DB-RN on both sides (*i.e.*, *Alice* and *Bob* stored the RSA1 and RSB1 previously), the SKR is ~61 Kbps; instead, the SKR is ~29 Kbps when the random sequences are used in real time. Thus, when the random sequences are not stored in the respective DB-RN, the COTS device requires more processing time to read the input port, processing, temporarily storing and sending the random sequence to the PM's driver. In addition, the digital processing time of the digital

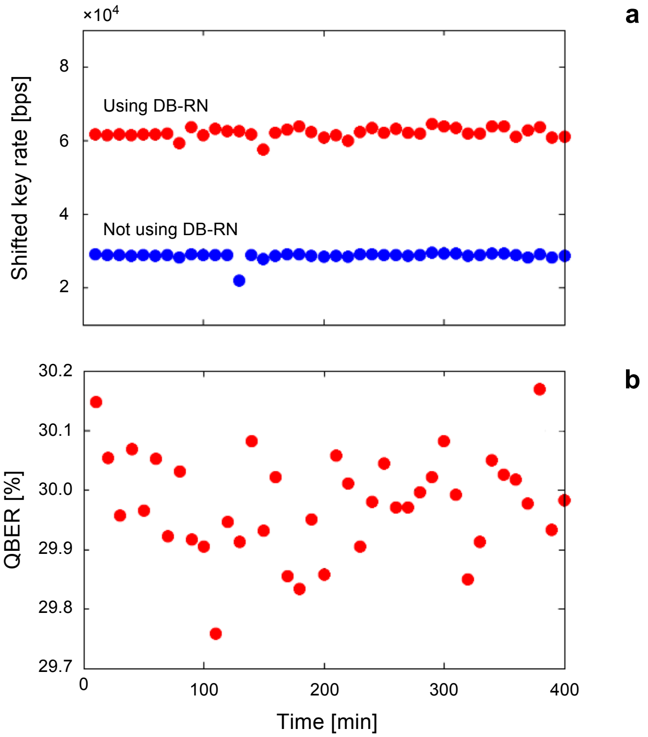

Fig. 3. Results of SKR with/without using a DB-RN (**a**). Results of the QBER of the SK (**b**).

subsystem of the TRNG is considered in the overall delay. Therefore, the using of the DB-RN adds ~32 Kbps to the final SKR, equivalent to reduce ~52.45% of the processing time.

Next, the QBER is measured each 10 minutes using the sifted key (SK) in a total analysis time of 400 minutes as shows the Fig. 3**b**. In particular, the QBER ~30% in both cases (using and not using the DB-RN); making sure that the security level is not affected by the processes corresponding to the use of the DB-RN. The QBER measurements are conducted according to the mathematical model of the reception scheme used, described as QBER = $0.5\mathrm{erfc}\sqrt{2\eta\mu}$), where η is the efficiency that involves the channel and overall system efficiencies ($\eta \approx 0.7$) and $\mu = [0.25, 5]$ is the average photons per pulse considering a Poisson distribution. Figure 4**a** shows the QBER theoretical results and the upper and lower limits in terms of the QBER for two different cases, $N_s = 0.25$ and $N_s = 0.5$. Such limits were established in a strict way based on the QBER performance showed in Fig. 3**b**. Therefore, the security threshold is ±16.5% (*i.e.*, any variation of the QBER greater than the security threshold will be considered as generated by a spy in the private channel). Using the threshold mentioned, the specific values allowed that the QBER = [25%, 35%] and [10%, 20%] for $N_s = 0.25$ and $N_s = 0.5$, re-

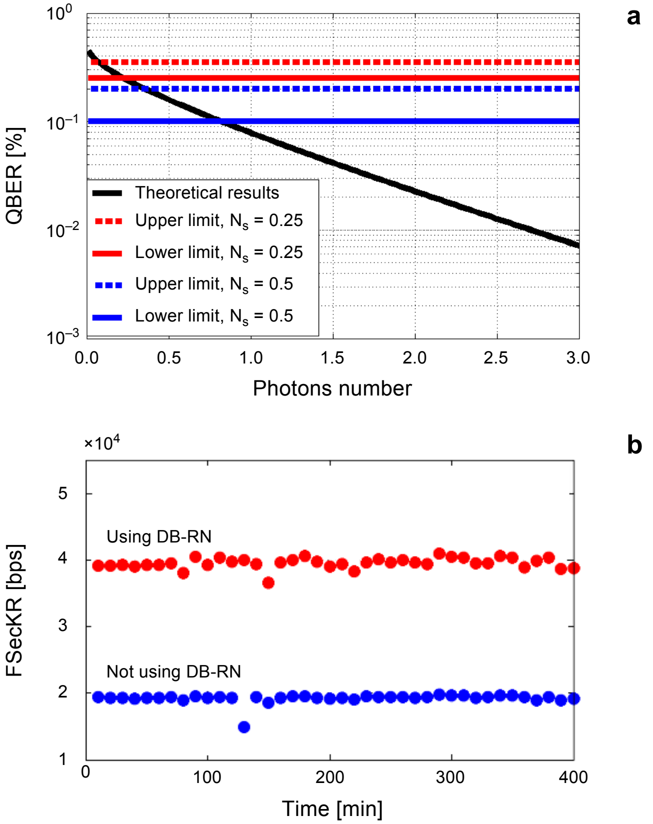

Fig. 4. Security threshold for different photons number (**a**). Experimental results of the FSecKR (**b**).

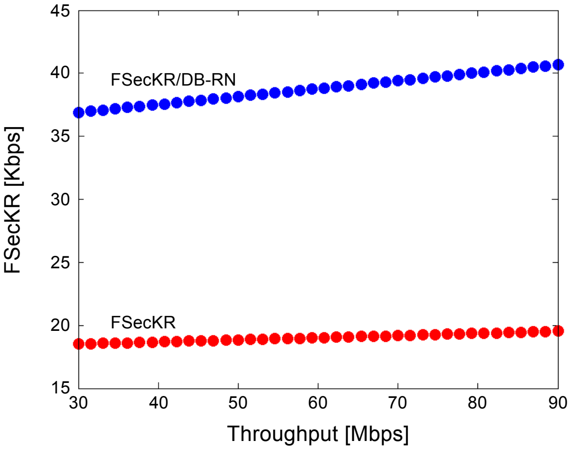

Fig. 5. Final secret key rate measurements for different throughputs.

spectively. Finally, Fig. 4**b** shows the experimental FSecKR using/not using the DB-RN. In particular, the FSecKR/DB-RN is ~39.5 Kbps and the FSecKR/DB-RN (without using the DB-RN) is ~19.5 Kbps.

Lastly, the performance of the FSecKR/DB-RN and FSecKR parameters for different throughputs (*i.e.*, considering the real variation of the network traffic) is shown in Fig. 5. The figure shows that the FSecKR/DB-RN is ~40 Kbps with the higher throughput (~90 Mbps) in the network in specific interval time; however, the FSecKR/DB-RN is reduced to ~36 Kbps for the lower throughput measured (~30 Mbps). Besides, the FSecKR is ~20 and ~18 Kbps for the higher and lower throughput, respectively. Basically, the variation of the FSecKR is due to the processing time required for the digital processor in order to perform the complete protocol and in addition, it is due to the throughput in the real networks in order to perform the quantum protocol used. Therefore, the relationship between the FSecKR and the throughput of the classical channel is extremely important for the complete performance of the QKD system.

4. Conclusions

A CV-QKD system based on a simplified quantum protocol and COTS devices in a real traffic network was successfully emulated in this work. Although the FSecKR/DB-RN performance (from about 36 to 40 Kbps) was calculated considering a real LAN with variable throughput (from about 30 to 90 Mbps), the measurements are highly adaptable for the wide area networks (WAN). Since the optical power received is related to different losses associated with both long distance channels (the atmospheric channel and optical fiber), the results may be easily adapted to other kind of classical communication links (radio frequency, copper cables, among others). The results show the advantage of using an external TRNG and a DB-RN in order to increase the FSecKR, although avoiding the use of a DB-RN permits measurements (FSecKR) from about

18 to 20 Kbps. These results are still adequate considering the general trade-off between the security level and the FSecKR. In general, the proposed system showed a better FSecKR performance than the available commercial systems when a fixed attenuation was considered (*i.e.*, free space link with fixed distance). Nevertheless, the commercial systems have shown results considering variable distances [17–19]. Therefore, an analysis of the FSecKR/DB-RN for different attenuations has to be made in future work, although the 0.25 photons per pulse achieved in our system may represent a long-distance link (considering that the atmospheric turbulence and other perturbations may affect the signal in a free space channel). The performance of the proposed system was achieved without the use of advanced and expensive digital processing devices and based just on a simplified quantum protocol. Clearly, the use of a not simplified quantum protocol (as in the commercial systems which make use of advanced digital devices) implemented in COTS devices, imposes an important restriction. In particular, the QBER was measured each 10 minutes based on the RK truly random; therefore the final secret key must be updated at the same time. However, the update time value of the final quantum key can be decreased up to update time values of commercial systems in a practical way. Finally, as mentioned earlier, although the use of the DB-RN does not affect the QBER, a side channel attack analysis should be made in order to ensure the security level [20].

References

[1] Takeoka M., Guha S., Wilde M.M., *Fundamental rate-loss tradeoff for optical quantum key distribution*, Nature Communications **5**, 2014, article ID 5235.

[2] Feihu Xu, Curty M., Bing Qi, Li Qian, Hoi-Kwong Lo, *Discrete and continuous variables for measurement-device-independent quantum cryptography*, Nature Photonics **9**, 2015, pp. 772–773.

[3] Lam P.K., Ralph T.C., *Quantum cryptography: continuous improvement*, Nature Photonics **7**, 2013, pp. 350–352

[4] Timofeev A.V., Molotkov S.N., *On the privacy-preserving cascade method for correcting errors in primary keys in quantum cryptography*, Journal of Experimental and Theoretical Physics Letters **82**(12), 2005, pp. 768–772

[5] Al-Daoud E., *Comparing two quantum protocols: BB84 and SARG04*, European Journal of Scientific Research **17**(1), 2007, pp. 25–30.

[6] Hamrick G., *Secrecy, computational loads and rates in practical quantum cryptography*, Algorithmica **34**(4), 2002, pp. 314–339.

[7] Dixon A.R., Sato H., *High speed and adaptable error correction for megabit/s rate quantum key distribution*, Scientific Reports **4**, 2014, article ID 7275.

[8] Hong-Fei Zhang, Jian Wang, Ke Cui, Chun-Li Luo, Sheng-Zhao Lin, Lei Zhou, Hao Liang, Teng-Yun Chen, Kai Chen, Jian-Wei Pan, *A real-time QKD system based on FPGA*, Journal of Lightwave Technology **30**(20), 2012, pp. 3226–3234.

[9] Zhang Q., Takesue H., Honjo T., Wen K., Hirohata T., Suyama M., Takiguchi Y., Kamada H., Tokura Y., Tadanaga O., *Megabits secure key rate quantum key distribution*, New Journal of Physics **11**, 2009, article ID 045010.

[10] Fujiwara M., Ishizuka H., Miki S., Yamashita T., Wang Z., Tanaka A., Yoshino K., Nambu Y., Takahashi S., Tajima A., Tomita A., Hasegawa T., Tsurumaru T., Matsui M., Honjo T., Tamaki K., Tokura Y., Sasaki M., *Field demonstration of quantum key distribution in the Tokyo QKD Network*, International Quantum Electronics Conference, Sydney, Australia, 2011.

[11] Jakobi M., Simon C., Gisin N., Bancal J-D., Branciard C., Walenta N., Zbinden H., *Practical private database queries based on a quantum-key-distribution protocol*, Physical Review A **83**(2), 2011, article ID 022301.

[12] Panduranga Rao M.V., Jakobi M., *Towards communication-efficient quantum oblivious key distribution*, Physical Review A **87**(1), 2013, article ID 012331.

[13] Zhiyuan Tang, Zhongfa Liao, Feihu Xu, Bing Qi, Li Qian, Hoi-Kwong Lo, *Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution*, Physical Review Letters **112**(19), 2014, article ID 190503.

[14] Duligall J.L., Godfrey M.S., Harrison K.A., Munro W.J., Rarity J.G., *Low cost and compact quantum key distribution*, New Journal of Physics **8**, 2006, article ID 249.

[15] Lopez Leyva J.A., Arvizu-Mondragón A., *Simultaneous dual true random numbers generator*, DYNA **83**(195), 2016, pp. 93–98.

[16] Lopez Leyva J.A., Arvizu Mondragón A., García E., Mendieta F.J., Alvarez Guzman E., Gallion P., *Detection of phase-diffused weak-coherent-states using an optical Costas loop*, Optical Engineering **51**(10), 2012, article ID 105002.

[17] Jouguet P., Kunz-Jacques S., Leverrier A., Grangier P., Diamanti E., *Experimental demonstration of continuous-variable quantum key distribution over 80 km of standard telecom fiber*, Conference on Lasers and Electro-Optics (CLEO), San Jose, CA, USA, 2013.

[18] *Cygnus: State-of-the-art CVQKD module*, http://sequrenet.com/datasheets/datasheet_cygnus.pdf, 2016.

[19] *Clavis the most versatile quantum key distribution research platform*, http://marketing.idquantique.com/acton/attachment/11868/f-00a0/1/-/-/-/-Clavis%20QKD%20Datasheet.pdf, 2016.

[20] Scarani V., Bechmann-Pasquinucci H., Cerf N., Dušek M., Lütkenhaus N., Peev M., *The security of practical quantum key distribution*, Reviews of Modern Physics **81**(3), 2009, pp. 1301–1350.

Received November 29, 2016
in revised form December 29, 2016