European Conference on Optical Communication (ECOC) 2022 © Optica Publishing Group 2022

Practical Network Encryption with Quantum Cryptographic Keys

Nitin Jain[1, †], Erik Bidstrup[2], Hou-Man Chin[1], Hossein Mani [1], Adnan A.E. Hajomer [1], Ulrik L. Andersen [1], Tobias Gehring [1,*]

[1] Center for Macroscopic Quantum States (bigQ), Department of Physics, Technical University of Denmark, 2800 Kongens Lyngby, Denmark, † nitinj@iitbombay.org * tobias.gehring@fysik.dtu.dk
[2] Zybersafe ApS, Erik Husfeldts Vej 7, Denmark

Abstract *We present a state-of-the-art continuous-variable quantum cryptographic prototype that operates at 1550 nm and distributes keys across a 10 km fiber channel to network encryptors operating at 1300 nm and using the same (wavelength-multiplexed) channel for data link layer encryption. ©2022 The Author(s)*

Introduction

Quantum cryptography is a method for solving the cryptographic problem of secure distribution of keys to users connected by an optical channel, which can be fully controlled by an adversary[1],[2]. The users, frequently called Alice and Bob, establish quantum correlations via preparation and measurement of quantum states propagating on the channel, and then try to distill a secret key from these correlations through classical data processing. In an ideal case, the adversary Eve, who tries to get information of the secret key, either fails (except with some small probability ϵ) in her attempts, or her presence gets disclosed to Alice and Bob, who can then abort the subsequent encryption and transmission of the confidential data. In other words, under the adversarial threat model of concealed eavesdropping, Eve remains a loser.

Continuous-variable quantum key distribution (CVQKD) is a quantum cryptographic method where the secret key information is coded in continuously valued properties such as the electromagnetic quadratures of the optical field[1]–[5]. The preparation and measurement of so-called optical coherent states, described by an amplitude quadrature value I and phase quadrature value Q, leverages standard telecommunication equipment, most notably in-phase and quadrature (IQ) modulators and heterodyne detectors.

An essential ingredient of any CVQKD system is a local oscillator (LO), typically several times stronger than the prepared (or measured) quantum signal. Alice and Bob employ a LO for sharing a common phase reference. The usage of a LO makes CVQKD similar to coherent optical communications. Moreover, the compatibility of fiber-optic CVQKD implementations with existing telecom technology, such as wavelength division multiplexing (WDM), makes them a suitable candidate for deployment in the secure communication infrastructure, i.e., for encryption of classical data traffic. A recent demonstration[6] has experimentally verified secret key generation through CVQKD signals co-propagating with 100 WDM coherent data channels.

However, the reported CVQKD system was based on a *transmitted* LO (TLO) design, i.e., where Alice transmits the LO together with the prepared quantum states on the channel to Bob. Implementing TLO-based CVQKD schemes requires constructing fairly complex setups to prevent crosstalk from the ‘strong’ LO to the ‘quite weak’ quantum signal. Furthermore, they also suffer from security issues[7],[8].

The alternative of deploying a *local* LO (LLO) for coherent detection has gained traction since its inception in 2015[10]–[15]. The task of distributing the phase reference is delegated to pilot tones or reference pulses, that have higher power than the quantum signal but are weaker than the LO[1]. LLO design eases the optical setup complexity and prevents security loopholes, though stabilizing phase fluctuations becomes a challenge. However, this can be tackled using digital signal processing (DSP) techniques, specially those employing machine learning frameworks[13],[15].

In this paper, we present a LLO-aided CVQKD system operating at 1550 nm that generates and provides secret keys for symmetric encryption and decryption to a pair of hardware/network encryptors, operating at wavelengths ∼1300 nm. Using a pair of coarse WDMs (CWDMs), the 1550 nm quantum communication is multiplexed to the 1300 nm classical optical communication on the same 10 km long fiber channel. We are able

[1] Typical ratio of the LO [pilot tone] power to quantum signal power varies in the $50-80$ $[5-30]$ dB range[12]–[15].

Disclaimer: Preliminary paper, subject to publisher revision

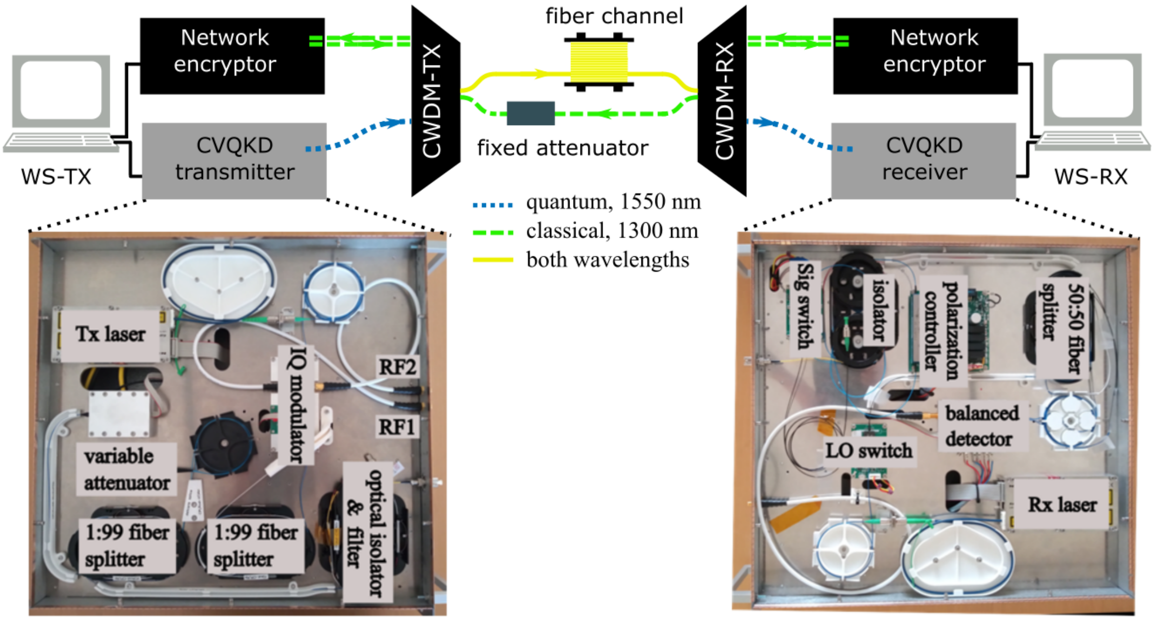

Fig. 1: Experimental scheme and details of the continuous-variable quantum key distribution system. The scheme is described in the main text. We use dashed-green, dotted-blue or solid-yellow lines, with single/pair indicating simplex/duplex, to depict fiber-optic connections. Both the transmitter and receiver boxes comprise a solid plate with the optical/optoelectronic components on one side (as shown) and the necessary control electronics on the other. *CVQKD transmitter*: The output of a 1550 nm CW laser (Tx laser) is fed to an IQ modulator, biased for performing carrier suppression and single sideband modulation[9]. A variable attenuator sets the modulation strength of the quantum signal to a desired level. The wavelength filter and isolator are for prevention of Trojan-horse attacks. *CVQKD receiver*: With the optical Sig switch in ON state, the incoming signal passes through a polarization controller so that it's polarization can be tuned to match that of the LLO, which is generated by the Rx laser (same type as Tx laser). A symmetric beam splitter followed by a homemade balanced detector performs radio-frequency (RF) heterodyne detection. TX: transmitter, RX: receiver, WS: workstation, CWDM: coarse wavelength division multiplexer.

to generate secret keys with lengths $l = 0.40 \pm 0.09$ Mbits per QKD run, which takes around 1 hour. The generated secret key bits are used to secure a confidential datastream using the 256-bit advanced encryption standard (AES).

Experimental scheme & implementation

Figure 1 illustrates the complete experimental scheme while Fig. 2(a) shows a photo with the actual implementation. The CVQKD system is capable of working semi-autonomously: it performs the entire state preparation, measurement, and classical data processing (including the secret key generation) without any user intervention. For instance, remotely controlled optical (Sig and LO) switches inside the CVQKD receiver allow frequent and independent shot noise calibration, a crucial part of state measurement.

A system on a chip acts as the central computer for controlling and monitoring the various hardware, and PCI Express based digital-to-analog converter (DAC) and analog-to-digital converter (ADC) cards inside two workstations (WS-TX and WS-RX) are used for IQ modulation and heterodyne output acquisition, respectively[16]. Notably, we use frequency-multiplexed pilot tones and a quadrature phase shift keying alphabet with a known header for the sake of digital synchronization of TX and RX[17].

The hardware encryption devices are commercially available from Zybersafe[18], and off-the-shelf 100G QSFP28 LR4 modules were hot-plugged for transmitting and receiving the encrypted data. Since QSFP28 LR4 operates in full-duplex mode (dashed-green line pairs in Fig. 1), we used a fixed attenuator that roughly matched the attenuation of the 10 km fiber for the reverse (right to left) communication path. The hardware encryptors require the AES keys to be refreshed every 2 minutes or after a maximum of 2^{32} frames. For 100G traffic, a frame size of 864 bits translates to requiring 14 bits/sec from the CVQKD system, which can supply > 70 bits/sec.

Figure 2(a) shows a standard 19" telecom rack containing our CVQKD system, the network encryption devices, the CWDMs, and the two workstations housing the ADC and DAC cards.

Results

After the state preparation and measurement, Alice and Bob performed error reconciliation to obtain uniformly correlated data for both quadratures, after which they estimated the channel parameters. This parameter estimation (PE) step

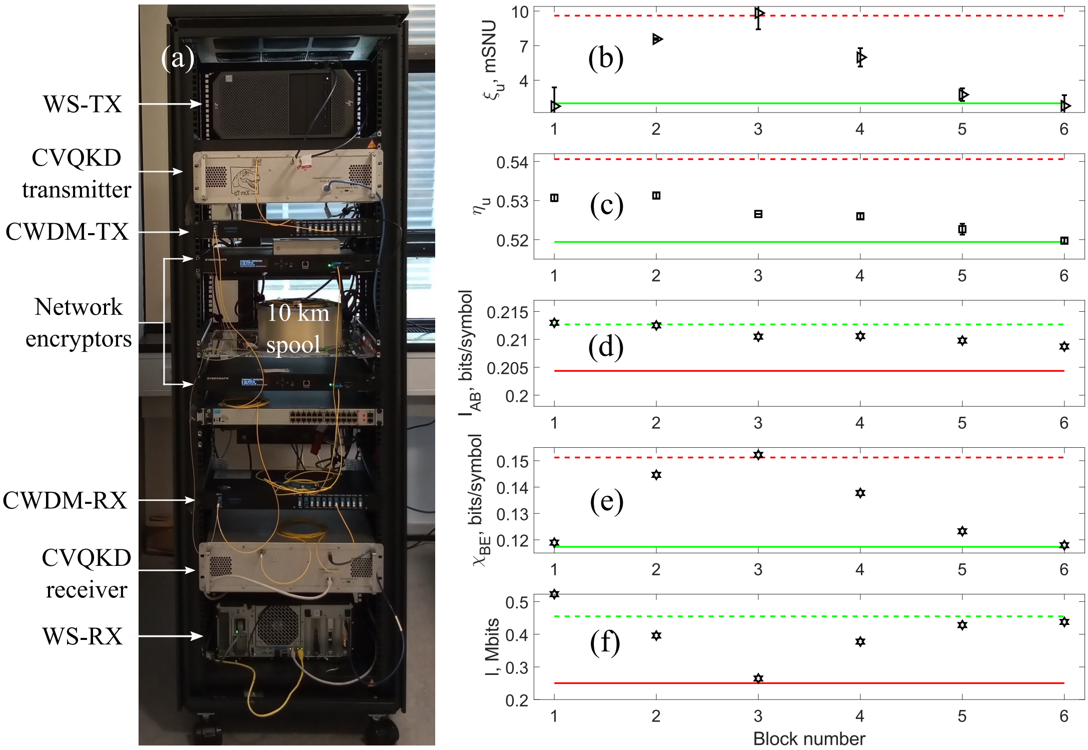

Fig. 2: Installed setup and experimental results. (a) The CVQKD transmitter and receiver are housed in two standard 19" boxes of 3U. The workstations communicate with them on Ethernet, and with the network encryptors via USB. All fiber-optic equipment is connected using LC cables. A 10 km long single mode fiber spool and a fixed attenuator are connected to the COM ports of both the CWDMs using two simplex LC cables; see Fig. 1. (b)-(f) Various results from the parameter estimation procedure. Trusted components $\xi_t = 0.022$ SNU and $\eta_t = 0.32$ were obtained through calibration[19], and reconciliation efficiency $\beta = 0.95$.

yielded the loss and noise that can be attributed to the channel[2], and from which the secret key length was calculated using,

$$l = N_s \left(\beta I_{AB} - \chi_{BE}\right), \tag{1}$$

in the asymptotic regime and assuming collective attacks by Eve[2],[5]. Here N_s denotes the number of exchanged coherent states, β is the reverse reconciliation efficiency, I_{AB} is the mutual information between Alice and Bob, and χ_{BE} bounds Eve's Holevo information[4].

Figures 2(b)–(f) show various results obtained after PE on a set of 6 data blocks ($N_s \approx 5.5 \times 10^6$ per block) processed and analyzed from the experiment. After calibrating the contributions from the CVQKD system itself, the overall noise ξ and loss η is partitioned into *untrusted* and *trusted* components; Figs. 2(b) and (c) show only the untrusted components ξ_u and η_u, respectively.

The solid-green [dashed-red] traces in (b) and (c) indicate the minimum [maximum] ξ_u and η_u values, respectively, measured in another experiment *without classical signals*, i.e., with only the quantum communication link active. With these parameter ranges, we simulated the lower and upper limits of I_{AB} and χ_{BE}, shown by the solid and dashed traces in Fig. 2(d) and (e); the color green [red] indicates a regime favorable to Alice-Bob [Eve]. Most of the corresponding experimental data points are within these limits, underscoring that the classical communication does not adversely affect the QKD link performance. Finally, Fig. 2(f) shows the distilled secret key length.

Conclusion

In conclusion, we have reported a wavelength-multiplexed setup comprising of a semi-autonomous local LO-based continuous-variable quantum cryptographic system at 1550 nm and commercial network encryption devices at 1300 nm for successfully generating keys and encrypting messages over a 10 km channel.

Acknowledgements

We acknowledge support from Innovation Fund Denmark (CryptQ project, grant agreement no. 0175-00018A) and the Danish National Research Foundation, Center for Macroscopic Quantum States (bigQ, DNRF142). We would also like to thank Danish e-infrastructure Cooperation (DeiC) for the equipment loan.

[2] In CVQKD, optical loss is generally expressed as a transmittance η, while the noise ξ is conveyed as whatever is in excess of shot noise in a relative sense, i.e., in shot noise unit (SNU) by normalizing w.r.t. the shot noise variance.

References

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution", *Reviews of Modern Physics*, vol. 81, no. 3, pp. 1301–1350, 2009. DOI: 10.1103/RevModPhys.81.1301. arXiv: 0802.4155.

[2] S. Pirandola, U. L. Andersen, L. Banchi, *et al.*, "Advances in quantum cryptography", *Advances in Optics and Photonics*, vol. 12, no. 4, p. 1012, 2020, ISSN: 1943-8206. DOI: 10.1364/AOP.361502. arXiv: 1906.01645. [Online]. Available: http://arxiv.org/abs/1906.01645%20http://dx.doi.org/10.1364/AOP.361502%20https://www.osapublishing.org/abstract.cfm?URI=aop-12-4-1012.

[3] T. C. Ralph, "Continuous variable quantum cryptography", *Phys. Rev. A*, vol. 61, p. 010 303, 1 1999. DOI: 10.1103/PhysRevA.61.010303. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.61.010303.

[4] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using gaussian-modulated coherent states", *Nature*, vol. 421, no. 6920, pp. 238–241, 2003, ISSN: 0028-0836. DOI: 10.1038/nature01289. [Online]. Available: https://www.nature.com/articles/nature01289%20http://www.nature.com/articles/nature01289.

[5] E. Diamanti and A. Leverrier, "Distributing secret keys with quantum continuous variables: Principle, security and implementations", *Entropy*, vol. 17, no. 9, pp. 6072–6092, 2015, ISSN: 10994300. DOI: 10.3390/e17096072. arXiv: 1506.02888.

[6] T. A. Eriksson, T. Hirano, B. J. Puttnam, *et al.*, "Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 Tbit/s data channels", *Communications Physics*, vol. 2, no. 1, p. 9, 2019, ISSN: 2399-3650. DOI: 10.1038/s42005-018-0105-5. [Online]. Available: http://www.nature.com/articles/s42005-018-0105-5.

[7] H. Häseler, T. Moroder, and N. Lütkenhaus, "Testing quantum devices: Practical entanglement verification in bipartite optical systems", *Physical Review A*, vol. 77, no. 3, p. 032 303, Mar. 2008, ISSN: 1050-2947, 1094-1622. DOI: 10.1103/PhysRevA.77.032303. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.77.032303 (visited on 01/14/2022).

[8] X.-C. Ma, S.-H. Sun, M.-S. Jiang, and L.-M. Liang, "Local oscillator fluctuation opens a loophole for Eve in practical continuous-variable quantum-key-distribution systems", en, *Physical Review A*, vol. 88, no. 2, p. 022 339, Aug. 2013, ISSN: 1050-2947, 1094-1622. DOI: 10.1103/PhysRevA.88.022339. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.88.022339 (visited on 01/14/2022).

[9] N. Jain, I. Derkach, H. M. Chin, *et al.*, "Modulation leakage vulnerability in continuous-variable quantum key distribution", *Quantum Science and Technology*, vol. 6, no. 4, 2021, ISSN: 20589565. DOI: 10.1088/2058-9565/ac0d4c.

[10] B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, "Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection", *Physical Review X*, vol. 5, no. 4, pp. 1–12, 2015, ISSN: 21603308. DOI: 10.1103/PhysRevX.5.041009. arXiv: 1503.00662.

[11] D. B. S. Soh, C. Brif, P. J. Coles, *et al.*, "Self-referenced continuous-variable quantum key distribution protocol", *Physical Review X*, vol. 5, no. 4, pp. 1–15, 2015, ISSN: 21603308. DOI: 10.1103/PhysRevX.5.041010. arXiv: 1503.04763.

[12] D. Huang, P. Huang, D. Lin, C. Wang, and G. Zeng, "High-speed continuous-variable quantum key distribution without sending a local oscillator.", *Optics letters*, vol. 40, no. 16, pp. 3695–8, 2015, ISSN: 1539-4794. DOI: 10.1364/OL.40.003695. [Online]. Available: http://www.osapublishing.org.proxy.findit.dtu.dk/viewmedia.cfm?uri=ol-40-16-3695%7B%5C&%7Dseq=0%7B%5C&%7Dhtml=true.

[13] S. Kleis, M. Rueckmann, and C. G. Schaeffer, "Continuous variable quantum key distribution with a real local oscillator using simultaneous pilot signals", *Optics Letters*, vol. 42, no. 8, pp. 1588–1591, 2017. [Online]. Available: https://doi.org/10.1364/OL.42.001588.

[14] H. Wang, Y. Pi, W. Huang, *et al.*, "High-speed Gaussian-modulated continuous-variable quantum key distribution with a local local oscillator based on pilot-tone-assisted phase compensation", *Optics Express*, vol. 28, no. 22, p. 32 882, 2020, ISSN: 1094-4087. DOI: 10.1364/OE.404611. [Online]. Available: https://www.osapublishing.org/abstract.cfm?URI=oe-28-22-32882.

[15] H.-M. Chin, N. Jain, D. Zibar, U. L. Andersen, and T. Gehring, "Machine learning aided carrier recovery in continuous-variable quantum key distribution", *npj Quantum Information*, vol. 7, no. 1, p. 20, 2021, ISSN: 2056-6387. DOI: 10.1038/s41534-021-00361-x. arXiv: 2002.09321. [Online]. Available: http://dx.doi.org/10.1038/s41534-021-00361-x%20http://www.nature.com/articles/s41534-021-00361-x.

[16] N. Jain, H.-M. Chin, H. Mani, E. Bidstrup, U. L. Andersen, and T. Gehring, *qTReX : A semi-autonomous continuous-variable quantum key distribution system*, More information at https://www.ofcconference.org/en-us/home/eposters/poster/?id=3689698. [Online]. Available: https://www.ofcconference.org/en-us/home/program-speakers/demo/.

[17] H.-M. Chin, N. Jain, U. L. Andersen, and T. Gehring, "Digital synchronization for continuous-variable quantum key distribution", *(to be submitted to Physical Review X Quantum)*, 2022. arXiv: 2203.08486. [Online]. Available: https://arxiv.org/abs/2203.08486.

[18] *Datasheet Zybersafe TrafficCloak â Ethernet Encryption*, https://zybersafe.com/wordpress/wp-content/uploads/2019/11/Zybersafe-Data-Sheet.pdf, Accessed: 2021-11-15.

[19] N. Jain, H.-M. Chin, H. Mani, *et al.*, "Practical continuous-variable quantum key distribution with composable security", *arXiv:2110.09262*, 2021. arXiv: 2110.09262. [Online]. Available: http://arxiv.org/abs/2110.09262.